RIGID LOCAL SYSTEMS AND FINITE GENERAL LINEAR GROUPS

NICHOLAS M. KATZ AND PHAM HUU TIEP

Abstract. We use hypergeometric sheaves on $\mathbb{G}_m/\mathbb{F}_q$, which are particular sorts of rigid local systems, to construct explicit local systems whose arithmetic and geometric monodromy groups are the finite general linear groups $\mathrm{GL}_n(q)$ for any $n \geq 2$ and and any prime power q, so long as $q > 3$ when $n = 2$. This paper continues a program of finding simple (in the sense of simple to remember) families of exponential sums whose monodromy groups are certain finite groups of Lie type, cf. [Gr], [KT1], [KT2], [KT3], [KT4] for (certain) finite symplectic and unitary groups, or certain sporadic groups, cf. [KRL], [KRLT1], [KRLT2], [KRLT3]. The novelty of this paper is obtaining $\mathrm{GL}_n(q)$ in this hypergeometric way. A pullback construction then yields local systems on $\mathbb{A}^1/\mathbb{F}_q$ whose geometric monodromy groups are $\mathrm{SL}_n(q)$. These turn out to recover a construction of Abhyankar.

Contents

Introduction 1
1. The set up 2
2. The trace function of $\mathcal{H}_{\mathbb{1}}$ 3
3. The trace function of $\mathcal{H}_\chi$ for $\chi \neq \mathbb{1}$ 3
4. Putting it all together 4
5. Galois groups in this context 9
6. Weil-type representations of special linear groups 9
7. Weil representations of $\mathrm{SL}_2(q)$ 17
8. The structure of monodromy groups 21
9. Relation to work of Abhyankar 24
References 25

Introduction

For any integer $n \geq 2$ and any prime power q, the finite general linear group $\mathrm{GL}_n(q)$ has a (reducible) *total Weil representation*, which has a very simple description. It is the action by composition of $\mathrm{GL}_n(q)$ on the space W of $\mathbb{C}$-valued, or for us $\overline{\mathbb{Q}_\ell}$-valued, functions on the n-dimensional $\mathbb{F}_q$ vector space $V := \mathbb{F}_q^n$. This is a representation of dimension q^n. We can split off the delta function δ_0 at 0, and we are left with the space $W^\star$ of functions on the nonzero vectors $V^\star := V \setminus \{0\}$. On the set $V^\star$, the group $\mathbb{F}_q^\times$ of invertible scalars acts by homothety, and so the action of $W^\star$ on

2010 *Mathematics Subject Classification.* 11T23, 20C33, 20G40.

Key words and phrases. Rigid local systems, Monodromy groups, Weil representations, Finite general linear groups.

The second author gratefully acknowledges the support of the NSF (grant DMS-1840702), and the Joshua Barlaz Chair in Mathematics.

The authors are grateful to the referee for careful reading of the paper and many comments and suggestions that help greatly improve the exposition of the paper.

$V^\star$ breaks in its $q-1$ eigenspaces under the $\mathbb{F}_q^\times$ action. Thus we have

$$W = \mathbb{C}\delta_0 \oplus \bigoplus_{\chi\in \mathrm{Irr}(\mathbb{F}_q^\times)} W_\chi.$$

Inside the space $W_{\mathbb{1}}$ of $\mathbb{F}_q^\times$-invariant functions (i.e. the space of radial functions) we have the one-dimensional space $\mathbb{C}\cdot 1_{V^\star}$ of constant functions, so we have a decomposition

$$W \cong \mathbb{C}\delta_0 \oplus \mathbb{C}\cdot 1_{V^\star} \oplus (W_{\mathbb{1}}/\mathbb{C}\cdot 1_{V^\star}) \ \oplus \bigoplus_{\chi\neq\mathbb{1}} W_\chi.$$

It is easy to see that each W_χ has dimension $(q^n-1)/(q-1)$, the number of points in the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$. One knows [Ge, Prop. 4.2 (b)] that $W_{\mathbb{1}}/\mathbb{C}\cdot 1_{V^*}$, and each W_χ with nontrivial χ, is an irreducible representation of $\mathrm{GL}_n(q)$, called an *irreducible Weil representation* of $\mathrm{GL}_n(q)$. This numerology leads us to search for hypergeometric sheaves of these ranks, indexed by these same χ, for which we can prove first, that they each have finite monodromy, cf. Theorem 4.2, and then that the monodromy of their direct sum, together with two copies of the trivial representation, is indeed $\mathrm{GL}_n(q)$ in its total Weil representation, cf. Theorem 8.1. The individual (irreducible) hypergeometric sheaves have the images of $\mathrm{GL}_n(q)$ in an irreducible Weil representation as their geometric and arithmetic monodromy groups. A pullback construction then yields local systems on $\mathbb{A}^1/\mathbb{F}_q$ whose geometric monodromy groups are $\mathrm{SL}_n(q)$, and also allows us to recover a construction of Abhyankar [Abh].

1. The set up

We refer the reader to [Ka-CC, §2] for the definition and basic facts about hypergeometric sheaves and their local monodromies, and for how to view the multiplicative characters which go into their definition. We refer the reader to [Ka-ESDE, 7.2.1, 7.2.2] for the notions of Artin-Schrier sheaves $\mathcal{L}_\psi$ and Kummer sheaves $\mathcal{L}_\chi$. We also use freely the fact (Chebotarev) that if a lisse sheaf $\mathcal{F}$ is arithmetically semisimple, then it its arithmetic isomorphism class is determined by its trace function. The arithmetic semisimplicity of $\mathcal{F}$ is automatic if $\mathcal{F}$ is geometrically irreducible, or if geometrically $\mathcal{F}$ is a suitable sum of pairwise distinct irreducbles, cf [KT4, Lemma 2.2]. [In general, one can only say that a lisse sheaf $\mathcal{F}$ is determined up to arithmetic semisimplification by its trace function.]

We work in characteristic $p>0$. We choose a prime $\ell\neq p$, so as to be able to work with $\overline{\mathbb{Q}_\ell}$-cohomology. We fix a nontrivial additive character ψ of $\mathbb{F}_p$, a power q of p, and an integer $n\geq 2$. We then define

$$A := (q^n-1)/(q-1), \quad B := (q^{n-1}-1)/(q-1).$$

Recall that given an integer $N\geq 1$ prime to p, and a multiplicative character χ, we define

$$\mathsf{Char}(N,\chi) := \{\text{characters } \rho \text{ with } \rho^N = \chi\}$$

and

$$\mathsf{Char}(N) := \mathsf{Char}(N,\mathbb{1}),$$

the group of characters of order dividing N.

Our interest will be in the (sheaves geometrically isomorphic to the) following hypergeometric sheaves, indexed by the multiplicative characters χ of order dividing $q-1$. We fix a nontrivial additive character ψ of $\mathbb{F}_p$. For the trivial character, we consider

$$\mathcal{H}_{\mathbb{1}} := \mathcal{H}yp_\psi(\mathsf{Char}(A)\setminus\mathbb{1};\mathsf{Char}(B)), \text{ of rank } A-1.$$

For each nontrivial character χ of order dividing $q-1$, we consider the hypergeometric sheaf

$$\mathcal{H}_\chi := \mathcal{H}yp_\psi(\mathsf{Char}(A,\chi);\mathsf{Char}(B,\chi),\mathbb{1}),\ \text{of rank } A.$$

Lemma 1.1. *If A is odd, then the geometric determinants are given by*

$$\det(\mathcal{H}_\chi) = \mathcal{L}_\chi.$$

If A is even (possible only when p is odd), then the geometric determinants are given by

$$\det(\mathcal{H}_\chi) = \mathcal{L}_{\chi\chi_2},$$

for χ_2 the quadratic character.

Proof. One knows that the geometric determinant of a hypergeometric sheaf of type (n,m) with $n-m\geq 2$ is the product of the "upstairs" characters, cf. [Ka-ESDE, 8.11.6]. For $\mathcal{H}_{\mathbb{1}}$, one knows that the product of all (or of all but $\mathbb{1}$) the elements of $\mathsf{Char}(A)$ is $\mathbb{1}$ if A is odd, and χ_2 otherwise. For the other $\mathcal{H}_\chi$, the assertion is that the product of all the elements of $\mathsf{Char}(A,\chi)$ is $\chi\times\prod_{\rho\in\mathsf{Char}(A)}\rho$. To see this, pick one character $\Lambda\in\mathsf{Char}(A,\chi)$. Then the elements of $\mathsf{Char}(A,\chi)$ are precisely the products $\Lambda\rho$ with $\rho\in\mathsf{Char}(A)$, which makes clear that the product is as asserted. □

2. The trace function of $\mathcal{H}_{\mathbb{1}}$

For any $N\geq 2$ prime to p, the Kloosterman sheaf $\mathcal{K}l_\psi(\mathsf{Char}(N)\setminus\mathbb{1})$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is given as follows: for $K/\mathbb{F}_p$ a finite extension and $t\in K^\times$, it is

$$t\mapsto -\sum_{x\in K}\psi_K(Nx-x^N/t),$$

cf. [KRLT2, Lemma 1.2, which concerns $\overline{\psi}$]. We also know that $\mathcal{K}l_\psi(\mathsf{Char}(N))$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is given as follows: for $K/\mathbb{F}_p$ a finite extension and $t\in K^\times$, it is

$$t\mapsto \sum_{x\in K,\,x^N=t}\psi_k(Nx),$$

cf. [Ka-GKM, 5.6.2].

Lemma 2.1. *The lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is given at $u\in K^\times$ for $K/\mathbb{F}_p$ a finite extension, by*

$$u\mapsto \sum_{x\in K,\,y\in K^\times}\psi_K\big((-1/u)x^A/y^B+x-y\big)$$

is geometrically isomorphic to $\mathcal{H}_{\mathbb{1}}$.

Proof. By defintion, $\mathcal{H}_{\mathbb{1}}$ is the multiplicative ! convolution of $\mathcal{K}l_\psi(\mathsf{Char}(A)\setminus\mathbb{1})$ with the multiplicative inverse of the complex conjugate of $\mathcal{K}l_\psi(\mathsf{Char}(B))$. Thus for $u\in K^\times$, $K/\mathbb{F}_p$ a finite extension, we are looking at

$$u\mapsto \sum_{s,t\in K^\times,\,st=u}\ \sum_{x\in K}\psi_K\big(Ax-x^A/t\big)\sum_{y\in K^\times,y^B=1/s}\psi_K(-By).$$

Now use $t=u/s=uy^B$ to write this as

$$\sum_{x\in K,\,y\in K^\times}\psi_K\big(Ax-x^A/(uy^B)-By\big),$$

and note that both A,B are 1 mod q, so 1 in $\mathbb{F}_p$. □

3. The trace function of $\mathcal{H}_\chi$ for $\chi \neq \mathbb{1}$

Lemma 3.1. *For χ a nontrivial character of order dividing $q-1$, the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ whose trace function at $u \in K^\times$ for $K/\mathbb{F}_q$ a finite extension is*

$$u \mapsto \sum_{x\in K,\, y\in K^\times} \psi_K\big((-1/u)x^A/y^B + x - y\big)\chi(x/y)$$

is geometrically isomorphic to $\mathcal{H}_\chi$.

Proof. Again by [Ka-GKM, 5.6.2], we know that for $N \geq 1$ prime to p, $\mathcal{K}l_\psi(\mathsf{Char}(N,\chi))$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ whose trace function is given as follows: for $K/\mathbb{F}_q$ a finite extension, and $t \in K^\times$,

$$t \mapsto \sum_{x\in K,\, x^N=t} \psi_K(Nx)\chi_K(x).$$

Applying this with $N = A$ and with $N = B$, we see that $\mathcal{H}yp_\psi(\mathsf{Char}(A,\chi);\mathsf{Char}(B,\chi))$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ whose trace function is given as follows: for $K/\mathbb{F}_q$ a finite extension, and $v \in K^\times$,

$$\begin{aligned} v \mapsto & \sum_{s,t\in K,\, st=v} \ \sum_{x\in K,\, x^A=t} \psi_K(Ax)\chi_K(x) \sum_{y\in K,\, y^B=1/s} \psi_K(-By)\chi_K(1/y) \\ = & \sum_{x,y\in K^\times,\, x^A/y^B=v} \psi_K(Ax-By)\chi_K(x/y) \\ = & \sum_{x,y\in K^\times,\, x^A/y^B=v} \psi_K(x-y)\chi_K(x/y), \end{aligned}$$

the last equality because both A, B are 1 mod q. To compute a sheaf geometrically isomorphic to $\mathcal{H}_\chi$, we must further convolve with $\mathcal{H}yp(\emptyset;\mathbb{1}) = \mathcal{L}_{\psi(-1/x)}$. So our trace function is given as follows: for $K/\mathbb{F}_q$ a finite extension, and $u \in K^\times$,

$$u \mapsto \sum_{v,w\in K,\, vw=u} \psi_K(-1/w) \sum_{x\in K^\times,\, y\in K^\times,\, x^A/y^B=v} \psi_K(x-y)\chi_K(x/y) =$$

$$= \sum_{x,y\in K^\times} \psi_K\big(-(x^A/y^B)/u + x - y\big)\chi_K(x/y),$$

the last equality by using $vw = u$ to solve for $-1/w = -v/u$. Because χ is nontrivial, the sum does not change if we also allow $x = 0$ in the summation. □

4. Putting it all together

In the previous sections, we found that for each χ of order dividing $q-1$, trivial or not, $\mathcal{H}_\chi$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ whose trace function is given as follows: for $K/\mathbb{F}_q$ a finite extension, and $u \in K^\times$,

$$u \mapsto \sum_{x\in K,\, y\in K^\times} \psi_K\big((-1/u)x^A/y^B + x - y\big)\chi_K(x/y).$$

We now make the substitution $(x,y) \mapsto (xy, y)$. Then the above sum becomes

$$u \mapsto \sum_{x\in K,\, y\in K^\times} \psi_K\big((-1/u)x^A y^{A-B} + xy - y\big)\chi_K(x).$$

To move to weight zero, we do a Tate twist **(1)**. Concretely, we consider the lisse sheaves on $\mathbb{G}_m/\mathbb{F}_q$, denoted $\mathcal{F}_\chi$, whose trace functions are given at $t \in K^\times$ for $K/\mathbb{F}_q$ a finite extension, by

$$\mathcal{F}_\chi : u \mapsto (1/\#K) \sum_{x\in K,\, y\in K^\times} \psi_K\big((-1/u)x^A y^{A-B} + xy - y\big)\chi_K(x).$$

Lemma 4.1. *For each $\chi \in \mathsf{Char}(q-1)$, the lisse sheaf $\mathcal{F}_\chi$ on $\mathbb{G}_m/\mathbb{F}_q$ is geometrically isomorphic to $\mathcal{H}_\chi$.*

Proof. Immediate from Lemmas 2.1 and 3.1. □

Theorem 4.2. *Each of the sheaves $\mathcal{F}_\chi$ has finite G_{arith} and (hence) finite G_{geom}.*

Proof. The key observation is that

$$A - B = q^{n-1}$$

is a power of q. Therefore the trace sum of $\mathcal{F}_\chi$ does not change if we raise some of the terms in the argument of ψ_K to the $(A-B)^{\mathrm{th}}$ power, since this does not alter $\mathrm{Trace}_{K/\mathbb{F}_q}$. Thus the trace sum for $\mathcal{F}_\chi$ at time $u \in K^\times$ is equal to

$$(1/\#K) \sum_{x\in K,\, y\in K^\times} \psi_K\big((-1/u)x^A y^{A-B} + x^{A-B}y^{A-B} - y^{A-B}\big)\chi_K(x).$$

Factoring out the y^{A-B} term, we rewrite this as

$$(1/\#K) \sum_{x\in K} \sum_{y\in K^\times} \psi_K\big(y^{A-B}((-1/u)x^A + x^{A-B} - 1)\big)\chi_K(x).$$

Because $y \mapsto y^{A-B}$ is an automorphism of K, so a bijection on $K^\times$, this sum is equal to

$$(1/\#K) \sum_{x\in K} \sum_{y\in K^\times} \psi_K\big(y((-1/u)x^A + x^{A-B} - 1)\big)\chi_K(x).$$

Interpreting $\psi_K\big(y((-1/u)x^A + x^{A-B} - 1)\big)$ as 1 when $y = 0$, the above sum can be written as

$$-\delta_{\mathbb{1},\chi} + (1/\#K) \sum_{x\in K} \sum_{y\in K} \psi_K\big(y((-1/u)x^A + x^{A-B} - 1)\big)\chi_K(x).$$

The sum over y is

$$0, \text{ unless } (-1/u)x^A + x^{A-B} - 1 = 0, \text{ in which case it is } \chi_K(x).$$

Thus the trace of $\mathcal{F}_\chi$ at time $u \in K^\times$ is

$$\begin{array}{ll} -1 + \text{ number of solutions } x \in K \text{ of } (-1/u)x^A + x^{A-B} - 1 = 0, & \text{if } \chi = \mathbb{1}, \\ \sum_{x\in K,\,(-1/u)x^A + x^{A-B} - 1 = 0} \chi_K(x), & \text{if } \chi \neq \mathbb{1}. \end{array} \tag{4.2.1}$$

So in all cases, $\mathcal{F}_\chi$ has algebraic integer traces, and we are done by [Ka-ESDE, 8.14.4, (1) $\iff$ (2) $\iff$ (6)]. □

Corollary 4.3. *Denote by $f(t)$ the polynomial*

$$f(t) := t^B(1-t)^{A-B},$$

and denote by inv *the multiplicative inversion $u \mapsto 1/u$ on $\mathbb{G}_m$. Then on $\mathbb{G}_m/\mathbb{F}_q$ we have arithmetic isomorphisms*

$$f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell \cong \mathsf{inv}^\star \mathcal{F}_{\mathbb{1}},$$

and, for each nontrivial χ of order dividing $q-1$,

$$f_\star \mathcal{L}_{\overline{\chi}} \cong \mathsf{inv}^\star \mathcal{F}_\chi.$$

Proof. According to (4.2.1), the trace function of $\mathsf{inv}^\star\mathcal{H}_\chi$ at $u \in K^\times$, $K/\mathbb{F}_q$ a finite extension, is

$$-\delta_{\mathbb{1},\chi} + \sum_{x\in K,\,(-u)x^A+x^{A-B}-1=0} \chi_K(x).$$

The polynomial $(-u)x^A + x^{A-B} - 1$ has all its roots nonzero. Dividing through by x^A, we may write it as a polynomial in $1/x := t$. It becomes (remembering that $A - B = q^{n-1}$ is a power of p)

$$\big((-u)x^A + x^{A-B} - 1\big)/x^A = -u + x^{-B} - x^{-A} = -u + t^B - t^A = t^B(1-t)^{A-B} - u.$$

Thus the trace becomes

$$-\delta_{\mathbb{1},\chi} + \sum_{t\in K,\,t^B(1-t)^{A-B}=u} \overline{\chi}_K(t),$$

which is precisely the trace function of $f_\star\mathbb{Q}_\ell/\mathbb{Q}_\ell$ for $\chi = \mathbb{1}$, and of $f_\star\mathcal{L}_{\overline{\chi}}$ when $\chi \neq \mathbb{1}$. Because the sheaves $\mathcal{F}_\chi$ are each (geometrically, and hence) arithmetically irreducible, this equality of trace functions implies arithmetic isomorphisms of sheaves. □

Corollary 4.4. *The trace function of* $\oplus_{\chi\in\mathsf{Char}(q-1)}\mathsf{inv}^\star\mathcal{F}_\chi$ *at* $u \in K^\times$, $K/\mathbb{F}_q$ *a finite extension, is*

$$-1 + \text{ number of solutions } T \in K \text{ of } T^{(q-1)B}(1-T^{q-1})^{A-B} = u.$$

Proof. The trace at $u \in K^\times$, $K/\mathbb{F}_q$ a finite extension, is -1 plus

$$\sum_{t\in K,\,t^B(1-t)^{A-B}=u}\ \sum_{\chi\in\mathsf{Char}(q-1)} \overline{\chi_K}(t).$$

The sum over χ vanishes unless t is a $(q-1)^{\text{th}}$ power in $K^\times$, in which case there exist exactly $q-1$ elements $T \in K^\times$ with the property that $t = T^{q-1}$. So the trace is -1 plus the number of solutions $T \in K$ of

$$T^{(q-1)B}(1-T^{q-1})^{A-B} = u.$$

□

From Corollary 4.3, we get

Corollary 4.5. *For f the polynomial $f(t) := t^B(1-t)^{A-B}$, we have an arithmetic isomorphism on $\mathbb{G}_m/\mathbb{F}_q$*

$$f_\star\big(\oplus_{\chi\in\mathsf{Char}(q-1)}\mathcal{L}_\chi\big) \cong \overline{\mathbb{Q}_\ell} \oplus \big(\oplus_{\chi\in\mathsf{Char}(q-1)}\mathsf{inv}^\star\mathcal{F}_\chi\big)$$

In what follows, we will let $\mathcal{W}(n,q)$ denote the local system $\oplus_{\chi\in\mathsf{Char}(q-1)}\mathcal{F}_\chi$.

Corollary 4.6. *For F the polynomial*

$$F(T) := T^{q^{n-1}-1} - T^{q^n-1},$$

we have an arithmetic isomorphism on $\mathbb{G}_m/\mathbb{F}_q$,

$$F_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell} \cong \mathsf{inv}^\star(\mathcal{W}(n,q)).$$

The local system $F_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$ lives on $\mathbb{G}_m/\mathbb{F}_p$, and thus provides a descent of $\mathcal{W}(n,q)$ to $\mathbb{G}_m/\mathbb{F}_p$.

Lemma 4.7. *Let $q_0 > 1$ be a power of a prime p, $K_0 := \mathbb{F}_{q_0^3}$. For each $u \in K_0$, let $N(u)$ denote the number of solutions in K_0 of the equation $T^{q_0^2} - T^{q_0} = uT$. Then the following statements hold.*

(i) *Suppose $p = 2$. Then $N(1) = q_0^2$. Furthermore, $N(u) = q_0$ for exactly q_0^2 values of $u \in K_0 \smallsetminus \{1\}$, and $N(u) = 1$ for all the remaining $q_0^3 - q_0^2 - 1$ values of $u \in K_0 \smallsetminus \{1\}$.*

(ii) *Suppose $p > 2$. Then $N(u) = q_0$ for exactly $q_0^2 + q_0 + 1$ values in $u \in K_0$, and $N(u) = 1$ for all the remaining $q_0^3 - q_0^2 - q_0 - 1$ values of $u \in K_0$.*

Proof. Note that $N(u) = \#(\mathcal{X}_u) + 1$, where $\mathcal{X}_u$ is the set of solutions in $K_0^\times$ of the equation $T^{q_0^2} - T^{q_0} = uT$, equivalently, of the equation $T^{q_0^2-1} - T^{q_0-1} = u$. In particular, $K_0^\times$ partitions into the disjoint union of all $\mathcal{X}_u$ when u varies over K_0, whence

$$\sum_{u \in K_0} (N(u) - 1) = q_0^3 - 1. \tag{4.7.1}$$

Suppose that $T \in \mathcal{X}_u$. As $T^{q_0^2} = T^{q_0} + uT$ and $T \in K_0^\times$, we have

$$T = T^{q_0^3} = T^{q_0^2} + u^{q_0}T^{q_0} = T^{q_0} + uT + u^{q_0}T^{q_0} = T^{q_0}(1+u)^{q_0} + uT.$$

Now if $u = -1$ then $2T = 0$, which is impossible if $p \neq 2$. On the other hand, if $u \neq -1$, then $T^{q_0-1} = (1-u)(1+u)^{-q_0}$. This last equation has at most $q_0 - 1$ solutions in $K_0^\times$. Conversely, if $T_0 \in \mathcal{X}_u$, then $\alpha T_0 \in \mathcal{X}_u$ for all $\alpha \in \mathbb{F}_{q_0}^\times$. Thus we have shown that

$$\text{If } u \neq -1, \text{ then } N(u) = 1 \text{ or } q_0, \tag{4.7.2}$$

and that $N(-1) = 1$ if $p \neq 2$. In particular, (4.7.1) implies (ii) if $p > 2$.

Assume now that $u = 1$ and $p = 2$. Then

$$T^{q_0^2} - T^{q_0} - uT = \mathrm{Tr}_{K_0/\mathbb{F}_{q_0}}(T),$$

and so $N(1) = q_0^2$. Together with (4.7.1), this also implies that

$$\sum_{1 \neq u \in K_0} (N(u) - 1) = q_0^3 - q_0^2,$$

and (i) now follows from (4.7.2). □

Theorem 4.8. *Let K be a finite extension of $\mathbb{F}_p$. Then the following statements holds for the trace at time $u \in K^\times$ on $F_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$.*

(i) *This trace plus 2 is a always a p-power.*
(ii) *If $K \supseteq \mathbb{F}_q$, then this trace is of the form $q^a - 2$ for some integer $0 \leq a \leq n$.*
(iii) *Suppose that $q = p^f$ with $f \geq 2$. For any prime divisor r of f, there exist an extension K_0 of $\mathbb{F}_p$ and an element $u_0 \in K_0^\times$ such that the trace at time u_0 is $p^{f/r^c} - 2$, where r^c is the r-part of f.*

In particular, (i) *and* (ii) *hold for the trace at time $u \in K^\times$ on $\mathcal{W}(n,q)$, now viewed as a local system on $\mathbb{G}_m/\mathbb{F}_p$ via Corollary 4.6.*

Proof. (a) It is equivalent to prove this for $\mathsf{inv}^\star$ of the direct sum sheaf in question. The trace is -1 plus the number of solutions $T \in K$ of

$$T^{(q-1)B}(1 - T^{q-1})^{A-B} = u.$$

Write out the polynomial $T^{(q-1)B}(1 - T^{q-1})^{A-B}$. It is

$$T^{(q-1)B} - T^{(q-1)B+(q-1)(A-B)} = T^{q^{n-1}-1} - T^{q^n-1}.$$

So the trace is -1 + the number of solutions $T \in K$ of

$$T^{q^{n-1}-1} - T^{q^n-1} = u.$$

$T = 0$ is visibly not a solution, so the trace is

$$-2 + \text{ number of solutions } T \in K \text{ of } T^{q^{n-1}} - T^{q^n} = uT.$$

The solution set of this last equation,

$$T^{q^{n-1}} - T^{q^n} = uT, \tag{4.8.1}$$

over any field $K \supseteq \mathbb{F}_p$ forms a vector space over $\mathbb{F}_p$ of finite dimension, hence (i) holds. If $K \supseteq \mathbb{F}_q$, then the solution set of (4.8.1) over K forms an $\mathbb{F}_q$ vector space of dimension $\leq n$, so the number of its solutions is indeed q^a for some integer $0 \leq a \leq n$, yielding (ii).

(b) The rest of the proof is to establish (iii). Write $f = f_0 r^c$ and $q_0 = p^{f_0}$. The idea is to show that for a well chosen prime $s \neq r$, we can take

$$K_0 := \mathbb{F}_{p^{sf_0}} = \mathbb{F}_{q_0^s}.$$

If $n \geq 3$, then, since $\gcd(n, n-1) = 1$, $n(n-1)$ is divisible by at least two distinct primes, so we can find a prime $s \neq r$ that divides exactly one of the two integers n and $n-1$. If $n = 2$ and $r > 2$, we choose $s = 2$. If $(n, r) = (2, 2)$, choose $s = 3$. With s chosen this way, we choose $K_0 := \mathbb{F}_{p^{sf_0}} = \mathbb{F}_{q_0^s}$, and solve the equation (4.8.1) over K_0, for certain $u \in K_0^\times$.

First we consider the case $n = r = 2$, whence $s = 3$. Then $\{nr^c, (n-1)r^c\} = \{2^{c+1}, 2^c\}$ is congruent to $\{1, 2\}$ modulo 3 (as a set), and for integers $a, b \geq 0$ we have

$$q_0^{a+3b} - 1 \equiv q_0^a - 1 (\mathrm{mod}\ (q_0^3 - 1)).$$

If $2|c$ then

$$T^{q^{n-1}} - T^{q^n} = T^{q_0^{(n-1)r^c}} - T^{q_0^{nr^c}} = T^{q_0} - T^{q_0^2},$$

and if $2 \nmid c$ then

$$T^{q^{n-1}} - T^{q^n} = T^{q_0^{(n-1)r^c}} - T^{q_0^{nr^c}} = T^{q_0^2} - T^{q_0}$$

for all $T \in K_0$. Hence we are done by Lemma 4.7.

(c) From now on we may assume that $(n, r) \neq (2, 2)$. The idea now is to view $K_0 := \mathbb{F}_{q_0^s}$ as vector space over $\mathbb{F}_{q_0}$. The $(q_0 - 1)^{\text{th}}$ power map

$$[q_0 - 1] : x \mapsto x^{q_0 - 1}$$

maps $K_0^\times$ onto $\mu_{(q_0^s-1)/(q_0-1)} := \{t \in K_0 \mid t^{(q_0^s-1)/(q_0-1)} = 1\}$, with fibres the nonzero elements in the $\mathbb{F}_{q_0}$-lines defined by the $(q_0^s - 1)/(q_0 - 1)$ equations

$$T^{q_0} = vT,$$

one for each $v \in \mu_{(q_0^s-1)/(q_0-1)}$. Conversely, for any $v \in \overline{\mathbb{F}_p}^\times$, the equation $T^{q_0} = vT$ has q_0 solutions in $\overline{\mathbb{F}_p}$, and for such a T we have

$$T^{q_0^i} = v^{(q_0^i-1)/(q_0-1)} T$$

for any $i \in \mathbb{Z}_{\geq 0}$. In particular, $T \in K_0^\times$ if and only if v belongs to $\mu_{(q_0^s-1)/(q_0-1)}$.

For $v \in \mu_{(q_0^s-1)/(q_0-1)}$ and T satisfying $T^{q_0} = vT$, using this last identity and remembering that q is $q_0^{r^c}$, we find that $T^{q^{n-1}} - T^{q^n} = H(v)T$, where

$$H : \mu_{(q_0^s-1)/(q_0-1)} \to K_0, \quad v \mapsto v^{(q_0^{(n-1)r^c}-1)/(q_0-1)} - v^{(q_0^{nr^c}-1)/(q_0-1)}.$$

We claim that

$$H \text{ is injective when } (n, r) \neq (2, 2). \tag{4.8.2}$$

Admit this for a moment. Then for each $v \in \mu_{(q_0^s-1)/(q_0-1)}$, the points in the line $T^{q_0} = vT$ are among the K_0-solutions of the equation

$$\mathrm{Eqn}(v) : T^{q^{n-1}} - T^{q^n} = H(v)T.$$

As the $H(v)$ are pairwise distinct, the nonzero K_0-solutions of these $(q_0^s - 1)/(q_0 - 1)$ equations partition $K_0^\times$ into $(q_0^s - 1)/(q_0 - 1)$ disjoint subsets, each of which consists of the $q_0 - 1$ nonzero points in the line $T^{q_0} = vT$. Therefore each $\mathrm{Eqn}(v)$ has precisely q_0 solutions in K_0. Furthermore,

since $H(1) = 0$, we see that for $v \neq 1$, $v \in \mu_{(q_0^s-1)/(q_0-1)}$, $H(v) \neq 0$. At any such point $u = H(v)$, we then have that the trace at time $u \in K_0^\times$ is q_0, as asserted.

We now prove (4.8.2). Suppose then that $H(v) = H(w)$, with $v, w \in \mu_{(q_0^s-1)/(q_0-1)}$, i.e. that we have

$$v^{(q_0^{(n-1)r^c}-1)/(q_0-1)} - v^{(q_0^{nr^c}-1)/(q_0-1)} = w^{(q_0^{(n-1)r^c}-1)/(q_0-1)} - w^{(q_0^{nr^c}-1)/(q_0-1)}. \tag{4.8.3}$$

As $(n, r) \neq (2, 2)$, s divides exactly one of n and $n-1$. For definiteness, say $s|n$ and $s \nmid (n-1)$. Then $(q_0^s - 1)/(q_0 - 1)$ divides $(q_0^n - 1)/(q_0 - 1)$, which divides $(q_0^{nr^c} - 1)/(q_0 - 1)$, and hence

$$w^{(q_0^{nr^c}-1)/(q_0-1)} = v^{(q_0^{nr^c}-1)/(q_0-1)} = 1.$$

Thus we have

$$w^{(q_0^{(n-1)r^c}-1)/(q_0-1)} = v^{(q_0^{(n-1)r^c}-1)/(q_0-1)}.$$

It follows that the order of w/v divides

$$\gcd\left(\frac{q_0^s - 1}{q_0 - 1}, \frac{q_0^{(n-1)r^c} - 1}{q_0 - 1}\right) = 1$$

since[1] $\gcd(s, (n-1)r^c) = 1$. Thus $w = v$, as asserted. □

5. Galois groups in this context

Let k be a field, and $f(t) \in k[t]$ a polynomial whose derivative $f'(t)$ is not identically zero. Recall that the critical values of f are its values at the zeroes of f'. On the dense open set

$$U := \mathbb{A}^1 \setminus \{\text{critical values of } f\},$$

the sheaf $f_\star\overline{\mathbb{Q}_\ell}$ is lisse, of rank the degree of f.

Let us recall the well known identification of G_{arith} with a Galois group.

Lemma 5.1. *The G_{arith} of $f_\star\overline{\mathbb{Q}_\ell}$ is the Galois group of the equation*

$$f(t) = u$$

over the rational function field $k(u)$. In particular we have

$$G_{\text{arith}} \subseteq \mathsf{S}_{\deg(f)},$$

and the quotient $f_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$ has the same G_{arith}, now acting through the deleted permutation representation of $\mathsf{S}_{\deg(f)}$.

Proof. Indeed, G_{arith} is the "monodromy group" of the finite étale covering of U defined by

$$f : \mathbb{A}^1 \setminus f^{-1}\{\text{critical values of } f\}$$

in the sense of [Ka-LGER, 1.2.2], which is the usual étale cohomological incarnation of the Galois group. □

[1]Recall that for an integer $a \neq 0, \pm 1$, and positive integers n, m with $\gcd(n, m) = 1$, one has $\gcd(a^n - 1, a^m - 1) = a - 1$. as one sees by working in the multiplicative group of $\mathbb{Z}/d\mathbb{Z}$ for any d dividing $\gcd(a^n - 1, a^m - 1)$.

6. Weil-type representations of special linear groups

Let q be a power of a prime p, $W = \mathbb{F}_q^n$, and consider the general linear group $\mathrm{GL}(W) \cong \mathrm{GL}_n(q)$ and the special linear group $\mathrm{SL}(W) \cong \mathrm{SL}_n(q)$. These groups act naturally on the set of q^n vectors of W, and the corresponding permutation character is denoted

$$\tau_n = \tau_{n,q} : g \mapsto q^{\dim_{\mathbb{F}_q} \mathrm{Ker}(g-1_W)}. \tag{6.0.1}$$

We will also refer to τ_n as the *total Weil character* of $\mathrm{SL}_n(q)$. When $n \geq 3$, $\tau_{n,q}$ decomposes over $\mathrm{SL}_n(q)$ as

$$\tau_n = 2 \cdot 1_{\mathrm{SL}_n(q)} + \sum_{i=0}^{q-2} \tau_n^i,$$

where $\tau_n^i \in \mathrm{Irr}(\mathrm{SL}_n(q))$ has degree $(q^n-1)/(q-1) - \delta_{i,0}$. We will refer to $\tau_n^i = \tau_{n,q}^i$ as *irreducible Weil characters* of $\mathrm{SL}_n(q)$.

Theorem 6.1. *Let p be any prime and q be any power of p. Let $L = \mathrm{SL}_n(q)$ with $n \geq 3$. Suppose ψ is a reducible complex character of L such that*

(a) $\psi(1) = q^n$;
(b) $\psi(g) \in \{q^i \mid 0 \leq i \leq n\}$ *for all* $g \in L$;
(c) $[\psi, 1_L]_L = 2$; *and*
(d) *every irreducible constituent of $\psi - 2 \cdot 1_L$ is among the $q-1$ irreducible Weil characters τ_n^u, $0 \leq u \leq q-2$, of L.*

Then ψ is the total Weil character τ_n of L, that is, $\psi = 2 \cdot 1_L + \sum_{u=0}^{q-2} \tau_n^u$.

Proof. (i) By assumption (d),

$$\psi = 2 \cdot 1_L + \sum_{u=0}^{q-2} a_u \tau_n^u,$$

where $a_u \in \mathbb{Z}_{\geq 0}$. Comparing the degrees, we obtain

$$1 - a_0 = \frac{q^n-1}{q-1}\Big(q - 1 - \sum_{u=0}^{q-2} a_u\Big);$$

in particular, $a_0 - 1$ is divisible by $(q^n-1)/(q-1)$. On the other hand,

$$-1 \leq a_0 - 1 \leq \frac{\psi(1)-2}{\tau_n^0(1)} - 1 = \frac{q^n-2}{(q^n-q)/(q-1)} - 1 \leq \frac{q^n-2}{q^2+q} - 1 < \frac{q^n-1}{q-1},$$

since $n \geq 3$. It follows that

$$a_0 = 1,\ \sum_{u=1}^{q-2} a_u = q-2. \tag{6.1.1}$$

In particular, if $2 \leq q \leq 3$, then $\psi = 2 \cdot 1_L + \sum_{u=0}^{q-2} \tau_n^u = \tau_n$. Hence we may assume $q \geq 4$.

(ii) Now, view L as $\mathrm{SL}(W)$ where $W = \mathbb{F}_q^n$, and consider the subgroup $H \cong \mathrm{SL}_3(q)$ of L that fixes a 3-dimensional subspace of W and acts trivially on its complement in W. The values of τ_n^i are well known, see e.g. [T, (1.1)]. An easy application of this character formula shows that

$$\psi_H = \sum_{u=0}^{q-2} b_u \tau_3^u,\ \text{where } b_u := a_u + (q^{n-3}-1), \tag{6.1.2}$$

in particular,

$$b_0 = q^{n-3},\ \sum_{u=1}^{q-2} b_u = q^{n-3}(q-2).$$

Also, let σ be a primitive $(q^2-1)^{\text{th}}$ root of unity in $\overline{\mathbb{F}}_q$, $\delta = \sigma^{q+1}$, $\tilde{\delta}$ be a primitive $(q-1)^{\text{th}}$ root of unity in $\mathbb{C}$, and set

$$\Sigma_k := \sum_{u=1}^{q-2} b_u \tilde{\delta}^{uk},\ \Delta_k := \sum_{u=0}^{q-2} a_u \tilde{\delta}^{uk}$$

for any $k \in \mathbb{Z}$. Note that both Σ_k and Δ_k depend only on $k (\mathrm{mod}\ (q-1))$. Then (6.1.1) and (6.1.2) imply that

$$\Delta_0 = q-1,\ |\Delta_k| \le q-1. \tag{6.1.3}$$

(iii) The character table of H is well known, see e.g. [SF]. Consider any $k \in \mathbb{Z}$ with $(q-1)/2 \nmid k$. Evaluating ψ at a semisimple element in L with eigenvalues $\delta^k, \delta^{-k}, 1$, we have by (b) that

$$\Sigma'_k := 2q^{n-3} + 2b_0 + \Sigma_0 + \Sigma_k + \Sigma_{-k} = q^{n-2} + \Delta_k + \overline{\Delta_k} \text{ belongs to } \mathcal{V} := \{q^i \mid 0 \le i \le n\}.$$

Next, by adding $q-1$ to k if necessary, which does not change Σ_k, we may assume that $(q+1) \nmid k$. Evaluating ψ at a semisimple element in L with eigenvalues $\delta^{-k}, \sigma^k, \sigma^{qk}$ (over $\overline{\mathbb{F}}_q$) and using (b) again, we have that

$$\mathcal{V} \ni 2q^{n-3} + \Sigma_k = q^{n-3} + \Delta_k.$$

Thus, for a fixed $k (\mathrm{mod}\ (q-1))$ with $(q-1)/2 \nmid k$, we can find $a, b \in \mathbb{Z}_{\ge 0}$ such that

$$q^{n-3} + \Delta_k = q^a,\ q^{n-2} + \Delta_k + \overline{\Delta_k} = q^b.$$

It follows that $\Delta_k = q^a - q^{n-3} = \overline{\Delta_k}$, and

$$q^b = (q-2)q^{n-3} + 2q^a > q^{n-3}.$$

Hence $b \ge n-2$, which in turn implies that $a \ge n-3$. Assume in addition that $a \ge n-2$. Then

$$\Delta_k \ge q^{n-2} - q^{n-3}.$$

In this case, using $n \ge 3$ and (6.1.3), we obtain that $n = 3$ and $a = 1$, and so $q^b = 3q-2$, which is impossible since $q > 2$. We have shown that $a = n-3$, i.e. $\Delta_k = 0$.

Thus the polynomial

$$f(t) := \sum_{u=0}^{q-2} a_u t^u \in \mathbb{Z}[t]$$

has $\tilde{\delta}^k$ with $1 \le k \le q-2$, $k \ne (q-1)/2$, as roots. Also, $f(1) = \sum_{u=0}^{q-2} a_u = q-1$ by (6.1.1). If $2|q$, it follows that $f(t)$ is divisible by $(t^{q-1}-1)/(t-1)$, and so $f(t) = \sum_{u=0}^{q-2} t^u$. If $2 \nmid q$, we have that $f(t)$ is divisible by $(t^{q-1}-1)/(t^2-1)$, whence $f(t) = (at+b)(t^{q-3} + t^{q-5} + \ldots + t^2 + 1)$ with $a, b \in \mathbb{Q}$. Evaluating at $t = 1$ we obtain $a + b = 2$. Next, $b = f(0) = a_0 = 1$, and so $a = 1$, whence $f(t) = \sum_{u=0}^{q-2} t^u$ again. In other words, $a_u = 1$ for all u, as stated. □

Theorem 6.1 will be used in tandem with the following result, which allows us to recognize the size of the ground field s for the special linear group $\mathrm{SL}_m(s)$ from the values of a sum of its Weil characters:

Proposition 6.2. *Let $n \ge 3$ and let q be a power of a prime p. Let s be a power of a prime r, possibly different from p, and $L = \mathrm{SL}_m(s)$ with $m \ge 2$. Suppose L possesses a reducible complex character of ψ such that*

(a) $\psi(1) = q^n$;

(b) $\psi(g)$ *is a* q*-power for any transvection* $g \in L$*;*
(c) $(q^n-1)/(q-1) = (s^m-1)/(s-1)$*, and*
(d) $\psi = 2\cdot 1_L + \sum_{u=0}^{s-2} a_u\tau_m^u$ *is a sum of trivial and irreducible Weil characters* $\tau_m^u = \tau_{m,s}^u$ *of* L*,* $a_u \in \mathbb{Z}_{\geq 0}$*, and* $a_0 = 1$*.*

Then $(m,s) = (n,q)$*.*

Proof. First we note that $m \geq 3$. Indeed, if $m = 2$, then (c) implies that $s = q\cdot(q^{n-1}-1)/(q-1)$ is a product of two coprime integers larger than 1, which is impossible since s is a prime power.

By hypothesis,

$$q^n = \psi(1) = 1 + \frac{s^m-1}{s-1}\cdot\sum_{u=0}^{s-2} a_u = 1 + \frac{q^n-1}{q-1}\cdot\sum_{u=0}^{s-2} a_u,$$

whence $\sum_{u=0}^{s-2} a_u = q-1$. Next we evaluate τ_m^u at a transvection $g \in L$ using the character formula [T, (1.1)]:

$$\tau_m^u = \frac{s^{m-1}-1}{s-1} - \delta_{u,0}.$$

By (b), there exists some $a \in \mathbb{Z}_{\geq 0}$ that

$$q^a = \psi(g) = 1 + \frac{s^{m-1}-1}{s-1}\cdot\sum_{u=0}^{s-2} a_u = 1 + (q-1)\frac{s^{m-1}-1}{s-1}.$$

In particular, $a \geq 2$ since $m \geq 3$. It follows that

$$s^{m-1} = \frac{s^m-1}{s-1} - \frac{s^{m-1}-1}{s-1} = \frac{q^n-1}{q-1} - \frac{q^a-1}{q-1} = q^a\cdot\frac{q^{n-a}-1}{q-1},$$

and so s^{m-1} is divisible by q^a, whence $r = p$. In this case, the p-part of $(s^m-1)/(s-1)-1$ is s, and the p-part of $(q^n-1)/(q-1)-1$ is q, and we conclude using (c) that $s = q$ and $m = n$. □

We will also need to work with permutation representations of $\mathrm{SL}_n(q)$ of degree q^n-1. Let us recall some of the group-theoretic notations used in the sequel. If G is a finite group with a subgroup L, then $\mathbf{C}_G(L)$ denotes the centralizer of L in G, $\mathrm{soc}(G)$ denotes the *socle* of G, i.e. the product of all minimal normal subgroups of G, and $G^{(\infty)}$ denotes the last term of the derived series of G.

Lemma 6.3. *Let* $n \geq 2$ *and let* $L = \mathrm{SL}(W) \cong \mathrm{SL}_n(q)$ *embed in* S_N *via its natural permutation action on the set* Ω *of* $N := q^n-1$ *nonzero vectors of* $W = \mathbb{F}_q^n$*. Then* $\mathbf{C}_{\mathsf{S}_N}(L)$ *coincides with* $\mathbf{Z}(\mathrm{GL}(W)) \cong C_{q-1}$ *acting on* Ω*.*

Proof. Clearly, $\mathbf{Z}(\mathrm{GL}(W))$ commutes with L as subgroups of $\mathrm{Sym}(\Omega) = \mathsf{S}_N$. Conversely, let $h \in \mathbf{C}_{\mathsf{S}_N}(L)$ and consider a nonzero $v \in W$. Then $\mathrm{Stab}_L(v)$ has exactly $q-1$ fixed points λv, $\lambda \in \mathbb{F}_q^\times$, on Ω. As h centralizes L, it permutes these $q-1$ fixed points, whence $h(v) = \alpha v$ for some $\alpha \in \mathbb{F}_q^\times$. Now, given any $0 \neq u \in W$, we can find $g \in L$ such that $u = g(v)$. It follows that

$$h(u) = h(g(v)) = g(h(v)) = g(\alpha v) = \alpha g(v) = \alpha u,$$

i.e. $h = \alpha\cdot 1_W \in \mathbf{Z}(\mathrm{GL}(W))$. □

Lemma 6.4. *Let* $n \geq 2$ *and let* $L = \mathrm{SL}(W) \cong \mathrm{SL}_n(q)$*. Then the following statements hold.*

(i) *Let* P *be a subgroup of* L *of index* $(q^n-1)/(q-1)$*. Then* P *is either the stabilizer in* L *of a line or the stabilizer of a hyperplane of* W*.*
(ii) *Let* Q *be a subgroup of* L *of index* q^n-1*, and let* τ *denote the transpose-inverse automorphism of* L *if* $n \geq 3$*. If* $n = 2$*, respectively if* $n \geq 3$*, then* Q*, respectively* Q *or* $\tau(Q)$*, is the stabilizer in* L *of some nonzero vector* $v \in W$*.*

Proof. Our proof uses the following result, which is known in the literature as *Borel-Tits theorem*, or *Tits' lemma*, cf. [Se, (1.6)]: *If G is a finite group of Lie type of simply connected type in characteristic p and if M is a maximal subgroup of G containing a Sylow p-subgroup of G, then M is a parabolic subgroup of G.*

(i) Let M be a maximal subgroup of L containing P. By the above statement, M is a maximal parabolic subgroup of L, that is, there is some $1 \leq i \leq n-1$ such that M is the stabilizer in L of some i-dimensional subspace of W. Note that $[L : M]$ is greater than $q(q^n-1)/(q-1)$ if $2 \leq i \leq n-2$, and equal to $(q^n-1)/(q-1)$ if $i \in \{1, n-1\}$. Since $[L : P] = (q^n-1)/(q-1)$, it follows that $i \in \{1, n-1\}$, and $P = M$.

(ii) Again, let M be a maximal subgroup of L containing Q. The arguments in (i) show that M is the stabilizer in L of a line or a hyperplane of W. Applying τ to both Q and M when $n \geq 3$ if necessary, we may assume that $M = \mathrm{Stab}_L(\langle v \rangle_{\mathbb{F}_q})$ for some $0 \neq v \in W$.

Note that $M = U \rtimes K$, where U is a normal p-subgroup (with p the prime dividing q) and $K \cong \mathrm{GL}_{n-1}(q)$, and $[M : Q] = q-1$. Hence $U \lhd Q$, $Q = U(Q \cap K)$, and

$$[K : Q \cap K] = [M : Q] = q-1. \tag{6.4.1}$$

If $n = 2$, then $|U| = q = |Q|$, whence $Q = U = \mathrm{Stab}_L(v)$, and so we are done in this case. We will now assume that $n \geq 3$. Now, $\mathrm{Stab}_L(v) = U[K, K]$, where $[K, K] \cong \mathrm{SL}_{n-1}(q)$. By (6.4.1), $[[K, K] : Q \cap [K, K]]$ divides $[K : Q \cap K] = q-1$. On the other hand, the index of proper subgroups of $\mathrm{SL}_{n-1}(q)$ is larger than $q-1$, see e.g. [KlL, Table 5.2.A], unless $(n, q) = (3, 9)$. In the exceptional case, any subgroup of $[K, K] \cong \mathrm{SL}_2(9) \cong 2\mathsf{A}_6$ of index dividing 8 must coincide with $[K, K]$. Thus in all cases $Q \geq [K, K]$, whence $Q = U[K, K]$ by order comparison. □

Lemma 6.5. *Let r be a prime, $m \in \mathbb{Z}_{\geq 2}$, and $(m, r) \neq (2, 2)$. Then the affine general linear group $\mathrm{AGL}_m(r)$ does not possess any element of order r^m.*

Proof. We can embed $\mathrm{AGL}_m(r)$ in $\mathrm{SL}_{m+1}(r)$ (as the stabilizer of a nonzero vector in $\mathbb{F}_r^{m+1}$). For any r-element $x \in \mathrm{SL}_{m+1}(r)$, we have $(x - \mathrm{Id})^{m+1} = 0$. As $m \geq 2$ and $(m, r) \neq (2, 2)$, we have that $r^{m-1} \geq m+1$. Hence $x^{r^{m-1}} - \mathrm{Id} = (x - \mathrm{Id})^{r^{m-1}} = 0$, and so the order of x is at most r^{m-1}. □

We will say that a linear transformation of $\mathrm{GL}(V)$ has *simple spectrum*, if it is diagonalizable and has pairwise distinct eigenvalues. We will need the following classification of certain doubly transitive permutation groups:

Theorem 6.6. *Let q be a prime power, $n \in \mathbb{Z}_{\geq 3}$, $N_0 := (q^n-1)/(q-1)$, and let $\Psi : \mathsf{S}_{N_0} \to \mathrm{GL}(V_0)$ denote the representation of S_{N_0} on the deleted permutation module $V_0 = \mathbb{C}^{N_0-1}$. Suppose that $G \leq \mathsf{S}_{N_0}$ is such that $\Psi|_G$ is irreducible and contains an element with simple spectrum. Also let S denote the socle $\mathrm{soc}(G)$ of G. Then one of the following statements holds.*

(i) *$S = \mathsf{A}_{N_0}$ and $\mathsf{A}_{N_0} \lhd G \leq \mathsf{S}_{N_0}$, with G acting naturally on N_0 points.*

(ii) *$S \lhd G \leq \mathrm{Aut}(S)$, and $S = \mathrm{PSL}_m(s)$ for some prime power s and $m \geq 2$ such that*

$$(s^m-1)/(s-1) = (q^n-1)/(q-1).$$

Furthermore, there is a bijection from $\{1, 2, \ldots, N_0\}$ to the set of lines or hyperplanes of $\mathbb{F}_s^m$, that identifies the action of S on $\{1, 2, \ldots, N_0\}$ with its natural action on the set of lines, respectively hyperplanes, of $\mathbb{F}_s^m$.

(iii) *$(q^n-1)/(q-1) = r^m$ for some prime r and $m \geq 1$, $S \cong C_r^m$, and $S \lhd G \leq \mathrm{AGL}_m(r)$. Furthermore, there is a bijection from $\{1, 2, \ldots, N_0\}$ to the set of points of $\mathbb{F}_r^m$, that identifies the action of G on $\{1, 2, \ldots, N_0\}$ with its natural action, as a subgroup of the group $\mathrm{AGL}_m(r)$ of all affine transformations of $\mathbb{F}_r^m$, on the set of points of $\mathbb{F}_r^m$.*

Proof. The irreducibility of $\Psi|_G$ is equivalent to that G be a doubly transitive permutation subgroup of S_{N_0}. We will apply the classification of finite doubly transitive permutation groups [Cam, Theorem 5.3], which is a consequence of the classification of finite simple groups. Now, if $S = \mathrm{soc}(G)$ is abelian then (iii) holds. So we will assume that S is non-abelian, whence it is a simple group. As (i) holds if $S \cong \mathsf{A}_{N_0}$, we will also assume that $S \ncong \mathsf{A}_{N_0}$. Furthermore, as in the proof of Proposition 6.2, the assumption $n \geq 3$ implies that $N_0 - 1$ cannot be a prime power. Direct computation shows that $N_0 \neq 11$, 22, 23, 36, 176, 276. Finally, assume we are in the case where $S \cong \mathrm{Sp}_{2m}(2)$ and $N_0 = 2^{m-1}(2^m \pm 1)$ for some $m \geq 4$. In this case, if $g \in G$ has simple spectrum, then the order of $g\mathbf{Z}(G)$, as an element of $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$, is at most 2^{m+1} by [GMPS, Theorem 2.16], which is smaller than $\deg(\Psi) = N_0 - 1$, a contradiction. It now follows from [Cam, Theorem 5.3] that (ii) holds. □

Remark 6.7. One may wonder if case (ii) of Theorem 6.6 may occur for some s coprime to q. One such occurrence is $2^5 - 1 = (5^3 - 1)/4$, and a computation on Mathematica reveals that this is the only occurence when $(p^a - 1)/(p - 1) = (r^b - 1)/(r - 1)$ for some distinct primes $p, r \leq 1223$ and $2 \leq a, b \leq 200$. If one relaxes the primeness condition, then this equation is known in literature as the *Goormaghtigh equation*, and the only other known solution is $2^{13} - 1 = (90^3 - 1)/89$.

On the other hand, for any given $n \geq 2$, $(q^n - 1)/(q - 1)$ can be a prime power, or even a prime; in fact, the *Bateman–Horn conjecture* [BH] implies in particular that this can happen infinitely often.

The main result of this section is the following theorem:

Theorem 6.8. *Let $q = p^f$ be a power of a prime p, $n \geq 3$, and $N := q^n - 1$. Let $G \leq \mathsf{S}_N$ be a subgroup with the following properties:*

(a) *If Φ denotes the representation of S_N on its natural permutation module $\mathbb{C}^N$, then*

$$\Phi|_G = \oplus_{i=0}^{q-2}\Phi_i \oplus 1_G,$$

where $\Phi_i \in \mathrm{Irr}(G)$ has degree $(q^n - 1)/(q - 1) - \delta_{i,0}$;

(b) *$G_0 := \Phi_0(G)$ embeds in S_{N_0}, where $N_0 := (q^n - 1)/(q - 1)$, in such a way that Φ_0 is the restriction to G_0 of the representation of S_{N_0} on its deleted permutation module $\mathbb{C}^{N_0-1}$. Furthermore, $\Phi_0(G)$ contains an element of order N_0 with simple spectrum and a p-subgroup of order q^{n-1}.*

(c) *For every $g \in G$, $\mathrm{Tr}(\Phi(g)) + 1$ is a q-power.*

Then $\mathrm{SL}(W) \cong L := G^{(\infty)} \lhd G \leq \mathrm{GL}(W)$ for $W = \mathbb{F}_q^n$. Moreover, $\Phi|_G$ is equivalent to the permutation action of G on the set Ω of nonzero vectors of W.

Proof. (i) Let φ, respectively φ_i, denote the character of Φ, respectively Φ_i. Also, let K denote the kernel of Φ_0, so that $G/K \cong G_0$. Note by (a) and faithfulness of Φ that $K = 1$ if $q = 2$. Since the trivial representation of G occurs with multiplicity exactly one in $\Phi|_G$ by (a), G is a transitive subgroup of S_N. Hence K acts semi-transitively on Ω, that is, all K-orbits have the same length, say k. As $K = \mathrm{Ker}(\Phi_0)$, we have

$$k = [\varphi|_K, 1_K]_K \geq 1 + \dim(\Phi_0) = N_0.$$

On the other hand, $\varphi(x) \leq q^{n-1} - 1$ for all $1 \neq x \in K$ by (c). It follows that

$$\frac{q^n - 1}{q - 1} \leq [\varphi|_K, 1_K]_K \leq \frac{(q^n - 1) + (q^{n-1} - 1)(|K| - 1)}{|K|},$$

and so

$$|K| \leq \frac{q^{n-1}(q - 1)^2}{(q^n - 1) - (q^{n-1} - 1)(q - 1)} < (q - 1)^2. \tag{6.8.1}$$

(ii) Now we use (b) and Theorem 6.6 (applied to $\Psi = \Phi_0$) to determine G_0. Suppose we are in the affine case 6.8(iii), that is $N_0 = r^m$ for some prime r and $C_r^m \cong \mathrm{soc}(G_0) \lhd G_0 \leq \mathrm{AGL}_m(r)$. If $m \geq 2$ and $(m, r) \neq (2, 2)$, then G_0 does not contain any element of order r^m by Lemma 6.5, and this contradicts (b). The case $(q^n - 1)/(q - 1) = 2^2$ is ruled out since $n \geq 3$.

Finally, assume that $m = 1$, so that $r = (q^n - 1)/(q - 1)$. Since $G_0 \leq \mathrm{AGL}_1(r)$ is a doubly transitive subgroup of S_r, we actually have

$$G_0 = \mathrm{AGL}_1(r) \cong C_r \rtimes C_{r-1}. \tag{6.8.2}$$

As $n \geq 3$, we have by (6.8.1) that $|K| < r$, whence

$$|G|_r = |G_0|_r = r. \tag{6.8.3}$$

If $q = 2$, then we have $r = 2^n - 1 \geq 7$ and $r - 1 = 2^n - 2 \equiv 2 (\mathrm{mod}\, 4)$. As $K = 1$ in this case, we have that $|G|_2 = |G_0|_2 = 2$, and so the Sylow 2-subgroups of G have order 2. On the other hand, G contains a subgroup P of order $2^{n-1} \geq 4$ by (b), a contradiction. Hence we may assume $q \geq 3$ in the affine case.

Let $\bar{g}$ be a generator of $\mathbf{O}_r(G_0) \cong C_r$ and let $g \in G$ be an inverse image of order r of $\bar{g}$. Recall by (6.8.2) that any power $g^i \neq g$ is conjugate to g in $G/K = G_0$. But K is a normal r'-subgroup of G, hence any such $g^i \neq g$ is also conjugate to g in G by [TZ2, Lemma 4.11]. Thus $\mathbf{N}_G(\langle g \rangle)$ acts transitively on $\langle g \rangle \smallsetminus \{1\}$ and so also on the $r - 1$ nontrivial irreducible characters of $\langle g \rangle$. It follows that any transitive permutation representation of $\mathbf{N}_G(\langle g \rangle)$ that is nontrivial on g has degree at least $r > |K|$. Applying this remark to the conjugation action of $\mathbf{N}_G(\langle g \rangle)$ on K, we conclude that g centralizes K.

Recall also that $\varphi_j(1) = N_0 = r$ for any $j > 0$, hence φ_j has r-defect 0 by (6.8.3). It follows that $\varphi_j(g) = 0$ and $\Phi_j(g)$ is conjugate to $\mathrm{diag}(1, \epsilon, \epsilon^2, \ldots, \epsilon^{r-1})$ (over $\mathbb{C}$) for a primitive r^{th} root of unity $\epsilon \in \mathbb{C}$. As K centralizes g, K fixes each of r one-dimensional eigenspaces of g in Φ_j, and so $(\Phi_j)|_K$ is a sum of one-dimensional representations. This holds for every $j > 0$, and also for $j = 0$ as $K = \mathrm{Ker}(\Phi_0)$. It follows by faithfulness of Φ that K is abelian. Now

$$K\langle g \rangle / K = \langle \bar{g} \rangle = \mathbf{O}_r(G_0) \lhd G_0,$$

whence $K\langle g \rangle$ is a normal subgroup of index $r - 1$ of G by (6.8.2). Also, $K\langle g \rangle$ is abelian, as K is abelian and $[g, K] = 1$. It follows by Ito's theorem [Is, (6.15)] that the degree of any irreducible character of G divides $r - 1$, and this contradicts the equality $\varphi_1(1) = r$.

(iii) We have ruled out the affine case, and hence have that $S := \mathrm{soc}(G_0)$ is a non-abelian simple group. By Theorem 6.6, we know that $S = \mathsf{A}_{N_0}$ acting on N_0 points, or (up to an automorphism) $S = \mathrm{PSL}_m(s)$ acting on

$$N_0 = \frac{s^m - 1}{s - 1} = \frac{q^n - 1}{q - 1} \tag{6.8.4}$$

lines of $\mathbb{F}_s^m$. As in the proof of Proposition 6.2, (6.8.4) and $n \geq 3$ imply that $m \geq 3$.

Here we handle the case $q = 2$; in particular, $K = 1$ and $G = G_0$. If $S = \mathsf{A}_{N_0}$, then we can take $x \in S$ to be a $(N_0 - 2)$-cycles, for which we have $\varphi(x) + 1 = 3$, contradicting (c). Hence $S = \mathrm{PSL}_m(s)$ and (6.8.4) holds. Applying Proposition 6.2 to $\psi := \varphi|_S + 1_S$, we see that $(m, s) = (n, q)$, that is, $\mathrm{soc}(G) = \mathrm{SL}_n(2)$, and the statement follows.

(iv) From now on we may assume $q \geq 3$; in particular, $N_0 \geq 13$ and $N_0 \neq 15$, whence $m \geq 3$ and $(m, s) \neq (3, 2)$, $(4, 2)$ in (6.8.4). Let $P(S)$ denote the smallest integer among the indices of proper subgroups of S. By [KlL, Table 5.2.A],

$$P(S) = N_0 > (q - 1)^2 > |K|. \tag{6.8.5}$$

Furthermore, using [GT, Lemma 6.1], [TZ1, Theorem 3.1], and also [Atlas] when $S = \mathrm{PSL}_3(4)$ and $\mathrm{PSL}_4(3)$, we see that

(6.8.6) Any nontrivial projective irreducible complex representation of S of degree dividing N_0 is a linear representation of $\hat{S}$ of degree N_0,

moreover, such a representation exists only when $S = \mathrm{PSL}_m(s)$, in which case $\hat{S} = \mathrm{SL}_m(s)$.

(v) Recalling $S = \mathrm{soc}(G_0)$, we let $M > K$ be the normal subgroup of G such that $M/K = S$. Certainly, K fixes every irreducible character of K. Now, (6.8.5) implies that the permutation action of M on $\mathrm{Irr}(K)$ is trivial, that is, every $\alpha \in \mathrm{Irr}(K)$ is M-invariant.

Let $i > 0$ and let α be any irreducible constituent of $(\varphi_i)|_M$. By the previous result and by Clifford's theorem, $\alpha|_K = c\gamma$ for some $c \in \mathbb{Z}_{\geq 1}$ and $\gamma \in \mathrm{Irr}(K)$. Again by Clifford's theorem, there is some projective irreducible complex representation Θ of S of degree c, and note that c divides $\varphi_i(1) = N_0$. Hence, by (6.8.6), $c = 1$ or $c = N_0$.

Suppose we are in the former case: $c = 1$. Then $\alpha(1) = \gamma(1) \leq \sqrt{|K|}$, whence $\alpha(1) < q - 1$ by (6.8.1). On the other hand,

$$\varphi_1(1)/\alpha(1) \leq [G : M] = |G_0/S|.$$

If $S = \mathsf{A}_{N_0}$, then we get $(q^n - 1)/(q - 1) = \varphi_i(1) < 2(q - 1)$, a contradiction since $n \geq 3$. Thus $S = \mathrm{PSL}_m(s)$ with $m \geq 3$. Since G_0 is acting doubly transitively on N_0 lines and has socle S, we have that $|G_0/S| \leq \gcd(m, s - 1)e$, if $s = r^e$. It follows that

$$N_0 = \frac{s^m - 1}{s - 1} < (q - 1) \cdot \gcd(m, s - 1)e. \tag{6.8.7}$$

The assumption $n \geq 3$ implies that $q - 1 < \sqrt{N_0}$. If $m \geq 5$, then

$$\gcd(m, s - 1)e \leq s(s - 1)/2 < \sqrt{(s^m - 1)/(s - 1)} = \sqrt{N_0},$$

contradicting (6.8.7). If $m = 4$, then as $s \geq 3$ we have

$$\gcd(m, s - 1)e \leq 4(s/2) = 2s < \sqrt{(s^4 - 1)/(s - 1)} = \sqrt{N_0},$$

again a contradiction. Suppose $m = 3$. If $s \neq 4, 8$, then $s = r^e \geq 3e$ and so

$$\gcd(m, s - 1)e \leq 3(s/3) = s < \sqrt{(s^3 - 1)/(s - 1)} = \sqrt{N_0},$$

again a contradiction. We also reach a contradiction with (6.8.7) when $s = 2, 8$. In the remaining case $(m, s) = (3, 4)$, whence $N_0 = 21$, implying that $(n, q) = (3, 4)$ and (6.8.7) is violated again.

We have shown that $c = N_0$, and so $\gamma(1) = \alpha(1)/c \leq 1$. Thus every irreducible constituent of each $(\varphi_i)|_K$ has degree 1 when $i > 0$. The same holds for $i = 0$ as $K = \mathrm{Ker}(\Phi_0)$. Thus every irreducible constituent of $\Phi|_K$ has degree 1, whence K is abelian since Φ is faithful. Now M acts on K via conjugation, with K acting trivially. Using (6.8.5), we conclude that M acts trivially on K, i.e. $K \leq \mathbf{Z}(M)$. Also, we have shown that $\alpha(1) = N_0$, i.e. $(\Phi_i)|_M$ is irreducible.

(vi) Now we consider $L := G^{(\infty)}$. Certainly, $L \lhd M$ (as $S \lhd G_0 \leq \mathrm{Aut}(S)$), and so $K \cap L \leq \mathbf{Z}(L)$. Also, since S is simple, we must have that S is a composition factor of L, whence $KL = M$ and $L/(K \cap L) = KL/K = M/K \cong S$. Thus L is a cover of S.

As $KL = M$ and $K = \mathrm{Ker}(\Phi_0)$, $(\Phi_0)|_L$ is irreducible of degree $N_0 - 1$. Next, recall that for $i > 0$, $(\Phi_i)|_M$ is irreducible of degree N_0, and $K \leq \mathbf{Z}(M)$ acts via scalars in Φ_i. Let d_i denote the common degree of irreducible constituents Φ_{ij} of $(\Phi_i)|_L$. If $d_i = 1$, then $\Phi_{ij} = 1_L$ as L is perfect. Thus $(\Phi_i)|_L$ is trivial, and so Φ_i cannot be irreducible over $M = KL$. So $d_i > 1$ and Φ_{ij} is a nontrivial irreducible projective representation of S. By (6.8.6), $d_i = N_0$, $S = \mathrm{PSL}_m(s)$, and $(\Phi_i)|_L$ comes from a linear irreducible representation of $\hat{S} = \mathrm{SL}_m(s)$. The same is true for $i = 0$. Ignoring the faithfulness of Φ (only in this paragraph of the proof), we may therefore replace L by $\hat{S} = \mathrm{SL}_m(s)$.

Applying [TZ1, Theorem 3.1], we see that each $(\Phi_i)|_L$ is a Weil representation. Now we can apply Proposition 6.2 to $\psi = \varphi|_L + 1_L$ to obtain that $(m,s) = (n,q)$, that is $L = \mathrm{SL}_n(q)$. We then apply Theorem 6.1 to the same ψ to conclude that $\psi = \tau_n$, the total Weil character of L. As τ_n is faithful, we also see that $G^{(\infty)} = \mathrm{SL}_n(q)$.

Recall that $K = \mathrm{Ker}(\Phi_0)$ centralizes L and that Φ_0 embeds G/K in S_{N_0}. As $n \geq 3$, we see that no element of G can induce a graph automorphism of L (modulo the inner, diagonal, and field automorphisms). Next, the diagonal automorphisms of L fix each of τ_n^i, but no nontrivial field automorphism can fix τ_n^1 (the one corresponding to a faithful character of $\mathbf{Z}(\mathrm{GL}_n(q))$ when we extend τ_n to $\mathrm{GL}_n(q)$). Thus G can induce only inner and diagonal automorphisms of L, that is,

$$G/\mathbf{C}_G(L) \leq \mathrm{PGL}_n(q). \tag{6.8.8}$$

We now return to the assumption that $G \leq \mathsf{S}_N$ with $N = q^n - 1$. Since $\varphi|_L = \tau_n - 1_L$, we see that $L = \mathrm{SL}_n(q)$ acts transitively in the natural permutation action of S_N. Applying Lemma 6.4(ii), we see that (after twisting with the inverse-transpose automorphism, equivalently, replacing W by the dual module, if necessary), this is the permutation action of L on the set Ω of nonzero vectors of $W = \mathbb{F}_q^n$. Consider any $h \in G$. By (6.8.8), the conjugation by h induces an inner-diagonal automorphism of $L = \mathrm{SL}(W)$. On the other hand, the action of L on Ω extends to the natural action of $\mathrm{GL}(W)$ on Ω. Hence we can find $h' \in \mathrm{GL}(W) < \mathsf{S}_N$ such that h and h' induce the same automorphism of L. Thus $(h')^{-1}h \in \mathsf{S}_N$ centralizes L, whence it belongs to $\mathrm{GL}(W)$ by Lemma 6.3. We conclude that $h \in \mathrm{GL}(W)$, i.e. $G \leq \mathrm{GL}(W)$. □

7. Weil representations of $\mathrm{SL}_2(q)$

As before, let $q = p^f$ be a power of a prime p, and let $L := \mathrm{SL}(W) \cong \mathrm{SL}_2(q)$ for $W = \mathbb{F}_q^2$. To deal with the case $n = 2$, we will need some more technical results, which are also interesting in their own right.

Lemma 7.1. *Let $V = \mathbb{C}^{q^2}$ and let $\Phi : G \to \mathrm{GL}(V)$ be a faithful representation such that*
(a) $\mathrm{Tr}(\Phi(g)) \in \{1, q, q^2\}$ *for all* $g \in G$.
(b) $\Phi \cong \oplus_{i=0}^{q-2}\Phi_i \oplus 2 \cdot 1_G$, *where the* $\Phi_i \in \mathrm{Irr}(G)$ *are pairwise inequivalent and nontrivial.*
Then $|G| = |\mathrm{GL}_2(q)|$.

Proof. Let $a := \#\{g \in G \mid \mathrm{Tr}(\Phi(g)) = q\}$ and let $b := \#\{g \in G \mid \mathrm{Tr}(\Phi(g)) = 1\}$, so that $|G| = a + b + 1$ by (a). The assumption (b) implies that

$$2 = [\varphi, 1_G]_G = \frac{q^2 + aq + b}{a + b + 1},\ q + 3 = [\varphi, \varphi]_G = \frac{q^4 + aq^2 + b}{a + b + 1},$$

if $\varphi = \mathrm{Tr}(\Phi)$. Solving for a and b, we obtain $a = q^3 - 2q - 1$, $b = q^4 - 2q^3 - q^2 + 3q$, and so $|G| = (q^2 - 1)(q^2 - q) = |\mathrm{GL}_2(q)|$. □

The total Weil character $\tau_2 = \tau_{2,q}$ of $\mathrm{GL}_2(q)$, cf. (6.0.1), decomposes as $2 \cdot 1_{\mathrm{GL}_2(q)} + \sum_{i=0}^{q-2} \tau_2^i$, with $\tau_2^i \in \mathrm{Irr}(\mathrm{GL}_2(q))$ of degree $q+1-\delta_{i,0}$ and pairwise distinct. The smaller-degree character τ_2^0 restricts to the Steinberg character St of L. Furthermore, if $1 \leq i \leq (q-2)/2$ then τ_2^i and τ_2^{q-1-i} restrict to the same irreducible character (denoted χ_i in [Do, §38]) of $L = \mathrm{SL}_2(q)$, and those $\lfloor (q-2)/2 \rfloor$ characters are pairwise distinct. If $2 \nmid q$, then $(\tau_2^{(q-1)/2})|_L$ is the sum of two distinct irreducible characters (denoted ξ_1, ξ_2 in [Do, §38]) of degree $(q+1)/2$. We will refer to these characters St, χ_i, and also ξ_1, ξ_2 when $2 \nmid q$, as *irreducible Weil characters* of $\mathrm{SL}_2(q)$, and τ_2 (or rather $(\tau_2)|_L$) as the *total Weil character* of $\mathrm{SL}_2(q)$.

Now we prove an analogue of Theorem 6.1 for $\mathrm{SL}_2(q)$.

Theorem 7.2. *Let p be any prime, q be any power of p, $q \geq 4$, and let $L = \mathrm{SL}_2(q)$. Suppose ψ is a reducible complex character of L such that*

(a) $\psi(1) = q^2$;
(b) $\psi(g) \in \{q^i \mid 0 \leq i \leq 2\}$ *for all* $g \in L$;
(c) $[\psi, 1_L]_L = 2$; *and*
(d) *every irreducible constituent of* $\psi - 2 \cdot 1_L$ *is among the irreducible Weil characters* St, χ_i, $0 \leq i \leq (q-2)/2$, *and also* ξ_1, ξ_2 *when* $2 \nmid q$, *of* L.

Then ψ is the total Weil character τ_2 of L.

Proof. (i) We will use the character tables of $\mathrm{SL}_2(q)$, Theorem 38.1 of [Do] for $2 \nmid q$ and Theorem 38.2 of [Do] for $2|q$. Write

$$\psi = \begin{cases} 2 \cdot 1_L + a \cdot \mathsf{St} + \sum_{i=1}^{(q-3)/2} b_i \chi_i + c_1 \xi_1 + c_2 \xi_2, & 2 \nmid q, \\ 2 \cdot 1_L + a \cdot \mathsf{St} + \sum_{i=1}^{(q-2)/2} b_i \chi_i, & 2|q, \end{cases} \tag{7.2.1}$$

with all coefficients $a, b_i, c_i \in \mathbb{Z}_{\geq 0}$. Evaluating ψ at an element x of order $q+1$, we see by (b) that $\psi(y) = 2 - a \leq 2$ is a q-power, which is possible only when $a = 1$, since $q \geq 3$. As before, let $\tilde{\delta}$ denote a primitive $(q-1)^{\text{th}}$ root of unity in $\mathbb{C}$.

First suppose that $2|q$. Then $\sum_i b_i = (q^2 - q - 2)/(q+1) = q - 2$ by degree comparison in (7.2.1). Next, we fix an element $y \in L$ of order $q-1$, and for $1 \leq l \leq (q-3)/2$ we have

$$\psi(y^l) = 3 + \sum_{i=1}^{(q-2)/2} b_i \big(\tilde{\delta}^{il} + \tilde{\delta}^{-il}\big).$$

It follows that

$$\sum_{l=1}^{(q-2)/2} \psi(y^l) = 3(q-2)/2 + \sum_{i=1}^{(q-2)/2} b_i \Big(\sum_{l=1}^{(q-2)/2} \big(\tilde{\delta}^{il} + \tilde{\delta}^{-il}\big) \Big) = 3(q-2)/2 - \sum_{i=1}^{(q-2)/2} b_i = (q-2)/2.$$

As each $\psi(y^l)$ is a q-power, we must have that $\psi(y^l) = 1$ for all $1 \leq l \leq (q-2)/2$. Thus, the polynomial

$$f(t) = \sum_{i=1}^{(q-2)/2} b_i \big(t^{q-1-i} + t^i\big) + 2 \in \mathbb{Q}[t]$$

of degree $q-2$ has all $\tilde{\delta}^l$, $1 \leq l \leq q-2$ as roots. Since $f(1) = 2\sum_{i=1}^{(q-2)/2} b_i + 2 = 2q - 2$, we conclude that $f(t) = 2(t^{q-1} - 1)/(t-1)$, i.e. $b_i = 2$ for all i, and so $\psi = \tau_2$, as stated.

(ii) Assume now that $2 \nmid q$. Then $\sum_i b_i + (c_1 + c_2)/2 = (q^2 - q - 2)/(q+1) = q - 2$ by degree comparison in (7.2.1). Evaluating ψ at an element $u \in L$ of order p and another element $v \in L$ of order p that is not conjugate to u, we obtain

$$\psi(u) = 2 + \sum_i b_i + \frac{c_1 + c_2}{2} + \sqrt{\epsilon q}\frac{c_1 - c_2}{2},\ \psi(v) = 2 + \sum_i b_i + \frac{c_1 + c_2}{2} - \sqrt{\epsilon q}\frac{c_1 - c_2}{2},$$

where $\epsilon := (-1)^{(q-1)/2}$. Thus $\psi(u) + \psi(v) = 2q$. As each of $\psi(u)$, $\psi(v)$ is a q-power, we must have that $\psi(u) = q$, whence $c_1 = c_2 =: c$, and so

$$\sum_{i=1}^{(q-3)/2} b_i + c = q - 2.$$

Next we evaluate ψ at the central involution $\mathbf{j}$ of L:

$$\psi(\mathbf{j}) = 2 + q + (q+1)\sum_i b_i(-1)^i + c\epsilon(q+1).$$

In particular,

$$q^2 - \psi(\mathbf{j}) = \psi(1) - \psi(\mathbf{j}) = 2(q+1)\big(\sum_{2\nmid i} b_i + \frac{1-\epsilon}{2}c\big)$$

is divisible by $2(q+1)$. On the other hand, $\psi(\mathbf{j}) \in \{1, q, q^2\}$, so $\psi(\mathbf{j}) \neq q$, and either

$$\psi(\mathbf{j}) = q^2,\ \sum_{2\nmid i} b_i + \frac{1-\epsilon}{2}c = 0,\ \sum_{2|i} b_i + \frac{1+\epsilon}{2}c = q-2, \tag{7.2.2}$$

or

$$\psi(\mathbf{j}) = 1,\ \sum_{2\nmid i} b_i + \frac{1-\epsilon}{2}c = \frac{q-1}{2},\ \sum_{2|i} b_i + \frac{1+\epsilon}{2}c = \frac{q-3}{2}. \tag{7.2.3}$$

As above, we fix an element $y \in L$ of order $q-1$, and for $1 \leq l \leq (q-3)/2$ we then have

$$\psi(y^l) = 3 + \sum_{i=1}^{(q-3)/2} b_i\big(\tilde{\delta}^{il} + \tilde{\delta}^{-il}\big) + 2c(-1)^l.$$

It follows that

$$\begin{aligned}\sum_{l=1}^{(q-3)/2}\psi(y^l) &= 3(q-3)/2 + \sum_{i=1}^{(q-3)/2} b_i\Big(\sum_{l=1}^{(q-3)/2}\big(\tilde{\delta}^{il} + \tilde{\delta}^{-il}\big)\Big) + 2c\sum_{l=1}^{(q-3)/2}(-1)^l \\ &= 3(q-3)/2 + \sum_{i=1}^{(q-2)/2} b_i\big(-1-(-1)^i\big) - c(1+\epsilon) \\ &= 3(q-3)/2 - 2\big(\sum_{2|i} b_i + c(1+\epsilon)/2\big).\end{aligned}$$

In the case of (7.2.2), $1 \leq \sum_l \psi(y^l) = 3(q-3)/2 - 2(q-2) = (5-q)/2 \leq 0$, a contradiction. Hence (7.2.3) holds, and we have that $\sum_{l=1}^{(q-3)/2}\psi(y^l) = 3(q-3)/2 - (q-3) = (q-3)/2$. As each $\psi(y^l)$ is a q-power, we must have that $\psi(y^l) = 1$ for all $1 \leq l \leq (q-3)/2$. Thus, the polynomial

$$g(t) = \sum_{i=1}^{(q-3)/2} b_i\big(t^{q-1-i} + t^i\big) + 2ct^{(q-1)/2} + 2 \in \mathbb{Q}[t]$$

of degree $q-2$ has all $\tilde{\delta}^l \neq \pm 1$, $0 \leq l \leq q-2$, as roots, and so $g(t) = (at+b)(t^{q-1}-1)/(t^2-1)$ for some $a, b \in \mathbb{Q}$. Since $b = g(0) = 2$ and $(a+b)(q-1)/2 = g(1) = 2\sum_{i=1}^{(q-3)/2} b_i + 2c + 2 = 2q-2$, we conclude that $a = b = 2$, $g(t) = 2(t^{q-1}-1)/(t-1)$, i.e. $b_i = 2$ for all i and $c_1 = c_2 = 1$, and so $\psi = \tau_2$, as stated. □

Recall that a subgroup Y of a group X is a *characteristic subgroup* of X, Y **char** X, if $\phi(Y) \leq Y$ for all $\phi \in \mathrm{Aut}(X)$.

Proposition 7.3. *Let $q \geq 4$ be a prime power and let X be a finite group with a normal subgroup K of order dividing $q-1$ such that $X/K \cong S := \mathrm{PSL}_2(q)$. Then the following statements hold.*

(i) K **char** X.

(ii) *X contains a characteristic subgroup D such that D is quasisimple and $D/\mathbf{Z}(D) \cong S$.*

Proof. First we prove (i). Consider any $\phi \in \mathrm{Aut}(X)$. Then $\phi(K) \lhd X$ and so $\phi(K)K/K$ is a normal subgroup of S of order dividing $q-1$. As S is simple of order $> q-1$, $\phi(K) = K$, and so K **char** X.

To prove (ii), we proceed by induction on $|K|$, with the induction base being trivial. For the induction base, as usual let $P(S)$ denote the smallest index of proper subgroups of $S = \mathrm{PSL}_2(q)$. By [KlL, Table 5.2.A],

$$P(S) \geq q > |K|, \tag{7.3.1}$$

unless $q = 9$, for which we have $P(S) = 6$.

(a) First we consider the case where K is abelian. We claim that

$$K \leq \mathbf{Z}(X). \tag{7.3.2}$$

Indeed, K centralizes K, and so the conjugation induces a permutation action of $S = X/K$ on $K \smallsetminus \{1\}$, of size $q-2$. If $q \neq 9$, then (7.3.1) implies that any transitive permutation of S of degree less than q is trivial, and thus any S-orbit on K has length 1, and so $K \leq \mathbf{Z}(X)$ as stated. Consider the case $q = 9$ and suppose that $K \not\leq \mathbf{C}_X(K)$. Then $K \in \{C_2^3, C_4 \times C_2, C_8\}$, $\mathbf{C}_X(K) = K$ (as $X/K = S$ is simple), and $S = X/K$ embeds in $\mathrm{Aut}(K)$, which is either $\mathrm{SL}_3(2)$ or solvable. This is a contradiction, since $S = \mathrm{PSL}_2(9)$ is simple of order 360 and $|\mathrm{SL}_3(2)| = 168$.

Now we take $D := X^{(\infty)}$ **char** X. Then D has S as a composition factor, and so does KD, which contains K. Since $|K| < |S|$, S must be a composition factor of KD/K. It follows that $KD = X$, $D/(K \cap D) \cong KD/K = X/K = S$. Since $K \cap D \leq \mathbf{Z}(D)$ by (7.3.2), we see that D is a cover of S, as desired.

(b) Now we may assume K is non-abelian, in particular, $C := \mathbf{C}_X(K)$ is a proper characteristic subgroup of X, and $q \geq 7$. We aim to show that $KC = X$.

Consider the case $q = 9$. As K has order dividing 8 and K is non-abelian, K is D_8 (dihedral) or Q_8 (quaternion). In both cases, X/C embeds in $\mathrm{Aut}(K)$, which is solvable. As S is a quotient of X, it follows that S is a composition factor of C, and so the same holds for KC. As in (i), we infer from this that $KC = X$, as stated.

Suppose now that $q \neq 9$. As $C < K$, there exists some $1 \neq x \in K$ such that $Y := \mathbf{C}_X(x) < X$. Then $[X : Y] \leq |K| - 1 \leq q - 2$, and so $[S : KY/K] = [X : KY] \leq q - 2$. Hence (7.3.1) implies that $KY = X$. Now $K \cap Y$ is a normal subgroup of Y of order dividing $q - 1$, and $Y/(K \cap Y) \cong KY/K = X/K = S$. Note that $|K \cap Y| < |K|$, as otherwise $Y = X$, contradicting the choice of x. Hence we may apply the induction hypothesis to Y and find a characteristic subgroup R of Y that is a cover of S. As $q \neq 4, 9$, $R = S$, or $2 \nmid q$ and $R \cong L := \mathrm{SL}_2(q)$. Now, (7.3.1) shows that proper subgroups of S have index $\geq q$. The same also holds for L. (Assume the contrary: $M < L$ and $[L : M] < q$. Then $q > [L : MZ] = [S : MZ/Z]$ for $Z := \mathbf{Z}(L)$, and so $MZ = L$ by (7.3.1). As $M < L$ and $|Z| = 2$, we then have $M \cap Z = 1$, and $L = M \times Z$, a contradiction.) Thus in either case proper subgroups of R have index $\geq q$. As $|K| < q$, this implies that all R-orbits on K have length 1, i.e. $R \leq C$. Now R, and so KR, admits S as a composition factor. Arguing as above, we see that $X = KR = KC$.

(c) We have shown that $KC = X$ for a proper characteristic subgroup C that does not contain K. It follows that $|K \cap C| < |K|$, $C/(K \cap C) \cong KC/K = X/K = S$. By the induction hypothesis applied to C, C contains a subgroup D **char** C that is a cover of S. As C **char** X, we conclude that D **char** X, as desired. □

Now we can prove the main result of this section:

Theorem 7.4. *Let $q = p^f \geq 4$ be a power of a prime p, and $N := q^2 - 1$. Let $G \leq \mathsf{S}_N$ be a subgroup with the following properties:*

(a) *If* Φ *denotes the representation of* S_N *on its natural permutation module* $\mathbb{C}^N$*, then*

$$\Phi|_G = \oplus_{i=0}^{q-2}\Phi_i \oplus 1_G,$$

where $\Phi_i \in \mathrm{Irr}(G)$ *have degree* $q+1-\delta_{i,0}$ *and all pairwise inequivalent.*

(b) $G_0 := \Phi_0(G)$ *embeds in* S_{q+1} *as the subgroup* $\mathrm{PGL}_2(q)$ *acting on* $N_0 := q+1$ *lines of* $\mathbb{F}_q^2$*, in such a way that* Φ_0 *is the restriction to* G_0 *of the representation of* S_{q+1} *on its deleted permutation module* $\mathbb{C}^q$*.*

(c) *For every* $g \in G$*,* $\mathrm{Tr}(\Phi(g))+1$ *is a* q*-power.*

Then $G \cong \mathrm{GL}(W) = \mathrm{GL}_2(q)$ *for* $W = \mathbb{F}_q^2$*. Moreover,* $\Phi|_G$ *is equivalent to the permutation action of* G *on the set* Ω *of nonzero vectors of* W*.*

Proof. (i) Let φ, respectively φ_i, denote the character of Φ, respectively Φ_i. Also, let K denote the kernel of Φ_0, so that $G/K \cong G_0$. By Lemma 7.1, $|G| = |\mathrm{GL}_2(q)|$, and by (b), $G_0 \cong \mathrm{PGL}_2(q)$. It follows that

$$|K| = q-1. \tag{7.4.1}$$

Let $S = \mathrm{soc}(G_0) \cong \mathrm{PSL}_2(q)$. Using [TZ1, Theorem 3.1], and also [Atlas] when $S = \mathrm{PSL}_2(9)$, we can check that

$$\begin{gathered}\text{Any nontrivial projective irreducible complex representation of } S\\ \text{of degree dividing } N_0 \text{ is a linear representation of } L := \mathrm{SL}_2(q)\\ \text{of degree } N_0, \text{ or } N_0/2 \text{ when } 2 \nmid q, \text{ or } N_0/3 \text{ when } q = 5.\end{gathered} \tag{7.4.2}$$

Let $M > K$ be the normal subgroup of G such that $M/K = S$; note that

$$|G/M| = \gcd(2, q-1) \tag{7.4.3}$$

as $G/K = G_0 \cong \mathrm{PGL}_2(q)$. By Proposition 7.3, M contains a subgroup D **char** M that is a cover of S. As $M \lhd G$, D is normal in G.

(ii) We also note that $KD = M$ (as $M/K \cong S$ and $S = D/\mathbf{Z}(D)$). Now, as $K = \mathrm{Ker}(\Phi_0)$, $(\Phi_0)|_D$ is irreducible of degree $N_0 - 1$.

Recall that, for any $i > 0$, Φ_i is irreducible of degree N_0. Let d_i denote the common degree of irreducible constituents Φ_{ij} of $(\Phi_i)|_D$. If $d_i = 1$, then $\Phi_{ij} = 1_D$ as D is perfect. Thus $(\Phi_i)|_D$ is trivial. So every irreducible constituent Ψ_{ij} of $(\Phi_i)|_M$ is now irreducible over K, and so has degree at most $\sqrt{q-1}$ by (7.4.1). Together with (7.4.3), this implies that $N_0 \le \sqrt{q-1}\cdot\gcd(2,q-1) < q+1$, a contradiction. Thus $d_i > 1$.

In the case $q = 5$, $|K| = 4$, hence K is abelian, and part (a) of the proof of Proposition 7.3 shows that we can take $D = M^{(\infty)} = G^{(\infty)}$ (with the second equality following from (7.4.3)) and that $K \le \mathbf{Z}(M)$. Thus K acts via scalars on Φ_i. Now, (7.4.3) shows that every Ψ_{ij} has degree N_0 or $N_0/2$ and it is irreducible over D, as $M = KD$. Thus $d_i = N_0$ or $N_0/2$ in this case.

Using (7.4.2) for $q \ne 5$, we now see that $d_i = N_0/2$ or N_0, and that every irreducible constituent of $(\Phi_i)|_D$ comes from a linear irreducible representation of $L = \mathrm{SL}_2(q)$. The same is true for $i = 0$. Ignoring the faithfulness of Φ (only in this paragraph of the proof), we may therefore replace D by $L = \mathrm{SL}_2(q)$. Applying [TZ1, Theorem 3.1], we see that each $(\Phi_i)|_L$ is a sum of irreducible Weil representations. Now we can apply Theorem 7.2 to $\psi = \varphi|_L + 1_L$ to conclude that $\psi = \tau_2$, the total Weil character of L. As τ_2 is faithful, we also see that $D = \mathrm{SL}_2(q)$.

(iii) As $q \ge 4$, at least one irreducible constituent of degree N_0 of τ_2 (χ_i in the notation of Theorem 7.2, and which corresponds to a faithful character of $\mathbf{Z}(\mathrm{GL}_2(q))$ when we extend χ_i to $\mathrm{GL}_2(q)$), is fixed by diagonal automorphisms but not by any nontrivial field automorphism of D. Thus G can induce only inner and diagonal automorphisms of D, that is,

$$G/\mathbf{C}_G(D) \le \mathrm{PGL}_2(q). \tag{7.4.4}$$

We now return to the assumption that $G \le \mathsf{S}_N$ with $N = q^2 - 1$. Since $\varphi|_D = \tau_2 - 1_D$, we see that $D = \mathrm{SL}_2(q)$ acts transitively in the natural permutation action of S_N. Applying Lemma 6.4(ii), we see that this is the permutation action of D on the set Ω of nonzero vectors of $W = \mathbb{F}_q^2$. Consider any $h \in G$. By (7.4.4), the conjugation by h induces an inner-diagonal automorphism of $L = \mathrm{SL}(W)$. On the other hand, the action of L on Ω extends to the natural action of $\mathrm{GL}(W)$ on Ω. Hence we can find $h' \in \mathrm{GL}(W) < \mathsf{S}_N$ such that h and h' induce the same automorphism of L. Thus $(h')^{-1}h \in \mathsf{S}_N$ centralizes L, whence it belongs to $\mathrm{GL}(W)$ by Lemma 6.3. We conclude that $h \in \mathrm{GL}(W)$, i.e. $G \le \mathrm{GL}(W) \cong \mathrm{GL}_2(q)$. Since $|G| = |\mathrm{GL}_2(q)|$, we have that $G = \mathrm{GL}(W)$, as stated. □

8. The structure of monodromy groups

Theorem 8.1. *Let q be a power of a prime p, $n \ge 2$, $q \ge 4$ when $n = 2$, and let K be an extension of $\mathbb{F}_q$. Then for the geometric and arithmetic monodromy groups G_{geom} and G_{arith} of the local system $\mathcal{W}(n,q)$ over $\mathbb{G}_m/K$ we have*

$$G_{\mathrm{geom}} = G_{\mathrm{arith}} \cong \mathrm{GL}_n(q),$$

with the groups acting on $\mathcal{W}(n,q) \otimes \overline{\mathbb{Q}_\ell} \cong F_\star \overline{\mathbb{Q}_\ell}$ as in its natural permutation action on the set Ω of nonzero vectors of the natural module $\mathbb{F}_q^n$.

Proof. (i) Let G denote either of G_{geom} and G_{arith} when $n \ge 3$, and $G = G_{\mathrm{geom}}$ when $n = 2$, and let Φ denote the representation of G on $\mathcal{W}(n,q) \otimes \overline{\mathbb{Q}_\ell}$. By Corollary 4.6 and Lemma 5.1, G embeds in S_N for $N := q^n - 1$ in such a way that Φ extends to the representation of S_N on its natural permutation module $\mathbb{C}^N$ which we also denote by Φ.

Fix a character $\theta \in \mathsf{Char}(q-1)$ of order $q-1$ and let Φ_i denote the representation of G on $\mathcal{F}_{\theta^i}$. By Corollary 4.3 and Lemma 5.1, $\Phi_0(G)$ embeds in S_{N_0} for $N_0 := (q^n - 1)/(q-1) = A$ in such a way that Φ_0 extends to the representation of S_{N_0} on its deleted natural permutation module $\mathbb{C}^{N_0 - 1}$. By Lemma 4.1, $\mathcal{F}_{\mathbb{1}}$ is geometrically isomorphic to the hypergeometric sheaf $\mathcal{H}_{\mathbb{1}}$, whence $G \ge G_{\mathrm{geom}}$ is irreducible in Φ_0, and $\Phi_0(G)$ contains an element of order N_0 with simple spectrum (namely, the image of a generator of $I(0)$). Furthermore, $\Phi_0(G)$ contains a p-subgroup of order $A - B = q^{n-1}$ (namely, the image of $P(\infty)$). If in addition $n = 2$, then $\mathcal{H}_{\mathbb{1}}$ is the Gross $\mathrm{PGL}_2(q)$ local system considered in [KT1, §13], and so $G_0 = \mathrm{PGL}_2(q)$ (acting on $q+1$ lines of $\mathbb{F}_q^2$). Next, for any $1 \le i \le q-2$, by Lemma 4.1, $\mathcal{F}_{\theta^i}$ is geometrically isomorphic to the hypergeometric sheaf $\mathcal{H}_{\theta^i}$, whence $G \ge G_{\mathrm{geom}}$ is irreducible in Φ_i (which has degree N_0). Together with Theorem 4.8, this ensures that (G, Φ) fulfills all the conditions (a)–(c) of Theorem 6.8 if $n \ge 3$. Applying Theorem 6.8 when $n \ge 3$, we obtain

$$\mathrm{SL}_n(q) \lhd G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} \le \mathrm{GL}_n(q),$$

with the groups acting on $\mathcal{W}(n,q) \otimes \overline{\mathbb{Q}_\ell}$ as in its natural permutation action on the set Ω of nonzero vectors of the natural module $W = \mathbb{F}_q^n$.

When $n = 2$, we also apply Lemma 1.1 to see that the representations Φ_i of G have distinct determinants and so are pairwise inequivalent for $0 \le i \le q-2$, and thus we have fulfilled all the conditions (a)–(c) of Theorem 7.4. Applying Theorem 7.4, we obtain $G_{\mathrm{geom}} = \mathrm{GL}_2(q)$, again with the group acting on $\mathcal{W}(2,q) \otimes \overline{\mathbb{Q}_\ell}$ as in its natural permutation action on the set Ω of nonzero vectors of the natural module $W = \mathbb{F}_q^2$. Now applying Lemma 7.1 to $G = G_{\mathrm{arith}}$ we see that $|G_{\mathrm{arith}}| = |\mathrm{GL}_2(q)| = |G_{\mathrm{geom}}|$, and so $G_{\mathrm{arith}} = G_{\mathrm{geom}}$.

(ii) It remains to show that $G_{\mathrm{geom}} = \mathrm{GL}_n(q)$ when $n \ge 3$. Here, $L := \mathrm{SL}_n(q)$ is perfect, whence $\Phi_i(L)$ is trivial. Note that

$$\mathrm{GL}_n(q) = \langle L, g \rangle, \tag{8.1.1}$$

for a regular semisimple element g of order q^n-1, which acts on Ω cyclically and such that $z = g^{N_0} = \delta \cdot 1_W$ is a generator of $\mathbf{Z}(\mathrm{GL}_n(q))$. Indeed, we can identify $\mathbb{F}_q^n$ with $\mathbb{F}_{q^n}$ to embed $\mathrm{GL}_1(q^n) = \mathbb{F}_{q^n}^\times$ in $GL_n(q)$, and then take for g a generator $\mathbb{F}_{q^n}^\times$. Hence, if $\zeta = \zeta_N \in \mathbb{C}^\times$ is a primitive N^{th} root of unity, then $\Phi(g)$ has simple spectrum, consisting of all powers of ζ. Now $\Phi(z)$ admits all powers $\tilde{\delta}^j$ of $\tilde{\delta} = \zeta^{N_0}$, $0 \le j \le q-2$, as eigenvalues, each with multiplicity N_0. Hence the corresponding z-eigenspaces V_j are invariant under $\Phi(\mathrm{GL}_n(q))$. By the definition of Weil representations [T, (1.1)], V_0 is the direct sum of the trivial representation and an irreducible representation, whose character over L is τ_n^0, whereas each V_i with $i > 0$ is an irreducible representation, whose character over L is τ_n^j. Thus the actions of G_{geom} on V_0, $V_1, \dots, V_{q-2}$ are each equivalent to one of $\Phi_0 \oplus \mathbb{1}$, and Φ_i, $1 \le i \le q-2$.

We will choose θ so that $\theta(\det(g)) = \tilde{\delta}$ and view θ as a linear character of $\mathrm{GL}_n(q)$ (trivial on $\mathrm{SL}_n(q)$). Then g has determinant $(-1)^{A+1}\tilde{\delta}^j$ on V_j. It follows that $\mathrm{GL}_n(q)$ has determinant $\lambda_j := \theta^j(\chi_2)^{A+1}$ on V_j. Now letting $t := [\mathrm{GL}_n(q) : G_{\mathrm{geom}}]$, we have by (8.1.1) that $G_{\mathrm{geom}} = \langle L, g^t \rangle$ and that $t|(q-1)$. In particular, the image of the determinantal character of G_{geom} has index divisible by t in $\mu_{q-1} = \langle \tilde{\delta} \rangle < \mathbb{C}^\times$.

On the other hand, choosing $\chi := \theta$ if $2 \nmid A$, and $\chi := \theta\chi_2$ if $2|A$, we see by Lemma 1.1 that the determinant of G_{geom} on $\mathcal{H}_\chi$ is exactly $\mathcal{L}_\theta$, and so the determinantal image of G_{geom} on $\mathcal{H}_\chi$ is the (full) image μ_{q-1} of θ. Applying Lemmas 2.1 and 3.1, we see that the same is true for the determinantal image of G_{geom} on $\mathcal{F}_\chi$. This can happen only when $t = 1$. □

Corollary 8.2. *Let q be a power of a prime p, $n \ge 2$, $q \ge 4$ when $n = 2$, and let K be an extension of $\mathbb{F}_q$. Then, for any $\chi \in \mathsf{Char}(q-1)$, the geometric monodromy group $G_{\mathrm{geom},\chi}$ of the hypergeometric sheaf $\mathcal{H}_\chi$ over $\mathbb{G}_m/K$ is the image of $\mathrm{GL}_n(q)$ in one of its $q-1$ irreducible Weil representations, of degree $(q^n-1)/(q-1) - \delta_{\chi,\mathbb{1}}$, which are among the $q-1$ nontrivial irreducible constituents Φ_i, $0 \le i \le q-2$, of the permutation action of $\mathrm{GL}_n(q)$ on the set of nonzero vectors of $\mathbb{F}_q^n$. In particular, $G_{\mathrm{geom},\mathbb{1}} \cong \mathrm{PGL}_n(q)$.*

Proof. By Lemma 4.1, $\mathcal{H}_\chi$ is geometrically isomorphic to the summand $\mathcal{F}_\chi$ of $\mathcal{W}(n,q)$. Hence the first statement follows by applying Theorem 8.1, as $G_{\mathrm{geom},\chi}$ is now some $\Phi_i(G_{\mathrm{geom}})$, $0 \le i \le q-2$. Among the nontrivial irreducible constituents of the total Weil representation of $\mathrm{GL}_n(q)$, the deleted permutation action on the lines of $\mathbb{F}_q^n$ is the only one that has degree $(q^n-q)/(q-1) = \mathrm{rank}(\mathcal{H}_\mathbb{1})$, and this representation factors through $\mathrm{PGL}_n(q)$. Hence this representation must be realized by $\mathcal{H}_\mathbb{1}$, and the second statement follows. □

Recall that $\mathcal{W}(n,q)$ on $\mathbb{G}_m/\mathbb{F}_q$ is arithmetically isomorphic to the local system $F_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$, by Corollary 4.6. Next we determine the arithmetic monodromy group of $F_\star\overline{\mathbb{Q}_\ell}$ on $\mathbb{G}_m/K$ for K any subfield of $\mathbb{F}_q$.

Theorem 8.3. *Let $q = p^f$ be a power of a prime p, $n \ge 2$, $q \ge 4$ when $n = 2$, and let $K = \mathbb{F}_{q^{1/e}}$ be a subfield of $\mathbb{F}_q$ for $e|f$. Then for the arithmetic monodromy group $G_{\mathrm{arith},K}$ of the local system $F_\star\overline{\mathbb{Q}_\ell}$ on $\mathbb{G}_m/K$ we have*

$$G_{\mathrm{arith},K} \cong \mathrm{GL}_n(q) \rtimes C_e \le \mathrm{GL}_{ne}(K),$$

where the cyclic subgroup C_e can be identified with $\mathrm{Gal}(\mathbb{F}_q/K)$, and with the groups acting on $F_\star\overline{\mathbb{Q}_\ell}$ as in their natural permutation action on the set Ω of nonzero vectors of the natural module $\mathbb{F}_q^n$.

Proof. In the case $e = 1$ or $f = 1$, the statement follows from Theorem 8.1. Next, $G_{\mathrm{arith},K}$ is a normal subgroup of $G_{\mathrm{arith},\mathbb{F}_p}$ with cyclic quotient of order dividing f/e, and $G_{\mathrm{arith},\mathbb{F}_q} = \mathrm{GL}_n(q)$ is a normal subgroup of $G_{\mathrm{arith},K}$ with cyclic quotient of order dividing e. Hence it suffices to prove the statement for $e = f > 1$, that is when $K = \mathbb{F}_p$.

By Lemma 5.1, $G := G_{\mathrm{arith},\mathbb{F}_p}$ embeds in $\mathrm{Sym}(\Omega) = \mathsf{S}_N$ for $N := q^n - 1$ in such a way that the action of G on $F_\star\overline{\mathbb{Q}_\ell}$ extends to the representation Φ of S_N on its natural permutation module $\mathbb{C}^N$. Furthermore, G contains the geometric monodromy group $G_{\mathrm{geom}} = G_{\mathrm{arith},\mathbb{F}_q} = \mathrm{GL}_n(q)$ as a normal subgroup; in particular, $L := G^{(\infty)} \cong \mathrm{SL}_n(q)$, and

$$L \lhd G \le \mathbf{N}_{\mathsf{S}_N}(L).$$

Note that we can view $\mathbb{F}_q^n$ as $\mathbb{F}_p^{nf}$ and thus embed L acting on Ω in $\mathrm{GL}_{nf}(p)$ acting on the set $\Omega_{\mathbb{F}_p}$ of N nonzero vectors of $\mathbb{F}_p^{nf}$. This embedding shows that

$$\mathbf{N}_{\mathsf{S}_N}(L) \ge \mathrm{GL}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathrm{GL}_n(q) \rtimes C_f. \tag{8.3.1}$$

We claim that in fact equality holds in (8.3.1). Indeed, by Lemma 6.3, $\mathbf{C}_{\mathsf{S}_N}(L) < \mathrm{GL}_n(q)$. Hence, if equality does not hold in (8.3.1), then $n \ge 3$ and $\mathbf{N}_{\mathsf{S}_N}(L)$ contains an element h that induces the transpose-inverse automorphism of L. In particular, h sends a point stabilizer

$$\mathrm{Stab}_L(v) = \left\{ \begin{pmatrix} 1 & x \\ 0 & X \end{pmatrix} \mid X \in \mathrm{SL}_{n-1}(q),\ {}^t x \in \mathbb{F}_q^{n-1} \right\}$$

to another point stabilizer in L, namely $\mathrm{Stab}_L(h(v))$. However, since $n \ge 3$,

$$h(\mathrm{Stab}_L(v))h^{-1} = \left\{ \begin{pmatrix} 1 & 0 \\ y & Y \end{pmatrix} \mid Y \in \mathrm{SL}_{n-1}(q),\ y \in \mathbb{F}_q^{n-1} \right\}$$

does not fix any nonzero vector in $\mathbb{F}_q^n$, a contradiction.

It remains to show that $G = \mathbf{N}_{\mathsf{S}_N}(L)$. Assume the contrary: G has index $j > 1$ in $\mathbf{N}_{\mathsf{S}_N}(L)$. By the above results, we have $j|f$ and that

$$G = \mathrm{GL}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{p^j}) = \mathrm{GL}_{nf/j}(p^j) \cap \mathbf{N}_{\mathsf{S}_N}(L).$$

Restricting Φ down to G via $\mathrm{GL}_{nf/j}(p^j)$, we see that

$$\mathrm{Tr}(\Phi(x)) + 1 \text{ is a power of } p^j \text{ for all } x \in G. \tag{8.3.2}$$

Now we can find a prime divisor r of j, and apply Theorem 4.8(iii) to get an element $g \in G$ with $\mathrm{Tr}(\Phi(g)) + 1 = p^{f_0}$, where f_0 is the r'-part of f. This certainly contradicts (8.3.2). □

Corollary 8.4. *Let q be a power of a prime p, $n \ge 2$, $q \ge 4$ when $n = 2$, and let K be an extension of $\mathbb{F}_q$. Then, for any divisor d of $q-1$, the geometric monodromy group $G_{\mathrm{geom},d}$ of the $[d]^\star$ Kummer pullback of the local system $\mathcal{W}(n,q)$ on $\mathbb{G}_m/K$ is the subgroup $\mathrm{SL}_n(q) \rtimes C_{(q-1)/d}$ of $\mathrm{GL}_n(q)$ (with $C_{(q-1)/d}$ being the cyclic group of diagonal matrices $\mathrm{diag}(x, 1, \dots, 1)$ where $x \in \mu_{(q-1)/d}$), or equivalently, is the subgroup of $\mathrm{GL}_n(q)$ on which $\det^{(q-1)/d} = 1$.*

Proof. In the case $d = 1$, the statement holds by Theorem 8.1: $G_{\mathrm{geom},1} = G_{\mathrm{geom}} = \mathrm{GL}_n(q)$. Next we prove the statement for $d = q - 1$. When we do any $[N]^\star$ Kummer pullback, with N prime to p, the new $G_{\mathrm{geom},N}$ after the pullback is a normal subgroup of the original G_{geom}, such that $G_{\mathrm{geom}}/G_{\mathrm{geom},N}$ is cyclic of order dividing N. [When $N|(q-1)$, $K \supseteq \mathbb{F}_q$ contains μ_N, and so the same statement is also true for G_{arith}.] In particular,

$$G_{\mathrm{geom},q-1} \ge [G_{\mathrm{geom}}, G_{\mathrm{geom}}] = \mathrm{SL}_n(q).$$

Furthermore, in the case of $\mathcal{W}(n,q)$, by Lemma 1.1, the geometric determinants of the individual summands $\mathcal{F}_\chi$, which for some summands have full order $q-1$, all become trivial after the $[q-1]$ Kummer pullback. It follows that $G_{\mathrm{geom},q-1}$ has full index $q-1$, and so $G_{\mathrm{geom},q-1} = \mathrm{SL}_n(q)$.

For any divisor d of $q-1$,

$$[G_{\mathrm{geom},1} : G_{\mathrm{geom},d}] \le d,\ [G_{\mathrm{geom},d} : G_{\mathrm{geom},q-1}] \le (q-1)/d.$$

Since $[G_{\mathrm{geom},1} : G_{\mathrm{geom},q-1}] = q-1$, equality must hold in both of these, and the statement follows for d. □

9. Relation to work of Abhyankar

After the $[q^n-1]^\star$ Kummer pullback, each of the $q-1$ summands $\mathcal{F}_\chi$ of $\mathcal{W}(n,q)$ becomes lisse on $\mathbb{A}^1/\mathbb{F}_q$, and the entire representation $\mathcal{L}_{\mathbb{1}} \oplus \mathcal{W}(n,q)$ is the local system on $\mathbb{A}^1/\mathbb{F}_q$ whose trace at time v is the number of solutions of

$$T^{q^n} - v^{(q-1)q^{n-1}} T^{q^{n-1}} = T.$$

[This can be seen by taking our original equation $T^{q^n} - T^{q^{n-1}} = T/u$, multiplying through by u, then writing $u = v^{q^n-1}$ and writing the equation in terms of the new variable vT.] Since this pullback is itself the pullback by $[(q^n-1)/(q-1)]^\star$ of $[q-1]^\star\mathcal{W}(n,q)$, whose G_{geom} is $\mathrm{SL}_n(q)$ by Corollary 8.4, we see that this pullback continues to have $G_{\mathrm{geom}} = \mathrm{SL}_n(q)$ (since this G_{geom} is a normal subgroup of index dividing $(q^n-1)/(q-1)$ in $\mathrm{SL}_n(q)$, a group generated by its p-Sylow subgroups).

The iterated Frobenius pullback $[q^{n-1}]^\star$ (i.e. the power q^{n-1} in the exponent of the variable v), does not alter either G_{geom} or G_{arith}, so we can instead look at the new local system on $\mathbb{G}_m/\mathbb{F}_q$, call it $\mathcal{A}(n)$, whose trace at time v is the number of solutions of

$$T^{q^n} - v^{q-1} T^{q^{n-1}} = T,$$

and whose G_{geom} remains $\mathrm{SL}_n(q)$.

This new local system $\mathcal{A}(n)$ is the $[q-1]$ Kummer pullback of the local system, call it $\mathcal{B}(n)$, on $\mathbb{A}^1/\mathbb{F}_q$ whose trace at time v is the number of solutions of

$$T^{q^n} - vT^{q^{n-1}} = T.$$

Thus $G_{\mathrm{geom},\mathcal{A}(n)} (= \mathrm{SL}_n(q))$ is a normal subgroup of $G_{\mathrm{geom},\mathcal{B}(n)}$ of index dividing $q-1$. But as $\mathcal{B}(n)$ is lisse on $\mathbb{A}^1/\mathbb{F}_q$, its $G_{\mathrm{geom},\mathcal{B}(n)}$ is generated by its p-Sylow subgroups, and hence has no nontrivial quotients of order dividing $q-1$. Thus $G_{\mathrm{geom},\mathcal{B}(n)} = \mathrm{SL}_n(q)$ as well. This in turn means that over the rational function field $\overline{\mathbb{F}_q}(v)$, the Galois group of the equation $T^{q^n} - vT^{q^{n-1}} = T$, or equivalently, of the equation

$$T^{q^n-1} - vT^{q^{n-1}-1} = 1$$

is $\mathrm{SL}_n(q)$. Thus we have recovered case (i) of [Abh, Theorem 1.2].

References

[Abh] Abhyankar, S., Nice equations for nice groups, *Israel J. Math.* **88** (1994), 1–23.

[Atlas] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A. and Wilson, R. A., Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.

[BH] Bateman, P. T., and Horn, R. A., A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.

[Cam] Cameron, P. J., Finite permutation groups and finite simple groups, *Bull. Lond. Math. Soc.* **13** (1981), 1–22.

[Do] Dornhoff, L., Group representation theory, Dekker, New York, 1971.

[Ge] Gérardin, P., Weil representations associated to finite fields, *J. Algebra* **46** (1977), 54–101.

[Gr] Gross, B. H., Rigid local systems on $\mathbb{G}_m$ with finite monodromy, *Adv. Math.* **224** (2010), 2531–2543.

[GMPS] Guest, S., Morris J., Praeger, C. E., and Spiga, P., On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[GT] Guralnick, R. M. and Tiep, P. H., The non-coprime $k(GV)$-problem, *J. Algebra* **293** (2005), 185–242.

[Is] Isaacs, I. M., Character Theory of Finite Groups, AMS-Chelsea, Providence, 2006.

[Ka-CC] Katz, N.. From Clausen to Carlitz: low-dimensional spin groups and identities among character sums, *Mosc. Math. J.* **9** (2009), 57–89.

[Ka-ESDE] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, 124. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka-LGER] Local-to-global extensions of representations of fundamental groups, *Ann. Inst. Fourier* (Grenoble) **36** (1986), 69–106.

[KRL] Katz, N., and Rojas-León, A., A rigid local system with monodromy group $2.J_2$. *Finite Fields Appl.* **57** (2019), 276–286.

[KRLT1] Katz, N., Rojas-León, A., and Tiep, P. H., Rigid local systems with monodromy group the Conway group Co_3, *J. Number Theory* **206** (2020), 1–23.

[KRLT2] Katz, N., Rojas-León, A., and Tiep, P. H., Rigid local systems with monodromy group the Conway group Co_2, *Int. J. Number Theory* **16** (2020), 341–360.

[KRLT3] Katz, N., Rojas-León, A., and Tiep, P. H., A rigid local system with monodromy group the big Conway group Co_1 and two others with monodromy group the Suzuki group $6.\mathsf{Suz}$, *Trans. Amer. Math. Soc.* **373** (2020), 2007–2044.

[KT1] Katz, N., with an Appendix by Tiep, P. H., Rigid local systems on $\mathbb{A}^1$ with finite monodromy, *Mathematika* **64** (2018), 785–846.

[KT2] Katz, N., and Tiep, P. H., Rigid local systems and finite symplectic groups, *Finite Fields Appl.* **59** (2019), 134–174.

[KT3] Katz, N., and Tiep, P. H., Local systems and finite unitary and symplectic groups, *Advances in Math.* **358** (2019), 106859, 37 pp.

[KT4] Katz, N., and Tiep, P. H., Exponential sums and and total Weil representations of finite symplectic and unitary groups, (submitted).

[KlL] Kleidman, P. B., and Liebeck, M. W., The subgroup structure of the finite classical groups, London Math. Soc. Lecture Note Ser. no. **129**, Cambridge University Press, 1990.

[Se] Seitz, G. M., Flag-transitive subgroups of finite Chevalley groups, *Annals of Math.* **97** (1973), 27–56.

[SF] Simpson, W., and Frame, J. S., The character tables for $SL(3,q)$, $SU(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$, *Canad. J. Math.* **25** (1973), 486–494.

[T] Tiep, P. H., Weil representations of finite general linear groups and finite special linear groups, *Pacific J. Math.* **279** (2015), 481–498.

[TZ1] Tiep, P. H., and Zalesskii, A. E., Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[TZ2] Tiep, P. H., and Zalesskii, A. E., Unipotent elements of finite groups of Lie type and realization fields of their complex representations, *J. Algebra* **271** (2004), 327–390.

Department of Mathematics, Princeton University, Princeton, NJ 08544
Email address: nmk@math.princeton.edu

Department of Mathematics, Rutgers University, Piscataway, NJ 08854
Email address: tiep@math.rutgers.edu