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 $S = K[x_1, \ldots, x_n]$, 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

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

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 $S = K[V] = K[x_1, \ldots, x_n]$, 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:

$$S^G = K[x_1^2, x_1 x_2, \ldots, x_n^2].$$

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

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

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

We claim that there is some $h \in K[e_1, \dots, e_n]$ 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 $K[e_1, \dots, e_n]$, 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 $S = K[x_1, \dots, x_n]$ 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

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

To see this, note first that Δ^2 is a symmetric polynomial, and hence an element of $K[e_1, \dots, e_n]$. Thus, we can write $K[e_1, \dots, e_n, \Delta] = K[e_1, \dots, e_n] \oplus K[e_1, \dots, e_n] \cdot \Delta$. 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) $\operatorname{frac}(S^G) = \operatorname{frac}(S)^G$.
(3) S is an S^G-module of rank $|G|$.
(4) S^G is integrally closed in $\operatorname{frac}(S^G)$.

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

The containment $\operatorname{frac}(S^G) \subseteq \operatorname{frac}(S)^G$ is clear. Let $a/b \in \operatorname{frac}(S)^G$, 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 $a/b \in \operatorname{frac}(S)^G$ implies $a \in S^G$, so $a/b \in \operatorname{frac}(S^G)$.

The third statement follows from the second.

Now, let $a/b \in \operatorname{frac}(S^G)$ be integral over S^G. Then since $a/b \in \operatorname{frac}(S)$ 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

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

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

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

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 $\pi : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(S^G)$ 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.

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