

HOMOLOGICAL PROPERTIES OF INVARIANT RINGS OF PERMUTATION GROUPS

ARYAMAN MAITHANI

ABSTRACT. Consider the action of a subgroup G of the permutation group on the polynomial ring $S := k[x_1, \dots, x_n]$ via permutations. We show that if k does not have characteristic two, then the following are independent of k : the a -invariant of S^G , the property of S^G being quasi-Gorenstein, and the Hilbert functions of $H_{\mathfrak{m}}^n(S^G)$ as well as $H_{\mathfrak{n}}^n(S^G)$; moreover, these Hilbert functions coincide. In particular, being independent of characteristic, they may be computed using characteristic zero techniques, such as Molien's formula. In characteristic two, we show that the ring of invariants is always quasi-Gorenstein and compute the a -invariant explicitly, and show that the Hilbert functions of $H_{\mathfrak{m}}^n(S^G)$ and $H_{\mathfrak{n}}^n(S^G)$ agree up to a shift, given by the number of transpositions. Lastly, we determine when the inclusion $S^G \hookrightarrow S$ splits, thereby proving the Shank–Wehlau conjecture for permutation subgroups.

1. INTRODUCTION

Let k be a field, and G a subgroup of the permutation group \mathcal{S}_n . The group G has a natural action on the polynomial ring $S := k[x_1, \dots, x_n]$ via k -algebra automorphisms given by

$$\sigma \cdot x_i := x_{\sigma(i)}.$$

The **invariant subring** is $S^G := \{f \in S : \sigma(f) = f \text{ for all } \sigma \in G\}$. The invariant rings of permutation groups have a rich history in producing counterexamples to several questions, both within and outside the realm of invariant theory.

Outside the realm of invariant theory, Samuel [Sam] raised the following question: are all noetherian UFDs Cohen–Macaulay? The first counterexample to this question was given by Bertin [Ber]; namely the ring of invariants S^G of the permutation action of $\langle(1234)\rangle$ on $\mathbb{F}_2[w, x, y, z]$. Later, Fossum and Griffith [FG] showed that the completion of S^G at its homogeneous maximal ideal produces an example of a *complete* local UFD that is not Cohen–Macaulay.

Within the realm of invariant theory of finite groups, one considers more generally a finite subgroup $G \leqslant \mathrm{GL}_n(k)$ with its natural action on S via linear change of coordinates. When G is *nonmodular*, i.e., $\mathrm{char}(k)$ does not divide the order of G , one has a wealth of results such as:

- (1) the inclusion $S^G \hookrightarrow S$ splits S^G -linearly, and thus, the invariant ring S^G is Cohen–Macaulay;
- (2) (Noether's bound) the invariant ring is generated by invariants of degree at most the order of G ; and
- (3) there is an S^G -linear isomorphism $H_{\mathfrak{m}}^n(S^G) \cong H_{\mathfrak{n}}^n(S^G)$, where \mathfrak{m} and \mathfrak{n} denote the respective homogeneous maximal ideals of S and S^G .

Each of these is known to be false in the modular case; indeed, one can find counterexamples using permutation groups: for (1) and (2), consider the action of the cyclic permutation group $\langle(12)(34)(56)\rangle$ on $S := \mathbb{F}_2[x_1, \dots, x_6]$, and for (3), the action of the alternating group \mathcal{A}_3 on $\mathbb{F}_3[x_1, x_2, x_3]$ [GJS, Example 5.2].

In [Has], Hashimoto constructs examples of permutation groups G acting on a polynomial ring S such that S^G is F -rational but not F -regular. As a consequence of our results, this cannot happen if G is a subgroup of the alternating group; indeed, S^G is then quasi-Gorenstein [Corollary 5.2], and an F -rational ring is Cohen–Macaulay, and thus, S^G would then be Gorenstein, for which the notions of F -rationality and F -regularity coincide [HH2, Theorem 4.2 (g)].

2020 Mathematics Subject Classification. 13A50.

Key words and phrases. Polynomial invariants, modular invariant theory, permutation action, local cohomology.

The author was supported by NSF grants DMS 2101671 and DMS 2349623 and a Simons Dissertation Fellowship.

On the other hand, we now draw attention to the fact that permutation groups enjoy some ‘uniform’ properties stemming from the fact that the definition of the action is independent of the ground field. The key point here is that $S = k[x_1, \dots, x_n]$ has a k -basis given by monomials, and that any subgroup G of \mathcal{S}_n permutes the elements of this basis. This simple observation has the immediate consequence that S^G has a k -basis given by orbit sums of monomials; this description is independent of the ground field k , and in particular, we deduce that the Hilbert series of the invariant ring is independent of k . This description is also used to prove that S^G is F -pure when $G \leq \mathcal{S}_n$ [HH1, page 77]. Hashimoto and Singh [HS] show that S^G is F -pure and has finite F -representation type whenever G acts via permutations, or more generally, via a monomial representation. Many results of this paper are in this spirit: we show that various homological properties and invariants are independent of the ground field — at least when the characteristic is not two; this discrepancy can be attributed to the fact that the character $\text{sgn}: \mathcal{S}_n \rightarrow k^\times$ is trivial if $\text{char}(k) = 2$. Our main results can be summarised as follows:

Theorem. *Let k be a field, and G a subgroup of \mathcal{S}_n acting on the polynomial rings $S := k[x_1, \dots, x_n]$ and $S_{\mathbb{Q}} := \mathbb{Q}[x_1, \dots, x_n]$ via permutations. Let c be the number of transpositions in G , and N the subgroup generated by the transpositions. Let \mathfrak{m} and \mathfrak{n} denote the respective homogeneous maximal ideals of S and S^G .*

If $\text{char}(k) \neq 2$, then

- (1) *there is an isomorphism of graded k -vector spaces $H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)$, and the Hilbert functions of the top local cohomology modules of S^G and $S_{\mathbb{Q}}^G$ coincide;*
- (2) *the canonical module ω_{S^G} is isomorphic to $S_{\text{sgn}}^G(-n)$;*
- (3) *the a -invariants of S^G and $S_{\mathbb{Q}}^G$ coincide, and equal $\deg \text{Hilb}(S^G)$;*
- (4) *the ring S^G is quasi-Gorenstein if and only if $S_{\mathbb{Q}}^G$ is quasi-Gorenstein if and only if $a(S^G) = -(c + n)$; the latter can be checked using Molien’s formula.*

If $\text{char}(k) = 2$, then

- (1) *there is an isomorphism of graded k -vector spaces $H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)(-c)$;*
- (2) *the canonical module ω_{S^G} is isomorphic to $S^G(-c - n)$;*
- (3) *the a -invariant of S^G equals $-(c + n)$;*
- (4) *the ring S^G is quasi-Gorenstein.*

In any characteristic, we have

- (5) *the inclusion $S^G \hookrightarrow S$ splits S^G -linearly if and only if $\text{char}(k)$ does not divide $|G/N|$.*

The above statements are proven as (1) Corollary 4.7; (2) Corollary 4.6; (3) Corollary 4.8, which also describes the a -invariant in the odd characteristic; (4) Theorem 5.1 and Corollary 5.2; (5) Theorem 6.2.

Results (1)–(3) above are motivated by the work of Goel, Jeffries, and Singh [GJS] where they characterise when $a(S^G) = a(S)$ and show the following [ibid. Corollary 5.1]: if G is a cyclic subgroup of $\text{GL}_n(k)$ without transvections acting on $S = k[x_1, \dots, x_n]$, then $H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)$ as graded k -vector spaces. While they show that the “cyclic” hypothesis cannot be dropped in general, our result (1) above shows that it may be dropped for permutation groups. We note that permutation groups contain transvections only in characteristic two, in which case these are precisely the transpositions, accounting for the shift.

As a consequence of (5) above, we prove the Shank–Wehlau conjecture [SW, Conjecture 1.1] for permutation groups; the general conjecture may be stated as follows: Suppose $G \leq \text{GL}_n(k)$ is a finite p -group acting linearly on the ring $S := k[x_1, \dots, x_n]$, where $\text{char}(k) = p$. Then, $S^G \hookrightarrow S$ splits if and only if S^G is a polynomial ring. This formulation is due to Broer [Bro1, Corollary 4], who then proved the conjecture for abelian p -groups [Bro2]. Since then, this has been extended for some classes of p -groups by Elmer and Sezer [ES], and by Kummini and Mondal [KM1; KM2; KM3].

ACKNOWLEDGMENTS

The author thanks Jack Jeffries and Anurag K. Singh for several interesting discussions.

2. PRELIMINARIES

We collect some definitions and facts that will be used later. Throughout, we use k to denote a field, n a positive integer, $S := k[x_1, \dots, x_n]$ the polynomial ring with its standard grading, and $\mathrm{GL} := \mathrm{GL}_n(k)$ the general linear group with its natural degree-preserving action on S . The homogeneous maximal ideal of S is denoted by \mathfrak{m} , and $H_{\mathfrak{m}}^n(S)$ is the top local cohomology of S supported at \mathfrak{m} . Given a finite group G of GL , the natural action of GL on S restricts to one of G .

2.1. Graded modules. Given a graded module M and an integer d , we denote the d -th graded component of M by $[M]_d$. By $M(i)$ we shall mean the graded module given by $[M(i)]_d := M_{i+d}$. All graded modules that we consider will be component-wise finite-dimensional, i.e., $\mathrm{rank}_k [M]_d < \infty$ for all $d \in \mathbb{Z}$. The [Hilbert function](#) of M is the function $\mathbb{Z} \rightarrow \mathbb{N}$ given by $d \mapsto \mathrm{rank}_k [M]_d$. If M and N are graded modules with the same Hilbert function, then they are isomorphic as graded k -vector spaces, and we write this as $M \simeq N$. If $[M]_d = 0$ for $d < 0$, then the [Hilbert series](#) of M is defined to be the power series

$$\mathrm{Hilb}(M, t) := \sum_{d \geq 0} \mathrm{rank}_k ([M]_d) t^d \in \mathbb{Q}[[t]].$$

The Hilbert–Serre theorem asserts that the above power series is a rational function when M is finitely generated. Writing $\mathrm{Hilb}(M) = f/g$ for polynomials f and g , we define the [degree](#) of $\mathrm{Hilb}(M)$ to be the difference $\deg \mathrm{Hilb}(M) := \deg(f) - \deg(g)$.

2.2. The twisted group algebra. The [twisted group algebra](#) $S * G$ is the graded k -algebra defined as follows: as a k -vector space, we have $S * G := S \otimes_k kG$, and the multiplication is given as

$$(s \otimes \sigma) \cdot (t \otimes \tau) := s\sigma(t) \otimes \sigma\tau.$$

The above inherits a natural grading from that on S and kG , where the latter lives in degree zero. Concretely, if $s \in [S]_d$ and $\sigma \in G$, then the simple tensor $s \otimes \sigma$ is homogeneous of degree d .

Here is an alternative way to think about $S * G$ -modules: the data of an $S * G$ -module M is precisely the data of an S -module M equipped with a k -linear action of G satisfying $\sigma(sm) = \sigma(s)\sigma(m)$ for all $(\sigma, s, m) \in G \times S \times M$. Moreover, M is graded as an $S * G$ -module if it is so as an S -module and the G -action preserves the grading. In particular, $[M]_d$ is then a kG -module for every $d \in \mathbb{Z}$. Similarly, a function $f: M \rightarrow N$ between $S * G$ -modules is $S * G$ -linear precisely if it is S -linear and G -equivariant; the latter means that we have $f(\sigma(m)) = \sigma(f(m))$ for all $(\sigma, m) \in G \times M$.

2.3. Twisted representation and semi-invariants. Given a character, i.e., a homomorphism $\chi: G \rightarrow k^\times$, and a graded $S * G$ -module M , we define $M \otimes \chi$ to be the graded $S * G$ -module $M \otimes_k k$ with the actions

$$s \cdot (m \otimes 1) := sm \otimes 1 \quad \text{and} \quad \sigma \cdot (m \otimes 1) := \sigma(m) \otimes \chi(\sigma)$$

for $(\sigma, s, m) \in G \times S \times M$. In particular, M and $M \otimes \chi$ are isomorphic as graded S -modules.

The module of [\\$\chi\\$-semi-invariants](#) is defined as

$$S_\chi^G := \{s \in S : \sigma(s) = \chi(\sigma)s \text{ for all } \sigma \in G\},$$

which is isomorphic to $(S \otimes \chi^{-1})^G$ as a graded S^G -module.

2.4. Duals. Given a finite kG -module V , we define its dual V^\vee to be the k -vector space $\mathrm{Hom}_k(V, k)$ with the action of G given by

$$(\sigma \cdot f)(v) := f(\sigma^{-1}v)$$

for $(\sigma, v, f) \in G \times V \times V^\vee$. This makes V^\vee a kG -module.

Next, given a graded $S * G$ -module M , we define its graded dual M^* to be the following graded $S * G$ -module: the degree d component is the kG -module $([M]_{-d})^\vee = \mathrm{Hom}_k([M]_{-d}, k)$, and given homogeneous elements $s \in [S]_e$ and $f \in [M^*]_d$, we define $(s \cdot f) \in [M^*]_{d+e}$ via

$$(s \cdot f)(m) := f(s \cdot m), \quad \text{for } m \in [M]_{-d-e}.$$

Both the duals above have an obvious definition on maps, yielding contravariant endofunctors on the categories of kG -modules and graded $S * G$ -modules, respectively.

We shall also use $(-)^*$ as an endofunctor on the category of graded S -modules and S^G -modules, with the analogous definitions.

2.5. Pseudoreflections. An element $\sigma \in \mathrm{GL}$ is a [pseudoreflection](#) if $\mathrm{rank}(1 - \sigma) = 1$, in which case, $\ker(1 - \sigma)$ is a hyperplane. A non-diagonalisable pseudoreflection is a [transvection](#). The element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a pseudoreflection in every characteristic, but a transvection precisely in characteristic two. More generally, viewing \mathcal{S}_n as a subgroup of $\mathrm{GL}_n(k)$ via permutation matrices, we see that the pseudoreflections are exactly the transpositions, and that these are transvections precisely when $\mathrm{char}(k) = 2$.

2.6. Local cohomology. In this subsection, we record how the group GL acts on the top local cohomology module $H_m^n(S)$. Following Kunz [Kun, §4], we use the notion of generalised fractions to represent the elements of local cohomology. A generalised fraction is an element of the form

$$\left[\frac{f}{t_1, \dots, t_n} \right],$$

where $f \in S$, and t_1, \dots, t_n is a homogeneous system of parameters for S . The above fraction represents (the cohomology class of) the element $\frac{f}{t_1, \dots, t_n}$ in the Čech complex $\check{\mathbf{C}}^\bullet(t_1, \dots, t_n)$. If t'_1, \dots, t'_n is another such system of parameters contained in $(t_1, \dots, t_n)S$, and A is an $n \times n$ matrix over S satisfying

$$(TL) \quad \left[\frac{t'_1}{t'_n} \right] = A \left[\frac{t_1}{t_n} \right], \quad \text{then} \quad \left[\frac{f}{t_1, \dots, t_n} \right] = \left[\frac{\det(A)f}{t'_1, \dots, t'_n} \right],$$

by [Kun, Theorem 4.18]. Using this, any two generalised fractions can be modified to have a common denominator. We remark that the transformation rule above, in particular, implies that the order of the elements in the denominator is relevant: swapping two elements in the denominator changes the fraction by a sign.

The action of GL on $H_m^n(S)$ is given in the natural way: given $\sigma \in \mathrm{GL}$ and $t \in S$, we first obtain an S^G -linear map $\sigma: R_t \longrightarrow R_{\sigma(t)}$ given by $f/t^N \longmapsto \sigma(f)/\sigma(t)^N$. Extending this in the obvious manner, we obtain an S^G -linear map of Čech complexes $\sigma: \check{\mathbf{C}}(t_1, \dots, t_n) \longrightarrow \check{\mathbf{C}}(\sigma(t_1), \dots, \sigma(t_n))$, giving us

$$\sigma \cdot \left[\frac{f}{t_1, \dots, t_n} \right] = \left[\frac{\sigma(f)}{\sigma(t_1), \dots, \sigma(t_n)} \right]$$

for $(\sigma, f) \in G \times S$, and t_1, \dots, t_n any homogeneous system of parameters.

Theorem 2.1 (Graded duality). *There is a GL -equivariant isomorphism of graded S -modules*

$$(S \otimes \det)^* \cong H_m^n(S)(-n),$$

where $\det = \det_{[S]_1}$.

We clarify the above notation regarding the character \det , as it may differ in the literature: often, S arises as the symmetric algebra on the dual space V^* , in which case, we have $\det_{[S]_1} = \det_V^{-1}$. To be explicit, if $\sigma \in \mathrm{GL}$ acts on S via $x_i \longmapsto \alpha_i x_i$, then we have $\det_{[S]_1}(\sigma) = \alpha_1 \cdots \alpha_n$.

For the purpose of this paper, we only use that the above isomorphism is \mathcal{S}_n -equivariant, for which the result follows directly from the transformation law (TL). We expect that the above is likely well-known to experts but failing to find a reference in the literature, we provide a proof below.

Proof. Graded duality [ILL+, Theorem 18.6] tells us that $S^* \cong H_m^n(S)(-n)$ as graded S -modules; hence, there is a graded S -isomorphism

$$\Phi: H_m^n(S)(-n) \longrightarrow (S \otimes \det)^*.$$

Setting $H := H_{\mathfrak{m}}^n(S)(-n)$ and $D := (S \otimes \det)^*$, we wish to show that $\Phi(\sigma(\eta)) = \sigma(\Phi(\eta))$ for all $\sigma \in \mathrm{GL}$ and all homogeneous $\eta \in H$. If η is a socle element, i.e., of degree zero, then this is clear in view of the transformation law (TL) because the action of σ on both $[H]_0$ and $[D]_0$ is scaling by $\det(\sigma^{-1})$. Next, fix $d > 0$, $\eta \in [H]_{-d}$, and $\sigma \in \mathrm{GL}$. Then, given any $s \in [S]_d$, the element $s\eta$ is in the socle, and thus,

$$\Phi(\sigma(s\eta)) = \sigma(\Phi(s\eta)).$$

Using the S -linearity of Φ and the fact that H and D are $S * \mathrm{GL}$ -modules, we rewrite both sides of the above equation to obtain

$$\begin{aligned} \Phi(\sigma(s\eta)) &= \sigma(\Phi(s\eta)) \\ \Rightarrow \Phi(\sigma(s)\sigma(\eta)) &= \sigma(s\Phi(\eta)) \\ \Rightarrow \sigma(s)\Phi(\sigma(\eta)) &= \sigma(s)\sigma(\Phi(\eta)) \\ \Rightarrow \sigma(s)[\Phi(\sigma(\eta)) - \sigma(\Phi(\eta))] &= 0 \end{aligned}$$

for all $s \in [S]_d$. Thus, the element $\delta := [\Phi(\sigma(\eta)) - \sigma(\Phi(\eta))] \in [D]_{-d}$ is annihilated by $[S]_d$. Because the pairing $[S]_d \times [D]_{-d} \rightarrow [D]_0$ is nondegenerate, we get $\delta = 0$, giving us the desired GL -equivariance. \square

Corollary 2.2. *As graded S^G -modules, one has*

$$((S \otimes \det)^*)^G \cong H_{\mathfrak{m}}^n(S)^G(-n).$$

3. TWISTED PERMUTATION REPRESENTATIONS

Let $\chi: G \rightarrow k^\times$ be a homomorphism, and V a finite kG -module. We say that V is a χ -permutation representation if there exists a k -basis $B = \{e_1, \dots, e_n\}$ of V and an action of G on $[n] := \{1, \dots, n\}$ such that the action of G on V is given by

$$\sigma(e_i) = \chi(\sigma)e_{\sigma(i)}$$

for $\sigma \in G$; such a basis B is a χ -basis. For the remainder of this section, we fix V and B as above.

An element $i \in [n]$ is χ -good if the stabiliser of i is contained in the kernel of χ , i.e., $\mathrm{Stab}_G(i) \subseteq \ker(\chi)$. The orbit $G \cdot i \subseteq [n]$ is χ -good if i is χ -good; this is independent of the orbit representative. Fix orbit representatives $a_1, \dots, a_r \in [n]$ such that we have a disjoint orbit decomposition

$$[n] = G \cdot a_1 \sqcup \cdots \sqcup G \cdot a_r.$$

Let $s \leq r$ be the number of χ -good orbits, and assume without loss of generality that a_1, \dots, a_s are χ -good. For each such $i \in [s]$, we define the *twisted orbit sum*

$$X(a_i) := \sum_{\sigma \in G / \mathrm{Stab}_G(a_i)} \chi(\sigma) e_{\sigma(a_i)} \in V,$$

where the above is well-defined (independent of the choice of coset representatives) because a_i is χ -good. A routine verification shows that $X(a_i) \in V^G$ for each $i \in [s]$. As the distinct $X(a_i)$ involve disjoint sets of basis vectors, we see that the set $C := \{X(a_i) : i \in [s]\}$ is k -linearly independent. If $f = \sum_{j=1}^n \alpha_j e_j \in V^G$, then for every $\sigma \in G$ and $j \in [n]$, we must have $\alpha_{\sigma(j)} = \alpha_j \chi(\sigma)$. In particular, if j is not χ -good, then choosing $\sigma \in \mathrm{Stab}_G(j) \setminus \ker(\chi)$ shows that $\alpha_j = 0$. Thus, the condition gives us

$$f = \sum_{i=1}^s \alpha_{a_i} X(a_i).$$

In other words, C is a k -basis for V^G , giving us:

Proposition 3.1. *The dimension of V^G is the number of χ -good orbits.* \square

Next, we analyse the dual module V^\vee . Let $\{e_1^*, \dots, e_n^*\}$ be the dual basis for V^\vee , determined by

$$e_i^*(e_j) = \delta_{i,j},$$

where δ denotes the Kronecker delta. Then, the function $\sigma \cdot e_i^* \in V^\vee$ is given as

$$\begin{aligned} (\sigma \cdot e_i^*)(e_j) &= e_i^*(\sigma^{-1}(e_j)) = e_i^*(\chi(\sigma^{-1})(e_{\sigma^{-1}(j)})) \\ &= \chi(\sigma^{-1})\delta_{i,\sigma^{-1}(j)} = \chi(\sigma^{-1})\delta_{\sigma(i),j}. \end{aligned}$$

Thus, $\sigma \cdot e_i^* = \chi(\sigma)^{-1}e_{\sigma(i)}^*$; letting $\chi^{-1}: G \rightarrow k^\times$ denote the multiplicative-inverse gives us:

Proposition 3.2. *The dual V^\vee is a χ^{-1} -permutation representation with $\{e_1^*, \dots, e_n^*\}$ being a χ^{-1} -basis. As k -vector spaces, we have $(V^G)^\vee \cong (V^\vee)^G$. If χ takes values in $\{\pm 1\}$, then the map $e_i \mapsto e_i^*$ induces a kG -module isomorphism.*

Proof. Only the second statement needs a proof, for which we note that $i \in [n]$ is χ -good if and only if it is χ^{-1} -good, and thus, the dimensions of V^G and $(V^\vee)^G$ are the same. \square

Remark 3.3. In the modular case, one cannot always commute duals and fixed points, as this example shows: Consider the group G generated by $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ with its canonical action on $V := k^3$, and corresponding dual action on V^\vee . We have $\dim V^G = 1 \neq 2 = \dim(V^\vee)^G$. Indeed, V^G is spanned by e_1 and $(V^\vee)^G$ by $\{e_2^*, e_3^*\}$.

4. INVARIANTS OF LOCAL COHOMOLOGY AND LOCAL COHOMOLOGY OF INVARIANTS

For the remainder of this paper, we fix G to be a subgroup of S_n with its permutation action on $S := k[x_1, \dots, x_n]$. In this case, the character \det coincides with the usual character $\text{sgn}: S_n \rightarrow k^\times$. Moreover, in the terminology of Section 3, each graded component $[(S \otimes \det)]_d = [(S \otimes \text{sgn})]_d$ is a sgn -permutation representation of G , with the monomials of degree d being a sgn -basis. When $\text{char}(k) = 2$, sgn is trivial, and thus, every monomial is sgn -good; in other characteristics, the sgn -good monomials are precisely those whose stabiliser is contained in the alternating group A_n . This observation has the following immediate consequences:

Theorem 4.1. *Let $G \leq S_n$ act on S by permutations. If $\text{char}(k) \neq 2$, then the Hilbert series of S_{sgn}^G is given as*

$$\text{Hilb}(S_{\text{sgn}}^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{\text{sgn}(\sigma)}{\det(1 - \sigma t)}.$$

If $\text{char}(k) = 2$, then $S_{\text{sgn}}^G = S^G$, and the Hilbert series is given as

$$\text{Hilb}(S_{\text{sgn}}^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(1 - \sigma t)}.$$

The right hand sides of both the equations above are to be interpreted as elements of $\mathbb{Q}(t)$.

Proof. It is known that for permutation actions, the Hilbert series of S^G can be computed over characteristic zero using the Molien series, see [Smi, Proposition 4.3.4]. This proves the statement for characteristic two.

Now let us assume that $\text{char}(k) \neq 2$. As noted earlier, the sgn -good monomials are then independent of characteristic, and thus, we may compute the Hilbert series using Molien's formula for semi-invariants in characteristic zero [Ben, Theorem 2.5.3]. \square

Theorem 4.2. *If $G \leq S_n$ acts on S via permutations, then we have an isomorphism of graded k -vector spaces*

$$H_{\mathfrak{m}}^n(S)^G(-n) \simeq (S_{\text{sgn}}^G)^*.$$

Coupled with Theorem 4.1, this yields a formula for the Hilbert function of $H_{\mathfrak{m}}^n(S)^G$.

Proof. In view of Corollary 2.2, one only needs to prove that

$$((S \otimes \text{sgn})^*)^G \simeq ((S \otimes \text{sgn})^G)^*,$$

and this follows from Proposition 3.2. \square

Our next goal is to compare $H_{\mathfrak{m}}^n(S)^G$ with $H_{\mathfrak{n}}^n(S^G)$, where \mathfrak{n} is the homogeneous maximal ideal of S^G . To this end, we define the [canonical module](#) of S^G as $\omega_{S^G} := H_{\mathfrak{n}}^n(S^G)^*$.

We follow [Bro1] to compute the canonical module. By [ibid. Corollary 7], we have

$$(4.1) \quad \omega_{S^G} \cong S_{\text{sgn}/\chi}^G \theta(-n),$$

where $\theta \in S$ will be described below, and $\chi: G \rightarrow k^\times$ is the homomorphism defined by

$$(4.2) \quad \chi(\sigma) := \frac{\sigma(\theta)}{\theta}.$$

Let $T \subseteq G$ be the subset of all transpositions in G , and $N := \langle T \rangle$ the subgroup generated by the transpositions.

We now describe θ following [Bro1, §2.6]: Let W_1, \dots, W_s be the different hyperplanes that arise as fixed points of elements of G . For each W_i , let $\alpha_i \in [S]_1$ be a nonzero linear form that vanishes on W_i , and let $H_i \leq G$ be the pointwise stabiliser of W_i . Let p be the characteristic of k if this is positive, else let $p = 1$. Then, we may write $|H_i| := e_i p^{a_i}$ with e_i coprime to p . Because our representation is defined over the prime subfield, we have $\theta = \alpha_1^{m_1} \cdots \alpha_n^{m_n}$, where $m_i := e_i + (p-1)a_i - 1$.

Proposition 4.3. *We have $\theta = \prod_{(i,j) \in T} (x_i - x_j)$, and thus, $\deg \theta = |T|$, the number of transpositions in G .*

Proof. The pseudoreflections in G are precisely the transpositions. Given a transposition $\tau = (i, j)$ in T , the pointwise-stabiliser of the hyperplane V^τ is precisely $\langle \tau \rangle$, which has order 2, and the corresponding linear form defining the hyperplane is $x_i - x_j$. This gives us the required statement. \square

Lemma 4.4. *Suppose $\text{char}(k) \neq 2$, and $f \in S$ satisfies $\tau(f) = -f$ for all $\tau \in T$. Then, $f \in \theta S$.*

Proof. Let $(i, j) \in T$ be a transposition. The hypothesis on f implies that f vanishes when $x_i = x_j$, and in turn, $x_i - x_j$ divides f . As these factors are coprime for distinct transpositions, we get the desired result. \square

Corollary 4.5. *If $\text{char}(k) = 2$, then $S_{\text{sgn}/\chi}^G = S^G$. If $\text{char}(k) \neq 2$, then $S_{\text{sgn}/\chi}^G \theta = S_{\text{sgn}}^G$.*

Proof. If $\text{char}(k) = 2$, then χ must be valued in \mathbb{F}_2^\times , and thus, χ and sgn are both trivial.

Now, suppose that $\text{char}(k) \neq 2$. By definition, we have that $\theta \in S_\chi^G$, and thus, $S_{\text{sgn}/\chi}^G \theta \subseteq S_{\text{sgn}}^G$. The reverse inclusion follows similarly, in view of Lemma 4.4. \square

Corollary 4.6. *Let $G \leq \mathcal{S}_n$ act on the polynomial ring $S = k[x_1, \dots, x_n]$ by permutations. Let c be the number of transpositions in G . We have the following isomorphisms as graded S^G -modules:*

- (1) *If $\text{char}(k) = 2$, then $\omega_{S^G} \cong S^G(-c - n)$. Equivalently, $H_{\mathfrak{n}}^n(S^G) \cong (S^G)^*(c + n)$.*
- (2) *If $\text{char}(k) \neq 2$, then $\omega_{S^G} \cong S_{\text{sgn}}^G(-n)$. Equivalently, $H_{\mathfrak{n}}^n(S^G) \cong (S_{\text{sgn}}^G)^*(n)$.*

Proof. The descriptions of ω_{S^G} follow from (4.1) and Corollary 4.5, and the rest from $\omega_{S^G}^* \cong H_{\mathfrak{n}}^n(S^G)$. \square

Putting this together with the isomorphism $H_{\mathfrak{m}}^n(S)^G(-n) \cong (S_{\text{sgn}}^G)^*$ from Theorem 4.2 gives us:

Corollary 4.7. *Let $G \leq S_n$ act on S by permutations. Let c be the number of transpositions in G . We have the following isomorphisms as graded k -vector spaces:*

(1) *If $\text{char}(k) = 2$, then $H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)(-c)$.*

(2) *If $\text{char}(k) \neq 2$, then $H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)$.* □

Recalling that the transpositions are transvections in characteristic two, and that there are no transvections in other characteristics, letting t denote the number of transvections gives us the characteristic-free statement:

$$H_{\mathfrak{m}}^n(S)^G \simeq H_{\mathfrak{n}}^n(S^G)(-t),$$

as graded k -vector spaces. Note that while both the objects above are graded S^G -modules, they need not be isomorphic as S^G -modules in the modular case, see [GJS, Example 5.2]. We also remark that outside the realm of permutation groups, even an isomorphism as graded vector spaces may not exist, see [GJS, Example 5.3].

We also deduce the a -invariant of S^G from Corollary 4.6. Recall that the *a -invariant* is the largest integer a such that $[H_{\mathfrak{n}}^n(S^G)]_a \neq 0$. If S^G is Cohen–Macaulay, then the a -invariant of S^G equals the degree of its Hilbert series. These statements can be found in [BH].

Corollary 4.8. *Let $G \leq S_n$ act on $S = k[x_1, \dots, x_n]$ by permutations. Let c be the number of transpositions in G .*

(1) *If $\text{char}(k) = 2$, then $a(S^G) = -(c + n)$.*

(2) *If $\text{char}(k) \neq 2$, then $a(S^G) = -(d + n)$, where d is the minimal degree of a monomial in S whose stabiliser is contained in the alternating group A_n . We also have $a(S^G) = \deg \text{Hilb}(S^G)$.*

In particular, the a -invariant is the same across all characteristics not equal to two.

Proof. Statement (1) is clear from Corollary 4.6. For (2), we first need to check that the lowest nonzero component of S_{sgn}^G is in degree d as defined in the corollary statement. This follows from the discussion preceding Theorem 4.1. Thus, $a(S^G) = -(d + n)$ is independent of characteristic (not equal to two). In the case of characteristic zero, S^G is Cohen–Macaulay, and thus, $a(S^G) = \deg \text{Hilb}(S^G)$. □

5. QUASI-GORENSTEIN

Continuing our earlier hypothesis of $G \leq S_n$ acting on $S := k[x_1, \dots, x_n]$, our next goal is to characterise when S^G is *quasi-Gorenstein*, i.e., $\omega_{S^G} \cong S^G(a)$, for some $a \in \mathbb{Z}$, in which case we must necessarily have $a = a(S^G)$. Thus, the ring S^G is Gorenstein precisely when it is Cohen–Macaulay and quasi-Gorenstein. Corollary 4.6 tells us that S^G is always quasi-Gorenstein in characteristic two. In a similar vein as before, we next show that quasi-Gorensteinness is independent of the base field in all other characteristics, and thus, we may reduce to characteristic zero where we have the theorems of Stanley [Sta] and Watanabe [Wat] characterising the Gorenstein property of invariant rings.

Theorem 5.1. *Let $G \leq S_n$ act by permutations. If $\text{char}(k) \neq 2$, then the following are equivalent:*

- (1) *The ring $k[x_1, \dots, x_n]^G$ is quasi-Gorenstein.*
- (2) *The character sgn/χ is trivial.*
- (3) *The ring $\mathbb{Q}[x_1, \dots, x_n]^G$ is quasi-Gorenstein, equivalently, Gorenstein.*

Proof. The equivalence (1) \Leftrightarrow (2) is [Bro1, Corollary 7 (iv)]. Thus, it suffices to show that the equality $\text{sgn} = \chi$ holds over k if and only if it holds over \mathbb{Q} . We now analyse χ using Proposition 4.3 and (4.2). For concreteness, we may modify θ up to a sign and assume that every factor $x_i - x_j$ of θ satisfies $i < j$. Then, $\chi(\sigma) = (-1)^s$, where s is the cardinality of the set $\{(i, j) \in T : i < j \text{ and } \sigma(i) > \sigma(j)\}$. Thus, both sgn and χ take values in $\{1, -1\}$, and equality can be checked over any field where $1 \neq -1$. □

Corollary 5.2. *Let $G \leqslant S_n$ act on S by permutations, and let c be the number of transpositions in G . The ring S^G is quasi-Gorenstein if and only if $a(S^G) = -(c + n)$. More precisely,*

- (1) *if $\text{char}(k) = 2$, then S^G is quasi-Gorenstein;*
- (2) *if $\text{char}(k) \neq 2$, then S^G is quasi-Gorenstein if and only if $\deg \text{Hilb}(S^G) = -(c + n)$. In particular, if G contains no transpositions, then S^G is quasi-Gorenstein if and only if G is contained in A_n .*

Proof. For $\text{char}(k) = 2$, the statement is a consequence of Corollary 4.6. Let us now assume that $\text{char}(k) \neq 2$. Then, by Theorem 5.1, we may assume that $k = \mathbb{Q}$. Equation (4.1) tells us that $\omega_{S^G} \cong S_{\text{sgn}/\chi}^G(-c - n)$ as $\deg \theta = c$. Thus, $a(S^G) = -(c + n)$ if and only if sgn/χ is trivial if and only if S^G is quasi-Gorenstein. Finally, if G contains no transpositions, then Watanabe's theorems [Wat] tell us that S^G is (quasi-)Gorenstein precisely when \det is trivial, i.e., precisely when $G \leqslant A_n$. \square

6. THE DIRECT SUMMAND PROPERTY

In this section, we characterise when S^G is a direct summand of S , i.e., the inclusion $S^G \hookrightarrow S$ splits S^G -linearly. This always happens in characteristic zero, whereas in positive characteristic, this happens precisely when S^G is *F-regular*. As a consequence of our characterisation, we show that the Shank–Wehlau conjecture is true for permutation subgroups [Corollary 6.3].

As before, G is a subgroup of S_n acting on $S := k[x_1, \dots, x_n]$ via permutations, and N is the (normal) subgroup generated by the transpositions in G .

Proposition 6.1. *The ring S^N is regular, i.e., a polynomial ring.*

Proof. It is well-known that N , being generated by transpositions, is equal to the subgroup $S_{A_1} \times \dots \times S_{A_r} \subseteq S_n$, where $\{A_1, \dots, A_r\}$ is a partition of $\{1, \dots, n\}$.¹ Thus, S^N is a polynomial ring [DK, Theorem 3.10.1]. \square

Theorem 6.2. *Let $G \leqslant S_n$ act on $S = k[x_1, \dots, x_n]$ via permutations, and let $N \leqslant G$ be the subgroup generated by the transpositions in G . The inclusion $S^G \hookrightarrow S$ splits if and only if $\text{char}(k)$ does not divide $|G/N|$.*

Proof. By [Bro1, Theorem 2], the inclusion $S^G \hookrightarrow S$ splits if and only if the inclusion $S^N \hookrightarrow S$ splits and $\text{char}(k)$ does not divide $|G/N|$. But S^N is regular by Proposition 6.1, and thus, $S^N \hookrightarrow S$ is split. \square

Corollary 6.3. *If $\text{char}(k) = p$ and $G \leqslant S_n$ is a p -group such that $S^G \hookrightarrow S$ splits, then S^G is a polynomial ring.*

Proof. By Theorem 6.2, we get that $G = N$, and thus, $S^G = S^N$ is a polynomial ring by Proposition 6.1. \square

Corollary 6.4. *If $G \leqslant S_n$ is such that $k[x_1, \dots, x_n]^G$ is F-regular for all fields k of positive characteristic, then G is generated by transpositions, and in turn, S^G is a polynomial ring.*

Proof. In view of Theorem 6.2, the hypothesis forces $G = N$. \square

We compare the above with [BM] which says: If $G \leqslant S_n$ and $k[x_1, \dots, x_n]^G$ is Cohen–Macaulay for all fields k (of positive characteristic), then G is generated by bireflections, i.e., elements σ satisfying $\text{rank}(1 - \sigma) \leqslant 2$.

¹To see this, define an equivalence relation on $[n]$ given by $i \sim j$ iff $i = j$ or $(i, j) \in N$. The equivalence classes give us the partition.

REFERENCES

- [Ben] D. J. Benson. *Polynomial invariants of finite groups*. Vol. 190. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1993, pp. x+118. [6](#)
- [Ber] Marie-José Bertin. “Anneaux d’invariants d’anneaux de polynomes, en caractéristique p ”. In: *C. R. Acad. Sci. Paris Sér. A-B* 264 (1967), A653–A656. [1](#)
- [BH] Winfried Bruns and Jürgen Herzog. “On the computation of a -invariants”. In: *Manuscripta Math.* 77.2-3 (1992), pp. 201–213. [8](#)
- [BM] Ben Blum-Smith and Sophie Marques. “When are permutation invariants Cohen-Macaulay over all fields?” In: *Algebra Number Theory* 12.7 (2018), pp. 1787–1821. [9](#)
- [Bro1] Abraham Broer. “The direct summand property in modular invariant theory”. In: *Transform. Groups* 10.1 (2005), pp. 5–27. [2](#), [7–9](#)
- [Bro2] Abraham Broer. “Invariant theory of abelian transvection groups”. In: *Canad. Math. Bull.* 53.3 (2010), pp. 404–411. [2](#)
- [DK] Harm Derksen and Gregor Kemper. *Computational invariant theory*. enlarged. Vol. 130. Encyclopaedia of Mathematical Sciences. With two appendices by Vladimir L. Popov, and an addendum by Norbert A’Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII. Springer, Heidelberg, 2015, pp. xxii+366. [9](#)
- [ES] Jonathan Elmer and Müfit Sezer. “Locally finite derivations and modular coinvariants”. In: *Q. J. Math.* 69.3 (2018), pp. 1053–1062. [2](#)
- [FG] Robert M. Fossum and Phillip A. Griffith. “Complete local factorial rings which are not Cohen-Macaulay in characteristic p ”. In: *Ann. Sci. École Norm. Sup. (4)* 8.2 (1975), pp. 189–199. [1](#)
- [GJS] Kriti Goel, Jack Jeffries, and Anurag K. Singh. “Local Cohomology of Modular Invariant Rings”. In: *Transformation Groups* (Mar. 2024). [1](#), [2](#), [8](#)
- [Has] Mitsuyasu Hashimoto. “ F -rationality of the ring of modular invariants”. In: *J. Algebra* 484 (2017), pp. 207–223. [1](#)
- [HH1] Melvin Hochster and Craig Huneke. “Infinite integral extensions and big Cohen-Macaulay algebras”. In: *Ann. of Math. (2)* 135.1 (1992), pp. 53–89. [2](#)
- [HH2] Melvin Hochster and Craig Huneke. “ F -regularity, test elements, and smooth base change”. In: *Trans. Amer. Math. Soc.* 346.1 (1994), pp. 1–62. [1](#)
- [HS] Mitsuyasu Hashimoto and Anurag K. Singh. “Frobenius representation type for invariant rings of finite groups”. In: *Adv. Math.* 458 (2024), Paper No. 109978. [2](#)
- [ILL+] Srikanth B. Iyengar, Graham J. Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag K. Singh, and Uli Walther. *Twenty-four hours of local cohomology*. Vol. 87. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2007, pp. xviii+282. [4](#)
- [KM1] Manoj Kummini and Mandira Mondal. “On Hilbert ideals for a class of p -groups in characteristic p ”. In: *Proc. Amer. Math. Soc.* 150.1 (2022), pp. 145–151. [2](#)
- [KM2] Manoj Kummini and Mandira Mondal. “On polynomial invariant rings in modular invariant theory”. In: *J. Pure Appl. Algebra* 228.12 (2024), Paper No. 107758, 15. [2](#)
- [KM3] Manoj Kummini and Mandira Mondal. “Ramification in modular invariant rings”. 2025. arXiv: [2502.17228](https://arxiv.org/abs/2502.17228) [math.AC]. [2](#)
- [Kun] Ernst Kunz. *Residues and duality for projective algebraic varieties*. Vol. 47. University Lecture Series. With the assistance of and contributions by David A. Cox and Alicia Dickenstein. American Mathematical Society, Providence, RI, 2008, pp. xiv+158. [4](#)
- [Sam] Pierre Samuel. “On unique factorization domains”. In: *Illinois J. Math.* 5 (1961), pp. 1–17. [1](#)
- [Smi] Larry Smith. *Polynomial invariants of finite groups*. Vol. 6. Research Notes in Mathematics. A K Peters, Ltd., Wellesley, MA, 1995, pp. xvi+360. [6](#)
- [Sta] Richard P. Stanley. “Invariants of finite groups and their applications to combinatorics”. In: *Bull. Amer. Math. Soc. (N.S.)* 1.3 (1979), pp. 475–511. [8](#)
- [SW] R. James Shank and David L. Wehlau. “The transfer in modular invariant theory”. In: *J. Pure Appl. Algebra* 142.1 (1999), pp. 63–77. [2](#)
- [Wat] Keiichi Watanabe. “Certain invariant subrings are Gorenstein. I, II”. In: *Osaka Math. J.* 11 (1974), 1–8, ibid. 11 (1974), 379–388. [8](#), [9](#)