Polynomial invariants of GL_2: Conjugation over finite fields

Aryaman Maithani

February 7, 2025 at University of Utah
February 24, 2025 at UC Sand Diego

Introduction

These are the notes that I made for the talks that I gave on my paper [Ma]. Talk abstract:

> Consider the conjugation action of $GL_2(K)$ 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.

Let K be a field, $S \coloneqq K[X_{n\times n}]$ the polynomial ring in n^2 variables, and $G \coloneqq GL_n(K)$ the general linear group. The group G acts on S via *conjugation*, i.e., the element $\sigma \in G$ acts on S via

$$X \mapsto \sigma X \sigma^{-1};$$

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 $\sigma^{-1} X \sigma$.

We are interested in the K-subalgebra

$$S^G \coloneqq \{f \in S : \sigma(f) = f \text{ for all } \sigma \in G\}.$$

Question. Are any of the following matrices similar (over $\mathbb{Q}$)? How would you tell?

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$$

How does this relate to question of invariants?

§1. Over infinite fields

Theorem 1.1. If K is an infinite field, then $S^G = K[\mathrm{trace}(X), \ldots, \det(X)]$, i.e., S^G is generated by the coefficients of the characteristic polynomial of X. Moreover, S^G is a polynomial ring.

Proof. Because the field is infinite, we may adopt the following point of view:

$$\text{elements of } S \equiv \text{polynomial functions on } K^{n\times n}$$
$$\text{elements of } S^G \equiv \text{polynomial functions constant on orbits,}$$

where by orbits we are referring to natural conjugation action of G on $K^{n\times n}$.

Write

$$\det(tI - X) = t^n - f_1 t^{n-1} + \cdots + (-1)^n f_n$$

for $f_i \in S$. We wish to show that $S^G = K[f_1, \ldots, f_n]$ and that the f_i are algebraically independent. The inclusion $(\supseteq)$ is clear. For the converse, let $f \in S^G$ be arbitrary.

Consider the subspace of diagonal matrices $D \leqslant V$, and the symmetric group S_n as a subgroup of $GL_n(K)$ in the natural way. Then, the action of G restricts to S_n, and S_n acts on D in the 'obvious' way: the transposition (i, j) swaps the i-th and j-th diagonal entries. Let $e_1, \ldots, e_n$ denote the elementary symmetric polynomials on $x_{11}, x_{22}, \ldots, x_{nn}$. The function $f|_D$ is S_n-invariant and thus, we may write

$$f|_D - p(e_1, \ldots, e_n) \equiv 0$$

for some polynomial p. In particular, this means that we have

$$f - p(f_1, \ldots, f_n) \equiv 0 \text{ on } D; \tag{†}$$

this is because the $f_i|_D = e_i$. This also shows that the f_i are algebraically independent. But f and each f_i is G-invariant. This means that the equation (†) holds on $G \cdot D$, the set of all diagonalisable matrices. But this set is Zariski-dense in V, showing that $f = p(f_1, \ldots, f_n)$ as elements of S. □

The above cannot hold if K is a finite field, and n is at least 2. Indeed, $GL_n(K)$ is then a finite group and thus, the inclusion

$$S^G \subseteq S$$

is integral. In particular, both rings must have Krull dimension n^2. However, the subring $K[\mathrm{trace}(X), \ldots, \det(X)]$ has Krull dimension n.

§2. Over finite fields

From now on, we fix some notations.

We have $K := \mathbb{F}_q$ the finite field on q elements, $G := GL_2(K)$ the general linear group, $S := K[X_{2\times 2}] = K\left[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right]$, and G acts on S by conjugation.

The idea is to compute S^G as follows: first, construct a *Noetherian normalisation* for S^G; this amounts to finding a homogeneous system of parameters $f_1, \ldots, f_4 \in S^G$ (it suffices to show that they form an hsop for S). In that case, the ring $R := K[f_1, f_2, f_3, f_4]$ is a polynomial ring such that S^G is a finite R-module. Next, we find $h_1, \ldots, h_n \in S^G$ such that $S^G = Rh_1 + \cdots Rh_n$ as R-modules. In particular, S^G is generated, as a K-algebra, by the f_i and h_j.

The f_i are called primary invariants, the h_j secondary invariants. These are not uniquely determined by any means. However, there are different notions of minimality that one may impose. Experiments on `Magma` [BCP] suggested that the ring of invariants is a hypersurface: more precisely, there exist primary invariants in degrees 1, 2, $q+1$, and $q^2 - q$, such that with these primary invariants, the secondary invariants are in degrees 0 and q^2.

§3. Primary invariants

Set $f_1 := a + d$, $f_2 := ad - bc$.

It is clear that the above are invariants. Using `Magma`, it looked that the third primary invariant took a particularly nice closed form. We define

$$f_3 := a^{q+1} + b^q c + bc^q + d^{q+1}.$$

It is not too difficult to check that the above is G-invariant. For example, one may use that

$$GL_2(K) = \left\langle \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \begin{bmatrix} \beta & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} \right\rangle, \tag{3.1}$$

where $K^\times = \langle \beta \rangle$.

The action of the three elements is respectively given as

$$\begin{gathered} a \leftrightarrow d, \quad b \leftrightarrow c, \\ a \mapsto a, \quad b \mapsto \beta^{-1} b, \quad c \mapsto \beta c, \quad d \mapsto d, \\ a \mapsto a - c, \quad b \mapsto a + b - c - d, \quad c \mapsto c, \quad d \mapsto c + d. \end{gathered}$$

One may then check $\sigma(f_3) = f_3$ for any of the above generators, noting that $\beta^{q-1} = 1$. However, there is a more abstract way to see this: we have

$$f_3 = (a + d)^{q+1} - (a^q d + ad^q - b^q c - bc^q)$$

and so, it suffices to show that the last element is an invariant; this follows by noting that it is $\mathcal{P}^1(ad - bc)$ for a 'nice' operation $\mathcal{P}^1$, a *Steenrod operation*.

Things now seemed to be a dead end. `Magma` suggested that the fourth primary invariant should have degree $q^2 - q$. But it was not clear what it should be. One way of producing invariants for finite groups is to look at orbit products. We get lucky with the following.

Fix an irreducible quadratic $g(x) \coloneqq x^2 - \tau x + \delta \in K[x]$.

Such a quadratic exists because K is a finite field. Straightforward linear algebra gives us the following fact.

Theorem 3.1. Let $\Omega \subseteq V$ be the set of 2×2 matrices with characteristic polynomial equal to $g(x)$. Then,

$$\Omega = \left\{ \begin{bmatrix} A & B \\ -\frac{g(A)}{B} & \tau - A \end{bmatrix} : A \in K, B \in K^\times \right\}.$$

In particular, $|\Omega| = q(q-1) = q^2 - q$.

Thus, we get a fourth invariant of the *correct degree* defined as

$$f_4 \coloneqq \prod_{\substack{A \in K \\ B \in K^\times}} \left(Aa + Bb - \frac{g(A)}{B} c + (\tau - A) d \right).$$

Theorem 3.2. The elements $f_1, \ldots, f_4$ form a homogeneous system of parameters for S and hence, for S^G.

Sketch. It suffices to show that the only solution to $f_1 = \cdots = f_4 = 0$ over $\overline{K}^4$ is the origin. Let $(a, b, c, d) \in \overline{K}^4$ be such a solution. We may discard $f_1 = 0$ by substituting $d = -a$ in the other equations and then it suffices to show that $a = b = c = 0$. The equation $f_4 = 0$ gives us the existence of $A \in K$ and $B \in K^\times$ such that one the factors in f_4 is zero. We may solve for b in terms of a and c and substitute this in $f_2 = 0$. We then get a quadratic equation in a that we may solve as

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

for some $\mu \in \overline{K}$ such that $g(\mu) = 0$. Necessarily $\mu \notin K$. In turn, we get b as

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

Letting $\gamma \coloneqq (A + \mu)/B \in \overline{K} \setminus K$, we substitute these values in $f_3 = 0$ to get

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

The first term is nonzero because $\gamma \notin K$. Thus, $c = 0$ and in turn, so are the others. $\square$

Thus, we now have a Noether normalisation for S^G,

$$R := K[f_1, f_2, f_3, f_4] \subseteq S^G.$$

In turn, we have a decomposition of R-modules

$$S = Rh_1 + Rh_2 + \cdots + Rh_n.$$

§4. Determining n

We now determine n by first showing that R is Cohen–Macaulay. First, we define P to be the following Sylow-p group of G:

$$V := \begin{bmatrix} 1 & K \\ & 1 \end{bmatrix} \leqslant G.$$

Lemma 4.1. We have $\dim(V^P) = 2$. Equivalently, $\operatorname{codim}(V^P) = 2$.

Sketch. The fixed points are precisely the elements that commute with elements of P. Check that $V^P = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix} \right) : a, b \in K \right\}$. □

Corollary 4.2. S^P is Cohen–Macaulay.

Proof. This follows from [CW, Theorem 3.9.2] as we have shown $\operatorname{codim}(V^P) = 2$. □

Corollary 4.3. S^G is Cohen–Macaulay.

Proof. The inclusion $S^G \hookrightarrow S^P$ is split via the splitting $s \mapsto \frac{1}{[G:P]} \sum_{g \in G/P} g(s)$. Because this is a finite extension, we obtain the result. □

Thus, we can improve the decomposition to

$$S = Rh_1 \oplus Rh_2 \oplus \cdots \oplus Rh_n.$$

We are now at a stage where we must take faith seriously: the conjugation is not faithful, action the scalar matrices act trivially.

Indeed, the action of G leads to a corresponding homomorphism

$$\rho\colon G \to GL(V).$$

The kernel of the above is precisely the subgroup of scalar matrices.

We let $\widehat{G}$ denote its image, i.e.,

$$\rho\colon G \twoheadrightarrow \widehat{G} \subseteq GL(V).$$

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

The action of $\widehat{G}$ on V (and S) is faithful and we have $S^G = S^{\widehat{G}}$.

Now, using [DK, Theorem 3.7.1], we obtain the (minimal) number of secondary invariants as

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

Thus,

$$S = Rh_1 \oplus Rh_2.$$

Moreover, we may always take $h_1 = 1$ as a minimal secondary invariant to obtain the decomposition

$$S = R \oplus Rh.$$

In particular, S is a hypersurface with

$$S = K[f_1, f_2, f_3, f_4, h].$$

Consequently, the Hilbert series of S^G is then given as

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

§5. **Determining** $\deg(h)$

To determine $\deg(h)$, it suffices to determine the degree of the Hilbert series[1] $\mathrm{Hilb}(S^G)$. Because the ring S^G is Cohen–Macaulay, this degree is given by the a-*invariant*.[2] We make

[1]The degree of a rational function is the difference of the degrees of the numerator and denominator.

[2]The a-invariant of a graded ring R is the highest degree in which the local cohomology module $H^{\dim(R)}_{\mathfrak{m}_R}(R)$ is nonzero.

use of the following theorem to determine the a-invariant.

Theorem 5.1 ([GJS, Theorem 4.4]). If $\widehat{G}$ is a subgroup of $SL(V)$ and contains no pseudoreflections, then $a(S^{\widehat{G}}) = a(S)$.

We recall that an element $\sigma \in GL(V)$ is said to be a pseudoreflection if $\operatorname{rank}(\sigma - \mathrm{id}) = 1$.

Proposition 5.2. For the $\widehat{G}$ in our context, the hypothesis of the above theorem holds. In particular, $a(S^G) = -4$.

Sketch. To check $\widehat{G} \leqslant SL(V)$, one checks that $\rho(\sigma) \in SL(V)$ for each of the three generators σ defined in (3.1). Alternately: we see that $\rho(\sigma)$ is the composition $L(\sigma) \circ R(\sigma)^{-1}$, where $L(\sigma)$ and $R(\sigma)$ denote the left and right multiplication maps, respectively. Thus, it suffices to show $\det(L(\sigma)) = \det(R(\sigma))$. Simple linear algebra tells us that both of these are indeed equal (and equal to $\det(\sigma)^2$).

To check that $\widehat{G}$ contains no pseudoreflections, it suffices to show that the dimension of the centraliser of any $M \in GL_2(K)$ is not 3. By considering Jordan forms, one sees that this dimension is either 2 or 4. $\square$

Thus,

$$-4 = \deg(h) - (1 + 2 + (q+1) + (q^2 - q)),$$

giving us $\deg(h) = q^2$.

§6. The missing invariant

We now need to construct a new invariant h of degree q^2. In fact, it is not difficult to check using normality that *any* homogeneous invariant $h \in S^G \setminus R$ of degree q^2 will do the job.

We define

$$\begin{aligned} h &\coloneqq \operatorname{Jac}(f_1, \ldots, f_4) \\ &= \det \begin{bmatrix} 1 & 0 & 0 & 1 \\ d & -c & -b & a \\ a^q & c^q & b^q & d^q \\ \frac{\partial f_4}{\partial a} & \frac{\partial f_4}{\partial b} & \frac{\partial f_4}{\partial c} & \frac{\partial f_4}{\partial d} \end{bmatrix}. \end{aligned} \tag{6.1}$$

Because the group $\widehat{G}$ is contained in $SL(V)$, the chain rule gives us that $h \in S^G$, see [Sm, Proposition 1.5.6].

Moreover, the degree of the entries of the i-th row is seen to be $\deg(f_i) - 1$, and thus,

$$\deg(h) = \sum_{i=1}^{4} (\deg(f_i) - 1) = \boxed{q^2},$$

as desired!

There is only one issue left: is $h \notin R$? As it turns, this fails precisely in characteristic 2.

Theorem 6.1. If $\mathrm{char}(K) \neq 2$, then $h \notin R$.

Proof. Consider the element $\tau_{ad} \in GL(V)$ that acts on S by fixing b and c, and swapping $a \leftrightarrow d$. Then, it is a quick check that all the f_i are τ_{ad}-invariant. Thus,

$$R \subseteq S^{\langle \widehat{G}, \tau_{ad} \rangle} \subseteq S^G.$$

However, the action of τ_{ad} on the matrix in (6.1) swaps the extreme columns and thus, $\tau_{ad}(h) = -h$. If $\mathrm{char}(K) \neq 2$, then this shows that h is not τ_{ad}-invariant and hence, $h \notin R$. $\square$

Remark 6.2. For the above argument to work, one needs that $h \neq 0$. This requires a slight calculation (but is true, in any characteristic).

Moreover, if $\mathrm{char}(K) = 2$, then the above calculation shows that $h \in S^{\langle \widehat{G}, \tau_{ad} \rangle}$. It is not too difficult to show that $S^{\langle \widehat{G}, \tau_{ad} \rangle} = R$ and thus, $h \in R$ in characteristic two.

§7. Additional results

Because the a-invariant remains the same and the group action is *modular*[3], it follows that the inclusion $S^G \hookrightarrow S$ is not split, see [GJS, Corollary 4.2]. Thus, S^G is not F-regular.

The class group of S^G is well-known. Because the group action contains no pseudoreflections, the class group of S^G is given by

$$\mathrm{Class}(S^G) \cong \mathrm{Hom}_{\mathbf{Grp}}(\widehat{G}, K^\times) \cong \mathrm{Hom}_{\mathbb{Z}}(\widehat{G}/[\widehat{G}, \widehat{G}], K^\times);$$

see [Be, Theorem 3.9.2] for the first isomorphism.

In particular, S^G is a UFD iff there is no nontrivial homomorphism $\widehat{G} \to K^\times$. One notes that $\widehat{G} \cong PGL_2(K)$. Some group theory gives us that

$$\mathrm{char}(K) = 2 \Leftrightarrow \mathrm{Class}(S^G) = 0 \Leftrightarrow S^G \text{ is a UFD}$$

[3] The order of $|\widehat{G}|$ is divisible by $\mathrm{char}(K)$

and

$$\mathrm{char}(K) \neq 2 \Leftrightarrow \mathrm{Class}(S^G) \cong \mathbb{Z}/2.$$

In fact, these results generalise readily to an arbitrary $n \geqslant 3$ with similar arguments: if $G \coloneqq \mathrm{GL}_n(K)$ acts on $S \coloneqq K[X_{n\times n}]$ via conjugation, then

(a) $a(S^G) = a(S) = -n^2$ and $S^G \hookrightarrow S$ does not split (hence, S^G is not F-regular), and

(b) S^G is a unique factorisation domain iff n and $q-1$ are coprime; with the class group being $\mathbb{Z}/\gcd(n, q-1)$ in general.

References

[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. 8

[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. 5

[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. 6

[GJS] Kriti Goel, Jack Jeffries, and Anurag K. Singh. "Local Cohomology of Modular Invariant Rings". In: *Transformation Groups* (Mar. 2024). 7, 8

[Ma] Aryaman Maithani. *Polynomial invariants of* GL_2*: Conjugation over finite fields*. 2025. arXiv: `2501.15080 [math.AC]`. 1

[Sm] Larry Smith. *Polynomial invariants of finite groups*. Vol. 6. Research Notes in Mathematics. A K Peters, Ltd., Wellesley, MA, 1995, pp. xvi+360. 7