# POLYNOMIAL INVARIANTS OF CLASSICAL SUBGROUPS OF GL<sub>2</sub>: CONJUGATION OVER FINITE FIELDS

## ARYAMAN MAITHANI

ABSTRACT. Consider the conjugation action of the general linear group  $GL_2(K)$  on the polynomial ring  $K[X_{2\times 2}]$ . When K is an infinite field, the ring of invariants is a polynomial ring generated by the trace and the determinant. We describe the ring of invariants when K is a finite field, and show that it is a hypersurface. We also consider the other classical subgroups, and the polynomial rings corresponding to other subspaces of matrices such as the traceless and symmetric matrices. In each case, we show that the invariant ring is either a polynomial ring or a hypersurface.

#### 1. Introduction

Let K be a field, and consider the *conjugation action* of the general linear group  $G = \operatorname{GL}_2(K)$  on the polynomial ring  $S = K[X_{2\times 2}] = k[x_{11}, x_{12}, x_{21}, x_{22}]$ : if X denotes the square matrix of variables, then the element  $\sigma \in G$  acts by mapping  $x_{ij}$  to the (i, j)-th entry of  $\sigma^{-1}X\sigma$ . When K is infinite, the ring of invariants is generated by the trace and determinant, i.e.,  $S^G = K[\operatorname{trace} X, \operatorname{det} X]$ . More generally, one may consider the conjugation action of  $\operatorname{GL}_n(K)$  on  $K[X_{n\times n}]$ . When the field K is infinite,  $K[X_{n\times n}]^{\operatorname{GL}_n(K)}$  is classically known to be generated by the coefficients of the characteristic polynomial of X, see for example [DK, Example 2.1.3]. It is easy to see that this can not hold when the field K is finite: indeed, K is then a finite group and thus, the Krull dimensions of K and K0 must be the same, telling us that the invariant subring is larger. The first part of the paper concerns the following description of K1 when K2 is finite, expanding on the work of Larry Smith [Sm2].

**Theorem 1.1.** Let K be a finite field with q elements. Consider the conjugation action of the general linear group  $G := \operatorname{GL}_2(K)$  on the polynomial ring  $S := K[X_{2 \times 2}]$ . Let  $f_1 = \operatorname{trace}$ ,  $f_2 = \det$ ,  $f_3 = \mathscr{P}^1(\det)$ , and  $f_4$  be the primary invariants as in Definition 3.1, and R the K-subalgebra generated by them. Then,  $S^G = K[f_1, f_2, f_3, f_4, h]$  for a secondary invariant h of degree  $q^2$ . More precisely, we have the decomposition  $S^G = R \oplus Rh$  as R-modules. In particular,  $S^G$  is a hypersurface with Hilbert series given as

$$\mathrm{Hilb}(S^G,z) = \frac{1+z^{q^2}}{(1-z)(1-z^2)(1-z^{q+1})(1-z^{q^2-q})}.$$

Additionally, the invariant ring  $S^G$  does not split from S (equivalently,  $S^G$  is not F-regular), has a-invariant -4, and is a unique factorisation domain precisely when the characteristic of K is two. If the characteristic is odd, then the class group of  $S^G$  is  $\mathbb{Z}/2$ , and the secondary invariant K can be chosen to be the Jacobian of the K in which case, we have  $K^G$  is K.

In the other parts of the paper, we consider the conjugation action for the other classical subgroups of  $GL_2(K)$ , namely, the *special linear group*  $SL_2(K)$  and the *orthogonal group*  $O_2(K)$ . Note that the *symplectic group*  $Sp_2(K)$  coincides with  $SL_2(K)$ . For each of these groups, we first consider the *generic* conjugation action, i.e., the conjugation action on the space  $\mathfrak{gl}_2$  of  $2 \times 2$  matrices. Next, we consider the conjugation actions of  $GL_2$  and  $GL_2$  on the space  $GL_2$  of traceless matrices, and the conjugation action of  $GL_2$  on the space  $GL_2$  of alternating matrices and on the space of symmetric matrices. In particular, this includes the *adjoint representation* of each classical group—the action of an algebraic group on its Lie algebra, induced by conjugation.

<sup>2020</sup> Mathematics Subject Classification. 13A50.

Key words and phrases. Conjugation action, polynomial invariants, finite fields.

The author was supported by NSF grants DMS 2101671 and DMS 2349623.

Group	Space	<b>K</b>	Primary invariants	Туре	UFD	Reference
$\operatorname{GL}_2(K)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	even	trace, det, $\mathscr{P}^1(\det)$ , $f_4$	Hypersurface	Yes	Theorem 1.1
		odd			No	
	$\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$	even	$\det,\mathscr{P}^1(\det),\sqrt{\widetilde{f}_4}$	Polynomial	Yes	- Theorem 7.1
		odd	$\det,\mathscr{P}^1(\det),\widetilde{f}_4$	Hypersurface	No	
$\mathrm{SL}_2(K)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	even	Same as $GL_2(K)$			
		odd	trace, det, $\mathscr{P}^1(\det)$ , $\sqrt{-f_4}$	Hypersurface	Yes	Theorem 8.1
	$\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$	even	Same as $GL_2(K)$			
		odd	$\det,\mathscr{P}^1(\det),\sqrt{-\widetilde{f}_4}$	Hypersurface	Yes	Theorem 8.3
$\mathrm{O}_2(K)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	even	trace, det, $b-c$ , $N(a)$	Hypersurface	Yes	Theorem 9.3
		odd	trace, det, $(b-c)^2$ , $N(a)$		No	
	$\begin{bmatrix} 0 & b \\ -b & 0 \end{bmatrix}$	even	b	Polynomial	Yes	Remark 10.1
		odd	$b^2$			
	$\begin{bmatrix} a & b \\ b & d \end{bmatrix}$	even	trace, det, $\sum_{k} b^{2^{k}} (a+d)^{q/2-2^{k}}$	Polynomial	Yes	Theorem 10.2
		odd	trace, det, $N(a)$			

TABLE 1. An overview of the descriptions of the invariant rings.

Table 1 summarises the description of the invariant ring in each case. In particular, we note that the invariant ring is never worse than a hypersurface. For all the rows saying 'hypersurface', the result is sharp: we know that the invariant ring is not a polynomial ring; in fact, its *a*-invariant is the same as that of the ambient polynomial ring. The failure of being a polynomial ring can also be explained by the lack of pseudoreflections in those actions. In each case, the set of primary invariants described is optimal. Moreover, the additional algebra generator (when required) can be chosen as the Jacobian of our choice of primary invariants, at least in odd characteristic. Our choice of primary invariants for the  $GL_2$  and  $SL_2$  actions is rather uniform as Table 1 shows; only the fourth invariant needs to be suitably modified in each case. For the  $O_2$  action, we have invariants of smaller degree, owing to the smaller order of the group. The ring of invariants is a unique factorisation domain whenever the characteristic is two; the class group turns out to be either  $\mathbb{Z}/2$  or  $(\mathbb{Z}/2)^2$  whenever the ring is not a unique factorisation domain, the latter appearing only for the generic action of  $O_2$ .

The terms "primary" and "secondary" above have their usual meanings as in the invariant theory of finite groups, that we elaborate on now. A good reference for this is [DK, §3]. If G is a finite group acting on a polynomial ring  $S = K[x_1, ..., x_n]$  by degree-preserving K-algebra automorphisms, then primary invariants are homogeneous invariants  $f_1, ..., f_n \in S^G$  satisfying any of the following equivalent properties:

- (a) The radical of  $(f_1, ..., f_n)S$  is the homogeneous maximal ideal of S, i.e., the  $f_i$  form a homogeneous system of parameters for S.
- (b) The set of common zeroes of  $\{f_1, \dots, f_n\}$  in  $\overline{K}^n$  is the origin, where  $\overline{K}$  is the algebraic closure of K.

(c) The subalgebra  $R := K[f_1, \dots, f_n]$  is a polynomial ring and  $S^G$  is a finite R-module. In this case, we refer to R as a Noether normalisation for  $S^G$ .

Once we have a set of primary invariants with corresponding Noether normalisation R, the next objective is to determine R-module generators for  $S^G$ . Finiteness tells us that we may (minimally) write

$$(1.1) S^G = Rh_1 + \dots + Rh_s$$

for some  $h_j \in S^G$ , called the secondary invariants. The above sum is direct precisely when the ring  $S^G$  is Cohen–Macaulay. In any case, we then obtain the equality of K-algebras

$$S^G = K[f_1, \dots, f_n, h_1, \dots, h_s].$$

We may always assume  $h_1 = 1$  and exclude it from the above algebra generating set. We remark that primary and secondary invariants are not uniquely determined; moreover, the minimal number of secondary invariants depends on the choice of primary invariants. A lower bound is given in [DK, Theorem 3.7.1]; the equality holds precisely when  $S^G$  is Cohen–Macaulay. We will see (Remark 4.9) that the choices of the primary and secondary invariants in Table 1 are optimal.

The outline of the proof of the main result—and of Part I—is as follows: We first introduce the relevant notation and definitions. In particular, we introduce a 'larger' group  $\Gamma$  acting on S such that  $S^{\Gamma} \subseteq S^{G}$ . We collect some facts about the conjugation action in Section 2 that only rely on basic linear algebra. In Section 3, we define the invariants  $f_1, f_2, f_3, f_4$  and show that these form a set of primary invariants; we denote the corresponding Noether normalisation as R. We then deduce homological properties of  $S^{G}$  and  $S^{\Gamma}$  in Section 4. In particular, we show that  $S^{G}$  is a hypersurface of the form  $R \oplus R\eta$ , and that  $S^{\Gamma}$  is the polynomial ring R. We make use of the a-invariant to obtain the degree of  $\eta$  to be  $q^2$ . Consequently, we obtain the Hilbert series of  $S^{G}$  and conclude that any element of  $S^{G} \setminus R$  of the correct degree can serve as  $\eta$ . In Section 5, we construct an invariant h of the correct degree, by defining it to be the Jacobian of the primary invariants. We make use of the  $\Gamma$ -action to show that  $h^2 \in R$ , and that  $h \notin R$  when  $\operatorname{char}(K)$  is odd; this finishes the problem of describing the generators and relations. The additional results about F-regularity and factoriality are proven in Section 6. To construct one of the primary invariants, we make use of the Steenrod operations; the relevant notation and results are reviewed in Appendix A. Part II concerns the action of  $GL_2$  on the space  $\mathfrak{sl}_2$  of traceless matrices, as well as the actions of  $SL_2$  on each of  $\mathfrak{gl}_2$  and  $\mathfrak{sl}_2$ . In Part III, we consider the actions of  $O_2$  on the space  $\mathfrak{ol}_2$  of alternating matrices, the space of symmetric matrices, and  $\mathfrak{gl}_2$ . The proof in each case follows the same template as for Theorem 1.1.

**Acknowledgements.** The author thanks Anurag K. Singh for several interesting discussions. Parts II and III arose out of the natural questions suggested by Karthik Ganapathy, Suhas Gondi, Vaibhav Pandey, Steven Sam, and Ramanujan Srihari; the author thanks them for the same. This work has greatly benefited from examples computed using the computer algebra system Magma [BCP], the use of which is gratefully acknowledged.

## **Part** I. The action of $GL_2$ on $\mathfrak{gl}_2$

Let q be a power of a positive prime p. We set  $K := \mathbb{F}_q$ , the field with q elements, and let  $\overline{K}$  denote its algebraic closure. Let  $G := \operatorname{GL}_2(K)$  be the general linear group, and S := K[a,b,c,d] the polynomial ring over K in four variables. We consider the conjugation action of G on S given by

(1.2) 
$$\sigma \colon \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \sigma^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \sigma,$$

i.e.,  $\sigma \in G$  maps each variable to the corresponding entry of  $\sigma^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \sigma$ .

We note that the above action comes from the conjugation action of G on  $V := M_2(K)$ , the space of  $2 \times 2$  matrices, as follows: the action of G on V is given by  $(\sigma,M) \longmapsto \sigma M \sigma^{-1}$ . Said otherwise, this is the adjoint representation of G on  $V = \mathfrak{gl}_2$ , which, in turn, gives us a left action of G on  $\mathrm{Sym}(V^*) \cong S$ . The isomorphism is constructed as follows: let  $E_{ij} \in V$  denote the matrix whose sole nonzero entry is a 1 in the (i,j) position. Then,  $B := \{E_{11}, E_{12}, E_{21}, E_{22}\}$  is a basis for V. If we let  $\{a,b,c,d\} \subseteq V^*$  denote its dual basis, then  $\mathrm{Sym}(V^*)$ 

is the polynomial ring S = K[a,b,c,d], and the action is precisely (1.2) under this identification. We shall use both perspectives in describing the ring of invariants  $S^G$ .

We denote the corresponding representation as

$$\rho: G \longrightarrow GL(V),$$

and set  $\widehat{G} := \rho(G) \leqslant \operatorname{GL}(V)$ . The group  $\widehat{G}$  acts faithfully on both V and S via the action of G. While we have the equality  $S^G = S^{\widehat{G}}$ , the distinction between G and  $\widehat{G}$  is necessary when we use results that require that the group action be faithful. Note that the action of G is not faithful, i.e.,  $\rho$  is not injective: the kernel consists precisely of the invertible scalar matrices and thus,  $\widehat{G} \cong \operatorname{PGL}_2(K)$ . In particular, the orders of the groups are

$$|G| = (q^2 - 1)(q^2 - q)$$
 and  $|\widehat{G}| = q(q^2 - 1)$ .

Thus, the action of G is *modular*, i.e.,  $|\rho(G)|$  is divisible by the characteristic of K.

We define the larger group  $\Gamma \coloneqq \langle \widehat{G}, \tau_{ad} \rangle \leqslant \operatorname{GL}(V)$ , where  $\tau_{ad} \in \operatorname{GL}(V)$  is the automorphism fixing  $E_{12}$  and  $E_{21}$ , and swapping  $E_{11} \leftrightarrow E_{22}$ . Equivalently, the action of  $\tau_{ad}$  on S is given by fixing b and c, and swapping  $a \leftrightarrow d$ .

As the field K is finite, there are monic irreducible polynomials in K[x] of any given positive degree. We fix an irreducible quadratic polynomial  $g(x) = x^2 - \tau x + \delta \in K[x]$  for the rest of Part I.

The ring S will have its standard  $\mathbb{N}$ -grading throughout the paper, i.e., all the variables have degree 1. The subrings that we construct will be graded subrings that are finitely generated algebras over K. For such a graded ring  $R = \bigoplus_{n \ge 0} R_n$ , its *Hilbert series* is the power series

$$\operatorname{Hilb}(R,z) := \sum_{n \ge 0} \operatorname{rank}_K(R_n) z^n \in \mathbb{Q}[\![z]\!].$$

We suppress the variable when no explicit mention is necessary. The Hilbert–Serre theorem asserts that the above power series is a rational function, see [AM, Theorem 11.1]. Writing Hilb(R) = f/g for polynomials f and g, we define the degree of Hilb(R) to be the difference deg Hilb(R) := deg(f) - deg(g).

## 2. Preliminaries about the conjugation action

We collect some basic facts pertaining to the linear algebra of the conjugation action. In particular, we show that the representation  $\rho$  factors through SL(V) and contains no pseudoreflections. Note that the (non-canonical) isomorphism  $(-)^*: V \longrightarrow V^*$  of K-vector spaces obtained by our choice of bases is given as

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \longmapsto Aa + Bb + Cc + Dd.$$

While this isomorphism is not G-equivariant, the following lemma describes how it interacts with G.

**Lemma 2.1.** For  $v \in V$  and  $\sigma \in G$ , we have  $(\sigma \cdot v)^* = (\sigma^{-1})^{tr} \cdot v^*$ .

*Proof.* For this proof, we use  $\rho$  and  $\rho^*$  to denote the respective homomorphisms  $G \longrightarrow \operatorname{GL}_4(K)$  obtained by the identifications  $V \cong K^4$  and  $V^* \cong K^4$  using our choice of standard bases. By [CW, Lemma 1.1.1], we have  $\rho^*(\sigma) = \rho(\sigma^{-1})^{\operatorname{tr}}$ . Thus, it suffices to show  $\rho(\sigma)^{\operatorname{tr}} = \rho(\sigma^{\operatorname{tr}})$ . To this end, note that the standard inner product on  $K^4$  translates to one on V as  $\langle M, N \rangle = \operatorname{trace}(MN^{\operatorname{tr}})$  for  $M, N \in V$ . Then, for  $\sigma \in G$ , we have

$$\langle \sigma \cdot M, N \rangle = \operatorname{trace}(\sigma M \sigma^{-1} N^{\operatorname{tr}}) = \operatorname{trace}(M \sigma^{-1} N^{\operatorname{tr}} \sigma) = \langle M, \sigma^{\operatorname{tr}} \cdot N \rangle.$$

Thus,  $\langle \rho(\sigma)M, N \rangle = \langle M, \rho(\sigma^{tr})N \rangle$ , giving us the desired assertion that  $\rho(\sigma)^{tr} = \rho(\sigma^{tr})$ .

**Lemma 2.2.** Let  $\Omega \subseteq V$  be the set of matrices whose characteristic polynomial is equal to g(x). Then, we have

$$\Omega = \left\{ egin{bmatrix} A & B \ -rac{g(A)}{B} & au - A \end{bmatrix} : A \in K, B \in K^ imes 
ight\}.$$

Moreover, any two elements of  $\Omega$  are similar, and thus,  $\Omega$  is a single orbit for the conjugation action of G on V.

*Proof.* Finite fields are perfect, and hence g(x) has distinct factors  $\mu, \nu \in \overline{K}$ . In turn, any  $M \in \Omega$  is similar to diag $(\mu, \nu)$  over  $\overline{K}$ . In particular, any two elements of  $\Omega$  are similar over  $\overline{K}$  which implies the same over K.

We now determine  $\Omega$ . Consider an arbitrary matrix

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in M_2(K).$$

For its characteristic polynomial to be  $g(x) = x^2 - \tau x + \delta$ , we must have  $\operatorname{trace}(M) = \tau$  and  $\det(M) = \delta$ . The first condition gives us  $D = \tau - A$  and in turn

$$A(\tau - A) - BC = \delta.$$

Rearranging the above give us

$$-BC = g(A)$$
.

Because g is irreducible, we have that  $g(A) \neq 0$  for all  $A \in K$  and thus, B is nonzero. We may then solve for C to obtain the desired result.

**Corollary 2.3.** The set of homogeneous linear polynomials in K[a,b,c,d] defined by

$$\Omega \coloneqq \left\{Aa + Bb - rac{g(A)}{B}c + ( au - A)d : A \in K, B \in K^ imes
ight\}$$

forms a single G-orbit of size  $q^2 - q$ . Moreover  $\Omega$  is stable under the action of  $\Gamma$ .

*Proof.* Only the last statement needs a proof. To this end, note that if  $A \in K$  and  $B \in K^{\times}$ , then

$$\tau_{ad}\left(Aa+Bb-\frac{g(A)}{B}c+(\tau-A)d\right)=(\tau-A)a+Bb-\frac{g(A)}{B}c+Ad.$$

Because  $g(A) = g(\tau - A)$ , we see that the above is indeed an element of  $\Omega$ .

**Lemma 2.4.** We have the inclusion  $\widehat{G} \subseteq SL(V)$  as subgroups of GL(V).

*Proof.* We wish to show that  $\rho(G) \subseteq \operatorname{SL}(V)$ . The representation  $\rho$  is given by  $\rho(\sigma)(M) = \sigma M \sigma^{-1}$  for  $\sigma \in G$  and  $M \in V$ . Said otherwise,  $\rho(\sigma) = L(\sigma) \circ R(\sigma)^{-1}$ , where  $L(\sigma)$  and  $R(\sigma)$  denote left and right multiplication by  $\sigma$ , respectively. Thus,  $\det(\rho(\sigma)) = \det(L(\sigma))/\det(R(\sigma))$  and it suffices to show that  $\det(L(\sigma)) = \det(R(\sigma))$ . This is now a simple linear algebra exercise, see for example, [HK, §5.4 Exercise 12].

**Lemma 2.5.** The action of G contains no pseudoreflections, i.e.,  $\operatorname{rank}(\rho(\sigma) - \operatorname{id}) \neq 1$  for all  $\sigma \in G$ .

*Proof.* In view of the rank-nullity theorem, we wish to show that if  $\sigma \in G$ , then  $\ker(\rho(\sigma) - \mathrm{id})$  has dimension different from 3. The kernel consists precisely of those  $M \in \mathrm{M}_2(K)$  that commute with  $\sigma$ . Because this dimension does not change upon enlarging the base field, we may assume that  $\sigma$  is in Jordan form. Considering the possibilities for a  $2 \times 2$  Jordan form, one sees that the requisite dimension is either 2 or 4.

We now analyse the action of G on V via its Sylow-p subgroups. To this end, consider the unipotent group

(2.1) 
$$P := \begin{bmatrix} 1 & K \\ 0 & 1 \end{bmatrix} = \left\{ \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix} : \alpha \in K \right\}.$$

**Lemma 2.6.** We have  $\dim(V^P) = 2$ , equivalently,  $\operatorname{codim}(V^P) = 2$ .

*Proof.* It is a straightforward computation that if  $\alpha \in K^{\times}$ , then the matrices commuting with  $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$  are precisely those of the form  $\begin{pmatrix} A & B \\ 0 & A \end{pmatrix}$  with  $A, B \in K$ . In turn,  $V^P$  is the two-dimensional space  $\left\{\begin{pmatrix} A & B \\ 0 & A \end{pmatrix}: A, B \in K\right\}$ . The statement about the codimension follows after noting that  $\dim(V) = 4$ .

**Lemma 2.7.** If  $K \neq \mathbb{F}_2$ , then  $\widehat{G}/[\widehat{G},\widehat{G}] \cong K^{\times}/(K^{\times})^2$ .

*Proof.* The commutator subgroup  $[GL_n(K), GL_n(K)]$  is equal to  $SL_n(K)$  except when n = 2 and  $K = \mathbb{F}_2$ ; see [Th] or [Ja, §6.7]. In turn, we get  $[PGL_n(K), PGL_n(K)] = PSL_n(K)$ . The result now follows from the fact that  $\widehat{G} \cong PGL_2(K)$  and the exact sequence of groups

$$1 \longrightarrow \mathrm{PSL}_n(K) \hookrightarrow \mathrm{PGL}_n(K) \xrightarrow{\det} K^{\times}/(K^{\times})^n \longrightarrow 0.$$

## 3. THE PRIMARY INVARIANTS

We now describe a set of primary invariants for the conjugation action. Two natural candidates to start with are the trace and determinant. As we are working over finite fields, we may use the *Steenrod operations*  $\mathcal{P}$  (see Appendix A) to produce a third new invariant from these. The fourth invariant is a certain orbit product.

**Definition 3.1.** The elements  $f_1, f_2, f_3, f_4 \in S$  are defined as

(3.1) 
$$f_{1} := a + d,$$

$$f_{2} := ad - bc,$$

$$f_{3} := a^{q}d + ad^{q} - b^{q}c - bc^{q},$$

$$f_{4} := \prod_{\substack{A \in K \\ B \in K^{\times}}} \left( Aa + Bb - \frac{g(A)}{B}c + (\tau - A)d \right).$$

The elements above are readily seen to be homogeneous of degrees 1, 2, q + 1, and  $q^2 - q$ , respectively. We set  $R := K[f_1, f_2, f_3, f_4] \subseteq S$ . We will show that R is a Noether normalisation for  $S^G$  and that we have a decomposition of the form  $S^G = R \oplus Rh$ . In particular,  $S^G$  is a hypersurface. Along the way, we will also show that  $R = S^\Gamma$ , i.e., R is itself a ring of invariants. This equality shows that while  $f_4$  depends on the choice of the irreducible quadratic g(x), the Noether normalisation R does not.

**Proposition 3.2.** We have  $R \subseteq S^{\Gamma} \subseteq S^{G}$ .

*Proof.* The elements  $f_1$  and  $f_2$  are the trace and determinant of  $\binom{a \ b}{c \ d}$  and are hence invariant under conjugation. These are also symmetric in a and d and hence Γ-invariant. The element  $f_3$  is  $\mathscr{P}^1(f_2)$  and hence is Γ-invariant in view of Lemma A.1. The invariance of  $f_4$  follows from Corollary 2.3.

We do our only gritty calculation below to show that the  $f_i$  form a homogeneous system of parameters for S; in particular, R is a Noether normalisation for each of  $S^G$  and  $S^{\Gamma}$ .

**Theorem 3.3.** The invariants  $f_1, f_2, f_3, f_4$  form a homogeneous system of parameters for S.

*Proof.* It suffices to show that the only solution in  $\overline{K}^4$  to  $f_1 = f_2 = f_3 = f_4 = 0$  is the origin. Let  $(a,b,c,d) \in \overline{K}^4$  be such a common solution. We immediately discard the equation  $f_1 = 0$  by substituting d = -a in the other equations. The equation  $f_4 = 0$  tells us that there exist  $A \in K$ ,  $B \in K^{\times}$  such that

(3.2) 
$$b = \frac{\tau - 2A}{B}a + \frac{g(A)}{B^2}c.$$

After the substitution d = -a, the equation  $f_2 = 0$  gives us  $a^2 + bc = 0$ . Using (3.2), we obtain

$$a^{2} + \frac{\tau - 2A}{R}ac + \frac{g(A)}{R^{2}}c^{2} = 0.$$

Writing  $g(A) = A^2 - \tau A + \delta$ , the above can be rearranged to get

$$\left(\frac{A}{B}c - a\right)^2 - \tau \left(\frac{A}{B}c - a\right) \left(\frac{c}{B}\right) + \delta \left(\frac{c}{B}\right)^2 = 0.$$

We may factor g(x) over  $\overline{K}$  to get  $g(x) = (x + \mu)(x + \nu)$  for some  $\mu, \nu \in \overline{K} \setminus K$ . In turn, the above factors as

$$\left(\frac{A}{B}c - a + \mu \frac{c}{B}\right) \left(\frac{A}{B}c - a + v \frac{c}{B}\right) = 0.$$

Without loss of generality, we may assume that the first factor is zero, giving us

$$a = \frac{A + \mu}{B}c.$$

Substituting this in (3.2) and using  $\mu + \nu = -\tau$  gives us

$$b = \frac{\tau - 2A}{B} \cdot \frac{A + \mu}{B} c + \frac{g(A)}{B^2} c$$

$$= \frac{-\mu - \nu - 2A}{B} \cdot \frac{A + \mu}{B} c + \frac{(A + \mu)(A + \nu)}{B^2} c$$

$$= -\left(\frac{A + \mu}{B}\right)^2 c.$$

Letting  $\gamma := (A + \mu)/B$ , we see that

(3.3) 
$$a = \gamma c$$
 and  $b = -\gamma^2 c$ .

Note that  $\mu \notin K$ , and hence  $\gamma \notin K$  as well.

We now substitute the above in  $f_3 = 0$ . We get

$$(-2\gamma^{q+1} + \gamma^{2q} + \gamma^2)c^{q+1} = 0.$$

The above factors as

$$(\gamma^q - \gamma)^2 \cdot c^{q+1} = 0.$$

The first term is nonzero because  $\gamma \notin K$ , and hence  $\gamma$  cannot be a root of the polynomial  $x^q - x$ . Thus, we get c = 0 and in view of (3.3), we are done.

# 4. HOMOLOGICAL PROPERTIES

In this section, we show that  $S^{\Gamma}$  is equal to the Noether normalisation R defined earlier, and that  $S^{G}$  is a hypersurface that decomposes as  $R \oplus R\eta$ . We begin by showing that  $S^{G}$  is a Cohen–Macaulay ring.

**Proposition 4.1.** The ring  $S^G$  is Cohen–Macaulay.

*Proof.* Recall the unipotent subgroup  $P := \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}$ . By Lemma 2.6, we have  $\operatorname{codim}(V^P) = \dim(V) - \dim(V^P) = 2$  and in turn,  $S^P$  is Cohen–Macaulay by [CW, Theorem 3.9.2]. Note that  $[G:P] = (q^2 - 1)(q - 1)$  is invertible in K and thus, the inclusion  $S^G \longrightarrow S^P$  splits. Indeed, the *relative transfer* map

$$S^P \longrightarrow S^G$$

$$s \longmapsto \frac{1}{[G:P]} \sum_{\sigma P \in G/P} \sigma(s)$$

defines an  $S^G$ -linear splitting. Because this is a finite extension, we get that  $S^G$  is Cohen–Macaulay.

**Porism 4.2.** Let  $H \leq GL_2(K)$  be any subgroup acting via conjugation on S. Then,  $S^H$  is Cohen–Macaulay.

*Proof.* Let Q be a Sylow-p subgroup of H. It suffices to show that  $S^Q$  is Cohen–Macaulay. Upon conjugation, we may assume that  $Q \leq P$ . But then,  $\operatorname{codim}(V^Q) \leq \operatorname{codim}(V^P) = 2$  and thus,  $S^Q$  is Cohen–Macaulay.

**Proposition 4.3.** The ring  $S^G$  is a hypersurface. Specifically, if R is the Noether normalisation defined as before, then there exists an invariant  $\eta \in S^G$  such that  $S^G = R \oplus R\eta$  as R-modules, and hence  $S^G = K[f_1, f_2, f_3, f_4, \eta]$  as K-algebras. In particular,

(4.1) 
$$\operatorname{Hilb}(S^{G}, z) = \frac{1 + z^{\deg \eta}}{(1 - z)(1 - z^{2})(1 - z^{q+1})(1 - z^{q^{2} - q})}.$$

*Proof.* Because  $S^G$  is Cohen–Macaulay, we may use [DK, Theorem 3.7.1] to determine the number of minimal secondary invariants (with respect to the  $f_i$ ) as

$$\frac{\prod_{i=1}^{4} \deg(f_i)}{|\widehat{G}|} = \frac{1 \cdot 2 \cdot (q+1) \cdot (q^2 - q)}{q(q^2 - 1)} = 2,$$

where  $\widehat{G}$  is the image of  $\rho$  defined in (1.3). As  $1 \in S^G$  is always a minimal secondary invariant, the other secondary invariant is the  $\eta$  as in the statement. The Hilbert series follows by our knowledge of the degrees of the  $f_i$  and the fact that R is a polynomial algebra on the  $f_i$ .

**Corollary 4.4.** We have the equality  $R = S^{\Gamma}$ . In particular,  $S^{\Gamma}$  is a polynomial ring, and R is independent of the choice of the irreducible quadratic g(x).

*Proof.* We have the integral extensions of normal domains  $R \subseteq S^{\Gamma} \subsetneq S^{G}$ ; to see that the latter inclusion is strict, note that  $\Gamma \neq \widehat{G}$  because  $\widehat{G}$  contains no pseudoreflections (Lemma 2.5) whereas  $\Gamma$  contains the pseudoreflection  $\tau_{ad}$ . By Proposition 4.3, the degree of the extension  $R \subseteq S^{G}$  is two, forcing  $R = S^{\Gamma}$ .

We now calculate the a-invariant of  $S^G$  and use it to determine the ring of invariants. For an introduction to the a-invariant, we refer the reader to [GW; BH]. For a graded Cohen–Macaulay ring, the a-invariant is simply the degree of the Hilbert series.

**Proposition 4.5.** *We have*  $a(S^{G}) = a(S) = -4$ .

*Proof.* By Lemmas 2.4 and 2.5, we know that  $\widehat{G}$  is a subgroup of SL(V) that contains no pseudoreflections. This result now follows from [GJS, Theorem 4.4].

**Porism 4.6.** Let  $H \leq \operatorname{GL}_2(K)$  be any subgroup acting via conjugation on S. Then,  $a(S^H) = a(S) = -4$ .

**Corollary 4.7.** The Hilbert series of  $S^G$  is given as

(4.2) 
$$\operatorname{Hilb}(S^{G}, z) = \frac{1 + z^{q^{2}}}{(1 - z)(1 - z^{2})(1 - z^{q+1})(1 - z^{q^{2} - q})}.$$

*Proof.* By Proposition 4.1,  $S^G$  is Cohen–Macaulay and thus, the equality  $a(S^G) = \deg \operatorname{Hilb}(S^G)$  holds. Using this, we may solve for  $\deg \eta$  in (4.1) and get the desired equality.

**Corollary 4.8.** There exists an invariant  $\eta \in S^G \setminus R$  of degree  $q^2$ . For any such  $\eta$ , we have the R-module decomposition  $S^G = R \oplus R\eta$ . In turn, we have  $S^G = K[f_1, f_2, f_3, f_4, \eta]$ .

*Proof.* The existence of such an  $\eta$  follows from the knowledge of the Hilbert series. Indeed, we have

$$Hilb(S^G, z) - Hilb(R, z) = \frac{z^{q^2}}{(1 - z)(1 - z^2)(1 - z^{q+1})(1 - z^{q^2 - q})}.$$

The coefficient of  $z^{q^2}$  in the above is 1, proving the first statement. For the second statement, we note that  $\eta$  is then of minimal degree.

Remark 4.9. We remark that our choices of invariants have been optimal in the following ways:

- (a) Because the ring  $S^G$  is a four-dimensional ring that is not a polynomial ring, we need at least 5 algebra generators for  $S^G$ , which is what we have obtained.
- (b) The primary invariants are optimal if we are trying to minimise the product of their degrees. Indeed, by [DK, Proposition 3.3.5, Theorem 3.7.1], the product of degrees is a multiple of  $|\widehat{G}|$ , with the product being equal to  $|\widehat{G}|$  only if  $S^G$  is a polynomial ring. Thus, in our situation, the smallest product that one can obtain is  $2|\widehat{G}|$ , which is what we do. Similarly, we see that the number of secondary invariants (with respect to any set of primary invariants) must be at least 2, and we obtain this minimum.

## 5. THE MISSING INVARIANT

We now show that the secondary invariant  $\eta$  may be chosen as the Jacobian of the  $f_i$ , when the characteristic is odd. To this end, we define

$$h := \operatorname{Jac}(f_1, f_2, f_3, f_4)$$

$$= \det \begin{bmatrix} 1 & 0 & 0 & 1 \\ d & -c & -b & a \\ d^q & -c^q & -b^q & a^q \\ \frac{\partial f_4}{\partial a} & \frac{\partial f_4}{\partial b} & \frac{\partial f_4}{\partial c} & \frac{\partial f_4}{\partial d} \end{bmatrix}.$$

The element h is readily seen to be homogeneous of degree  $q^2$  with the caveat that h may be zero. We first prove that this is not the case. For ease of notation, let J denote the matrix in the above equation.

## **Lemma 5.1.** *The element h is nonzero.*

*Proof.* Consider the lexicographic monomial ordering on S with a > b > c > d, and let LM(f) denote the leading monomial of a polynomial  $f \in S$ . Examining the product in (3.1) gives us  $LM(f_4) = a^{(q-1)^2}b^{q-1}$ . This monomial does not vanish after applying  $\partial/\partial b$  and thus, we get

$$\operatorname{LM}(J) = \begin{bmatrix} \boxed{1} & 0 & 0 & 1 \\ d & c & \boxed{b} & a \\ d^q & c^q & b^q & \boxed{a^q} \\ \operatorname{LM}\left(\frac{\partial f_4}{\partial a}\right) & \boxed{a^{(q-1)^2}b^{q-2}} & \operatorname{LM}\left(\frac{\partial f_4}{\partial c}\right) & \operatorname{LM}\left(\frac{\partial f_4}{\partial d}\right) \end{bmatrix}.$$

One then verifies that the product of the boxed monomials above is a monomial that does not appear in any of the other summands when computing the determinant. In particular, we get that h is nonzero.

**Proposition 5.2.** We have  $h \in S^G$ , and  $h^2 \in R$ . If the characteristic of K is odd, then  $h \notin R$ .

*Proof.* Because h is the Jacobian of G-invariant elements and the action of G factors through SL(V) (by Lemma 2.4), the chain rule yields  $h \in S^G$ , see [Sm1, Proposition 1.5.6].

For the remaining statements, note that by Corollary 4.4, we have  $R = S^{\Gamma} = S^{G} \cap S^{\tau_{ad}}$ . Thus, it suffices to show that  $h^2$  is  $\tau_{ad}$ -invariant and that h is not  $\tau_{ad}$ -invariant in odd characteristic. The automorphism  $\tau_{ad}$  switches the extreme columns of J, giving us  $\tau_{ad} \cdot h = -h$  and  $\tau_{ad} \cdot h^2 = h^2$ . This finishes the proof.

**Remark 5.3.** The same proof above shows that if char(K) = 2, then h is indeed an element of R. Therefore, we need to pick a different element of degree  $q^2$  to generate the invariant ring, the existence of such an element being ensured by Corollary 4.8.

Thus, for odd characteristic, h fulfils the hypothesis of  $\eta$  as in Corollary 4.8, giving us the corresponding statements of Theorem 1.1.

#### 6. ADDITIONAL PROPERTIES OF THE INVARIANT RING

We now prove the additional ring-theoretic properties of the invariant ring mentioned in Theorem 1.1.

A natural question to ask is whether the inclusion  $S^G \hookrightarrow S$  splits  $S^G$ -linearly. Because this is a finite extension and S is a polynomial ring, this question is equivalent to asking whether  $S^G$  is F-regular; indeed, a direct summand of a polynomial ring is F-regular and conversely, an F-regular ring splits off from any finite extension, see [HH, Theorem 5.25].

**Proposition 6.1.** The inclusion  $S^G \hookrightarrow S$  does not split  $S^G$ -linearly. Equivalently, the ring  $S^G$  is not F-regular.

*Proof.* By Proposition 4.5, the *a*-invariants of S and  $S^G$  are the same. Because the action of G is modular, we get the result by [Je, Theorem 2.18] or [GJS, Corollary 4.2].

Alternatively, by Lemma 2.5, the action of G is modular and contains no pseudoreflections. The result then follows from [Br, 2.2 Corollary 2].

A second natural question to ask is whether the normal domain  $S^G$  is a UFD.

**Proposition 6.2.** The ring  $S^G$  is a unique factorisation domain if and only if char(K) = 2. If char(K) is odd, then the class group of  $S^G$  is isomorphic to  $\mathbb{Z}/2$ .

*Proof.* As noted in Lemma 2.5, the action of G contains no pseudoreflections. Thus, by [Be, Theorem 3.9.2], the class group  $Cl(S^G)$  is isomorphic to  $Hom(\widehat{G}, K^{\times})$ . Note that  $S^G$  is a UFD precisely when  $Cl(S^G)$  is trivial. Because  $K^{\times}$  is abelian, we obtain

$$\mathrm{Cl}(S^G) \cong \mathrm{Hom}(\widehat{G},K^\times) \cong \mathrm{Hom}(\widehat{G}/[\widehat{G},\widehat{G}],K^\times).$$

Thus, the result is clear when  $K = \mathbb{F}_2$  for then  $K^{\times}$  is trivial. We now assume that K has at least three elements. Then, by Lemma 2.7, we have

$$\frac{\widehat{G}}{|\widehat{G},\widehat{G}|} \cong \frac{K^{\times}}{(K^{\times})^2} \cong \frac{\mathbb{Z}/(q-1)}{2\mathbb{Z}/(q-1)} \cong \mathbb{Z}/(2,q-1).$$

Observing that  $\operatorname{Hom}\left(\frac{\mathbb{Z}}{(2,q-1)},\frac{\mathbb{Z}}{(q-1)}\right)\cong\frac{\mathbb{Z}}{\gcd(2,q-1)}$  gives us the desired result.

**Remark 6.3.** We note that the results on the *a*-invariant and the class group readily generalise to the conjugation action of  $GL_n(K)$  on  $K[X_{n\times n}]$  for any n>2 and finite field K. If we continue to use G and S respectively to denote the group and the polynomial ring, we then obtain:

- (a)  $a(S^G) = a(S) = -n^2$  and the inclusion  $S^G \longrightarrow S$  does not split, and
- (b)  $S^G$  is a unique factorisation domain precisely when n and q-1 are coprime; more generally, the class group of  $S^G$  is  $\mathbb{Z}/\gcd(n,q-1)$ .

The same proofs as in Propositions 4.5 and 6.1 are easily adapted for (a); the proofs of Lemmas 2.4 and 2.5 work with slight modifications to show that the action of G contains no pseudoreflections and factors through SL. For (b), the same proof as Proposition 6.2 works mutatis mutandis noting that we have  $\hat{G} \cong PGL_n(K)$ .

**Remark 6.4.** Continuing our notation from the previous remark, we now observe that the homological properties of  $S^G$  do not generalise. If n > 2 and  $P \le G$  is the unipotent subgroup, then  $S^G$  is not a complete intersection and  $S^P$  is not Cohen–Macaulay. These facts follow from [KW, Theorem A] and [Ke, Corollary 3.7], respectively, after noting that the action of G contains no *bireflections* for n > 2; a non-identity element  $\sigma \in GL(V)$  is said to be a bireflection if  $rank(\sigma - id_V) \le 2$ .

# Part II. The special linear group and traceless matrices

We now describe how we can obtain other invariant rings from the above. Recall that the Lie algebra of  $SL_2(K)$  is the space of *traceless* matrices

$$\mathfrak{sl}_2 := \{ M \in \mathcal{M}_2(K) : \operatorname{trace}(M) = 0 \},$$

and is stable under the conjugation action. Thus, we may ask for the polynomial invariants of this conjugation action. We set  $T := \operatorname{Sym}(\mathfrak{sl}_2^*)$ , and identify T with a polynomial algebra after choosing the basis  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  for  $\mathfrak{sl}_2$  and letting  $\{a,b,c\}$  be the dual basis. We then have T = K[a,b,c], and suggestively arranging these variables in a  $2 \times 2$  matrix as  $Y := \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ , we get that the element  $\sigma \in G$  then acts on T by

$$\sigma: Y \longmapsto \sigma^{-1}Y\sigma$$
.

Similarly, we may also ask for the polynomial invariants for the conjugation actions of  $SL_2(K)$  on  $\mathfrak{gl}_2$  and  $\mathfrak{sl}_2$ . We answer all three questions below. As it turns out, the structures of the invariant rings are very similar, and they all essentially follow from the description and techniques of Part I.

We continue the use of the notation K, G, V, S as in Part I. Because the inclusion  $\mathfrak{sl}_2 \longrightarrow V$  is G-equivariant, so is the corresponding K-algebra homomorphism

$$\pi \colon S \longrightarrow T$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \begin{bmatrix} a & b \\ c & -a \end{bmatrix},$$

that is,  $\pi(\sigma \cdot f) = \sigma \cdot \pi(f)$  for all  $f \in S$  and  $\sigma \in G$ . In particular,  $\pi(S^G) \subseteq T^G$ . We will show that all invariants arise this way if the characteristic is odd; this will be an easy consequence of the inclusion  $\mathfrak{sl}_2 \hookrightarrow V$  splitting G-equivariantly. In particular, the invariant ring is then a hypersurface. If the characteristic is two, then there are more invariants and the invariant ring is even a polynomial ring. The reason for the homological change in characteristic two can be attributed to the action of  $GL_2$  on  $\mathfrak{sl}_2$  contains pseudoreflections precisely in characteristic two. We continue to denote  $\pi(\det)$  by  $\det$ , i.e.,  $\det = -a^2 - bc \in T$ .

**Theorem 7.1.** Let  $K := \mathbb{F}_q$  be a finite field with q elements. Consider the conjugation action of  $G := GL_2(K)$  on  $T := Sym(\mathfrak{sl}_2^*)$ .

(i) If q is even, then  $T^G$  is a polynomial ring given as

$$T^G = K[\det, \mathscr{P}^1(\det), \sqrt{\pi(f_4)}].$$

The a-invariant of  $T^G$  is  $-(3+q+\binom{q}{2})$ .

(ii) If q is odd, then  $\pi(S^G) = T^G$ . Thus,  $T^G$  is a hypersurface given as

$$T^G = K[\det, \mathscr{P}^1(\det), \pi(f_4), \pi(h)],$$

where h is any secondary invariant as in Theorem 1.1. In particular,  $\pi(h)$  may be replaced with the Jacobian of the other three invariants above. The Hilbert series of  $T^G$  is given as

(7.1) 
$$\operatorname{Hilb}(T^{G}, z) = \frac{1 + z^{q^{2}}}{(1 - z^{2})(1 - z^{q+1})(1 - z^{q^{2} - q})}.$$

Additionally,  $T^G$  is not F-regular, has class group  $\mathbb{Z}/2$  and a-invariant -3.

Proof of (ii). Assume that q is odd. Then, the  $2 \times 2$  identity matrix  $I_2$  is not in  $\mathfrak{sl}_2$  and we thus have the decomposition of K-vector spaces  $V = \mathfrak{sl}_2 \oplus K \cdot I_2$ . Because  $K \cdot I_2$  is G-stable, the injection  $\mathfrak{sl}_2 \longrightarrow V$  is split and thus, applying the contravariant functor  $(\operatorname{Sym}((-)^*))^G$  gives us the claimed surjection  $S^G \longrightarrow T^G$ . The kernel is seen to be  $(a+d)S^G$ , giving us the Hilbert series of  $T^G$  from our knowledge of  $\operatorname{Hilb}(S^G)$  by Theorem 1.1. This also gives us the a-invariant as  $T^G$  is then a hypersurface, and hence  $a(T^G) = \deg \operatorname{Hilb}(T^G)$ . In turn, we get the failure of F-regularity as in Proposition 6.1 after noting that the action of G continues to be modular. The class group follows as in Proposition 6.2. To see the statement about the Jacobian, let h be the Jacobian of the  $f_i$  as in Section 5. It suffices to show that  $\pi(h)$  is the Jacobian of the written invariants. Because  $\pi$  is a ring homomorphism, we have

$$\pi(h) = \det egin{bmatrix} 1 & 0 & 0 & 1 \ -a & -c & -b & a \ a^q & c^q & b^q & -a^q \ \pi\left(rac{\partial f_4}{\partial a}
ight) & \pi\left(rac{\partial f_4}{\partial b}
ight) & \pi\left(rac{\partial f_4}{\partial c}
ight) & \pi\left(rac{\partial f_4}{\partial d}
ight) \end{bmatrix}.$$

Subtracting the last column from the first and expanding along the first row, we get

$$\pi(h) = \det \begin{bmatrix} 0 & 0 & 0 & 1 \\ -2a & -c & -b & a \\ 2a^q & c^q & b^q & -a^q \\ \pi\left(\frac{\partial f_4}{\partial a} - \frac{\partial f_4}{\partial d}\right) & \pi\left(\frac{\partial f_4}{\partial b}\right) & \pi\left(\frac{\partial f_4}{\partial c}\right) & \pi\left(\frac{\partial f_4}{\partial d}\right) \end{bmatrix} = -\det \begin{bmatrix} -2a & -c & -b \\ 2a^q & c^q & b^q \\ \frac{\partial \pi(f_4)}{\partial a} & \frac{\partial \pi(f_4)}{\partial b} & \frac{\partial \pi(f_4)}{\partial c} \end{bmatrix}$$
$$= \operatorname{Jac}(\det, \mathscr{P}^1(\det), \pi(f_4));$$

the second equality above suggests how  $\pi$  commutes with the partials, which can be verified on monomials.  $\square$ 

To finish the proof for characteristic two, we now prove the analogous results about the action of G on  $\mathfrak{sl}_2$  as we had for V. We let  $P \leq G$  denote the unipotent subgroup as in (2.1).

**Lemma 7.2.** Let q be even, and  $\varphi \colon G \longrightarrow GL(\mathfrak{sl}_2)$  be the conjugation representation of G. Then,

- (i) The kernel of  $\varphi$  consists precisely of the scalar matrices. In particular,  $|\varphi(G)| = q(q-1)(q+1)$ .
- (ii) The codimension  $\dim(\mathfrak{sl}_2) \dim(\mathfrak{sl}_2^P)$  is 1. Consequently,  $T^G$  is Cohen–Macaulay.

*Proof.* The first statement is a straightforward computation. For the second, note that  $\mathfrak{sl}_2^P$  is the *K*-span of  $I_2$  and  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ . As before,  $\operatorname{codim}(\mathfrak{sl}_2^P) \leqslant 2$  tells us that  $T^P$  is Cohen–Macaulay by [CW, Theorem 3.9.2]. As in the proof of Proposition 4.1, we are now done.

**Lemma 7.3.** If q is even, then  $\pi(f_4)$  is a square, i.e.,  $\pi(f_4) = f^2$  for some  $f \in T$ . Necessarily,  $f \in T^G$ .

*Proof.* Assume that char(K) = 2. Then,  $\pi(f_4)$  takes the form

$$\pi(f_4) = \prod_{\substack{A \in K \ B \in K^{ imes}}} \left( au a + Bb + rac{g(A)}{B} c 
ight).$$

Note that because  $\operatorname{char}(K) = 2$ , we must necessarily have  $\tau \neq 0$  because every element of K is a perfect square. Thus, the map  $A \longmapsto \tau - A$  is an involution of K with no fixed points. Because  $g(A) = g(\tau - A)$ , we see that in the product above, each linear factor has multiplicity exactly two, giving us that  $\pi(f_A)$  is a perfect square.

For the last statement, note that  $\pi(f_4)$  is an invariant and square roots are unique in characteristic two.

**Lemma 7.4.** When q is even, the invariants det,  $\mathscr{P}^1(\det)$ ,  $\sqrt{\pi(f_4)}$  form a system of parameters for T.

*Proof.* This follows from Theorem 3.3 after noting that T is obtained from S by killing the first term of a system of parameters.

The lemmas above assemble as before to finish the proof of Theorem 7.1.

*Proof Theorem* 7.1 (i). Assume that q is even. In view of Lemma 7.2, the product of degrees of our choice of primary invariants is given by

$$2 \cdot (q+1) \cdot \frac{(q^2-q)}{2} = q(q-1)(q+1) = |\varphi(G)|.$$

Because  $T^G$  is Cohen–Macaulay, we get that  $T^G = K[\det, \mathscr{P}^1(\det), \sqrt{\pi(f_4)}]$ , by [DK, Theorem 3.7.1]. The a-invariant of a polynomial ring is then the negative of the sum of the degrees of the generators.

## 8. The action of $SL_2$ on $\mathfrak{gl}_2$ and $\mathfrak{sl}_2$

We now consider the conjugation action of  $SL_2(K)$  on the space  $V = M_2(K)$  of all  $2 \times 2$  matrices. As before, we see that the kernel of this action is precisely the scalar matrices, i.e., we obtain a faithful action of  $PSL_2(K)$ . Because  $PSL_2(\mathbb{F}_q) = PGL_2(\mathbb{F}_q)$  when q is even, we get the same invariant ring as in Theorem 1.1. For this reason, we now consider K to be a finite field of odd characteristic. In this case, we may fix an irreducible quadratic of the form  $g(x) = x^2 + \delta \in K[x]$ . We then define

(8.1) 
$$f_4 := -\prod_{\substack{A \in K \\ B \in K^{\times}}} \left( Aa + Bb - \frac{A^2 + \delta}{B}c - Ad \right).$$

Up to a sign,  $f_4$  above coincides with our choice as in Definition 3.1. We obtain the following result.

**Theorem 8.1.** Let q be an odd prime power,  $K = \mathbb{F}_q$  the finite field with q elements,  $G := \operatorname{SL}_2(K)$  the special linear group, and  $S := K[X_{2\times 2}]$  the polynomial ring. For the conjugation action of G on S, we have

$$K[X]^{SL_2(K)} = K[\text{trace, det, } \mathscr{P}^1(\text{det}), \sqrt{f_4}, h],$$

where  $f_4$  is as in (8.1), and h is the Jacobian of the other four invariants listed. The invariant ring is a hypersurface with Hilbert series

$$Hilb(S^G, z) = \frac{1 + z^{\binom{q+1}{2}}}{(1 - z)(1 - z^2)(1 - z^{q+1})(1 - z^{\binom{q}{2}})}$$

Additionally,  $S^G$  is not F-regular, is a unique factorisation domain, and has a-invariant -4.

The proof follows the same recipe as before. The additional ingredient is that  $f_4$  above is indeed a perfect square, as we now show. We continue to use the same notation as in the theorem. In particular, K is a finite field of odd characteristic.

**Lemma 8.2.** There exists  $f \in K[X]^{SL_2(K)}$  such that  $f^2 = f_4$ .

*Proof.* The idea is simple: we show that the linear factors appearing in (8.1) occur in pairs, up to sign; thus, we may construct a square root  $f \in K[X]$  by considering only half the factors. To this end, for  $A \in K$  and  $B \in K^{\times}$ , we define  $\lambda(A,B)$  to be the linear factor given by

$$\lambda(A,B) := Aa + Bb - \frac{A^2 + \delta}{B}c - Ad.$$

Because  $\alpha \longmapsto -\alpha$  is an involution of  $K^{\times}$  with no fixed points, we may decompose  $K^{\times}$  as  $P \sqcup -P$  for some subset  $P \subseteq K^{\times}$  of cardinality (q-1)/2. Set

$$f := \prod_{\substack{A \in K \\ B \in P}} \lambda(A, B).$$

We first show that  $f^2 = \pm f_4$ . Noting that  $\lambda(-A, -B) = -\lambda(A, B)$ , we get

$$\begin{split} -f_4 &= \prod_{\substack{A \in K \\ B \in P}} \lambda(A,B) \cdot \prod_{\substack{A \in K \\ B \in -P}} \lambda(A,B) = \prod_{\substack{A \in K \\ B \in P}} \lambda(A,B) \cdot \prod_{\substack{A \in K \\ B \in P}} \lambda(-A,-B). \\ &= (-1)^{|K||P|} \prod_{\substack{A \in K \\ B \in P}} \lambda(A,B) \cdot \prod_{\substack{A \in K \\ B \in P}} \lambda(A,B) = (-1)^{|P|} f^2. \end{split}$$

Thus,  $f^2 = (-1)^{\frac{q+1}{2}} f_4$ . If (q+1)/2 is even, then we are done. Otherwise,  $q \equiv 1 \pmod{4}$  and we have shown  $f^2 = -f_4$ . However, for such a field, -1 has a square root, and we may modify f with a scalar to obtain  $f^2 = f_4$ .

We now show that f is  $SL_2(K)$ -invariant. Let  $\sigma \in GL_2(K)$  be arbitrary. Because  $f_4$  is  $\sigma$ -invariant by Proposition 3.2, we get that  $\sigma(f)^2 = f^2$ . Thus,  $\sigma(f) \in \{f, -f\}$  for all  $\sigma \in GL_2(K)$ , giving us the homomorphism

$$\chi \colon \operatorname{GL}_2(K) \longrightarrow K^{\times}$$

$$\sigma \longmapsto \frac{\sigma(f)}{f}.$$

By Lemma 2.7, we know that the above must be trivial on  $SL_2(K)$ .

*Proof of Theorem 8.1.* The first four invariants listed form a system of primary invariants in view of Theorem 3.3. We now follow the same steps as in Sections 4 and 5. By Porism 4.2,  $S^G$  is Cohen–Macaulay. The product of degrees of the primary invariants is exactly twice the order of  $PSL_2(K)$ , giving us that  $S^G$  is a hypersurface with secondary invariants 1 and  $\eta$ . We obtain  $a(S^G) = a(S) = -4$  and conclude  $deg(\eta) = {q+1 \choose 2}$ . The Jacobian of the chosen primary invariants has this degree, and one checks that this works.

As in Section 7, we now consider the conjugation action of the special linear group on the vector space  $\mathfrak{sl}_2$  of traceless matrices. We continue to denote the corresponding polynomial ring as  $T := K \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ . As before, we have the projection  $\pi : S \longrightarrow T$ , and we define

(8.2) 
$$\widetilde{f}_4 := \pi(f_4) = -\prod_{\substack{A \in K \\ B \in K^{\times}}} \left( 2Aa + Bb - \frac{A^2 + \delta}{B}c \right).$$

In this case, we have the following.

**Theorem 8.3.** Let q be a power of an odd prime,  $K = \mathbb{F}_q$  the finite field with q elements,  $G := \mathrm{SL}_2(K)$  the special linear group, and  $T := \mathrm{Sym}(\mathfrak{sl}_2^*) = K \left[ \begin{smallmatrix} a & b \\ c & -a \end{smallmatrix} \right]$ . For the conjugation action of G on T, we have

$$T^G = K[\det, \mathscr{P}^1(\det), \sqrt{\widetilde{f}_4}, h],$$

where  $\widetilde{f}_4$  is as in (8.2), and h is the Jacobian of the other three invariants listed. The invariant ring is a hypersurface with Hilbert series

$$Hilb(T^G, z) = \frac{1 + z^{\binom{q+1}{2}}}{(1 - z^2)(1 - z^{q+1})(1 - z^{\binom{q}{2}})}.$$

Additionally,  $T^G$  is not F-regular, is a unique factorisation domain, and has a-invariant -3.

*Proof.* The proof proceeds the same way as that of Theorem 7.1 by making use of the corresponding description from Theorem 8.1.

## Part III. The actions of O<sub>2</sub>

We now focus on the conjugation action of the *orthogonal group*  $O_2(K)$ . As usual, we let K denote the finite field with q elements, and define

$$O_2(K) := \{ \sigma \in GL_2(K) : \sigma^{-1} = \sigma^{tr} \}.$$

We use the following bijection to parametrise *G*:

(8.3) 
$$\Phi \colon \{(s,t) \in K \times K : s^2 + t^2 = 1\} \times \{\pm 1\} \longrightarrow \mathcal{O}_2(K)$$

$$(s,t,\varepsilon) \longmapsto \begin{bmatrix} s & t \\ -\varepsilon t & \varepsilon s \end{bmatrix}$$

The above is a bijection even when q is even, with the understanding that the set  $\{\pm 1\}$  is then a singleton.

9. The action of 
$$O_2$$
 on  $\mathfrak{gl}_2$ 

We first consider the conjugation action of G on  $V := M_2(K)$  and in turn on  $S := \operatorname{Sym}(V^*) = K \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ . As before, we set  $\widehat{G} \leq \operatorname{GL}(V)$  to be the image of the conjugation representation; the kernel consists precisely of the scalar matrices. The only scalar orthogonal matrices are  $\pm I_2$ , giving us

$$|\widehat{G}| = \begin{cases} |G| & \text{if } q \text{ is even,} \\ |G|/2 & \text{if } q \text{ is odd.} \end{cases}$$

With the notation of (8.3), we calculate the conjugation action to be

$$(9.1) \qquad \Phi(s,t,\varepsilon): \begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \begin{bmatrix} s^2a - st\varepsilon(b+c) + t^2d & st(a-d) + \varepsilon s^2b - \varepsilon t^2c \\ st(a-d) - \varepsilon t^2b + \varepsilon s^2c & t^2a + \varepsilon st(b+c) + s^2d \end{bmatrix}$$

Thus,  $(b-c) \longmapsto \varepsilon(s^2+t^2)(b-c) = \pm (b-c)$ . The above also gives us that the stabiliser of a consists of the matrices corresponding to t=0; this gives us the matrices  $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ . Thus, we get the following lemma.

**Lemma 9.1.** We have the following for the G-action on S.

- (i) If q is even, then b-c is invariant, and the orbit of a has size |G|.
- (ii) If q is odd, then  $(b-c)^2$  is invariant, and the orbit of a has size |G|/4.

In view of the above lemma, we now define the following invariants.

(9.2) 
$$f_{1} \coloneqq a + d,$$

$$f_{2} \coloneqq ad - bc,$$

$$f_{3} \coloneqq \begin{cases} b - c & \text{if } q \text{ is even,} \\ (b - c)^{2} & \text{if } q \text{ is odd,} \end{cases}$$

$$f_{4} \coloneqq N(a),$$

where N(a) denotes the orbit product of a, i.e., the product of all the polynomials in the orbit of a. We now show that they form a system of primary invariants.

**Theorem 9.2.** The invariants  $f_1, \ldots, f_4$  form a system of parameters for S. We have  $\prod_{i=1}^4 \deg(f_i) = 2|\widehat{G}|$ .

*Proof.* We proceed as in the proof of Theorem 3.3 to show that the only common zero of these polynomials is the origin. For  $f_4$  to vanish, one of its linear factors must vanish. Because the linear factors form a G-orbit and the other  $f_i$  are G-invariant, we may assume without loss of generality that a = 0. It is now clear that the vanishing of the other polynomials forces b = c = d = 0 as well. The second statement follows from the knowledge of deg(N(a)) from Lemma 9.1.

**Theorem 9.3.** Let K be a finite field,  $G := O_2(K)$  the orthogonal group acting via conjugation on  $S := K \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ . The invariant ring  $S^G$  is a hypersurface of the form  $K[f_1, \ldots, f_4, h]$ , where the  $f_i$  are as in (9.2), and h is an invariant of degree  $-4 + \sum_{i=1}^4 \deg(f_i)$ . The Hilbert series of  $S^G$  is given as

$$Hilb(S^G, z) = \frac{1 + z^{\deg h}}{(1 - z)(1 - z^2)(1 - z^{\deg f_3})(1 - z^{\deg f_4})}$$

Additionally, the invariant ring  $S^G$  has a-invariant -4, is F-regular precisely when  $\operatorname{char}(K) \neq 2$ , and is a unique factorisation domain precisely when  $\operatorname{char}(K) = 2$ . When  $\operatorname{char}(K) \neq 2$ , we may take h to be  $\operatorname{Jac}(f_1, \ldots, f_4)$ , and the class group of  $S^G$  is  $(\mathbb{Z}/2)^2$ .

*Proof.* By Porisms 4.2 and 4.6, we know that  $S^G$  is Cohen–Macaulay with a-invariant -4. The rest of the proof is as we have seen in Part I: By Theorem 9.2, we see that  $S^G$  is a hypersurface with the degree of h as listed. Because  $a(S^G) = a(S)$ , we see that  $S^G$  is F-regular precisely when the action is nonmodular. In view of Lemma 9.4, this is equivalent to  $\operatorname{char}(K) \neq 2$ . Next, we have  $\operatorname{Cl}(S^G) \cong \operatorname{Hom}(\widehat{G}/[\widehat{G},\widehat{G}],K^\times)$ ; this is (0) when q is even because  $\widehat{G}$  and  $K^\times$  then have coprime orders. When q is odd, it is known that  $G/[G,G] \cong (\mathbb{Z}/2)^2$ , by [Di, pp. 50, 55]. Because -I is the commutator of  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ , we get that  $\widehat{G}/[\widehat{G},\widehat{G}] \cong G/[G,G] \cong (\mathbb{Z}/2)^2$  and the result follows after noting that  $K^\times$  is a cyclic group of even order.

We now record the order of G and the degrees of the above invariants.

**Lemma 9.4.** Continuing with the earlier notation, we have the following.

- (i) If q is even, then  $|G| = |\widehat{G}| = q$ . We have  $\deg(f_3) = 1$ ,  $\deg(f_4) = q$ , and  $\deg(h) = q$ .
- (ii) If  $q \equiv 1 \pmod{4}$ , then  $|G|/2 = |\widehat{G}| = q 1$ . We have  $\deg(f_3) = 2$ ,  $\deg(f_4) = (q - 1)/2$ , and  $\deg(h) = (q + 1)/2$ .
- (iii) If  $q \equiv -1 \pmod{4}$ , then  $|G|/2 = |\widehat{G}| = q + 1$ . We have  $\deg(f_3) = 2$ ,  $\deg(f_4) = (q+1)/2$ , and  $\deg(h) = (q+3)/2$ .

*Proof.* We only need to calculate |G|. In view of (8.3), this comes down to calculating the size of the circle  $S := \{(s,t) \in K \times K : s^2 + t^2 = 1\}$ . When q is even, the condition  $s^2 + t^2 = 1$  is equivalent to s + t = 1 and the result follows. When q is odd, it is well-known that the cardinality of S is  $q - (-1)^{(q-1)/2}$ ; alternatively, the order of G may be found in [Ja, §6.10] after noting that -1 is a square in K precisely when  $q \equiv 1 \pmod{4}$ .  $\square$ 

10. The action of 
$$O_2$$
 on  $\mathfrak{o}_2$  and symmetric matrices

The polynomial invariants for the adjoint representation of  $G = O_2(K)$  are easily calculated.

**Remark 10.1.** The group G is one-dimensional and its Lie algebra  $\mathfrak{o}_2 \leqslant M_2(K)$  consists of alternating matrices; in fact, the adjoint representation is simply the map  $\det\colon G \longrightarrow K^\times$ . Thus, if we let K[b] denote  $\operatorname{Sym}(\mathfrak{o}_2^*)$ , then  $K[b]^G$  is either  $k[b^2]$  or k[b] according to whether the characteristic is either odd or even.

A more interesting action is obtained by noticing that the space of symmetric matrices is stable under conjugation by the orthogonal group. We continue with the notation from the previous section and further define

$$W := \{M \in V : M = M^{\operatorname{tr}}\}$$
 and  $T := \operatorname{Sym}(W^*)$ .

The invariant ring turns out to be a polynomial ring, regardless of the characteristic, as we now show. We have the suggestive coordinates for T given as  $T = K \begin{bmatrix} a & b \\ b & d \end{bmatrix}$ . As in Section 7, we have the G-equivariant K-algebra map  $\pi : S \longrightarrow T$  given by  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & b \\ b & d \end{pmatrix}$ . Moreover, as before, the inclusion  $W \hookrightarrow V$  splits G-equivariantly in odd characteristic, and we obtain the invariant ring as  $T^G = \pi(S^G)$  when  $\operatorname{char}(K)$  is odd. The following theorem describes the invariant ring. As before, we continue to interpret trace,  $\operatorname{det}, N(a)$  as elements of T.

**Theorem 10.2.** Let  $K := \mathbb{F}_q$  be a finite field with q elements. Consider the conjugation action of  $G := O_2(K)$  on  $T = K[X_{2 \times 2}^{sym}] = K\begin{bmatrix} a & b \\ b & d \end{bmatrix}$ . Then,  $T^G$  is a polynomial ring given as

$$T^G = K[\text{trace}, \text{det}, f_3],$$

where  $f_3$  is chosen as follows:

- (i) If q is odd, then  $f_3 = N(a)$ ; we have  $\deg(f_3) = |G|/4$ , and  $a(S^G) = -\left(3 + \frac{1}{2}\left(q (-1)^{(q-1)/2}\right)\right)$ .
- (ii) If  $q = 2^{e+1}$  with  $e \ge 0$ , then

$$f_3 := \sum_{k=0}^{e} b^{2^k} (a+d)^{2^e-2^k};$$

we have  $\deg(f_3) = |G|/2 = q/2$ , and  $a(S^G) = -(3 + \frac{q}{2})$ .

*Proof.* Note that  $\binom{1\ 0}{0\ 1} \in W^G$ , and so  $\operatorname{codim}(W^G) \leq 2$ , giving us that  $T^G$  is Cohen–Macaulay. In either case, the product of the degrees of the claimed generators is equal to  $|G/\{\pm I\}|$ , and the a-invariant is the negative of the sum of degrees. Thus, it suffices to show that the claimed generators are indeed invariant and that they form a system of parameters. For odd characteristic, this follows from the work done in Section 9. Thus, we now assume that  $q = 2^{e+1}$ . In view of (8.3) and (9.1), the group G consists of matrices of the form  $\varphi(t) = \binom{1-t}{t} \binom{t}{1-t}$  for  $t \in K$ , and we have  $\varphi(t) \cdot b = b + (t-t^2)(a+d)$ . As a+d is invariant, the Freshman's Dream [NT] yields

$$\varphi(t) \cdot f_3 = \sum_{k=0}^{e} \left( b^{2^k} + (t - t^2)^{2^k} (a + d)^{2^k} \right) (a + d)^{2^e - 2^k} = f_3 + \sum_{k=0}^{e} (t^{2^k} - t^{2^{k+1}}) (a + d)^{2^e}.$$

The sum telescopes to give us  $\varphi(t) \cdot f_3 = f_3 + (t - t^q)(a + d)^{q/2}$ . Because K is the field with q elements, we have  $t = t^q$ , giving us the invariance of  $f_3$ . It is clear that they form a system of parameters because  $(a+d,ad-b^2,f_3)T = (a+d,ad-b^2,b^{2^e})T$ , giving us the radical as (a,b,d)T.

## APPENDIX A. STEENROD OPERATIONS

In this section, we describe how one may produce new invariants from old using the Steenrod operations, a feature available over finite fields. A reference for the material presented here is [Sm1, Chapter 11].

Let q be a prime power, and  $K = \mathbb{F}_q$  the finite field with q elements. Let  $S = K[x_1, \dots, x_n]$  be a polynomial ring over K, and S[T] the polynomial ring obtained by adjoining an additional variable. We define the K-algebra map  $\mathscr{P} \colon S \longrightarrow S[T]$  by defining it on the variables as  $x_i \longmapsto x_i + x_i^q T$ . This definition is coordinate-free in the sense that  $\mathscr{P}(x) = x + x^q T$  for any homogeneous linear element  $x \in S$ . For any nonnegative integer  $i \geqslant 0$  and  $f \in S$ , we define  $\mathscr{P}^i(f)$  to be the coefficient of  $T^i$  in  $\mathscr{P}(f)$ . In other words, we have K-linear maps  $\mathscr{P}_i \colon S \longrightarrow S$  satisfying, for all  $f \in S$ , the equation

$$\mathscr{P}(f) = \sum_{i>0} \mathscr{P}^i(f)T^i.$$

These operations are natural in the following sense: Let  $R = K[y_1, ..., y_m]$  be a polynomial ring, and  $\varphi : S \longrightarrow R$  a degree-preserving K-algebra map. Then, the diagram below on the left commutes. In turn, so does the diagram below on the right, for all  $i \ge 0$ .

In particular, if  $\varphi: S \longrightarrow S$  is a degree-preserving K-algebra automorphism and  $f \in S$  is fixed by  $\varphi$ , then so is  $\mathscr{P}^i(f)$  for any i. This lets us produce new invariants from old, giving us the following.

**Lemma A.1.** Let K be a finite field, S a polynomial ring over K, and G a group acting on S by degree-preserving K-algebra automorphisms. If  $f \in S^G$  is an invariant, then  $\mathscr{P}^i(f) \in S^G$  for all  $i \geqslant 0$ .

## REFERENCES

- [AM] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128. 4
- [BCP] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. 3
- [Be] D. J. Benson. *Polynomial invariants of finite groups*. Vol. 190. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1993, pp. x+118. 10
- [BH] Winfried Bruns and Jürgen Herzog. "On the computation of *a*-invariants". In: *Manuscripta Math.* 77.2-3 (1992), pp. 201–213. 8
- [Br] Abraham Broer. "The direct summand property in modular invariant theory". In: *Transform. Groups* 10.1 (2005), pp. 5–27. 10
- [CW] H. E. A. Eddy Campbell and David L. Wehlau. *Modular invariant theory*. Vol. 139. Encyclopaedia of Mathematical Sciences. Invariant Theory and Algebraic Transformation Groups, 8. Springer-Verlag, Berlin, 2011, pp. xiv+233. 4, 7, 12
- [Di] Jean Dieudonné. *La géométrie des groupes classiques*. Vol. Heft 5. Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.) Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955, pp. vii+115. 16
- [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. 1–3, 8, 9, 13
- [GJS] Kriti Goel, Jack Jeffries, and Anurag K. Singh. "Local Cohomology of Modular Invariant Rings". In: *Transformation Groups* (Mar. 2024). 8, 10
- [GW] Shiro Goto and Keiichi Watanabe. "On graded rings. I". In: *J. Math. Soc. Japan* 30.2 (1978), pp. 179–213. 8
- [HH] Melvin Hochster and Craig Huneke. "Tight closure of parameter ideals and splitting in module-finite extensions". In: *J. Algebraic Geom.* 3.4 (1994), pp. 599–670. 10
- [HK] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1971, pp. viii+407. 5
- [Ja] Nathan Jacobson. *Basic algebra. I.* Second. W. H. Freeman and Company, New York, 1985, pp. xviii+499. 6,
- [Je] Kenneth Carl Jeffries. *Rings of invariants, F-regularity, and local cohomology*. Thesis (Ph.D.)–The University of Utah. ProQuest LLC, Ann Arbor, MI, 2015, p. 55. 10
- [Ke] Gregor Kemper. "On the Cohen-Macaulay property of modular invariant rings". In: *J. Algebra* 215.1 (1999), pp. 330–351. 11
- [KW] Victor Kac and Keiichi Watanabe. "Finite linear groups whose ring of invariants is a complete intersection". In: *Bull. Amer. Math. Soc.* (*N.S.*) 6.2 (1982), pp. 221–223. 11
- [NT] Numberphile and Kevin Tucker. *The Freshman's Dream (a classic mistake)*. YouTube. 2024. URL: https://www.youtube.com/watch?v=vW5qLFDsZ30. 17
- [Sm1] Larry Smith. *Polynomial invariants of finite groups*. Vol. 6. Research Notes in Mathematics. A K Peters, Ltd., Wellesley, MA, 1995, pp. xvi+360. 9, 17
- [Sm2] Larry Smith. "Invariants of 2 × 2-matrices over finite fields". In: *Finite Fields Appl.* 8.4 (2002), pp. 504–510. 1
- [Th] R. C. Thompson. "Commutators in the special and general linear groups". In: *Trans. Amer. Math. Soc.* 101 (1961), pp. 16–33. 6