RINGS OF INVARIANTS OF FINITE GROUPS

JACK JEFFRIES

These are lecture notes and exercises for a short graduate lecture series on invariant theory for the summer school Recent Developments in Commutative Algebra at IIT Dharwad in 2025. This course has three 90 minute lectures and two problem sessions of 60 minutes each. The first lecture will focus on some basic terminology, results, and examples about rings of invariants of finite groups. The second lecture will discuss polynomial invariant rings and separating sets. The third lecture will discuss Cohen-Macaulay invariant rings and local cohomology.

References for these notes include the books of Benson [?], Campbell and Wehlau [?], and Derksen and Kemper [?] the survey articles of Hochster [?] and Stanley [?], and the recent paper of Goel-Jeffries-Singh [?].

1. Rings of invariants of finite groups

Throughout these lectures, K is a field, and $S = K[x_1,\dots,x_n]$ is a polynomial ring in n variables over K.

Linear actions on polynomial rings. Let G be a finite group, K a field, and V be a finite dimensional vector space. Recall that a (left) ***representation*** of G on V is a (left) group action such that for each $g \in G$, the map $V \xrightarrow{g} V$ is K-linear; i.e., given a basis of $V \cong K^n$, we have

$$V \xrightarrow{g} V \quad v \longmapsto A_g v$$

for some matrix A_g. Any subgroup of $\mathrm{GL}(V)$ has a natural representation as such: elements of $\mathrm{GL}(V)$ tautologically act on V by linear transformations.

Given a representation of G on V, there is an induced representation of G^{op} on $V^\star$, the space of linear forms, by the rule $g(\ell)(v) = \ell(g(v))$; equivalently, we can think of this as a right representation of G on V. The oppositeness comes from the fact that dualizing is contravariant. To fix this, we consider the left action by the rule $g(\ell)(v) = \ell(g^{-1}(v))$ instead. This gives the same collection of endomorphisms of $V^\star$, this way we still get a left action.

Explicitly, equip $V = K^n$ with the standard basis, take $x_1,\dots,x_n$ the dual basis of $V^\star$, and let $A_g$be the matrix of the action of g on K^n. Then the matrix of g on $V^\star$ in this basis is $(A_g^T)^{-1}$: the transpose arises from the acting on the forms, and the inverse from our choice of using g^{-1} instead of g.

Given the vector space V, we have the space of linear forms $V^\star$, and taking the symmetric algebra of $V^\star$, one has the ring of polynomial functions $K[V] = \mathrm{Sym}(V^\star)$ on V. Explicitly, if $V^\star = K\{x_1,\dots,x_n\}$, then $K[V]$ is the polynomial ring $K[x_1,\dots,x_n]$. Any K-linear endomorphism of $V^\star$ (or of V) determines a degree preserving K-algebra automorphism of $K[V]$ simply because this is a polynomial ring in a basis for $V^\star$. Conversely, any degree-preserving K-algebra automorphism of $K[V]$ arises from a unique K-linear endomorphism of $V^\star$ (or of V) in this way: one restricts to the degree-one piece of $K[V]$ (or its dual).

Thus, given a representation of G on V, then one gets a left action of G on $K[V]$ by degree-preserving K-algebra homomorphisms, and every such action of G on a polynomial ring S

arises in this way. We say G acts ***linearly*** on a polynomial ring S to mean that G acts by degree-preserving K-algebra homomorphisms. For a linear action of G on S, we take V to be the dual of S_1, the space of one-forms.

For a linear action of G on $S = K[x_1, \dots, x_n]$, one also gets an action of G on the space of maximal ideals on S by $g \cdot \mathfrak{m} = g^{-1}(\mathfrak{m})$; here g^{-1} means preimage. Among these are the K-rational points

$$\mathfrak{m}_v = \{f \in S \mid f(v) = 0\} = (x_1 - v_1, \dots, x_n - v_n)$$

for some $v \in V \cong K^n$; if K is algebraically closed, these are all of the maximal ideals. Then

$$f \in g^{-1}(\mathfrak{m}_v) \Longleftrightarrow f(g(v)) = 0 \Longleftrightarrow f \in \mathfrak{m}_{g(v)},$$

so the action of G on the space of K-rational points is, up to swapping inverses, exactly the same as the action of G on V.

Given a linear action of G on S, an element $f \in S$ is ***invariant*** if $g(f) = f$ for all $g \in G$. The ***ring of invariants*** is the subring of S consisting of all invariant elements, denoted S^G. We note two easy observations about S^G: first, it is a K-algebra, since linear actions are K-algebra automorphisms. Second, it is a graded K-subalgebra of S: if $f = f_0 + \cdots + f_n \in S^G$ is the homogeneous decomposition of f, then since the action of G is degree-preserving, the homogeneous decomposition of $g(f)$ is $g(f_0) + \cdots + g(f_n)$, so if $f \in S^G$, so is each f_i.

We will often specify the linear action

Examples of invariant rings.

Example 1.1. Let K be a field of characteristic not equal to 2, and let $G = \mathbb{Z}/2 = \{e, g\}$ act on K^n by $g(v) = -v$. Then for $S = K[V] = K[x_1, \dots, x_n]$, one has $g(x_i) = -x_i$ for all i. Note that f is invariant if and only if $g(f) = f$ in this case. Then for any homogeneous element $f \in S$, one has $g(f) = (-1)^{\deg(f)} f$. Writing a general polynomial

$$f = f_0 + f_1 + \cdots + f_n$$

as a sum of its homogeneous components, we have

$$g(f) = f_0 - f_1 + f_2 - \cdots + (-1)^n f_n$$

and $g(f) = f$ if and only if every homogeneous component has even degree. In this case, we can easily write down generators for S^G as a K-algebra, namely, S^G is generated by all monomials of degree two:

$$S^G = K[x_1^2, x_1x_2, \dots, x_n^2].$$

Example 1.2. Let $G = \mathfrak{S}_n$ be the symmetric group on n letters, and let G act on $V = K^n$ by permuting the standard basis. Then G acts on $S = K[V]$ by

$$g(x_i) = x_{g(i)}.$$

The invariant polynomials are called symmetric polynomials. We claim that the ring of symmetric polynomials is generated as a K-algebra by the elementary symmetric polynomials

$$e_1 = \sum_i x_i, \ e_2 = \sum_{i<j} x_i x_j, \ \dots, \ e_n = x_1 \cdots x_n.$$

To prove it, suppose to the contrary that there is some homogeneous invariant f not in $K[e_1, \dots, e_n]$. Order the monomials in S lexicographically, and consider the leading monomial of f.

We claim that there is some $h \in K[e_1, \ldots, e_n]$ with the same leading monomial as f. Indeed, note that the leading monomial of f must be of the form $x_1^{a_1} \cdots x_n^{a_n}$ with $a_1 \geq \cdots \geq a_n$, since any permutation of the a's gives another monomial of f. Then $h = e_n^{a_n} e_{n-1}^{a_{n-1}-a_n} \cdots e_1^{a_1-a_2}$ does the job.

Thus, $f - h$ is an element of the same degree that is not in $K[e_1, \ldots, e_n]$, but with a smaller leading monomial in the lexicographic order. Since there are finitely many monomials of a given degree, one can repeat this finitely many times to get a contradiction.

Example 1.3. Let $G = \mathfrak{A}_n$ be the alternating group on n letters, and let G act on $V = K^n$ by permuting the standard basis. Then $\mathfrak{A}_n$ acts linearly on $S = K[x_1, \ldots, x_n]$ by the rule

$$g(x_i) = x_{g(i)}.$$

For convenience, let's assume that K has characteristic other than 2. Clearly $S^{\mathfrak{S}_n} \subseteq S^{\mathfrak{A}_n}$. An additional invariant of interest is the discriminant

$$\Delta = \prod_{i<j} (x_i - x_j).$$

We claim that

$$S^{\mathfrak{A}_n} = K[e_1, \ldots, e_n, \Delta].$$

To see this, note first that Δ^2 is a symmetric polynomial, and hence an element of $K[e_1, \ldots, e_n]$. Thus, we can write $K[e_1, \ldots, e_n, \Delta] = K[e_1, \ldots, e_n] \oplus K[e_1, \ldots, e_n] \cdot \Delta$. Now, the action of $\mathfrak{S}_n$ on S restricts to an action on $S^{\mathfrak{A}_n}$, and since $\mathfrak{A}_n$ acts trivially on $S^{\mathfrak{A}_n}$, we get an induced action of $\mathbb{Z}/2 \cong \mathfrak{S}_n/\mathfrak{A}_n$ on $S^{\mathfrak{A}_n}$. We can decompose this as a direct sum of the $+1$ eigenspaces and -1 eigenspaces since the characteristic is not two. The $+1$ eigenspace is elements fixed by $\mathfrak{A}_n$ and an additonal transposition, hence $S^{\mathfrak{S}_n}$. The -1 eigenspace is a $S^{\mathfrak{S}_n}$ submodule of $S^{\mathfrak{A}_n}$. We claim that the -1 eigenspace is $S^{\mathfrak{S}_n} \cdot \Delta$. To show this, it suffices to show that any element in the -1 eigenspace is a multiple of Δ in S. Using that S is a UFD, it suffices to show that $x_i - x_j$ divides such an f, or that $f_{x_i = x_j}$ is zero. But $(i\,j)(f) = -f$, so it is true.

Transfer and norm. There are some elementary recipes to turn arbitrary polynomials into invariant polynomials. We define the **transfer map** from $\mathrm{Tr}^G : S \longrightarrow S^G$ by

$$\mathrm{Tr}(s) = \sum_{g \in G} g(s).$$

The image is indeed an invariant, since $h\mathrm{Tr}^G(s) = \sum_{g \in G} hg(s)$ is the same sum, permuted. Thus, one can construct elements by computing transfers of various elements of S. Moreover, this map is S^G-linear since $r \in S^G$ and $s \in S$ yield

$$\mathrm{Tr}^G(rs) = \sum_{g \in G} g(rs) = \sum_{g \in G} g(r)g(s) = \sum_{g \in G} rg(s) = r \sum_{g \in G} g(s) = r\mathrm{Tr}^G(s).$$

It is also a degree-preserving map.

We say that G is **nonmodular** if the order of G is a unit in K, and **modular** otherwise. In the nonmodular case, we define the **Reynolds operator** to be the map

$$\rho : S \longrightarrow S^G, \rho(s) = \frac{1}{|G|} \sum_{g} g(s) = \frac{1}{|G|} \mathrm{Tr}(s).$$

Like with the transfer, this is an S^G-linear map with image in S^G. Moreover, for $r \in S^G$, we have $\rho(r) = r$. Thus, in the nonmodular case, the transfer map and Reynolds map are surjective. This gives a simple quasi-algorithm to compute invariants: evaluate the Reynolds operator at various polynomials in S. Of course, to compute all invariants, one needs some extra information if one wants to account for all invariants this way. Note also that the transfer map is never surjective in the modular case, since $\rho(1) = |G| = 0$, and thus no element of s can map to 1 for degree reasons.

Another useful construction is the **norm** map from S to S^G given by

$$\mathrm{N}^G(s) = \prod_{g\in G} g(s).$$

In particular, any element $s \in S$ has a nonzero S-multiple $N^G(s)$ in S^G.

We establish some basic properties of invariant rings.

Proposition 1.4. *Let G be a finite group acting linearly on S.*

(1) The inclusion $S^G \subseteq S$ is integral.
(2) $\mathrm{frac}(S^G) = \mathrm{frac}(S)^G$.
(3) S is an S^G-module of rank $|G|$.
(4) S^G is integrally closed in $\mathrm{frac}(S^G)$.

Proof. Any element $s \in S$ is a root of the monic polynomial $\prod_g(T - g(s)) \in S^G[T]$.

The containment $\mathrm{frac}(S^G) \subseteq \mathrm{frac}(S)^G$ is clear. Let $a/b \in \mathrm{frac}(S)^G$, so $a/b = g(a)/g(b)$ for all $g \in G$. We can multiply the numerator and denominator by $\prod_{g\neq e} g(b)$ to rewrite a/b with $b \in S^G$. Then $g(a)/g(b) = g(a)/b$, so $a/b \in \mathrm{frac}(S)^G$ implies $a \in S^G$, so $a/b \in \mathrm{frac}(S^G)$.

The third statement follows from the second.

Now, let $a/b \in \mathrm{frac}(S^G)$ be integral over S^G. Then since $a/b \in \mathrm{frac}(S)$ is integral over S, and hence in S. But if $a/b = s$ with $a, b \in S^G$ and $s \in S$, then $s \in S^G$ as well. □

Example 1.5. We return to the symmetric polynomials. Since $K[e_1,\dots,e_n] \subseteq K[x_1,\dots,x_n]$ is integral, we deduce that $\dim(K[e_1,\dots,e_n]) = n$. Using the fact that $K[e_1,\dots,e_n]$ is n-generated, we find that $e_1,\dots,e_n$ are algebraically independent.

Finite generation. We now turn to the question of describing all invariants. We will show that every invariant ring in our setting is a finitely generated K-algebra.

We will use the grading on R in a crucial way. For an $\mathbb{N}$-graded K-algebra R, we define

$$R_+ := (r \in R_i \mid i > 0)$$

for the ideal generated by homogeneous elements of positive degree.

Lemma 1.6. *Let R be an $\mathbb{N}$-graded K-algebra with $R_0 = K$ a field. If $R_+ = (f_1,\dots,f_t)$ for some homogeneous elements $f_i \in R$, then $R = K[f_1,\dots,f_t]$.*

Proof. Let $A = K[f_1,\dots,f_t]$. Clearly A is a graded K-algebra and $A \subseteq R$. If $A \neq R$, we can take a homogeneous element r of smallest degree in $R \smallsetminus A$. Since $\deg(r) > 0$, we have $r \in R_+ = (f_1,\dots,f_t)$, and we can write $r = \sum r_i f_i$ with r_i homogeneous of degree $\deg(r) - \deg(f_i) < \deg(r)$. By minimality, we have $r_i \in A$, and then $r \in A$, contradicting the existence of $r \notin A$. □

Theorem 1.7. *Let G be a finite group acting linearly on S. Then the ring of invariants $R = S^G$ is a finitely generated K-algebra.*

We use the proposition above to give two proofs of this theorem. The first is specific to the nonmodular case.

Hilbert's proof, nonmodular case. Consider the ideal $(R_+)S$ of S. By definition, this ideal is generated by homogeneous elements of R; by the Hilbert Basis Theorem, it is generated over S by a finite set $f_1,\dots,f_t$ of homogeneous elements in R_+.

We claim that $R_+ = (f_1,\dots,f_t)$. Indeed, let $r \in R_+$. Then $r \in (R_+)S$, so $r = \sum_i f_i s_i$. Applying the Reynolds operator ρ, we get

$$r = \rho(r) = \rho(\sum_i f_i s_i) = \sum_i f_i \rho(s_i), \quad \text{with } \rho(s_i) \in R,$$

so $r \in (f_1,\dots,f_t)$. Then, by the previous Lemma, we conclude that $R = K[f_1,\dots,f_t]$. □

Noether's proof, general case. Each x_i is integral over R. Take the coefficients of these n integral equations and let $A \subseteq R$ be the K-algebra they generate. This is a finitely generated K-algebra by construction. Also by construction $A \subseteq S$ is integral and algebra-finite, so it is module-finite. But A is Noetherian, so $A \subseteq R$ is module-finite, and hence R is Noetherian. In particular R_+ is generated by finitely many homogeneous elements, so R is a finitely generated algebra by the Lemma. □

Degree bounds. We have succeeding in finding generating sets for rings of invariants in our earlier examples. Our goal now is to turn our quasi-algorithm for computing invariant rings into a proper algorithm, at least in the nonmodular case. Supposing that we have a bound d for the degrees of generators of the invariant ring, we can compute by brute force: take the Reynolds operator for all monomials in S of degree at most d.

Lemma 1.8 (Benson). *Let G be a finite group acting linearly on $S = K[x_1,\dots,x_n]$, and suppose that $|G| \in K^\times$; i.e., that the action is nonmodular. Then $(S_+)^m \subseteq (S_+^G)S$.*

Proof. Let $\{s_g\}_{g\in G}$ be m homogeneous elements of S of positive degree, indexed by the elements of G. We want to show that $\prod_{g\in G} s_g \in (S_+^G)S$. Take $h \in G$. We have

$$X_h = \prod_{g\in G}\Big(\big((hg)(s_g)\big) - s_g\Big) = 0,$$

since one of the factors is zero. On the other hand, one can foil all of this out: there is a term for each subset $A \subseteq G$, corresponding to the collection of binomials for which one chooses the first factor. Working like so, one gets

$$\sum_{h\in G} X_h = \prod_{g\in G}\Big(\big((hg)(s_g)\big) - s_g\Big) = \sum_{A\subseteq G}(-1)^{m-|A|}\left(\sum_{h\in G}\prod_{g\in A} h(gs_g)\right)\left(\prod_{G\setminus A} s_g\right).$$

Comparing with above, one obtains that this sum is zero.

When $A = \varnothing$, the summand is $(-1)^m m \prod_{g\in G} s_g$. For every other summand, the term $\sum_{h\in G}\prod_{g\in A} h(gs_g)$ is a G-invariant of positive degree, and hence every other summand lies in $(R_+)S$. This shows the lemma. □

Theorem 1.9 (Fogarty, Fleischmann). *Let G be a finite group of order m, and suppose that $m \in K^\times$. Then $R = S^G$ is generated as an K-algebra by homogeneous elements of degree at most m.*

Proof. By the Lemma, $S_m = (S_+)^m \subseteq (R_+)S$. Thus, the ideal $(R_+)S$ is generated by elements of degree at most m. Take a generating set $f_1,\dots,f_t \in R_+$ of homogeneous elements of degree at most m. From Hilbert's proof of finite generation in the nonmodular case, we deduce that $R = K[f_1,\dots,f_t]$. □

Example 1.10. Let $G = \mathbb{Z}/3 = \langle g \rangle$ act on $S = \mathbb{F}_2[x,y]$ by

$$g \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} y \\ x+y \end{bmatrix}.$$

We can compute the invariant ring by brute force by the image under the Reynolds operator of

$$1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3$$

to get

$$1,\ 0,\ 0,\ 0,\ x^2+xy+y^2,\ 0,\ x^2y+xy^2,\ x^3+x^2y+y^3,\ x^3+xy^2+y^3,\ x^2y+xy^2$$

respectively. We deduce that

$$S^G = \mathbb{F}_2[x^2+xy+y^2, x^2y+xy^2, x^3+x^2y+y^3].$$

This bound can fail in the modular case:

Example 1.11. Let $S = \mathbb{F}_2[x_1,x_2,x_3,y_1,y_2,y_3]$. Let $G = \mathbb{Z}/2$ act by swapping x_i with y_i for each i. Then the invariant ring is not generated in degree 2.

However, one has the following.

Theorem 1.12 (Symonds). *Let G be a finite group acting linearly on $S = K[x_1,\dots,x_n]$. Then $R = S^G$ can be generated by elements of degree at most $n(m-1)$.*

We will not prove this theorem, but we will outline some of the basic ideas behind the proof later on in this series.

Molien's Theorem. A more sophisticated version of the algorithm above can be executed using Hilbert series. Recall that the Hilbert series of a graded K-algebra A is the generating function $H_A(t) = \sum_i \dim_K(A_i)t^i$. Given the Hilbert series of the invariant ring, one can then know in which degrees invariants live. Even better, given a guess of generating invariants, one can then verify that the proposed set is correct, or otherwise find in which degrees invariants are missing. It turns out that one can compute these in characteristic zero.

Theorem 1.13 (Molien). *Let K be a field of characteristic zero, and G be a finite group acting linearly on $S = K[x_1,\dots,x_n]$. Then*

$$H_{S^G}(t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-gt,V)}.$$

Proof. We can replace K by $\overline{K}$ without affecting the Hilbert function S^G or the right-hand side above, so we assume K is algebraically closed.

First, consider the Reynolds map $\rho : S \longrightarrow S^G$, and write $\pi : S \longrightarrow S$ for the composition of ρ with the inclusion map $S^G \subseteq S$. For each $j \in \mathbb{N}$, the map π restricts to a K-linear map $\pi_j : S_j \longrightarrow S_j$ such that $\pi^2 = \pi$. We can then write $S_j = \ker(\pi) \oplus S_j^G$, and taking bases with elements from each, the matrix for π is diagonal with ones corresponding to basis elements from S_j^G and zeroes elsewhere. Thus

$$\dim_K(S_j^G) = \operatorname{trace}(\pi_j, S_j) = \operatorname{trace}(\frac{1}{|G|}\sum_{g\in G} g, S_j) = \frac{1}{|G|}\sum_{g\in G}\operatorname{trace}(g, S_j).$$

It remains to show that

$$\sum_j \operatorname{trace}(g, S_j)t^j = \frac{1}{\det(1-gt, V)}.$$

We can change basis and assume that the matrix of g acting on V is in Jordan form. By considering Jordan blocks and since g has finite order, we see that the Jordan form is diagonal:

$$g \sim \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}.$$

Then $g(x_1^{a_1}\cdots x_n^{a_n}) = \lambda_1^{a_1}\cdots\lambda_n^{a_n}x_1^{a_1}\cdots x_n^{a_n}$. Thus, the eigenvalues of the action of the action of g on S_j are the j-fold products of the eigenvalues of g on V, which yields

$$\sum_j \operatorname{trace}(g, S_j)t^j = \left(\sum_j \lambda_1^j t^j\right)\cdots\left(\sum_j \lambda_n^j t^j\right) = \frac{1}{\prod_i (1-\lambda_i t)} = \frac{1}{\det(1-gt, V)}.$$

This completes the proof. □

Example 1.14. Let $G = \mathbb{Z}/3 = \langle g\rangle$ acts linearly on $S = \mathbb{C}[x,y]$ by $g = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1}\end{bmatrix}$, with $\omega = e^{2\pi i/3}$. We have

$$\begin{aligned}
\det(1-et, V) &= \begin{vmatrix} 1-t & 0 \\ 0 & 1-t \end{vmatrix} = (1-t)^2 \\
\det(1-gt, V) &= \begin{vmatrix} 1-\omega t & 0 \\ 0 & 1-\omega^2 t \end{vmatrix} = (1-\omega t)(1-\omega^2 t) = 1+t+t^2 \\
\det(1-g^2t, V) &= \begin{vmatrix} 1-\omega^2 t & 0 \\ 0 & 1-\omega t \end{vmatrix} = (1-\omega t)(1-\omega^2 t) = 1+t+t^2.
\end{aligned}$$

Thus

$$H_{S^G}(t) = \frac{1}{3}\left(\frac{1}{(1-t)^2} + \frac{2}{1+t+t^2}\right) = \frac{1}{3}\frac{(1+t+t^2)+2(1-t)^2}{(1-t)(1-t^3)} = \frac{t^2-t+1}{(1-t)(1-t^3)}.$$

We can expand this as $1+t^2+2t^3+t^4+\cdots$. In particular, there is a nonzero invariant of degree 2 and two linearly independent invariants of degree 3. We can find these by inspiration, or elsewise, by Reynolds: one has xy, x^3, y^3, so

$$\mathbb{C}[x^3, y^3, xy] \subseteq S^G.$$

We claim that equality holds. One way to show this is by showing that the Hilbert series are equal. To compute the Hilbert series of $\mathbb{C}[x^3,y^3,xy]$, let us first note that x^3, y^3 are algebraically independent, and xy is a root of the irreducible monic polynomial $T^3 - x^3y^3$ over $\mathbb{C}[x^3,y^3]$. By division, $\mathbb{C}[x^3,y^3,xy] = \bigoplus \mathbb{C}[x^3,y^3]\cdot\{1, xy, x^2y^2\}$. We can add the Hilbert series to get $\frac{1+t^2+t^4}{(1-t^3)^2}$. After making a common denominator, we obtain the equality.

Problem Set #1

(1) Let $M = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$ and let $G = \mathbb{Z}/4 = \langle g \rangle$. Consider the natural action of G on $V = K^2$ and the induced linear action on $S = \mathbb{C}[x,y]$. Find some nonzero elements of S^G. Can you find a generating set? (Hint: Compare to Example 1.1).

(2) Let $M = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $N = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{Q})$. Consider the natural action of G and H on $V = K^2$ and the induced linear action on $S = \mathbb{C}[x,y]$.
 (a) Compute the groups $H = \langle M \rangle$ and $G = \langle M, N \rangle$.
 (b) Use Molien's formula to find the Hilbert series of S^H and S^G. Compute both of them up to the t^4 term.
 (c) Find algebraically independent G-invariants of degrees 2 and 4. Explain why they must generate S^G.
 (d) Use the previous parts to determine the smallest degree of an element f that is H-invariant but not G-invariant, and find such an element f.
 (e) Observe something interesting about f^2. Can you find a generating set for S^H?

(3) Let G be a finite group. Given a homomorphism $G \hookrightarrow \mathfrak{S}_n$, for any field K one obtains a linear action of G on $K[x_1,\dots,x_n]$ by $g(x_i) := x_{g(i)}$, which we will call a permutation action. Show that, for such an action, S^G has a K-vector space basis given by orbit sums of monomials, i.e., elements of the form $\sum_{m' \in G\cdot m} m'$ where m is a monomial of S. Deduce that, in this setting, the Hilbert function of S^G is independent of K.

(4) Let $\mathfrak{A}_n$ be the alternating group on n letters, and let $\mathfrak{A}_n$ act by permuting the variables. Let K be a field of characteristic two.
 (a) Show that if K has characteristic two, then the discriminant $\Delta = \prod_{i<j}(x_i - x_j)$ is an element of $S^{\mathfrak{S}_n}$ and deduce that $S^{\mathfrak{A}_n} \neq K[e_1,\dots,e_n,\Delta]$.
 (b) Show that $\mu = \mathrm{Tr}^{\mathfrak{A}_n}(x_1^{n-1}x_2^{n-2}\cdots x_{n-1}) \in S^{\mathfrak{A}_n} \smallsetminus S^{\mathfrak{S}_n}$.
 (c) Show that $S^{\mathfrak{A}_n} = K[e_1,\dots,e_n,\mu]$.

(5) Let $M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ in $\mathrm{GL}_2(\mathbb{F}_p)$ and $G = \langle M \rangle \cong \mathbb{Z}/p$. Consider the natural action of G on $V = K^2$ and the induced linear action on $S = K[x,y]$.
 (a) Explain why Molien's Theorem does not directly apply.
 (b) Show that $\mathbb{F}_p[x_1, N(x_2)] \subseteq S^G$, and explain why $\mathbb{F}_p[x_1, N(x_2)]$ is isomorphic to a polynomial ring in two variables. In particular, $\mathbb{F}_p[x_1, N(x_2)]$ is normal.
 (c) Show that $\mathbb{F}_p(x_1, N(x_2)) = \mathbb{F}_p(x_1,x_2)^G$.
 (d) Show that $\mathbb{F}_p[x_1, N(x_2)] \subseteq \mathbb{F}_p[x_1,x_2]$ is integral. Deduce that $S^G = \mathbb{F}_p[x_1, N(x_2)]$.

(6) Let $K = \mathbb{F}_2$, and let $G = \mathbb{Z}/2$ act on $S = K[x_1, x_2, x_3, y_1, y_2, y_3]$ by swapping x_i with y_i for each i. In this problem, we will show that S^G is not generated by elements of degree ≤ 2.
   (a) Let $A = K[S^G_{\leq 2}]$ be the subalgebra of S^G generated by elements of degree at most 2. Show that A is generated by $\{x_i + y_i, x_i y_i, x_i y_j + x_j y_i \mid 1 \leq i < j \leq 3\}$.
   (b) Let $I \subseteq S$ be the ideal generated by $\{x_i^2, x_i y_i, y_i^2 \mid i = 1, 2, 3\}$ and let $\overline{A}$ be the image of A in S/I. Compute the graded pieces $\overline{A_1}$ and $\overline{A_2}$ and find four linearly independent elements in $\overline{A_3}$.
   (c) Show that the vector space $\overline{A_1} \cdot \overline{A_2}$ has $\mathbb{F}_2$-dimension at most three, and deduce the result.

(7) Let G be a finite group acting linearly on S. Show that the map $\pi : \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(S^G)$ induced by the inclusion map is surjective and $\pi(\mathfrak{p}) = \pi(\mathfrak{q})$ if and only if $G \cdot \mathfrak{p} = G \cdot \mathfrak{q}$. In particular, when $K = \overline{K}$, the maximal ideals of S^G correspond naturally to the G-orbits in V.

(8) Let G be a finite group of order m acting linearly on S. Let $A = K[S^G_{\leq m}]$ be the subalgebra of S^G generated by elements of degree at most m; in the modular case, this may be a proper subalgebra. Let $K = \overline{K}$. Show that the maximal ideals of A correspond naturally to the G-orbits in V.

2. Cohen-Macaulay rings and Polynomial rings

We will discuss some properties of graded rings that will help us understand invariant rings more concretely. We will first recall the two main notions that interest us today. By a graded ring, we mean a finitely generated $\mathbb{N}$-graded K-algebra with $R_0 = K$, but not necessarily generated in degree one. From last time, every ring of invariants of a finite group is graded in this sense.

Polynomial rings and systems of parameters. Of course, among the graded rings we understand best are polynomial rings; for us, we will say a ring is a polynomial ring as long as it is isomorphic to a polynomial ring, i.e., generated by algebraically independent elements. For example, the invariant ring of $\mathfrak{S}_n$ is a polynomial ring. The Hilbert series of a polynomial ring is easy to compute: if $S = K[f_1,\dots,f_n]$ is a polynomial ring with $\deg(f_i) = d_i$, one has

$$H_S(t) = \frac{1}{\prod_{i=1}^n (1-t^{d_i})}.$$

A *homogeneous system of parameters* for a graded ring R of dimension n is a set $f_1,\dots,f_n$ of homogeneous elements such that $(f_1,\dots,f_n)$ is R_+-primary. Every graded ring has a homogeneous system of parameters, by a variation of the usual local argument. Moreover, for $f_1,\dots,f_n$ homogeneous, $f_1,\dots,f_n$ is a homogeneous system of parameters if and only if $K[f_1,\dots,f_n]$ is a Noether normalization.

One can easily find systems of parameters for invariants of finite groups.

Proposition 2.1. *Let $S = K[x_1,\dots,x_n]$ and G be a finite group acting linearly on S.*

(1) If K is infinite, and $\ell_1,\dots,\ell_n$ are general linear forms, then $N^G(\ell_1),\dots,N^G(\ell_n)$ is homogeneous system of parameters for S^G.

(2) If G is a permutation group, the elementary symmetric polynomials form a homogeneous system of parameters for S^G.

Proof. (1) We will show that for general $\ell_1,\dots,\ell_n$, the vanishing locus $V((N(\ell_1),\dots,N(\ell_n))S)$ is just the origin. Inductively, assume that $X_i = V((N(\ell_1),\dots,N(\ell_i))S)$ is a finite union of linear spaces of codimension i. Then $\bigcup_{g\in G} g^{-1}(X_i)$ is a finite union of linear spaces of codimension i, and for $i < n$, one can choose a linear form ℓ_{i+1} that does not vanish identically on of these, and this works.

(2) The elementary symmetric polynomials are fixed by any permutation action, so $K[e_1,\dots,e_n] \subseteq S^G$, and since $K[e_1,\dots,e_n] \subseteq S$ is module-finite, so is $K[e_1,\dots,e_n] \subseteq S^G$. That is, this is a Noether normalization, so this is a homogeneous system of parameters.

□

Cohen-Macaulay graded rings. A graded ring is *Cohen-Macaulay* if some, equivalently every, homogeneous system of parameters is a regular sequence. The following alternative characterization is also quite useful.

Proposition 2.2. *Let $R \subseteq S$ be a graded module-finite inclusion of Noetherian positively graded K-algebras, with R a polynomial ring. Then S is Cohen-Macaulay if and only if S is a free R-module.*

Proof. By the Hilbert syzygy theorem, S has finite projective dimension over R. Then by Auslander-Buchsbaum,

$$\mathrm{pd}_R(S) = \mathrm{depth}(R) - \mathrm{depth}_R(S) = \dim(R) - \mathrm{depth}(S).$$

Then S is free over R if and only if $\mathrm{pd}_R(S) = 0$ which happens if and only if $\mathrm{depth}(S) = \dim(R)(= \dim(S))$. □

Theorem 2.3 (Hochster-Eagon). *Let G be a finite group of order m acting linearly on a polynomial ring S with $m \in K^\times$. Then $R = S^G$ is Cohen-Macaulay.*

Proof. Take a homogeneous system of parameters $f_1, \dots, f_n$ of R. Then this is a system of parameters for S, and hence a regular sequence there. If $r_{i+1} f_{i+1} \in (f_1, \dots, f_i)$, then we have $r_{i+1} f_{i+1} \in (f_1, \dots, f_i)S$ implies $r_{i+1} \in (f_1, \dots, f_i)S$, since it is a regular sequence in S. Applying the Reynolds operator ρ, we get

$$r_{i+1} = \rho(r_{i+1}) \in \rho((f_1, \dots, f_i)S) = (f_1, \dots, f_i)R.$$

This shows that $f_1, \dots, f_d$ is a regular sequence. □

We will see later that the nonmodular hypothesis is strictly necessary.

We can use this to give more concrete descriptions of rings of invariants. When we write a ring in terms of generators and relations, it is not always clear when two expressions are the same. Instead, we can use Noether normalization.

Corollary 2.4. *Let G be a finite group of order m acting linearly on a polynomial ring S with $m \in K^\times$. Then there exist sets of* primary invariants $f_1, \dots, f_n \in R^G$ *and* secondary invariants $h_1, \dots, h_m \in R^G$ *such that $f_1, \dots, f_n$ are algebraically independent and $R^G = \bigoplus_{i=1}^m K[f_1, \dots, f_n] h_i$. Namely, every invariant $f \in R^G$ has a unique expression of the form*

$$f = a_1(f_1, \dots, f_n) h_1 + \cdots + a_m(f_1, \dots, f_n) h_m,$$

for some (uniquely determined) tuple $a_1, \dots, a_m \in K[t_1, \dots, t_n]$.

Example 2.5. Consider $\mathcal{A}_n$ acting linearly on $S = K[x_1, \dots, x_n]$ with the natural permutation action. Then we can write

$$S^{\mathcal{A}_n} = K[e_1, \dots, e_n] \oplus K[e_1, \dots, e_n]\Delta,$$

where Δ is the discriminant in characteristic other than two, and a suitable orbit sum otherwise. Then $e_1, \dots, e_n$ form a set of primary invariants, and $1, \Delta$ form a set of secondary invariants.

If R is a graded ring with homogeneous system of parameters $f_1, \dots, f_n$ with degrees $d_1, \dots, d_n$ and $h_1, \dots, h_m$ form a free basis for R over $K[f_1, \dots, f_n]$ with degrees $e_1, \dots, e_m$, then

$$H_R(t) = \frac{\sum_{i=1}^m t^{e_i}}{\prod_{i=1}^n (1 - t^{d_i})}.$$

Polynomial invariant rings. Our goal now is to characterize polynomial invariant rings in the nonmodular case. In this case, this can be detected easily by the action of G.

Definition 2.6. Let G be a finite group acting linearly on $S = K[x_1, \dots, x_n]$. We say that g is a *pseudoreflection* if $\operatorname{codim}_K(\operatorname{Fix}(g, V)) \leq 1$.

The identity is, by our convention, a pseudoreflection.

For $g \in G$, the matrix of g on V can be put into Jordan form after perhaps extending the field K. In the nonmodular case, this is a diagonal matrix, and $g \neq e$ is a pseudoreflection if and only if it is of the form

$$\begin{bmatrix} \zeta & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

In the modular case, one may have nondiagonalizable pseudoreflections with Jordan form

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

which are called *transvections.*

Theorem 2.7 (Shephard-Todd). *Let G be a finite group acting linearly on $S = K[x_1, \dots, x_n]$.*

(1) If $|G| \in K^\times$, and G is generated by pseudoreflections, then $R = S^G$ is isomorphic to a polynomial ring.

(2) If $R = S^G$ is isomorphic to a polynomial ring, then G is generated by pseudoreflections.

Example 2.8. Let $\mathcal{S}_n$ act on $S = K[x_1, \dots, x_n]$ by permutations. The group $\mathcal{S}_n$ is generated by transpositions. The fixed space of the transposition $(i\,j)$ includes all e_k, $k \neq i, j$, and $e_i + e_j$, so the fixed space is codimension one. That is, $\mathcal{S}_n$ is generated by pseudoreflections, and the invariant ring is a polynomial ring.

Example 2.9. Let $\mathcal{A}_n$ act on $S = K[x_1, \dots, x_n]$ by permutations. The group $\mathcal{A}_n$ in fact has no nontrivial pseudoreflections: the fixed space of an k-cycle is codimension $k-1$, and the fixed space of disjoint k_i-cycles is $\sum_i (k_i - 1)$. The invariant ring is not a polynomial ring.

Lemma 2.10. *Let $A \subseteq B$ be a module-finite inclusion of graded K-algebras with B polynomial. If the map $\mu : A_+ \otimes_A B \longrightarrow B$ induced by multiplication is injective, then A is regular.*

Proof. Suppose that the map $\mu : A_+ \otimes_A B \longrightarrow B$ induced by multiplication is injective. Then the short exact sequence

$$0 \longrightarrow A_+ \longrightarrow A \longrightarrow K \longrightarrow 0$$

induces the long exact sequence

$$0 \longrightarrow \operatorname{Tor}_1^A(B, K) \longrightarrow A_+ \otimes_A B \longrightarrow A \otimes_A B \longrightarrow K \otimes_A B \longrightarrow 0,$$

and the map $A_+ \otimes_A B \longrightarrow A \otimes_A B \cong B$ is μ. Thus, μ is injective implies that $\operatorname{Tor}_1^A(B, K) = 0$, and hence B is free over A by Nakayama's Lemma.

Now let F be the minimal graded resolution of K over A. If B is free over A, then $B \otimes_A F$ is exact, and is a minimal free resolution of $B \otimes_A K$. Since B is regular, this resolution is finite. It follows that F is finite, and hence A is regular. □

Proof of Shephard-Todd. (1) Following the lemma, we show that the multiplication map

$$\mu : R_+ \otimes_R S \longrightarrow S$$

is injective.

First we claim that the restriction of μ to $(R_+ \otimes_R S)^G$ is injective. This is where we use the Reynolds operator. Indeed, from the diagram

$$\begin{tikzcd}
 & S \arrow[dr] & & \rightsquigarrow & & R_+ \otimes_R S \arrow[dr] & \\
R \arrow[ur] \arrow[rr] & & R & & R_+ \otimes_R R \arrow[ur] \arrow[rr] & & R_+ \otimes_R R
\end{tikzcd}$$

we have that $R_+ \otimes_R R$ injects into $R_+ \otimes_R S$, and

$$(R_+ \otimes_R S)^G = \rho(R_+ \otimes_R S) = R_+ \otimes_R \rho(S) = R_+ \otimes_R R$$

so we can identify $(R_+ \otimes_R S)^G = R_+ \otimes_R R$. But μ restricted to $R_+ \otimes_R R$ is injective.

Now we will show that a nonzero element of $\ker(\mu)$ of monomial degree is G invariant. Let g be a pseudoreflection and $V^g = V(\ell)$ be its fixed space with ℓ a linear form. For any $f \in S$, the functions f and $g(f)$ agree on V^g, so $g(f) - f$ is zero on V^g, and hence $\ell \mid (g(f) - f)$. Write $g(f) - f = \ell f'$. In the same way, if $\zeta \in R_+ \otimes_R S$ homogeneous, we can write

$$(1-g)\zeta = \zeta'(1 \otimes \ell)$$

for some ζ' of degree one less.

Let ζ be an element in $\ker(\mu)$ of minimal degree. We claim that ζ is fixed by G. Indeed, $g(\zeta) \in \ker(\mu)$, since $\mu(g(\zeta)) = g(\mu(\zeta)) = 0$, so

$$0 = \mu(\zeta) - \mu(g(\zeta)) = \mu((1-g)\zeta) = \mu((1 \otimes \ell)\zeta') = \ell\mu(\zeta').$$

Then since S is a domain, $\mu(\zeta') = 0$, and by minimality of degree, $\zeta' = 0$, so $g(\zeta) = \zeta$. Now, G is generated by pseudoreflections g, so

$$\zeta \in (R_+ \otimes_R S)^G = R_+ \otimes_R R,$$

as claimed. This completes the argument.

(2) We consider the special case $K = \mathbb{C}$. Suppose that $R = S^G$ is a polynomial ring. Then $V/G = \mathrm{Spec}(R)$, considered as a variety, is a copy of $\mathbb{C}^n$, as is $V = \mathrm{Spec}(R)$.

Let $X \subseteq V = \mathrm{Spec}(S)$ be

$$X = \bigcup_{\substack{g \in G \\ \text{not pseudoreflection}}} \mathrm{Fix}(g).$$

Let us write $V/G = \mathrm{Spec}(R)$ and $\pi : V \longrightarrow V/G$. Note that X is G-stable: if x is fixed by a nonpseudoreflection h, and $g \in G$, then gx is fixed by ghg^{-1}, which is conjugate to h, and hence also a nonpseudoreflection. Then since $X \subseteq V$ has codimension ≥ 2, then $\pi(X) \subseteq V/G$ has codimension at least two (as a complex variety) by going down. In particular, it has codimension strictly greater than two over $\mathbb{R}$, so $\widetilde{V/G} := (V/G) \smallsetminus \pi(X)$ is simply connected.

Let $\widetilde{V} = V \smallsetminus X$, which is a dense open subset of V with

$$\pi : \widetilde{V} \longrightarrow \widetilde{V/G} = \widetilde{V}/G.$$

By definition, the stabilizer of any $v \in \widetilde{V}$ must consist only of pseudoreflections. Let N be the subgroup of G generated by all $g \in G$ that fix some point in $\widetilde{V}$; this is a normal subgroup. Consider the orbit space $\widetilde{V}/N$. This has an induced action of G/N, and this action is free (no fixed points) by construction. Thus, $\widetilde{V}/N \longrightarrow \widetilde{V/G}$ is a covering space, and since $\widetilde{V}/N$ is connected and $\widetilde{V/G}$ is simply connected, this must be a homeomorphism. Then, for degree reasons, we deduce that $G = N$.

For arbitrary fields, one proceeds along similar lines in the étale topology. □

The proof of Shepard-Todd is not constructive, but the following is useful in arbitrary characteristic.

Proposition 2.11. *Let G be a finite group acting linearly on S. Then if $R = S^G$ is a polynomial ring, we have $R = K[f_1, \dots, f_n]$ with $\deg(f_1) \cdots \deg(f_n) = |G|$.*

Proof. Note that when $R = S^G$ is a polynomial ring, then R is a Noether normalization for S, so S is a free R-module (because R is Cohen-Macaulay), and from an earlier Proposition, of rank $|G|$.

Let $d_i = \deg(f_i)$. Using the Noether normalization formula we have

$$H_S(t) = \frac{1}{(1-t)^n} = \frac{\sum_j t^{e_j}}{\prod_i (1-t^{d_i})} = \frac{\sum_j t^{e_j}}{\prod_i \Big((1-t)(1+t+\cdots+t^{d_i-1})\Big)},$$

where the sum $\sum_j t^{e_j}$ has $|G|$ summands. Then multiplying by $(1-t)^n$ and taking $\lim_{t\longrightarrow 1}$, we get

$$1 = \frac{|G|}{\prod_i d_i},$$

and the claim follows. □

We can prove a result of a similar flavor that gives a sufficient condition for the Cohen-Macaulay property in the modular case.

Theorem 2.12. *Let G be a group acting linearly on $S = K[x_1, \dots, x_n]$. If $\operatorname{codim}_K(V^G \subseteq V) \leq 2$, then S^G is Cohen-Macaulay.*

Proof. By standard techniques we can reduce to the case where K is algebraically closed. For $w \in V^G$, the map $V \xrightarrow{+w} V$ is an isomorphism that commutes with the action of G. This induces an isomorphism $S \xrightarrow{\psi_w} S$ that maps the maximal ideal $\mathfrak{m}_w$ of functions vanishing on w to the homogeneous maximal ideal S_+. Since ψ_w commutes with the action of G, this induces isomorphisms $S^G \xrightarrow{\varphi_w} S^G$ mapping $\mathfrak{n}_w := S^G \cap \mathfrak{m}_w$ to S^G_+. In particular, $S^G_{\mathfrak{n}_w} \cong S^G_{S^G_+}$, so S^G is Cohen-Macaulay if and only if $S^G_{\mathfrak{n}_w}$ is Cohen-Macaulay, and so if S^G is not Cohen-Macaulay, its localization at any maximal ideal in a subvariety of dimension 2 is also not Cohen-Macaulay. But S^G is normal, hence (S_2), so this is impossible, and hence S^G is Cohen-Macaulay. □

There is something of a converse to this theorem in the case of p-groups. To state it we need the following.

Definition 2.13. Let G be a finite group acting linearly on $S = K[x_1, \dots, x_n]$. We say that g is a *bireflection* if $\operatorname{codim}_K(\operatorname{Fix}(g, V)) \leq 2$.

Theorem 2.14 (Kemper). *Let G be a p-group acting linearly on S with K of characteristic p. If S^G is Cohen-Macaulay, then G is generated by bireflections.*

Problem Set #2

(1) Use the Shephard-Todd Theorem to determine for which of the following group actions on $S = \mathbb{C}[x,y]$ the invariant ring is a polynomial ring.

(a) $G = \langle \begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix} \rangle$, where $\omega = e^{2\pi i/3}$.

(b) $G = \langle \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix} \rangle$.

(c) $G = \langle \begin{bmatrix} \omega & 0 \\ 0 & -1 \end{bmatrix} \rangle$.

(2) Find primary and secondary invariants for the following group actions.

(a) $S = \mathbb{C}[x_1, x_2]$, $G = \mathbb{Z}/2 = \langle g \rangle$ with $g(x_i) = -x_i$.

(b) $S = \mathbb{C}[x_1, x_2]$, $G = \mathbb{Z}/3 = \langle g \rangle$ with $g(x_i) = \omega x_i$, where $\omega = e^{2\pi i/3}$.

(3) Let $K = \mathbb{F}_2$, and let $G = \mathbb{Z}/2$ act on $S = K[x_1, x_2, x_3, y_1, y_2, y_3]$ by swapping x_i with y_i for each i. In this problem, we will verify directly (without the use of Kemper's Theorem) that $R = S^G$ is not Cohen-Macaulay.

(a) Show that $\{x_i + y_i, x_i y_i \mid i = 1,2,3\}$ is a homogeneous system of parameters for R.

(b) Show that $H_R(t) = \frac{1+3t^2}{(1-t)^3(1-t^2)^3}$.

(c) Show that R if Cohen-Macaulay then R is a free $K[x_i + y_i, x_i y_i]$-module with basis 1 and $\{x_i y_j - x_j y_i \mid 1 \le i < j \le 3\}$.

(d) Find a relation on the elements above and deduce that R is not Cohen-Macaulay.

(4) Let K be a field and G a finite group such that $\operatorname{Hom}(G, K^\times) = \{1\}$. In this problem we will show that $R = S^G$ is a unique factorization domain.

- First, show that if G is a p-group and $\operatorname{char}(K) = p$, then the hypothesis applies.

Let $r \in R$. Take an S-irreducible decomposition $r = s_1 \cdots s_t$. The group G partitions the principal ideals $(s_i)S$ into orbits, and let $t_1, \dots, t_\ell$ be the orbit products, so $r = t_1 \cdots t_\ell$.

- Show that $t_i \in R$. Hint: For each $g \in G$, there is $\theta(g) \in S^\times$ such that $g(t_i) = \theta(g) t_i$. Show that θ is a group homomorphism.
- Show that $t_i \in R$ is irreducible.
- Show that $r = t_1 \cdots t_\ell$ is the unique irreducible decomposition of r.

(5) Let $G = \mathbb{Z}/4$ act on $\mathbb{F}_2[x_1, x_2, x_3, x_4]$ by cyclically permuting the variables. Use the results above to deduce that S^G is a unique factorization domain that is not Cohen-Macaulay.

(6) Let K be a finite field and

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(a) Is $G = \langle A, B, C \rangle$ generated by pseudoreflections? Does Shephard-Todd apply?

(b) Show that $S^{\langle A,B \rangle} = K[x_1, x_2, N(x_3), N(x_4)]$.

(c) Show that if S^G is a polynomial ring, the generators live in degrees $1, 1, p, p^2$.

(d) Show that S^G has no generator of degree p and deduce that S^G is not a polynomial ring.

(e) Show that, moreover, every point stabilizer of G is generated by pseudoreflections.

(7) Modify the proof of Shephard-Todd to show that if $R = S^G$ is a polynomial ring, then for each $v \in V$, the group $\mathrm{Stab}(v) \leq G$ is generated by pseudoreflections. (You can keep the hypothesis $K = \mathbb{C}$ as we did in the proof.) Now show that the previous example is such that for each $v \in V$, the group $\mathrm{Stab}(v) \leq G$ is generated by pseudoreflections.

(8) Let $f_1, \dots, f_n$ be a homogeneous system of parameters for $R = S^G$. Show that $\deg(f_1) \cdots \deg(f_t) = m|G|$ for some integer $m \geq 1$, and when $m = 1$, this system of parameters generates R as an algebra.

3. Local cohomology of invariant rings

We now want to discuss some aspects of local cohomology in invariant theory of finite groups.

Local cohomology. We first review some basics with local cohomology. Let R be a Noetherian ring. The Cech complex on a sequence of elements $f_1,\dots,f_t$ is the complex

$$C(f_1,\dots,f_t) \;=\; 0\longrightarrow R\longrightarrow \bigoplus_i R_{f_i}\longrightarrow \bigoplus_{i<j} R_{f_if_j}\longrightarrow\cdots\longrightarrow R_{f_1\cdots f_t}\longrightarrow 0$$

where the maps are localization maps with a suitable sign convention to make this a complex. The ith local cohomology with support in an ideal $I=(f_1,\dots,f_t)$ is

$$H^i_I(R)=H^i(C(f_1,\dots,f_t))$$

and more generally, ith local cohomology with support in an ideal $I=(f_1,\dots,f_t)$ and coefficients in a module M is

$$H^i_I(M)=H^i(C(f_1,\dots,f_t)\otimes_R M).$$

This is independent (up to isomorphism) of choice of generating set for I. Moreover, this is independent (up to isomorphism) of a choice of generating set up to radical, meaning that if $\sqrt{I}=\sqrt{(f_1,\dots,f_t)}$, then $H^i_I(R)=H^i(C(f_1,\dots,f_t))$, and likewise with a module M. One can show this directly by reducing to the case of comparing the Cech complex on $f_1,\dots,f_t$ with the Cech complex on $f_1,\dots,f_t,g$ with $g^n\in(f_1,\dots,f_t)$, though the typical approach is by showing both compute the right derived functors of I-torsion.

Because each term in the Cech complex is flat, tensoring $C(f_1,\dots,f_t)$ with a short exact sequence of modules gives a short exact sequence of complexes, and hence a long exact sequence of local cohomology modules.

We will be particularly interested in the case R is a graded ring and $I=R_+$. Then, the local cohomology modules $H^i_{R_+}(R)$ are the cohomology modules of the Cech complex on a homogeneous system of parameters. Note that these local cohomology modules then admit a grading, since the Cech complex is graded.

In the case of a polynomial ring $S=K[x_1,\dots,x_n]$, computing the local cohomology by the Cech complex on $x_1,\dots,x_n$, one has

$$H^n_{S_+}(S)=\bigoplus_{a_1,\dots,a_n>0} K\cdot\left[\frac{1}{x_1^{a_1}\cdots x_n^{a_n}}\right]$$

with the direct sum as a K-vector space, and $H^i_{S_+}(S)=0$ for $i<n$; one way to do this is to observe that the Cech complex is $\mathbb{N}^n$-graded, and to compute the graded strands. A useful alternative description of $H^n_{S_+}(S)$ as an S-module is as the graded K-dual of S, the graded K-linear homomorphisms from S to K, but shifted down in degree by n. That is, as S-modules,

$$S^\star(n)\cong H^n_{S_+}(S)\quad (x_1^{a_1}\cdots x_n^{a_n})^\star\longmapsto\left[\frac{1}{x_1^{a_1+1}\cdots x_n^{a_n+1}}\right].$$

Observe that the top degree is $-n=\deg(\left[\frac{1}{x_1\cdots x_n}\right])$. The **a-invariant** of a graded ring R of dimension n is the top degree of $H^n_{R_+}(R)$.

Let us apply Noether normalization to compute local cohomology for a graded Cohen-Macaulay ring R. Let $f_1,\dots,f_n$ be a homogeneous system of parameters for R, and $h_1,\dots,h_m$

a graded free basis for R over $A = K[f_1,\dots,f_n]$. Then we can compute $H^i_{R_+}(R)$ via the Cech complex on $f_1,\dots,f_n$ on R. This splits as a direct sum, so

$$H^i_{R_+}(R) = \bigoplus_j H^i_{A_+}(A)\cdot g_j.$$

In particular, using the calculation of A as a polynomial ring, we have $H^i_{R_+}(R) = 0$ for $i < n$; in general the first nonvanishing local cohomology of a graded ring is at the depth, so this vanishing is equivalent to the Cohen-Macaulay property.

We also consider the degrees of $H^n_{R_+}(R)$. The top degree of $H^n_{A_+}(A)$ is $-\deg(f_1)-\cdots-\deg(f_n)$, so the top degree of $H^i_{R_+}(R)$ is this plus the largest degree of a g_j. That is,

$$a(R) = \max\Big\{\deg(g_j)\Big\} - \sum_i \deg(f_i).$$

When $R = S/(h)$ is a graded hypersurface cut out by one equation h of degree v, one can compute the a-invariant of R by considering the short exact sequence

$$0 \longrightarrow S(-v) \xrightarrow{h} S \longrightarrow R \longrightarrow 0.$$

The long exact sequence of local cohomology has only three nonzero terms

$$0 \longrightarrow H^{n-1}_{R_+}(R) \longrightarrow H^n_{S_+}(S(-v)) \xrightarrow{h} H^n_{S_+}(S) \longrightarrow 0.$$

From this, we compute that $a(R) = v - n$.

A similar relationship between the degree of a homogeneous system of parameters, degree of module generators over the system of parameters, and degrees of local cohomology holds even when R is not Cohen-Macaulay. In this case, one has the following:

Proposition 3.1. *Let R be a graded ring and $f_1,\dots,f_n$ a homogeneous system of parameters. Let $A = K[f_1,\dots,f_n]$, and $g_1,\dots,g_m$ be a minimal generating set for R as an A-module. Let $a^\star(R)$ be the top degree of $H^i_{R_+}(R)$ as i varies. Then*

$$a^\star(R) \geq \max\Big\{\deg(g_j)\Big\} - \sum_i \deg(f_i). \qquad \square$$

Theorem 3.2 (Symonds). *Let G be a finite group acting linearly on $S = K[x_1,\dots,x_n]$. Then $R = S^G$ is generated by elements of degree at most $(n-1)|G|$.*

Outline of proof. The main point of the proof is to show that $a^*(R) \leq -n$; we will say nothing about this. We can extend scalars and assume K is infinite. Then the norms of generic linear forms are a SOP, so we can take $\deg(f_i) = |G|$ for all i. Then

$$\max\Big\{\deg(g_j)\Big\} \leq \sum_i \deg(f_i) + a^\star(R) \leq n|G| - n = (n-1)|G|.$$

Since the f_i's and g_j's generate as an algebra, the desired bound holds. □

Action of G on local cohomology. Let G act linearly on $S = K[x_1,\dots,x_n]$. Let $f_1,\dots,f_n$ be a homogeneous system of parameters for S^G; this is also a homogeneous system of parameters for S consisting of invariants. Then G acts on the Cech complex of $f_1,\dots,f_t$ on S, which induces an action of G on $H^n_{S_+}(S)$. That is,

$$g \cdot \left[\frac{s}{f_1^t \cdots f_n^t}\right] = \left[\frac{g(s)}{f_1^t \cdots f_n^t}\right].$$

This action is compatible with the action of G on S in the sense that

$$g(s \cdot \mu) = g(s) \cdot g(\mu).$$

We can compute the action of G on $H^n_{S_+}(S)$ explicitly.

Proposition 3.3. *Let G act linearly on $S = K[x_1,\dots,x_n]$. Consider the dual action of G on $S^\star$ given by $g(\varphi) = \varphi \circ g$. Let $\circ$ denote the induced action of G on $H^n_{S_+}(S)$ translated by the isomorphism $S^\star \cong H^n_{S_+}(S)$. Then the natural action of G on $H^n_{S_+}(S)$ is given by*

$$g \cdot \mu = \det(g, V)(g \circ \mu).$$

Proof. First we compute the action on the socle

$$\eta = \left[\frac{1}{x_1 \cdots x_n}\right].$$

First we rewrite η in terms of the Cech complex on an invariant homogeneous system of parameters $f_1,\dots,f_n$.

We can write

$$\begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} = A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

for some matrix A with entries in S. Then $\det(A)$ is a nonzero socle element for $S/(f_1,\dots,f_n)$, and it follows that η is a nonzero scalar multiple of

$$\left[\frac{\det(A)}{f_1 \cdots f_n}\right];$$

we will abuse notation and rename η to be this element. Then

$$g(\eta) = \left[\frac{g(\det(A))}{f_1 \cdots f_n}\right] = \left[\frac{\det(g(A))}{f_1 \cdots f_n}\right] = \det(g)\left[\frac{\det(A)}{f_1 \cdots f_n}\right] = \det(g)\eta.$$

Now, given $\mu \in H^n_{S_+}(S)_{-n-t}$, since $H^n_{S_+}(S)_{-n-t} \cong (S^\star)_{-t}$, there is a unique $f \in S_t$ such that $f\mu = \eta$. Then

$$g(f)g(\mu) = g(f\mu) = g(\eta) = \det(g)\eta,$$

so

$$\det(g)^{-1} g(f) g(\mu) = \eta.$$

Now, since $\det(g)^{-1} g(f) \det(g)(g \circ \mu) = \eta$, again by duality, $g(\mu) = \det(g)(g \circ \mu)$. □

Computing local cohomology of invariant rings. In the nonmodular case, we can compute the local cohomology of an invariant ring as the invariant part of the local cohomology of the polynomial ring.

Proposition 3.4. *Let $|G| \in K^\times$ and $R = S^G$. Then $H^i_{R_+}(R) \cong H^i_{S_+}(S)^G$ for all i.*

Proof. We use the Reynolds operator

$$\begin{tikzcd} & S \arrow[dr, "\rho"] & \\ R \arrow[ur, "i"] \arrow[rr, "\mathrm{id}"'] & & R \end{tikzcd} \qquad \begin{tikzcd} & H^i_{R_+}(S) = H^i_{S_+}(S) \arrow[dr, "\rho"] & \\ H^i_{R_+}(R) \arrow[ur, "i"] \arrow[rr, "\mathrm{id}"'] & & H^i_{R_+}(R) \end{tikzcd}$$

and this diagram is compatible with the G-action. Thus, the inclusion map induces an inclusion $H^i_{R_+}(R) \hookrightarrow H^i_{S_+}(S)$. Since this is compatible with the action, the image is contained in $H^i_{S_+}(S)^G$. Now, for $\mu \in H^i_{S_+}(S)^G$, observe that $\mu = i\rho(\mu)$, so $\mu \in \mathrm{image}(i)$. Thus, i gives the desired isomorphism. □

Note that this gives a second proof of the Hochster-Eagon Theorem.

A graded ring A of dimension n is Gorenstein if it is Cohen-Macaulay and $H^n_{A_+}(A) \cong A^\star(a)$ for some a.

Theorem 3.5 (Watanabe). *Let G act linearly on $S = K[x_1, \dots, x_n]$ with $|G| \in K^\times$. Suppose that the image of G in* $\mathrm{GL}(V)$ *is in* $\mathrm{SL}(V)$. *Then $R = S^G$ is Gorenstein.*

Proof. By Hochster-Eagon, R is Cohen-Macaulay, and by the previous proposition, $H^n_{R_+}(R) \cong H^n_{S_+}(S)^G$. By assumption, $\det(g) = 1$ for all g, so the action of G on $H^n_{S_+}(S)$ is just the dual action on $S^\star$. Thus, the invariant part is $(S^G)^\star$. Putting this together gives the theorem. □

Theorem 3.6 (Goel-Jeffries-Singh). *Let G be a finite group acting linearly on the polynomial ring $S = K[x_1, \dots, x_n]$, and $R = S^G$.Then there is an exact sequence*

$$\bigoplus_{g \in G} H^n_{S_+}(S) \xrightarrow{\alpha} H^n_{S_+}(S) \xrightarrow{\mathrm{Tr}} H^n_{R_+}(R) \longrightarrow 0,$$

where

$$\alpha \colon (\eta_g)_{g \in G} \longmapsto \sum_{g \in G} \big(\eta_g - g(\eta_g)\big).$$

Sketch of proof. Consider the complex

$$(\dagger) \qquad \bigoplus_{g \in G} S \xrightarrow{\alpha} S \xrightarrow{\mathrm{Tr}} R \longrightarrow 0,$$

where

$$\alpha \colon (s_g)_{g \in G} \longmapsto \sum_{g \in G} \big(s_g - g(s_g)\big).$$

(1) The map $\mathrm{Tr} : S \longrightarrow R$ is surjective in codimension one; this follows from a theorem describing $V(\mathrm{Tr}^G(S)S)$ as $\bigcup_{|g|=p} \mathrm{Fix}(g, V)$.

(2) The complex (†) is exact in codimension zero: after passing to fraction fields, setting $L = \operatorname{frac}(S)$, we get

$$\bigoplus_{g\in G} L \xrightarrow{\alpha} L \xrightarrow{\mathrm{Tr}} L^G \longrightarrow 0.$$

The kernel of Tr above is an L^G-vector space of dimension $|G|-1$ by rank considerations. By the normal basis theorem, we can write $L = \bigoplus_{g\in G} L^G g(\lambda)$ for some $\lambda \in L$. Then $\{\lambda - g(\lambda) \mid g \neq e\}$ are L^G linearly independent elements in the image of α, so the sequence is exact.

(3) The statement then follows from a formal argument, using Grothendieck vanishing. □

The following theorem has been obtained independently by Hashimoto:

Corollary 3.7. *For K a field, let G be a finite subgroup of $\mathrm{GL}_n(K)$ acting on the polynomial ring $R := K[x_1,\dots,x_n]$. Then $a(R^G) = a(R)$ if and only if G is a subgroup of $\mathrm{SL}_n(K)$ that contains no pseudoreflections.*

Case of no pseudoreflections. We verify that if G has no pseudoreflections, then $a(R^G) = a(R)$ if and only if G is a subgroup of $\mathrm{SL}_n(K)$. The exact sequence from the previous theorem, when restricted to the degree $-n$ strand, gives an exact sequence of K-vector spaces

$$\bigoplus_{g\in G} [H^n_{\mathfrak{m}}(R)]_{-n} \xrightarrow{\alpha} [H^n_{\mathfrak{m}}(R)]_{-n} \xrightarrow{\mathrm{Tr}} [H^n_{\mathfrak{n}}(R^G)]_{-n} \longrightarrow 0.$$

Since $[H^n_{\mathfrak{m}}(R)]_{-n}$ is a rank one vector space, it follows that $a(R^G) = -n$ if and only if the map α above is identically zero, i.e., if and only if the map

$$[H^n_{\mathfrak{m}}(R)]_{-n} \xrightarrow{1-g} [H^n_{\mathfrak{m}}(R)]_{-n}$$

is zero for each $g \in G$. Taking

$$\eta := \left[\frac{1}{x_1\cdots x_n}\right],$$

this is equivalent to the condition that

$$\eta - g(\eta) \;=\; \eta - (\det g)^{-1}\eta$$

is zero for each g, i.e., that $\det g = 1$ for each $g \in G$. □

Using the a-invariant. We end by illustrating how the previous result can be applied for our initial motivating question: calculating rings of invariants.

Theorem 3.8 (Maithani). *Let $\mathbb{F}_q$ be a finite field, and $G = \mathrm{GL}_2(K)$ act on $\mathrm{Mat}_2(K)$ by conjugation. Then $S^G = K[f_1, f_2, f_3, f_4, h]$ for explicit invariants of degrees $1, 2, q+1, q^2-q, q^2$.*

Theorem 3.9 (Chen, Ren). *Let $\mathbb{F}_q$ be a finite field, and $G = \mathrm{GL}_2(K)$ act on $\mathrm{Mat}_2(K)$ by $g\cdot M = gMg^T$. Then $S^G = K[f_1, f_2, f_3, f_4, h]$ for explicit invariants.*

We outline the method of proof of both theorems.

Proof outline. (1) Find primary invariants f_1, f_2, f_3, f_4 of low degree.

(2) One has a p-Sylow subgroup $P \leq G$ for which the codimension $V^P \subseteq V$ is 2. By a theorem from last time, S^P is Cohen-Macaulay. Then the relative transfer map $\sum_{g\in G/P} g : S^P \longrightarrow S^G$ admits a splitting, so by a similar argument to the Hochster-Eagon theorem, S^G is also Cohen-Macaulay.

(3) For the explicit primary invariants, one computes $\deg(f_1)\deg(f_2)\deg(f_3)\deg(f_4) = 2|G|$. Thus, S^G is free of rank two over $K[f_1, f_2, f_3, f_4]$, and we can choose a homogeneous basis $\{1, h\}$.

(4) One shows that the action of G has no pseudoreflections and has determinant one. By the corollary above, $a(S^G) = -4$, and one finds $\deg(h) = \sum \deg(f_i) - 4$, so there is an invariant in that degree that is not generated by the primary invariants, and any such invariant along with the primary invariants generates all invariants. Then one identifies such an h, completing the proof. □

Department of Mathematics, University of Nebraska, 203 Avery Hall, Lincoln, NE-68588, USA
Email address: jack.jeffries@unl.edu