THE INVARIANTS OF THE THIRD SYMMETRIC POWER REPRESENTATION OF $SL_2(\mathbb{F}_p)$

ASHLEY HOBSON AND R. JAMES SHANK

Abstract. For a prime $p > 3$, we compute a finite generating set for the $SL_2(\mathbb{F}_p)$-invariants of the third symmetric power representation. The proof relies on the construction of an infinite SAGBI basis and uses the Hilbert series calculation of Hughes and Kemper.

1. Introduction

Consider the generic binary cubic over a field $\mathbb{F}$ of characteristic not 3:

$$a_0X^3 + 3a_1X^2Y + 3a_2XY^2 + a_3Y^3.$$

Identifying

$$X = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

induces a left action of the general linear group $GL_2(\mathbb{F})$ on the third symmetric power

$$V := \mathrm{Span}_{\mathbb{F}}[\, Y^3, 3Y^2X, 3YX^2, X^3\,]$$

and a right action on the dual $V^* = \mathrm{Span}_{\mathbb{F}}[a_3, a_2, a_1, a_0]$. For example

$$\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{acts on } V^* \text{ as} \quad \begin{bmatrix} 1 & 3 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

with $a_3 = [1\ 0\ 0\ 0]$, $a_2 = [0\ 1\ 0\ 0]$, $a_1 = [0\ 0\ 1\ 0]$, $a_0 = [0\ 0\ 0\ 1]$. The action on V^* extends to an action by algebra automorphisms on the symmetric algebra $\mathbb{F}[V] = \mathbb{F}[a_3, a_2, a_1, a_0]$. For any subgroup $G \leq GL_2(\mathbb{F})$, we denote the subring of invariant polynomials by $\mathbb{F}[V]^G$.

Throughout we assume that $\mathbb{F}$ has characteristic $p > 3$. Thus $\mathbb{F}_p \subseteq \mathbb{F}$ and $SL_2(\mathbb{F}_p) \leq GL_2(\mathbb{F})$. The primary goal of this paper is to compute a finite generating set for $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$. We note that V is the unique four-dimensional irreducible representation of $SL_2(\mathbb{F}_p)$ (see, for example, [2, pp. 14–16]). Also, for $p \neq 7$, $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ is not Cohen-Macaulay and in fact has depth 3 [13, §5]. In the language of L.E. Dickson [6, Lecture III §9], we give a fundamental

Date: June 2, 2010.
1991 *Mathematics Subject Classification.* 13A50.
The research of the first author was supported by grants from EPSRC.

system for the formal modular invariants of the binary cubic. Dickson considered this problem but was only able to identify a few specific invariants. We proceed by constructing the required invariants and then proving that the given set generates $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$. Our proof relies on the construction of an infinite SAGBI basis and uses the Hilbert series calculation of Hughes and Kemper [8]. Recall that a SAGBI basis is a **S**ubalgebra **A**nalog of a **G**röbner **B**asis for **I**deals. SAGBI bases were introduced independently by Robbiano-Sweedler [11] and Kapur-Madlener [9]; a useful reference is Chapter 11 of Sturmfels [15] (who uses the term *canonical subalgebra basis*). The ring of invariants of a modular representation of a p-group always has a finite SAGBI basis for an appropriate choice of term order, see [14]. A finite SAGBI basis for the ring of invariants of the Sylow p-subgroup of $SL_2(\mathbb{F}_p)$ was computed in [12]. Extensive preliminary calculations for small primes, using MAGMA [4], involving SAGBI bases and the relative transfer map, lead to the given generating set (see [7]). We use the graded reverse lexicographic order with $a_0 < a_1 < a_2 < a_3$. For background material on term orders and Gröbner bases see Adams-Loustaunau [1]. For background material on the invariant theory of finite groups see Benson [3], Derksen-Kemper [5] or Neusel-Smith [10].

A classical example of an invariant of a binary form is the discriminant, which in this case can be written as

$$D := 3a_2^2a_1^2 - 4a_3a_1^3 - 4a_2^3a_0 + 6a_3a_2a_1a_0 - a_3^2a_0^2.$$

Following Lecture III of L. E. Dickson's Madison Colloquium [6] we identify the $SL_2(\mathbb{F}_p)$-invariant

$$L := 3(a_2^pa_1 - a_2a_1^p) - (a_3^pa_0 - a_3a_0^p).$$

Let B denote the Borel subgroup of $SL_2(\mathbb{F}_p)$ consisting of upper triangular matrices and let P denote the unique Sylow p-subgroup of B. Observe that P is cyclic of order p and is also a Sylow p-subgroup of $SL_2(\mathbb{F}_p)$. Define

$$N := \prod_{\tau\in P}(a_3)\tau.$$

By Corollary 2.4, $N \cdot a_0$ is $SL_2(\mathbb{F}_p)$-invariant (or see [6]).

For a subgroup H of a group G, choose coset representatives G/H and define the relative transfer

$$\begin{array}{rcl}\mathrm{tr}_H^G : \mathbb{F}[V]^H & \to & \mathbb{F}[V]^G \\ f & \mapsto & \displaystyle\sum_{\tau\in G/H}(f)\tau.\end{array}$$

The transfer, tr^G, is the special case when H is the trivial group. Define

$$K := -\mathrm{tr}^{SL_2(\mathbb{F}_p)}(a_1^{p-1}).$$

We show in Lemma 2.10 that K is non-zero with lead monomial a_2^{p-1}.

For $\omega \in \mathbb{F}_p^*$, the diagonal matrix

$$\rho_\omega = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix} \text{ acts on } V^* \text{ as } \begin{bmatrix} \omega^3 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & \omega^{-1} & 0 \\ 0 & 0 & 0 & \omega^{-3} \end{bmatrix}.$$

This motivates the definition of a multiplicative weight function on monomials by

$$\mathrm{wt}(a_i) = 2i - 3.$$

Thus for any monomial β, we have $(\beta)\rho_\omega = \omega^{\mathrm{wt}(\beta)}\beta$. Since $\omega^{p-1} = 1$, it is convenient to assume that the weight function takes values in $\mathbb{Z}/(p-1)\mathbb{Z}$. Since B is generated by elements of P and ρ_ω for $\omega \in \mathbb{F}_p^*$, it is clear that the B-invariants are precisely the isobaric P-invariants of weight zero (modulo $p-1$).

We show in Lemma 2.1 that N is isobaric of weight 3 (modulo $p-1$). Let c denote the smallest positive integer satisfying $3c \equiv_{(p-1)} 0$. Thus $c = (p-1)/3$ if $p \equiv_{(3)} 1$ and $c = p-1$ if $p \equiv_{(3)} -1$. Then N^c is B-invariant and

$$\delta := \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(N^c)$$

is $SL_2(\mathbb{F}_p)$-invariant. It follows from Theorem 2.5 that the lead monomial of δ is a_3^{pc}. We show in Theorem 2.12 that $\{D, K, Na_0, \delta\}$ forms a homogeneous system of parameters, i.e., the set is algebraically independent and $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ is a finite module over $\mathbb{F}[D, K, Na_0, \delta]$.

It is easily verified that $d := a_1^2 - a_2a_0$ and $e := 2a_1^3 + a_0(a_3a_0 - 3a_2a_1)$ are isobaric P-invariants of weight -2 and -3 respectively. Define

$$\tilde{e} := \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(Ne).$$

We will show, see Theorem 3.1, that for $p \equiv_{(3)} 1$, the $SL_2(\mathbb{F}_p)$-invariants are generated by

$$D, K, L, Na_0, \delta, \tilde{e}$$

and an explicitly described finite subset of the image of the transfer. For $p \equiv_{(3)} -1$ the additional invariant

$$\tilde{d} := \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(N^{\frac{p+1}{3}}d)$$

is required.

2. Preliminaries, lead monomials and tête-à-têtes

For the remainder of the paper we use G to denote $SL_2(\mathbb{F}_p)$. The following generalises [13, 2.4].

Lemma 2.1. *If f is an isobaric polynomial of weight λ, then $\mathrm{tr}^P(f)$ is isobaric of weight λ. Furthermore N is isobaric of weight 3.*

Proof. The result follows from the fact that P is normal in B. For $\omega \in \mathbb{F}_p^*$

$$\begin{aligned}\left(\mathrm{tr}^P(f)\right)\rho_\omega &= \sum_{\tau\in P}(f)\,\tau\rho_\omega = \sum_{\tau'\in P}(f)\,\rho_\omega\tau' \\ &= \sum_{\tau'\in P}\omega^\lambda(f)\,\tau' = \omega^\lambda \mathrm{tr}^P(f).\end{aligned}$$

Thus $\mathrm{tr}^P(f)$ is isobaric of weight λ. A similar calculation gives $\mathrm{wt}(N) = \mathrm{wt}(a_3) = 3$. □

Let Q denote the subgroup generated by the transpose of σ, i.e., the lower triangular Sylow p-subgroup, and define

$$\eta := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Lemma 2.2. *$Q \cup \{\eta\}$ is a set of coset representatives for B in $SL_2(\mathbb{F}_p)$.*

Proof. Since the index of B in $SL_2(\mathbb{F}_p)$ is $p+1$, we have the right number of elements. To show that the cosets $(\sigma^T)^n B$ are distinct for $n = 1, \ldots, p$, it is sufficient to show that $(\sigma^T)^n B \neq B$ for $n < p$; this is clear. To show that $\eta B \neq (\sigma^T)^n B$, it is sufficient to show that $\eta^{-1}(\sigma^T)^n \notin B$; this is a straight forward calculation. □

Lemma 2.3. *$Na_0 = -a_3 \prod_{\tau\in Q}(a_0)\tau$.*

Proof. Consider the orbits

$$a_3P = \{a_3 + 3sa_2 + 3s^2a_1 + s^3a_0 \mid s \in \mathbb{F}_p\}$$

and

$$a_0Q = \{s^3a_3 + 3s^2a_2 + 3sa_1 + a_0 \mid s \in \mathbb{F}_p\}.$$

Thus

$$\begin{aligned} Na_0 &= a_0 \prod_{s\in\mathbb{F}_p}(a_3 + 3sa_2 + 3s^2a_1 + s^3a_0) = a_0a_3 \prod_{s\in\mathbb{F}_p^*}(a_3 + 3sa_2 + 3s^2a_1 + s^3a_0) \\ &= a_0a_3 \prod_{s\in\mathbb{F}_p^*} s^3\left(\left(s^{-1}\right)^3 a_3 + 3\left(s^{-1}\right)^2 a_2 + 3s^{-1}a_1 + a_0\right) \\ &= a_3\left(\prod_{s\in\mathbb{F}_p^*} s^3\right)\prod_{\tau\in Q}(a_o)\,\tau = -a_3\prod_{\tau\in Q}(a_o)\,\tau \end{aligned}$$

□

Since $\{\sigma, \sigma^T\}$ generates $SL_2(\mathbb{F}_p)$, any polynomial which is both P-invariant and Q-invariant is $SL_2(\mathbb{F}_p)$-invariant, giving the following corollary (see also Lecture III §9 of [6]).

Corollary 2.4. *Na_0 is $SL_2(\mathbb{F}_p)$-invariant.*

Theorem 2.5. *Suppose f is an isobaric P-invariant with* $\mathrm{wt}(N\cdot f)=0$*. Then a_0 divides $\mathrm{tr}^G_B(N\cdot f)-N\cdot f$ and, if a_0 does not divide f, the lead terms of $\mathrm{tr}^G_B(N\cdot f)$ and $N\cdot f$ are equal.*

Proof. Using the fact that Na_0 is $SL_2(\mathbb{F}_p)$-invariant we see that

$$\begin{aligned}\mathrm{tr}^G_B(N\cdot f)-N\cdot f &= Na_0\left(\mathrm{tr}^G_B\left(fa_0^{-1}\right)\right)-N\cdot f\\ &= N\left(a_0\mathrm{tr}^G_B\left(fa_0^{-1}\right)-f\right).\end{aligned}$$

Observe that $(a_0)\eta=-a_3$. Thus, using the coset representatives from Lemma 2.2, we have

$$a_0\mathrm{tr}^G_B\left(fa_0^{-1}\right)-f=a_0\left(\sum_{\tau\in Q\setminus\{1\}}\frac{(f)\tau}{(a_0)\tau}-\frac{(f)\,\eta}{a_3}\right).$$

From Lemma 2.3, N is a least common multiple of $\{a_3\}\cup\{(a_0)\tau\mid\tau\in Q\setminus\{1\}\}$. Taking N as the common denominator in the above sum gives

$$a_0\mathrm{tr}^G_B(fa_0^{-1})-f=\frac{a_0J}{N}$$

for some polynomial J. Therefore $\mathrm{tr}^G_B(N\cdot f)-N\cdot f=a_0J$. If a_0 does not divide f, then the lead term of $N\cdot f$ is not divisible by a_0 and is also the lead term of $\mathrm{tr}^G_B(N\cdot f)$. □

We use LM to denote lead monomial and LT to denote lead term. It is clear that $\mathrm{LM}(N)=a_3^p$. In the following lemmas, we use the lead monomial calculations from [12]. Note that although the basis used in [12] is different from the one used here, the change of basis is upper triangular and so the lead monomial calculations still apply.

Lemma 2.6. *For $m=2+\lfloor 3j/(p-1)\rfloor$,*

$$\mathrm{LM}\left(\mathrm{tr}^G_B\left(N^j\mathrm{tr}^P\left(a_2^{(m-1)(p-1)-3j}a_3^{p-1}\right)\right)\right)=a_3^{pj}a_2^{m(p-1)-3j}=:\gamma_j.$$

Proof. We know from [12, 3.3] that $\mathrm{tr}^P(a_2^ba_3^{p-1})$ has lead monomial a_2^{b+p-1} if $1\le b\le p-1$. Since $m=2+\lfloor 3j/(p-1)\rfloor$, we have $3j/(p-1)-1<m-2\le 3j/(p-1)$, which simplifies to $0<(m-1)(p-1)-3j\le p-1$. The result then follows from Lemma 2.1 and Theorem 2.5. □

Lemma 2.7. *For $0\le j\le (p-1)/2$,*

$$\mathrm{LM}\left(\mathrm{tr}^G_B\left(N^j\mathrm{tr}^P\left(a_3^{p-1-j}\right)\right)\right)=a_3^{pj}a_2^{p-1-2j}a_1^j=:\beta_j.$$

Proof. From [12, 3.2], $\mathrm{tr}^P(a_3^b)$ has lead monomial $a_2^{2b-(p-1)}a_1^{p-1-b}$ if $(p-1)/2\le b\le p-1$. Simplifying $(p-1)/2\le p-1-j\le p-1$ gives $0\le j\le (p-1)/2$. The result then follows from Lemma 2.1 and Theorem 2.5. □

Lemma 2.8. *For $m=2+\lfloor 3j/(p-1)\rfloor$ and $j\ne\lceil (m-2)(p-1)/3\rceil$,*

$$\mathrm{LM}\left(\mathrm{tr}^G_B\left(N^j\mathrm{tr}^P\left(a_3^{p-2}a_2^{(m-1)(p-1)+3-3j}\right)\right)\right)=a_3^{pj}a_2^{m(p-1)+1-3j}a_1=:\Delta_j.$$

Proof. Using [12, 3.4], $\mathrm{LM}(\mathrm{tr}^P(a_3^{p-2}a_2^b)) = a_2^{b+p-3}a_1$ for $2 \le b \le p-1$. As in the proof of Lemma 2.6, we have $0 < (m-1)(p-1) - 3j \le p-1$. Therefore $3 < (m-1)(p-1) + 3 - 3j \le p+2$. Thus the lead monomial calculation is valid as long as $(m-1)(p-1)+3-3j \notin \{p, p+1, p+2\}$. This simplifies to $j \notin \{(m-2)(p-1)/3 + \varepsilon/3 \mid \varepsilon \in \{0,1,2\}\}$, i.e., $j \neq \lceil (m-2)(p-1)/3 \rceil$. The result then follows from Lemma 2.1 and Theorem 2.5. □

Lemma 2.9. *For $p \equiv_{(3)} -1$ and $j = (2p-1)/3, \ldots, p-2$,*

$$\mathrm{LM}\left(\mathrm{tr}_B^G\left(N^j \mathrm{tr}^P\left(a_3^{\frac{5p-7}{3}-j}a_2^2\right)\right)\right) = a_3^{pj}a_2^{\frac{7p-5}{3}-2j}a_1^{j-\frac{2p-4}{3}} =: \phi_j.$$

Proof. From [12, 3.5], $\mathrm{LM}(\mathrm{tr}^P(a_3^b a_2^2)) = a_2^{2b-p+3}a_1^{p-1-b}$ for $(p-2)/3 \le b \le p-1$. The inequalities $(p-2)/3 \le (5p-7)/3 - j \le p-1$ simplify to $(2p-4)/3 \le j \le (7p-5)/6 = p-1+(p+1)/6$. Thus the lead monomial calculation is valid for the given range of j. The result then follows from Lemma 2.1 and Theorem 2.5. □

Define $\xi = 3a_2^2 - 4a_3a_1$.

Lemma 2.10. $K = -\mathrm{tr}^P(a_3^{p-1}) - a_0^{p-1} \equiv_{(a_0)} (3\xi)^{\frac{p-1}{2}} + a_1^{p-1}$.

Proof. A simple calculation gives $\mathrm{tr}^P(a_1^{p-1}) = -a_0^{p-1}$ (or see [12, 3.2]). Since $\mathrm{wt}(a_0^{p-1}) = 0$ and the index of P in B is $p-1$, we have $\mathrm{tr}^B(a_1^{p-1}) = a_0^{p-1}$. Using the coset representatives from Lemma 2.2 gives

$$\begin{aligned}
-K &= \mathrm{tr}^G(a_1^{p-1}) = \mathrm{tr}_B^G(a_0^{p-1}) = ((a_0)\eta)^{p-1} + \mathrm{tr}^Q(a_0^{p-1}) = a_3^{p-1} + \mathrm{tr}^Q(a_0^{p-1}) \\
&= a_3^{p-1} + \sum_{s\in\mathbb{F}_p}(s^3a_3 + 3s^2a_2 + 3sa_1 + a_0)^{p-1} \\
&= a_3^{p-1} + a_0^{p-1} + \sum_{s\in\mathbb{F}_p^*}(s^3a_3 + 3s^2a_2 + 3sa_1 + a_0)^{p-1} \\
&= a_3^{p-1} + a_0^{p-1} + \sum_{s\in\mathbb{F}_p^*} s^{3(p-1)}(a_3 + 3s^{-1}a_2 + 3(s^{-1})^2a_1 + (s^{-1})^3a_0)^{p-1} \\
&= a_0^{p-1} + \sum_{t\in\mathbb{F}_p}(a_3 + 3ta_2 + 3t^2a_1 + t^3a_0)^{p-1} = a_0^{p-1} + \mathrm{tr}^P(a_3^{p-1}) \\
&\equiv_{(a_0)} \sum_{t\in\mathbb{F}_p}(a_3 + 3ta_2 + 3t^2a_1)^{p-1} \\
&\equiv_{(a_0)} \sum_{t\in\mathbb{F}_p}\sum_{a+b+c=p-1}\binom{p-1}{a,b,c}t^{b+2c}a_3^a(3a_2)^b(3a_1)^c.
\end{aligned}$$

It is well known that $\sum_{t\in\mathbb{F}_p} t^i$ is -1 if i is a positive multiple of $p-1$ and 0 otherwise. Thus, for a, b, c non-negative with $a+b+c = p-1$, we see that $\sum_{t\in\mathbb{F}_p} t^{b+2c}$ is non-zero only when $b+2c = p-1$ or $b+2c = 2(p-1)$. If $b+2c = 2(p-1)$ then $c = p-1$ and $a = b = 0$. If $b+2c = p-1$ then $a = c$.

Therefore

$$-K \equiv_{(a_0)} \binom{p-1}{0,0,p-1}(-1)(3a_1)^{p-1} - \sum_{c=0}^{\frac{p-1}{2}} \binom{p-1}{c,b,c}(3a_2)^{p-1-2c}(3a_1a_3)^c$$

$$-K \equiv_{(a_0)} -a_1^{p-1} - 3^{\frac{p-1}{2}} \sum_{c=0}^{\frac{p-1}{2}} \binom{p-1}{c,b,c}(3a_2^2)^{\frac{p-1}{2}-c}(a_1a_3)^c.$$

Simplifying binomial coefficients modulo p gives

$$\binom{p-1}{c,p-1-2c,c} = \binom{2c}{c} = (-4)^c\binom{\frac{p-1}{2}}{c}.$$

Thus

$$K \equiv_{(a_o)} a_1^{p-1} + 3^{\frac{p-1}{2}}(3a_2^2 - 4a_1a_3)^{\frac{p-1}{2}},$$

as required. ☐

A similar calculation using the identity

$$\binom{p-2}{a,p-3-2a,a+1} \equiv_{(p)} -2(a+1)\binom{2a+1}{a} \equiv_{(p)} -2(-4)^a\binom{\frac{p-3}{2}}{a}$$

gives the following lemma.

Lemma 2.11. $\mathrm{tr}^P(a_3^{p-2}) \equiv_{(a_0)} 6a_1(3\xi)^{\frac{p-3}{2}}$.

Theorem 2.12. *The set $\{D, K, Na_0, \delta\}$ is a homogeneous system of parameters.*

Proof. With out loss of generality, we may assume $\mathbb{F}$ is algebraically closed. We will show that the variety associated to $(D, K, Na_0, \delta)\mathbb{F}[V]$, say $\mathcal{V}$, consists of the zero vector.

Suppose $v \in \mathcal{V}$. Since $Na_0(v) = 0$, there exits $g \in SL_2(\mathbb{F}_p)$ such that $a_0g(v) = 0$. Replacing v with $g(v)$ if necessary, we may assume $a_0(v) = 0$. Note that $D \equiv_{(a_0)} a_1^2\xi$. From Lemma 2.10, $K \equiv_{(a_0)} (3\xi)^{\frac{p-1}{2}} + a_1^{p-1}$. Thus $a_1^2K - 3(3\xi)^{\frac{p-3}{2}}D \equiv_{(a_0)} a_1^{p+1}$. Therefore $a_1(v) = 0$. Since $\mathrm{LM}(K) = a_2^{p-1}$ in the grevlex order, we have $a_2(v) = 0$. Since $\mathrm{LM}(\delta) = a_3^{pc}$, we have $a_3(v) = 0$. Therefore v is the zero vector. ☐

If f and h are polynomials with $\mathrm{LT}(f) = \mathrm{LT}(h)$, we refer to $f - h$ as a tête-à-têtes (see [11] or [12]).

Theorem 2.13. *There is an infinite family of tête-à-têtes in $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$, defined as follows:*

$$\begin{aligned} h_1 &= K \cdot \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(Ne) - D \cdot \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(N\mathrm{tr}^P(a_3^{p-2})), \\ h_2 &= K \cdot h_1 - (3D)^{\frac{p-1}{2}} \cdot \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(Ne), \\ h_i &= K \cdot h_{i-1} - (3D)^{\frac{p-1}{2}} \cdot h_{i-2} \text{ for } i \geq 3, \end{aligned}$$

with $\mathrm{LT}(h_i) = 2a_3^pa_1^{p+2+(i-1)(p-1)}$ *for* $i \geq 1$.

Proof. The proof is by induction on i. Recall that $\mathrm{LT}(D) = 3a_1^2a_2^2$. From Lemma 2.10, $\mathrm{LT}(K) = a_2^{p-1}$. Using Theorem 2.5 and Lemma 2.11, we have $\mathrm{LT}(\mathrm{tr}_B^G(N\,\mathrm{tr}^P(a_3^{p-2})) = \frac{2}{3}a_1a_2^{p-3}a_3^p$ and $\mathrm{LT}(\mathrm{tr}_B^G(Ne)) = 2a_1^3a_3^p$. Thus h_1 is indeed a tête-à-tête. Since $\mathrm{LT}((3D)^{(p-1)/2}) = (a_1a_2)^{p-1}$, it is sufficient to prove $\mathrm{LT}(h_i) = 2a_3^pa_1^{p+2+(i-1)(p-1)}$ for $i \geq 1$.

Define

$$\begin{aligned} r_1 &= K \cdot e - D \cdot \mathrm{tr}^P(a_3^{p-2}), \\ r_2 &= K \cdot r_1 - (3D)^{\frac{p-1}{2}} \cdot e, \\ r_i &= K \cdot r_{i-1} - (3D)^{\frac{p-1}{2}} \cdot r_{i-2} \text{ for } i \geq 3. \end{aligned}$$

Since K and D are G-invariant, we have $h_i = \mathrm{tr}_B^G(Nr_i)$. Thus, using Theorem 2.5, it is sufficient to prove $\mathrm{LT}(r_i) = 2a_1^{p+2+(i-1)(p-1)}$ for $i \geq 1$.

Note that $e \equiv_{(a_0)} 2a_1^3$ and $D \equiv_{(a_0)} a_1^2\xi$. Thus, using Lemma 2.10 and Lemma 2.11,

$$r_1 \equiv_{(a_0)} ((3\xi)^{\frac{p-1}{2}} + a_1^{p-1}) \cdot 2a_1^3 - a_1^2\xi \cdot 2(3^{\frac{p-1}{2}})a_1\xi^{\frac{p-3}{2}} = 2a_1^{p+2}.$$

Similarly

$$r_2 \equiv_{(a_0)} ((3\xi)^{\frac{p-1}{2}} + a_1^{p-1}) \cdot 2a_1^{p+2} - (3a_1^2\xi)^{\frac{p-1}{2}} \cdot 2a_1^3 = 2a_1^{(p+2)+(p-1)}.$$

Using the induction hypothesis,

$$\begin{aligned} r_i &\equiv_{(a_0)} ((3\xi)^{\frac{p-1}{2}} + a_1^{p-1}) \cdot 2a_1^{p+2+(i-2)(p-1)} - (3a_1^2\xi)^{\frac{p-1}{2}} \cdot 2a_1^{p+2+(i-3)(p-1)} \\ &\equiv_{(a_0)} 2a_1^{p+2+(i-1)(p-1)}, \end{aligned}$$

as required. □

3. Generators and Hilbert series

This section is devoted to the proof of the main theorem.

Theorem 3.1. *For $p > 3$, $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ is generated by*

- *elements from the image of the transfer*
- *$D, K, L, \delta, Na_0, \tilde{e}$ and*
- *for $p \equiv -1$ mod 3, $\tilde{d}$.*

The generators from the image of the transfer fall into three families:

(1) *$tr^{SL_2(\mathbb{F}_p)}(N^ja_2^{(m-1)(p-1)-3j}a_3^{p-1})$ where*

$$j = \begin{cases} 1, \ldots, (p-4)/3 & \text{for } p \equiv 1 \text{ mod } 3 \\ 1, \ldots, p-2 & \text{for } p \equiv -1 \text{ mod } 3 \end{cases}$$

and $m = 2 + \lfloor 3j/(p-1) \rfloor$;

(2) $tr^{SL_2(\mathbb{F}_p)}(N^j a_3^{p-1-j})$ *where*

$$j = \begin{cases} 1,\ldots,(p-4)/3 & \text{for } p \equiv 1 \bmod 3 \\ 1,\ldots,(p-2)/3 & \text{for } p \equiv -1 \bmod 3; \end{cases}$$

(3) *and* $tr^{SL_2(\mathbb{F}_p)}(N^j a_3^{p-2} a_2^{(m-1)(p-1)+3-3j})$ *where*

$$j = \begin{cases} 2,\ldots,(p-4)/3 & \text{for } p \equiv 1 \bmod 3 \\ 2,\ldots,p-2 \text{ with } j \neq (p+1)/3, (2p-1)/3 & \text{for } p \equiv -1 \bmod 3 \end{cases}$$

and $m = 2 + \lfloor 3j/(p-1) \rfloor$.

For $p \equiv -1$ *mod 3, we have the further family of invariants:*

$$tr^{SL_2(\mathbb{F}_p)}(N^j a_3^{\frac{5p-7-3j}{3}} a_2^2), \quad j = \frac{2p-1}{3}, \ldots, p-2.$$

Let $\mathcal{C}$ denote the proposed generating set and let R denote the algebra generated by $\mathcal{C}$. Since the elements of $\mathcal{C}$ are homogeneous invariants, R is a graded subalgebra of $\mathbb{F}[V]^G$. Recall that the *Hilbert Series* of a graded vector space $M = \oplus_{\ell=0}^{\infty} M_\ell$ is the formal power series $HS(M,t) = \sum_{\ell=0}^{\infty} \dim(M_\ell) t^\ell$. Since R is a graded subalgebra of $\mathbb{F}[V]^G$, we have $HS(R,t) \leq HS(\mathbb{F}[V]^G, t)$. We prove the theorem by showing these series are equal.

Define $\mathcal{G} := \mathcal{C} \cup \{h_i, \forall i \geq 1\}$ and let $\mathrm{LT}(\mathcal{G})$ denote the subalgebra generated by the lead monomials of the elements of $\mathcal{G}$. In each of the two cases, $p \equiv 1$ mod 3 and $p \equiv -1$ mod 3, we choose a graded subspace Z of $\mathrm{LT}(\mathcal{G})$, giving a chain of inequalities:

$$HS(Z,t) \leq HS(LT(\mathcal{G}),t) \leq HS(LT(R),t) = HS(R,t) \leq HS(\mathbb{F}[V]^G, t).$$

We calculate $HS(Z,t)$ and compare with Hughes-Kemper [8] to show $HS(Z,t) = HS(\mathbb{F}[V]^G, t)$. This proves that $\mathcal{C}$ is a generating set and $\mathcal{G}$ is a SAGBI basis.

The invariants D, K, Na_0, and δ have lead monomials $LM(D) = a_2^2 a_1^2$, $LM(K) = a_2^{p-1}$, $LM(Na_0) = a_3^p a_0$ and $LM(\delta) = a_3^{pc}$, where $c = (p-1)/3$ if $p \equiv_{(3)} 1$ and $a = p-1$ if $p \equiv_{(3)} -1$. Define

$$A := \mathbb{F}[a_2^2 a_1^2, a_2^{p-1}, a_3^p a_0, a_3^{pc}],$$

the algebra generated by $LM(D), LM(K), LM(Na_0)$ and $LM(\delta)$. In each of the two cases we will define Z as an A - submodule of $\mathrm{LT}(\mathcal{G})$. For a monomial $a_3^{e_3} a_2^{e_2} a_1^{e_1} a_0^{e_0}$ we assign a *parity* $(e_2 \bmod 2, e_1 \bmod 2)$ and observe that the action of A preserves parity.

The $p \equiv 1$ mod 3 Case

Recall from Theorem 2.13 that the lead monomials of the tête-à-têtes h_i are $LM(h_i) = a_3^p a_1^{p+2+(i-1)(p-1)}$ for $i \geq 1$. By Lemma 2.5 the lead monomial of the invariant $\tilde{e} = \mathrm{tr}_B^{SL_2(\mathbb{F}_p)}(Ne)$ is equal to $a_3^p a_1^3$. Hence we have

$$n_i := a_3^p a_1^{3+i(p-1)} \text{ for } i \geq 0$$

as the lead monomials of $\tilde{e}$ and h_i. Denote

$$\alpha_{ij} := n_0^{j-1} n_i = a_3^{pj} a_1^{3j+(p-1)i}, \;\; 1 \leq j \leq (p-1)/3, \;\; i \geq 0$$

and

$$\epsilon_{ij} := LM(L)\alpha_{ij} = a_3^{pj} a_2^p a_1^{1+3j+(p-1)i}, \;\; 1 \leq j \leq (p-1)/3, \;\; i \geq 0.$$

Define Z to be the A - module generated by the monomials

$$\mathcal{B} := \{1, LM(L), \gamma_j, \beta_j, \Delta_j, \alpha_{ij}, \epsilon_{ij} \mid i \in \mathbb{N}\}.$$

where $1 \leq j \leq (p-1)/3$ for the α and ϵ families, $1 \leq j < (p-1)/3$ for the γ and β families, and $1 < j < (p-1)/3$ for the Δ family; see Lemma 2.6, Lemma 2.7 and Lemma 2.8 for the definition of γ_j, β_j and Δ_j, and compare with the range of j for the families of transfers in Theorem 3.1.

The action of $LM(Na_0)$ and $LM(\delta)$ on Z is essentially free: every monomial in Z with a factor of $a_0^{e_0}$ is divisible by $LM(Na_0)^{e_0}$ and the remaining power of a_3 determines the power of LM(δ). Let $\widetilde{Z}$ denote the span of the monomials in Z which are reduced with respect to LM(Na_0) and LM(δ). Then

$$HS(Z,t) = \frac{HS(\widetilde{Z},t)}{(1-t^{p+1})(1-t^{p(p-1)/3})}.$$

Define $\widetilde{Z}_j$ to be the span of the monomials in $\widetilde{Z}$ of the form $a_3^{pj} a_2^{e_2} a_1^{e_1}$. Then

$$\widetilde{Z} = \bigoplus_{j=0}^{(p-1)/3} \widetilde{Z}_j.$$

We proceed by computing $HS(\widetilde{Z}_j, t)$ for $j = 0, 1, \ldots, (p-1)/3$. For fixed j, we determine the monomials $a_3^{pj} a_2^x a_1^y \in \widetilde{Z}_j$. This set can be identified with a subset of the integral lattice in the xy-plane. Each element of $\mathcal{B}$ gives rise to a $\mathbb{F}[\mathrm{LM}(D), \mathrm{LM}(K)]$-submodule corresponding to a cone in the xy-plane. The monomials in $\widetilde{Z}_j$ correspond to the union of these cones. The cones corresponding to elements of $\mathcal{B}$ of different parity are disjoint.

For $j = 0$, the only elements of $\mathcal{B}$ are 1 and $LM(L) = a_2^p a_1$, of parity $(0,0)$ and $(1,1)$ respectively. Thus

$$HS(\widetilde{Z}_0, t) = \frac{1 + t^{p+1}}{(1-t^4)(1-t^{p-1})}.$$

For $j = (p-1)/3 = c$, the elements of $\mathcal{B}$ fall into two families:

- $\alpha_{ic} = a_3^{pc} a_1^{p-1+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(0,0)$;
- $\epsilon_{ic} = a_3^{pc} a_2^p a_1^{p+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(1,1)$.

For parity $(0,0)$: Note that $\alpha_{0c}\,\mathrm{LM}(K) = \mathrm{LM}(\delta)\,\mathrm{LM}(D)^{\frac{p-1}{2}} \notin \widetilde{Z}$. Furthermore, for $i>0$, we have $\alpha_{ic}\,\mathrm{LM}(K) = \alpha_{i-1,c}\,\mathrm{LM}(D)^{\frac{p-1}{2}}$. Thus it is sufficient to count the monomials $\alpha_{ic}\,\mathrm{LM}(D)^\ell$ with $i,\ell\in\mathbb{N}$.

For parity $(1,1)$: Note that $\epsilon_{0c}\,\mathrm{LM}(K) = \mathrm{LM}(\delta)\,\mathrm{LM}(L)\,\mathrm{LM}(D)^{\frac{p-1}{2}} \notin \widetilde{Z}$. Furthermore, for $i>0$, we have $\epsilon_{ic}\,\mathrm{LM}(K) = \epsilon_{i-1,c}\,\mathrm{LM}(D)^{\frac{p-1}{2}}$. Thus it is sufficient to count the monomials $\epsilon_{ic}\,\mathrm{LM}(D)^\ell$ with $i,\ell\in\mathbb{N}$.

Counting monomials and identifying the appropriate geometric series gives

$$HS(\widetilde{Z}_c,t) = \frac{t^{pc}(t^{p-1}+t^{2p})}{(1-t^4)(1-t^{p-1})} = \frac{t^{pc+p-1}(1+t^{p+1})}{(1-t^4)(1-t^{p-1})}.$$

In the case $j=1$, we have the following elements of $\mathcal{B}$:

- $\alpha_{i1} = a_3^p a_1^{3+i(p-1)}$ for $i\in\mathbb{N}$, with parity $(0,1)$;
- $\beta_1 = a_3^p a_2^{p-3} a_1$, with parity $(0,1)$;
- $\gamma_1 = a_3^p a_2^{2p-5}$, with parity $(1,0)$;
- $\epsilon_{i1} = a_3^p a_2^p a_1^{4+i(p-1)}$ for $i\in\mathbb{N}$, with parity $(1,0)$.

For Parity $(0,1)$: Since $\alpha_{01}\,\mathrm{LM}(K) = \beta_1\,\mathrm{LM}(D)$ and $\alpha_{i1}\,\mathrm{LM}(K) = \alpha_{i-1,1}\,\mathrm{LM}(D)^{\frac{p-1}{2}}$, for $i>0$, it is sufficient to count the monomials $\alpha_{i1}\,\mathrm{LM}(D)^\ell$ and $\beta_1\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

For Parity $(1,0)$: Since $\epsilon_{01}\,\mathrm{LM}(K) = \gamma_1\,\mathrm{LM}(D)$ and $\epsilon_{i1}\,\mathrm{LM}(K) = \epsilon_{i-1,1}\,\mathrm{LM}(D)^{\frac{p-1}{2}}$, for $i>0$, it is sufficient to count the monomials $\epsilon_{i1}\,\mathrm{LM}(D)^\ell$ and $\gamma_1\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives

$$HS(\widetilde{Z}_1,t) = \frac{t^p(t^3+t^{p-2}+t^{p+4}+t^{2p-5})}{(1-t^4)(1-t^{p-1})}.$$

We now consider the case where $j=2k$ is even and $2\le j<\frac{p-1}{3}$. The relevant monomials are:

- $\alpha_{ij} = a_3^{pj} a_1^{3j+i(p-1)}$ for $i\in\mathbb{N}$, with parity $(0,0)$;
- $\beta_j = a_3^{pj} a_2^{p-1-2j} a_1^j$, with parity $(0,0)$;
- $\gamma_j = a_3^{pj} a_2^{2p-2-3j}$, with parity $(0,0)$;
- $\Delta_j = a_3^{pj} a_2^{2p-1-3j} a_1$, with parity $(1,1)$;
- $\epsilon_{ij} = a_3^{pj} a_2^p a_1^{3j+1+i(p-1)}$ for $i\in\mathbb{N}$, with parity $(1,1)$.

For parity $(0,0)$: Observe that $\beta_j\,\mathrm{LM}(K) = \gamma_j\,\mathrm{LM}(D)^k$, $\alpha_{0j}\,\mathrm{LM}(K) = \beta_j\,\mathrm{LM}(D)^j$ and $\alpha_{ij}\,\mathrm{LM}(K) = \alpha_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i>0$. Thus it is sufficient to count the monomials $\alpha_{ij}\,\mathrm{LM}(D)^\ell$, $\beta_j\,\mathrm{LM}(D)^\ell$ and $\gamma_j\,\mathrm{LM}(D)^\ell\,\mathrm{LM}(K)^i$, for $i,\ell\in\mathbb{N}$.

For parity $(1,1)$: Since $\epsilon_{0j}\,\mathrm{LM}(K) = \Delta_j\,\mathrm{LM}(D)^{3k}$ and $\epsilon_{ij}\,\mathrm{LM}(K) = \epsilon_{i-1,j}\,\mathrm{LM}(D)^{\frac{p-1}{2}}$ for $i>0$, it is sufficient to count the monomials $\epsilon_{ij}\,\mathrm{LM}(D)^\ell$ and $\Delta_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives

$$HS(\widetilde{Z}_{2k},t) = t^{2kp}\left(\frac{t^{6k}+t^{2p-2-6k}+t^{p+6k+1}+t^{2p-6k}}{(1-t^4)(1-t^{p-1})} + \frac{t^{p-1-2k}}{1-t^4}\right)$$

for $k = 1, \ldots, \frac{p-7}{6}$.

For $j = 2k+1$ odd with $1 < j < (p-1)/3$, the elements of $\mathcal{B}$ are:

- $\alpha_{ij} = a_3^{pj} a_1^{3j+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(0,1)$;
- $\beta_j = a_3^{pj} a_2^{p-1-2j} a_1^j$ with parity $(0,1)$;
- $\Delta_j = a_3^{pj} a_2^{2p-1-3j} a_1$ with parity $(0,1)$;
- $\gamma_j = a_3^{pj} a_2^{2p-2-3j}$ with parity $(1,0)$;
- $\epsilon_{ij} = a_3^{pj} a_2^p a_1^{3j+1+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(1,0)$.

For parity $(0,1)$: Observe that $\beta_j \operatorname{LM}(K) = \Delta_j \operatorname{LM}(D)^k$, $\alpha_{0j} \operatorname{LM}(K) = \beta_j \operatorname{LM}(D)^j$ and $\alpha_{ij} \operatorname{LM}(K) = \alpha_{i-1,j} \operatorname{LM}(D)^{(p-1)/2}$ for $i > 0$. Thus it is sufficient to count the monomials $\alpha_{ij} \operatorname{LM}(D)^\ell$, $\beta_j \operatorname{LM}(D)^\ell$ and $\Delta_j \operatorname{LM}(D)^\ell \operatorname{LM}(K)^i$, for $i, \ell \in \mathbb{N}$.

For parity $(1,0)$: Since $\epsilon_{0j} \operatorname{LM}(K) = \gamma_j \operatorname{LM}(D)^{3k}$ and $\epsilon_{ij} \operatorname{LM}(K) = \epsilon_{i-1,j} \operatorname{LM}(D)^{\frac{p-1}{2}}$ for $i > 0$, it is sufficient to count the monomials $\epsilon_{ij} \operatorname{LM}(D)^\ell$ and $\gamma_j \operatorname{LM}(K)^i \operatorname{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives

$$HS(\widetilde{Z}_{2k+1}, t) = t^{(2k+1)p} \left(\frac{t^{6k+3} + t^{2p-2-6k-3} + t^{p+6k+4} + t^{2p-6k-3}}{(1-t^4)(1-t^{p-1})} + \frac{t^{p-2-2k}}{1-t^4} \right)$$

for $k = 1, \ldots, \frac{p-7}{6}$.

The even and odd formulae can be put in a common form: for $1 < j < (p-1)/3$,

$$HS(\widetilde{Z}_j, t) = \frac{t^{jp} \left(t^{3j} + t^{2p-2-3j} + t^{p+1+3j} + t^{2p-3j} + t^{p-1-j}(1 - t^{p-1}) \right)}{(1-t^4)(1-t^{p-1})}.$$

Summing over j and simplifying gives

$$HS(Z, t) = \frac{Numer(t)}{Denom(t)}$$

where

$$\begin{aligned} Numer(t) &= (1 + t^{p+1} + t^{p+3} + t^{2p-2} + t^{2p+4} + t^{3p-5} + t^{p-1}(t^{2p-2} - t^{(p-1)(p-1)/3}) \\ &+ t^{\frac{p(p-1)}{3}+p-1} + t^{\frac{p(p-1)}{3}+2p})(1 - t^{p-3})(1 - t^{p+3}) \\ &+ (t^{2p-2} + t^{2p})(t^{2p-6} - t^{(p-3)(p-1)/3})(1 - t^{p+3}) \\ &+ (1 + t^{p+1})(t^{2p+6} - t^{(p+3)(p-1)/3})(1 - t^{p-3}) \end{aligned}$$

and

$$Denom(t) = (1-t^4)(1-t^{p-3})(1-t^{p-1})(1-t^{p+1})(1-t^{p+3})(1-t^{\frac{p(p-1)}{3}}).$$

This agrees with the calculation of $HS(\mathbb{F}[V]^G, t)$ by Hughes-Kemper [8, 2.7(d)].

The $p \equiv -1$ mod 3 Case

In this case the lead monomial of $\delta = \mathrm{tr}_B^G(N^c)$ is $a_3^{p(p-1)}$ and the generators of Z will be monomials divisible by a_3^{pj} for $j \leq p-1$. Using Lemma 2.5 the lead monomial of $\tilde{d}$ is $a_3^{(p+1)/3}a_1^2$. As in the proof of the $p \equiv_{(3)} 1$ case, we denote the lead monomials of $\tilde{e}$ and h_i by $n_i = a_3^p a_1^{3+i(p-1)}$ for $i \geq 0$. Define $s := \lfloor 3j/(p-1) \rfloor$,

$$\alpha_{ij} := \mathrm{LM}(\tilde{d})^s n_i n_0^{j-1-s(p-1)/3} = a_3^{pj} a_1^{3j+(p-1)(i-s)}, \;\; 1 \leq j \leq (p-1), \;\; i \in \mathbb{N}$$

and

$$\epsilon_{ij} := \mathrm{LM}(L)\alpha_{ij} = a_3^{pj} a_2^p a_1^{3j+(p-1)(i-s)+1}, \;\; 1 \leq j \leq (p-1), \;\; i \in \mathbb{N}.$$

Further, we assign the following notation:

$$\begin{aligned}
\lambda &:= \mathrm{LM}(\tilde{d})\gamma_{\frac{p-2}{3}} = a_3^{p\frac{2p-1}{3}} a_2^p a_1^2, \\
\mu &:= \beta_1 \cdot \gamma_{\frac{p-2}{3}} = a_3^{p\frac{p+1}{3}} a_2^{2p-3} a_1, \\
\eta_j &:= \mathrm{LM}(\tilde{d})\beta_{j-(p+1)/3} = a_3^{pj} a_2^{\frac{5p-1}{3}-2j} a_1^{j-\frac{p-5}{3}} \quad \text{for } \frac{p+4}{3} \leq j \leq \frac{2p-1}{3}.
\end{aligned}$$

Define Z to be the A – module generated by

$$\mathcal{B} := \{1, LM(L), \alpha_{i,j}, \epsilon_{i,j}, \gamma_j, \beta_j, \Delta_j, \phi_j, \lambda, \mu, \eta_j \mid i \in \mathbb{N}\}.$$

where the ranges in j are given above or in the statement of Theorem 3.1

As in the $p \equiv_{(3)} 1$ case, the action of $\mathrm{LM}(Na_0)$ and $\mathrm{LM}(\delta)$ on Z is essentially free. Let $\widetilde{Z}$ denote the span of the monomials of Z which are reduced with respect to $\mathrm{LM}(Na_0)$ and $\mathrm{LM}(\delta)$. Then

$$HS(Z,t) = \frac{HS(\widetilde{Z},t)}{(1-t^{p+1})(1-t^{p(p-1)})}.$$

Define $\widetilde{Z}_j$ to be the span of the monomials in $\widetilde{Z}$ of the form $a_3^{pj}a_2^x a_1^y$. Then

$$\widetilde{Z} = \bigoplus_{j=0}^{p-1} \widetilde{Z}_j.$$

The calculation of $HS(\widetilde{Z}_j,t)$ for $j < (p-1)/3$ is precisely as in the $p \equiv_{(3)} 1$ case.

For $j = \frac{p+1}{3}$ the elements of $\mathcal{B}$ are:

- $\alpha_{i,\frac{p+1}{3}} = a_3^{p\frac{p+1}{3}} a_1^{2+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(0,0)$;

- $\gamma_{\frac{p+1}{3}} = a_3^{p\frac{p+1}{3}} a_2^{2p-4}$ with parity $(0,0)$;
- $\epsilon_{i,\frac{p+1}{3}} = a_3^{p\frac{p+1}{3}} a_2^p a_1^{3+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(1,1)$;
- $\mu = a_3^{p\frac{p+1}{3}} a_2^{2p-3} a_1$ with parity $(1,1)$.

For parity $(0,0)$: Observe that $\mathrm{LM}(D)\gamma_{\frac{p+1}{3}} = \mathrm{LM}(K)^2\alpha_{0,\frac{p+1}{3}}$ and $\alpha_{ij}\,\mathrm{LM}(K) = \alpha_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i > 0$. Thus it is sufficient to count the monomials $\alpha_{i+1,(p+1)/3}\,\mathrm{LM}(D)^\ell$, $\alpha_{0,(p+1)/3}\,\mathrm{LM}(D)^\ell\,\mathrm{LM}(K)^i$, and $\gamma_{(p+1)/3}\,\mathrm{LM}(K)^i$ for $i, \ell \in \mathbb{N}$.

For parity $(1,1)$: Observe that $\mathrm{LM}(D)\mu = \mathrm{LM}(K)\epsilon_{0,\frac{p+1}{3}}$ and $\epsilon_{ij}\,\mathrm{LM}(K) = \epsilon_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i > 0$. Thus it is sufficient to count the monomials $\mu\,\mathrm{LM}(K)^i$ and $\epsilon_{i,(p+1)/3}\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives

$$HS\left(\widetilde{Z}_{\frac{p+1}{3}}, t\right) = t^{p(p+1)/3}\left(\frac{t^2 + t^{p+1} + t^{p+3} + t^{2p-2}}{(1-t^4)(1-t^{p-1})} + \frac{t^{2p-4}}{1-t^{p-1}}\right).$$

We now consider the range $\frac{p+4}{3} \leq j \leq \frac{2p-4}{3}$. The following table indicates the monomials and their respective parities:

Monomial		Parity j even	Parity j odd
$\alpha_{i,j}$	$a_3^{pj} a_1^{3j-p+1+i(p-1)}$, $i \in \mathbb{N}$	(0,0)	(0,1)
η_j	$a_3^{pj} a_2^{\frac{5p-1-6j}{3}} a_1^{\frac{3j-p+5}{3}}$	(0,0)	(0,1)
γ_j	$a_3^{pj} a_2^{3p-3-3j}$	(0,0)	(1,0)
Δ_j	$a_3^{pj} a_2^{3p-2-3j} a_1$	(1,1)	(0,1)
$\epsilon_{i,j}$	$a_3^{pj} a_2^p a_1^{3j-p+2+i(p-1)}$, $i \in \mathbb{N}$	(1,1)	(1,0)

For j even, parity $(0,0)$: We have $\eta_j\,\mathrm{LM}(K) = \gamma_j\,\mathrm{LM}(D)^{(3j-p+5)/6}$, $\alpha_{0j}\,\mathrm{LM}(K) = \eta_j\,\mathrm{LM}(D)^{j-(p+1)/3}$ and $\alpha_{ij}\,\mathrm{LM}(K) = \alpha_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i > 0$. Thus we need to count $\alpha_{ij}\,\mathrm{LM}(D)^\ell$, $\eta_j\,\mathrm{LM}(D)^\ell$ and $\gamma_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

For j even, parity $(1,1)$: $\epsilon_{ij}\,\mathrm{LM}(K) = \epsilon_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ and $\epsilon_{0j}\,\mathrm{LM}(K) = \Delta_j\,\mathrm{LM}(D)^{(3j-p+1)/2}$. Thus we need to count $\epsilon_{ij}\,\mathrm{LM}(D)^\ell$ and $\Delta_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives:

$$HS(\widetilde{Z}_j, t) = t^{jp}\left(\frac{t^{3j+2} + t^{3p-3-3j} + t^{3p-1-3j} + t^{3j-p+1}}{(1-t^4)(1-t^{p-1})} + \frac{t^{4(p+1)/3-j}}{1-t^4}\right).$$

For j odd, the calculations are analogous with the roles of γ_j and Δ_j reversed. The contribution to $HS(\widetilde{Z}, t)$ is the same for both j even and j odd. Thus for $(p+1)/3 < j < (2p-1)/3$ we have:

$$HS(\widetilde{Z}_j, t) = t^{jp}\left(\frac{t^{3j+2} + t^{3p-3-3j} + t^{3p-1-3j} + t^{3j-p+1} + t^{4(p+1)/3-j}(1-t^{p-1})}{(1-t^4)(1-t^{p-1})}\right).$$

For $j = \frac{2p-1}{3}$ the monomials to consider are:

- $\alpha_{i,\frac{2p-1}{3}} = a_3^{p\frac{2p-1}{3}} a_1^{p+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(0,1)$;
- $\phi_{\frac{2p-1}{3}} = a_3^{p\frac{2p-1}{3}} a_2^{p-1} a_1$ with parity $(0,1)$;
- $\eta_{\frac{2p-1}{3}} = a_3^{p\frac{2p-1}{3}} a_2^{\frac{p+1}{3}} a_1^{\frac{p+4}{3}}$ with parity $(0,1)$;
- $\gamma_{\frac{2p-1}{3}} = a_3^{p\frac{2p-1}{3}} a_2^{2p-3}$ with parity $(1,0)$;
- $\epsilon_{i,\frac{2p-1}{3}} = a_3^{p\frac{2p-1}{3}} a_2^p a_1^{p+1+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(1,0)$;
- $\lambda = a_3^{p\frac{p+1}{3}} a_2^p a_1^2$ with parity $(1,0)$.

For parity $(0,1)$: $\alpha_{ij}\,\mathrm{LM}(K) = \alpha_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i > 0$, $\alpha_{0j}\,\mathrm{LM}(K) = \eta_j\,\mathrm{LM}(D)^{(p-2)/3}$ and $\eta_j\,\mathrm{LM}(K) = \phi_j\,\mathrm{LM}(D)^{(p+1)/6}$. Thus we need to count $\alpha_{ij}\,\mathrm{LM}(D)^\ell$, $\eta_j\,\mathrm{LM}(D)^\ell$ and $\phi_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

For parity $(1,0)$: $\epsilon_{ij}\,\mathrm{LM}(K) = \epsilon_{i-1,j}\,\mathrm{LM}(D)$ for $i > 0$, $\epsilon_{0j}\,\mathrm{LM}(K) = \lambda\,\mathrm{LM}(D)^{(p-1)/2}$ and $\lambda\,\mathrm{LM}(K) = \gamma_j\,\mathrm{LM}(D)$. Thus we need to count $\epsilon_{ij}\,\mathrm{LM}(D)^\ell$, $\lambda\,\mathrm{LM}(D)^\ell$ and $\gamma_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives:

$$HS\left(\widetilde{Z}_{\frac{2p-1}{3}}, t\right) = t^{p(2p-1)/3}\left(\frac{2t^p + t^{2p-3} + t^{2p+1}}{(1-t^4)(1-t^{p-1})} + \frac{t^{p+2} + t^{(2p+5)/3}}{1-t^4}\right). \tag{3.1}$$

We now consider the range $\frac{2p+2}{3} \le j \le p-2$. The following table gives the relevant monomials and their parities:

Monomial		Parity j even	Parity j odd
$\alpha_{i,j}$	$a_3^{pj} a_1^{3j-2p+2+i(p-1)}$, $i \in \mathbb{N}$	(0,0)	(0,1)
ϕ_j	$a_3^{pj} a_2^{\frac{7p-5-6j}{3}} a_1^{\frac{3j-2p+4}{3}}$	(0,0)	(0,1)
γ_j	$a_3^{pj} a_2^{4p-4-3j}$	(0,0)	(1,0)
Δ_j	$a_3^{pj} a_2^{4p-3-3j} a_1$	(1,1)	(0,1)
$\epsilon_{i,j}$	$a_3^{pj} a_2^p a_1^{3j-2p+3+i(p-1)}$, $i \in \mathbb{N}$	(1,1)	(1,0)

For j even, parity $(0,0)$: We have $\phi_j\,\mathrm{LM}(K) = \gamma_j\,\mathrm{LM}(D)^{(3j-2p+4)/6}$, $\alpha_{0j}\,\mathrm{LM}(K) = \phi_j\,\mathrm{LM}(D)^{j-(2p-1)/3}$ and $\alpha_{ij}\,\mathrm{LM}(K) = \alpha_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ for $i > 0$. Thus we need to count $\alpha_{ij}\,\mathrm{LM}(D)^\ell$, $\phi_j\,\mathrm{LM}(D)^\ell$ and $\gamma_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

For j even, parity $(1,1)$: $\epsilon_{ij}\,\mathrm{LM}(K) = \epsilon_{i-1,j}\,\mathrm{LM}(D)^{(p-1)/2}$ and $\epsilon_{0j}\,\mathrm{LM}(K) = \Delta_j\,\mathrm{LM}(D)^{(3j-2p+2)/2}$. Thus we need to count $\epsilon_{ij}\,\mathrm{LM}(D)^\ell$ and $\Delta_j\,\mathrm{LM}(K)^i\,\mathrm{LM}(D)^\ell$.

Counting monomials and identifying the appropriate geometric series gives:

$$HS(\widetilde{Z}_j, t) = t^{jp}\left(\frac{t^{3j-2p+2} + t^{4p-4-3j} + t^{4p-4-3j} + t^{3j-p+3}}{(1-t^4)(1-t^{p-1})} + \frac{t^{5(p+1)/3-j-2}}{1-t^4}\right).$$

For j odd, the calculations are analogous with the roles of γ_j and Δ_j reversed. The contribution to $HS(\widetilde{Z},t)$ is the same for both j even and j odd. Thus for $(2p-1)/3 < j < p-1$ we have:

$$HS(\widetilde{Z}_j,t) = t^{jp}\left(\frac{t^{3j+2-2p}+t^{4p-4-3j}+t^{4p-2-3j}+t^{3j-p+3}+t^{5(p+1)/3-j-2}(1-t^{p-1})}{(1-t^4)(1-t^{p-1})}\right).$$

Finally, we consider the case $j = p-1$. The only monomials we have here are

- $\alpha_{i,p-1} = a_3^{p(p-1)} a_1^{p-1+i(p-1)}$ for $i \in \mathbb{N}$, with parity $(0,0)$;
- $\epsilon_{i,p-1} = a_3^{p(p-1)} a_2^p a_1^{p+i(p-1)}$ for $i \in \mathbb{N}$, with $(1,1)$.

Note that $\alpha_{0,p-1}\operatorname{LM}(K) = \operatorname{LM}(\delta)\operatorname{LM}(D)^{(p-1)/2} \notin \widetilde{Z}$ and, for $i > 0$, we have $\alpha_{i,p-1}\operatorname{LM}(K) = \alpha_{i-1,p-1}\operatorname{LM}(D)^{(p-1)/2}$. Similarly,

$$\epsilon_{0,p-1}\operatorname{LM}(K) = \operatorname{LM}(\delta)\operatorname{LM}(L)\operatorname{LM}(D)^{(p-1)/2} \notin \widetilde{Z}$$

and, for $i > 0$, $\epsilon_{i,p-1}\operatorname{LM}(K) = \epsilon_{i-1,p-1}\operatorname{LM}(D)^{(p-1)/2}$. Thus it is sufficient to count the monomials $\alpha_{i,p-1}\operatorname{LM}(D)^{\ell}$ and $\epsilon_{i,p-1}\operatorname{LM}(D)^{\ell}$ with $i,\ell \in \mathbb{N}$. Counting monomials and identifying the appropriate geometric series gives

$$HS(\widetilde{Z}_{p-1},t) = \frac{t^{p(p-1)}(t^{p-1}+t^{2p})}{(1-t^4)(1-t^{p-1})}.$$

Summing over j and simplifying gives

$$HS(Z,t) = \frac{Numer(t)}{Denom(t)}$$

where

$$\begin{aligned}
Numer(t) &= \chi_1(t)(1-t^{p-3})(1-t^{p+3}) + \chi_2(t)(1-t^{p+3}) + \chi_3(t)(1-t^{p-3}),\\
\chi_1(t) &= 1 + t^{p+1} + t^{p(p+1)} + t^{(p+1)(p-1)} + t^p(t^3 + t^{p-2} + t^{p+4} + t^{2p-5})\\
&+ t^{p(p+1)/3}(t^2 + t^{p+1} + t^{p+3} + t^{2p-4} + t^{2p-2} - t^{2p})\\
&+ t^{p(2p-1)/3}(2t^p + t^{p+2} + t^{2p-3} + t^{(2p+5)/3}(1-t^{p-1}))\\
&+ t^{3(p-1)}(1-t^{(p-1)(p-5)/3})(1+t^{p(p-2)/3+3}+t^{2p(p-2)/3+2}),\\
\chi_2(t) &= t^{4(p-2)}(1-t^{(p-3)(p-5)/3})(1+t^2)(1+t^{p(p-2)/3+1}+t^{2p(p-2)/3+2}),\\
\chi_3(t) &= t^{2p+6}(1-t^{(p+3)(p-5)/3})(1+t^{p+1})(1+t^{p(p-2)/3-1}+t^{2p(p-2)/3-2})\\
&\text{and}\\
Denom(t) &= (1-t^4)(1-t^{p-3})(1-t^{p-1})(1-t^{p+1})(1-t^{p+3})(1-t^{p(p-1)}).
\end{aligned}$$

This agrees with the calculation of $HS(\mathbb{F}[V]^G,t)$ by Hughes-Kemper [8, 2.7(d)].

4. Concluding Remarks

We do not claim that the generating sets given in Theorem 3.1 are minimal. However, for $p = 5$ and $p = 7$, MAGMA [4] calculations confirm that the given sets are minimal generating sets. Recall that the *Noether number* is the maximum degree of an element in a minimal homogeneous generating set. Thus the Noether number is 22 for $p = 5$ and 16 for $p = 7$. Examining the degrees of the polynomials occurring in Theorem 3.1 gives the following.

Corollary 4.1. *The Noether number of* $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ *is bounded above by*

- $p^2 - p + 4$ *if* $p \equiv_{(3)} -1$,
- $\frac{p^2-p+12}{3}$ *if* $p \equiv_{(3)} 1$.

It follows from the proof of Theorem 3.1 that $\mathcal{G}$ is a SAGBI basis for $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$. This means that the set $\mathrm{LM}(\mathcal{G})$ generates the lead term algebra of $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ and if $f \in \mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ then $\mathrm{LM}(f)$ can be written as a product of elements from $\mathrm{LM}(\mathcal{G})$.

Corollary 4.2. $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$ *does not have a finite SAGBI basis using the graded reverse lexicographical order with* $a_0 < a_1 < a_2 < a_3$.

Proof. Observe that if $a_1^j \in LM(\mathcal{G})$ then $j = 0$ and if $m \in LM(\mathcal{G})$ with a_3 dividing m, then a_3^p divides m. Thus $LM(h_i) = a_3^p a_1^{p+2+(i-1)(p-1)}$ is indecomposable in the lead term algebra of $\mathbb{F}[V]^{SL_2(\mathbb{F}_p)}$. □

References

[1] W. W. Adams and P. Loustaunau *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics vol. 3, The American Mathematical Society, 1994.

[2] J. L. Alperin, *Local Representation Theory*, Cambridge Studies in Advanced Mathematics vol. 11, Cambridge Univ. Press, 1986.

[3] D.J. Benson, *Polynomial Invariants of Finite Groups*, London Mathematical Society Lecture Note Series vol. 190, Cambridge Univ. Press, 1993.

[4] W. Bosma, J. J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. **24** (1997), 235–265.

[5] H. Derksen and G. Kemper, *Computational Invariant Theory*, Encyclopaedia of Math. Sci. **130**, Springer, 2002.

[6] L.E. Dickson, *On Invariants and the Theory of Numbers*, The Madison Colloquium (1913, Part 1) A.M.S., reprinted by Dover, 1966.

[7] A. Hobson, *On the invariants of the third symmetric power representation of* $SL_2(\mathbb{F}_p)$, PhD thesis, University of Kent, Canterbury, 2009.

[8] I.P. Hughes and G. Kemper, *Symmetric Powers of Modular Representations for Groups with a Sylow Subgroup of Prime Order*, Journal of Algebra **241** (2001), 759–788.

[9] D. Kapur and K. Madlener, *A completion procedure for computing a canonical basis of a k-subalgebra*, Proceedings of Computers and Mathematics **89** (1989), ed. E. Kaltofen and S. Watt, MIT, 1–11.

[10] M. D. Neusel and L. Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs vol. 94, American Mathematical Society, 2002.

[11] L. Robbianno and M. Sweedler, *Subalgebra bases*, Lecture Notes in Math. **1430** Springer (1990), 61–87.

[12] R.J. Shank, *S.A.G.B.I. Bases for Rings of Formal Modular Seminvariants*, Comment. Math. Helv. **73** (1998) no. 4, 548–565.

[13] R.J. Shank and D.L. Wehlau, *On the Depth of the Invariants of the Symmetric Power Representations of $SL_2(\mathbb{F}_p)$*, Journal of Algebra **218** (1999), 642–653.

[14] R. J. Shank and D. L. Wehlau, *Computing modular invariants of p-groups*, J. Symbolic Comput. **34** (2002) no. 5, 307–327.

[15] B. Sturmfels, *Gröbner bases and Convex Polytopes*, University Lecture Ser. **8**, Amer. Math. Society, 1996.

School of Mathematics, Statistics & Actuarial Science,
University of Kent, Canterbury, CT2 7NF, UK

E-mail address: ashleyghobson@googlemail.com

School of Mathematics, Statistics & Actuarial Science,
University of Kent, Canterbury, CT2 7NF, UK

E-mail address: R.J.Shank@kent.ac.uk