RIGID LOCAL SYSTEMS WITH MONODROMY GROUP THE CONWAY GROUP Co_2

NICHOLAS M. KATZ, ANTONIO ROJAS-LEÓN, AND PHAM HUU TIEP

Abstract. We first develop some basic facts about hypergeometric sheaves on the multiplicative group $\mathbb{G}_m$ in characteristic $p > 0$. Certain of their Kummer pullbacks extend to irreducible local systems on the affine line in characteristic $p > 0$. One of these, of rank 23 in characteristic $p = 3$, turns out to have the Conway group Co_2, in its irreducible orthogonal representation of degree 23, as its arithmetic and geometric monodromy groups.

Contents

Introduction

In the first two sections, we give the general set up. In the third section, we apply known criteria to show that certain local systems of rank 23 over the affine line in characteristic 3 have finite (arithmetic and geometric) monodromy groups. In the final section, we show that the finite monodromy groups in question are the Conway group Co_2 in its 23-dimensional irreducible orthogonal representation.

1. The basic set up, and general results

We fix a prime number p, a prime number $\ell \neq p$, and a nontrivial $\overline{\mathbb{Q}_\ell}^\times$-valued additive character ψ of $\mathbb{F}_p$. For $k/\mathbb{F}_p$ a finite extension, we denote by ψ_k the nontrivial additive character of k given by $\psi_k := \psi \circ \mathrm{Trace}_{k/\mathbb{F}_p}$. In perhaps more down to earth terms, we fix a nontrivial $\mathbb{Q}(\mu_p)^\times$-valued additive character ψ of $\mathbb{F}_p$, and a field embedding of $\mathbb{Q}(\mu_p)$ into $\overline{\mathbb{Q}_\ell}$ for some $\ell \neq p$.

2010 *Mathematics Subject Classification.* Primary 11T23, Secondary 20C15, 20C34, 20D08.

Key words and phrases. Rigid local systems, Monodromy groups, Sporadic simple groups.

The second author was partially supported by MTM2016-75027-P (Ministerio de Economía y Competitividad) and FEDER. The third author gratefully acknowledges the support of the NSF (grant DMS-1840702).

The authors are grateful to the referee for helpful comments on the paper.

We fix two integers $N > D > 1$ which are both prime to p and with $\gcd(N, D) = 1$. We first describe a rigid local system on $\mathbb{G}_m/\mathbb{F}_p$, denoted

$$\mathcal{H}(\psi, N, D),$$

which is pure of weight 2 and whose trace function at a point $t \in K^\times$, K a finite extension of $\mathbb{F}_p$, is given by the exponential sum

$$\sum_{x\in K, y\in K^\times} \psi_K(tx^D/y^N - Dx + Ny).$$

It will also turn out that after pullback by N^{th} power, the pullback system

$$\mathcal{F}(\psi, N, D) := [N]^\star\mathcal{H}(\psi, N, D)$$

extends to an irreducible local system on $\mathbb{A}^1/\mathbb{F}_p$, whose trace function at a point $t \in K$, K a finite extension of $\mathbb{F}_p$, is given by the exponential sum

$$\sum_{x\in K, y\in K^\times} \psi_K(x^D/y^N - Dx + tNy).$$

[In the $\mathcal{H}$ sum, replace t by t^N, and then make the change of variable $y \mapsto ty$, to see what happens over $\mathbb{G}_m$.]

To understand this situation, we must relate $\mathcal{H}(\psi, N, D)$ to the hypergeometric sheaf

$$\mathcal{H}yp(\psi, N, D) := \mathcal{H}yp\left(\begin{array}{c}\psi, \text{all characters of order dividing } N;\\ \text{all nontrivial characters of order dividing } D\end{array}\right).$$

This hypergeometric sheaf is only defined on $\mathbb{G}_m/\mathbb{F}_q$, with $\mathbb{F}_q/\mathbb{F}_p$ an extension large enough to contain all the ND^{th} roots of unity. We know that it is an irreducible rigid local system on $\mathbb{G}_m$ which is not geometrically isomorphic to any nontrivial multiplicative translate of itself.

In terms of the Kloosterman sheaves

$$\mathcal{A} := \mathcal{K}l(\psi, \text{all characters of order dividing } N)$$

and

$$\mathcal{B} := \mathcal{K}l(\overline{\psi}, \text{all nontrivial characters of order dividing } D),$$

we obtain $\mathcal{H}yp(\psi, N, D)$ as the lower ! multiplicative convolution

$$\mathcal{H}yp(\psi, N, D) = \mathcal{A} *_{\times,!} inv^\star\mathcal{B}.$$

Lemma 1.1. *We have a geometric isomorphism*

$$\mathcal{K}l(\psi, \textit{all characters of order dividing } N) \cong [N]_\star\mathcal{L}_{\psi(Nx)}.$$

Proof. This is [Ka-GKM, 5.6.3]. The twisting factor over extensions $K/\mathbb{F}_p$ containing the N^{th} roots of unity is

$$A(\psi, N, K) = \prod_{\text{characters } \rho,\ \rho^N=\mathbb{1}} (-\mathsf{Gauss}(\psi_K, \rho)).$$

□

The second member, $[N]_\star\mathcal{L}_{\psi(Nx)}$, makes sense on $\mathbb{G}_m/\mathbb{F}_p$, with trace function given by

$$t \in K^\times \mapsto \sum_{y\in K,\ y^N=t} \psi_K(Ny).$$

Lemma 1.2. *We have a geometric isomorphism of*

$$\mathcal{B} := \mathcal{K}l(\overline{\psi}, \text{all nontrivial characters of order dividing } D)$$

with the local system $\mathcal{B}_0$ on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is

$$t \in K^\times \mapsto -\sum_{x\in K} \psi_K(x^D/t - Dx).$$

Proof. It suffices to show that over every $K/\mathbb{F}_p$ containing the D^{th} roots of unity, the two local systems have trace functions related by

$$\text{Trace}(Frob_{K,t}|\mathcal{B}) = \text{Trace}(Frob_{K,t}|\mathcal{B}_0) \times A(\overline{\psi}, D, K)/(\#K),$$

for $A(\overline{\psi}, D, K)$ the twisting factor

$$A(\overline{\psi}, D, K) = \prod_{\text{characters } \rho,\ \rho^D=\mathbb{1}} (-\mathsf{Gauss}(\overline{\psi_K}, \rho)).$$

To show this, it is equivalent to show that their multiplicative Mellin transforms coincide. For $\mathcal{B}$, the Mellin transform is an explicit product of Gauss sums, cf. [Ka-ESDE, 8.2.8]. For $\mathcal{B}_0$, using the Hasse-Davenport relation [Ka-GKM, 5.6.1, line -1 on page 84], we find that the Mellin transform is another product of Gauss sums. The asserted identity is then a straightforward if tedious calculation using Hasse-Davenport, which we leave to the reader. □

Proposition 1.3. *$\mathcal{H}yp(\psi, N, D)$ is geometrically isomorphic to the lisse sheaf*

$$\mathcal{A}_0 \star_{\times,!} inv^\star\mathcal{B}_0$$

on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is that of $\mathcal{H}(\psi, N, D)$.

Proof. The trace function of $\mathcal{A}_0 \star_{\times,!} inv^\star\mathcal{B}_0$ is minus the multiplicative convolution of the trace functions of $\mathcal{A}_0$ and of $inv^\star\mathcal{B}_0$. Thus $\mathcal{H}yp(\psi, N, D)$ is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is given by

$$\begin{aligned} u \in K^\times \mapsto & \sum_{s,t\in K,\ st=u} \left(\sum_{y\in K,\ y^N=s} \psi_K(Ny)\right)\left(\sum_{x\in K} \psi_K(x^D t - Dx)\right) \\ & \text{(now solve for } s = y^N, t = u/s = u/y^N) \\ = & \sum_{x\in K, y\in K^\times} \psi_K(Ny + ux^D/y^N - Dx). \end{aligned}$$

Because $\mathcal{H}yp(\psi, N, D)$ is geometrically irreducible, the lisse sheaf $\mathcal{H}(\psi, N, D)$ is geometrically and hence arithmetically irreducible, and hence is uniquely determined by its trace function. Thus we have an arithmetic isomorphism

$$\mathcal{H}(\psi, N, D) \cong \mathcal{A}_0 \star_{\times,!} inv^\star\mathcal{B}_0.$$

□

Lemma 1.4. *The sheaf $\mathcal{H}(\psi, N, D)$ is pure of weight two. More precisely, we have an arithmetic isomorphism over any extension $K/\mathbb{F}_p$ containing the ND^{th} roots of unity,*

$$\mathcal{H}(\psi, N, D) \otimes (A(\psi, N, K)A(\overline{\psi}, D, K)/(\#K)) \cong \mathcal{H}yp(\psi, N, D).$$

Proof. The twisting factor $A(\overline{\psi}, D, K)/(\#K)$ has weight $D-3$, and the twisting factor $A(\psi, N, K)$ has weight $N-1$. The hypergeometric sheaf $\mathcal{H}yp(\psi, N, D)$ is pure of weight $N+D-2$, cf. [Ka-ESDE, 7.3.8 (5), page 264, and 8.4.13]. □

Lemma 1.5. *For any integer M prime to p, the pullback $[M]^\star\mathcal{H}(\psi, N, D)$ is geometrically irreducible. The pullback $[N]^\star\mathcal{H}(\psi, N, D)$ extends to a lisse, geometrically irreducible sheaf on $\mathbb{A}^1/\mathbb{F}_p$, whose trace function is given, at points $u \in K$, K a finite extension of $\mathbb{F}_p$, by*

$$u \mapsto \sum_{x\in K, y\in K^\times} \psi_K(x^D/y^N - Dx + uNy).$$

Proof. To see the asserted geometric irreducibility of $[M]^\star\mathcal{H}(\psi, N, D)$, we argue as follows. The inner product

$$\langle [M]^\star\mathcal{H}(\psi, N, D), [M]^\star\mathcal{H}(\psi, N, D)\rangle =$$

$$= \langle \mathcal{H}(\psi, N, D), [M]_\star[M]^\star\mathcal{H}(\psi, N, D)\rangle.$$

By the projection formula,

$$[M]_\star[M]^\star\mathcal{H}(\psi, N, D) = \mathcal{H}(\psi, N, D) \otimes [M]_\star\overline{\mathbb{Q}_\ell} =$$

$$= \mathcal{H}(\psi, N, D) \otimes \bigoplus_{\chi, \chi^M=\mathbb{1}} \mathcal{L}_\chi =$$

$$= \bigoplus_{\chi, \chi^M=\mathbb{1}} \mathcal{L}_\chi \otimes \mathcal{H}(\psi, N, D).$$

In general, hypergeometric sheaves behave under tensoring with $\mathcal{L}_\chi$ by

$$\mathcal{L}_\chi \otimes \mathcal{H}yp(\psi, \rho_i' s; \Lambda_j' s) \cong \mathcal{H}yp(\psi, \chi\rho_i' s; \chi\Lambda_j' s).$$

One knows that hypergeometric sheaves are determined geometrically up to multiplicative translation by the sets of their upstairs and downstairs characters. Because N and D are relatively prime, for any nontrivial χ, the sheaf $\mathcal{L}_\chi \otimes \mathcal{H}(\psi, N, D)$ will not have the same upstairs and downstairs characters as $\mathcal{H}(\psi, N, D)$. Indeed, either the upstairs characters change, or χ is nontrivial of order dividing N, in which case the downstairs characters change.

That the $[N]^\star\mathcal{H}(\psi, N, D)$ pullback is lisse across 0 is obvious, since the local monodromy at 0 of $\mathcal{H}(\psi, N, D)$ is the direct sum of characters of order dividing N, so this local monodromy dies after $[N]^\star$. The formula for the trace results from the formula for the trace of $\mathcal{H}(\psi, N, D)$, namely

$$u \mapsto \sum_{x\in K, y\in K^\times} \psi_K(ux^D/y^N - Dx + Ny),$$

by replacing u by u^N and making the substitution $y \mapsto uy$. □

We now view $\mathcal{H}(\psi, N, D)$ as a representation of the arithmetic fundamental group

$$\pi_1^{arith}(\mathbb{G}_m/\mathbb{F}_p) := \pi_1(\mathbb{G}_m/\mathbb{F}_p)$$

and of its normal subgroup

$$\pi_1^{geom}(\mathbb{G}_m/\mathbb{F}_p) := \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}).$$

We also view the pullback $[N]^\star\mathcal{H}(\psi, N, D)$ as a representation of

$$\pi_1^{arith}(\mathbb{A}^1/\mathbb{F}_p) := \pi_1(\mathbb{A}^1/\mathbb{F}_p)$$

and of its normal subgroup

$$\pi_1^{geom}(\mathbb{A}^1/\mathbb{F}_p) := \pi_1(\mathbb{A}^1/\overline{\mathbb{F}_p}).$$

Lemma 1.6. (Primitivity Lemma) *Suppose that $N > D > 1$ are both prime to p and have $\gcd(N, D) = 1$. Then we have the following results.*

(i) *Unless D is 3 or 4 or 6, the local system $[N]^\star\mathcal{H}(\psi, N, D)$ on $\mathbb{A}^1/\mathbb{F}_p$ is not geometrically induced, i.e., there is no triple $(U, \pi, \mathcal{G})$ consisting of a connected smooth curve $U/\overline{\mathbb{F}_p}$, a finite etale map $f : U \to \mathbb{A}^1/\overline{\mathbb{F}_p}$ of degree $d \geq 2$, and a local system $\mathcal{H}$ on U such that there exists an isomorphism of $\pi_\star\mathcal{G}$ with (the pullback to $\mathbb{A}^1/\overline{\mathbb{F}_p}$ of) $[N]^\star\mathcal{H}(\psi, N, D)$.*

(ii) *Unless D is 3 or 4 or 6, the local system $\mathcal{H}(\psi, N, D)$ on $\mathbb{G}_m/\mathbb{F}_p$ is not geometrically induced.*

(iii) *Suppose $D = 3$. Then $[N]^\star\mathcal{H}(\psi, N, D)$ is not geometrically induced unless $N = 1 + q$ for some power q of p. In this case, $\mathcal{H}(\psi, N = 1 + q, D = 3)$ is geometrically induced, and hence so is $[N]^\star\mathcal{H}(\psi, N, D)$.*

(iv) *Suppose $D = 4$. Then $[N]^\star\mathcal{H}(\psi, N, D)$ is not geometrically induced unless $N = 1 + 2q$ or $N = 2 + q$ for some power q of p. In this case, both $\mathcal{H}(\psi, N = 1 + 2q, D = 4)$ and $\mathcal{H}(\psi, N = 2 + q, D = 4)$ are geometrically induced, and hence so are both $[N]^\star\mathcal{H}(\psi, N = 1 + 2q, D = 4)$ and $[N]^\star\mathcal{H}(\psi, N = 2 + q, D = 4)$.*

(v) *Suppose $D = 6$. Then $[N]^\star\mathcal{H}(\psi, N, D)$ is not geometrically induced (and hence $\mathcal{H}(\psi, N, D)$ is not geometrically induced).*

Proof. For (i), we argue as follows. The pullback sheaf $[N]^\star\mathcal{H}(\psi, N, D)$ has Euler characteristic zero, as its rank, N, is equal to its Swan conductor. So if such a triple $(U, \pi, \mathcal{G})$ exists, we have the equality of Euler characteristics

$$EP(U, \mathcal{G}) = EP(\mathbb{A}^1/\overline{\mathbb{F}_p}, \pi_\star\mathcal{G}) = EP(\mathbb{A}^1/\overline{\mathbb{F}_p}, [N]^\star\mathcal{H}(\psi, N, D)) = 0.$$

Denote by X the complete nonsingular model of U, and by g_X its genus. Then π extends to a finite flat map of X to $\mathbb{P}^1$, and the Euler-Poincaré formula gives

$$0 = EP(U, \mathcal{G}) = \mathrm{rank}(\mathcal{G})(2 - 2g_X - \#(\pi^{-1}(\infty))) - \sum_{w \in \pi^{-1} - (\infty)} \mathsf{Swan}_w(\mathcal{G}).$$

Thus $g_X = 0$, otherwise already the first term alone is strictly negative. So now $X = \mathbb{P}^1$, and we have

$$0 = \mathrm{rank}(\mathcal{G})(2 - \#(\pi^{-1}(\infty))) - \sum_{w \in \pi^{-1} - (\infty)} \mathsf{Swan}_w(\mathcal{G}).$$

If $\#(\pi^{-1}(\infty)) \geq 3$, then already the first term alone is strictly negative. If $\#(\pi^{-1}(\infty)) = 1$, then U is $\mathbb{P}^1 \setminus$ (one point) $\cong \mathbb{A}^1$, and so π is a finite etale map of $\mathbb{A}^1$ to itself of degree > 1.

But any such map has degree divisible by p, and hence $\pi_\star\mathcal{G}$ would have rank divisible by p. But its rank is N, which is prime to p. Thus we must have $\#(\pi^{-1}(\infty)) = 2$ (and $g_X = 0$).

Throwing the two points to 0 and ∞, we have a finite etale map

$$\pi : \mathbb{G}_m \to \mathbb{A}^1.$$

The equality of EP's now gives

$$0 = \mathsf{Swan}_0(\mathcal{G}) + \mathsf{Swan}_\infty(\mathcal{G}).$$

Thus $\mathcal{H}$ is lisse on $\mathbb{G}_m$ and everywhere tame, so a successive extension of lisse, everywhere tame sheaves of rank one. But $\pi_\star\mathcal{H}$ is irreducible, so $\mathcal{H}$ must itself be irreducible, hence of rank one, and either $\overline{\mathbb{Q}_\ell}$ or an $\mathcal{L}_\rho$. [It cannot be $\overline{\mathbb{Q}_\ell}$, because $\pi_\star\overline{\mathbb{Q}_\ell}$ is not irreducible when π has degree > 1; by adjunction $\pi_\star\overline{\mathbb{Q}_\ell}$ contains $\overline{\mathbb{Q}_\ell}$.]

Now consider the maps induced by π on punctured formal neighborhoods

$$\pi(0) : \mathbb{G}_m(0) \to \mathbb{A}^1(\infty), \quad \pi(\infty) : \mathbb{G}_m(\infty) \to \mathbb{A}^1(\infty).$$

The $I(\infty)$-representation of $\mathcal{F}_{p,D,f,\chi}$ is then the direct sum

$$\pi(0)_\star\mathcal{L}_\rho \oplus \pi(\infty)_\star\mathcal{L}_\rho.$$

Denote by d_0 and d_∞ their degrees. Because $\mathcal{G}$ has rank one, the degree of π must be N, and hence

$$N = d_0 + d_\infty.$$

Both d_0 and d_∞ cannot be prime to p, for then the $I(\infty)$ representation would be the sum of $d_0 + d_\infty = N$ tame characters. But the $I(\infty)$ representation of $[N]^\star\mathcal{H}(\psi, N, D)$ is the direct sum of the $D - 1 < N$ nontrivial characters of order dividing D and a wild part of rank $N - (D - 1)$.

After interchanging 0 and ∞ if necessary, we may assume that d_0 is prime to p, and that

$$d_1 = n_1 q$$

with n_1 prime to p and with q a positive power of p. Then $\pi(0)_\star\mathcal{L}_\rho$ consists of d_0 distinct characters, the d_0^{th} roots of $\mathcal{L}_\rho$, while $\pi(\infty)_\star\mathcal{L}_\rho$ consists of n_1 distinct characters (the $n_1 q^{\text{th}}$ roots of $\mathcal{L}_\rho$), together with a wild part. As the total number of tame characters is $D - 1$, we have the equalities

$$N = d_0 + n_1 q, \quad D - 1 = d_0 + n_1.$$

There is now a further observation to be made. The d_0 tame characters occuring in $\pi(0)_\star\mathcal{L}_\rho$ are a torsor under the characters of order dividing d_0. So the ratio of any two has order dividing d_0. But each of these d_0 characters has order dividing D, and hence so does any ratio of them. Therefore d_0 divides D. Similarly, we see that n_1 divides D.

Thus we have $D - 1 = d_0 + n_1$, with both d_0 and n_1 divisors of D. We will see that this is very restrictive. Write

$$d_0 = D/A, \ n_1 = D/B,$$

with A, B each divisors of D.

We first observe that both A, B must be ≥ 2, otherwise one of the terms D/A or D/B is D, already too large.

Suppose first D is even. We cannot have $A = B = 2$, because then $D/A + D/B = D$ is too large. So the largest possible value of $D/A + D/B$ is $D/2 + D/3 = 5D/6$. This is too

small, i.e. $5D/6 < D-1$, so long as $5D < 6D-6$, i.e., so long as $D > 6$. And we note that for $D = 6$, we indeed have $D-1 = 5 = 2+3$ is the sum of divisors of D.

Suppose next that D is odd. Then the largest possible value of $D/A+D/B$ is $D/3+D/3 = 2D/3$. This is too small, i.e., $2D/3 < D-1$, so long as $D > 3$. Notice that $D-1 = 2 = 1+1$ is the sum of divisors of D.

The case $D = 2$ cannot be induced, because the lowest value for $D-1 = 1$ is $1+1$ (coming from $N = 1+q$), too large.

This concludes (!) the proof of (i).

Assertion (ii) follows trivially, since if a representation of the group is primitive, it is all the more primitive on an overgroup.

For assertion (iii), the case $D = 3$, we can only achieve $D-1 = 2$ as as the sum of two divisors of $D = 3$ as $D-1 = 2 = 1+1$, i.e. if $N = 1+q$. In this case, q must be 1 mod 3 (simply because $N = q+1$ is prime to $D = 3$, as is p and hence also q). In this case, one checks that the finite etale map $\pi : x \mapsto 1/(x^q(x-1))$ from $\mathbb{G}_m \setminus \{1\}$ to $\mathbb{G}_m$ has

$$\pi_\star(\mathcal{L}\chi_3(x) \otimes \mathcal{L}\chi_3^2(x)),$$

for χ_3 either character of order 3, geometrically isomorphic to a multiplicative translate of $\mathcal{H}yp(\psi, N, D)$.

For assertion (iv), the case $D = 4$, we can only achieve $D-1 = 3$ as $1+2$, i.e. as $N = 1+2q$ or as $N = 2+q$. Here q must be odd, as p is prime to $D = 4$. One checks that for both of the finite etale maps $\pi : x \mapsto 1/(x^q(x-1)^2)$ and $\pi : x \mapsto 1/(x^2(x-1)^q)$,

$$\pi_\star\mathcal{L}\chi_2(x(x-1)),$$

for χ_2 the quadratic character, is geometrically isomorphic to a multiplicative translate of $\mathcal{H}yp(\psi, N, D)$.

For assertion (v), the case $D = 6$, we argue by contradiction. The two possibilities are $N = 2+3q$ and $N = 3+2q$. In both cases, the tame characters at ∞ will be, for some nontrivial character ρ, the union of the square roots of either ρ or of ρ^q and the cube roots of either ρ or of ρ^q. These are to be the nontrivial characters of order dividing $D = 6$. Thus ρ is the cube of some character of order dividing 6, but is nontrivial, so ρ must be the quadratic character. But ρ is also the square of some character of order dividing 6, but being nontrivial must have order 3. So this $D = 6$ case cannot be induced. A fortiori, in this $D = 6$ case $\mathcal{H}yp(\psi, N, D)$ cannot be induced, cf. the proof of (ii). □

Lemma 1.7. (Determinant Lemma) *Suppose that $N > D > 1$ are both prime to p and have $\gcd(N, D) = 1$. Then we have the following results.*

(i) *If N is odd, then $\det(\mathcal{H}(\psi, N, D)(1))$ is geometrically constant, It is of the form A^{deg}, with $A = \zeta$ for some root of unity $\zeta \in \mathbb{Z}[\zeta_p]$.*

(ii) *if N is even, then $\det([N]^\star\mathcal{H}(\psi, N, D)(1))$ is geometrically constant. It is of the form A^{deg}, with $A = \zeta$ for some root of unity $\zeta \in \mathbb{Z}[\zeta_p]$.*

(iii) *Suppose N is odd (respectively even) and we have the congruence*

$$D \equiv N+1 (\text{mod } p-1).$$

Then $\mathcal{H}(\psi, N, D)(1)$ (respectively $[N]^\star\mathcal{H}(\psi, N, D)(1)$) has all Frobenius traces in $\mathbb{Q}$, and has determinant A^{deg} with A some choice of ± 1.

(iv) *Under the hypotheses of (iii), denote by d the degree of $\mathbb{F}_p(\mu_N)/\mathbb{F}_p$. If N is odd, or if N is even and either D is a square in $\mathbb{F}_p$ or d is even, then $A^d = 1$. If N is even, and D is a nonsquare in $\mathbb{F}_{p^d}$, then $A^d = -1$. In particular, if N and d are both odd, then we have $A = 1$ in (iii) above.*

Proof. To prove (i) and (ii), we appeal to [Ka-ESDE, 8.11.6]. Here the upper characters are all the characters of order dividing N, so their product is trivial when N is odd, and the quadratic character χ_2 when N is even. Thus the determinant is geometrically trivial when N is odd, and is geometrically $\mathcal{L}_{\chi_2}$ when N is even. In the N even case, it becomes geometrically trivial after $[N]^\star$ (or just after $[2]^\star$). So we can compute A as the determinant at, say, the point $s = 1$ (which is certainly an N^{th} power).

This determinant lies in $\mathbb{Z}[\zeta_p][1/p]$, and is pure of weight zero, i.e., it has absolute value 1 for every complex embedding of $\mathbb{Q}(\zeta_p)$. Because $\mathbb{Q}(\zeta_p)$ has a unique place over p, this determinant and its complex conjugate have the same p-adic ord. So being of weight zero, the determinant is a unit at the unique place over p. As it lies in $\mathbb{Z}[\zeta_p][1/p]$, it is integral at all ℓ-adic places over primes $\ell \neq p$. So by the product formula, it must be a unit everywhere, and so is a root of unity in $\mathbb{Q}(\zeta_p)$.

To prove (iii), we first show that under the asserted congruence, each sum

$$\sum_{x\in K, y\in K^\times} \psi_K(tx^D/y^N - Dx + Ny).$$

lies in $\mathbb{Z}$. Indeed, this sum lies in $\mathbb{Z}[\zeta_p]$, so it suffices to show that it is invariant under the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. This group is $\mathbb{F}_p^\times$, with $\alpha \in \mathbb{F}_p^\times$ moving this sum to

$$\sum_{x\in K, y\in K^\times} \psi_K(\alpha t x^D/y^N - D\alpha x + N\alpha y) =$$

$$= \sum_{x\in K, y\in K^\times} \psi_K(t(\alpha x)^D/(\alpha y)^N - D\alpha x + N\alpha y),$$

(equality because $\alpha = \alpha^{D-N}$ by the congruence $D \equiv N + 1 \bmod p - 1$) which is the original sum after the change of variable $x \mapsto \alpha x,\ y \mapsto \alpha y$. Once the traces lie in $\mathbb{Q}$, the same argument used in (ii) above now shows that the determinant is a root of unity in $\mathbb{Q}$.

To prove (iv), we argue as follows. The assertion is about the sign of A^d, which we can compute for $[N]^\star\mathcal{H}(\psi, N, D)(1)$ at any point $t \in \mathbb{F}_{p^d}$. We take the point $t = 0$. We will compute the trace over all extensions $K = \mathbb{F}_q$ of $\mathbb{F}_{p^d}$ in order to calculate the eigenvalues of $Frob_{t=0,\mathbb{F}_{p^d}}$ on $[N]^\star\mathcal{H}(\psi, N, D)(1)$. Over such a K, the trace is

$$\sum_{x\in K, y\in K^\times} \psi_K(x^D/y^N - Dx)/q.$$

In **this** sum, we may invert y, so the sum becomes

$$(1/q)\sum_{x\in K} \psi_K(-Dx) \sum_{y\in K^\times} \psi_K(x^D y^N).$$

Because all the characters of order dividing N exist over K, we rewrite the second term as

$$\sum_{y\in K^\times} \psi_K(x^D y^N) = \sum_{u\in K^\times} \psi_K(x^D u) \sum_{\text{char.'s } \rho, \rho^N = \mathbb{1}} \rho(u).$$

So our K sum becomes

$$(1/q)\sum_{x\in K}\psi_K(-Dx)\sum_{\text{char.'s }\rho,\rho^{\mathrm{N}}=\mathbb{1}}\ \sum_{u\in K^\times}\psi_K(x^Du)\rho(u).$$

For each nontrivial ρ, the ρ term is

$$\sum_{u\in K^\times}\psi_K(x^Du)\rho(u)=\overline{\rho}(x^D)\mathsf{Gauss}(\psi_K,\rho).$$

So each $\rho\neq\mathbb{1}$ term in the K sum is

$$\sum_{x\in K}\psi_K(-Dx)\overline{\rho}(x^D)\mathsf{Gauss}(\psi_K,\rho)/q=\rho^D(D)\mathsf{Gauss}(\overline{\psi_K},\overline{\rho}^D)\mathsf{Gauss}(\psi_K,\rho)/q.$$

The $\rho=\mathbb{1}$ term in the K sum is

$$(1/q)\sum_{x\in K}\psi_K(-Dx)\sum_{u\in K^\times}\psi_K(x^Du)=$$

$$=(1/q)\sum_{x\in K}\psi_K(-Dx)(-1+\sum_{u\in K}\psi_K(x^Du))=$$

$$=(1/q)\sum_{x\in K^\times}\psi_K(-Dx)(-1)+(1/q)(-1+q)=(1/q)(1+q-1)=1.$$

Thus the eigenvalues are precisely 1 and, for each of the $N-1$ nontrivial ρ of order dividing N, the product

$$\rho^D(D)\mathsf{Gauss}(\overline{\psi_{\mathbb{F}_{p^d}}},\overline{\rho}^D)\mathsf{Gauss}(\psi_{\mathbb{F}_{p^d}},\rho)/p^d.$$

So the determinant is the product

$$\prod_{\rho^N=\mathbb{1},\ \rho\neq\mathbb{1}}\rho^D(D)[\mathsf{Gauss}(\overline{\psi_{\mathbb{F}_{p^d}}},\overline{\rho}^D)\mathsf{Gauss}(\psi_{\mathbb{F}_{p^d}},\rho)/p^d].$$

Because D is prime to N, the ρ^D are just a rearrangement of the ρ. So defining

$$\Lambda:=\prod_{\rho^N=\mathbb{1},\ \rho\neq\mathbb{1}}\rho,$$

we see that the determinant is

$$\Lambda(D)\prod_{\rho^N=\mathbb{1},\ \rho\neq\mathbb{1}}[\mathsf{Gauss}(\overline{\psi_{\mathbb{F}_{p^d}}},\overline{\rho})\mathsf{Gauss}(\psi_{\mathbb{F}_{p^d}},\rho)/p^d]=\Lambda(D).$$

If N is odd, then $\Lambda=\mathbb{1}$. If N is even, the Λ is the quadratic character of $\mathbb{F}_{p^d}$. In this case, $\Lambda(D)=1$ if either D is already a square in $\mathbb{F}_p$, or if d is even, so that D becomes a square in $\mathbb{F}_{p^d}$. $\square$

2. The criterion for finite monodromy

Denote by V Kubert's V-function

$$V : (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p} \to \mathbb{Q}_{\geq 0}.$$

It has the following property. For $f \geq 1$, $q := p^f$, $\mathsf{Teich}_f : \mathbb{F}_q^\times \to \mathbb{Q}_p(\mu_{q-1})$ the Teichmuller character (for a fixed p-adic place of $\mathbb{Q}_p(\mu_{q-1})$), and $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$ of order dividing $q-1$, we have

$$V(x) = \text{ord}_{p^f}(\mathsf{Gauss}(\psi_{\mathbb{F}_q}, \mathsf{Teich}_f^{-(q-1)x})).$$

Lemma 2.1. *Suppose that $N > D > 1$ are both prime to p and have $\gcd(N, D) = 1$. Then $\mathcal{H}(\psi, N, D)(-1)$ has algebraic integer traces, and hence finite arithmetic monodromy group G_{arith}, if and only if the following inequalities hold. For every $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have*

$$V(Nx) + V(-Dx) - V(-x) \geq 0.$$

Equivalently (since this trivially holds for $x = 0$), the condition is that for every nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, we have

$$V(Nx) + V(-Dx) + V(x) \geq 1.$$

Proof. From Lemma 1.4, we see that $\mathcal{H}(\psi, N, D)(-1)$ has algebraic integer traces if and only if, for every finite extension $K/\mathbb{F}_p$ containing the ND^{th} roots of unity, the hypergeometric sheaf $\mathcal{H}yp(\psi, N, D)$ has traces at K-points which are of the form $A(N, K)A(D, K)$ times algebraic integers. Equivalently, as explained in [Ka-RL-T, Proof of Theorem 2.7], it suffices that the multiplicative Mellin transform of the trace function of $\mathcal{H}yp(\psi, N, D)$ on $K^\times$ has all values with ord at least that of $A(N, K)A(D, K)$. The value at χ is

$$(-1)^{N-D}\left(\prod_{\rho,\ \rho^N=\mathbb{1}} \mathsf{Gauss}(\psi_K, \chi\rho)\right) \times \left(\prod_{\sigma,\sigma^D=\mathbb{1},\sigma\neq\mathbb{1}} \mathsf{Gauss}(\overline{\psi}_K, \overline{\chi\rho})\right).$$

The first product is, up to a root of unity factor,

$$A(N, K)\mathsf{Gauss}(\psi_K, \chi^N).$$

The second product is, up to a root of unity factor,

$$A(D, K)\mathsf{Gauss}(\overline{\psi}_K, \overline{\chi}^D)/\mathsf{Gauss}(\overline{\psi}_K, \overline{\chi}).$$

So the requirement is that for all χ, the product

$$\mathsf{Gauss}(\psi_K, \chi^N)\mathsf{Gauss}(\overline{\psi}_K, \overline{\chi}^D)/\mathsf{Gauss}(\overline{\psi}_K, \overline{\chi})$$

have nonnegative ord. This is precisely the

$$V(Nx) + V(-Dx) - V(-x) \geq 0$$

version of the criterion. □

Remark 2.2. As Will Sawin pointed out to us, there are a number of sheaves $\mathcal{H}yp(\psi, N, D)$ which, although not induced, are very nearly so. Namely, for any power q of p, and for any $D \geq 2$ prime to p, the direct image $\pi_\star\overline{\mathbb{Q}_\ell}$, for $\pi : \mathbb{G}_m \setminus \{1\} \to \mathbb{G}_m$ the finite étale map given by $x \mapsto x^{Dq-1}(x-1)$, is geometrically isomorphic to the direct sum of the constant sheaf $\overline{\mathbb{Q}_\ell}$ and $\mathcal{H}yp(\psi, Dq-1, D)$. The case $D = 2$ was the subject of the paper [G-K-T].

From this direct image picture, we see that $\mathcal{H}yp(\psi, Dq-1, D)$ has finite geometric monodromy, and hence that $\mathcal{H}(\psi, Dq-1, D)(1)$ has finite G_{arith}. In other words, the inequality of Lemma 2.1 is satisfied by the data $N = Dq-1, D$ in the characteristic p of which q is a power and to which D is prime.

The induced cases, being induced from rank one, also have finite geometric monodromy. Thus $\mathcal{H}(\psi, q+1, 3)(1)$ has finite G_{arith} for any prime power q which is 1 mod 3 in the characteristic of which q is a power. And both $\mathcal{H}(\psi, q+2, 4)(1)$ and $\mathcal{H}(\psi, 2q+1, 4)(1)$ have finite G_{arith} in the odd characteristic of which q is a power. This gives other cases of data satisfying the inequality of Lemma 2.1.

In the next section, we will exhibit another datum, **not** of either of these types, satisfying the inequality. How many others are there?

3. Theorems of finite monodromy

In this section, we will prove

Theorem 3.1. *For $p = 3$, $N = 23$ and $D = 4$, the sheaf $\mathcal{H}(\psi, N, D)(1)$ has finite arithmetic and geometric monodromy groups.*

By lemma 2.1, we need to show that for every nonzero $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } 3}$, we have

$$V(23x) + V(-4x) - V(-x) \geq 0$$

or, equivalently,

$$V(-23x) + V(4x) - V(x) \geq 0.$$

Applying the duplication formula $V(x) + V(x+\frac{1}{2}) = V(2x) + \frac{1}{2}$, see [Ka-G2hyper, p.206], twice, this is equivalent to

$$1 - V(-23x) \leq V\left(2x + \frac{1}{2}\right) + V\left(x + \frac{1}{2}\right).$$

For $x = \frac{1}{2}$ this is obvious so, making the change of variable $x \mapsto x + \frac{1}{2}$, we get the equivalent condition

$$1 - V\left(-23x - \frac{1}{2}\right) \leq V\left(2x + \frac{1}{2}\right) + V(x).$$

If $x = \frac{1}{4}$ or $x = \frac{3}{4}$ the inequality (equality in this case) is trivial. Otherwise, $2x + \frac{1}{2} \neq 0$, and we can rewrite it as

$$1 - V\left(-23x - \frac{1}{2}\right) \leq 1 - V\left(-2x - \frac{1}{2}\right) + V(x).$$

We now restate the inequality in terms of the function $[\,-\,]_r := [\,-\,]_{3,r}$ defined in [R-L], given by

$$[x]_{3,r} = \text{the sum of the 3-adic digits of the representative of}$$
$$\text{the congruence class of } x \text{ modulo } 3^r - 1 \text{ in } [1, 3^r - 1].$$

By [Ka-RL, Appendix] we have $[x]_r = 2r(1 - V(-\frac{x}{3^r-1}))$, so the finite monodromy condition can be restated as

$$\left[23x + \frac{3^r-1}{2}\right]_r \leq [x]_r + \left[2x + \frac{3^r-1}{2}\right]_r$$

for every $r \geq 1$ and every integer $0 < x < 3^r - 1$.

For a non-negative integer x, let $[x]$ denote the sum of the 3-adic digits of x. For use below, we recall the following result from [Ka-RL, Prop. 2.2]:

Proposition 3.2. *For strictly positive integers x and y, and any $r \geq 1$, we have:*

(i) $[x+y] \leq [x] + [y]$;
(ii) $[x]_r \leq [x]$;
(iii) $[3x] = [x]$.

Lemma 3.3. *Let $r \geq 1$ and $0 \leq x < 3^r$ an integer. Then*

$$\left[23x + \frac{3^r - 1}{2}\right] \leq [x] + \left[2x + \frac{3^r - 1}{2}\right] + 2.$$

Moreover, if $r = 1$ and $x \neq 1$, $r = 2$ and $x \neq 3$ or $r \geq 3$ and the first three 3-adic digits of x (after adding leading 0's so it has exactly r digits) are not 100 or 202, then

$$\left[23x + \frac{3^r - 1}{2}\right] \leq [x] + \left[2x + \frac{3^r - 1}{2}\right].$$

Proof. We proceed by induction on r: for $r \leq 3$ one checks it by hand. Let $r \geq 4$ and $0 \leq x < 3^r$.

Case 1: $x \equiv 0 \pmod 3$.

Write $x = 3y$ with $0 \leq y < 3^{r-1}$. Then

$$\begin{aligned}
\left[23x + \frac{3^r - 1}{2}\right] &= \left[3\left(23y + \frac{3^{r-1} - 1}{2}\right) + 1\right] \\
&= \left[23y + \frac{3^{r-1} - 1}{2}\right] + 1 \\
&\leq [y] + \left[2y + \frac{3^{r-1} - 1}{2}\right] + 3 \\
&= [y] + \left[3\left(2y + \frac{3^{r-1} - 1}{2}\right) + 1\right] + 2 \\
&= [x] + \left[2x + \frac{3^r - 1}{2}\right] + 2
\end{aligned}$$

by induction. Since the first three digits of x and y are the same, the better inequality holds when those three digits are not 100 or 202, also by induction.

Case 2: The last $r - 3$ digits of x contain the string 00 or the string 01.

Say the string is located at position $s \leq r - 3$, counting from the right. Write $x = 3^s y + z$, where $y < 3^{r-s}$ and $z < 2 \cdot 3^{s-2}$. Then

$$2z + \frac{3^s - 1}{2} < 4 \cdot 3^{s-2} + \frac{3^s - 1}{2} < 3^s\left(\frac{4}{9} + \frac{1}{2}\right) < 3^s,$$

so

$$\begin{aligned}
\left[2x + \frac{3^r - 1}{2}\right] &= \left[3^s\left(2y + \frac{3^{r-s} - 1}{2}\right) + 2z + \frac{3^s - 1}{2}\right] \\
&= \left[2y + \frac{3^{r-s} - 1}{2}\right] + \left[2z + \frac{3^s - 1}{2}\right],
\end{aligned}$$

and therefore

$$\begin{aligned}\left[23x+\frac{3^r-1}{2}\right] &= \left[3^s\left(23y+\frac{3^{r-s}-1}{2}\right)+23z+\frac{3^s-1}{2}\right]\\ &\le \left[23y+\frac{3^{r-s}-1}{2}\right]+\left[23z+\frac{3^s-1}{2}\right]\\ &\le [y]+\left[2y+\frac{3^{r-s}-1}{2}\right]+2+[z]+\left[2z+\frac{3^s-1}{2}\right]\\ &= [x]+\left[2x+\frac{3^r-1}{2}\right]+2\end{aligned}$$

by induction. Again, since the first three digits of x and y are the same, the better inequality holds if they are not 100 or 202.

Case 3: The last $r-3$ digits of x contain one of the strings 02, 10, 11 or 12, and the previous digit is not a 2.

Say the string is located at position $s \le r-3$, counting from the right. Write $x = 3^s y + z$, where $y < 3^{r-s}$ is not $\equiv 2 \bmod 3$ and $z < 2\cdot 3^{s-1}$. Then

$$2z+\frac{3^s-1}{2} < 4\cdot 3^{s-1}+\frac{3^s-1}{2} < 3^s\left(\frac{4}{3}+\frac{1}{2}\right) < 2\cdot 3^s$$

and the last digit of $2y+(3^{r-s}-1)/2$ is not 2, so

$$\begin{aligned}\left[2x+\frac{3^r-1}{2}\right] &= \left[3^s\left(2y+\frac{3^{r-s}-1}{2}\right)+2z+\frac{3^s-1}{2}\right]\\ &= \left[2y+\frac{3^{r-s}-1}{2}\right]+\left[2z+\frac{3^s-1}{2}\right].\end{aligned}$$

We conclude as in case 1 **unless** $s=2$ and $z=3$ (in which case we can apply case 1) or $s\ge 3$ and the first three digits of z are 100 (in which case we can apply case 2).

If x is not included in the cases proved so far and the last $r-3$ digits of x contain a 0, it must be enclosed between two 2's. If they contain a 1, it must be enclosed between two 2's, with the possible exception of the last two digits in the case when x ends with 211 or 21.

Case 4: The last $r-3$ digits of x contain a 2 which is preceded by a 1 and the next two digits (if they exist) are not 02.

Write $x = 3^s y + z$, where $y < 3^{r-s}$ is congruent to 1 mod 3 and $z < 3^s$ starts with 2 (but not with 202). Then

$$2z+\frac{3^s-1}{2} < 2\cdot 3^s+\frac{3^s-1}{2} < 3^{s+1}$$

and the last digit of $2y+(3^{r-s}-1)/2$ is 0, so

$$\begin{aligned}\left[2x+\frac{3^r-1}{2}\right] &= \left[3^s\left(2y+\frac{3^{r-s}-1}{2}\right)+2z+\frac{3^s-1}{2}\right]\\ &= \left[2y+\frac{3^{r-s}-1}{2}\right]+\left[2z+\frac{3^s-1}{2}\right].\end{aligned}$$

We conclude as in the previous two cases.

Case 5: A digit of x which is not one of the first four or the last two is a 1. By the note after case 3, we can assume that the 1 is enclosed bewteen two 2's. If the digit after the following 2 is not 0 we apply case 4. If it is 0 and is the last digit, we apply case 1. Otherwise, by case 4 we can assume that there is a 2 after the 0, so the last $r-3$ digits of x contain the string 21202. If the previous digit is 1 we apply case 4.

Otherwise, write $x = 3^s y + z$, where the last three digits of y are 021 or 221, and the first three digits of z are 202. Then the last 3 digits of $2y + (3^{r-s}-1)/2$ are 000 or 100 and $2z + (3^s-1)/2 < 3^{s+2}$, so

$$\begin{aligned}\left[2x + \frac{3^r-1}{2}\right] &= \left[3^s\left(2y + \frac{3^{r-s}-1}{2}\right) + 2z + \frac{3^s-1}{2}\right] \\ &= \left[2y + \frac{3^{r-s}-1}{2}\right] + \left[2z + \frac{3^s-1}{2}\right].\end{aligned}$$

On the other hand, the last three digits of $23y + (3^{r-s}-1)/2$ are 110 or 210, and $23 = 212_3$. Since $212_3 \cdot 202_3 = 122011_3$, $23z + (3^s-1)/2$ has exactly $s+3$ digits, the first three of them being at least 122. In any case, in the sum $3^s\big(23y + (3^{r-s}-1)/2\big) + \big(23z + (3^s-1)/2\big)$ there is at least one digit carry, so

$$\begin{aligned}\left[23x + \frac{3^r-1}{2}\right] &= \left[3^s\left(23y + \frac{3^{r-s}-1}{2}\right) + 23z + \frac{3^s-1}{2}\right] \\ &\le \left[23y + \frac{3^{r-s}-1}{2}\right] + \left[23z + \frac{3^s-1}{2}\right] - 2 \\ &\le [y] + \left[2y + \frac{3^{r-s}-1}{2}\right] + 2 + [z] + \left[2z + \frac{3^s-1}{2}\right] \\ &= [x] + \left[2x + \frac{3^r-1}{2}\right] + 2.\end{aligned}$$

As usual, if the first three digits of x (or y) are not 100 or 202 one gets the better bound.

Case 6: The last $r-1$ digits of x contain the string 2202. Write $x = 3^s y + z$, where $y < 3^{r-s}$ ends with 22 and $z < 3^s$ starts with 02. Then the last two digits of $2y + (3^{r-s}-1)/2$ are 02, and $2z + (3^s-1)/2$ has at most $s+1$ digits. So

$$\begin{aligned}\left[2x + \frac{3^r-1}{2}\right] &= \left[3^s\left(2y + \frac{3^{r-s}-1}{2}\right) + 2z + \frac{3^s-1}{2}\right] \\ &\ge \left[2y + \frac{3^{r-s}-1}{2}\right] + \left[2z + \frac{3^s-1}{2}\right] - 2.\end{aligned}$$

On the other hand, the last two digits of $23y + (3^{r-s}-1)/2$ are 22, and $23z + (3^s-1)/2$ has $s+2$ digits, the first two being at least 12. In any case, in the sum $3^s\big(23y + (3^{r-s}-1)/2\big) +$

$\big(23z + (3^s - 1)/2\big)$ there is at least one digit carry, so

$$\begin{aligned}\left[23x + \frac{3^r - 1}{2}\right] &= \left[3^s\left(23y + \frac{3^{r-s} - 1}{2}\right) + 23z + \frac{3^s - 1}{2}\right] \\ &\leq \left[23y + \frac{3^{r-s} - 1}{2}\right] + \left[23z + \frac{3^s - 1}{2}\right] - 2 \\ &\leq [y] + \left[2y + \frac{3^{r-s} - 1}{2}\right] + 2 + [z] + \left[2z + \frac{3^s - 1}{2}\right] - 2 \\ &\leq [x] + \left[2x + \frac{3^r - 1}{2}\right] + 2.\end{aligned}$$

As usual, if the first three digits of x (or y) are not 100 or 202 one gets the better bound.

Case 7: The last $r - 1$ digits of x contain the string 2222. This case is similar to the previous one, with the difference that $23z + (3^s - 1)/2$ has now $s + 3$ digits, the first three being 202, 210, 211 or 212.

For all remaining cases, all digits except for the first four and the last two must be 0's and 2's. Among them, there can not be two consecutive 0's or four consecutive 2's, and if there is a string of two or three consecutive 2's, it can not be followed by a 0. So the last $r - 4$ digits of x are of the form

$$\begin{gathered}(\text{possibly a } 0) + (a \text{ copies of } 20) + \\ (1, 2 \text{ or } 3\ 2\text{'s}) + (\text{possibly } 1 \text{ or } 2\ 1\text{'s})\end{gathered}$$

for some $a \geq 0$. Here is a table with the last digits of $2x + (3^r - 1)/2$ and $23x + (3^r - 1)/2$ in each case for $a \geq 2$:

last digits of x	last digits of $2x+\frac{3^r-1}{2}$	last digits of $23x+\frac{3^r-1}{2}$
$\overbrace{2020...20}^{a\times 20}2$	$\overbrace{22...2}^{2a\times 2}2$	$\overbrace{2020...20}^{(a-1)\times 20}112$
$\overbrace{2020...20}^{a\times 20}22$	$\overbrace{00...0}^{2a\times 0}02$	$\overbrace{2020...20}^{(a-2)\times 20}210022$
$\overbrace{2020...20}^{a\times 20}222$	$\overbrace{00...0}^{2a\times 0}102$	$\overbrace{2020...20}^{(a-2)\times 20}2102122$
$\overbrace{2020...20}^{a\times 20}21$	$\overbrace{00...0}^{2a\times 0}00$	$\overbrace{2020...20}^{(a-1)\times 20}2110$
$\overbrace{2020...20}^{a\times 20}221$	$\overbrace{00...0}^{2a\times 0}100$	$\overbrace{2020...20}^{(a-1)\times 20}2101210$
$\overbrace{2020...20}^{a\times 20}2221$	$\overbrace{00...0}^{2a\times 0}1100$	$\overbrace{2020...20}^{(a-2)\times 20}21022210$
$\overbrace{2020...20}^{a\times 20}211$	$\overbrace{00...0}^{2a\times 0}010$	$\overbrace{2020...20}^{(a-1)\times 20}22020$
$\overbrace{2020...20}^{a\times 20}2211$	$\overbrace{00...0}^{2a\times 0}1010$	$\overbrace{2020...20}^{(a-2)\times 20}21020020$
$\overbrace{2020...20}^{a\times 20}22211$	$\overbrace{00...0}^{2a\times 0}11010$	$\overbrace{2020...20}^{(a-2)\times 20}211000020$

In any case, when $a \geq 2$ adding an extra 20 block increases the digit sums of x and $23x + (3^r - 1)/2$ by 2. So, by induction, we may assume that $a \leq 2$. It remains to check the cases where $a \leq 2$, which can be done by a computer search. □

Corollary 3.4. *Let $r \geq 2$ and $0 \leq x < 3^r$ an integer such that $x \not\equiv 2$ or $6 \pmod 9$. Then*

$$\left[23x + \frac{3^r-1}{2}\right] \leq [x] + \left[2x + 2 + \frac{3^r-1}{2}\right] + 2.$$

Proof. If $x \not\equiv 2$ or $6 \pmod 9$, then $2x + \frac{3^r-1}{2} \not\equiv 7$ or $8 \pmod 9$, and therefore

$$\left[2x + \frac{3^r-1}{2}\right] \leq \left[2x + 2 + \frac{3^r-1}{2}\right].$$

□

We can now finish the proof of theorem 3.1. Let $r \geq 2$ and let $0 < x < 3^r - 1$ be an integer such that $x \not\equiv 2$ or $6 \pmod 9$. Then $2x + 2 + (3^r - 1)/2 < 3^{r+1}$, and

$$\left[3^{r+1} - 1 - \left(2x + 2 + \frac{3^r-1}{2}\right)\right] = 2(r+1) - \left[2x + 2 + \frac{3^r-1}{2}\right].$$

By the previous corollary, we have

$$\left[23x + \frac{3^r-1}{2}\right] + \left[3^{r+1} - 3 - 2x - \frac{3^r-1}{2}\right] \leq [x] + 2r + 4.$$

Hence,

$$\left[23x+\frac{3^r-1}{2}\right]_r+\left[-2x-\frac{3^r-1}{2}\right]_r=$$
$$=\left[23x+\frac{3^r-1}{2}\right]_r+\left[3(3^r-1)-2x-\frac{3^r-1}{2}\right]_r\leq$$
$$\leq\left[23x+\frac{3^r-1}{2}\right]+\left[3^{r+1}-3-2x-\frac{3^r-1}{2}\right]\leq$$
$$\leq[x]+2r+4=[x]_r+2r+4.$$

Using [Ka-RL-T, Lemma 2.10], we conclude (as in the proof of [Ka-RL-T, Theorem 2.12]) that

$$\left[23x+\frac{3^r-1}{2}\right]_r+\left[-2x-\frac{3^r-1}{2}\right]_r\leq[x]_r+2r$$

or, equivalently,

$$\left[23x+\frac{3^r-1}{2}\right]_r\leq[x]_r+\left[2x+\frac{3^r-1}{2}\right]_r$$

If $x\equiv 2$ or $6 \pmod 9$, then either $x=2020\ldots20_3=3(3^r-1)/4$ or $x=0202\ldots02_3=(3^r-1)/4$, in which case the inequality is trivial, or we can multiply x by a suitable power of 3 (which cyclically permutes its digits modulo 3^r-1) to obtain an x which is not $\equiv 2$ or $6 \pmod 9$, to which we can apply the previous argument.

4. Determination of the monodromy groups

In this section, we will determine the monodromy of $\mathcal{H}(\psi,23,4)(1)$ in characteristic $p=3$. In this case, the field $\mathbb{F}_3(\mu_{23})$ is the field $F_{3^{11}}$. So by Lemma 1.7, the arithmetic monodromy group lies in $\mathrm{SL}_{23}(\mathbb{C})$. [In fact it lies in $\mathrm{SO}_{23}(\mathbb{C})$, since it is an irreducible subgroup with real (in fact integer) traces.]

Looking at the Frobenius $Frob_{-1,\mathbb{F}_3}$ at the point $t=-1$, we have, by computer calculation, that its first seven powers have traces

$$0,-2,0,2,0,-2,7.$$

First we prove the following theorem on finite subgroups of $\mathrm{SL}_{23}(\mathbb{C})$:

Theorem 4.1. *Let $V=\mathbb{C}^{23}$ and let $G<\mathrm{SL}(V)$ be a finite irreducible subgroup. Let χ denote the character of G afforded by V, and suppose that all the following conditions hold:*

(i) *χ is real-valued;*
(ii) *χ is primitive;*
(iii) *G contains an element γ such that the traces of $\gamma,\gamma^2,\ldots,\gamma^7$ acting on V are 0, -2, 0, 2, 0, -2, 7, respectively.*

Then $G\cong\mathsf{Co}_2$ in its unique (orthogonal) irreducible representation of degree 23.

Proof. By the assumption, the G-module V is irreducible and primitive; furthermore, it is tensor indecomposable and not tensor induced since $\dim V=23$ is prime. Next, we observe by Schur's Lemma that condition (i) implies $\mathbf{Z}(G)=1$. Now we can apply [G-T, Proposition 2.8] (noting that the subgroup H in its proof is just G since $G<\mathrm{SL}(V)$) and arrive at one of the following two cases.

(a) *Extraspecial case*: $P \lhd G$ for some extraspecial 23-group of order 23^3 that acts irreducibly on V. But in this case, $\chi|_P$ cannot be real-valued (in fact, $\mathbb{Q}(\chi|_P)$ would be $\mathbb{Q}(\exp(2\pi i/23))$, violating (i).

(b) *Almost simple case*: $S \lhd G \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. In this case, we can apply the main result of [H-M] and arrive at one of the following possibilities for S.

- $S = \mathsf{A}_{24}$, M_{24}, or $\mathrm{PSL}_2(23)$. Correspondingly, we have that $G = \mathsf{A}_{24}$ or S_{24}, M_{24}, and $\mathrm{PSL}_2(23)$ or $\mathrm{PGL}_2(23)$. In all of these possibilities, $\chi(x) \geq -1$ for $x \in G$ by [ATLAS], violating (iii).
- $S = \mathrm{PSL}_2(47)$. This is ruled out since $\mathbb{Q}(\chi|_S)$ would be $\mathbb{Q}(\sqrt{-47})$, violating (i).
- $S = \mathsf{Co}_3$. In this case, $G = \mathsf{Co}_3$, and this possibility is ruled out by the existence of the (conjugacy class of the) element γ in (iii). Now γ^7 has trace 7. In Co_3, the only class with trace 7 is class 2 in `Magma` notation. The only class γ with γ^7 in class 2 is either class 2 or class 29. But γ cannot be in class 2, because its trace is 0, not 7. So γ must be in class 29, which does have trace 0. However, the square of class 29 in Co_3 is class 16, whose trace is 2, not -2. Therefore we do not have Co_3.
- $S = \mathsf{Co}_2$. In this case $G = \mathsf{Co}_2$, as stated. □

Theorem 4.2. *In characteristic* 3, *the rigid local system* $\mathcal{H}(\psi, 23, 4)(1)$ *on* $\mathbb{G}_m/\mathbb{F}_3$ *has* $G_{geom} = G_{arith} = \mathsf{Co}_2$.

Proof. We know that $[23]^\star\mathcal{H}(\psi, 23, 4)(1)$ is not geometrically induced, so a fortiori $\mathcal{H}(\psi, 23, 4)(1)$ is not geometrically induced, and hence $\mathcal{H}(\psi, 23, 4)(1)$ is not arithmetically induced (as primitivity passes to overgroups). We know that $\mathcal{H}(\psi, 23, 4)(1)$ is geometrically irreducible, hence all the more arithmetically irreducible. By the Determinant Lemma 1.7, and the finiteness theorem, we know that $\mathcal{H}(\psi, 23, 4)(1)$ has integer traces and trivial determinant. In view of the Theorem 4.1, this forces G_{arith} to be Co_2. Now G_{geom} is a normal subgroup of G_{arith}, and it is nontrivial because it is itself irreducible. But Co_2 is a simple group, so G_{geom} must be Co_2. □

Corollary 4.3. *For any integer* $M \geq 1$ *prime to* 3, *the Kummer pullback* $[M]^\star\mathcal{H}(\psi, 23, 4)(1)$ *on* $\mathbb{G}_m/\mathbb{F}_3$ *has* $G_{geom} = G_{arith} = \mathsf{Co}_2$.

Proof. By Lemma 1.5, $[M]^\star\mathcal{H}(\psi, 23, 4)(1)$ is geometrically irreducible. Its G_{geom} is a then a normal subgroup of the G_{geom} of $\mathcal{H}(\psi, 23, 4)(1)$, namely Co_2, with a quotient cyclic of order dividing M. Because Co_2 is simple and nonabelian, this quotient must be trivial. Thus $[M]^\star\mathcal{H}(\psi, 23, 4)(1)$ on $\mathbb{G}_m/\mathbb{F}_3$ has $G_{geom} = \mathsf{Co}_2$. From Theorem 4.1, we see that Co_2 is maximal (and from [ATLAS] that it is minimal as well, although we will not use this) among finite irreducible subgroups of $\mathrm{SO}_{23}(\mathbb{C})$. Thus the G_{arith} of the pullback must itself be Co_2. □

References

[ATLAS] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups. Maximal Subgroups and Ordinary Characters for Simple Groups. With computational assistance from J. G. Thackray* (Oxford University Press, Eynsham, 1985).

[G-K-T] R. M. Guralnick, N. M. Katz, and P. H. Tiep, Rigid local systems and alternating groups, *Tunisian J. Math.* **1** (2019), 295–320.

[G-T] R. M. Guralnick and P. H. Tiep, Symmetric powers and a conjecture of Kollár and Larsen, *Invent. Math.* **174** (2008), 505–554.

[H-M] G. Hiss and G. Malle, Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4** (2001), 22–63.

[Ka-ESDE] N. M. Katz, *Exponential Sums and Differential Equations*, Annals of Mathematics Studies, **124** (Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.)

[Ka-G2hyper] N. M. Katz, G_2 and hypergeometric sheaves, *Finite Fields Appl.* **13** (2007), 175–223.

[Ka-GKM] N. M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Annals of Mathematics Studies, **116** (Princeton University Press, Princeton, NJ, 1988. x+246 pp.)

[Ka-RL] N. M. Katz and A. Rojas-León, Rigid local systems with monodromy group $2.J_2$, *Finite Fields Appl.* **57** (2019), 276–286.

[Ka-RL-T] N. M. Katz, A. Rojas-León, and P. H. Tiep, Rigid local systems with monodromy group the Conway group Co_3, *J. Number Theory* (to appear).

[R-L] A. Rojas-León, Finite monodromy of some families of exponential sums, *J. Number Theory* **197** (2019), 37–48.

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
E-mail address: nmk@math.princeton.edu

Departamento de Álgebra, Universidad de Sevilla, c/Tarfia s/n, 41012 Sevilla, Spain
E-mail address: arojas@us.es

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA
E-mail address: tiep@math.rutgers.edu