RIGID LOCAL SYSTEMS AND SPORADIC SIMPLE GROUPS

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

Abstract. We continue the program set up in [KT5] to study the monodromy groups of hypergeometric and Kloosterman sheaves. We gave there easy to apply criteria on these sheaves that their monodromy groups satisfy the group-theoretic condition ($\mathbf{S}+$), and showed that many of the finite almost quasisimple groups occur as monodromy groups of such sheaves. Here, we show that precisely 12 of the 26 sporadic simple groups occur in this way (and explain why the others cannot occur this way). We also treat some small rank finite groups of Lie type, as well as certain primitive complex reflection groups.

Contents

2010 *Mathematics Subject Classification.* Primary 11T23, Secondary 20C15, 20C33, 20C34, 20D06, 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 (grants DMS-1840702 and DMS-2200850), the Simons Foundation, the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton).

Part of this work was done while the third author visited the Isaac Newton Institute for Mathematical Sciences (Cambridge, UK) in Spring 2020, and the Department of Mathematics, Princeton University in Fall 2022. It is a pleasure to thank the Newton Institute and the Princeton University for hospitality and support.

The authors are grateful to Andrew Sutherland for helping them with a big computation to complete the proof of Theorem 20.6.

The authors are grateful to the referee for careful reading and thoughtful comments that helped improve the exposition of the paper.

1. Introduction

Given a prime p, it was conjectured by Abhyankar [Abh1] and proven by Raynaud [Ray] (see also [Pop]) that any finite group G which is generated by its Sylow p-subgroups occurs as a quotient of the fundamental group of the affine line $\mathbb{A}^1/\overline{\mathbb{F}_p}$. The analogous result for the multiplicative group $\mathbb{G}_m := \mathbb{A}^1 \smallsetminus \{0\}$, also conjectured by Abhyankar and proven by Harbater [Har] is that any finite group G which, modulo the subgroup $\mathbf{O}^{p'}(G)$ generated by its Sylow p-subgroups, is cyclic, occurs as a quotient of the fundamental group of $\mathbb{G}_m/\overline{\mathbb{F}_p}$. In the ideal world, given such a finite group G, and a complex representation V of G, we would be able, for any prime $\ell \neq p$, to choose an embedding of $\mathbb{C}$ into $\overline{\mathbb{Q}_\ell}$, and to write down an explicit $\overline{\mathbb{Q}_\ell}$-local system on either $\mathbb{A}^1/\overline{\mathbb{F}_p}$ or on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ whose geometric monodromy group is G, in the given representation.

In some earlier papers [KT1], [KT2], [KT3], [KT4], we have been able to do this for some particular pairs (G, V). When we were able to do this on $\mathbb{A}^1$, it was through one-parameter families of "simple to remember" exponential sums, often but not always rigid local systems on $\mathbb{A}^1$. When we have been able to do this on $\mathbb{G}_m$, it was through explicit irreducible hypergeometric sheaves of type (D, m) with $D > m$ (which include Kloosterman sheaves as the special case $m = 0$).

We took a new point of view in [KT5], where we investigated what possible (G, V) can hypergeometric sheaves of type (D, m) with $D > m$ give rise to? We consider only those that are geometrically irreducible, i.e., those that have no common character both "upstairs" and "downstairs". These are precisely the hypergeometric sheaves of type (D, m) with $D > m$ on which their geometric monodromy groups G_{geom} acts irreducibly. One also knows that if G_{geom} is finite for a hypergeometric sheaf of type (D, m) with $D > m$, then a generator of local monodromy at 0 is an element of G which has all distinct eigenvalues in the given representation (a "simple spectrum" element). And by Abhyankar, if G_{geom} is finite, then $G/\mathbf{O}^{p'}(G)$ is cyclic.

To avoid confusion, let us explain the difference between hypergeometric sheaves of type (D, m) with $D > m$, which we consider here, and hypergeometric sheaves of type (D, D). The latter correspond to the classical hypergeometric equation ${}_DF_{D-1}$, which in the case $D = 2$ carries the name of Gauss. They have been beautifully studied for general D by Beukers and Heckman [BH]. These hypergeometric sheaves are not lisse on $\mathbb{G}_m$, but rather have nontrivial local monodromy at the point 1 which is a pseudoreflection. Their monodromy groups have been completely classified by Beukers and Heckman. When they are finite, they are only "interesting" in rank $D \leq 8$.

As in [KT5], let us say that a triple (G, V, g) satisfies *the Abhyankar condition at* p if G is a finite group such that $G/\mathbf{O}^{p'}(G)$ is cyclic, V a faithful, irreducible, finite-dimensional complex representation of G, and $g \in G$ is an element of order coprime to p that has simple spectrum on V. The main objective of [KT5] was to study the natural question of which triples (G, V, g), with G a finite group, either almost quasisimple or an extraspecial normalizer, that satisfy the Abhyankar condition at p, occur "hypergeometrically", that is, as $(G_{\mathrm{geom}}, \mathcal{H}, g)$ for a hypergeometric sheaf $\mathcal{H}$ and a simple spectrum element $g \in G_{\mathrm{geom}}$ which generates local monodromy around 0 on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ such that V realizes the action of $G = G_{\mathrm{geom}}$ on $\mathcal{H}$.

The main results of [KT5] essentially classify all such triples (G, V, g) that can possibly arise from hypergeometric sheaves, and also determine the possible structure of geometric monodromy groups of hypergeometric sheaves that satisfy the group-theoretic condition ($\mathbf{S}$+). The converse problem of determining whether such triples do indeed arise from hypergeometric sheaves is the subject of [KT6], [KT7] (devoted to finite classical groups) and the present paper (dealing with sporadic groups and small-rank groups of Lie type).

A natural question is which of the 26 sporadic groups, or more generally which almost quasisimple groups G whose unique non-abelian composition factor is a sporadic group, can occur hypergeometrically, say with a hypergeometric sheaf of type (D, m) with $D > m$. As mentioned above, the first obstruction is that G must have a faithful irreducible D-dimensional representation in which some element (the one that will provide local monodromy at 0 for the hypergeometric sheaf) has simple spectrum, i..e. has D distinct eigenvalues in the representation. Such an element must have order $\geq D$ in G (for it has order $d < D$, all of its eigenvalues will be among the d^{th} roots of unity). In particular, G must have a conjugacy class of elements whose order is at least the dimension of the lowest dimensional nontrivial irreducible representation of G. This kind of obstruction rather dramatically shows that the Fischer–Griess Monster does not occur hypergeometrically: its lowest dimensional nontrivial irreducible representation has dimension 196883, whereas the largest order of any of its elements is 119. In fact, this "simple spectrum" obstruction rules out 12 of the sporadic groups as well as any of the almost quasisimple groups in which these 12 sporadic groups occur. The 14 "survivors" of this obstruction are listed in lines 2 through 15 in Table 1. Two of these survivors, namely M_{12} and HS, were shown in [KT5, Lemmas 9.6 and 9.7] not to occur hypergeometrically. What about the remaining 12 candidates? Earlier papers of ours, namely [KRL], [KRLT1]–[KRLT3], showed that $2 \cdot \mathrm{J}_2$ and each of Co_3, Co_2, $6 \cdot \mathrm{Suz}$, and $2 \cdot \mathrm{Co}_1$ occurred. One of the main results of this paper is to show that all the remaining candidates also occur, and to give for each a hypergeometric sheaf whose monodromy group it is.

We also obtain some small groups of Lie type groups in "non-generic" situations, either via a hypergeometric sheaf in the "wrong" characteristic, or a hypergeometric sheaf in the expected characteristic but which is not (known to be) part of any "family". It seems worth pointing out that each of these groups displays a group-theoretically exceptional property: either it has exceptional Schur multiplier (e.g. $\mathrm{PSL}_3(4)$ with Schur multiplier $C_4 \times C_{12}$ or $\mathrm{Sp}_6(2)$ with Schur multiplier C_2), or it can be realized as an exceptional group of Lie type (e.g. $G_2(2) \cong \mathrm{SU}_3(3) \cdot 2$ or ${}^2G_2(3) \cong \mathrm{SL}_2(8) \cdot C_3$). Furthermore, we also exhibit hypergeometric sheaves, which realize several primitive complex reflection groups in dimension 2, 4, 6, and 8, in their reflection representations (these "reflection sheaves" are marked by symbol ♠ in Table 2.) As shown in [KT9, Theorem 4.10], primitive complex reflection groups in odd dimensions ≥ 3 cannot occur this way. Finally, we construct a few multi-parameter local systems on $\mathbb{A}^m$ with finite monodromy, whose trace functions are again some "simple" exponential character sums.

To identify candidate hypergeometric sheaves $\mathcal{H}$ for a given triple (G, V, g), we use the spectrum of g on V to determine the shape of the set of "upstairs" characters of $\mathcal{H}$. To control the shape of the set of "downstairs" characters, in particular the number of them, which is the dimension of the tame part for the inertia group $I(\infty)$, we use local group theory to analyze possible candidates for the image of $I(\infty)$ in G. Each such candidate can live in many different characteristics p, and a priori there is no guarantee a given such candidate has finite geometric monodromy group $G_{\rm geom}$. A key part of the proof is to use Kubert's V-function [Ku], [Ka7, §13], to establish finite monodromy for suitable candidates (and to quickly eliminate others). Once this is done, another key part of the proof is to use representation theory to identify $G_{\rm geom}$ (as well as the arithmetic monodromy groups $G_{\rm arith}$ of suitable descents of $\mathcal{H}$). All in all, we have been able to show that all pairs (G,V) that are predicted in [KT5] to lead to hypergeometric sheaves with finite, almost quasisimple, geometric monodromy groups satisfying condition ($\mathbf{S}+$), do in fact occur hypergeometrically.

We recall from [KT5] some group-theoretic definitions that will be used throughout. For a finite group G and a prime p, $\mathbf{O}_p(G)$ denotes the largest normal subgroup of p-power order of G, $\mathbf{O}_{p'}(G)$ denotes the largest normal subgroup of order coprime to p, $\mathbf{O}^{p'}(G)$ denotes the normal subgroup of G generated by all Sylow p-subgroups of G, $\mathbf{Z}(G)$ denotes the center of G, and $G^{(\infty)}$ denotes the last term of the derived series of G. A finite group G is *quasisimple* if $G=[G,G]$ and if $G/\mathbf{Z}(G)$ is simple; it is *almost quasisimple* if $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ for some finite non-abelian simple group S. Let $\mathfrak{d}(S)$ denote the smallest degree of faithful projective irreducible complex representations of a simple group S, and let $\bar{\mathsf{o}}(g)$ denote the order of the element $g\mathbf{Z}(G)$ in $G/\mathbf{Z}(G)$ for any $g \in G$. Adopting the notation of [GMPS], let $\mathrm{meo}(X)$ denote the largest order of elements in a finite group X; also, by an *outer* automorphism of X we mean an automorphism of X which is not inner.

We also recall some basic algebro-geometric notions. A connected scheme X has (once chosen a base point $\overline{\eta}$) a profinite fundamental group $\pi_i(X,\overline{\eta})$, which up to inner automorphism is independent of the auxiliary choice of base point. Given a topological ring R, a *rank n R-local system $\mathcal{F}$ on X*, also called a *lisse R-sheaf of rank n on X*, is just a continuous homomorphism $\rho_{\mathcal{F}} : \pi_i(X,\overline{\eta}) \to \mathrm{GL}_n(R)$. When X is a connected scheme over a finite field k such that $X \otimes \overline{k}$ is connected, we refer to $\pi_1(X)$ as the *arithmetic fundamental group* of X, and we refer to $\pi_1(X \otimes \overline{k})$ as its *geometric fundamental group*. For brevity, we denote these groups $\pi_1^{\rm arith}(X)$ and $\pi_1^{\rm geom}(X)$. In this situation, for each finite extension field K/k, and each point $x \in X(K)$, the group $\pi_1^{\rm arith}(X)$ contains a well-defined *Frobenius conjugacy class $Frob_{x,K}$*. [When X/k is of finite type, these Frobenius conjugacy classes are dense; this is the Chebotarev density theorem.] Given a rank n R-local system $\mathcal{F}$ on X, with corresponding representation $\rho_{\mathcal{F}}$, the *trace function* of $\mathcal{F}$ is the rule which attaches to each pair (K,x) with K/k a finite field extension and $x \in X(K)$ the *trace of Frobenius*, i.e.,

$$\mathrm{Trace}(Frob_{x,K}|\mathcal{F}) := \mathrm{Trace}\big(\rho_{\mathcal{F}}(Frob_{x,K})\big).$$

It is often useful to think of this trace function as providing, for each finite field extension K/k, the R-valued function on the set $X(k)$ given by

$$x \in X(K) \mapsto \mathrm{Trace}(Frob_{x,K}|\mathcal{F}) := \mathrm{Trace}\big(\rho_{\mathcal{F}}(Frob_{x,K})\big).$$

A local system $\mathcal{F}$ on X is said to be *geometrically irreducible*, respectively *arithmetically irreducible*, if it is irreducible as a representation of $\pi_1^{\rm geom}(X)$, respectively of $\pi_1^{\rm arith}(X)$. Similarly, $\mathcal{F}$ is said to be *geometrically semisimple*, respectively *arithmetically semisimple*, if it is completely reducible as a representation of $\pi_1^{\rm geom}(X)$, respectively of $\pi_1^{\rm arith}(X)$.

In this paper, we are typically concerned with the case when X/k is either $\mathbb{A}^1/\mathbb{F}_q$ or $\mathbb{G}_m/\mathbb{F}_q$, with $\mathbb{F}_q$ a finite extension of $\mathbb{F}_p$, the ring R is the field $\overline{\mathbb{Q}_\ell}$ for some prime $\ell \neq p$, and $\mathcal{F}$ is a local system whose trace function is given by a simple (in the sense of simple to remember) explicit formula involving exponential sums. Our particular interest is in local systems $\mathcal{F}$ for which the images under $\rho_{\mathcal{F}}$ of $\pi_1^{\rm arith}(X) = \pi_1(X)$ and $\pi_1^{\rm geom}(X) = \pi_1(X/\overline{k})$ are finite groups, which we call the *arithmetic monodromy group*, respectively, *geometric monodromy group*, of $\mathcal{F}$. When $\mathcal{F}$ is a hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, we frequently work with its local monodromy groups at 0 and ∞: its inertia subgroup $I(0)$ with its wild inertia subgroup $P(0)$, and its inertia subgroup $I(\infty)$ with its wild inertia subgroup $P(\infty)$. We say that such an $\mathcal{F}$ has *type* (D, m), if it has rank D and, furthermore, the $I(\infty)$-tame part has dimension m (so the $I(\infty)$-wild part, usually referred to as the wild part and denoted by Wild, has dimension $W := D - m$). Given a prime p and an integer $N \geq 1$ coprime to p, μ_N denotes the unique (cyclic) subgroup of order N of $\overline{\mathbb{F}}_p^\times$, $\mathsf{Char}_N = \mathsf{Char}(N)$ denotes the set of all $\overline{\mathbb{Q}_\ell}^\times$-valued characters of $(\mathbb{F}_p(\mu_N))^\times$ of order dividing N, $\mathsf{Char}_N^\times$ denotes the subset of all such characters of order exactly N, ξ_N denotes a fixed such character of exact order N, $\mathbb{1}$ denotes the trivial character, and $\mathsf{Char}_{\rm ntriv}(N) := \mathsf{Char}(N) \smallsetminus \{\mathbb{1}\}$.

2. Almost quasisimple groups containing elements with simple spectra

One of the main results of [KT5] is the determination of all triples (G, V, g) subject to the following condition:

($\star$): G is an almost quasisimple finite group, with S the unique non-abelian composition factor, V a faithful irreducible $\mathbb{C}G$-module, and $g \in G$ has simple spectrum on V.

With G as in ($\star$), $G^{(\infty)}$ is quasisimple and $S \cong G^{(\infty)}/\mathbf{Z}(G^{(\infty)})$. On the other hand, $G/\mathbf{Z}(G)$ is almost simple: $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. We will frequently identify G with its image in $\mathrm{GL}(V)$. An element $g \in G \leq \mathrm{GL}(V)$ is called an ss-*element*, or an *element with simple spectrum*, if the multiplicity of any eigenvalue of g acting on V is 1.

Recall [Is-FGT, 9A, pp. 273-274] that for a finite group G, $E(G)$ denotes the *layer* of G, the subgroup of G generated by its subnormal quasisimple subgroups. These subgroups, the *components* of G, commute with each other, and thus $E(G)$ is the product, inside G, of its components. Under the assumption that G is almost quasisimple, $E(G)$ coincides with $G^{(\infty)}$.

Table 1, taken from [KT5], summarizes the classification of ss-elements in the non-generic cases of sporadic groups and A_7 and some small rank Lie-type groups, under the additional condition that $V|_{E(G)}$ is irreducible. For each V, we list all almost quasisimple groups G with common $E(G)$ that act on V, and we list the number of isomorphism classes of such representations in a given dimension, for a largest possible G up to scalars (if no number is given, it means the representation is unique up to equivalence in given dimension). For each representation, we list the names of conjugacy classes of ss-elements in a largest possible G, as listed in [GAP], and/or the total number of them. [Let us clarify the notion of "a largest possible G". For a pair (L, χ) in question, where L is quasisimple and χ is a faithful irreducible character of L, we list an almost quasisimple group G such that $E(G) = L$, χ extends to G, and $G/\mathbf{Z}(G)$ (which is a subgroup of $Aut(L)$ containing L) is maximal (with respect to inclusion). Modulo its center, such a group G is well-defined, but not unique a priori. However, in the cases under consideration, $G/\mathbf{Z}(G)$ turns out to be unique.]

We also give a reference where a local system realizing the given representation is constructed. The indicator $^\sharp$ signifies that we have a local system conjectured to realize the given representation, whereas (-) means that no hypergeometric sheaf with G as monodromy group can exist, as shown in [KT5, §9].

Theorem 2.1. [KT5, Theorem 6.4] *In the situation of* ($\star$)*, assume that S is one of* 26 *sporadic simple groups, or* A_7*, and that $V|_{E(G)}$ is irreducible. Then (S, G, V, g) is as listed in* Table 1.

Table 2, also (almost entirely) reproduced from [KT5, Table 3], lists certain hypergeometric sheaves

$$\mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m)$$

in characteristic p that were conjectured to produce G as geometric monodromy groups.

S	meo(Aut(S))	$\mathfrak{d}(S)$	G	dim(V)	ss-classes
A_7	12	4	$2\mathsf{A}_7$	4 (2 reps) ♯	9 classes
			S_7	6 (2 reps) [KT5, 9.3]	$7A$, $6C$, $10A$, $12A$ (4 classes)
			$3\mathsf{A}_7$	6 (2 reps) ♯	6 classes
			$6\mathsf{A}_7$	6 (4 reps) ♯	15 classes
M_{11}	11	10	M_{11}	10 (3 reps) ♯	$11AB$ (2 classes)
				11 ♯	$11AB$ (2 classes)
M_{12}	12	10	$2\mathrm{M}_{12}\cdot 2$	10 (4 reps) (-)	11 classes
			M_{12}	11 (2 reps) (-)	$11AB$ (2 classes)
			$2\mathrm{M}_{12}\cdot 2$	12 (2 reps) (-)	$24AB$ (2 classes)
M_{22}	14	10	$2\mathrm{M}_{22}\cdot 2$	10 (4 reps) ♯	10 classes
M_{23}	23	22	M_{23}	22 ♯	$23AB$ (2 classes)
M_{24}	23	23	M_{24}	23 ♯	$23AB$ (2 classes)
J_2	24	6	$2\mathrm{J}_2$	6 (2 reps) [KRL]	17 classes
			$2\mathrm{J}_2\cdot 2$	14 (2 reps) ♯	$28AB$, $24CDEF$ (6 classes)
J_3	34	18	$3\mathrm{J}_3$	18 (4 reps) ♯	$19AB$, $57ABCD$ (6 classes)
HS	30	22	$\mathrm{HS}\cdot 2$	22 (2 reps) (-)	$30A$
McL	30	22	$\mathrm{McL}\cdot 2$	22 (2 reps) ♯	$30A$, $22AB$ (3 classes)
Ru	29	28	2Ru	28 ♯	$29AB$, $58AB$ (4 classes)
Suz	40	12	6Suz	12 (2 reps) [KRLT3]	57 classes
Co_1	60	24	$2\mathrm{Co}_1$	24 [KRLT3]	17 classes
Co_2	30	23	Co_2	23 [KRLT2]	$23AB$, $30AB$ (4 classes)
Co_3	30	23	Co_3	23 [KRLT1]	$23AB$, $30A$ (3 classes)
$\mathrm{PSL}_3(4)$	21	6	$6S\cdot 2_1$	6 (4 reps) ♯	many classes
			$4_1S\cdot 2_3$	8 (8 reps) ♯	12 classes
			$2S\cdot 2_2$	10 (4 reps) ♯	$14CDEF$ (4 classes)
$\mathrm{PSU}_4(3)$	28	6	$6_1S\cdot 2_2$	6 (4 reps) ♯	many classes
$\mathrm{Sp}_6(2)$	15	7	$\mathrm{Sp}_6(2)$	7 ♯	$7A$, $8B$, $9A$, $12C$, $15A$
			$2\mathrm{Sp}_6(2)$	8 ♯	8 classes
			$\mathrm{Sp}_6(2)$	15 (-)	$15A$
$\Omega_8^+(2)$	30	8	$2\Omega_8^+(2)\cdot 2$	8 ♯	22 classes
${}^2B_2(8)$	15	14	${}^2B_2(8)\cdot 3$	14 (6 reps) ♯	$15AB$ (2 classes)
$G_2(3)$	18	14	$G_2(3)\cdot 2$	14 (2 reps) ♯	$14A$, $18ABC$ (4 classes)
$G_2(4)$	24	12	$2G_2(4)\cdot 2$	12 (2 reps) ♯	20 classes

Table 1. Elements with simple spectra in non-generic cases

In Table 2, we fix a nontrivial additive character ψ of the prime field $\mathbb{F}_p$, and for each integer $N \geq 1$ coprime to p we fix a multiplicative character ξ_N of order N. The last column indicates the conjectured image of $I(\infty)$. The shape of these sheaves was predicted using the spectrum of the ss-elements g on V as classified in Theorem 2.1, and p-local subgroups of the hypothetical group G and their possible action on V. We have also included certain local systems for the exceptional cover $3\cdot\mathsf{A}_6$, and for the two "exceptional" groups of Lie type $\mathrm{SU}_3(3)\cdot 2 \cong G_2(2)$ and $\mathrm{SL}_2(8)\cdot 3 \cong {}^2G_2(3)$, as well as certain cross-characteristic sheaves for some finite groups of Lie type (that is, when the characteristics of the sheaf and the group are unequal; this must be the case unless the rank of the sheaf is small, see [KT5, Theorem 7.3]). Furthermore, we have added local systems that realize

S	G	p	rank	$\chi_1,\dots,\chi_D$	$\rho_1,\dots,\rho_m$	Image of $I(\infty)$
A_6	$3S$	3	3	$\mathbb{1},\xi_5,\xi_5^{-1}$	$\emptyset$	$3^{1+2}:2$
	$(2\times 3S)\cdot 2_3$	5	6	$\mathsf{Char}_8 \smallsetminus \{\xi_8,\xi_8^{-1}\}$	ξ_{12},ξ_{12}^7	$5:4$
A_7	$2S$	3	4	$\mathbb{1},\xi_7,\xi_7^2,\xi_7^4$	$\emptyset$	$3^2:4$
	$2S$	5	4	$\mathbb{1},\xi_7,\xi_7^2,\xi_7^4$	$\emptyset$	$5:4$
	$3S$	5	6	$\xi_3\cdot\mathsf{Char}_7^\times$	$\mathbb{1},\xi_2$	$5:4$
	$6S$	5	6	$\xi_6\cdot\mathsf{Char}_7^\times$	ξ_8,ξ_8^{-1}	$5:8$
M_{11}	S	3	10	$\mathsf{Char}_{11}^\times$	Char_2	$3^2:8$
	S	3	10	$\mathsf{Char}_{11}^\times$	ξ_8,ξ_8^3	$3^2:8$
	S	3	11	Char_{11}	$\mathsf{Char}_4\smallsetminus\{\mathbb{1}\}$	$3^2:8$
M_{22}	$2S$	2	10	$\mathsf{Char}_{11}^\times$	ξ_7,ξ_7^2,ξ_7^4	$2^3:7$
M_{23}	S	2	22	$\mathsf{Char}_{23}^\times$	$\mathsf{Char}_{15}\smallsetminus\mathsf{Char}_{15}^\times$	$2^4:15$
M_{24}	S	2	23	Char_{23}	$\mathsf{Char}_3^\times$	$2^6:21$
McL	$S\cdot 2$	3	22	Char_{22}	$\mathsf{Char}_5^\times$	$3^{1+4}:20$
	$S\cdot 2$	5	22	Char_{22}	$\mathsf{Char}_3^\times$	$5^{1+2}:24$
J_2	$2S$	5	6	$\mathsf{Char}_{12}^\times\sqcup\mathsf{Char}_3^\times$	$\emptyset$	$5^2:12$
	$2S\cdot 2$	5	14	$\mathsf{Char}_{28}\smallsetminus\mathsf{Char}_{14}$	ξ_8,ξ_8^{-1}	$5^2:24$
J_3	$3S$	2	18	$\xi_3\cdot\mathsf{Char}_{19}^\times$	$\mathbb{1},\xi_5,\xi_5^{-1}$	$2^4:15$
Ru	$2S$	5	28	$\mathsf{Char}_{29}^\times$	$\xi_{12},\xi_{12}^3,\xi_{12}^5,\xi_{12}^9$	$5^2:24$
$\mathrm{PSL}_3(4)$	$6S$	2	6	$\mathsf{Char}_7^\times$	ξ_3	$2^4:5$
	$4_1S\cdot 2_3$	7	8	$\xi_{20}^{1,3,5,7,9,13,15,17}$	ξ_3,ξ_3^2	$7:6$
	$2S\cdot 2_2$	3	10	$\mathsf{Char}_{14}\smallsetminus\{\xi_7^{0,1,2,4}\}$	$\mathsf{Char}_4^\times$	$3^2:8$
$\mathrm{PSU}_4(3)$	$6_1\cdot S$	3	6	$\mathsf{Char}_7^\times$	ξ_2	$3^4:10$
	$6_1\cdot S$	3	6	$\mathsf{Char}_7^\times$	ξ_2,ξ_4,ξ_4^{-1}	$3_+^{1+2}:4$
$\mathrm{Sp}_6(2)$	S	7	7	$\mathsf{Char}_5\sqcup\mathsf{Char}_3^\times$	ξ_2	$7:6$
	$2S$	7	8	$\mathsf{Char}_{15}^\times$	Char_2	$7:6$
$\Omega_8^+(2)$	$2S\cdot 2$	5	8	$\mathsf{Char}_9^\times\sqcup\mathsf{Char}_2$	$\emptyset$	$5^2:8$
	$2S\cdot 2$	5	8	$\mathsf{Char}_7\sqcup\{\xi_2\}$	$\emptyset$	$5^2:8$
$G_2(3)$	$S\cdot 2$	13	14	$\mathsf{Char}_{18}\smallsetminus\{\xi_6^{0,1,2,3}\}$	$\mathsf{Char}_4^\times$	$13:12$
$G_2(4)$	$2\cdot S$	2	12	$\mathsf{Char}_{13}^\times$	$\mathsf{Char}_3^\times$	2-group : 15
$\mathrm{SU}_3(3)$	$S\cdot 2$	7	6	$\mathsf{Char}_{12}^\times\sqcup\{\xi_6,\xi_6^2\}$	$\emptyset$	$7:6$
	$S\cdot 2$	7	7	$\mathsf{Char}_{12}^\times\sqcup\mathsf{Char}_3$	ξ_2	$7:6$
${}^2B_2(8)$	$S\cdot 3$	13	14	$\mathsf{Char}_{15}\smallsetminus\{\mathbb{1}\}$	ξ_{12},ξ_{12}^5	$13:12$
$\mathrm{SL}_2(8)$	$S\cdot 3$	7	7	$\mathsf{Char}_9^\times\sqcup\{\mathbb{1}\}$	ξ_2	$7:6$
	$S\cdot 3$	7	8	$\mathsf{Char}_9\smallsetminus\{\mathbb{1}\}$	Char_2	$7:6$
$\mathrm{SU}_3(4)$	$(2\times S)\cdot 4$	5	12	$\mathsf{Char}_{16}\smallsetminus\{\xi_8^{0,1,4,7}\}$	$\emptyset$	$5^2:24$
	$(2\times S)\cdot 4$	13	12	$\mathsf{Char}_{16}\smallsetminus\{\xi_8^{0,1,4,7}\}$	$\emptyset$	$13:24$
$\Omega_8^+(2)$	$W(E_8)=2S\cdot 2$	2	$8^{\spadesuit}$	$\mathsf{Char}_{15}^\times$	$\mathsf{Char}_9\smallsetminus\mathsf{Char}_3^\times$	C_{18}
$\mathrm{PSU}_4(3)$	$6_1\cdot S\cdot 2_2$	2	$6^{\spadesuit}$	$\mathsf{Char}_7^\times$	$\xi_9^{1,3,4,6,7}$	C_{18}
$\mathrm{SU}_4(2)$	$W(E_6)=S\cdot 2$	2	$6^{\spadesuit}$	$\mathsf{Char}_9^\times$	Char_5	C_{10}
$\cong\mathrm{PSp}_4(3)$	$2S\times 3$	3	$4^{\spadesuit}$	$\mathsf{Char}_5^\times$	$\mathsf{Char}_4\smallsetminus\{\mathbb{1}\}$	C_{12}
A_5	$2S\times 5$	5	$2^{\spadesuit}$	$\mathsf{Char}_3^\times$	ξ_2	C_{10}
1	$\mathrm{SL}_2(3)$	3	$2^{\spadesuit}$	$\mathsf{Char}_4^\times$	$\mathbb{1}$	C_3

TABLE 2. Hypergeometric sheaves in non-generic cases

the Weyl groups $W(E_6) = \mathrm{SU}_4(2) \cdot 2$ and $W(E_8) = 2 \cdot \Omega_8^+(2) \cdot 2$, as well as the extended binary icosahedral group $5 \times \mathrm{SL}_2(5)$, the Witting group $3 \times \mathrm{Sp}_4(3)$, and the Mitchell group $6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$, in their reflection representations; these "reflection sheaves" are marked by symbol ♠ in the table. The notation for outer automorphisms like 2_1, 2_2, etc. is taken from [Atlas].

Each of the local systems in Table 2 will be proved in this paper to have the conjectured group G as its geometric monodromy group G_{geom} (and to satisfy $(\mathbf{S}+)$). In all cases, we also determine the arithmetic monodromy groups of suitable descents of the constructed hypergeometric sheaves.

3. Preliminary results on condition $(\mathbf{S}+)$

We work over an algebraically closed field $\mathbb{C}$ of characteristic zero, which we will take to be $\overline{\mathbb{Q}_\ell}$ for some prime ℓ in the rest of this paper. Given a finite-dimensional $\mathbb{C}$-vector space V and a Zariski closed subgroup $G \le \mathrm{GL}(V)$, recall from [GT, 2.1] that G (or more precisely the pair (G, V)) is said *to satisfy* $(\mathbf{S})$ if each of the following four conditions is satisfied.

(i) The G-module V is irreducible.
(ii) The G-module V is primitive.
(iii) The G-module V is tensor indecomposable.
(iv) The G-module V is not tensor induced.

[Note that (ii) already implies (i), but we have stated condition (i) for clarity.] We will say that (G, V) *satisfies* $(\mathbf{S}+)$ if in addition to satisfying $(\mathbf{S})$, the center $\mathbf{Z}(G)$ is finite. More generally, if Γ is any group given with a finite-dimensional representation $\Phi : \Gamma \to \mathrm{GL}(V)$, then we say (Γ, V) *satisfies* $(\mathbf{S}+)$, if $(\Phi(\Gamma), V)$ satisfies the four conditions of $(\mathbf{S})$ and, in addition, $\det(\Phi(\Gamma))$ is finite. Roughly speaking, condition $(\mathbf{S}+)$ corresponds to Aschbacher's class $\mathcal{S}$ of maximal subgroups of classical groups [Asch].

Lemma 3.1. [KT5, Lemmas 1.1, 1.4] *Suppose (G, V) satisfies the condition $(\mathbf{S}+)$, $\dim(V) > 1$, and $\mathbf{Z}(G)$ is finite. Then we have three possibilities:*

(a) *The identity component G° is a simple algebraic group, and $V|_{G^\circ}$ is irreducible.*
(b) *G is finite, and almost quasisimple, i.e. there is a finite non-abelian simple group S such that $S \lhd G/\mathbf{Z}(G) < \mathrm{Aut}(S)$. Furthermore, V is irreducible over the last term $G^{(\infty)}$ of the derived series of G.*
(c) *G is finite and it is an "extraspecial normalizer" (in characteristic r), that is, $\dim(V) = r^n$ is a power of a prime r, and G contains a normal r-subgroup $R = \mathbf{Z}(R)E$, where E is an extraspecial r-group E of order r^{1+2n} that acts irreducibly on V, and either $R = E$ or $\mathbf{Z}(R) \cong C_4$.*

Lemma 3.2. [KT5, Lemma 1.6] *Let Γ be a group, $\mathbb{C}$ an algebraically closed field of characteristic zero, $n \in \mathbb{Z}_{\ge 1}$, $\Phi : \Gamma \to \mathrm{GL}_n(\mathbb{C}) = \mathrm{GL}(V)$ a representation of Γ, and $G \le \mathrm{GL}(V)$ the Zariski closure of $\Phi(\Gamma)$. Then (Γ, V) satisfies $(\mathbf{S}+)$ if and only if (G, V) satisfies $(\mathbf{S}+)$. This equivalence holds separately for each of the four conditions defining $(\mathbf{S}+)$.*

We work in characteristic p, and use $\overline{\mathbb{Q}_\ell}$-coefficients for a chosen prime $\ell \ne p$. We fix a nontrivial additive character ψ of $\mathbb{F}_p$, with values in $\mu_p(\overline{\mathbb{Q}_\ell})$. We will consider Kloosterman and hypergeometric sheaves on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ as representations of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$, and prove that, under various hypotheses, they satisfy $(\mathbf{S}+)$ as representations of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$. As noted in Lemma 3.2, this is equivalent to their satisfying $(\mathbf{S}+)$ as representations of their geometric monodromy groups.

On $\mathbb{G}_m/\overline{\mathbb{F}_p}$, we consider a Kloosterman sheaf

$$\mathcal{K}l := \mathcal{K}l_\psi(\chi_1, \dots, \chi_D)$$

of rank $D \geq 2$, defined by an unordered list of D not necessarily distinct multiplicative characters of some finite subfield $\mathbb{F}_q$ of $\overline{\mathbb{F}_p}$. Recall [Ka4, 8.4.10.1] that any Kloosterman sheaf is geometrically irreducible.

Theorem 3.3. [KT5, Theorem 1.7] *Let $\mathcal{K}$ be a Kloosterman sheaf of rank $D \geq 2$ in characteristic p which is primitive. Suppose that $D \neq 4$. If $p = 2$, suppose also that $D \neq 8$. Then $\mathcal{K}$ satisfies* (**S+**).

There are certain cases in which a primitive Kloosterman sheaf of rank 4 satisfies (**S+**).

Lemma 3.4. *Let $\mathcal{K}$ be a Kloosterman sheaf of rank $D = 4$ in characteristic p which is primitive. Suppose that one of the following two conditions holds.*

(i) $p = 2$.

(ii) *There exists an odd integer N prime to p such that $\mathcal{K}$ is of the form*

$$\mathcal{K}l(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$$

with each $\alpha_i^N = \mathbb{1}$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Suppose further that $\prod_i \alpha_i = \mathbb{1}$, and that $\mathcal{K}$ is not geometrically self-dual (i.e., the α_i are not stable by complex conjugation).

Then $\mathcal{K}$ satisfies (**S+**).

Proof. From [KT5, Lemma 2.2], $\mathcal{K}$ is tensor indecomposable. It remains to show that it is not tensor induced. We argue by contradiction. Since $D = 4$, the only possibility is that it is 2-tensor induced. By [KT5, Lemma 3.2], this forces 2 to be prime to p. Suppose now that (ii) holds. Then $[2]^\star\mathcal{K}$ is tensor decomposable, say

$$[2]^\star\mathcal{K} \cong \mathcal{A} \otimes \mathcal{B},$$

with $\mathcal{A}, \mathcal{B}$ local systems of rank 2 on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, cf. [KT5, Lemma 2.1 (i)]. Moreover, by [KT5, Lemma 2.1 (ii)], we may assume both of $\mathcal{A}, \mathcal{B}$ are tame at 0.

We now consider the $I(0)$ representations. That of $[2]^\star\mathcal{K}$ is the direct sum of the characters α_i^2. Therefore the $I(0)$ representations of each of $\mathcal{A}, \mathcal{B}$ must be semisimple, say $\mathcal{A}_{I(0)} = \Lambda_1 + \Lambda_2$, $\mathcal{B}_{I(0)} = \Lambda_3 + \Lambda_4$. replacing $\mathcal{A}$ by $\mathcal{L}_{1/\Lambda_1} \otimes \mathcal{A}$ and replacing $\mathcal{B}$ by $\mathcal{L}_{\Lambda_1} \otimes \mathcal{B}$, we may assume further that

$$\mathcal{A}_{I(0)} = \mathbb{1} + \Lambda_2, \quad \mathcal{B}_{I(0)} = \Lambda_3 + \Lambda_4.$$

Expanding their tensor product, we get that Λ_3, Λ_4 are each among the α_i^2, so each have order dividing N. This then forces Λ_2 to have order dividing N. Fix a character ρ of order N, and write

$$\Lambda_1 = \rho^a, \;\; \Lambda_2 = \rho^b, \quad \Lambda_1 = \rho^s.$$

Thus

$$(\mathbb{1} + \rho^a) \otimes (\rho^b + \rho^c) = \rho^b + \rho^c + \rho^{a+b} + \rho^{a+c}$$

is the sum of the α_i^2. By assumption, the product of the α_i is $\mathbb{1}$, so also the product of their squares. Therefore the product of the four characters $\rho^b, \rho^c, \rho^{a+b}, \rho^{a+c}$ is trivial. So we have

$$b + c + a + b + a + c \equiv 0 \pmod{N},$$

i.e. $2(a + b + c) \equiv 0 \pmod{N}$. As N is odd, we have $a + b + c \equiv 0 \pmod{N}$. Thus the four characters are $\rho^b, \rho^c, \rho^{-c}, \rho^{-b}$, which occur in complex conjugate pairs. Therefore the α_i^2 occur in complex conjugate pairs, say $\alpha_1^2\alpha_2^2 = \mathbb{1}, \alpha_3^2\alpha_4^2 = \mathbb{1}$. As N is odd, this forces $\alpha_1\alpha_2 = \mathbb{1}, \alpha_3\alpha_4 = \mathbb{1}$. $\square$

We next consider a hypergeometric sheaf $\mathcal{H}$ of type (D, m) with $D > m \geq 0$, thus

$$\mathcal{H} = \mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m).$$

Here the χ_i and ρ_j are (possibly trivial) multiplicative characters of some finite subfield $\mathbb{F}_q$, with the proviso that no χ_i is any ρ_j. [The case $m = 0$ is precisely the Kloosterman case.]

Theorem 3.5. [KT5, Theorem 1.9] *Let $\mathcal{H}$ be a hypergeometric sheaf of type (D, m) with $D > m > 0$, with $D \geq 4$. Suppose that $\mathcal{H}$ is primitive, $p \nmid D$, and $W > D/2$. If p is odd and $D = 8$, suppose $W > 6$. If $p \neq 3$, suppose that either $D \neq 9$, or that both $D = 9$ and $W > 6$. Then $\mathcal{H}$ satisfies* $(\mathbf{S+})$.

In the case when p divides D, we need stronger hypotheses to show that $(\mathbf{S+})$ holds.

Theorem 3.6. [KT5, Theorem 1.12] *Let $\mathcal{H}$ be a hypergeometric of type (D, m) with $D > m > 0$, with $D > 4$. Suppose that $\mathcal{H}$ is primitive. Suppose that $p|D$, and $W > (2/3)(D-1)$. If $p = 2$, suppose $D \neq 8$. If $p = 3$, suppose (D, m) is not $(9, 1)$. Then $\mathcal{H}$ satisfies* $(\mathbf{S+})$.

To determine the primitivity of a sheaf $\mathcal{H}$, we will use

Proposition 3.7. [KRLT3, Proposition 1.2] *Suppose that $\mathcal{H}$ is geometrically induced, i.e. that there exists a smooth connected curve $U/\overline{\mathbb{F}_q}$, a finite étale map $\pi : U \to \mathbb{G}_m/\overline{\mathbb{F}_q}$ of degree $d \geq 2$, a lisse sheaf $\mathcal{G}$ on U, and an isomorphism $\mathcal{H} \cong \pi_\star \mathcal{G}$. Then up to isomorphism we are in one of the following situations.*

(i) (**Kummer induced**) *$U = \mathbb{G}_m$, π is the N^{th} power map $x \mapsto x^N$ for some $N \geq 2$ prime to p with $N|n$ and $N|m$, $\mathcal{G}$ is a hypergeometric sheaf of type $(n/N, m/N)$, and the lists of χ_i and of ρ_j are each stable under multiplication by any character Λ of order dividing N.*

(ii) (**Belyi induced**) *$U = \mathbb{G}_m \smallsetminus \{1\}$, π is either $x \mapsto x^A(1-x)^B$ or is $x \mapsto x^{-A}(1-x)^{-B}$, $\mathcal{G}$ is $\mathcal{L}_{\Lambda(x)} \otimes \mathcal{L}_{\sigma(x-1)}$ for some multiplicative characters Λ and σ, and one of the following holds:*
  (a) *Both A, B are prime to p, but $A + B = d_0 p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^A(1-x)^B$, the χ_i are all the A^{th} roots of Λ and all B^{th} roots of σ, and the ρ_j are all the ${d_0}^{\text{th}}$ roots of $(\Lambda\sigma)^{1/p^r}$.*
  (b) *A is prime to p, $B = d_0 p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^{-A}(1-x)^{-B}$, the χ_i are all the $(A+B)^{\text{th}}$ roots of $\Lambda\sigma$, and the ρ_j are all the A^{th} roots of Λ and all the ${d_0}^{\text{th}}$ roots of σ^{1/p^r}.*
  (c) *B is prime to p, $A = d_0 p^r$ with $p \nmid d_0$ and $r \geq 1$. In this case π is $x \mapsto x^{-A}(1-x)^{-B}$, the χ_i are all the $(A+B)^{\text{th}}$ roots of $\Lambda\sigma$, and the ρ_j are all the B^{th} roots of σ together with all the ${d_0}^{\text{th}}$ roots of Λ^{1/p^r}.*

The following two statements are useful in studying representations with irrational traces:

Lemma 3.8. [KT5, Lemma 6.3] *Let $\Phi : G \to \mathrm{GL}(V) \cong \mathrm{GL}_{n-1}(\mathbb{C})$ be a faithful irreducible representation of a finite almost quasisimple group G, which contains a normal subgroup $S \cong \mathsf{A}_n$ with $n \geq 7$. Suppose that*

(a) *$V|_S \cong S^{(n-1,1)}|_S$, where $S^{(n-1,1)}$ denotes the "deleted permutation representation" of S_n, and*
(b) *$\mathbb{Q}(\varphi) \subseteq \mathbb{K}$ for some number field $\mathbb{K}$, if φ denotes the character of Φ.*

Then $\mathbb{Q}(\varphi) \subseteq \mathbb{K}_0$, the subfield obtained by joining to $\mathbb{Q}$ all roots of unity that belong to $\mathbb{K}$. In fact, $\mathbb{Q}(\varphi)$ is some cyclotomic extension $\mathbb{Q}(\zeta_m)$ contained in $\mathbb{K}$, and $\mathrm{Tr}(\Phi(g))$ is an integer multiple of a root of unity for any $g \in G$.

Lemma 3.9. *Let G and H be two finite, almost quasisimple groups with $G^{(\infty)} = H^{(\infty)}$ and $G/\mathbf{Z}(G) = H/\mathbf{Z}(H)$ (as subgroups of $\mathrm{Aut}(S)$ for S the unique non-abelian composition factor of G). Let $\varphi \in \mathrm{Irr}(G)$ and $\psi \in \mathrm{Irr}(H)$ be irreducible characters such that $\varphi|_L = \psi|_L \in \mathrm{Irr}(L)$. Then there exists a root of unity $\gamma \in \mathbb{C}$ such that*

(a) *$\mathbb{Q}(\varphi) \subseteq \mathbb{Q}(\psi)(\gamma)$ and $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\varphi)(\gamma)$, and*
(b) *If $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\varphi)$ in addition, then $\mathbb{Q}(\varphi) = \mathbb{Q}(\psi)(\gamma)$.*

Under the extra assumption that $\mathbb{Q}(\psi) = \mathbb{Q}$, we also have that $\varphi(g)$ is an integer multiple of a root of unity for any $g \in G$.

Proof. Let φ be afforded by a representation $\Phi : G \to \mathrm{GL}(V)$ and let ψ be afforded by a representation $\Psi : H \to \mathrm{GL}(V)$, for a complex vector space V. Since $\varphi|_L = \psi|_L \in \mathrm{Irr}(L)$, we may assume that $\Phi|_L = \Psi|_L$. Consider any $g \in G$. Since $G/\mathbf{Z}(G) = H/\mathbf{Z}(H)$, there is $h \in H$ such that g and h induce the same automorphism of $S = L/\mathbf{Z}(L)$ via conjugations. Applying Φ and Ψ, we see that $x := \Psi(h^{-1})\Phi(g)$ centralizes $\Phi(L)$ modulo scalars in $\mathrm{GL}(V)$, i.e. $[x, \Phi(L)] \leq \mathbf{Z}(\mathrm{GL}(V))$ and so $[[x, \Phi(L)], \Phi(L)] = 1$. But $L = [L, L]$, so $\Phi(L) = [\Phi(L), \Phi(L)]$ and $[x, \Phi(L)] = [x, [\Phi(L), \Phi(L)]] = 1$ by the Three Subgroups Lemma. Hence $x = \alpha_g \cdot \mathrm{Id}$ for some $\alpha_g \in \mathbb{C}$, i.e. $\Phi(g) = \alpha_g \Psi(h)$. Since both g and h are of finite order, in fact α_g is a root of unity. Taking

$$N := \mathrm{lcm}\big(\mathsf{o}(\alpha_g) \mid \varphi(g) \neq 0\big),$$

and $\gamma := \zeta_N$, we see that $\varphi(g) = \alpha_g\psi(h) \in \mathbb{Q}(\psi)(\gamma)$ and $\psi(h) = \alpha_g^{-1}\varphi(g) \in \mathbb{Q}(\varphi)(\gamma)$, proving the first two inclusions. Assume now that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\varphi)$. Then, when $\varphi(g) \neq 0$, we have that $\psi(h) \neq 0$ and $\alpha_g = \varphi(g)/\psi(h) \in \mathbb{Q}(\varphi)$. This implies by the choice of N that $\gamma \in \mathbb{Q}(\varphi)$, and so $\mathbb{Q}(\varphi) = \mathbb{Q}(\psi)(\gamma)$.

Under the extra assumption that $\mathbb{Q}(\psi) = \mathbb{Q}$, we also see that $\varphi(g) = \alpha_g\psi(h) \in \alpha_g\mathbb{Z}$. □

4. G_{geom} AND G_{arith}

Let k be a finite field of characteristic p, X/k a geometrically connected smooth k-scheme of dimension $d \geq 1$, $\ell \neq p$ a prime number, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on X. We view $\mathcal{F}$ as a representation of $\pi_1^{\mathrm{arith}}(X) := \pi_1(X)$ and also as a representation of $\pi_1^{\mathrm{geom}}(X) := \pi_1(X \otimes_k \overline{k})$, a closed normal subgroup of $\pi_1^{\mathrm{arith}}(X)$ which sits in a short exact sequence

$$1 \to \pi_1^{\mathrm{geom}}(X) \to \pi_1^{\mathrm{arith}}(X) \to Gal(\overline{k}/k) \to 1.$$

We define algebraic groups $G_{\mathrm{geom}} \lhd G_{\mathrm{arith}}$ to be the Zariski closures of the images of $\pi_1^{\mathrm{geom}}(X)$ and of $\pi_1^{\mathrm{arith}}(X)$ respectively.

For ease of later reference, we state a useful fact about the compatibility of the formation of Zariski closure with group homomorphisms, cf. [Bor, Chapter I, &2, 2.1(f)].

Lemma 4.1. *Let G, H be linear algebraic groups over an algebraically closed field k, and $f : G \to H$ a k-homomorphism of algebraic groups. Let $\Gamma \subset G(k)$ be a subgroup of the "abstract" group $G(k)$. Denote by $\overline{\Gamma}$ the Zariski closure of Γ in G, and by $\overline{f(\Gamma)}$ the Zariski closure of $f(\Gamma)$ in H. Then $f(\overline{\Gamma}) = \overline{f(\Gamma)}$.*

Lemma 4.2. *Suppose G_{arith} for $\mathcal{F}$ is finite. Then the quotient group $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ is a finite cyclic group. It is generated by the image in $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ of any Frobenius element $Frob_{x,k}$ at any k valued point $x \in X(k)$. Its order is the least integer $N \geq 1$ such that $Frob_{x,k}^N$ lands in G_{geom}.*

Proof. If G_{arith} is finite, then its quotient $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ is a finite quotient of the pro-cyclic group $\mathrm{Gal}(\overline{k}/k)$. In $\mathrm{Gal}(\overline{k}/k)$, the image of any $Frob_{x,k}$ is a topological generator. Thus $G_{\mathrm{arith}}/G_{\mathrm{geom}}$ is the finite cyclic group generated by the image of any $Frob_{x,k}$. □

Corollary 4.3. *In the situation of the lemma, let $d \geq 1$ be an integer, let k_d/k denote the extension of degree d, and let $N := |G_{\mathrm{arith}}/G_{\mathrm{geom}}|$. Then for the pullback $\mathcal{F}_d$ of $\mathcal{F}$ to $X \otimes_k k_d$, $G_{\mathrm{geom},\mathcal{F}_d} = G_{\mathrm{geom},\mathcal{F}}$ remains the same, but $G_{\mathrm{arith},\mathcal{F}_d} \lhd G_{\mathrm{arith},\mathcal{F}}$ is the subgroup of index $\gcd(d, N)$. In particular, $G_{\mathrm{arith},\mathcal{F}_d} = G_{\mathrm{geom}}$ if and only if $N|d$.*

Proof. The invariance of G_{geom} is a tautology. Pick $x \in X(k)$. The quotient $G_{\mathrm{arith},\mathcal{F}_d}/G_{\mathrm{geom}}$ is the subgroup of $G_{\mathrm{arith},\mathcal{F}}/G_{\mathrm{geom}}$ generated by $Frob_{x,k_d} = (Frob_{x,k})^d$. So this is the statement that the subgroup of $\mathbb{Z}/N\mathbb{Z}$ generated by the integer d is as asserted. □

5. Structure of G_{geom}

First we recall several results concerning the structure of the geometric monodromy group G_{geom} of an irreducible hypergeometric sheaf, and the images of local monodromies $I(0)$ and $I(\infty)$ in G_{geom}.

Theorem 5.1. [KT5, Theorem 4.1] *Let $\mathcal{H}$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, with $p \neq \ell$, and of type (D, m) with wild part of dimension $D - m \geq 2$. Denote by G_0 the Zariski closure inside the geometric monodromy group G_{geom} of the normal subgroup generated by all G_{geom}-conjugates of the image of $I(0)$. Then $G_0 = G_{\mathrm{geom}}$. In particular, if G_{geom} is finite then it is generated by all G_{geom}-conjugates of the image of $I(0)$, and $G_{\mathrm{geom}} = \mathbf{O}^p(G_{\mathrm{geom}})$.*

The next theorem is the $D - m = 1$ analogue of Theorem 5.1.

Theorem 5.2. *Let $\mathcal{H} = \mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_{D-1})$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, with $p \neq \ell$, and of type (D, m) with wild part of dimension $D - m = 1$. Denote by G_0 the Zariski closure inside the geometric monodromy group G_{geom} of the normal subgroup generated by all G_{geom}-conjugates of the image of $I(0)$. Then the quotient G_{geom}/G_0 is the additive group $\mathbb{F}_p$, and the projection of G_{geom} onto this $\mathbb{F}_p$, viewed by composition as a homomorphism $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \to \mathbb{F}_p$ is the geometric monodromy group of $\mathcal{L}_\psi$.*

Proof. Let $K := G_{\mathrm{geom}}/G_0$. Because $\mathcal{H}$ is geometrically irreducible, G_{geom} has a faithful irreducible representation, and hence is reductive. Therefore its quotient K is reductive.

By the arithmetic determinant formula [Ka4, Theorem 8.12.2 (3)], a prime to p power of $\det(\mathcal{H})$ is $\mathcal{L}_{\psi(ax)}$ for some $a \in \mathbb{F}_p^\times$, which is certainly trivial on the (pro) prime to p image of $I(0)$. So the quotient K admits a nontrivial quotient $\mathcal{L}_\psi$. So K is nontrivial.

Consider a nontrivial irreducible representation, say ρ, of K. View ρ as an irreducible representation of the reductive group G_{geom}. Then ρ, indeed any irreducible representation of G_{geom}, is a direct summand of some

$$\mathcal{H}^{\otimes a} \otimes (\mathcal{H}^\vee)^{\otimes b}.$$

Consider now the $P(\infty)$-representation of $\mathcal{H}$. By hypothesis, it is of the form $(\mathsf{Wild}_1) \oplus (D-1)\mathbb{1}$, with Wild_1 a one-dimensional representation with $\mathsf{Swan}_\infty = 1$. From the arithmetic determinant formula, we see that $\mathsf{Wild}_1 = \mathcal{L}_\psi$. From this retain only that the $P(\infty)$-representation of $\mathcal{H}$ is a direct sum of various $\mathcal{L}_{\psi(ax)}$ with $a \in \mathbb{F}_p$. Therefore the $P(\infty)$-representation of $\mathcal{H}^{\otimes a} \otimes (\mathcal{H}^\vee)^{\otimes b}$ is also such a direct sum, and hence the $P(\infty)$-representation of ρ is such a direct sum.

Now view ρ as a representation of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$. So viewed, ρ is trivial on $I(0)$, so may be viewed as a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{F}_\rho$ on the affine line $\mathbb{A}^1/\overline{\mathbb{F}_p}$ which is irreducible and nontrivial. Therefore $H^i_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}_\rho) = 0$ for $i \neq 1$. By the Euler-Poincare formula [Ka3, 2.3.1],

$$\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}_\rho) = \mathrm{rank}(\mathcal{F}_\rho) - \mathsf{Swan}_\infty(\mathcal{F}_\rho),$$

and hence

$$h^1_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}_\rho) = \mathsf{Swan}_\infty(\mathcal{F}_\rho) - \mathrm{rank}(\mathcal{F}_\rho).$$

As $h^1_c \geq 0$, we find that

$$\mathsf{Swan}_\infty(\mathcal{F}_\rho) \geq \mathrm{rank}(\mathcal{F}_\rho).$$

The $P(\infty)$-representation of $\mathcal{F}_\rho$ is a direct sum with multiplicities of various $\mathcal{L}_{\psi(ax)}$ with $a \in \mathbb{F}_p$. Thus $\mathsf{Swan}_\infty(\mathcal{F}_\rho)$ is the total number of constituents $\mathcal{L}_{\psi(ax)}$ with $a \in \mathbb{F}_p^\times$. In particular,

$$\mathsf{Swan}_\infty(\mathcal{F}_\rho) \leq \mathrm{rank}(\mathcal{F}_\rho).$$

Therefore we have equality:

$$\mathsf{Swan}_\infty(\mathcal{F}_\rho) = \mathrm{rank}(\mathcal{F}_\rho),$$

and the $P(\infty)$-representation of $\mathcal{F}_\rho$ is a direct sum

$$\mathcal{F}_\rho|_{P(\infty)} = \bigoplus_{a \in \mathbb{F}_p^\times} n_a \mathcal{L}_{\psi(ax)}.$$

Because $\mathcal{F}_\rho$ is lisse and geometrically irreducible on $\mathbb{A}^1$, it is perverse irreducible. Therefore its Fourier Transform $FT_\psi(\mathcal{F}_\rho)$ is perverse irreducible. But this FT has generic rank zero (indeed vanishes outside $\mathbb{F}_p^\times$), and so is punctual. But the only punctual sheaf which is perverse irreducible is a single delta sheaf. So our FT must be δ_{-a} for some $a \in \mathbb{F}_p^\times$. By Fourier inversion, we find that $\mathcal{F}_\rho$ is $\mathcal{L}_{\psi(-x)}$.

Here is another, more elementary, version of the argument of this last paragraph. We first show that $\mathcal{F}_\rho$ has rank one. Indeed, it is has rank 2 or more, and we choose an $a \in \mathbb{F}_p^\times$ such that $\mathcal{L}_{\psi(ax)}$ occurs in the $P(\infty)$-representation of $\mathcal{F}_\rho$, then $\mathcal{F}_\rho \otimes \mathcal{L}_{\psi(-ax)}$ remains geometrically irreducible and nontrivial, and keeps the same rank, but its Swan_∞ has decreased, which violates the inequality $\mathsf{Swan}_\infty \geq$ rank. Once $\mathcal{F}_\rho$ has rank one, then $\mathcal{F}_\rho \otimes \mathcal{L}_{\psi(-ax)}$ is both lisse at 0 and tame at ∞, so is geometrically trivial, which is to say that $\mathcal{F}_\rho \cong \mathcal{L}_{\psi(ax)}$.

Thus the only nontrivial irreducible representations of the reductive group K are the $p-1$ characters of order p given by the $\mathcal{L}_{\psi(ax)}$ as a ranges over $\mathbb{F}_p^\times$. Therefore K is itself the additive group of $\mathbb{F}_p$, and each nontrivial character of K is an $\mathcal{L}_{\psi(-ax)}$. □

Theorem 5.3. [KT5, Theorem 4.7] *Let $\mathcal{H}$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ definable on $\mathbb{G}_m/\mathbb{F}_q$ for some finite extension $\mathbb{F}_q/\mathbb{F}_p$, with $p \neq \ell$, and of type (D,m) with $D > m$. Denote by $G_{P(\infty)}$ the Zariski closure inside the geometric monodromy group $G_{\rm geom}$ of the normal subgroup generated by all $G_{\rm geom}$-conjugates of the image of the wild inertia group $P(\infty)$. Then $G_{\rm geom}/G_{P(\infty)}$ is a finite cyclic p'-group.*

We can be more specific about the order of the finite cyclic p'-group of Theorem 5.3. Recall that $\mathbb{G}_m(\overline{\mathbb{F}_p})$ acts on itself via translations $x \mapsto ax$, $a \in \overline{\mathbb{F}_p}^\times$. These translations fix each of the points 0 and ∞, and hence yield outer automorphism (outer because of not fixing chosen base points) on each of the groups $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$, $I(0)$, $I(\infty)$, $P(\infty)$. Because this action, for a fixed $a \in \overline{\mathbb{F}_p}^\times$, is well-defined up to an inner automorphism on each of these groups, it has a well-defined action, called *multiplicative translation by* a, on equivalence classes of irreducible $\overline{\mathbb{Q}_\ell}$-representations Φ of each of these groups, sending the equivalence class of Φ to its *multiplicative translate by* a.

Corollary 5.4. *Let $\mathcal{H} := \mathcal{H}yp_\psi(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m)$ be an irreducible $\overline{\mathbb{Q}_\ell}$-hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, definable on $\mathbb{G}_m/\mathbb{F}_q$ for some finite extension $\mathbb{F}_q/\mathbb{F}_p$, with $p \neq \ell$* (i.e. all the characters χ_i, ρ_j are of finite order). *Suppose $D > m$. Write $W := D - m$, the dimension of* Wild *(the wild part of the $I(\infty)$-representation) as $W = w_0 p^a$ with w_0 prime to p and $a \geq 0$. Define integers A, B, C, E as follows.*

(a) $A :=$ lcm(orders of the χ_i).
(b) $B :=$ lcm(orders of the ρ_j) *if* $m > 0$, $B := 1$ *if* $m = 0$.
(c) $C := w_0$ *if* $a = 0$ (i.e. if $p \nmid w$), $C := w_0(p^a + 1)$ *if* $a > 0$.
(d) *D is the order of any character Λ such that* $\Lambda^{pW} = \det(\mathsf{Wild})^p \otimes \xi_2^{W-1}$, *with the understanding that if $p = 2$ then $\xi_2 := \mathbb{1}$, cf.* (5.4.1) *for the explicit formula for* $\det(\mathsf{Wild})$.

Then the order of the finite cyclic p'-group $G_{\rm geom}/G_{P(\infty)}$ divides $\gcd(A, \mathrm{lcm}(B, C, D))$.

Proof. Let us denote by K the finite cyclic p'-group $G_{\rm geom}/G_{P(\infty)}$, and by $K(0)$ and $K(\infty)$ the images of $I(0)$ and $I(\infty)$, respectively, in K. We know that the resulting map $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow K$ corresponds to a Kummer sheaf $\mathcal{L}_\sigma$ for some character σ of finite order, which is $\#K(0) = \#K(\infty)$. $K(0)$ is a rank one quotient of the image of $I(0)$ on $\mathcal{H}$, so has order dividing A. The group $K(\infty)$

is a quotient of the image of $I(\infty)$ on $\mathcal{H}$. Let us write this image as $\mathsf{Wild} + \mathsf{Tame}$ (in the category of $I(\infty)$-representations). The image of $I(\infty)$ on $\mathsf{Wild} + \mathsf{Tame}$ is a subgroup of the product

$$(\text{the image of } I(\infty)|\mathsf{Tame}) \times (\text{the image of } I(\infty)|\mathsf{Wild}).$$

Thus $K(\infty)$ is a subgroup of the product of a rank one quotient of $I(\infty)|\mathsf{Tame}$ with a rank one quotient of $I(\infty)|\mathsf{Wild}$). The first factor has order dividing B.

It remains to explain that $\mathrm{lcm}(C, D)$ is the order the quotient of $I(\infty)|\mathsf{Wild}$ by its p-Sylow subgroup. [Note that while $I(\infty)|\mathsf{Tame}$ need not be a finite group, indeed will be finite precisely when the ρ_j are all distinct, the group $I(\infty)|\mathsf{Wild}$ is always finite, cf. [KT9, Proposition 5.2].]

Suppose first that $W = 1$. Then Wild is of the form $\mathcal{L}_\psi \otimes \mathcal{L}_\tau$, and we recover τ as the Λ in the definition of D. So here $C = 1$ and D is the order of τ, so indeed $\mathrm{lcm}(C, D)$ is as asserted in this case.

Suppose next that $W \geq 2$, so that $\det(\mathsf{Wild})$ is tame (because all slopes of Wild are $1/W < 1$, hence $\det(\mathsf{Wild})$ has its unique slope, which is its Swan conductor, < 1 and hence, being a nonnegative integer, is 0). Thus $\det(\mathcal{H})$ is tame at both 0 and ∞, and hence the determinants at both 0 and ∞ are the **same** Kummer sheaf $\mathcal{L}_\sigma$. At 0, the determinant is $\prod_i \chi_i$. At ∞, the determinant is $\det(\mathsf{Wild}) \otimes \prod_j \rho_j$. Equating the two expressions, we see that

$$\det(\mathsf{Wild}) = \big(\prod_i \chi_i\big)/\big(\prod_j \rho_j\big). \tag{5.4.1}$$

The idea now is to exploit the fact that the isomorphism class of Wild as an $I(\infty)$-representation is determined, up to a multiplicative translation, by its determinant, cf. [Ka4, 8.6.3]. This allows us to consider the *canonical extension* of a given $I(\infty)$-representation: it is a lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ with the imposed $I(\infty)$-representation and which is tame at 0. It has the remarkable property that If we form the canonical extension $\mathcal{F}_{\mathsf{Wild}}$ of Wild in the sense of [Ka2, §1.5], then by [Ka2, 1.4.12] the quotient of $I(\infty)|\mathsf{Wild}$ by its p-Sylow subgroup is precisely the image of $I(0)$ on $\mathcal{F}_{\mathsf{Wild}}$.

In the case when $W > 1$ is prime to p, one knows [Ka2, 1.3.2, 4)] that $\mathcal{K}l_\psi(\mathsf{Char}_W)$ is a canonical extension. Its determinant is $\mathbb{1}$ if W is odd, and is the quadratic character ξ_2 if W is even (which forces p to be odd), so its Wild has determinant $\mathbb{1}$ if W is odd, and ξ_2 if is even. If we tensor $\mathcal{K}l_\psi(\mathsf{Char}_W)$ with $\mathcal{L}_\Lambda$, then we have the canonical extension of the previous Wild tensored with $\mathcal{L}_\Lambda$, whose determinant is thus $\Lambda^W \xi_2^{W-1}$. Thus $\mathrm{lcm}(C, D)$ is as asserted in this case.

In the case when $W = w_0 p^a$ with $a \geq 1$, we know, by a theorem of Pink, cf. [KT1, 20.3] and [Ka2, 1.3.2 (4)], that the Kummer direct image

$$[w_0]_\star \mathcal{K}l_{\psi_{w_0}}\big(\mathsf{Char}_{\mathrm{ntriv}}(p^a + 1)\big) \cong \mathcal{K}l_\psi\big(\mathsf{Char}(w_0(p^a + 1)) \setminus \mathsf{Char}(w_0)\big)$$

is a canonical extension. Its determinant, which is also $\det(\mathsf{Wild})$, is $\mathbb{1}$ if pw_0 is even, and is $\mathbb{1}$ if pw_0 is odd. If we tensor with $\mathcal{L}_\Lambda$, we change $\det(\mathsf{Wild})$ by a factor of Λ^W, and we now have characters of the form Λ(a character of order dividing $w_0(p^a+1)$). Thus $\mathrm{lcm}(C, D)$ is as asserted in this case. ☐

Remark 5.5. Here is an immediate application of Corollary 5.4. Let $q = p^a$ with $a > 0$, and $\mathcal{K}l_\psi(\chi_1, \ldots, \chi_q)$. Suppose that $\prod_i \chi_i = \xi_2$. Then the order of the finite cyclic p'-group $G_{\mathrm{geom}}/G_{P(\infty)}$ divides both lcm(orders of the χ_i) and $q + 1$. For an apparently more striking application, take the Kloosterman sheaf of any rank $n \geq 2$ with all its characters $\mathbb{1}$, i.e. the "classical" rank n Kloosterman sheaf $\mathcal{K}l_n$ studied in [Ka3, 11.0.1]. Here we have $A = 1$, and hence $G_{\mathrm{geom}} = G_{P(\infty)}$ for $\mathcal{K}l_n$.

As another application, take any (irreducible) hypergeometric of type (D, m) with $D > m$ and all "upstairs" characters $\mathbb{1}$. Again here we have $A = 1$, and hence $G_{\mathrm{geom}} = G_{P(\infty)}$. But there is a simpler explanation. The action of $I(0)$ is unipotent, and so the group G_0 of Theorem 5.1 is connected. If $D - m \geq 2$, then $G_{\mathrm{geom}} = G_0$ by Theorem 5.1, hence G_{geom} is connected, so has no nontrivial finite quotient. If $D - m = 1$, then by Theorem 5.2, the quotient G_{geom}/G_0 has order p. So in this $W = 1$ case, $G_{\rm geom}$ has no finite quotient of order prime to p, and once again $G_{\rm geom} = G_{P(\infty)}$.

Proposition 5.6. [KT5, Proposition 4.8] *Let $\mathcal{H}$ be an (irreducible) hypergeometric sheaf of type (D,m) in characteristic p, with $D > m$ and with geometric monodromy group $G = G_{\rm geom}$. Then the following statements hold for the image Q of $P(\infty)$ in G:*

(i) *If $\mathcal{H}$ is not Kloosterman, i.e. if $m > 0$, then $Q \cap \mathbf{Z}(G) = 1$.*
(ii) *Suppose $\mathcal{H}$ is Kloosterman and $D > 1$. Then $Q \not\leq \mathbf{Z}(G)$. If $p \nmid D$, then $Q \cap \mathbf{Z}(G) = 1$. If $p|D$ then either $Q \cap \mathbf{Z}(G) = 1$ or $Q \cap \mathbf{Z}(G) \cong C_p$.*
(iii) *If $D > 1$, then $1 \neq Q/(Q \cap \mathbf{Z}(G)) \hookrightarrow G/\mathbf{Z}(G)$ and p divides $|G/\mathbf{Z}(G)|$.*
(iv) *If $D - m \geq 2$, the determinant of G is a p'-group. If moreover $p \nmid D$, then $\mathbf{Z}(G)$ is a p'-group.*
(v) *Suppose that $p = 2$ and G is finite. Then the trace of any element $g \in G$ on $\mathcal{H}$ is 2-rational* (i.e. lies in a cyclotomic field $\mathbb{Q}(\zeta_N)$ for some odd integer N)*; in particular, the 2-part of $|\mathbf{Z}(G)|$ is at most 2.*

Remark 5.7. If the rank D of a hypergeometric sheaf $\mathcal{H}$ is divisible by its characteristic p, then, even when the sheaf has trivial geometric determinant, the center of its geometric monodromy group can still have order divisible by p – see e.g. Theorems 18.2 and 25.2, as well as the sheaves of rank 24 with geometric monodromy group $2 \cdot \mathrm{Co}_1$ and of rank 12 with geometric monodromy group $6 \cdot \mathrm{Suz}$ in [KRLT3]. Moreover, if $D - m = 1$, then the determinant of G has order divisible by p, simply because a nontrivial element in the image of $P(\infty)$ acts as a complex reflection, i.e., a pseudoreflection, of p-power order; see Theorem 30.7 (below) for examples of such sheaves.

Proposition 5.8. [KT5, Proposition 4.10] *Let $\mathcal{H}$ be an irreducible hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ of type (D,m) with $W := D - m > 0$ the dimension of the wild part Wild of the $I(\infty)$-representation. If $p \nmid W$, then we have the following results.*

(i) Wild *is the Kummer direct image $[W]_\star(\mathcal{L})$ of some linear character $\mathcal{L}$ of Swan conductor* 1.
(ii) Wild *as a $P(\infty)$ representation is the direct sum of the W multiplicative translates of $\mathcal{L}|_{P(\infty)}$ by μ_W (with μ_W acting through its translation action on $\mathbb{G}_m$).*
(iii) *Any element of $I(\infty)$ of pro-order prime to p which maps onto a generator of $I(\infty)/P(\infty)$ acts on the set of the W irreducible constituents of $\mathsf{Wild}|_{P(\infty)}$ through the quotient μ_W of $I(\infty)$, cyclically permuting these irreducible constituents.*
(iv) *The image of $P(\infty)$ is isomorphic to the additive group of the finite field $\mathbb{F}_p(\mu_W)$.*

Next is an analogue of Proposition 5.8 in the case $p|\dim \mathsf{Wild}$.

Proposition 5.9. *Let $\mathcal{H}$ be an irreducible hypergeometric sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ of type (D,m) with $W := D - m > 0$ the dimension of the wild part Wild of the $I(\infty)$-representation. Suppose $W = p^a W_0$ with $a \geq 1$ and $p \nmid W_0$. Let $\gamma \in I(\infty)$ be an element of of pro-order prime to p which maps onto a generator of $I(\infty)/P(\infty)$. Then we have the following results.*

(i) Wild *is the Kummer direct image $[W_0]_\star(P)$ of an irreducible $I(\infty)$-representation P of dimension p^a, all of whose slopes are $1/p^a$, and whose restriction to $P(\infty)$ is irreducible.*
(ii) Wild *as a $P(\infty)$ representation is the direct sum of the W_0 multiplicative translates of $P|_{P(\infty)}$ by μ_W.*
(iii) *The action of γ on the set of the W_0 irreducible constituents of $\mathsf{Wild}|_{P(\infty)}$ factors through the quotient μ_W of $I(\infty)$, cyclically permuting these multiplicative translates of $P|_{P(\infty)}$.*
(iv) *The action of γ^{W_0} on Wild maps each of the W_0 multiplicative translates of $P|_{P(\infty)}$ to itself.*
(v) *There exists a root of unity ζ of order prime to p such that the spectrum of γ^{W_0} on each multiplicative translates of $P|_{P(\infty)}$ is the set $\zeta\cdot(\mu_{p^a+1} \smallsetminus \{1\})$ of multiples by ζ of the nontrivial roots of unity of order dividing $p^a + 1$.*

Proof. The first three assertions are proven in [Ka3, 1.14], and the fourth follows formally from the third. To deal with (v), we will reduce to the case when $W_0 = 1$. For this, we must distinguish the group $I(\infty)$, to which γ belongs, from its normal subgroup of cyclic index W_0 from which P is induced. We will denote this subgroup situation as $I(W_0) < I(1)$. Then $\gamma^{W_0} \in I(W_0)$. The pullback to $I(W_0)$ of $\mathsf{Wild} = \mathrm{Ind}_{I(W_0)}^{I(1)}(P)$ is the direct sum of the representations

$$g \mapsto P(\gamma^i g \gamma^{-i})$$

of $I(W_0)$, indexed by i (mod W_0). Thus for $g := \gamma^{W_0}$, the spectrum of γ^{W_0} is the same in each of these W_0 summands. So we must understand the spectrum of γ^{W_0} on P. But in $I(W_0)$, γ^{W_0} is an element of pro-order prime to p which maps onto a generator of $I(W_0)/P(W_0)$, and P is an irreducible $I(W_0)$-representation P of dimension p^a, all of whose slopes are $1/p^a$. Thus we are reduced to treating the case $W_0 = 1$.

According to [Ka4, 8.6.3]. for any $d \geq 2$, the isomorphism class of any $I(\infty)$-representation of dimension d with all slopes $1/d$ is determined, up to multiplicative translation, by its determinant, which is necessarily tame. Applying this to our Wild of dimension p^a, we see that we by replacing Wild with $\mathsf{Wild} \otimes \mathcal{L}_\chi$, which changes the determinant by a factor χ^{p^a}, we can achieve any tame determinant we like, while the effect of replacing Wild with $\mathsf{Wild} \otimes \mathcal{L}_\chi$ on the spectrum of $\gamma|_{\mathsf{Wild}}$ is simply to multiply every eigenvalue by the scalar $\chi(\gamma)$.

We now reduce further to the case $D = p^a, m = 0$, so that Wild is the entire $I(\infty)$-representation. Consider the Kloosterman sheaf

$$\mathcal{K}(p^a + 1) := \mathcal{K}l(\mathsf{Char}_{p^a+1} \smallsetminus \{\mathbb{1}\}).$$

It suffices to show that on its Wild, γ has spectrum $\mu_{p^a+1} \smallsetminus \{1\}$. The Kummer pullback $[p^a + 1]^\star \mathcal{K}(p^a+1)$ is (visibly) lisse on $\mathbb{A}^1$, and up to a multiplicative translate is isomorphic to the Fourier Transform $FT(\mathcal{L}_{\psi(x^{p^a+1})})$, cf. [Ka4, 9.2.3]. According to a result [KT1, 20.1] of Pink, this Kummer pullback has geometric monodromy group a finite p-group. It then follows from [Ka1, 1.3.2] that $\mathcal{K}(p^a+1)$ defines a "special" covering of $\mathbb{G}_m$, which means that $\mathcal{K}(p^a+1)$ is the canonical extension [Ka1, 1.5.7] of its Wild. By [Ka1, 1.4.12], the group $G_{\mathrm{geom},\mathcal{K}}$ for $\mathcal{K}(p^a + 1)$ is equal to the image $G_{\infty,\mathcal{K}}$ of $I(\infty)|_{\mathsf{Wild}}$. Moreover, the quotient of $G_{\mathrm{geom},\mathcal{K}} = G_{\infty,\mathcal{K}}$ by its unique p-Sylow subgroup $P_{\infty,\mathcal{K}}$ is cyclic of order $p^a + 1$, and a prime to p element of $G_{\infty,\mathcal{K}}$ which generates $G_{\infty,\mathcal{K}}/P_{\infty,\mathcal{K}}$, e.g. the image of γ, is a generator of the image $G_{0,\mathcal{K}}$ of $I(0)$ on $\mathcal{K}(p^a+1)|_{I(0)}$, and $G_{\infty,\mathcal{K}}$ is the semidirect product

$$G_{\mathrm{geom},\mathcal{K}} = G_{\infty,\mathcal{K}} \cong P_{\infty,\mathcal{K}} \rtimes G_{0,\mathcal{K}}.$$

Let us denote by ρ the representation of $G_{\mathrm{geom},\mathcal{K}} = G_{\infty,\mathcal{K}}$ defined by $\mathcal{K}(p^a + 1)$. If we view the image of γ as lying in $G_{\infty,\mathcal{K}}$, then $\rho(\gamma)$ is the action of γ on Wild. If we view the image of γ as lying in $G_{\mathrm{geom},\mathcal{K}}$, then $\rho(\gamma)$ is the action of γ on the $I(0)$-representation $\mathcal{K}(p^a+1)|_{I(0)}$ of $\mathcal{K}(p^a+1)$. Thus the spectrum of $\gamma|_{\mathsf{Wild}}$ is equal to the spectrum of γ on $\mathcal{K}(p^a + 1)|_{I(0)}$. This $I(0)$-representation is the direct sum of all the nontrivial characters of order dividing $p^a + 1$, and thus the spectrum of γ on it consists of $\mu_{p^a+1} \smallsetminus \{1\}$, as asserted. $\square$

Lemma 5.10. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf of type (D, m) in characteristic p with $D > m$ which is definable on some $\mathbb{G}_m/\mathbb{F}_q$. Suppose that on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, the dual $\mathcal{H}^\vee$ is geometrically isomorphic to $\mathcal{H} \otimes \mathcal{L}$ for some $\mathcal{L}$ which is lisse of rank one. Suppose that either $D \geq 3$ or that $(D, m) = (2, 0)$. Then there exists a multiplicative character ρ of finite order such that $\mathcal{H} \otimes \mathcal{L}_\rho$ is geometrically self-dual.*

Notice that if $W := D - m > 1$, then all slopes of $\mathcal{H}$ at both 0 and ∞ are < 1, while if $W := D - m = 1$ then all slopes at 0 and all but one slope at ∞ are 0, and there is one slope 1 at ∞. Thus Lemma 5.10 is a special case of the following result.

Lemma 5.11. *Let $\mathcal{F}$ be a lisse sheaf on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ which is definable on some $\mathbb{G}_m/\mathbb{F}_q$, whose dual $\mathcal{F}^\vee$ is (geometrically) isomorphic to $\mathcal{F}\otimes\mathcal{L}$ for some $\mathcal{L}$ which is lisse of rank one. Suppose that at both* 0 *and ∞, $\mathcal{F}$ has strictly more than* $\mathrm{rank}(\mathcal{F})/2$ *slopes which are < 1. Then there exists a multiplicative character ρ of finite order such that $\mathcal{H}\otimes\mathcal{L}_\rho$ is geometrically self-dual.*

Proof. The key point is to show that $\mathcal{L}$ is tame at both 0 and ∞. For then $\mathcal{L}$ is of the form $\mathcal{L}_\chi$ for some character of $\pi_1^{\text{tame at } 0,\infty} := \pi_1^{\text{tame}}(\mathbb{G}_m/\overline{\mathbb{F}_p})$. Both $\mathcal{F}$ and its dual have determinants which are geometrically of finite order, because each of these determinants is definable on some $\mathbb{G}_m/\mathbb{F}_q$: this finiteness is Grothendieck's local monodromy theorem in the form [De, 1.3.8], applied to $\det(\mathcal{F})$ and its dual. Equating their determinants, we see that their ratio, $\mathcal{L}^{\otimes\mathrm{rank}(\mathcal{F})}$, is geometrically of finite order, which in turn forces χ to be of finite order. Then we look for a tame character ρ of finite order such that $\mathcal{F}\otimes\mathcal{L}_\rho$ is (geometrically) self-dual, i.e., we want $(\mathcal{F}\otimes\mathcal{L}_\rho)^\vee\cong\mathcal{F}\otimes\mathcal{L}_\rho$. But $(\mathcal{F}\otimes\mathcal{L}_\rho)^\vee$ is $\mathcal{F}^\vee\otimes(\mathcal{L}_\rho)^{\otimes -1}\cong\mathcal{F}\otimes\mathcal{L}_\chi\otimes(\mathcal{L}_\rho)^{\otimes-1}$. So ρ will work provided that

$$\mathcal{L}_\chi\otimes(\mathcal{L}_\rho)^{\otimes-1}\cong\mathcal{L}_\rho, \text{ i.e., provided } \rho^2=\chi.$$

In odd characteristic p, χ has two square roots, both tame, and we may take either one. In characteristic 2, χ has some odd order $2m+1$, and then χ^{m+1} is its unique tame square root.

To show that $\mathcal{L}$ is tame at 0, we use the fact [Ka3, Lemma 1.3] that $\mathcal{F}$ and $\mathcal{F}^\vee$ have the same slopes as each other at 0. If $\mathcal{L}$ is not tame at 0, then its Swan conductor r_0 at 0 is a strictly positive integer $r_0\geq 1$. But then by [Ka3, Lemma 1.3], applied to $\mathcal{L}$ and to the part of $\mathcal{F}|_{I(0)}$ of slope <1, $\mathcal{F}\otimes\mathcal{L}$ will have strictly more than $\mathrm{rank}(\mathcal{F})/2$ slopes equal to r_0 at 0, and hence $\mathcal{F}^\vee$ has these same slopes. But then $\mathcal{F}^\vee$ has strictly fewer than $\mathrm{rank}(\mathcal{F})/2$ slopes which are <1 at 0, contrary to hypothesis. Therefore $r_0=0$. The same argument shows that $r_\infty=0$, and thus $\mathcal{L}$ is tame at both 0 and ∞. $\square$

Lemma 5.12. *Let $\mathcal{F}$ be a lisse sheaf $\mathcal{H}$ on $\mathbb{G}_m/\overline{\mathbb{F}_p}$ of rank $D\geq 1$. Let χ be any multiplicative character of finite order and let $G_{\mathrm{geom},\mathcal{H}_\chi}$ be the geometric monodromy group of $\mathcal{H}_\chi:=\mathcal{H}\otimes\mathcal{L}_\chi$. Then $G_{\mathrm{geom},\mathcal{H}_\chi}$ is finite if and only if $G_{\mathrm{geom},\mathcal{H}}$ is finite. Furthermore, denoting by $\mathbb{G}_m\subset\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$ the subgroup of scalars, we have*

$$G_{\mathrm{geom},\mathcal{H}}/(G_{\mathrm{geom},\mathcal{H}}\cap\mathbb{G}_m)=G_{\mathrm{geom},\mathcal{H}_\chi}/(G_{\mathrm{geom},\mathcal{H}_\chi}\cap\mathbb{G}_m),\ [G_{\mathrm{geom},\mathcal{H}},G_{\mathrm{geom},\mathcal{H}}]=[G_{\mathrm{geom},\mathcal{H}_\chi},G_{\mathrm{geom},\mathcal{H}_\chi}].$$

Similarly, $(G_{\mathrm{geom},\mathcal{H}})^{(\infty)}=(G_{\mathrm{geom},\mathcal{H}_\chi})^{(\infty)}$.

Proof. To say that $\mathcal{H}$ has finite $G_{\mathrm{geom},\mathcal{H}}$ is to say that there exists a finite étale $f:E\to\mathbb{G}_m/\overline{\mathbb{F}_p}$ which trivializes $\mathcal{H}$, i.e., such that $f^\star\mathcal{H}$ is constant. For N the (necessarily prime to p) order of χ, the Kummer covering $[N]:\mathbb{G}_m/\overline{\mathbb{F}_p}\to\mathbb{G}_m/\overline{\mathbb{F}_p}$ trivializes $\mathcal{L}_\chi$. Then any connected component of the fibre product over $\mathbb{G}_m/\overline{\mathbb{F}_p}$ of these two coverings is a finite etale covering which trivializes $\mathcal{H}\otimes\mathcal{L}_\chi$. Since we obtain $\mathcal{H}$ from $\mathcal{H}\otimes\mathcal{L}_\chi$ by tensoring with $\mathcal{L}_{\overline{\chi}}$, the implication of finiteness goes both ways. For the second statement, let

$$\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})\overset{\phi}{\twoheadrightarrow}G_{\mathrm{geom},\mathcal{H}}\overset{\Phi}{\to}\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$$

realize $\mathcal{H}$ and let

$$\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})\overset{\varpi}{\twoheadrightarrow}G_{\mathrm{geom},\mathcal{H}_\chi}\overset{\Psi}{\to}\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$$

realize $\mathcal{H}_\chi$. Tensoring $\mathcal{H}$ with $\mathcal{L}_\chi$ has the effect of changing $(\Phi\circ\phi)(g)$ for any $g\in\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ by some scalar multiple of it, indeed, $(\Phi\circ\phi)(g)=\chi(g)(\Psi\circ\varpi)(g)$ as elements of $\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$. Moreover, if $h\in\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ then

$$[(\Phi\circ\phi)(g),(\Phi\circ\phi)(h)]=[(\Psi\circ\varpi)(g),(\Psi\circ\varpi)(h)],$$

again as elements in $\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$. Thus the two subgroups

$$\Gamma := \Phi(\phi(\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})))$$

and

$$\Gamma_\chi = \Psi(\varpi(\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})))$$

of $\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$ have the same image in $\mathrm{PGL}_D(\overline{\mathbb{Q}_\ell})$. Passing to Zariski closures, and applying Lemma 4.1 to the canonical map $f : \mathrm{GL}_D(\overline{\mathbb{Q}_\ell}) \to \mathrm{PGL}_D(\overline{\mathbb{Q}_\ell})$ and to each of the groups Γ and Γ_χ, we get

$$G_{\mathrm{geom},\mathcal{H}}/(G_{\mathrm{geom},\mathcal{H}} \cap \mathbb{G}_m) = G_{\mathrm{geom},\mathcal{H}_\chi}/(G_{\mathrm{geom},\mathcal{H}_\chi} \cap \mathbb{G}_m)$$

as subgroups of $\mathrm{PGL}_D(\overline{\mathbb{Q}_\ell})$. Hence we have

$$[G_{\mathrm{geom},\mathcal{H}}, G_{\mathrm{geom},\mathcal{H}}] = [G_{\mathrm{geom},\mathcal{H}_\chi}, G_{\mathrm{geom},\mathcal{H}_\chi}]$$

as subgroups of $\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$. This last equality implies that

$$(G_{\mathrm{geom},\mathcal{H}})^{(\infty)} = (G_{\mathrm{geom},\mathcal{H}_\chi})^{(\infty)}$$

as subgroups of $\mathrm{GL}_D(\overline{\mathbb{Q}_\ell})$. ☐

Recall that we fix a nontrivial additive character ψ of $\mathbb{F}_p$. For any finite extension $\mathbb{F}_q$ of $\mathbb{F}_p$, ξ_2 is the quadratic character of $\mathbb{F}_q^\times$, and $\psi_{\mathbb{F}_q}$ is the composition of ψ with the trace map $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$.

Proposition 5.13. [KT7, Cor.14.15] *Suppose $\mathcal{H}$ is a geometrically irreducible hypergeometric sheaf $\mathcal{H}$ of type (D, m) with $D > m \geq 0$ on $\mathbb{G}_m/\mathbb{F}_q$. Then G_{geom} is finite if and only if for G the quadratic Gauss sum over $\mathbb{F}_q$,*

$$\mathsf{G} := \left(-\mathsf{Gauss}(\psi_{\mathbb{F}_q}, \xi_2)\right)^{D+m-1},$$

the constant field twist $\mathcal{H} \otimes \mathsf{G}^{-\deg/\mathbb{F}_q}$ has finite G_{arith}.

Let us write explicitly the local system $\mathcal{H}$ of Proposition 5.13 as

$$\mathcal{H} := \mathcal{H}yp(\chi_1, \ldots, \chi_D; \rho_1, \ldots, \rho_m).$$

Here all the χ_i and ρ_j have order dividing $q-1$. Choose an embedding of $\mathbb{Z}[\mu_{q-1}]$ into the Witt vectors $W(\mathbb{F}_q)$, and write each χ_i and each ρ_j as a power of the Teichmuller character Teich_q, say

$$\chi_i = \mathsf{Teich}_q^{a_i(q-1)}, \rho_j = \mathsf{Teich}_q^{b_j(q-1)},$$

with fractions $a_i, b_j \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$ whose denominators divide $q-1$. [Recall that Teich_q is the unique multiplicative character of $\mathbb{F}_q^\times$ with values in $\mu_{q-1}(W(\mathbb{F}_q))$ which attaches to an element α of $\mathbb{F}_q^\times$ the unique $(q-1)^{\mathrm{st}}$ root of unity in $W(\mathbb{F}_q)$ which reduces mod $pW(\mathbb{F}_q)$ to α. In other words, $\mathsf{Teich}(\alpha)$ is the "Teichmuller lifting" of α.]

As explained in [Ka7, §13], Kubert's *V-function* is the $\mathbb{Q}$-valued function on $(\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$ which attaches to an element a with denominator dividing $q-1$ the ord_q of the Gauss sum $\mathsf{Gauss}(\psi_{\mathbb{F}_q}, \mathsf{Teich}_q^{a(q-1)})$. It is given explicitly by Stickelberger's formula, cf. [Ka7, 13.4].

Proposition 5.14. [Ka7, 13.2] *In terms of Kubert's V-function* [Ka7, §13]*, the criterion for $\mathcal{H}$ to have finite geometric monodromy group, or equivalently for*

$$\mathcal{H} \otimes \left(\left(-\mathsf{Gauss}(\psi_{\mathbb{F}_q}, \xi_2)\right)^{D+m-1}\right)^{-\deg/\mathbb{F}_q}$$

to have finite arithmetic monodromy group, is the following. For every $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, and for every $N \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times$, we have

$$\sum_i V(Na_i + x) + \sum_j V(-Nb_j - x) \geq (D + m - 1)/2.$$

6. Rationality, moments, and reduction mod ℓ of hypergeometric sheaves

Proposition 6.1. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf*

$$\mathcal{H} := \mathcal{H}yp_\psi(\chi_1,\dots,\chi_n;\rho_1,\dots,\rho_d)$$

of type (n,d) with $n \neq d$ in characteristic p. Denote by $\Lambda := \prod_i \chi_i/\prod_j \rho_j$, and by M the order of Λ. Denote by N the lcm *of the orders of the χ_i and the ρ_j. Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p(\mu_N)$ in which every element of $\mathbb{F}_p^\times$ becomes an M^{th} power. Then we have the following results for every finite extension $E/\mathbb{F}$.*

(i) *For any $u \in E^\times$,* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in \mathbb{Q}(\zeta_N,\zeta_p)$.

(ii) *Suppose that $n \equiv d \pmod{p-1}$. Then each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in \mathbb{Q}(\zeta_N)$.

(ii-bis) *Suppose that $r|(p-1)$, and $rn \equiv rd \pmod{p-1}$. Let $K \subset \mathbb{Q}(\zeta_p)$ be the extension $K/\mathbb{Q}$ of degree r inside $\mathbb{Q}(\zeta_p)$. Then each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in K(\zeta_N)$.

(iii) *Suppose that L is an intermediate field $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_N)$, and that each of the multisets $\{\chi_i\}_i$ and $\{\rho_j\}_j$ is fixed (as a multiset) by* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/L)$. *Then each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in L(\zeta_p)$. *If in addition $n \equiv d \pmod{p-1}$, then each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in L$.

(iii-bis) *Suppose that $r|(p-1)$, and $rn \equiv rd \pmod{p-1}$. Suppose that L is an intermediate field $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_N)$, and that each of the multisets $\{\chi_i\}_i$ and $\{\rho_j\}_j$ is fixed (as a multiset) by* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/L)$. *Let $K \subset \mathbb{Q}(\zeta_p)$ be the extension $K/\mathbb{Q}$ of degree r inside $\mathbb{Q}(\zeta_p)$. Then each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) \in KL$, *$KL$ denoting the compositum of K and L inside $\mathbb{Q}(\zeta_p,\zeta_N)$.*

Moreover, if $\mathcal{H}$ has finite G_{geom}, then the above statements hold for the traces $\mathrm{Trace}(\gamma|\mathcal{H})$ *of all elements of G_{geom}.*

Proof. The first assertion is immediate from fact [Ka4, 8.2.7] that the trace function of $\mathcal{H}$ is given as follows.

$$(-1)^{n+d-1}\mathrm{Trace}(Frob_{u,E}|\mathcal{H}) = \sum_{\substack{x_1,\dots,x_n,y_1,\dots,y_d \in E,\\ \prod_i x_i = u\prod_j y_j}} \psi_E(\sum_i x_i - \sum_j y_j)\prod_i \chi_i(x_i)\prod_j \overline{\rho_j}(y_j).$$

To show (ii), (ii-bis), and (iii), we use the fact that $=\mathrm{Gal}(\mathbb{Q}(\zeta_N,\zeta_p)/\mathbb{Q})$ is the product group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

For (ii), suppose that $n \equiv d \pmod{p-1}$. The for each $\alpha \in \mathbb{F}_p^\times$, the domain of summation is invariant under the homothety multiplying each x_i and each y_j by α. So the trace is also equal to

$$\begin{aligned}
&\sum_{\substack{x_1,\dots,x_n,y_1,\dots,y_d \in E,\\ \prod_i x_i = u\prod_j y_j}} \psi_E(\alpha(\sum_i x_i - \sum_j y_j))\prod_i \chi_i(\alpha x_i)\prod_j \overline{\rho_j}(\alpha y_j)\\
=&\sum_{\substack{x_1,\dots,x_n,y_1,\dots,y_d \in E,\\ \prod_i x_i = u\prod_j y_j}} \Lambda(\alpha)\psi_E(\alpha(\sum_i x_i - \sum_j y_j))\prod_i \chi_i(x_i)\prod_j \overline{\rho_j}(y_j)\\
=&\sum_{\substack{x_1,\dots,x_n,y_1,\dots,y_d \in E,\\ \prod_i x_i = u\prod_j y_j}} \psi_E(\alpha(\sum_i x_i - \sum_j y_j))\prod_i \chi_i(x_i)\prod_j \overline{\rho_j}(y_j),
\end{aligned}$$

simply because $\Lambda(\alpha)=1$. Thus the trace is invariant under $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_N,\zeta_p)/\mathbb{Q}(\zeta_N))$.

For (ii-bis), repeat the same argument with α^r to see that the trace is invariant under

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K) = \mathrm{Gal}(\mathbb{Q}(\zeta_p,\zeta_N)/K(\zeta_N)).$$

For (iii), if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ fixes each of the multisets $\{\chi_i\}_i$ and $\{\rho_j\}_j$, then the trace is invariant under σ, viewed now as lying in $\mathrm{Gal}(\mathbb{Q}(\zeta_N,\zeta_p)/\mathbb{Q}(\zeta_p))$, simply by making the corresponding permutations of the x_i and of the y_j.

For (iii-bis), the trace lies both in $L(\zeta_p)$ by (iii) and in $K(\zeta_N)$ by (ii-bis). The intersection of these two fields is KL. To see this, we use the fact that $\mathrm{Gal}(\mathbb{Q}(\zeta_N, \zeta_p)/\mathbb{Q})$ is the product group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Denote by

$$A := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K) \leq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}), B := \mathrm{Gal}(\mathbb{Q}(\zeta_N)/L) \leq \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}).$$

Then $K(\zeta_N)$ is the fixed field of $A \times \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, and $L(\zeta_p)$ is the fixed field of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \times B$. Therefore the intersection of these two fields is the fixed field of the intersection of $A \times \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \times B$ (inside $\mathrm{Gal}(Q(\zeta_p, \zeta_N)/\mathbb{Q})$). This intersection is $A \times B$, whose fixed field we claim is KL. Indeed, KL certainly lies in the fixed field of $A \times B$. But K and L are linearly disjoint, being subfields of the linearly disjoint fields $Q(\zeta_p)$ and $Q(\zeta_N)$, so $\deg(KL/\mathbb{Q}) = \deg(K/\mathbb{Q})\deg(L/\mathbb{Q})$. But this is precisely the degree over $\mathbb{Q}$ of the fixed field of $A \times B$.

If G_{geom} for $\mathcal{H}$ is finite, then we argue as follows. At the expense of replacing $\mathbb{F}$ by a quadratic extension, we reduce to the case when the clearing factor $-\mathsf{Gauss}(\psi_{\mathbb{F}}, \xi_2)$ is a rational number, in fact some choice of $\pm\sqrt{\#\mathbb{F}}$. So the sheaf

$$\mathcal{H}_0 := \mathcal{H} \otimes (-\mathsf{Gauss}(\psi_{\mathbb{F}}, \xi_2))^{-(n+d-1)\deg(E/\mathbb{F})}$$

has the same trace field as $\mathcal{H}$. By Proposition 5.13, $\mathcal{H}_0$ has finite $G_{\mathrm{arith},\mathcal{H}_0}$. Thus $G_{\mathrm{geom}} < G_{\mathrm{arith},\mathcal{H}_0}$, and because $G_{\mathrm{arith},\mathcal{H}_0}$ is finite, every element in $G_{\mathrm{arith},\mathcal{H}_0}$ is some $Frob_{u,E}|\mathcal{H}_0$ for some finite extension $E/\mathbb{F}$ and some $u \in E^\times$. $\square$

Corollary 6.2. *We have the following results.*

(i) *Suppose that* $n \equiv d \pmod{(p-1)}$. *Let* $L \subseteq \mathbb{Q}(\zeta_N)$ *be the fixed field of those* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ *which fix both of the multisets* $\{\chi_i\}_i$ *and* $\{\rho_j\}_j$. *Then* L *is the field generated over* $\mathbb{Q}$ *by the traces* $\mathrm{Trace}(\gamma|\mathcal{H})$ *of the elements* $\gamma \in G_{\mathrm{geom}}$.

(ii) *Suppose that* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ *fixes both the multisets* $\{\chi_i\}_i$ *and* $\{\rho_j\}_j$. *Let* r *be the smallest divisor of* $p-1$ *such that* $((p-1)/r)|(n-d)$, *i.e.* $\gcd(n-d, p-1) = (p-1)/r$. *Let* $K \subset \mathbb{Q}(\zeta_p)$ *be the extension* $K/\mathbb{Q}$ *of degree* r *inside* $\mathbb{Q}(\zeta_p)$. *Then* K *is the field generated over* $\mathbb{Q}$ *by the traces* $\mathrm{Trace}(\gamma|\mathcal{H})$ *of the elements* $\gamma \in G_{\mathrm{geom}}$.

Proof. For (i), we know that the trace field lies in L, by the "moreover" statement of Theorem 6.1. Suppose that $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ fixes all traces $\mathrm{Trace}(\gamma|\mathcal{H})$. We must show that σ fixes both the sets $\{\chi_i\}_i$ and $\{\rho_j\}_j$. Consider the hypergeometric sheaf

$$\mathcal{H}^\sigma := \mathcal{H}yp_\psi(\chi_1^\sigma, \ldots, \chi_n^\sigma; \rho_1^\sigma, \ldots, \rho_d^\sigma)$$

obtained using the characters $\chi_i^\sigma := \sigma \circ \chi_i$ and $\rho_j^\sigma := \sigma \circ \rho_j$. Then $\mathcal{H}$ and $\mathcal{H}^\sigma$ have the same trace function on all $Frob_{u,E}$, and hence the same trace function on π_1^{geom}. Therefore $\mathcal{H}$ and $\mathcal{H}^\sigma$, being geomerically irreducible, are geometrically isomorphic as local systems on $\mathbb{G}_m/\mathbb{F}$. But we recover the multisets $\{\chi_i\}_i$, respectively $\{\rho_j\}_j$, as the multiset of characters in the $I(0)$-representation, respectively as the tame characters in the $I(\infty)$-representation. Therefore σ fixes both these multisets.

For (ii), we again know that the trace field lies in K, by the "moreover" statement of Theorem 6.1. Suppose that $\alpha \in \mathbb{F}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ fixes all traces $\mathrm{Trace}(\gamma|\mathcal{H})$. We must show that α acts as the identity on K, or equivalently that $\alpha^{(p-1)/r} = 1$, or equivalently that $\alpha^{n-d} = 1$. The effect of replacing ψ by $\psi_\alpha : x \mapsto \psi(\alpha x)$ is to replace $\mathcal{H}$ by its multiplicative translate by α^{n-d}, but leave the traces of all all $Frob_{u,E}$ unchanged. Just as in the proof of (i) above, this implies a geometric isomorphism between $\mathcal{H}$ and its multiplicative translate by α^{n-d}. This in turn implies a geometric isomorphism between the wild part Wild of the $I(\infty)$-representation of $\mathcal{H}$ and it multiplicative translate by α^{n-d}. By [Ka3, 4.1.6 (3)], there is no such isomorphism unless $\alpha^{n-d} = 1$. $\square$

We now consider the following situation, in which the trace field of a hypergeometric sheaf $\mathcal{H}$ is a quadratic extension $\mathbb{Q}(\sqrt{r})$ of $\mathbb{Q}$, and we ask when the sum of the trace of $\mathcal{H}$ and its $\mathrm{Gal}(\mathbb{Q}(\sqrt{r}/\mathbb{Q})$-conjugate takes only even integer values.

Proposition 6.3. *Suppose p is an odd prime, $r \neq p$ is another odd prime, ξ_r is a character of order r, and N is an integer prime to p. Denote by ξ_2 the quadratic character. Denote by $T_{\rm sq}$ the set of characters ξ_r^s as s runs over the squares in $\mathbb{F}_r^\times$, and by $T_{\rm nsq}$ the set of characters ξ_r^s as s runs over the nonsquares in $\mathbb{F}_r^\times$. Denote by $\xi_2 T_{\rm nsq}$ the set of characters $\xi_2\rho$ with $\rho \in T_{\rm nsq}$. Let A and B be (possibly empty) $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable sets of characters of order dividing N. Suppose $\#A + r - 1 \equiv \#B (\bmod\ (p-1))$ but $\#A + r - 1 \neq \#B$. Define*

$$N_r := \mathrm{lcm}(N, r).$$

Suppose that the hypergeometric sheaf in characteristic p on $\mathbb{G}_m/\mathbb{F}_p(\mu_{N_r})$ given by

$$\mathcal{H} := \mathcal{H}yp_\psi(A, T_{\rm sq}, \xi_2 T_{\rm nsq}; B)$$

is geometrically irreducible.

(i) *Denote by ϵ the choice of ± 1 for which $\epsilon r \equiv 1 (\bmod\ 4)$. For each finite extension $k/\mathbb{F}_p(\mu_{N_r})$ such that $k/\mathbb{F}_p$ has even degree, and each $u \in k^\times$, $\mathrm{Trace}(Frob_{u,k}|\mathcal{H})$ is an algebraic integer in $\mathbb{Q}(\sqrt{\epsilon r})$, i.e., lies in $\mathbb{Z}[(1+\sqrt{\epsilon r})/2]$.*

(ii) *For each finite extension $k/\mathbb{F}_p(\mu_{N_r})$ such that $k/\mathbb{F}_p$ has even degree, and each $u \in k^\times$,*

$$\mathrm{Trace}_{\mathbb{Q}(\sqrt{r})/\mathbb{Q}}\big(\mathrm{Trace}(Frob_{u,k}|\mathcal{H})\big) \in 2\mathbb{Z}.$$

(iii) *Suppose in addition that $\mathcal{H}$ has finite $G_{\rm geom}$. Denote by $\mathcal{H}_0$ the constant field twist of $\mathcal{H}$ by the correct power of $-\mathsf{Gauss}(\psi, \xi_2)$, cf. Proposition 5.13, so that $\mathcal{H}_0$ has finite $G_{\rm arith}$. Then for each finite extension $k/\mathbb{F}_p(\mu_{N_r})$ such that $k/\mathbb{F}_p$ has even degree,*

$$\mathrm{Trace}_{\mathbb{Q}(\sqrt{r})/\mathbb{Q}}\big(\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0)\big) \in 2\mathbb{Z}.$$

In particular, each element $\gamma \in G_{\rm geom}$ has

$$\mathrm{Trace}_{\mathbb{Q}(\sqrt{r})/\mathbb{Q}}\big(\mathrm{Trace}(\gamma|\mathcal{H})\big) \in 2\mathbb{Z}.$$

Proof. For (i), we apply Proposition 6.1. The character Λ there is $\xi_2^{(r-1)/2}\tau$ for a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant character τ, so Λ itself is either $\mathbb{1}$ or ξ_2. That the traces are algebraic integers is obvious from the explicit formula recalled there, and their being in $\mathbb{Q}(\sqrt{r})$ results from Proposition 6.1(iii).

The first statement of (iii) follows from (ii), because the clearing factor is $\pm$ a power of p, which does not affect parity. The second statement follows from this one, simply because $G_{\rm geom}$ is a subgroup of $G_{\rm arith}$. To prove (ii), we argue as follows. The group $\mathrm{Gal}(\mathbb{Q}(\sqrt{r})/\mathbb{Q})$ conjugates of the traces of $\mathcal{H}$ are the traces of the "conjugate" hypergeometric sheaf $\mathcal{H}^{conj}$, which is defined exactly as $\mathcal{H}$ but using a choice ${\xi_r}^{conj}$ which is ξ_r^s for s any nonsquare in $\mathbb{F}_r^\times$. The effect of this choice is to interchange the two sets $T_{\rm sq}$ and $T_{\rm nsq}$. We use the same ψ, because the condition that $\#A+r-1 \equiv \#B \ (\bmod\ (p-1))$ insures that the traces are independent of the choice of ψ. To show that $\mathcal{H} \oplus \mathcal{H}^{conj}$ has traces in $2\mathbb{Z}$, i.e., to show that $\mathcal{H} \oplus \mathcal{H}^{conj}$ has all traces zero in $\mathbb{Z}/2\mathbb{Z}$, it suffices to show that $\mathcal{H} \oplus \mathcal{H}^{conj}$ has all traces zero in the larger finite ring

$$R := \mathbb{Z}[\zeta_{prN}]/2\mathbb{Z}[\zeta_{prN}].$$

This will be trivially true if $\mathcal{H}$ and $\mathcal{H}^{conj}$ have equal traces in R. But mod 2, the quadratic character becomes trivial, so each of the sheaves $\mathcal{H}$ and $\mathcal{H}^{conj}$ has traces in R equal to the traces in R of the hypergeometric sheaf $\mathcal{H}yp_\psi(A, \mathsf{Char}_r^\times; B)$. $\square$

Remark 6.4. Thanks to Corollary 6.2, there are other situations in which Frobenius traces a priori lie in a quadratic extension of $\mathbb{Q}$, and one can ask if there is any imposed congruence on the trace down to $\mathbb{Q}$ of these Frobenius traces. The answer is no in general. Here are some examples. Consider, for odd $p \geq 5$, the following one-parameter family: for variable finite extensions $k/\mathbb{F}_p$,

$$t \in k \mapsto (1/\mathsf{Gauss}(\psi_k, \xi_2)) \sum_{x \in k} \psi_k(x^{(p+1)/2} + tx).$$

This is a descent to $\mathbb{G}_m/\mathbb{F}_p$ of $[(p+1/2]$ Kummer pullback of the Kloosterman sheaf

$$\mathcal{K}l_\psi(\mathsf{Char}_{(p+1)/2} \smallsetminus \{\mathbb{1}\}),$$

which naturally lives on $\mathbb{G}_m/\mathbb{F}_{p^2}$. By Corollary 6.2, this Kloosterman sheaf has trace field the quadratic field $\mathbb{Q}(\sqrt{\epsilon p})$ for ϵ the choice of ± 1 for which $\epsilon p \equiv 1 \pmod 4$. So the trace field of the descent must contain $\mathbb{Q}(\sqrt{\epsilon p})$, but it is obvious that our one parameter family has traces in this field. For the descent, one knows [KT1, Theorem 17.2] that $G_{\mathrm{arith}} = G_{\mathrm{geom}}$ is either $\mathrm{SL}_2(p)$ (if $p \equiv 1 \pmod 4$) or $\mathrm{PSL}_2(p)$ (if $p \equiv 3 \pmod 4$). In both cases, from the character table of $\mathrm{SL}_2(p)$ one knows that among the traces that occur for G_{geom} are both $(-1 \pm \sqrt{\epsilon p})/2$, each of which has trace -1 down to $\mathbb{Q}$. On the other hand, both 0, ± 1 and $(p-1)/2$ occur as traces for G_{geom} as well.

Next we turn to the consideration of moments. Recall that for a finite dimensional $\overline{\mathbb{Q}_\ell}$-representation V of a group G, the *moment* $M_{a,b}$ of the pair (G, V) is the dimension of the space of G-invariants in $V^{\otimes a} \otimes (V^*)^{\otimes b}$. For an odd integer a, we write $M_a := M_{a,0}$. [For an even integer $2n$, each of $M_{2n,0}$ and $M_{n,n}$ is sometimes called M_{2n}. The two can differ, unless V is self-dual; e.g. $M_{3,3} = 6$ but $M_{6,0} = 2$ for a faithful 6-dimensional complex representation of $6_1 \cdot \mathrm{PSU}_4(3)$ [GAP] – this has been exploited in part in the proof of Theorem 20.6 to distinguish between $6 \cdot \mathrm{PSL}_3(4)$ and $6_1 \cdot \mathrm{PSU}_4(3)$.]

Theorem 6.5. *Let $\mathcal{H}$ be a (geometrically irreducible) hypergeometric sheaf on $\mathbb{G}_m/\mathbb{F}_q$ of type (D, m) with $W := D - m > 0$. Let a, b be nonnegative integers, and consider the moment $M_{a,b}$ of the D-dimensional representation of $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$ defined by $\mathcal{H}$. Denote by $\mathcal{H}_0$ any lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ which is pure of weight zero and which is geometrically isomorphic to $\mathcal{H}$. Denote by*

$$\mathcal{H}_0^{a,b} := \mathcal{H}_0^{\otimes a} \otimes (\mathcal{H}_0^\vee)^{\otimes b}.$$

Denote by A, B, C the following constants.

$$C := \text{dimension of the space of } I(0)\text{-invariants in } \mathcal{H}_0^{a,b}.$$

$$B := \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b}.$$

$$A := B - C.$$

Then we have the following estimate.

$$\left| \frac{1}{q-1} \sum_{u \in \mathbb{F}_q^\times} \mathrm{Trace}(Frob_{u,\mathbb{F}_q} | \mathcal{H}_0^{a,b}) \right| \leq \frac{q}{q-1} M_{a,b} + \frac{A\sqrt{q}}{q-1} + \frac{B}{q-1}.$$

Proof. The key point is that $M_{a,b}$ is the dimension $h_c^2(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{H}_0^{a,b}) = h_c^2(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{H}^{a,b})$.

We first recall some facts about the $h_c^i(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})$ for lisse sheaves $\mathcal{F}$ on $\mathbb{G}_m/\mathbb{F}_q$. The Lefschetz trace formula gives

$$\sum_{x \in \mathbb{F}_q^\times} \mathrm{Trace}(Frob_{u,\mathbb{F}_q} | \mathcal{F}) = \mathrm{Trace}\big(Frob_{\mathbb{F}_q} | H_c^2(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})\big) - \mathrm{Trace}\big(Frob_{\mathbb{F}_q} | H_c^1(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})\big).$$

If $\mathcal{F}$ is pure of weight zero, then H^2_c is pure of weight 2, and H^1_c is mixed of weight ≤ 1, indeed

$$H^1_c = H^1_c(\mathrm{wt}=1) \oplus H^1_c(\mathrm{wt} \leq 0).$$

Thus for $\mathcal{F}$ pure of weight zero, we have

$$\Big|\sum_{x\in\mathbb{F}_q^\times} \mathrm{Trace}(Frob_{u,\mathbb{F}_q}|\mathcal{F})\Big| \leq qh^2_c + \sqrt{q}h^1_c(\mathrm{wt.}=1) + h^1_c(\mathrm{wt.}\leq 0) \leq qh^2_c + \sqrt{q}h^1_c(\mathrm{wt.}=1) + h^1_c.$$

When $\mathcal{F}$ is lisse on $\mathbb{G}_m/\overline{\mathbb{F}_p}$, the Euler-Poincaré formula is

$$\chi_c(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{F}) = -\mathsf{Swan}_0(\mathcal{F}) - \mathsf{Swan}_\infty(\mathcal{F}).$$

When $\mathcal{F}$ is tame at 0, this becomes

$$\mathsf{Swan}_\infty(\mathcal{F}) = h^1_c - h^2_c.$$

To compute the dimension of $H^1_c(\mathrm{wt}=1)$, we use the fact that for the inclusion $j : \mathbb{G}_m \subset \mathbb{P}^1$, the group $H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F})$ is pure of weight one. We exploit this by looking at the short exact sequence of sheaves on $\mathbb{P}^1/\overline{\mathbb{F}_q}$ given by

$$0 \to j_!\mathcal{F} \to j_\star\mathcal{F} \to (\mathcal{F}^{I(0)})_0 \oplus (\mathcal{F}^{I(\infty)})_\infty \to 0,$$

where the last two summands are skyscraper sheaves at 0 and ∞. The group

$$H^0(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) = H^0(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F})$$

is the space of π_1^{geom} invariants in $\mathcal{F}$, so it injects into the space $\mathcal{F}^{I(\infty)}$ of $I(\infty)$-invariants in $\mathcal{F}$. This injectivity, together with the long exact sequence

$$0 \to H^0(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) \to \mathcal{F}^{I(0)} \oplus \mathcal{F}^{I(\infty)} \to H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{F}) \to H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}_0) \to 0,$$

gives the inequality

$$h^1_c(\mathrm{wt.}=1) = h^1_c - \dim\mathcal{F}^{I(0)} - (\dim\mathcal{F}^{I(\infty)} - \dim h^0) \leq h^1_c - \dim\mathcal{F}^{I(0)}.$$

Apply this with $\mathcal{F}$ taken to be $\mathcal{H}_0^{a,b}$. Then h^2_c is $M_{a,b}$, and the Euler-Poincaré formula gives

$$h^1_c = \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b}.$$

Thus

$$h^1_c(\mathrm{wt.}=1) \leq h^1_c - \dim\mathcal{F}^{I(0)} = \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b} - \dim\mathcal{F}^{I(0)}.$$

Then the estimate

$$|\sum_{x\in\mathbb{F}_q^\times} \mathrm{Trace}(Frob_{u,\mathbb{F}_q}|\mathcal{F})| \leq qh^2_c + \sqrt{q}h^1_c(\mathrm{wt.}=1) + h^1_c$$

becomes

$$\Big|\sum_{x\in\mathbb{F}_q^\times} \mathrm{Trace}(Frob_{u,\mathbb{F}_q}|\mathcal{H}_0^{a,b})\Big| \leq qM_{a,b} + \big(\mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b} - \dim\mathcal{F}^{I(0)}\big)\sqrt{q} + \mathsf{Swan}_\infty(\mathcal{H}_0^{a,b}) + M_{a,b}.$$

□

To make this last result usable in practice, we need upper bounds for Swan conductors, and lower bounds for dimensions of $I(0)$-invariants. For these tasks, we give the following lemmas.

Lemma 6.6. *Let $\mathcal{H}$ be a geometrically irreducible hypergeometric sheaf on $\mathbb{G}_m/\mathbb{F}_q$ of type (D, m) with $W := D - m > 0$. Let a, b be nonnegative integers. Denote by*

$$\mathcal{H}^{a,b} := \mathcal{H}^{\otimes a} \otimes (\mathcal{H}^\vee)^{\otimes b}.$$

Then

$$\mathsf{Swan}_\infty(\mathcal{H}^{a,b}) \leq (D^{a+b} - m^{a+b})/W.$$

Proof. The $I(\infty)$-representation of both $\mathcal{H}$ and $\mathcal{H}^\vee$ are of the form $\mathsf{Tame}_m \oplus \mathsf{Wild}_W$, with Tame_m tame of rank m and Wild_W of rank W, with all slopes $1/W$. Any multiple tensor product of such Wild_W's has all slopes $\leq 1/W$. So expanding $D^{a+b} = (m + W)^{a+b}$ by the binomial theorem,

$$D^{a+b} = \sum_{i=0}^{a+b} \binom{a+b}{i} W^i m^{a+b-i},$$

we see that

$$\mathsf{Swan}_\infty(\mathcal{H}^{a,b}) \leq \frac{1}{W} \sum_{i=1}^{a+b} \binom{a+b}{i} W^i m^{a+b-i} = \frac{D^{a+b} - m^{a+b}}{W}.$$

□

Lemma 6.7. *Suppose $M \geq 1$ is an integer prime to p and V is an $I(0)$-representation which factors through the μ_M quotient of $I(0)$. Fix a character $\xi := \xi_M$ of order M, and write the characters in V as powers of ξ, say*

$$V = \oplus_i \xi^{e_i}.$$

Then the character of the $I(0)$-representation $V^{a,b} := V^{\otimes a} \otimes (V^\vee)^{\otimes b}$ takes value

$$(\sum_i \zeta^{e_i})^a (\sum_i \zeta^{-e_i})^b$$

at $\zeta \in \mu_M$. Furthermore,

$$\dim(V^{a,b})^{I(0)} = \frac{1}{M} \sum_{\zeta \in \mu_M} (\sum_i \zeta^{e_i})^a (\sum_i \zeta^{-e_i})^b.$$

Proof. By hypothesis, $I(0)$ acts through its quotient μ_M, so this is just the calculation of the dimension of invariants in a representation of a finite group as the integral of its trace over the group. □

Remark 6.8. Here are two examples. When the $I(0)$-representation is the direct sum of the characters in the set

$$\mathsf{Char}_{\mathrm{ntriv}}(M) := \mathsf{Char}(M) \smallsetminus \{\mathbb{1}\}, \tag{6.8.1}$$

it is self-dual, and we are looking at the average over μ_M of the restriction to μ_M of the function

$$((X^M - 1)/(X - 1) - 1)^{a+b}.$$

At $\zeta \neq 1$, its value is $(-1)^{a+b}$. At $\zeta = 1$, its value is $(M - 1)^{a+b}$. So in this case the dimension of the space of $I(0)$-invariants is

$$(1/M)\big((M-1)^{a+b} + (M-1)(-1)^{a+b}\big) = \frac{M-1}{M}\big((M-1)^{a+b-1} - (-1)^{a+b-1}\big),$$

a number familiar in Hodge theory as the dimension of the middle primitive Betti number of a smooth hypersurface of degree M and dimension $a + b - 2$, cf. [KS, 11.4.1].

When the $I(0)$-representation is the direct sum of the characters $\mathsf{Char}(M) \setminus \{\xi^e, \xi^f\}$, then we are looking at the average over μ_M of the restricion to μ_M of the function

$$((X^M - 1)/(X-1) - X^e - X^f)^a((X^M - 1)/(X-1) - X^{-e} - X^{-f})^b.$$

So the dimension of the space of invariants is

$$\begin{aligned}&(1/M)\big((M-2)^{a+b} + \sum_{\zeta \neq 1}(\zeta^e + \zeta^f)^a(\zeta^{-e} + \zeta^{-f})^b)\big)\\ =&(1/M)(M-2)^{a+b} + \big(\text{“error” term } \le ((M-1)/M)2^{a+b}\big)\\ \ge&(1/M)(M-2)^{a+b} - 2^{a+b}.\end{aligned}$$

We now give a version of Theorem 6.5 adapted to the situation on $\mathbb{A}^1$.

Theorem 6.9. *Let $\mathcal{F}$ be a lisse sheaf on $\mathbb{A}^1/\mathbb{F}_q$ of rank $D \ge 1$ which is pure of weight zero. Let a, b be nonnegative integers, and consider the moment $M_{a,b}$ of the D-dimensional representation of $\pi_1(\mathbb{A}^1/\overline{\mathbb{F}_p})$ given by $\mathcal{F}$. Suppose that the $I(\infty)$-representation of $\mathcal{F}$ has a tame part of dimension $\ge m$ and has all $I(\infty)$ slopes $\le \alpha$. Denote by $H_{a,b}$ the constant*

$$H_{a,b} := M_{a,b} + (\alpha - 1)D^{a+b} - \alpha m^{a+b}.$$

Then we have the following estimate.

$$\left|\frac{1}{q}\sum_{u \in \mathbb{F}_q} \mathrm{Trace}(Frob_{u,\mathbb{F}_q}|\mathcal{F}^{a,b})\right| \le M_{a,b} + \frac{H_{a,b}}{\sqrt{q}}.$$

Proof. The Euler-Poincaré formula for a lisse $\mathcal{G}$ on $\mathbb{A}^1/\overline{\mathbb{F}_p}$ is

$$\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{G}) := h^2_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{G}) - h^1_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{G}) = \mathrm{rank}(\mathcal{G}) - \mathsf{Swan}_\infty(\mathcal{G}).$$

We apply this to $\mathcal{F}^{a,b}$. Its $I(\infty)$-representation has a tame part of dimension at least m^{a+b} (namely $\mathsf{Tame}^{a,b}$), and so its wild part has dimension at most $D^{a+b} - m^{a+b}$. As all $I(\infty)$ slopes of $\mathcal{F}^{a,b}$ are $\le \alpha$, we get

$$\mathsf{Swan}_\infty(\mathcal{F}^{a,b}) \le \alpha(D^{a+b} - m^{a+b}),$$

and hence

$$-\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}^{a,b}) = \mathsf{Swan}_\infty(\mathcal{F}^{a,b}) - D^{a+b} \le (\alpha-1)D^{a+b} - \alpha m^{a+b}.$$

On the other hand $h^2_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}^{a,b}) = M_{a,b}$, and so we get the inequality

$$h^1_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}^{a,b}) \le H_{a,b}.$$

Now we apply the Lefschetz trace formula:

$$\sum_{u \in \mathbb{F}_q} \mathrm{Trace}(Frob_{u,\mathbb{F}_q}|\mathcal{F}^{a,b}) = \mathrm{Trace}(Frob_{\mathbb{F}_q}|H^2_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}^{a,b}) - \mathrm{Trace}(Frob_{\mathbb{F}_q}|H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_p}, \mathcal{F}^{a,b}).$$

Applying Deligne's fundamental estimate [De, 3.3.4 and 3.2.3] that the H^1_c is mixed of weight ≤ 1 while the H^2_c is pure of weight two, we divide through by q and get the asserted inequality. □

We now turn to a discussion of hypergeometric sheaves “mod ℓ”. We begin with the case of Kloosterman sheaves.

Fix a prime $\ell \neq p$, a finite extension $k_\ell/\mathbb{F}_\ell$ such that $p|\#k_\ell^\times$, and denote by R_ℓ the ring of Witt vectors $\mathsf{Witt}(k_\ell)$, and by $R_{\ell,a}$ the ring $R_\ell[\zeta_{\ell^a}]$. [Thus for ℓ a prime which is 1 (mod p) and $k_\ell = \mathbb{F}_\ell$, R_ℓ is just $\mathbb{Z}_\ell$, and $R_{\ell,a}$ is $\mathbb{Z}_\ell[\zeta_{\ell^a}]$.] The ring $R_{\ell,a}$ is a discrete valuation ring, with uniformizing parameter

$$\boldsymbol{\lambda} := \zeta_{\ell^a} - 1$$

and residue field k_ℓ. In [Ka3, 4.1.1, 4.1.2], the theory of Kloosterman sheaves is developed over $R_{\ell,a}$. We may speak of $\mathcal{K}l_\psi(\chi_1,\ldots,\chi_n)$ for any choice of characters χ_i whose orders are prime to p and divide $\ell^a\#(k_\ell^\times)$. It is a local system on $\mathbb{G}_m/\mathbb{F}_p[\mu_{\ell^a\#(k_\ell^\times)}]$ (with the convention that $\mathbb{F}_p[\mu_N]:=\mathbb{F}_p[\mu_{N_0}]$ for N_0 the prime-to-p part of N) of free $R_{\ell,a}$ modules of rank n, which after extension of scalars from $R_{\ell,a}$ to $\overline{\mathbb{Q}_\ell}$ is the Kloosterman sheaf we have been concerned with up to now. We will refer to it as a Kloosterman sheaf over $R_{\ell,a}$. For a shorthand, we will write

$$\mathcal{K}l_\psi(\chi_1,\ldots,\chi_n)_{k_\ell}:=\mathcal{K}l_\psi(\chi_1,\ldots,\chi_n)\otimes_{R_{\ell,a}}k_\ell.$$

The key point is that $\mathcal{K}l_\psi(\chi_1,\ldots,\chi_n)_{k_\ell}$ depends only on the reductions mod $\boldsymbol{\lambda}$ of the characters χ_i, i.e., on the χ_i as characters with values in $k_\ell^\times$. It is a local system on $\mathbb{G}_m/\mathbb{F}_p[\mu_{\#(k_\ell^\times)}]$ of k_ℓ-spaces of rank n.

Theorem 6.10. *Let $\mathcal{K}l:=\mathcal{K}l_\psi(\chi_1,\ldots,\chi_D)_{k_\ell}$ be a Kloosterman sheaf over $R_{\ell,a}$, with reduction mod ℓ denoted $\mathcal{K}l_{k_\ell}$. Then we have the following results.*

(a) *The $I(\infty)$-representation of $\mathcal{K}l_{k_\ell}$ is totally wild, with $\mathsf{Swan}=1$ and all slopes $1/D$.*
(b) *The $I(\infty)$-representation of $\mathcal{K}l_{k_\ell}$ is absolutely irreducible as k_ℓ-representation.*
(c) *The $\pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p})$-representation of $\mathcal{K}l_{k_\ell}$ is absolutely irreducible as k_ℓ-representation.*
(d) *For any integer $N\geq 1$ which is prime to p, the Kummer direct image $[N]_\star(\mathcal{K}l_{k_\ell})$ is a Kloosterman sheaf of rank ND. If $R_{\ell,a}$ is large enough to contain all the N^{th} roots of all the $R_{\ell,a}^\times$-valued the characters χ_i, this direct image is geometrically isomorphic to the reduction mod ℓ of the Kloosterman sheaf*

$$\mathcal{K}l_{\psi_{1/N}}(\text{all } N^{\text{th}} \text{ roots of all the } \chi_i).$$

(e) *Suppose that all the χ_i have order dividing a power of ℓ. Then we have an isomorphism of Kloosterman sheaves over k_ℓ*

$$\mathcal{K}l_\psi(\chi_1,\ldots,\chi_D)_{k_\ell}\cong\mathcal{K}l_\psi(\mathbb{1}\text{ repeated } D \text{ times})_{k_\ell}.$$

(f) *If N is a power of ℓ we have geometric isomorphisms of Kloosterman sheaves over k_ℓ*

$$[N]_\star(\mathcal{K}l_{\psi_N}(\mathbb{1}\text{ repeated } D \text{ times})_{k_\ell})\cong\mathcal{K}l_\psi(\mathbb{1}\text{ repeated } ND \text{ times})_{k_\ell}.$$

Proof. Assertion (a) results from [Ka3, 5.1, (1) and (5)], and (b) results from (a) and [Ka3, 1.14]. Trivially we have $(b)\implies(c)$. For (d), [Ka3, 1.13.2] shows that $[N]_\star(\mathcal{K}l_{k_\ell})$ has all $I(\infty)$ slopes $1/ND$. As it is tame at 0, it is Kloosterman by [Ka3, 8.7.1]. The direct image formula [Ka3, 5.6.2] asserts that the direct image formula holds over $R_{\ell,a}$ if we do a constant field twist of the source by a power of the product of minus the Gauss sums for all the nontrivial characters of order dividing N. The square of this twisting factor is $\pm$ a power of p. Thus if we work over a large enough ground field $\mathbb{F}_q/\mathbb{F}_p$, this twisting factor reduces mod ℓ to 1 in k_ℓ. So when we reduce mod ℓ, this twisting factor disappears, yielding the asserted isomorphism as representations of $\pi_1(\mathbb{G}_m/\text{a sufficiently large extension of }\mathbb{F}_p)$, so in particular as representations of π_1^{geom}. Assertion (e) is a tautology, and (f) is immediate from (d) and (e). ☐

The following corollary is immediate from (f) of the above Theorem 6.10, we state it for ease of later reference.

Corollary 6.11. *Let N be a power of ℓ, and $D\geq 1$. Then we have a geometric isomorphism*

$$\mathcal{K}l_\psi(\mathbb{1}\text{ repeated } ND \text{ times})_{k_\ell}\cong[N]_\star(\mathcal{K}l_{\psi_N}((\mathbb{1}\text{ repeated } D \text{ times})_{k_\ell}.$$

For G the image of π_1^{geom} in $\mathrm{GL}_{ND}(k_\ell)$ under the representation given by the first factor, this representation of G is induced from a D-dimensional representation of a normal subgroup $H\lhd G$ with G/H cyclic of order N.

We now turn to the discusssion of general hypergeometric sheaves mod ℓ.

Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be Kloosterman sheaves over $R_{\ell,a}$, of ranks n and d respectively, and assume $n > d$. Say

$$\mathcal{K}_1 = \mathcal{K}l_\psi(\chi_1, \ldots, \chi_n),\ \mathcal{K}_2 = \mathcal{K}l_\psi(\rho_1, \ldots, \rho_d).$$

We define the hypergeometric sheaf

$$\mathcal{H}yp_\psi(\chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_d)$$

as a local system on $\mathbb{G}_m/\mathbb{F}_p[\mu_{\ell^a\#(k_\ell^\times)}]$ of free $R_{\ell,a}$ modules of rank n as the ! multiplicative convolution of $\mathcal{K}_1 := \mathcal{K}l_\psi(\chi_1, \ldots, \chi_n)$ with $\mathrm{inv}^\star\overline{\mathcal{K}_2} := \mathrm{inv}^\star\mathcal{K}l_{\overline{\psi}}(\overline{\rho_1}, \ldots, \overline{\rho_d})$. Concretely, for the multiplication map $\mathrm{mult} : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$, we define

$$\mathcal{K}_1 \star_{\times,!} \mathrm{inv}^\star\overline{\mathcal{K}_2} := R(\mathrm{mult})_!(\mathcal{K}_1 \boxtimes \mathrm{inv}^\star\overline{\mathcal{K}_2}).$$

In more down to earth terms, for the projection pr_2 of $\mathbb{G}_m \times \mathbb{G}_m$ with coordinates (x,t) on the second factor, this is

$$R(\mathrm{pr}_2)_!(\mathcal{K}_1(x) \otimes \overline{\mathcal{K}_2}(x/t)).$$

Each of the sheaves $\mathcal{K}_1 \otimes k_\ell$ and $\overline{\mathcal{K}_2} \otimes k_\ell$ is geometrically irreducible (because already $I(\infty)$-irreducible), so fibre by fibre the R^2 vanishes, and the R^1 has rank n (because the tensor product has all slopes $1/d$). Moreover, by the long exact cohomology sequence attached to the universal coefficient short exact sequence

$$0 \to \mathcal{K}_1(x) \otimes \overline{\mathcal{K}_2}(x/t) \xrightarrow{\boldsymbol{\lambda}} \mathcal{K}_1(x) \otimes \overline{\mathcal{K}_2}(x/t) \to (\mathcal{K}_1(x) \otimes k_\ell) \otimes (\overline{\mathcal{K}_2}(x/t) \otimes k_\ell) \to 0$$

one shows, fibre by fibre, that R^1 is a lisse sheaf of free R_ℓ modules, and that its formation commutes with extension of scalars either $R_\ell \twoheadrightarrow k_\ell$ or $R_\ell \hookrightarrow \overline{\mathbb{Q}_\ell}$. In particular, the reduction mod $\boldsymbol{\lambda}$,

$$\mathcal{H}yp_\psi(\chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_d)_{k_\ell}$$

is the hypergeometric sheaf over k_ℓ defined by the same convolution recipe applied to $\mathcal{K}l_\psi(\chi_1, \ldots, \chi_n)_{k_\ell}$ and $\mathcal{K}l_\psi(\rho_1, \ldots, \rho_d)_{k_\ell}$.

Theorem 6.12. *Consider a hypergeometric $\mathcal{H}_{k_\ell} := \mathcal{H}yp_\psi(\chi_1, \ldots, \chi_n; \rho_1, \ldots, \rho_d)_{k_\ell}$ in which no χ_i is a ρ_j as a $k_\ell^\times$-valued character. Then $\mathcal{H}$ is absolutely* (i.e., after extension of scalars from k_ℓ to $\overline{\mathbb{F}_\ell}$) *geometrically irreducible.*

Proof. Repeat the proof [Ka4, 8.4.2 (1)] given in the $\overline{\mathbb{Q}_\ell}$ case, using the mod $\boldsymbol{\lambda}$ Fourier transform here in place of the $\overline{\mathbb{Q}_\ell}$ Fourier transform used there. □

We will also use the fact that when there is a common character upstairs and downstairs, the mod $\boldsymbol{\lambda}$ representation is always reducible.

Theorem 6.13. *The hypergeometric sheaf*

$$\mathcal{H}yp_\psi(\mathbb{1}, \chi_2, \ldots, \chi_n; \mathbb{1}, \rho_2, \ldots, \rho_d)_{k_\ell}$$

sits in a $\pi_1(\mathbb{G}_m/\mathbb{F}_p[\mu_{\#(k_\ell^\times)}])$-equivariant short exact sequence

$$0 \to U \to \mathcal{H}yp_\psi(\mathbb{1}, \chi_2, \ldots, \chi_n; \mathbb{1}, \rho_2, \ldots, \rho_d)_{k_\ell} \to \mathcal{H}yp_\psi(\chi_2, \ldots, \chi_n; \rho_2, \ldots, \rho_d)_{k_\ell}(-1) \to 0,$$

where $U := H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathcal{H}yp_\psi(\chi_2, \ldots, \chi_n; \rho_2, \ldots, \rho_d)_{k_\ell})$ is a rank 1 constant sheaf.

Proof. We have the convolution formula

$$\mathcal{H}yp_\psi(\mathbb{1}, \chi_2, \ldots, \chi_n; \mathbb{1}, \rho_2, \ldots, \rho_d)_{k_\ell} = \mathcal{H}yp(\mathbb{1}; \mathbb{1})_{k_\ell} \star_{\times,!} \mathcal{H}yp_\psi(\chi_2, \ldots, \chi_n; \rho_2, \ldots, \rho_d)_{k_\ell}.$$

Following the lines of the proof of the analogous result in [Ka4, 8.4.7], we must analyze the object $\mathcal{H}yp(\mathbb{1}; \mathbb{1})_{k_\ell}$. It is $R(\mathrm{pr}_2)_!)\mathcal{L}_{\psi(x-x/t)}$. It is clear that the R^2 vanishes outside $t = 1$, and there is it

$\delta_1(-1)$. Fibre by fibre, one sees that the R^0 vanishes, and the R^1 has constant rank 1, and its trace function is constant, equal to 1. Moreover, the R^1 is a sheaf of perverse origin, so it is lisse of rank one. Having constant trace, it must be the constant sheaf k_ℓ. Thus the entire R is perverse (shifted by 2 (its $R^0 = 0$, its R^1 is lisse, and its R^2 is punctual)). So we have a short exact sequence of perverse sheaves

$$0 \to k_\ell[1] \to \mathcal{H}yp(\mathbb{1};\mathbb{1})_{k_\ell} \to \delta_1(-1) \to 0,$$

and the proof concludes exactly as in [Ka4, 8.4.7]. □

7. Descents of hypergeometric sheaves

There are a number of situations in which a hypergeometric sheaf has a "simple to remember" descent to a lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$. Here are three of them.

Proposition 7.1. *Let A and B be prime to p positive integers with $\gcd(A,B) = 1$. Then we have the following results, in which we continue to use the notation $\mathsf{Char}_{\mathrm{ntriv}}(A)$ of (6.8.1).*

(i) *Choose integers α, β with $\alpha A - \beta B = 1$. Suppose $(A,B) \neq (1,1)$ and p is odd. Then the hypergeometric sheaf*

$$\mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(A); \mathsf{Char}_{\mathrm{ntriv}}(B)),$$

which is pure of weight $A+B-3$, is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ which is pure of weight one and whose trace function is as follows: for variable finite extensions $k/\mathbb{F}_p$,

$$u \in k \mapsto -\sum_{x\in k} \psi_k(Au^\alpha x^B - Bu^\beta x^A).$$

(i-bis) *Choose integers α, β with $\alpha A - \beta B = 1$. Suppose $(A,B) \neq (1,1)$ and $p = 2$. Then the hypergeometric sheaf*

$$\mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(A); \mathsf{Char}_{\mathrm{ntriv}}(B)),$$

which is pure of weight $A+B-3$, is geometrically isomorphic to the lisse sheaf on $\mathbb{G}_m/\mathbb{F}_4$ which is pure of weight one and whose trace function is as follows: for variable finite extensions $k/\mathbb{F}_4$,

$$u \in k \mapsto -\sum_{x\in k} \psi_k(Au^\alpha x^B - Bu^\beta x^A).$$

(ii) *The hypergeometric sheaf $\mathcal{H}yp_\psi(\mathsf{Char}(A); \mathsf{Char}_{\mathrm{ntriv}}(B))$, which is pure of weight $A+B-2$, is geometrically isomorphic to the lisse sheaf $\mathcal{G}_{A,B_{\mathrm{ntriv}}}$ on $\mathbb{G}_m/\mathbb{F}_p$ which is pure of weight two and whose trace function is as follows: for variable finite extensions $k/\mathbb{F}_p$,*

$$u \in k \mapsto \sum_{x\in k,\, y \in k^\times} \psi_k(ux^B/y^A + Ay - Bx).$$

(iii) *The hypergeometric sheaf $\mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(B); \mathsf{Char}(A))$, which is pure of weight $A+B-2$, is geometrically isomorphic to the lisse sheaf $\mathcal{G}_{B_{\mathrm{ntriv}},A}$ on $\mathbb{G}_m/\mathbb{F}_p$ which is pure of weight two and whose trace function is as follows: for variable finite extensions $k/\mathbb{F}_p$,*

$$u \in k \mapsto \sum_{x\in k,\, y \in k^\times} \psi_k(-u^{-1}x^B/y^A - Ay + Bx).$$

Proof. The first statement is proven in [KT6, Lemma 3.9 (i)]. The second is proven in [KRLT2, Lemmas 1.3 and 1.4]. The third follows from the second and the fact [Ka4, 8.2.14] that the sheaf $\mathcal{H}yp_\psi \mathsf{Char}_{\mathrm{ntriv}}(B); \mathsf{Char}(A))$ is just $\mathrm{inv}^\star \mathcal{H}yp_{\overline{\psi}}(\mathsf{Char}(A); \mathsf{Char}_{\mathrm{ntriv}}(B))$. □

Proposition 7.2. *Suppose A and B are prime to p positive integers with $\gcd(A,B) = 1$ and $A - B \geq 2$. Suppose further that A is odd. Choose integers α, β with $\alpha A - \beta B = 1$. If p is odd, denote by $\mathcal{S}_{A,B}$ the local system on $\mathbb{G}_m/\mathbb{F}_p$ whose trace function is given by*

$$u \in k/\mathbb{F}_p \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \xi_2)} \sum_{x \in k} \psi_k(Au^\alpha x^B - Bu^\beta x^A).$$

If $p = 2$, denote by $\mathcal{S}_{A,B}$ the local system on $\mathbb{G}_m/\mathbb{F}_4$ whose trace function is given by

$$u \in k/\mathbb{F}_4 \mapsto \frac{1}{2^{\deg(k/\mathbb{F}_4)}} \sum_{x \in k} \psi_k(Au^\alpha x^B - Bu^\beta x^A).$$

If p is odd and either p or A is $1 (\mathrm{mod}\ 4)$, then the arithmetic determinant of $\mathcal{S}_{A,B}$ on $\mathbb{G}_m/\mathbb{F}_p$ is trivial. If $p = 2$, the arithmetic determinant $\mathcal{S}_{A,B}$ on $\mathbb{G}_m/\mathbb{F}_4$ is trivial. If both p and A are $3 (\mathrm{mod}\ 4)$, then the arithmetic determinant $\mathcal{S}_{A,B}$ on $\mathbb{G}_m/\mathbb{F}_p$ is $(-1)^{\deg}$.

Proof. In all cases $\mathcal{S}_{A,B}$ is geometrically isomorphic to $\mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(A); \mathsf{Char}_{\mathrm{ntriv}}(B))$. Because A is odd and $A - B \geq 2$, the geometric determinant of $\mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(A); \mathsf{Char}_{\mathrm{ntriv}}(B))$, and hence of $\mathcal{S}_{A,B}$, is trivial. Therefore the arithmetic determinant is of the form $\delta^{\deg}$, and δ is the common value of $\det(Frob_{u,\mathbb{F}_p}|\mathcal{S}_{A,B})$ at points $u \in \mathbb{F}_p^\times$ for p odd, and the common value of $\det(Frob_{u,\mathbb{F}_4}|\mathcal{S}_{A,B})$ at points $u \in \mathbb{F}_4^\times$ if $p = 2$.

We take the point $u = 1$. Consider the Kummer pullback $[A]^\star\mathcal{S}_{A,B}$, whose trace function [KT6, Corollary 3.10(i)] is as follows: for p odd, it is

$$u \in k/\mathbb{F}_p \mapsto \frac{1}{\mathsf{Gauss}(\psi_k, \xi_2)} \sum_{x \in k} \psi_k(Aux^B - Bx^A),$$

and for p even it is

$$u \in k/\mathbb{F}_4 \mapsto \frac{1}{2^{\deg(k/\mathbb{F}_4)}} \sum_{x \in k} \psi_k(Aux^B - Bx^A).$$

So the pullback local system is lisse on $\mathbb{A}^1$, and continues to have trivial geometric determinant. Because $1^A = 1$, we have $\delta = \det(Frob_{1,\mathbb{F}_p}|[A]^\star\mathcal{S}_{A,B})$ for p odd, and $\delta = \det(Frob_{1,\mathbb{F}_4}|[A]^\star\mathcal{S}_{A,B})$ for p even. Because $[A]^\star\mathcal{S}_{A,B}$ is lisse on $\mathbb{A}^1$, the determinant at $u = 1$ is the same as the deterninant at $u = 0$. At $u = 0$, we are looking at

$$\mathrm{Trace}(Frob_{0,k}|[A]^\star\mathcal{S}_{A,B}) = \frac{1}{\mathsf{Gauss}(\psi_k, \xi_2)} \left(\sum_{x \in k} \psi_k(-Bx^A) \right),$$

for p odd, and at

$$\mathrm{Trace}(Frob_{0,\mathbb{F}_{4^n}}|[A]^\star\mathcal{S}_{A,B}) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_{4^n}} \psi_k(-Bx^A)$$

for $p = 2$.

If $p = 2$ or if $p \equiv 1 (\mathrm{mod}\ 4)$, this is symplectic, so has determinant 1. If $p \equiv 3 (\mathrm{mod}\ 4)$, then this $i \times$ symplectic (because we need to have cleared by $\pm\sqrt{p}$ to have been symplectic), so the determinant is i^{A-1}. ☐

There are further cases where a hypergeometric sheaf has a descent to $\mathbb{G}_m$ over a smaller field. Some have been described in Proposition 7.1. The key new input is the following. We have a finite field $\mathbb{F}_{p^f}$ and a multiplicative character χ of $\mathbb{F}_{p^f}^\times$ such that the f characters $\chi, \chi^p, \ldots, \chi^{p^{f-1}}$ are all distinct. As explained in [Ka3, Section 8.8], the Kloosterman sheaf

$$\mathcal{K}l_\psi(\chi, \chi^p, \ldots, \chi^{p^{f-1}})$$

has a natural descent to a lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$, pure of weight $f-1$, which we will denote

$$\mathcal{K}l_\psi(\chi, p^f).$$

Let us briefly recall the overall set up. Given a field k, and a finite étale k-algebra K/k, we form the "restriction of scalars" group scheme $\mathbb{K}^\times$ over k, defined as follows. For any k-algebra A, we form the K-algebra $A \otimes_k K$, and define

$$\mathbb{K}^\times(A) := (A \otimes_k K)^\times.$$

When L/k is a finite extension, then $L \otimes_k K$ is finite flat over L, over K, and over k. So we have two norm maps

$$\mathrm{Norm}_1 : L \otimes_k K \to L,$$

and

$$\mathrm{Norm}_2 : L \otimes_k K \to K,$$

and we have an absolute trace map

$$\mathrm{Trace} : L \otimes_k K \to k.$$

When k is a finite field, ψ is an additive character of k, and χ is a multiplicative character of $K^\times$, we can form the following sum: for each finite extension L/k, and each $u \in L^\times$,

$$u \mapsto (-1)^{\dim_k(K)-1} \sum_{x \in L \otimes_k K,\ \mathrm{Norm}_1(x)=u} \psi(\mathrm{Trace}(x))\chi(\mathrm{Norm}_2(x)).$$

When the finite etale algebra K is the f-fold self product $K = k^f$, this is the usual Kloosterman sum. When $k = \mathbb{F}_p$, $K = \mathbb{F}_{p^f}$, and χ is a character of $\mathbb{F}_{p^f}^\times$ with f distinct conjugates $\chi, \chi^p, \ldots, \chi^{p^{f-1}}$, this is the trace function of a lisse sheaf

$$\mathcal{K}l_\psi(\chi, p^f)$$

on $\mathbb{G}_m/\mathbb{F}_p$, which is pure of weight $f-1$ and which, pulled back to $\mathbb{G}_m/\mathbb{F}_{p^f}$, is isomorphic to $\mathcal{K}l_\psi(\chi, \chi^p, \ldots, \chi^{p^{f-1}})$.

At this point, the reader may wonder about the apparently arbitrary choice of χ among the various χ^{p^j} in the formula

$$u \mapsto (-1)^{\dim_k(K)-1} \sum_{x \in L \otimes_k K,\ \mathrm{Norm}_1(x)=u} \psi(\mathrm{Trace}(x))\chi(\mathrm{Norm}_2(x)).$$

Lemma 7.3. *Let $k = \mathbb{F}_p$, K/k and L/k finite extension fields, and χ a character of $K^\times$. For any $u \in L$, we have the identity*

$$\sum_{x \in L \otimes_k K,\ \mathrm{Norm}_1(x)=u} \psi(\mathrm{Trace}(x))\chi(\mathrm{Norm}_2(x)) = \sum_{x \in L \otimes_k K,\ \mathrm{Norm}_1(x)=u} \psi(\mathrm{Trace}(x))\chi^p(\mathrm{Norm}_2(x)).$$

Proof. For an element $\sum_i a_i \otimes b_i$ with the $a_i \in L$ and the $b_i \in K$, we have

$$\mathrm{Norm}_1(\sum_i a_i \otimes b_i) = \prod_{\sigma \in \mathrm{Gal}(K/k)} (\sum_i a_i \otimes \sigma(b_i)),$$

$$\mathrm{Norm}_2(\sum_i a_i \otimes b_i) = \prod_{\rho \in \mathrm{Gal}(L/k)} (\sum_i \rho(a_i) \otimes b_i).$$

Thus for $\sigma \in \mathrm{Gal}(K/k)$, we have $\mathrm{id}_L \otimes \sigma$ acting on $L \otimes_k K$, and the equivariance formulas that for $x \in L \otimes_k K$,

$$\mathrm{Norm}_1((\mathrm{id}_L \otimes \sigma)(x)) = \mathrm{Norm}_1(x), \quad \mathrm{Norm}_2((\mathrm{id}_L \otimes \sigma)(x)) = \sigma(\mathrm{Norm}_2(x)).$$

Apply this with σ taken to be the Frobenius automorphism $x \mapsto x^p$ of K. $\square$

Notice that when $f = 1$, χ is a character of $\mathbb{F}_p^\times$, and $\mathcal{K}l_\psi(\chi, p)$ is just $\mathcal{L}_\psi \otimes \mathcal{L}_\chi$.

Lemma 7.4. *Let χ be a multiplicative character of of $\mathbb{F}_{p^f}^\times$. The character $\prod_{i=0}^{f-1} \chi^{p^i}$ has order dividing $p-1$, so may be viewed as a character of $\mathbb{F}_p^\times$, call it $(\prod_{i=0}^{f-1} \chi^{p^i})_{\mathbb{F}_p}$. For $a \in \mathbb{F}_p^\times$, we have the identity*

$$\chi(a, \text{viewed in } \mathbb{F}_{p^f}^\times) = (\prod_{i=0}^{f-1} \chi^{p^i})_{\mathbb{F}_p}(a).$$

Proof. Because χ as a character of $\mathbb{F}_{p^f}^\times$ has finite order prime to p, we lose no information as viewing χ as having values in $\mathbb{F}_{p^f}^\times$ (instead of in . Because the source group is cyclic, χ is of the form $\chi(x) = x^n$ for some integer n, well defined mod $p^f - 1$. Viewing χ this way, we have $\chi(a) = a^n$. The character $\prod_{i=0}^{f-1} \chi^{p^i}$ is then the character

$$x \mapsto x^{n(p^f-1)/(p-1)} = \mathrm{Norm}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(x)^n,$$

which is to say that $\prod_{i=0}^{f-1} \chi^{p^i}$, viewed as a character of $\mathbb{F}_p^\times$, is the character $x \mapsto x^n$. $\square$

Here are some further cases of descents of hypergeometric sheaves to $\mathbb{G}_m/\mathbb{F}_p$. To describe them, we use the symbol (Kl_χ) to denote a list of multiplicative characters of the form $\chi, \chi^p, \ldots, \chi^{p^{f-1}}$ consisting of f distinct characters of $\mathbb{F}_{p^f}^\times$, and by $\mathcal{K}l_\psi(\mathsf{Kl}_\chi)$ the descent $\mathcal{K}l_\psi(\chi, p^f)$ described above. Let us also denote by

$$\Lambda_{\mathsf{Kl}_\chi} \tag{7.4.1}$$

the character $(\prod_{i=0}^{f-1} \chi^{p^i})_{\mathbb{F}_p}$ of $\mathbb{F}_p^\times$ described in Lemma 7.4 attached to $\mathcal{K}l_\psi(\chi, p^f)$.

Let us denote by Known any of the sets of characters

$$\mathsf{Char}_{\mathrm{ntriv}}(A),\ [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A),\ \mathsf{Char}(A),\ (\mathsf{Kl}_\chi),$$

and denote by

$$\mathcal{D}(A)_{\mathrm{ntriv}},\ \mathcal{D}([M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A)),\ \mathcal{D}(A),\ \mathcal{D}(\mathsf{Kl}_\chi)$$

their Kloosterman descents. One checks that $\mathcal{D}([M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A))$ is the $[M]_\star$ of the descent of $\mathsf{Char}_{\mathrm{ntriv}}(A)$ formed using the additive character $x \mapsto \psi(Mx)$, i.e., $\mathcal{D}([M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A))$ has trace function

$$u \in L^\times \mapsto -\sum_{t \in L,\ t^M = u}\ \sum_{x \in L} \psi_L(-Mx^A/t + MAx).$$

We will refer to these as "easy" Known's, and their descents as "easy" descents. For each "easy" descent $\mathcal{D}$, we define

$$\Lambda_{\mathcal{D}} := \mathbb{1}. \tag{7.4.2}$$

We then add to the list of Known's any list of characters each of which has order dividing $p-1$, which we descend simply as the Kloosterman with these characters. For this descent $\mathcal{D}$, we define $\Lambda_{\mathcal{D}}$ to be the product of the occurring characters. For any single χ of order dividing $p-1$, we also add to the list of Known's any the lists

$$\{\chi\rho : \rho \text{ in one of the lists } \mathsf{Char}_{\mathrm{ntriv}}(A), [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A), \mathsf{Char}(A)\}.$$

We descend these as

$$\mathcal{L}_\chi \otimes (\text{the known descent of } \mathsf{Char}_{\mathrm{ntriv}}(A), [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A), \mathsf{Char}(A)).$$

For such a descent $\mathcal{D} := \mathcal{L}_\chi \otimes (\text{an “easy” descent, of rank } r(\mathcal{D}))$, we define

$$\Lambda_{\mathcal{D}} := \chi^{r(\mathcal{D})}, \tag{7.4.3}$$

but cf. Remark 7.8. We will refer to these descents, together with the (Kl_χ) cases, as the “hard” Knowns.

For each Known, we must keep track of the “weight drop” it affords. This data is given in Table 3. In its first three rows, ρ is any character of order dividing $p-1$.

input characters	input weight	Descent	Descent weight	weight loss
$\rho\mathsf{Char}_{\mathrm{ntriv}}(A)$	$A-2$	$\mathcal{L}_\rho \otimes \mathcal{D}(A)_{\mathrm{ntriv}}$	1	$A-3$
$\rho[M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A)$	$M(A-2)$	$\mathcal{L}_\rho \otimes \mathcal{D}([M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A))$	1	$M(A-2)-1$
$\rho\mathsf{Char}(A)$	$A-1$	$\mathcal{L}_\rho \otimes \mathcal{D}(A)$	0	$A-1$
$\chi, \chi^p, \dots, \chi^{p^{f-1}}$	$f-1$	$\mathcal{K}l_\psi(\chi, p^f)$	$f-1$	0
list of f characters of $\mathbb{F}_p^\times$	$f-1$	same list	$f-1$	0

TABLE 3. Weight loss in passing to descent, ρ any character of order dividing $p-1$

Theorem 7.5. *Let $\mathcal{H}$ be an irreducible hypergeometric of type (n,m) with $n \neq m$, of the form*

$$\mathcal{H}yp_\psi\big(\sqcup(\text{various } \mathsf{Known}_1\text{'s}) \smallsetminus \sqcup(\text{various } \mathsf{Known}_2\text{'s}); \sqcup(\text{various } \mathsf{Known}_3\text{'s})\big).$$

Denote by L the fixed field of the subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *which fixes as a set each of the following sets:*

(a) *For each* Known_1*, the set of characters occurring in* Known_1.
(b) *For each* Known_2*, the set of characters occurring in* Known_2.
(c) *For each* Known_3*, the set of characters occurring in* Known_3.

[Here we understand that when (Kl_χ) is a list of χ^{p^j}, then all the χ^{p^j} are the “characters which occur in” the corresponding $\mathcal{K}l_\psi(\mathsf{Kl}_\chi)$.] *Then we have the following results.*

(i) *$\mathcal{H}$ has a descent $\mathcal{H}_0$ to a lisse sheaf on $\mathbb{G}_m/\mathbb{F}_p$ which is pure of integer weight $w(\mathcal{H}_0)$. If p is odd, then*

$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes (-\mathsf{Gauss}(\psi, \xi_2))^{-w(\mathcal{H}_0)\deg/\mathbb{F}_p}$$

is pure of weight zero. If $p=2$ and the weight $w(\mathcal{H}_0)$ is even, then

$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes 2^{-(w(\mathcal{H}_0)/2)\deg/\mathbb{F}_2}$$

is pure of weight zero. If $p=2$ and the weight $(w(\mathcal{H}_0)$ is odd, then pulled back to $\mathbb{G}_m/\mathbb{F}_4$,

$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes 2^{-w(\mathcal{H}_0)\deg/\mathbb{F}_2}$$

is pure of weight zero.

(ii) *Define the character Λ of $\mathbb{F}_p^\times$ using* (7.4.2), (7.4.3) *as follows:*

$$\Lambda := \Big(\prod_{\mathsf{Known}_1\text{'s}} \Lambda_{\mathsf{Known}}\Big) \Big/ \Big(\prod_{\mathsf{Known}_2\text{'s and } \mathsf{Known}_3\text{'s}} \Lambda_{\mathsf{Known}}\Big).$$

Suppose $n \equiv m \pmod{p-1}$. If Λ is trivial, then for $k/\mathbb{F}_p$ a finite extension, each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$*, lies in L. If either the weight $w(\mathcal{H}_0)$ is even or if $k/\mathbb{F}_p$ is an extension of even degree, the same is true for each Frobenius trace* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$*. More generally, if Λ has order d, then for $k/\mathbb{F}_{p^d}$ a finite extension, each Frobenius trace* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$*, lies in L. If either the product $dw(\mathcal{H}_0)$ is even, or if $k/\mathbb{F}_{p^d}$ has even degree, the same is true is true for each Frobenius trace* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$.

(iii) *If we drop the hypothesis that* $n \equiv m \pmod{(p-1)}$ *in* (ii) *above, then for every finite extension* $k/\mathbb{F}_p$ *of degree divisible by the order* d *of* Λ*, each Frobenius trace* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$*, lies in* $L(\zeta_p)$*. The same statement holds for* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00})$ *if either* p *is odd or if in addition* $k/\mathbb{F}_p$ *has even degree.*

(iii-bis) *Suppose that* $r|(p-1)$*, and* $rn \equiv rd \pmod{(p-1)}$*. Suppose that* L *is an intermediate field* $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_N)$*, and that each of the sets* $\{\chi_i\}_i$ *and* $\{\rho_j\}_j$ *is fixed (as a set) by* $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/L)$*. Let* $K \subset \mathbb{Q}(\zeta_p)$ *be the extension* $K/\mathbb{Q}$ *of degree* r *inside* $\mathbb{Q}(\zeta_p)$*. Then for every finite extension* $k/\mathbb{F}_p$ *of degree divisible by the order* d *of* Λ*, each* $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}_0), u \in k^\times$*, lies in* KL*. If either* r *is even or if the product* $dw(\mathcal{H}_0)$ *is even, or if* $k/\mathbb{F}_{p^d}$ *has even degree, the same statement holds for* $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$*.*

Proof. The case when there is a "subtraction" of Known_2's is handled moving them "downstairs" and treating the (no longer irreducible) hypergeometric sheaf

$$\mathcal{H}yp_\psi\big(\sqcup(\text{various } \mathsf{Known}_1\text{'s}; \sqcup(\text{various } \mathsf{Known}_2\text{'s}) \sqcup (\text{various } \mathsf{Known}_3\text{'s})\big)$$

and then forming its **Cancel**, i.e., its highest weight quotient, cf. [KT7, Theorem 7.1 and Section 10]. To treat the case of

$$\mathcal{H}yp_\psi(\sqcup(\text{various } \mathsf{Known}_1\text{'s}); \sqcup(\text{various } \mathsf{Known}_3\text{'s})),$$

we form the ! multiplicative convolution of the descents $\mathcal{D}(\mathsf{Known})$ of the "upstairs" Known's with the $\mathrm{inv}^\star(\overline{\mathcal{D}(\mathsf{Known})}$ of the descents of the "downstairs" Known's.

In either case, we end up with a (not necessarily irreducible) hypergeometric of some type (n, m) of the form

$$\mathcal{H}yp_\psi(\sqcup(\text{various } \mathsf{Known}_1\text{'s}); \sqcup(\text{various } \mathsf{Known}_3\text{'s})).$$

The weight of $\mathcal{H}_0$ is then

$$w(\mathcal{H}_0) = n + m - 1 - \sum_{\text{"upstairs" and "downstairs" descents } \mathcal{D}_i} (\text{weight loss in passing to } \mathcal{D}_i),$$

with the weight losses tabulated in Table 3.

From the explicit trace formulas of the descents of the Known's, we see that the only multiplicative characters that occur are those in the (Kl) components. By insisting that either the weight $w(\mathcal{H}_0)$ is even or that $k/\mathbb{F}_p$ has even degree, we insure that the clearing factor is $\pm$ a power of p, so does not alter the field of traces. If the integer r of (iii-bis) is even, then the quadratic Gauss sum which enters into the clearing factor lies in the field K, so does not alter the fact that traces lie in KL.

It remains only to recall how the fact that $n \equiv m \pmod{(p-1)}$ implies that the traces are independent of the choice of ψ. Let us illustrate in a special case, before treating the general case. Consider a hypergeometric of the form

$$\mathcal{H} := \mathcal{H}yp_\psi(\mathsf{Char}_{\mathrm{ntriv}}(A); (\mathsf{Kl})), \text{ where } (\mathsf{Kl}) = \{\chi, \chi^p, \ldots, \chi^{p^{f-1}}\},$$

in which $\#A - 1 \equiv f \pmod{(p-1)}$. Here the character Λ of $\mathbb{F}_p^\times$ is just χ, restricted to $\mathbb{F}_p^\times \subset \mathbb{F}_{p^f}^\times$, and is assumed trivial.

For $L/\mathbb{F}_p$ a finite extension, and $u \in L^\times$, $\mathrm{Trace}(Frob_{u,L}|\mathcal{H}_0)$ is $(-1)^{\#A-1-f-1}$ times

$$\sum_{st=u} \sum_{x \in L} \psi_L(-x^A/s + Ax) \sum_{y \in L \otimes_{\mathbb{F}_p} K, \mathrm{Norm}_1(y) = 1/t} \psi_k(\mathrm{Trace}(y)) \overline{\chi}(\mathrm{Norm}_2(y)) =$$

(solve for $t = 1/\mathrm{Norm}_1(y)$, then for $s = u/t = u\mathrm{Norm}_1(y)$)

$$= \sum_{x \in L,\ y \in L \otimes_{\mathbb{F}_p} K} \psi_L\big(-x^A/(u\mathrm{Norm}_1(y)) + Ax\big) \psi_k(\mathrm{Trace}(y)) \overline{\chi}(\mathrm{Norm}_2(y).$$

If we replace ψ by $x \mapsto \psi(ax)$ with $a \in \mathbb{F}_p^\times$, this expression changes to

$$= \sum_{x \in L,\ y \in L \otimes_{\mathbb{F}_p} K} \psi_L\big(-ax^A/(u\mathrm{Norm}_1(y)) + aAx\big)\psi_k(\mathrm{Trace}(ay))\overline{\chi}(\mathrm{Norm}_2(y).$$

Making the substitutions $x \mapsto x/a, y \mapsto y/a$, this becomes

$$= \sum_{x \in L,\ y \in L \otimes_{\mathbb{F}_p} K} \psi_L\big(-a(x/a)^A/(u\mathrm{Norm}_1(y/a)) + Ax\big)\psi_k(\mathrm{Trace}(y))\overline{\chi}(\mathrm{Norm}_2(y/a) =$$

$$= \sum_{x \in L,\ y \in L \otimes_{\mathbb{F}_p} K} \psi_L\big(-a(x^A/a^A)/(u\mathrm{Norm}_1(y)/a^f) + Ax\big)\psi_k(\mathrm{Trace}(y))\overline{\chi}(\mathrm{Norm}_2(y)/a^{\deg(L/\mathbb{F}_p)}).$$

In the first sum, the factor aa^f/a^A is 1 by the imposed congruence $\#A - 1 \equiv f \pmod{(p-1)}$, so this expression is just $\overline{\chi}(1/a^{\deg(L/\mathbb{F}_p)}) = \Lambda(1/a^{\deg(L/\mathbb{F}_p)})$ times the original sum.

In the general case, the argument goes as follows. Fix a finite extension $L/\mathbb{F}_p$. For each known descent $\mathcal{D}$, with rank $r(\mathcal{D})$, view $u \in L^\times \mapsto \mathrm{Trace}(Frob_{u,L}|\mathcal{D})$ as a function $u \mapsto \mathcal{D}(u)$ on $L^\times$, which (L being fixed) we will refer to as "the trace function of $\mathcal{D}$". For $a \in \mathbb{F}_p^\times$, denote by $\mathcal{D}_a(u)$ the trace function we get by replacing ψ by $x \mapsto \psi(ax)$. Equivalently, if we denote by σ_a the automorphism of $\mathbb{Q}(\zeta_p, \mu_{\text{prime to } p})/\mathbb{Q}(\mu_{\text{prime to } p})$ which maps ζ_p to ζ_p^a, then $\mathcal{D}_a(u) = \sigma_a(\mathcal{D}(u))$. The key identity is

$$\mathcal{D}_a(u) = \mathcal{D}(ua^{r(\mathcal{D})})\Lambda_{\mathcal{D}}(a^{-\deg(L/\mathbb{F}_p)}).$$

When we form a multiple ! multiplicative convolution of, say S various $\mathcal{D}^{(i)}$'s and T various $\mathrm{inv}^\star\overline{\mathcal{D}^{(j)}}$'s, its trace function is $(-1)^{S+T-1}$ times

$$\sum_{\prod_i s_i = u \prod_j t_j} \prod_i \mathcal{D}^{(i)}(s_i) \prod_j \overline{\mathcal{D}^{(j)}}(t_j).$$

When we replace each $\mathcal{D}^{(i)}$ by $\mathcal{D}_a^{(i)}$ and each $\overline{\mathcal{D}^{(j)}}$ by $\overline{\mathcal{D}_a^{(j)}}$, this sum becomes $\Lambda(1/a^{\deg(L/\mathbb{F}_p)})$ times

$$\sum_{\prod_i s_i = u \prod_j t_j} \prod_i \mathcal{D}^{(i)}(s_i a^{r(\mathcal{D}^{(i)})}) \prod_j \overline{\mathcal{D}^{(j)}}(t_j a^{r(\mathcal{D}^{(j)})}).$$

Our assumption on the type (n, m) that $n - m$ is divisble by $p-1$ means that $\sum_i r(\mathcal{D}^{(i)}) \equiv \sum_j r(\mathcal{D}^{(j)}) \pmod{(p-1)}$. Thus in the above sum, the domain of summation

$$\prod_i s_i = u \prod_j t_j$$

is equal to the domain of summation

$$\prod_i (s_i a^{r(\mathcal{D}^{(i)})}) = u \prod_j (t_j a^{r(\mathcal{D}^{(j)})}).$$

So if $\deg(L/\mathbb{F}_p)$ is divisible by the order d of Λ, trace function of this multiple convolution is independent of the choice of nontrivial additive character ψ of $\mathbb{F}_p$.

To prove (iii-bis), repeat the proof of (iii-bis) given in Proposition 6.1. ☐

Remark 7.6. In the above discussion, we focused on and used the additional descents of Kloosterman sheaves of the form

$$\mathcal{K}l_\psi(\chi, \chi^p, \ldots, \chi^{p^{f-1}}),$$

in which the χ^{p^i} are f distinct characters of $\mathbb{F}_{p^f}^\times$. There is nothing special about $\mathbb{F}_p$ here: we could have descended Kloosterman sheaves

$$\mathcal{K}l_\psi(\chi, \chi^q, \ldots, \chi^{q^{f-1}}),$$

in which the χ^{q^i} are f distinct characters of $\mathbb{F}_{q^f}^\times$, and used the same recipe to get a descent $\mathcal{K}l_\psi(\chi, q^f)$ to $\mathbb{G}_m/\mathbb{F}_q$. Let us allow these, and also as Known any list of characters each of which has order dividing $q-1$. For any single χ of order dividing $q-1$, we may also add to the list of Known's any the lists

$$\{\chi\rho : \rho \text{ in one of the lists } \mathsf{Char}_{\mathrm{ntriv}}(A), [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A), \mathsf{Char}(A), (\mathsf{Kl}_\chi)\}.$$

Then the obvious reformulation of Theorem 7.5 produces descents to $\mathbb{G}_m/\mathbb{F}_q$ with the same rationality properties when $n \equiv m \pmod{(p-1)}$. In this situation, the character Λ becomes a character of $\mathbb{F}_q^\times$, but it is still the order d of its restriction to $\mathbb{F}_p^\times$, and **not** its order as a character of $\mathbb{F}_q^\times$, by which the degrees of extensions $L/\mathbb{F}_q$ must be divisible to have traces in L. One example of this sort of descent situation is in characteristic $p = 2$, χ of order 5, and $\mathcal{K}l_\psi(\chi, \chi^4)$, which is an $\mathbb{F}_4$ instance. Another is in characteristics $p = 3, 5$, with χ a character of order 7, and $\mathcal{K}l_\psi(\chi, \chi^2, \chi^4)$, which is an $\mathbb{F}_{p^2}$ instance for $p = 3, 5$ (but an $\mathbb{F}_p$ instance for $p = 2, 11$).

To avoid any ambiguity, let us formulate explicitly the $\mathbb{F}_q$-version of Theorem 7.5. We have the "easy" descents as before. For each character ρ of order dividing $q-1$, we have objects

$$\{\chi\rho : \rho \text{ in one of the lists } \mathsf{Char}_{\mathrm{ntriv}}(A), [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A), \mathsf{Char}(A)\}.$$

We descend these as

$$\mathcal{L}_\chi \otimes (\text{the known descent of } \mathsf{Char}_{\mathrm{ntriv}}(A), [M]_\star\mathsf{Char}_{\mathrm{ntriv}}(A), \mathsf{Char}(A)).$$

For such a descent $\mathcal{D} := \mathcal{L}_\chi \otimes (\text{an "easy" descent, of rank } r(\mathcal{D}))$, , we define $\Lambda_\mathcal{D}$ as a character of $\mathbb{F}_p^\times$ by

$$\Lambda_\mathcal{D} := \chi^{r(\mathcal{D})} \text{ restricted to } \mathbb{F}_p^\times. \tag{7.6.1}$$

For each subfield $\mathbb{F}_{q_0} \subset \mathbb{F}_q$, we may define the (Kl_ρ) data over $\mathbb{F}_{q_0}$, i.e., a multiplicative character ρ of some degree $f \geq 2$ extension of $\mathbb{F}_{q_0}$ which has f distinct conjugates under $\rho \mapsto \rho^{q_0}$, which allows us to form $\mathcal{K}l_\psi(\rho, (q_0)^f)$ on $\mathbb{G}_m/\mathbb{F}_{q_0}$. We then take the pull back of $\mathcal{K}l_\psi(\rho, (q_0)^f)$ to $\mathbb{G}_m/\mathbb{F}_q$ to be the descent $\mathcal{D}$ of this (Kl_ρ) data, and define its $\Lambda_\mathcal{D}$ as a character of $\mathbb{F}_p^\times$ by

$$\Lambda_\mathcal{D} := \rho^{r(\mathcal{D})} \text{ restricted to } \mathbb{F}_p^\times. \tag{7.6.2}$$

With these notions of what is a Known over $\mathbb{F}_q$, we may state the $\mathbb{F}_q$ version of Theorem 7.5.

Theorem 7.7. *Let $\mathcal{H}$ be an irreducible hypergeometric of type (n, m) with $n \neq m$, of the form*

$$\mathcal{H}yp_\psi\big(\sqcup(\text{various } \mathsf{Known}_1\text{'s}) \smallsetminus \sqcup(\text{various } \mathsf{Known}_2\text{'s}); \sqcup(\text{various } \mathsf{Known}_3\text{'s})\big).$$

Denote by L the fixed field of the subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which fixes as a set each of the following sets:

(a) *For each Known_1, the set of characters occurring in Known_1.*
(b) *For each Known_2, the set of characters occurring in Known_2.*
(c) *For each Known_3, the set of characters occurring in Known_3.*

[Here we understand that when (Kl_ρ) is the list of ρ^{q^j}, then all the ρ^{q^j} are the "characters which occur in" the corresponding $\mathcal{K}l_\psi(\mathsf{Kl}_\rho)$.] *Then we have the following results.*

(i) *$\mathcal{H}$ has a descent $\mathcal{H}_0$ to a lisse sheaf on $\mathbb{G}_m/\mathbb{F}_q$ which is pure of integer weight $w(\mathcal{H}_0)$. If p is odd, then*
$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes (-\mathsf{Gauss}(\psi, \xi_2))^{-w(\mathcal{H}_0)\deg/\mathbb{F}_q}$$
is pure of weight zero.If $p = 2$ and either the weight $w(\mathcal{H}_0)$ is even or $\deg(\mathbb{F}_q/\mathbb{F}_p)$ is even, then
$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes 2^{-\deg(\mathbb{F}_q/\mathbb{F}_p)(w(\mathcal{H}_0)/2)\deg/\mathbb{F}_q}$$
is pure of weight zero. If $p = 2$ and $\deg(\mathbb{F}_q/\mathbb{F}_p)w(\mathcal{H}_0)$ is odd, then pulled back to $\mathbb{G}_m/\mathbb{F}_{q^2}$,
$$\mathcal{H}_{00} := \mathcal{H}_0 \otimes 2^{-w(\mathcal{H}_0)\deg/\mathbb{F}_q}$$
is pure of weight zero.

(ii) *Define the character Λ of $\mathbb{F}_p^\times$ using (7.4.2), (7.4.3) as follows:*
$$\Lambda := \Big(\prod_{\mathsf{Known}_1{}'\mathrm{s}} \Lambda_{\mathsf{Known}}\Big)/\Big(\prod_{\mathsf{Known}_2{}'\mathrm{s}\ \text{and}\ \mathsf{Known}_3{}'\mathrm{s}} \Lambda_{\mathsf{Known}}\Big).$$
Suppose $n \equiv m \,(\mathrm{mod}\ (p-1))$. If Λ is trivial, then for $k/\mathbb{F}_q$ a finite extension, each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$, lies in L. If either the weight $w(\mathcal{H}_0)$ is even or if $k/\mathbb{F}_p$ is also an extension of even degree, the same is true for each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$. More generally, if Λ has order d, then for $k/\mathbb{F}_q$ a finite extension such that $k/\mathbb{F}_p$ has degree divisible by d, each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$, lies in L. If either the product $dw(\mathcal{H}_0)$ is even, or if $k/\mathbb{F}_p$ also has even degree, the same is true is true for each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$

(iii) *If we drop the hypothesis that $n \equiv m \,(\mathrm{mod}\ (p-1))$ in (ii) above, then for every finite extension $k/\mathbb{F}_q$ such that $k/\mathbb{F}_p$ has degree divisible by the order d of Λ, each Frobenius trace $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_0), u \in k^\times$, lies in $L(\zeta_p)$. The same statement holds for $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00})$ if either p is odd or if in addition $k/\mathbb{F}_p$ has even degree.*

(iii-bis) *Suppose that $r|(p-1)$, and $rn \equiv rd \ (\mathrm{mod}\ (p-1))$. Suppose that L is an intermediate field $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_N)$, and that each of the sets $\{\chi_i\}_i$ and $\{\rho_j\}_j$ is fixed (as a set) by $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/L)$. Let $K \subset \mathbb{Q}(\zeta_p)$ be the extension $K/\mathbb{Q}$ of degree r inside $\mathbb{Q}(\zeta_p)$. Then for every finite extension $k/\mathbb{F}_q$ such that $k/\mathbb{F}_p$ has degree divisible by the order d of Λ, each $\mathrm{Trace}(Frob_{u,E}|\mathcal{H}_0), u \in k^\times$, lies in KL. If either r is even or if the product $dw(\mathcal{H}_0)$ is even, or if in addition $k/\mathbb{F}_p$ has even degree, the same statement holds for $\mathrm{Trace}(Frob_{u,k}|\mathcal{H}_{00}), u \in k^\times$.*

Proof. Repeat verbatim the proof of Theoreom 7.5, replacing $\deg(L/\mathbb{F}_p)$ by $\deg(L/\mathbb{F}_q)$, and replacing $L \otimes_{\mathbb{F}_p} K$ by $L \otimes_{\mathbb{F}_q} K$. ☐

Remark 7.8. Even in the case of descents to $\mathbb{G}_m/\mathbb{F}_p$, there can be several ways to proceed, which can give different descents $\mathcal{D}$ with different characters $\Lambda_{\mathcal{D}}$. Here is a simple example. Fix $p \geq 5$, a character ρ of order $p-1$, and consider the Kloosterman sheaf
$$\mathcal{K}l_\psi(\rho, \rho^2, \ldots, \rho^{p-1}).$$
We can recognize its list of its characters as being $\mathsf{Char}(p-1)$, which provide one descent, call it $\mathcal{D}_1$. We might (foolishly) recognize the list of characters as being $\rho \cdot \mathsf{Char}(p-1)$, and form the descent $\mathcal{D}_2 := \mathcal{L}_\rho \otimes \mathcal{D}_1$. Or we might simply descend this Kloosterman sheaf as itself; call this descent $\mathcal{D}_3$. Their associated characters Λ are succesively $\mathbb{1}, \rho$, and the quadratic character ξ_2, which are all distinct (because $p \geq 5$, ρ cannot be ξ_2). So a fortiori, these three descents are all distinct.

Here is another example. Fix an integer $n \geq 3$, and a prime p which is 1 $(\mathrm{mod}\ n(n+1))$. Let ρ be a character of order n, and consider the list of characters $\rho \cdot \mathsf{Char}_{\mathrm{ntriv}}(A)$ for $A = n+1$. We can descend it as $\mathcal{D}_1 := \mathcal{L}_\rho \otimes \mathcal{D}(A)_{\mathrm{ntriv}}$, or we can form the Kloosterman sheaf with this list of characters and descend it as itself; call this descent $\mathcal{D}_2$. Here the associated characters Λ are successively ρ and ξ_2^n.

8. The notational scheme for descents

In each of the following sections, we will prove results in the following three part form.

(A) A certain hypergeometric sheaf $\mathcal{H}$ has a finite geometric monodromy group $G_{\mathrm{geom},\mathcal{H}}$. The characters occurring in $\mathcal{H}$ will be listed either individually or in terms of the sets Char_N and $\mathsf{Char}_N^\times$.
(B) The determination of the finite group $G_{\mathrm{geom},\mathcal{H}}$.
(C) Specifying a descent $\mathcal{H}_{00}$ of $\mathcal{H}$ to $\mathbb{G}_m$ over a small field, often $\mathbb{F}_p$ but in some cases $\mathbb{F}_{p^2}$, and specifying its finite arithmetic group $G_{\mathrm{arith},\mathcal{H}_{00}}$.

For part (C), we will name the descents as $\mathcal{H}(\mathcal{D}_1;\mathcal{D}_2)$ or $\mathcal{H}(\mathcal{D}_1 \setminus \mathcal{D}_2;\mathcal{D}_3)$ or as $\mathcal{H}(\mathcal{D}_1 \sqcup \mathcal{D}_2;\mathcal{D}_3)$ or as $\mathcal{H}(\mathcal{D}_1;\mathcal{D}_2 \sqcup \mathcal{D}_3)$, in this way specifying which descents $\mathcal{D}_i$ are to be used in the construction of $\mathcal{H}_0$, by the operations of multiple $_!$ convolution, $\mathcal{D} \mapsto \mathrm{inv}^\star\overline{\mathcal{D}}$, and **Cancel**, as explained in the first paragraph of the proof of Theorem 7.5. Once we have this $\mathcal{H}_0$, $\mathcal{H}_{00}$ is then obtained by constant field twisting by the appropriate power of the quadratic Gauss sum if p is odd, or by the appropriate power of 2 if $p=2$, see Theorems 7.5 and 7.7. The descents $\mathcal{D}_i$ descending the sets $\mathsf{Char}(N)$ or $\mathsf{Char}_{\mathrm{ntriv}}(N)$ will be denoted by those sets; the Kloosterman descents $\mathcal{K}l_\psi(\mathsf{Kl}_\xi)$ will be noted $(\mathsf{Kl})_{\xi,q_0^f}$. We will also specify the character Λ of $\mathbb{F}_p^\times$.

The descents occurring in the paper are all listed in Table 4.

9. Proving finiteness of G_{geom}

As already explained in Propositions 5.13 and 5.14, to prove finiteness of the geometric monodromy group for a hypergeometric sheaf, one needs to prove an inequality for Kubert's V-function [Ka7, 13.2] of the following form. One is given positive integers $n, m, \alpha_1, \dots, \alpha_n$, one is given representatives $\beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_m$ in $[0,1)$ of elements of $(\mathbb{Q}/\mathbb{Z})_{\text{prime to } p}$, and one is given a rational number $A \in \mathbb{Q}$. What must be proved is the inequality

$$V(\alpha_1 x + \beta_1) + \cdots + V(\alpha_n x + \beta_n) \le V(x+\gamma_1) + \cdots + V(x+\gamma_m) + A$$

for every $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to}\, p}$.

For the finitely many values $x = -\gamma_j$ $(j = 1, \dots, m)$ and $x = \frac{-\beta_i + k}{\alpha_i}$ $(i = 1, \dots, n,\ k = 0, \dots, \alpha_i - 1)$ the inequality can be checked directly.

Otherwise, we proceed as follows. For $r \ge 1$ and an integer x, define $[x]_r$ to be the sum of the p-adic digits of the representative in $\{1, \dots, p^r-1\}$ of the congruence class of x modulo p^r-1. For $x \in \{1, \dots, p^r-2\}$, one has [KRL, §4]

$$V\left(\frac{x}{p^r-1}\right) = \frac{1}{r(p-1)}[x]_r.$$

Denote by r_0 the smallest positive integer such that $(p^{r_0}-1)\beta_i, (p^{r_0}-1)\gamma_j \in \mathbb{Z}$ for every i, j. Then one needs to show that for every $r \in r_0\mathbb{Z}_+$ and every integer $1 \le x \le p^r-1$ not equal to $(p^r-1)(1-\gamma_j)$ for any j, one has

$$\sum_{i=1}^{m}[\alpha_i x + (p^r-1)\beta_i]_r \le \sum_{j=1}^{n}[x+(p^r-1)\gamma_j]_r + (p-1)rA. \tag{9.0.1}$$

No.	p	$\mathcal{H}$	Descent $\mathcal{H}_0$	on	Λ
1	3	$\mathcal{K}l(\mathbb{1},\xi_5,\xi_5^4)$	$\mathcal{H}(\mathsf{Char}(1)\sqcup(\mathsf{Kl})_{\xi_5,9^2};\emptyset)$	$\mathbb{G}_m/\mathbb{F}_9$	$\mathbb{1}$
2	5	$\mathcal{H}yp(\mathsf{Char}_8\smallsetminus\{\xi_8,\xi_8^{-1}\};\xi_{12},\xi_{12}^7)$	$\mathcal{H}yp(\mathsf{Char}_8\smallsetminus\{\xi_8,\xi_8^{-1}\};\xi_{12},\xi_{12}^7)$	$\mathbb{G}_m/\mathbb{F}_{25}$	$\mathbb{1}$
3	3	$\mathcal{K}l(\mathbb{1},\xi_7,\xi_7^2,\xi_7^4)$	$\mathcal{H}(\mathsf{Char}(1)\sqcup(\mathsf{Kl})_{\xi_7,9^3};\emptyset)$	$\mathbb{G}_m/\mathbb{F}_9$	$\mathbb{1}$
4	5	$\mathcal{H}yp(\xi_6\cdot\mathsf{Char}_7^\times;\xi_8,\xi_8^7)$	$\mathcal{H}(\xi_6\otimes\mathsf{Char}_{\rm ntriv}(7);\{\xi_8,\xi_8^7\})$	$\mathbb{G}_m/\mathbb{F}_{25}$	$\mathbb{1}$
5	5	$\mathcal{H}yp((\xi_3\cdot\mathsf{Char}_7^\times;\mathbb{1},\xi_2)$	$\mathcal{H}(\xi_3\otimes\mathsf{Char}_{\rm ntriv}(7);\mathsf{Char}(2))$	$\mathbb{G}_m/\mathbb{F}_{25}$	$\mathbb{1}$
6	5	$\mathcal{K}l(\mathbb{1},\xi_7,\xi_7^2,\xi_7^4)$	$\mathcal{H}(\mathsf{Char}(1)\sqcup(\mathsf{Kl})_{\xi_7,25^3};\emptyset)$	$\mathbb{G}_m/\mathbb{F}_{25}$	$\mathbb{1}$
7	3	$\mathcal{H}yp(\xi_2\cdot\mathsf{Char}_{11}^\times;\xi_8,\xi_8^3)$	$\mathcal{H}(\xi_2\otimes\mathsf{Char}_{\rm ntriv}(11);(\mathsf{Kl})_{\xi_8,3^2})$,	$\mathbb{G}_m/\mathbb{F}_9$	ξ_2
8	2	$\mathcal{H}yp(\mathsf{Char}_{11}^\times;\xi_7,\xi_7^2,\xi_7^4)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(11);(\mathsf{Kl})_{\xi_7,2^3})$	$\mathbb{G}_m/\mathbb{F}_2$	$\mathbb{1}$
9	3	$\mathcal{H}yp(\mathsf{Char}_{22};\mathsf{Char}_5^\times)$	$\mathcal{G}_{22,5_{\rm ntriv}}$, $\mathcal{H}(\mathsf{Char}(22);\mathsf{Char}_{\rm ntriv}(5))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
10	5	$\mathcal{H}yp(\mathsf{Char}_{22};\mathsf{Char}_3^\times)$	$\mathcal{G}_{22,3_{\rm ntriv}}$, $\mathcal{H}(\mathsf{Char}(22);\mathsf{Char}_{\rm ntriv}(3))$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
11	5	$\mathcal{H}yp(\mathsf{Char}_{28}\smallsetminus\mathsf{Char}_{14};\xi_8,\xi_8^7)$	$\mathcal{H}([14]_\star\mathsf{Char}_{\rm ntriv}(2);\{\xi_8,\xi_8^7\})$	$\mathbb{G}_m/\mathbb{F}_{25}$	$\mathbb{1}$
12	2	$\mathcal{H}yp(\xi_3\cdot\mathsf{Char}_{19}^\times;\mathbb{1},\xi_5,\bar{\xi}_5)$	$\mathcal{H}(\xi_3\otimes\mathsf{Char}_{\rm ntriv}(19);(\mathsf{Kl})_{\xi_5,4^2})$	$\mathbb{G}_m/\mathbb{F}_4$	$\mathbb{1}$
13	5	$\mathcal{H}yp(\mathsf{Char}_{29}^\times;\xi_{12},\xi_{12}^3,\xi_{12}^5,\xi_{12}^9)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(29);\{\xi_{12}^3,\xi_{12}^9\}\sqcup(\mathsf{Kl})_{\xi_{12},5^2})$	$\mathbb{G}_m/\mathbb{F}_5$	ξ_2
14	3	$\mathcal{H}yp(\mathsf{Char}_{14}\smallsetminus\{\mathbb{1},\xi_7,\xi_7^2,\xi_7^4\};$ $\xi_4,\xi_4^3)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(14)\setminus(\mathsf{Kl})_{\xi_7,9^3};(\mathsf{Kl})_{\xi_4,3^2})$, $\mathcal{H}((\mathsf{Kl})_{\xi_{14},3^6}\sqcup(\mathsf{Kl})_{\xi_7^3,9^3}\sqcup\mathsf{Char}_{\rm ntriv}(2);(\mathsf{Kl})_{\xi_4,3^2})$	$\mathbb{G}_m/\mathbb{F}_9$	$\mathbb{1}$
15	7	$\mathcal{H}yp(\xi_{20}^{1,3,5,7,9,13,15,17};\xi_3,\xi_3^2)$	$\mathcal{H}([10]_\star\mathsf{Char}_{\rm ntriv}(2)\smallsetminus(\mathsf{Kl})_{\xi_{20}^{11},49^2};\mathsf{Char}_{\rm ntriv}(3))$, $\mathcal{H}((\mathsf{Kl})_{\xi_{20},7^4}\sqcup(\mathsf{Kl})_{\xi_{20}^5,7^2}\sqcup(\mathsf{Kl})_{\xi_{20}^{13},49^2};\mathsf{Char}_{\rm ntriv}(3))$	$\mathbb{G}_m/\mathbb{F}_{49}$	$\mathbb{1}$
16	2	$\mathcal{H}yp(\mathsf{Char}_7^\times;\xi_3)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(7);\{\xi_3\})$	$\mathbb{G}_m/\mathbb{F}_4$	$\mathbb{1}$
17	3	$\mathcal{H}yp(\mathsf{Char}_7^\times;\xi_2)$	$\mathcal{S}_{7,2}$, $\mathcal{H}(\mathsf{Char}_{\rm ntriv}(7);\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
18	3	$\mathcal{H}yp(\mathsf{Char}_7^\times;\mathsf{Char}_4\smallsetminus\{\mathbb{1}\})$	$\mathcal{S}_{7,4}$, $\mathcal{H}(\mathsf{Char}_{\rm ntriv}(7);\mathsf{Char}_{\rm ntriv}(4))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
19	7	$\mathcal{H}yp(\mathsf{Char}_5\sqcup\mathsf{Char}_3^\times;\xi_2)$	$\mathcal{H}(\mathsf{Char}(5)\sqcup\mathsf{Char}_{\rm ntriv}(3);\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_7$	$\mathbb{1}$
20	7	$\mathcal{H}yp(\mathsf{Char}_{15}^\times;\mathsf{Char}_2)$	$\mathcal{H}((\mathsf{Kl})_{\xi_{15},7^4}\sqcup(\mathsf{Kl})_{\xi_{15}^2,7^4};\mathsf{Char}(2))$	$\mathbb{G}_m/\mathbb{F}_7$	$\mathbb{1}$
21	5	$\mathcal{K}l(\mathsf{Char}_9^\times\sqcup\mathsf{Char}_2)$	$\mathcal{H}(\mathsf{Char}(2)\sqcup[3]_\star\mathsf{Char}_{\rm ntriv}(3);\emptyset)$, $\mathcal{H}((\mathsf{Kl})_{\xi_9,5^6}\sqcup\mathsf{Char}(2);\emptyset)$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
22	5	$\mathcal{K}l(\mathsf{Char}_7\sqcup\{\xi_2\})$	$\mathcal{H}(\mathsf{Char}(7)\sqcup\mathsf{Char}_{\rm ntriv}(2);\emptyset)$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
23	13	$\mathcal{H}yp(\mathsf{Char}_{18}\smallsetminus\{\mathbb{1},\xi_6,\xi_6^2,\xi_6^3\};$ $\xi_4,\xi_4^3)$	$\mathcal{H}(\mathsf{Char}(18)\setminus\{\mathbb{1},\xi_6,\xi_6^2,\xi_6^3\};\{\xi_4,\xi_4^3\})$,	$\mathbb{G}_m/\mathbb{F}_{13}$	$\mathbb{1}$
24	2	$\mathcal{H}yp(\mathsf{Char}_{13}^\times;\mathsf{Char}_3^\times)$	$\mathcal{S}_{13,3}$, $\mathcal{H}(\mathsf{Char}_{\rm ntriv}(13);\mathsf{Char}_{\rm ntriv}(3))$	$\mathbb{G}_m/\mathbb{F}_2$	$\mathbb{1}$
25	7	$\mathcal{K}l(\{\mathsf{Char}_{12}^\times\cup\{\xi_6,\xi_6^3\})$	$\mathcal{H}((\mathsf{Kl})_{\xi_{12},7^2}\sqcup(\mathsf{Kl})_{\xi_{12}^{11},7^2}\sqcup\{\xi_6,\xi_6^3\};\emptyset)$	$\mathbb{G}_m/\mathbb{F}_7$	ξ_6^4
26	7	$\mathcal{H}yp(\mathsf{Char}_{12}^\times\cup\mathsf{Char}_3;\xi_2)$	$\mathcal{H}(\mathbb{1},\xi_{12},\xi_{12}^4,\xi_{12}^5,\xi_{12}^7,\xi_{12}^8,\xi_{12}^{11};\xi_2)$	$\mathbb{G}_m/\mathbb{F}_{49}$	$\mathbb{1}$
27	13	$\mathcal{H}yp(\mathsf{Char}_{15}\smallsetminus\{\mathbb{1}\};\xi_{12},\xi_{12}^5)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(15);\{\xi_{12},\xi_{12}^5\})$	$\mathbb{G}_m/\mathbb{F}_{13}$	ξ_2
28	7	$\mathcal{H}yp(\mathsf{Char}_9^\times\sqcup\{\mathbb{1}\};\xi_2)$	$\mathcal{H}(\mathsf{Char}(1),[3]_\star\mathsf{Char}_{\rm ntriv}(3);\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_7$	$\mathbb{1}$
29	7	$\mathcal{H}yp(\mathsf{Char}_9\smallsetminus\{\mathbb{1}\};\mathsf{Char}_2)$	$\mathcal{G}_{9_{\rm ntriv},2}$, $\mathcal{H}(\mathsf{Char}_{\rm ntriv}(9);\mathsf{Char}(2))$	$\mathbb{G}_m/\mathbb{F}_7$	$\mathbb{1}$
30	2	$\mathcal{H}yp(\mathsf{Char}_{39}^\times;\mathbb{1})$	$\mathcal{H}((\mathsf{Kl})_{\xi_{39},2^{12}}\sqcup(\mathsf{Kl})_{\xi_{39}^7,2^{12}};\mathsf{Char}(1))$	$\mathbb{G}_m/\mathbb{F}_2$	$\mathbb{1}$
31	3	$\mathcal{H}yp(\mathsf{Char}_{20}\smallsetminus(\mathsf{Char}_4\cup\mathsf{Char}_5);$ $\mathbb{1})$	$\mathcal{H}((\mathsf{Kl})_{\xi_{20},3^4}\sqcup(\mathsf{Kl})_{\xi_{20}^2,3^4}\sqcup(\mathsf{Kl})_{\xi_{20}^{11},3^4};\mathsf{Char}(1))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
32	3	$\mathcal{H}yp(\mathsf{Char}_{28}^\times;\mathbb{1})$	$\mathcal{H}yp((\mathsf{Kl})_{\xi_{28},3^6}\sqcup(\mathsf{Kl})_{\xi_{28}^5,3^6};\mathsf{Char}(1))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
33	2	$\mathcal{H}yp(\mathsf{Char}_{15}^\times;\mathsf{Char}_9\smallsetminus\mathsf{Char}_3^\times)$	$\mathcal{H}((\mathsf{Kl})_{\xi_{15},2^4}\sqcup(\mathsf{Kl})_{\xi_{15}^7,2^4};\mathsf{Char}(1),[3]_\star\mathsf{Char}_{\rm ntriv}(3))$	$\mathbb{G}_m/\mathbb{F}_2$	$\mathbb{1}$
34	2	$\mathcal{H}yp(\mathsf{Char}_9^\times;\mathsf{Char}_5)$	$\mathcal{H}([3]_\star\mathsf{Char}_{\rm ntriv}(3);\mathsf{Char}(5))$	$\mathbb{G}_m/\mathbb{F}_2$	$\mathbb{1}$
35	2	$\mathcal{H}yp(\mathsf{Char}_7^\times;\mathsf{Char}_3^\times\sqcup\xi_9,\xi_9^4,\xi_9^7)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(7);\mathsf{Char}_{\rm ntriv}(3)\sqcup(\mathsf{Kl})_{\xi_9,4^3})$	$\mathbb{G}_m/\mathbb{F}_4$	$\mathbb{1}$
36	3	$\mathcal{H}yp(\mathsf{Char}_5^\times;\mathsf{Char}_4\smallsetminus\mathsf{Char}_1)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(5);\mathsf{Char}_{\rm ntriv}(4))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
37	5	$\mathcal{H}yp(\mathsf{Char}_3^\times;\mathsf{Char}_2^\times)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(3);\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
38	3	$\mathcal{H}yp(\mathsf{Char}_4^\times;\mathbb{1})$	$\mathcal{H}([2]_\star\mathsf{Char}_{\rm ntriv}(2);\mathsf{Char}(1))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
39	5	$\mathcal{K}l(\mathsf{Char}_{12}^\times\sqcup\mathsf{Char}_3^\times)$	$\mathcal{K}l((\xi_4)\mathsf{Char}_{\rm ntriv}(3),(\xi_4^3)\mathsf{Char}_{\rm ntriv}(3),\mathsf{Char}_{\rm ntriv}(3))$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
40	5	$\mathcal{K}l((\mathsf{Char}_{16}\smallsetminus\mathsf{Char}_8)\sqcup\xi_8^{2,3,5,6})$	$\mathcal{K}l(([8]_\star\mathsf{Char}_{\rm ntriv}(2),\xi_8^{2,3,5,6})$	$\mathbb{G}_m/\mathbb{F}_{5^2}$	$\mathbb{1}$
41	13	$\mathcal{K}l(\mathsf{Char}_{16}\smallsetminus\mathsf{Char}_8)\sqcup\xi_8^{2,3,5,6})$	$\mathcal{K}l([8]_\star\mathsf{Char}_{\rm ntriv}(2),\xi_8^{2,3,5,6})$	$\mathbb{G}_m/\mathbb{F}_{13^2}$	$\mathbb{1}$
42	5	$\mathcal{H}yp(\mathsf{Char}_7;\xi_6^{1,3,5})$	$\mathcal{H}(\mathsf{Char}(7),[3]_\star\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_5$	$\mathbb{1}$
43	3	$\mathcal{H}yp(\mathsf{Char}_7;\xi_2\mathsf{Char}_5)$	$\mathcal{H}(\mathsf{Char}(7),[5]_\star\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_3$	$\mathbb{1}$
44	7	$\mathcal{H}yp(\mathsf{Char}_5^\times;\xi_2)$	$\mathcal{H}(\mathsf{Char}_{\rm ntriv}(5),\mathsf{Char}_{\rm ntriv}(2))$	$\mathbb{G}_m/\mathbb{F}_7$	$\mathbb{1}$

TABLE 4. Descents of some hypergeometric sheaves

Lemma 9.1. *For a positive integer x, denote by $[x]$ the sum of its p-adic digits. Suppose that there exists some $B \geq 0$ such that*

$$[\alpha_1 x+(p^r-1)\beta_1]+\cdots+[\alpha_n x+(p^r-1)\beta_n] \leq [x+(p^r-1)\gamma_1]+\cdots+[x+(p^r-1)\gamma_m]+(p-1)rA+B$$

for every $r \in r_0\mathbb{Z}_+$ and every $0 \leq x \leq p^r-1$. Then (9.0.1) holds for every $r \in r_0\mathbb{Z}_+$ and every $1 \leq x \leq p^r-1$ not equal to $(p^r-1)(1-\gamma_j)$ for any j.

Proof. For any such x, notice that each of the sums

$$\alpha_1 x+(p^r-1)\beta_1, \dots, \alpha_n x+(p^r-1)\beta_n$$

is strictly positive. Using the fact that $[z]_r \leq [z]$ for $z > 0$ [KRL, Proposition 2.2] we get

$$\begin{aligned}
&[\alpha_1 x+(p^r-1)\beta_1]_r+\cdots+[\alpha_n x+(p^r-1)\beta_n]_r \\
\leq\ &[\alpha_1 x+(p^r-1)\beta_1]+\cdots+[\alpha_n x+(p^r-1)\beta_n] \\
\leq\ &[x+(p^r-1)\gamma_1]+\cdots+[x+(p^r-1)\gamma_m]+(p-1)rA+B.
\end{aligned}$$

If, for some $j=1,\dots,m$, $x+(p^r-1)\gamma_j \leq p^r-1$, then $[x+(p^r-1)\gamma_j]=[x+(p^r-1)\gamma_j]_r$. Otherwise, $p^r-1 < x+(p^r-1)\gamma_j < 2(p^r-1)$ and the representative in $\{1,\dots,p^r-1\}$ of the congruence class of $x+(p^r-1)\gamma_j$ modulo p^r-1 is then $x+(p^r-1)\gamma_j-p^r+1$. Therefore

$$\begin{aligned}
[x+(p^r-1)\gamma_j]_r &= [x+(p^r-1)\gamma_j-p^r+1] \\
&= [x+(p^r-1)\gamma_j+1]-1 \\
&= [x+(p^r-1)\gamma_j]-q(p-1)
\end{aligned}$$

where q is the number of consecutive "$p-1$" digits at the end of the p-adic digit expansion of $x+(p^r-1)\gamma_j$. Since $x+(p^r-1)\gamma_j < 2(p^r-1)$ and $x+(p^r-1)\gamma_j \neq p^r-1$ for every j, q is at most $r-1$, so

$$\begin{aligned}
&[\alpha_1 x+(p^r-1)\beta_1]_r+\cdots+[\alpha_n x+(p^r-1)\beta_n]_r \\
\leq\ &[x+(p^r-1)\gamma_1]+\cdots+[x+(p^r-1)\gamma_m]+(p-1)rA+B \\
\leq\ &[x+(p^r-1)\gamma_1]_r+\cdots+[x+(p^r-1)\gamma_m]_r+(p-1)rA+(p-1)(r-1)m+B.
\end{aligned}$$

Furthermore, for every $s \geq 1$, the last r digits of $\frac{p^{rs}-1}{p^r-1}x+(p^{rs}-1)\gamma_j = \frac{p^{rs}-1}{p^r-1}(x+(p^r-1)\gamma_j)$ are the same as the last r digits of $x+(p^r-1)\gamma_j$ and, in particular, the last r digits are not all $p-1$, so we get (letting $y=\frac{p^{rs}-1}{p^r-1}x$):

$$\begin{aligned}
&[\alpha_1 y+(p^{rs}-1)\beta_1]_{rs}+\cdots+[\alpha_n y+(p^{rs}-1)\beta_n]_{rs} \\
\leq\ &[y+(p^{rs}-1)\gamma_1]_{rs}+\cdots+[y+(p^{rs}-1)\gamma_m]_{rs}+(p-1)rsA+(p-1)(r-1)m+B.
\end{aligned}$$

Using the Hasse-Davenport relation $[y]_{rs}=s[x]_r$ [KRLT1, Lemma 2.10], we conclude that

$$\begin{aligned}
&[\alpha_1 x+(p^r-1)\beta_1]_r+\cdots+[\alpha_n x+(p^r-1)\beta_n]_r \\
\leq\ &[x+(p^r-1)\gamma_1]_r+\cdots+[x+(p^r-1)\gamma_m]_r+(p-1)rA+\frac{(p-1)(r-1)m+B}{s}
\end{aligned}$$

and letting $s \to \infty$ we obtain (9.0.1). □

In order to prove the inequality

$$[\alpha_1 x+(p^r-1)\beta_1]+\cdots+[\alpha_n x+(p^r-1)\beta_n] \leq [x+(p^r-1)\gamma_1]+\cdots+[x+(p^r-1)\gamma_m]+(p-1)rA+B \tag{9.1.1}$$

for every $r \in r_0\mathbb{Z}_+$ and every $0 \le x \le p^r - 1$ we proceed by induction on r. For a few small values of r it is done by a computer check. Then we proceed as follows for a given r, assuming it has already been proved for smaller r. Let

$$\Delta(r,x) = [x+(p^r-1)\gamma_1]+\cdots+[x+(p^r-1)\gamma_m]+(p-1)rA-[\alpha_1 x+(p^r-1)\beta_1]-\cdots-[\alpha_n x+(p^r-1)\beta_n],$$

we need to show that $\Delta(r,x) \ge -B$.

We first prove a few cases of (9.1.1), in the following way. For some small $s < r$ which is also a multiple of r_0 we split off the last s digits of x. That is, we write $x = p^s y + z$ with $0 \le y < p^{r-s}$ and $0 \le z < p^s$. For every $i = 1, \dots, n$ let u_i be the number of digit carries in the sum

$$\alpha_i x + (p^r - 1)\beta_i = p^s(\alpha_i y + (p^{r-s} - 1)\beta_i) + (\alpha_i z + (p^s - 1)\beta_i)$$

and for every $j = 1, \dots, m$ let v_j be the number of digit carries in the sum

$$x + (p^r - 1)\gamma_j = p^s(y + (p^{r-s} - 1)\gamma_j) + (z + (p^s - 1)\gamma_j)$$

then

$$[\alpha_i x + (p^r - 1)\beta_i] = [\alpha_i y + (p^{r-s} - 1)\beta_i] + [\alpha_i z + (p^s - 1)\beta_i] - (p-1)u_i$$

and

$$[x + (p^r - 1)\gamma_j] = [y + (p^{r-s} - 1)\gamma_j] + [z + (p^s - 1)\gamma_j] - (p-1)v_j.$$

Assume $\Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \ge 0$. Then

$$\Delta(r,x) = \Delta(r-s,y) + \Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \ge \Delta(r-s,y)$$

and we conclude by induction.

For the remaining cases of (9.1.1), we use the following substitution method: for some small $s < r$ which is also a multiple of r_0 we write $x = p^s y + z$ with $0 \le y < p^{r-s}$ and $0 \le z < p^s$. Let $s' \le s$ and $0 \le z' \le p^{s'} - 1$, and let $x' = p^{s'} y + z'$ and $r' = r - s + s'$. Assume that $\Delta(r', x') \ge -B$ has already been proved (which is true by induction if $s' < s$). For every $i = 1, \dots, n$ let b_i (respectively b'_i) be the number obtained by removing the last s digits of $\alpha_i z + (p^s - 1)\beta_i$ (resp. by removing the last s' digits of $\alpha_i z' + (p^{s'} - 1)\beta_i$) and for every $j = 1, \dots, m$ let c_j (respectively c'_j) be the number obtained by removing the last s digits of $z + (p^s - 1)\gamma_j$ (resp. by removing the last s' digits of $z' + (p^{s'} - 1)\gamma_j$), which is always 0 or 1. Assume that $b_i = b'_i$ for every i and $c_j = c'_j$ for every j, and that $\Delta(s,z) \ge \Delta(s',z')$. Then the number of digit carries in the sum

$$\alpha_i x' + (p^{r'} - 1)\beta_i = p^{s'}(\alpha_i y + (p^{r'-s'} - 1)\beta_i) + (\alpha_i z' + (p^{s'} - 1)\beta_i)$$

is u_i, and the number of digit carries in the sum

$$x' + (p^{r'} - 1)\gamma_j = p^{s'}(y + (p^{r'-s'} - 1)\gamma_j) + (z' + (p^{s'} - 1)\gamma_j)$$

is v_j. So we get

$$\begin{aligned}
\Delta(r,x) &= \Delta(r-s,y) + \Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \\
&\ge \Delta(r'-s',y) + \Delta(s',z') - (p-1)\sum_j v_j + (p-1)\sum_i u_i \\
&= \Delta(r',x') \\
&\ge -B.
\end{aligned}$$

For some local systems for which r_0 is large, it will me more convenient to use the following variant of the previous procedure. Note that multiplication by p^{r_0} fixes the γ_j modulo 1. Suppose that there is some r_1 such that p^{r_1} *permutes* the γ_j modulo 1, and assume that $(p^{r_1} - 1)\beta_i \in \mathbb{Z}$ for every i for simplicity (the argument could be extended to the case where multiplication by p^{r_1} also permutes the β_i, but we will not need this case here). Let r_1 be the smallest positive integer with such property, then $r_1|r_0$ and r_0/r_1 is the order of the permutation under which multiplying by p^{r_1} acts on the γ_j.

Suppose, after relabeling the γ_j, that $\gamma_1, \dots, \gamma_e$ form a cycle for this action. Then $e|(r_0/r_1)$, let $r_0 = r_1 ef$. Splitting the p-adic digits of $(p^{r_0}-1)\gamma_1$ in groups of r_1, we can write

$$(p^{r_0}-1)\gamma_1 = h_{ef}p^{r_1(ef-1)} + h_{ef-1}p^{r_1(ef-2)} + \cdots + h_2 p^{r_1} + h_1$$

with $0 \le h_i \le p^{r_1}-1$. Since $p^{r_1}(p^{r_0}-1)\gamma_j \equiv (p^{r_0}-1)\gamma_{j+1}$ for $j = 1, \dots, e-1$ and $p^{r_1}(p^{r_0}-1)\gamma_e \equiv (p^{r_0}-1)\gamma_1 \pmod{p^{r_0}-1}$, we conclude that $h_{e+i} = h_i$ for $0 \le i \le e(f-1)$ and

$$(p^{r_0}-1)\gamma_j = h_{\overline{e+1-j}}p^{r_1(ef-1)} + h_{\overline{e-j}}p^{r_1(ef-2)} + \cdots + h_{\overline{3-j}}p^{r_1} + h_{\overline{2-j}}$$

for $1 \le j \le e$, where $\bar{l}$ is the representative in $\{1, \dots, e\}$ of the congruence class of l modulo e.

For every $k = 1, \dots, ef$ and $1 \le j \le e$, let

$$h_{k,j} = \sum_{l=0}^{k-1} h_{\overline{j+l}}p^{lr_1}.$$

Roughly speaking, these are the numbers formed by taking k consecutive (from the cyclic point of view) groups of r_1 digits of $(p^{r_0}-1)\gamma_1$, the last of them being the j-th one (counting from the right). Then $0 \le h_{k,j} < p^{kr_1}$, $h_{1,j} = h_j$, and $(p^{r_0}-1)\gamma_j = h_{ef,\overline{2-j}}$. Also, if $k > 1$, $h_{k,j} = p^{r_1}h_{k-1,\overline{j+1}} + h_j$ and, more generally, $h_{k,j} = p^{ir_1}h_{k-i,\overline{j+i}} + h_{i,j}$ for $0 < i < k$. We use this last formula to extend the definition of $h_{k,j}$ to every positive integer k. In particular, we have $h_{ef+k,j} = p^{kr_1}h_{ef,\overline{j+k}} + h_{k,j} = p^{kr_1}(p^{r_0}-1)\gamma_{\overline{2-j-k}} + h_{k,j}$.

Similarly, using the other cycles for the action of multiplication by p^{r_1} on the γ_j, we define h_j and $h_{k,j}$ for every $j = 1, \dots, m$ and $k \ge 1$.

In this situation, the inequality (9.1.1) is a special case of the following inequality: for every $k \ge 1$ and every $0 \le x \le p^r - 1$, where $r = kr_1$,

$$[\alpha_1 x + (p^r-1)\beta_1] + \cdots + [\alpha_n x + (p^r-1)\beta_n] \le [x + h_{k,1}] + \cdots + [x + h_{k,m}] + (p-1)rA + B. \tag{9.1.2}$$

When k is a multiple of ef (that is, when $r_0|r$) this inequality reduces to (9.1.1), since the $h_{k,j}$ are a permutation of the $(p^r-1)\gamma_j$. We define

$$\Delta(r,x) = [x + h_{k,1}] + \cdots + [x + h_{k,m}] + (p-1)rA - [\alpha_1 x + (p^r-1)\beta_1] - \cdots - [\alpha_n x + (p^r-1)\beta_n],$$

and want to show that $\Delta(r,x) \ge -B$.

The induction step now works as follows. For some small $l < k$ we split off the last $s := lr_1$ digits of x: we write $x = p^s y + z$ with $0 \le y < p^{r-s}$ and $0 \le z < p^s$. For every $i = 1, \dots, n$ let u_i be the number of digit carries in the sum

$$\alpha_i x + (p^r-1)\beta_i = p^s(\alpha_i y + (p^{r-s}-1)\beta_i) + (\alpha_i z + (p^s-1)\beta_i)$$

as before, and let v_j be the number of digit carries in the sum

$$x + h_{k,j} = p^s(y + h_{k-l,\overline{j+l}}) + (z + h_{l,j})$$

then

$$[\alpha_i x + (p^r-1)\beta_i] = [\alpha_i y + (p^{r-s}-1)\beta_i] + [\alpha_i z + (p^s-1)\beta_i] - (p-1)u_i$$

and

$$[x + h_{k,j}] = [y + h_{k-l,\overline{j+l}}] + [z + h_{l,j}] - (p-1)v_j.$$

Assume $\Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \geq 0$. Then

$$\Delta(r,x) = \Delta(r-s,y) + \Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \geq \Delta(r-s,y)$$

and we conclude by induction.

For the remaining cases of (9.1.2) we proceed by replacing the last digits as in the previous case: let $s = lr_1$ and $s' = l'r_1$ with $l' \leq l < k$, write $x = p^s y + z$ with $0 \leq y < p^{r-s}$ and $0 \leq z < p^s$, let $0 \leq z' \leq p^{s'} - 1$ and $x' = p^{s'}y + z'$, and define $r' = r - s + s'$, $k' = k - l + l'$. Assume that $\Delta(r', x') \geq -B$ has already been proved. Let b_i and b'_i be as above, and for every $j = 1, \ldots, m$ let c_j (respectively c'_j) be the number obtained by removing the last s digits of $z + h_{l,j}$ (resp. by removing the last s' digits of $z' + h_{l',\overline{j+l-l'}}$). Assume that $b_i = b'_i$ for every i and $c_j = c'_j$ for every j, and that $\Delta(s,z) \geq \Delta(s',z')$. Then the number of digit carries in the sum

$$\alpha_i x' + (p^{r'} - 1)\beta_i = p^{s'}(\alpha_i y + (p^{r'-s'} - 1)\beta_i) + (\alpha_i z' + (p^{s'} - 1)\beta_i)$$

is u_i, and the number of digit carries in the sum

$$x' + h_{k',\overline{j-l+l'}} = p^{s'}(y + h_{k-l,\overline{j+l}}) + (z' + h_{l',\overline{j+l-l'}})$$

is v_j. So we get

$$\begin{aligned}
\Delta(r,x) &= \Delta(r-s,y) + \Delta(s,z) - (p-1)\sum_j v_j + (p-1)\sum_i u_i \\
&\geq \Delta(r'-s',y) + \Delta(s',z') - (p-1)\sum_j v_j + (p-1)\sum_i u_i \\
&= \Delta(r',x') \\
&\geq -B.
\end{aligned}$$

10. The alternating group A_6

We begin by noting that

$$S := \mathsf{A}_6 \cong \mathrm{PSL}_2(9) \cong \mathrm{PSU}_2(9),$$

and, in the notation of [Atlas], $S \cdot 2_1 \cong \mathsf{S}_6$ and $S \cdot 2_2 \cong \mathrm{PGL}_2(9) \cong \mathrm{PGU}_2(9)$. Hence, using results of [KT1, Theorem 17.1] we can get hypergeometric sheaves in characteristic $p = 3$ which realize the 4-dimensional faithful representations of $2\mathsf{A}_6 \cong \mathrm{SL}_2(9)$. Likewise, using [KT5, Theorem 9.3] we can get hypergeometric sheaves in characteristic $p = 3$ which realize the 5-dimensional irreducible representations of A_6. Next, using [KT4, Corollary 8.2] we can get hypergeometric sheaves, still in characteristic $p = 3$, which realize irreducible representations of $2 \cdot \mathsf{A}_6 \cdot 2_2$ of degree 9 and 10 (that are irreducible over $2 \cdot \mathsf{A}_6$). Finally, using [KT7, Theorem 17.4] we can get hypergeometric sheaves, again in characteristic $p = 3$, which realize irreducible representations of $2 \cdot \mathsf{A}_6 \cdot 2_2$ of degree 8 (that are irreducible over $2 \cdot \mathsf{A}_6$).

Now we settle the question whether the exceptional covers $3 \cdot \mathsf{A}_6$ and $6 \cdot \mathsf{A}_6$ can occur as G_{geom} of some hypergeometric sheaves: the answer is "no" for $6 \cdot \mathsf{A}_6$ and "yes" for $3 \cdot \mathsf{A}_6$.

Lemma 10.1. *There are no hypergeometric sheaves of type (D,m) with $D > m$ in characteristic p that satisfy $(\mathbf{S}+)$ and have $G_{\mathrm{geom}} \rhd 6 \cdot \mathsf{A}_6$.*

Proof. Suppose such a sheaf $\mathcal{H}$ exists and let g_0 be the image of a generator of $I(0)$ in $G := G_{\mathrm{geom}}$. Then g_0 has simple spectrum on $\mathcal{H}$, and so D cannot exceed $\bar{\mathsf{o}}(g_0)$. On the other hand, condition $(\mathbf{S}+)$ and the hypothesis $G \rhd L := 6 \cdot \mathsf{A}_6$ imply by Lemma 3.1 that $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(\mathsf{A}_6)$ and so $\bar{\mathsf{o}}(g_0) \leq 10$ by [Atlas]. Thus $D \leq 10$. But L acts irreducibly and faithfully on $\mathcal{H}$, so $D = 6$ by

[Atlas]. Now, $\bar{\mathsf{o}}(g_0) \geq 6$ implies $g_0 \notin \mathbf{Z}(G)L$, and so G must induce an outer automorphism of L. But this is impossible, because no outer automorphism of L can stabilize the equivalence class of a faithful 6-dimensional representation of L (see [Atlas]). □

Theorem 10.2. *The local system $\mathcal{K} := \mathcal{K}l(\mathbb{1}, \xi_5, \xi_5^4)$ in characteristic $p = 3$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(x) + V\left(x + \frac{1}{5}\right) + V\left(x + \frac{4}{5}\right) \geq 1$$

and

$$V(x) + V\left(x + \frac{2}{5}\right) + V\left(x + \frac{3}{5}\right) \geq 1,$$

which are equivalent via the change of variable $x \mapsto 3x$. Using the fact that $V(\frac{i}{5}) = V(\frac{16i}{3^4-1}) = \frac{1}{8}[16i]$ for $1 \leq i \leq 4$ we check thate second inequality holds for $5x \in \mathbb{Z}$. For all other values of x, following §9, it suffices to prove

$$0 \leq \left[x + \frac{2(3^r-1)}{5}\right] + \left[x + \frac{3(3^r-1)}{5}\right] + [x] - 2r$$

for every $r \geq 1$ divisible by $r_0 = 4$ and every $0 \leq x \leq 3^r - 1$. Since multiplication by 3^2 permutes $\gamma_1 = \frac{2}{5}$ and $\gamma_2 = \frac{3}{5}$ and fixes $\gamma_3 = 0$ modulo 1, we can take $r_1 = 2$. Then, with the notation of §9, we have $(3^4-1)\gamma_1 = 1012_3$; $h_j = 12_3, 10_3$ and $h_{2,j} = 1012_3, 1210_3$ for $j = 1, 2$ respectively. We will prove that

$$0 \leq [x + h_{k,1}] + [x + h_{k,2}] + [x] - 2r$$

for every $r = 2k \geq 2$ and $0 \leq x \leq 3^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. Here $\sum_i u_i$ is always 0, since there are no terms on the left-hand side of the inequality.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
00,01,02,10	2	00,01,02,10	≥ 0	0	0	≥ 0
$ab11; ab \neq 12$	2	11,12	≥ 2	0	≤ 1	≥ 0
$ab20; ab \neq 10, 12$	2	20,21,22	≥ 2	0	≤ 1	≥ 0
$a1020; a \neq 2$	4	1020	1	0	0	1
021020	6	021020	3	0	0	3

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_3 = c_3'$ corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$c_1 = c_1'$	$c_2 = c_2'$
1211,1220	4	20	2	3	2	1	1
12	2	11	2	5	2	1	0
121020,221020	6	20	2	≥ 2	2	1	1
21,22	2	20	2	≥ 3	2	1	1

□

Theorem 10.3. *The local system $\mathcal{K} := \mathcal{K}l(\mathbb{1}, \xi_5, \xi_5^4)$ in characteristic $p = 3$ has geometric monodromy group $G_{\mathrm{geom}} = 3 \cdot \mathsf{A}_6$. Moreover, $\mathcal{H} := \mathcal{K} \otimes \mathcal{L}_{\xi_2}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_9$ with arithmetic monodromy group $G_{\mathrm{arith},k,\mathcal{H}'} = G_{\mathrm{geom},\mathcal{H}'} \cong (3 \cdot \mathsf{A}_6) \times C_2$ over any finite extension $k \supseteq \mathbb{F}_9$.*

Proof. (i) By Theorem 10.2, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to {\rm GL}(V)$ of G realizing $\mathcal{K}$. Now, $\mathcal{K}$ is visibly not Kummer induced, so (being Kloosterman) it is primitive. As $\dim(V) = 3$, (G, V) is tensor indecomposable, and not tensor induced. Hence (G, V) satisfies $(\mathbf{S}+)$. Next, by the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains $\sqrt{5}$. Indeed, for a generator g_0 of the image $I(0)$ in G we have $\varphi(g_0) = (1 + \sqrt{5})/2$ and moreover g_0 has central order 5. Furthermore, the image Q of $P(\infty)$ acts irreducibly on V by Proposition 5.9. In particular, Q is a non-abelian 3-group, so of order at least 3^3. Moreover, $\mathbf{Z}(Q) \neq 1$ acts faithfully, as scalars, on V, hence $\varphi(z) = 3\zeta_3$ for some $z \in \mathbf{Z}(Q)$ of order 3. It follows that $\mathbb{Q}(\varphi) \ni \sqrt{-3}$, and so $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$ by Proposition 6.1(iii). Now, since the cyclic group $\mathbf{Z}(G)$ acts via scalars, we have that

$$\mathbf{Z}(G) \leq C_6. \tag{10.3.1}$$

Suppose G satisfies conclusion (c) of Lemma 3.1. Then G contains an irreducible normal 3-subgroup R, and

$$G/\mathbf{C}_G(R)R \hookrightarrow {\rm Out}(R) \hookrightarrow {\rm SL}_2(3) \cong 2 \cdot \mathsf{A}_4.$$

But this is a contradiction, since $\mathbf{C}_G(R) = \mathbf{Z}(G)$ and 5 divides $|G/\mathbf{Z}(G)|$ but not $|\mathsf{S}_4|$.

Thus G is almost quasisimple. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\rm o}(g_0) = 5$ and 3^3 divides $|Q|$, we have by (10.3.1) that $3^2 \cdot 5$ divides the order of $G/\mathbf{Z}(G) \leq {\rm Aut}(S)$. Now we can apply the main result of [HM] to see that $S = \mathsf{A}_6$ and $L = 3 \cdot \mathsf{A}_6$. Since $5 \nmid |{\rm Out}(S)|$, g_0 must lie in the inverse image $\mathbf{Z}(G)L$ of S in G, whence $g_0 \in L \lhd G$ because $5 \nmid |\mathbf{Z}(G)$ by (10.3.1). It now follows from Theorem 5.1 that $G = L = 3 \cdot \mathsf{A}_6$.

(ii) By Theorem 7.7, $\mathcal{K}$ has a descent $\mathcal{K}_{00}$ to $\mathbb{F}_9$ for which any element in $G_{{\rm arith},k,\mathcal{K}_{00}}$ still has trace in $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$ when $k \supseteq \mathbb{F}_9$, and with $\mathcal{K}_0$ given on line 1 of Table 4. Now we take $\mathcal{H}' := \mathcal{K}_{00} \otimes \mathcal{L}_{\xi_2}$, and note that any element in $G_{{\rm arith},k,\mathcal{H}'}$ has trace in $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$, whence

$$\mathbf{Z}(G_{{\rm arith},k,\mathcal{H}'}) \leq C_6. \tag{10.3.2}$$

Let $H := G_{{\rm geom},\mathcal{H}} = G_{{\rm geom},\mathcal{H}'}$. By Lemma 5.12, we have that $H/\mathbf{Z}(H) \cong G/\mathbf{Z}(G) \cong \mathsf{A}_6$ and $H^{(\infty)} \cong G^{(\infty)} = 3 \cdot \mathsf{A}_6$. In particular, $H^{(\infty)}$ acts irreducibly on $\mathcal{H}$; and

$$\mathbf{Z}(G_{{\rm arith},k,\mathcal{H}'}) \geq \mathbf{Z}(H) \geq \mathbf{Z}(H^{(\infty)}) = C_3.$$

Next, a generator h_0 of the image of $I(0)$ in H has eigenvalues $-1, -\zeta_5, -\zeta_5^4$ on $\mathcal{H}$, whence h_0^5 acts as the scalar -1 on $\mathcal{H}$. It now follows from (10.3.2) that $\mathbf{Z}(G_{{\rm arith},k,\mathcal{H}'}) = \mathbf{Z}(H) = C_6$. Now, since no outer automorphism of $H^{(\infty)}$ fixes the equivalence class of the $H^{(\infty)}$-module $\mathcal{H}$, we conclude that $G_{{\rm arith},k,\mathcal{H}'} = H = \mathbf{Z}(H)H^{(\infty)} = (3 \cdot \mathsf{A}_6) \times C_2$. $\square$

Theorem 10.4. *The local system $\mathcal{H}_2 := \mathcal{H}yp(\mathsf{Char}_8 \smallsetminus \{\xi_8, \bar{\xi}_8\}; \xi_{12}, \xi_{12}^7)$ in characteristic $p = 5$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(8x) - V\left(x + \frac{1}{8}\right) - V\left(x + \frac{7}{8}\right) + V\left(-x - \frac{1}{12}\right) + V\left(-x - \frac{7}{12}\right) \geq 0,$$
$$V(8x) - V\left(x + \frac{3}{8}\right) - V\left(x + \frac{5}{8}\right) + V\left(-x - \frac{1}{12}\right) + V\left(-x - \frac{7}{12}\right) \geq 0,$$
$$V(8x) - V\left(x + \frac{1}{8}\right) - V\left(x + \frac{7}{8}\right) + V\left(-x + \frac{1}{12}\right) + V\left(-x + \frac{7}{12}\right) \geq 0,$$
$$V(8x) - V\left(x + \frac{3}{8}\right) - V\left(x + \frac{5}{8}\right) + V\left(-x + \frac{1}{12}\right) + V\left(-x + \frac{7}{12}\right) \geq 0.$$

The first two and the last two are equivalent via the change of variable $x \mapsto x + \frac{1}{2}$, and the change of variable $x \mapsto 5x$ interchanges the first and fourth ones, so they are all equivalent. Using the fact that $V(\frac{i}{24}) = V(\frac{i}{5^2-1}) = \frac{1}{8}[i]$ for $1 \leq i \leq 23$ we check that the inequalities hold for $24x \in \mathbb{Z}$. For all other values of x we can rewrite the third inequality, using that $V(x) + V(-x) = 1$ for $x \neq 0$, as

$$V(8x) \leq V\left(x + \frac{1}{8}\right) + V\left(x + \frac{7}{8}\right) + V\left(x + \frac{1}{12}\right) + V\left(x + \frac{7}{12}\right) - 1$$

and, following §9, it suffices to prove

$$[8x] \leq \left[x + \frac{5^r - 1}{8}\right] + \left[x + \frac{7(5^r - 1)}{8}\right] + \left[x + \frac{5^r - 1}{12}\right] + \left[x + \frac{7(5^r - 1)}{12}\right] - 4r$$

for every $r \geq 1$ multiple of $r_0 = 2$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
$00, 01, 02, 03$	2	$00, 01, 02, 03$	≥ 0	≥ 0	0	≥ 0
$a04, \ldots, a20; a \neq 3$	2	$04, \ldots, 20$	≥ 0	≥ 0	0	≥ 0
$a21, \ldots, a41; a \neq 0, 3$	2	$21, \ldots, 41$	≥ 0	≥ 0	0	≥ 0
$242, 442$	2	42	8	≥ 0	0	≥ 8
$443, 444$	2	44	0	≥ 0	0	≥ 0
$00ab, 01ab, 02ab$	4	$00ab, 01ab, 02ab$	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$	$c_3 = c'_3$	$c_4 = c'_4$
$0304,\ldots,0344$	4	04	2	≥ 0	0	1	0	1	0	0
$1304,\ldots,1344$	4	14	2	≥ 0	0	2	0	1	0	0
$2304,\ldots,2344$	4	24	2	≥ 0	0	4	0	1	0	1
$3304,\ldots,3333$	4	33	2	≥ 4	4	10	0	1	0	1
$3334,\ldots,3344$	4	34	2	≥ 8	8	11	0	1	0	1
$4304,\ldots,4344$	4	44	2	≥ 0	0	12	1	1	1	1
$1021,\ldots,1044$	4	11	2	≥ 0	0	1	0	1	0	0
$2021,\ldots,2044$	4	21	2	≥ 0	0	3	0	1	0	1
$3021,\ldots,3030$	4	24	2	≥ 0	0	4	0	1	0	1
$3031,\ldots,3044$	4	31	2	≥ 8	8	10	0	1	0	1
$4021,\ldots,4044$	4	41	2	≥ 8	8	11	0	1	0	1
$1142, 1143, 1144$	4	12	2	≥ 4	4	2	0	1	0	0
$2142, 2143, 2144$	4	22	2	≥ 0	0	3	0	1	0	1
$3142, 3143, 3144$	4	32	2	≥ 8	8	10	0	1	0	1
$4142, 4143, 4144$	4	42	2	≥ 8	8	12	1	1	0	1
$1243, 1244$	4	13	2	0	0	2	0	1	0	0
$2243, 2244$	4	23	2	0	0	3	0	1	0	1
$3243, 3244$	4	33	2	4	4	10	0	1	0	1
$4243, 4244$	4	43	2	0	0	12	1	1	1	1

$\square$

Theorem 10.5. *The local system $\mathcal{H}_2 := \mathcal{H}yp(\mathsf{Char}_8 \smallsetminus \{\xi_8, \bar{\xi}_8\}; \xi_{12}, \xi_{12}^7)$ in characteristic $p = 5$ has geometric monodromy group $G_{\mathrm{geom}} = (2 \times 3\mathsf{A}_6) \cdot 2_3$. Moreover, $\mathcal{H}_2$ is defined over $\mathbb{F}_{25}$, and has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ over any finite extension k of $\mathbb{F}_{25}$.*

Proof. (i) By Theorem 10.4, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}_2$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}_2$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence (G, V) satisfies $(\mathbf{S}+)$ by Theorem 3.5. Next, among the nontrivial Galois automorphisms of $\mathbb{Q}(\zeta_{24})/\mathbb{Q}$, only $\zeta_{24} \mapsto \zeta_{24}^7$ fixes each of the set of "upstairs" characters and the set of "downstairs" characters of $\mathcal{H}_2$. Hence the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is

$$\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{2}, \sqrt{-3}) \tag{10.5.1}$$

by Proposition 6.1(iii). Now, since the cyclic group $\mathbf{Z}(G)$ acts via scalars, we have that

$$\mathbf{Z}(G) \leq C_6. \tag{10.5.2}$$

We now have that G is almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, if g_0 denotes a generator of the image of $I(0)$ in G, then $\bar{\mathsf{o}}(g_0) = 8$, and the image Q of $P(\infty)$ has order 5 by Proposition 5.8(iv). Hence, by (10.5.2) we have that $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$ contains elements of order 8 and 5. Now we can apply the main result of [HM] to arrive at the following possibilities.

- $S = \mathsf{A}_7$. In this case, $G/\mathbf{Z}(G) \leq \mathsf{S}_7$ cannot contain any element of order 8, a contradiction.
- $(S, L) = (\mathrm{SU}_3(3), \mathrm{SU}_3(3))$, $(\mathrm{SU}_4(2), \mathrm{SU}_4(2))$, or $(\mathrm{PSU}_4(3), 6_1 \cdot \mathrm{PSU}_4(3))$. In all these cases, we can find an almost quasisimple group $M \leq L \cdot 2$ and an irreducible character ψ of M such that $M^{(\infty)} = L = G^{(\infty)}$, $M/\mathbf{Z}(M) \cong G/\mathbf{Z}(G)$, $\psi|_L = \varphi|_L$, and $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\sqrt{-3}) \subset \mathbb{Q}(\varphi)$. By Lemma 3.9, we can find a root of unity γ such that $\mathbb{Q}(\varphi) = \mathbb{Q}(\psi)(\gamma)$, contrary to (10.5.1).

• $(S, L) = (\mathrm{PSL}_3(4), 6\cdot\mathrm{PSL}_3(4))$. In this case, using [GAP] we can check that Φ (in fact already $\Phi|_L$) has $M_{2,2} = 2$. Now we apply Theorem 6.5, with $(a, b) = (2, 2)$, and $C = 146$, $B \le 322$, $A \le 176$ (according to Lemmas 6.6, 6.7, and Remark 6.8), which implies that the approximation of $M_{2,2}$ over $\mathbb{F}_{5^6}$ is at most 3.43. However, a calculation with Mathematica yields an approximation of (at least) 4.24 over $\mathbb{F}_{5^6}$, a contradiction.

• $(S, L) = (\mathrm{J}_2, 2\mathrm{J}_2)$. In this case, $\mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, contradicting (10.5.1).

• $S = \mathsf{A}_6$ and $L = 6\cdot\mathsf{A}_6$ or $3\cdot\mathsf{A}_6$. Note that the former possibility is ruled out by Lemma 10.1. Hence $L = 3\cdot\mathsf{A}_6$. Since $G/\mathbf{Z}(G) \le \mathrm{Aut}(S) = S\cdot 2^2$ contains an element of order 6, $G/\mathbf{Z}(G) > S$. Next, $\Phi|_L$ is irreducible, hence $G/\mathbf{Z}(G)$ cannot be $S\cdot 2_1$ or $S\cdot 2_2$ by [Atlas]. It follows that $G/\mathbf{Z}(G) = S\cdot 2_3$. We also know that $C_3 = \mathbf{Z}(L) \le \mathbf{C}_G(L) = \mathbf{Z}(G) \le C_6$ by (10.5.2). As g_0 has central order 8, we can find an element h in the group $H = 3S\cdot 2_3$ listed in [GAP] and an irreducible character ψ of H, afforded by a representation $\Psi : H \to \mathrm{GL}(V)$, such that $\Psi|_L = \Phi|_L$ and g_0 and h induce the same automorphism of L. Arguing as in the proof of Lemma 3.9, we can find $\alpha \in \mathbb{C}^\times$ such $\Phi(g_0) = \alpha\Psi(h)$. Now we have

$$\mathrm{Trace}(\Phi(g_0)) = \varphi(g_0) = \sqrt{2},\ \mathrm{Trace}(\Psi(h)) = \psi(h) = \pm\sqrt{-2},$$

and so $\alpha = \pm\sqrt{-1}$. Also note that $g_0^2 \in G$ and $h^2 \in L$. It follows that $g_0^2h^{-2} \in G$ and

$$\Phi(g_0^2) = \Phi(g_0)^2 = -\Psi(h^2),$$

i.e. $\Phi(g_0^2h^{-2}) = -\mathrm{Id}$. Thus $g_0^2h^{-2}$ is a central element of order 2, and we conclude that $\mathbf{Z}(G) \cong C_6$ and $G = (2\times 3\mathsf{A}_6)\cdot 2_3$.

(ii) The sheaf $\mathcal{H}_2$ is visibly defined over $\mathbb{F}_{25}$. Furthermore, over any finite extension k of $\mathbb{F}_{25}$, by Proposition 6.1(iii), any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$, we see that $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_6 = \mathbf{C}_G(L)$. Hence, if $G_{\mathrm{arith},k} > G_{\mathrm{geom}}$, we see that some element of $G_{\mathrm{arith},k}$ must induce an outer automorphism of S lying outside of $S\cdot 2_3$, which is impossible under the condition that it fixes $L = 3\cdot S$ and $\varphi|_L$, see [Atlas]. Therefore we must have that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. □

11. The alternating group A_7

Theorem 11.1. *The Kloosterman sheaf $\mathcal{K}l(\mathbb{1}, \xi_7, \xi_7^2, \xi_7^4)$ in characteristic $p = 3$, where ξ_7 is a character of order 7, has finite geometric monodromy group.*

Proof. We need to show:

$$V(x) + V\left(x + \frac{1}{7}\right) + V\left(x + \frac{2}{7}\right) + V\left(x + \frac{4}{7}\right) \ge \frac{3}{2}$$

or

$$V(x) + V\left(x - \frac{1}{7}\right) + V\left(x - \frac{2}{7}\right) + V\left(x - \frac{4}{7}\right) \ge \frac{3}{2}$$

depending on the choice of χ. Note that these two inequalities are equivalent via the change of variable $x \mapsto 3x$, since $V(3x) = V(x)$, so we will consider only the first one. Using the fact that $V(\frac{i}{7}) = V(\frac{104i}{3^6-1}) = \frac{1}{12}[104i]$ for $1 \le i \le 6$ we check that the inequality holds for $7x \in \mathbb{Z}$. For all other values of x, following §9, it suffices to prove

$$0 \le \left[x + \frac{3^r-1}{7}\right] + \left[x + \frac{2(3^r-1)}{7}\right] + \left[x + \frac{4(3^r-1)}{7}\right] + [x] - 3r$$

for every $r \ge 1$ divisible by $r_0 = 6$ and every $0 \le x \le 3^r - 1$. Since multiplication by 3^2 permutes $\gamma_1 = \frac{1}{7}$, $\gamma_2 = \frac{2}{7}$ and $\gamma_3 = \frac{4}{7}$ cyclically modulo 1, we can take $r_1 = 2$. Then, with the notation of §9, we have $(3^6-1)\gamma_1 = 010212_3$; $h_j = 12_3, 02_3, 01_3$; $h_{2,j} = 0212_3, 0102_3, 1201_3$ and $h_{3,j} = 010212_3, 120102_3, 021201_3$ for $j = 1,2,3$ respectively. We will prove that

$$0 \le [x+h_{k,1}] + [x+h_{k,2}] + [x+h_{k,3}] + [x] - 3r$$

for every $r = 2k \ge 2$ and $0 \le x \le 3^r - 1$. For $r \le 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. Here $\sum_i u_i$ is always 0, since there are no terms on the left-hand side of the inequality.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
00,01,02,10	2	00,01,02,10	≥ 0	0	0	≥ 0
$ab11, ab12, ab20; ab \ne 20$	2	11,12,20	≥ 2	0	≤ 1	≥ 0
$ab21; ab \ne 20, 21$	2	21	4	0	≤ 1	≥ 2
$ab22; ab \ne 10, 20, 21$	2	22	4	0	≤ 2	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the c_4 corresponding to $\gamma_4 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
2011,2012,2020,2021,2022	4	21	2	≥ 4	4	1	1	0
2121,2122	4	22	2	4	4	1	1	1
1022	4	11	2	2	2	0	1	0

$\square$

Theorem 11.2. *The local system $\mathcal{K} := \mathcal{K}l(\mathbb{1}, \xi_7, \xi_7^2, \xi_7^4)$ in characteristic $p = 3$ has geometric monodromy group $G_{\rm geom} = 2\mathsf{A}_7$. Moreover, it has a descent $\mathcal{K}'$ to $\mathbb{F}_9$ with arithmetic monodromy group $G_{{\rm arith},k} = G_{\rm geom}$ over any finite extension $k \supseteq \mathbb{F}_9$.*

Proof. By Theorem 11.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{K}$. By the construction of $\mathcal{H}$, the field of values

$$\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$$

contains $\sqrt{-7}$. Indeed, for a generator g_0 of the image $I(0)$ in G we have $\varphi(g_0) = (1+\sqrt{-7})/2$ and moreover g_0 has central order 7. Using Corollary 6.2(i) we see that $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$. Now, $\mathcal{K}$ is visibly not Kummer induced, so (being Kloosterman) it is primitive, whence it satisfies (**S**+) by Lemma 3.4.

We have shown that (G,V) satisfies (**S**+), and G contains g_0 with $\bar{\mathsf{o}}(g_0) = 7$. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$, we have that

$$\mathbf{Z}(G) \le C_2. \tag{11.2.1}$$

Furthermore, the image Q of $P(\infty)$ is elementary abelian of order 3^2 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(ii). Suppose G satisfies conclusion (c) of Lemma 3.1. Then G contains an irreducible normal 2-subgroup R, and

$$G/\mathbf{C}_G(R)R \hookrightarrow \mathrm{Out}(R) \hookrightarrow \mathrm{Sp}_4(2) \cong \mathsf{S}_6.$$

But this is a contradiction, since $\mathbf{C}_G(R) = \mathbf{Z}(G) \le C_2$ by (11.2.1), and 7 divides $|G|$ but not $|\mathsf{S}_6|$.

Thus G is almost quasisimple. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 7$ and $|Q| = 3^2$ we have that $3^2 \cdot 7$ divides the order of $G/\mathbf{Z}(G) \le \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to see that

$S = \mathsf{A}_7$ and $L = 2\mathsf{A}_7$. In this case we also have that $\mathbf{Z}(G) = \mathbf{Z}(L) = C_2$ by (11.2.1). Since $7 \nmid |\mathrm{Out}(S)|$, g_0 must lie in the inverse image L of S in G, whence $G_{\mathrm{geom}} = L$ by Theorem 5.1.

By Theorem 7.7, $\mathcal{K}$ has a descent $\mathcal{K}' = \mathcal{K}_{00}$ to $\mathbb{F}_9$ for which any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-7})$ whenever $k \supseteq \mathbb{F}_9$, with $\mathcal{K}_0$ given on line 3 of Table 4. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith}})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{-7})$, we see that

$$\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_2 = \mathbf{Z}(L).$$

Since no outer automorphism of L can fix the character $\varphi|_L$, we conclude that $G_{\mathrm{arith},k} = L = G_{\mathrm{geom}}$. $\square$

Theorem 11.3. *The local system $\mathcal{H}yp(\xi_6 \cdot \mathsf{Char}_7^{\times}; \xi_8, \bar{\xi}_8)$ in characteristic $p = 5$, where ξ_6 is a character of order 6 and ξ_8 a character of order 8, has finite geometric monodromy group.*

Proof. Here the four inequalities to prove are, depending on the choice of ξ_6 and ξ_8:

$$V\left(7x + \frac{1}{6}\right) - V\left(x + \frac{1}{6}\right) + V\left(-x + \frac{1}{8}\right) + V\left(-x - \frac{1}{8}\right) \geq \frac{1}{2},$$

$$V\left(7x - \frac{1}{6}\right) - V\left(x - \frac{1}{6}\right) + V\left(-x + \frac{1}{8}\right) + V\left(-x - \frac{1}{8}\right) \geq \frac{1}{2},$$

$$V\left(7x + \frac{1}{6}\right) - V\left(x + \frac{1}{6}\right) + V\left(-x + \frac{3}{8}\right) + V\left(-x - \frac{3}{8}\right) \geq \frac{1}{2}$$

and

$$V\left(7x - \frac{1}{6}\right) - V\left(x - \frac{1}{6}\right) + V\left(-x + \frac{3}{8}\right) + V\left(-x - \frac{3}{8}\right) \geq \frac{1}{2}.$$

The change of variable $x \mapsto 5x$ interchanges the first and fourth and the second and third inequalities, so we will focus on the second and fourth ones. Using the fact that $V(\frac{i}{24}) = V(\frac{i}{5^4-1}) = \frac{1}{16}[i]$ for $1 \leq i \leq 23$ we check that the inequalities hold for $24x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ for $x \neq 0$, the second inequality is equivalent, via the change of variable $x \mapsto x + \frac{1}{8}$, to

$$V\left(7x + \frac{1}{24}\right) \leq V\left(x + \frac{7}{24}\right) + V\left(x + \frac{1}{4}\right) + V(x) - \frac{1}{2}$$

and, following §9, it suffices to prove

$$\left[7x + \frac{5^r - 1}{24}\right] \leq \left[x + \frac{7(5^r - 1)}{24}\right] + \left[x + \frac{5^r - 1}{4}\right] + [x] - 2r$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. Note that $\frac{7(5^r-1)}{24} = 1212\ldots12_5$ and $\frac{5^r-1}{2} = 1111\ldots11_5$.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
$00,\ldots,32$	2	$00,\ldots,32$	≥ 0	≥ 0	0	≥ 0
$ab33; ab \neq 32$	2	33	8	≥ 0	≤ 1	≥ 4
$a34,\ldots,a44; a \neq 2,3$	2	$34,\ldots,44$	≥ 0	≥ 0	0	≥ 0
$ab34, ab44; ab \leq 31$	4	$ab34, ab44$	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the c_3 corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$
3233,3234,3244	4	33	2	≥ 8	8	10	1	0
3334,3344	4	34	2	≥ 0	0	10	1	1
4234,4244	4	43	2	≥ 4	4	11	1	1
4334,4344	4	44	2	≥ 0	0	11	1	1
40,41	2	34	2	≥ 0	0	10	1	1
42,43	2	44	2	≥ 4	0	11	1	1

For $24x \notin \mathbb{Z}$ the fourth inequality is equivalent, via the change of variable $x \mapsto x + \frac{1}{8}$, to

$$V(7x) \leq V\left(x + \frac{5}{24}\right) + V\left(x + \frac{11}{24}\right) + V(x) - \frac{1}{2}$$

and, following §9, it suffices to prove

$$[7x] \leq \left[x + \frac{5(5^r-1)}{24}\right] + \left[x + \frac{11(5^r-1)}{24}\right] + [x] - 2r$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. Note that $\frac{5(5^r-1)}{24} = 1010\ldots10_5$ and $\frac{11(5^r-1)}{24} = 2121\ldots21_5$; we also denote $\Sigma := \Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	Σ
$00,\ldots,23$	2	$00,\ldots,23$	≥ 0	≥ 0	0	≥ 0
$a24,\ldots,a34; a \neq 3$	2	$24,\ldots,34$	≥ 0	≥ 0	0	≥ 0
$a40,\ldots,a44; a \neq 3,4$	2	$40,\ldots,44$	≥ 0	≥ 0	0	≥ 0
$ab24, ab40, ab42; ab \leq 22$	4	$ab24, ab40, ab42$	≥ 0	≥ 0	0	≥ 0
$a330; a \neq 2$	2	30	0	≥ 1	1	≥ 0
$a334; a \neq 2$	2	34	8	≥ 0	1	≥ 4
04440,14440,24440	4	4440	0	≥ 0	0	≥ 0
034440,134440	6	034440,134440	4	≥ 0	0	≥ 4
044440,144440	6	044440,144440	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the c_3 corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$
2324,2330,2334,2340,2342	4	24	2	≥ 0	0	3	0	1
2440,2442	4	30	2	≥ 0	0	4	0	1
3324,3340,3342	4	34	2	≥ 8	8	10	0	1
3440,3442	4	40	2	≥ 0	0	10	1	1
4324,4340,4342,4442	4	44	2	≥ 4	4	11	1	1
234440	6	24	2	0	0	3	0	1
244440	6	30	2	0	0	4	0	1
334440	6	34	2	8	8	10	0	1
344440	6	40	2	0	0	10	1	1
434440	6	44	2	4	4	11	1	1
444440	6	4440	4	0	0	11	1	1
31,32	2	30	2	0	0	4	0	1
33	2	34	2	12	8	10	0	1
41	2	40	2	0	0	10	1	1
43,44	2	42	2	≥ 4	4	11	1	1

□

Theorem 11.4. *The local system* $\mathcal{H} := \mathcal{H}yp(\xi_6 \cdot \mathsf{Char}_7^\times; \xi_8, \bar{\xi}_8)$ *in characteristic* $p = 5$ *has geometric monodromy group* $G_{\rm geom} = 6\mathsf{A}_7$. *Moreover,* $\mathcal{H}$ *has a descent* $\mathcal{H}'$ *to* $\mathbb{F}_{25}$ *with arithmetic monodromy group* $G_{{\rm arith},k} = G_{\rm geom}$ *over any finite extension* k *of* $\mathbb{F}_{25}$.

Proof. By Theorem 11.3, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to {\rm GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains both ζ_6 and $\sqrt{2}$. Indeed, for a generator g_0 of the image $I(0)$ in G we have $\varphi(g_0) = -\zeta_6$ and moreover g_0^7 acts a central element of order 6. Furthermore, a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has trace 0 on Wild and $\zeta_8 + \bar{\zeta}_8 = \sqrt{2}$ on Tame, whence $\varphi(g_\infty) = \sqrt{2}$. Now using Corollary 6.2(i) we see that $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G, V) satisfies (**S**+). As $D = \dim(V) = 6$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$, but $g_0^7 \in \mathbf{Z}(G)$ has order 6, we have that

$$\mathbf{Z}(G) \cong C_6. \tag{11.4.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for

$$L := E(G) = G^{(\infty)}.$$

Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 7$ we have $C_7 \hookrightarrow G/\mathbf{Z}(G) \leq {\rm Aut}(S)$. Moreover, the image Q of $P(\infty)$ is cyclic of order 5 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

• $(S, L) = ({\rm PSL}_3(4), 6 \cdot {\rm PSL}_3(4))$ or $({\rm PSU}_4(3), 6_1 \cdot {\rm PSU}_4(3))$. In these two cases, $\mathbf{Z}(G) = \mathbf{Z}(L) = C_6$. Next, since $7 \nmid |{\rm Out}(S)|$, the element g_0 of central order 7 must lie in the inverse image L of S in G, whence $G = L$ by Theorem 5.1. Now, using [GAP] we can check that no element of G has trace of absolute value $\sqrt{2}$, contrary to $\varphi(g_\infty) = \sqrt{2}$.

• $(S, L) = ({\rm J}_2, 2 \cdot {\rm J}_2)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, a contradiction.

• $S = \mathsf{A}_7$. Again since $7 \nmid |{\rm Out}(S)|$, g_0 must lie in the inverse image $\mathbf{Z}(G)L$ of S in G, whence $G = \mathbf{Z}(G)L$ by Theorem 5.1. Now, if $L = \mathsf{A}_7$ or $3 \cdot \mathsf{A}_7$, then according to [GAP], no element in

$\mathbf{Z}(G)L$ can have trace $\sqrt{2}$, contradicting the existence of the element g_∞. Hence $L = 6 \cdot A_7$, in which case we have $\mathbf{Z}(G) = \mathbf{Z}(L)$ and $G_{\rm geom} = L = 6\mathsf{A}_7$.

By Theorem 7.7, $\mathcal{H}$ has a descent $\mathcal{H}' = \mathcal{H}_{00}$ to $\mathbb{F}_{25}$, for which any element in $G_{{\rm arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$ when $k \supseteq \mathbb{F}_{25}$, with $\mathcal{H}_0$ given on line 4 of Table 4. Since any element in $\mathbf{C}_{G_{{\rm arith},k}}(L) = \mathbf{Z}(G_{{\rm arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$, we see that $\mathbf{C}_{G_{{\rm arith},k}}(L) = C_6 = \mathbf{Z}(L)$. Since no outer automorphism of L fixes the character $\varphi|_L$, we conclude that $G_{{\rm arith},k} = L = G_{\rm geom}$.

For the next application, we identify g_∞ in G. Since it has central order divisible by 4, it belongs to class $4A$ in $G/\mathbf{Z}(G)$, in the notation of [Atlas]. Also, recall that g_∞ permutes the 4 eigenspaces for Q in Wild cyclically, and has eigenvalues ζ_8 and $\bar\zeta_8$ on Tame. It follows that the central element g_∞^4 acts as a scalar α on Wild for some $\alpha \in \mathbb{C}^\times$, and as the scalar -1 on Tame. This implies that $\alpha = -1$ by Schur's lemma, and thus $\mathsf{o}(g_\infty) = 8$. Now, $G = 6\mathsf{A}_7$ has two classes of elements of order 8, $8a$ and $8b$ in the notation of [GAP], and (modulo the central involution) we may assume g_∞ belongs to class $8a$. □

Theorem 11.5. *The following statements hold.*

(i) *The local system $\mathcal{H}_1 := \mathcal{H}yp(\xi_3 \cdot \mathsf{Char}_7^\times; \mathbb{1}, \xi_2)$ in characteristic $p = 5$ has geometric monodromy group $G_{{\rm geom},\mathcal{H}_1} = 3\mathsf{A}_7$. Moreover, $\mathcal{H}_1 \otimes \mathcal{L}_{\xi_2}$ has a descent $\mathcal{H}_1^\sharp$ to $\mathbb{F}_{25}$ with arithmetic monodromy group $G_{{\rm arith},k,\mathcal{H}_1^\sharp} = G_{{\rm geom},\mathcal{H}_1^\sharp} \cong (3\mathsf{A}_7) \times C_2$ over any finite extension $k \supseteq \mathbb{F}_9$.*

(ii) *The local system $\mathcal{H}_2 := \mathcal{K}l(\mathbb{1}, \xi_7, \xi_7^2, \xi_7^4)$ in characteristic $p = 5$ has geometric monodromy group $G_{{\rm geom},\mathcal{H}_2} = 2\mathsf{A}_7$. Moreover, $\mathcal{H}_2$ has a descent $(\mathcal{H}_2)_{00}$ to $\mathbb{F}_{25}$, with arithmetic monodromy group $G_{{\rm arith},k,(\mathcal{H}_2)_{00}} = G_{\rm geom}$ over any finite extension k of $\mathbb{F}_{25}$.*

Proof. (i) Let $G = 6\mathsf{A}_7$. The hypergeometric sheaf $\mathcal{H}$ in Theorem 11.4 gives rise to a surjection $\phi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow G$, together with a faithful irreducible representation $\Phi : G \to \mathrm{GL}_6(\overline{\mathbb{Q}_\ell})$. We also consider an irreducible representation $\Phi_1 : G \to \mathrm{GL}_6(\overline{\mathbb{Q}_\ell})$ with kernel C_2 and an irreducible representation $\Phi_2 : G \to \mathrm{GL}_4(\overline{\mathbb{Q}_\ell})$ with kernel C_3. Note that, for any p-element $h \in G$,

$$\mathrm{Trace}(\Phi_1(h)) = \mathrm{Trace}(\Phi(h)),\ \mathrm{Trace}(\Phi_2(h)) = \mathrm{Trace}(\Phi(h)) - 2.$$

It follows from [KT5, Theorem 5.1] that $\Phi_i \circ \phi$ gives rise to a hypergeometric sheaf $\mathcal{H}'_i$, of type $(6, 2)$ and with geometric monodromy group $G/C_2 \cong 3\mathsf{A}_7$ if $i = 1$, and of type $(4, 0)$ and with geometric monodromy group $G/C_3 \cong 2\mathsf{A}_7$ if $i = 2$. Furthermore, in the notation of the proof of Theorem 11.4, g_0 is an element of order 42 in G. Changing g_0 to a suitable generator of $\langle g_0 \rangle$, we may assume that the spectrum of $\Phi_1(g_0)$ consists of $\zeta_6\zeta_7^j$, $1 \le j \le 6$, and thus the "upstairs" characters of $\mathcal{H}'_1$ match the "upstairs" characters of $\mathcal{H}_1$. Next, the spectrum of any element of order 8, including g_∞, in Φ_1 consists of single eigenvalues ζ_4 and ζ_4^{-1}, and double eigenvalues 1 and -1. Since g_∞ permutes the 4 eigenspaces for $P(\infty)$ on the wild part of $\mathcal{H}'_1$ cyclically by Proposition 5.8(iii), it must admit eigenvalues 1 and -1 on the tame part Tame of $\mathcal{H}'_1$, and thus the "downstairs" characters of $\mathcal{H}'_1$ match the "downstairs" characters of $\mathcal{H}_1$. Consequently, $\mathcal{H}'_1$ is geometrically isomorphic to $\mathcal{H}_1$, and the statement about $G_{{\rm geom},\mathcal{H}_1}$ is proved.

By Theorem 7.7, $\mathcal{H}_1$ has a descent $(\mathcal{H}_1)_{00}$ to $\mathbb{F}_{25}$ for which any element in $G_{{\rm arith},k,\mathcal{K}_{00}}$ still has trace in $\mathbb{Q}(\sqrt{-3})$ when $k \supseteq \mathbb{F}_{25}$, and with $(\mathcal{H}_1)_0$ given on line 5 of Table 4. Now we take $\mathcal{H}_1^\sharp := (\mathcal{H}_1)_{00} \otimes \mathcal{L}_{\xi_2}$, and note that any element in $G_{{\rm arith},k,\mathcal{H}_1^\sharp}$ has trace in $\mathbb{Q}(\sqrt{-3})$, whence

$$\mathbf{Z}(G_{{\rm arith},k,\mathcal{H}_1^\sharp}) \le C_6. \tag{11.5.1}$$

Let $H := G_{\mathrm{geom},\mathcal{H}_1^\sharp} = G_{\mathrm{geom},\mathcal{H}_1\otimes\mathcal{L}_{\xi_2}}$. Then a generator h_0 of the image of $I(0)$ in H has eigenvalues $-\zeta_3\zeta_7^i$, $1 \le i \le 6$, on $\mathcal{H}_1^\sharp$, whence h_0^7 acts as the scalar $-\zeta_3$ on $\mathcal{H}_1^\sharp$. It now follows from (11.5.1) that

$$\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_1^\sharp}) = \mathbf{Z}(H) = C_6. \tag{11.5.2}$$

By Lemma 5.12, we also have that

$$H/\mathbf{Z}(H) \cong G_{\mathrm{geom},\mathcal{H}_1}/\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_1}) \cong S, \text{ and } H^{(\infty)} \cong (G_{\mathrm{geom},\mathcal{H}_1})^{(\infty)} \cong 3\cdot S, \tag{11.5.3}$$

with $S = \mathsf{A}_7$. It now follow from (11.5.2) that $H = \mathbf{Z}(H)H^{(\infty)} = (3\cdot S)\times C_2$. Now, since no outer automorphism of $H^{(\infty)}$ fixes the equivalence class of the $H^{(\infty)}$-module $\mathcal{H}_1^\sharp$, we conclude from (11.5.2) that $G_{\mathrm{arith},k,\mathcal{H}_1^\sharp} = \mathbf{Z}(H)H^{(\infty)} = H = (3\cdot\mathsf{A}_6)\times C_2$.

(ii) Likewise, changing g_0 to a suitable generator of $\langle g_0\rangle$, we may assume that the spectrum of $\Phi_2(g_0)$ consists of $-1, -\zeta_7, -\zeta_7^2, -\zeta_7^4$. It follows that the Kloosterman sheaf $\mathcal{H}_2'$ is geometrically isomorphic to $\mathcal{K} := \mathcal{K}l(\xi_2, \xi_2\xi_7, \xi_2\xi_7^2, \xi_2\xi_7^4)$, and thus $\mathcal{H}_2 \cong \mathcal{K}\otimes\mathcal{L}_{\xi_2}$. Applying Lemma 5.12 to $H := G_{\mathrm{geom},\mathcal{H}_2}$, we have $H/\mathbf{Z}(H) \cong (G/C_3)/\mathbf{Z}(G/C_3) \cong \mathsf{A}_7$ and

$$H^{(\infty)} \cong (G_{\mathrm{geom},\mathcal{K}})^{(\infty)} = (\Phi_2(G))^{(\infty)} \cong 2\mathsf{A}_7.$$

By Corollary 6.2(i), the field of traces of $\mathcal{H}_2$ is $\mathbb{Q}(\sqrt{-7})$, which implies that $\mathbf{C}_H(H^{(\infty)}) = \mathbf{Z}(H) = C_2 = \mathbf{Z}(H^{(\infty)})$. Also, since outer automorphisms of $2\mathsf{A}_7$ do not preserve the equivalence class of any 4-dimensional irreducible representation of $2\mathsf{A}_7$, H can only induce inner automorphisms of $H^{(\infty)}$. It follows that $H = H^{(\infty)} = 2\mathsf{A}_7$. By Theorem 7.7, $\mathcal{H}_2$ has a descent $(\mathcal{H}_2)_{00}$ to $\mathbb{F}_{25}$, for which any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-7})$ when $k \supseteq \mathbb{F}_{25}$, with $(\mathcal{H}_2)_0$ given on line 6 of Table 4. The statement about $G_{\mathrm{arith},k,(\mathcal{H}_2)_{00}}$ can now be proved using the same arguments as in the proof of Theorem 11.4. □

12. The Mathieu group M_{11}

Theorem 12.1. *Consider the hypergeometric sheaves*

$$\mathcal{H}_1 = \mathcal{H}yp(\mathsf{Char}_{11}^\times; \mathsf{Char}_2),\ \mathcal{H}_2 = \mathcal{H}yp(\xi_2\cdot\mathsf{Char}_{11}^\times; \xi_8, \xi_8^3),\ \mathcal{H}_3 = \mathcal{H}yp(\mathsf{Char}_{11}, \mathsf{Char}_4 \smallsetminus \{\mathbb{1}\})$$

in characteristic $p = 3$. Then each $\mathcal{H}_i$ has a descent $\mathcal{H}_i'$ to $\mathbb{F}_3$, such that, over any finite extension k of $\mathbb{F}_3$, which contains $\mathbb{F}_9$ when $i = 2$, for $\mathcal{H}_i'$ we have that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$, where $G_{\mathrm{geom}} = \mathrm{M}_{11}$ if $i = 1, 3$ and $G_{\mathrm{geom}} = \mathrm{M}_{11}\times C_2$ if $i = 2$.

Proof. (i) First we consider the case $i = 1, 3$. The statement about G_{geom} was proved in [KT5, Lemma 9.5]. As explained in [KT5, Lemma 9.2], the sheaf $\mathcal{H}_1$ is Sawin-like, and so it has a descent to $\mathbb{F}_3$ which is $(1/f)_\star(\overline{\mathbb{Q}_\ell})/\overline{\mathbb{Q}_\ell}$, with $f = x^9(1-x)^2$. Similarly, $\mathcal{H}_3$ is Sawin-like and has a descent to $\mathbb{F}_3$ which is $f_\star(\overline{\mathbb{Q}_\ell})/\overline{\mathbb{Q}_\ell}$, with $f = x^{11}(1-x)$. Moreover, $G_{\mathrm{arith},k}$ is contained in S_n with $n = 11$, respectively $n = 12$, as a subgroup which contains $S := \mathrm{M}_{11}$ as a normal subgroup and which acts irreducibly on the deleted permutation module $S^{(n-1,1)}$ of S_n. The centralizer of S in S_n consists of permutations that act as scalars on the module, hence it is trivial. Since $\mathrm{Aut}(S) = S$, see [GLS, §5.3], it follows that $\mathbf{N}_{\mathsf{S}_n}(S) = S$ and so $G_{\mathrm{arith},k} = S$.

(ii) Consider the case $i = 2$. As shown in [KT5, Lemma 9.5], the sheaf $\mathcal{H}_2\otimes\mathcal{L}_{\xi_2}$ (and after replacing ξ_8 by $\bar{\xi_8}$) has geometric monodromy group $G_{\mathrm{geom},\mathcal{H}_2\otimes\mathcal{L}_{\xi_2}} = S$. Hence $G/\mathbf{Z}(G) = S$ for $G := G_{\mathrm{geom}}$ by Lemma 5.12. Next we note that $\mathcal{H}_2$ has a descent $\mathcal{H}_2' = (\mathcal{H}_2)_{00}$ to $\mathbb{F}_3$ by Theorem 7.5, which has $\mathbb{Q}(\sqrt{-2})$ as the field of traces of elements in $G_{\mathrm{arith},k}$ when $k \supseteq \mathbb{F}_9$, with $(\mathcal{H}_2)_0$ specified in Table 4, line 7. Now $G^{(\infty)}$ is a cover of S, and so $G^{(\infty)} = S$. Next, the centralizer C of S in $G_{\mathrm{arith},k} < \mathrm{GL}_{10}(\mathbb{C})$ consists of scalar transformations, and since $\mathbf{Z}(S) = 1$ and $\mathrm{Aut}(S) = S$, we have that $G_{\mathrm{arith},k} = C\times S$ with $C \le C_2$. Moreover, if g_0 generates the image of $I(0)$ in G, then g_0^{11} acts as the scalar -1 on $\mathcal{H}_2$, whence $g_0^{11} \in C$. Thus $C = C_2$ and $G_{\mathrm{arith},k} = S \times C_2$. Since $g_0^{11} \in C \smallsetminus S$, we see that the normal closure of g_0 contains $C \times S$, and so $G_{\mathrm{geom}} = G_{\mathrm{arith},k}$ by Theorem 5.1. ☐

13. The Mathieu group M_{22}

Theorem 13.1. *The local system $\mathcal{H}yp(\mathsf{Char}_{11}^{\times}; \xi_7, \xi_7^2, \xi_7^4)$ in characteristic 2 has finite geometric monodromy group.*

Proof. For one of the possible choices of characters of order 7, we need to show

$$V(11x) - V(x) + V\left(-x+\frac{1}{7}\right) + V\left(-x+\frac{2}{7}\right) + V\left(-x+\frac{4}{7}\right) - 1 \geq 0$$

Using the fact that $V(\frac{i}{7}) = \frac{1}{3}[i]$ for $i = 1, \ldots, 6$ we get that $V(\frac{i}{7}) = 0, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}$ for $i = 0, 1, \ldots, 6$ respectively, so the inequality holds for $7x \in \mathbb{Z}$. Similarly, using that

$$V(\frac{i}{77}) = V(\frac{13944699i}{2^{30}-1}) = \frac{1}{30}[13944699i]$$

for $i = 1, \ldots, 10$ we check that the inequality holds for $11x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \neq 0$, we can rewrite the inequality as

$$V(11x) \leq V\left(x+\frac{1}{7}\right) + V\left(x+\frac{2}{7}\right) + V\left(x+\frac{4}{7}\right) + V(x) - 1.$$

As described in §9, it suffices to prove

$$[11x] \leq \left[x + \frac{2^r-1}{7}\right] + \left[x + \frac{2(2^r-1)}{7}\right] + \left[x + \frac{4(2^r-1)}{7}\right] + [x] - r$$

for every $r \geq 1$ divisible by $r_0 = 3$ and every $0 \leq x \leq 2^r - 1$. Notice that, in this case, multiplication by 2 permutes $\gamma_1 = \frac{1}{7}$, $\gamma_2 = \frac{2}{7}$ and $\gamma_3 = \frac{4}{7}$ cyclically, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(2^3-1)\gamma_1 = 1 = 001_2$, $h_1 = 1$, $h_2 = h_3 = 0$, $h_{2,j} = 01_2, 00_2, 10_2$ and $h_{3.j} = 001_2, 100_2, 010_2$ for $j = 1, 2, 3$ respectively. For $\gamma_4 = 0$, which is fixed by multiplication by 2, it is clear that $h_4 = h_{r,4} = 0$ for every r. We will prove that

$$[11x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - r$$

for every $r \geq 1$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9. First we prove some cases by splitting off the last digits of x. These cases are enumerated in the following table, depending on the last 2-adic digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
0	1	0	0	0	0	0
01	2	01	0	≥ 0	0	≥ 0
011	3	011	3	≥ 0	0	≥ 3
00111	5	00111	1	≥ 0	0	≥ 1
010111	6	010111	0	≥ 0	0	≥ 0
001111	6	001111	2	≥ 2	0	≥ 2

For the remaining cases, we replace the last digits of x by different digits for which the inequality is already proved, as described at the end of §9. The substitutions are summarized in the following table (we do not include the c_4 corresponding to $\gamma_4 = 0$, since it is always 0):

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1=b'_1$	$c_1=c'_1$	$c_2=c'_2$	$c_3=c'_3$
110111	6	111	3	2	2	1001	1	1	1
101111	6	11	2	5	3	1000	0	1	1
11111	5	1111	4	3	3	1010	1	1	1

For the other possible choice of characters of order 7, we need to show

$$V(11x) - V(x) + V\left(-x-\frac{1}{7}\right) + V\left(-x-\frac{2}{7}\right) - V\left(-x-\frac{4}{7}\right) - 1 \geq 0$$

As in the previous case, we can check manually that the inequality holds for $7x \in \mathbb{Z}$ and $11x \in \mathbb{Z}$. For all other values of x, Using the fact that $V(x)+V(-x)=1$ if $x \neq 0$, we can rewrite the inequality as

$$V(11x) \leq V\left(x+\frac{3}{7}\right) + V\left(x+\frac{6}{7}\right) + V\left(x+\frac{5}{7}\right) + V(x) - 1,$$

and it suffices to prove

$$[11x] \leq \left[x+\frac{3(2^r-1)}{7}\right] + \left[x+\frac{6(2^r-1)}{7}\right] + \left[x+\frac{5(2^r-1)}{7}\right] + [x] - r + 1$$

for every $r \geq 1$ divisible by $r_0 = 3$ and every $0 \leq x \leq 2^r - 1$. Again, multiplication by 2 permutes $\gamma_1 = \frac{3}{7}$, $\gamma_2 = \frac{6}{7}$ and $\gamma_3 = \frac{5}{7}$ cyclically, so we can take $r_1 = 1$. In this case we have $(2^3-1)\gamma_1 = 1 = 011_2$, $h_1 = h_2 = 1$, $h_3 = 0$, $h_{2,j} = 11_2, 01_2, 10_2$ and $h_{3.j} = 011_2, 101_2, 110_2$ for $j = 1,2,3$ respectively. For $\gamma_4 = 0$, $h_4 = h_{r,4} = 0$ for every r. We will prove that

$$[11x] \leq [x+h_{r,1}] + [x+h_{r,2}] + [x+h_{r,3}] + [x] - r + 1$$

for every $r \geq 1$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 7$ we check it by computer. For $r > 7$ we proceed by induction as before, proving first some cases by splitting off the last digits:

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
0	1	0	1	0	0	1
001	3	001	1	≥ 0	0	≥ 0
000101	6	000101	0	0	0	0
10101	2	01	0	≥ 2	2	≥ 0
0001101	7	0001101	2	≥ 0	0	≥ 2
111101	4	1101	2	≥ 0	1	≥ 1
1011	1	1	0	≥ 3	2	≥ 1
111	1	1	0	≥ 1	1	≥ 0

For the remaining cases we apply the following substitutions:

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1=b'_1$	$c_1=c'_1$	$c_2=c'_2$	$c_3=c'_3$
0100101	7	010101	6	-1	-1	11	1	1	0
1100101	7	1101	4	2	2	1000	1	1	1
1001101	7	1001010	7	1	1	110	1	1	1
101101	6	10101	5	0	0	111	1	1	1
011101	6	01101	5	1	1	100	0	1	1
0011	4	0100	4	2	2	10	0	1	0

$\square$

Theorem 13.2. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{11}^{\times}; \xi_7, \xi_7^2, \xi_7^4)$ in characteristic $p = 2$ has geometric monodromy group $G_{\rm geom} = 2\mathrm{M}_{22}$, the double cover of the Mathieu group M_{22}. The sheaf $\mathcal{H}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_2$, such that, over any finite extension k of $\mathbb{F}_4$, $\mathcal{H}'$ has $G_{{\rm arith},k} = G_{\rm geom}$.*

Proof. By Theorem 13.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains $\sqrt{-7}$; indeed, a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has trace $\zeta_7 + \zeta_7^2 + \zeta_7^4 = (-1+\sqrt{-7})/2$ on Tame and 0 on Wild, whence $\varphi(g_\infty) = (-1+\sqrt{-7})/2$. In fact, by Corollary 6.2(i) we have $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 10$, G must be almost quasisimple by Lemma 3.1. Furthermore, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{13.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\bar{\mathsf{o}}(g_0) = 11$ for a generator g_0 of the image of $I(0)$, and $7|\bar{\mathsf{o}}(g_\infty)$, whence both cyclic groups C_{11} and C_7 embed in $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to arrive at the following two possibilities for (S, L).

- $S = \mathsf{A}_{11}$, and $V|_L$ is just the deleted permutation module $S^{(10,1)}|_L$. In this case, since $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = \mathsf{S}_{11}$, the element g_0 of order 11 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G. Using (13.2.1), we see that in fact $g_0 \in S$, hence $G = S$ by Theorem 5.1. But this is a contradiction, since $\mathbb{Q}(\varphi)$ would have been equal to $\mathbb{Q}$.
- $(S, L) = (\mathrm{M}_{22}, 2 \cdot 22)$. Now we have $\mathbf{Z}(G) = \mathbf{Z}(L) = C_2$ by (13.2.1). Furthermore, the element g_0 lies in $L \lhd G$, hence $G_{\rm geom} = L$ by Theorem 5.1.

We now use $\mathcal{H}' = \mathcal{H}_{00}$ as constructed in Theorem 7.5 (where $\mathcal{H}_0$ indicated in Table 4, line 8, has weight 4 in this case), for which the field of traces of elements in $G_{{\rm arith},k}$ is still $\mathbb{Q}(\sqrt{-7})$. Hence, analogously to (13.2.1), we still have $\mathbf{Z}(G_{{\rm arith},k}) = \mathbf{C}_{G_{{\rm arith},k}}(L) = \mathbf{Z}(L) = C_2$. Now, if $G_{{\rm arith},\mathbb{F}_2} = L$ then we are done. Consider the case $G_{{\rm arith},\mathbb{F}_2} > L$. As $G_{{\rm arith},\mathbb{F}_2}/\mathbf{Z}(L)$ embeds in $\mathrm{Aut}(S) = S \cdot 2$, we must then have that $G_{{\rm arith},k} = L \cdot 2 = \langle L, h \rangle$. Thus modulo $L = G_{\rm geom}$, any element in $G_{{\rm arith},k}$ is $h^{\rm deg}$ with $h^2 \in L$. Hence $G_{{\rm arith},k} = L$ when $k \supseteq \mathbb{F}_4$. $\square$

14. The Mathieu group M_{23}

In this section, we work with the hypergeometric sheaf

$$\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{23}^{\times}; \mathbb{1}, \xi_3, \xi_3^2, \xi_5, \xi_5^2, \xi_5^3, \xi_5^4)$$

in characteristic $p = 2$.

Lemma 14.1. *For $f(X) := X^{20}(X-1)^3 \in \mathbb{F}_2[X]$, there exists a geometric isomorphism*

$$\mathcal{H} \cong (1/f)_\star \overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}.$$

Proof. This is a particular case of Sawin's result [KT5, Lemma 9.2 (ii)], applied with $A = 20, B = 3$ in characteristic $p = 2$. $\square$

Theorem 14.2. *The geometric monodromy group $G_{\rm geom}$ of $\mathcal{H}$ is the Mathieu group M_{23} in its 22-dimensional irreducible representation.*

Proof. From the $(1/f)_\star$ description, $G_{\mathrm{geom},\mathcal{H}}$ is a subgroup of the Galois group of the equation

$$X^{20}(X-1)^3 = 1/t,$$

in $\overline{\mathbb{F}_2}(t)[X]$. This Galois group is a subgroup of the symmetric group S_{23}.

We now pass to the Kummer pullback $[23]^\star\mathcal{H}$ and see that

$$G_{\mathrm{geom},[23]^\star\mathcal{H}} \lhd G_{\mathrm{geom},\mathcal{H}}$$

is a normal subgroup (of index dividing 23), which is the Galois group of the polynomial

$$X^{20}(X-1)^3 = 1/t^{23}.$$

Next we show that the Galois group of $X^{20}(X-1)^3 = 1/t^{23}$ is M_{23}, by making use of a result [Abh2, Theorem 2], according to which M_{23} is the Galois group of the equation

$$Y^{23} + tY^3 - 1 = 0$$

in $\overline{\mathbb{F}_2}(t)[Y]$. Since the derivative of this polynomial is $Y^{22} + tY^2$, this equation has 23 distinct roots $\alpha_1, \dots, \alpha_{23}$.

Let us write $K := \overline{\mathbb{F}_2}(t)$, and L/K the Galois extension

$$L := K(\text{all roots } \alpha_i \text{ of } Y^{23} + tY^3 - 1 = 0).$$

Let us denote by $L_0 \subset L$ the subfield

$$L_0 := K(\text{the cubes of the roots of } Y^{23} + tY^3 - 1 = 0).$$

We claim that $L_0 = L$. Indeed, if L_0 were a proper subfield of L, there would exist nontrivial elements $\sigma \in \mathrm{Gal}(L/K)$ which fix the cubes of all roots. But if $\sigma(\alpha_i^3) = \alpha_i^3$, then $\sigma(\alpha_i) = \omega_i\alpha_i$ for some $\omega_i \in \mu_3$. If $\omega_i\alpha_i$ and α_i are both roots of $Y^{23} + tY^3 - 1 = 0$, then as they have the same cubes, we infer that

$$\alpha_i^{23} = (\omega_i\alpha_i)^{23}.$$

As $\alpha_i \neq 0$, this implies that $\omega_i^{23} = 1$. As $\omega_i^3 = 1$, we get $\omega_i = 1$, and hence σ is the identity.

The same argument shows that the 23 cubes α_i^3 are pairwise distinct.

So it suffices to compute the polynomial $f(X)$ satisfied by the 23 cubes of the roots of $Y^{23} + tY^3 - 1 = 0$, or equivalently the polynomial satisfied by the quantities $1/t\alpha_i^3$, $1 \le i \le 23$, for the Galois group of that polynomial will be $\mathrm{Gal}(L/K) = \mathrm{M}_{23}$. We write the equation as

$$Y^{20} = Y^{-3} - t.$$

Thus

$$Y^{60} = (Y^{-3} - t)^3.$$

Write

$$X := 1/(tY^3),$$

so that $Y^{-3} = tX$. Then in terms of X this equation becomes

$$(1/tX)^{20} = (tX - t)^3, \ \text{ i.e. } \ t^{23}X^{20}(X-1)^3 = 1, \ \text{ i.e. } \ X^{20}(X-1)^3 = 1/t^{23}.$$

Since the latter polynomial has degree 23 in X, this must be $f(X)$.

We have shown that $S := \mathrm{M}_{23} = G_{\mathrm{geom},[23]^\star\mathcal{H}} \lhd G_{\mathrm{geom},\mathcal{H}} \le \mathsf{S}_{23}$. Note that $\mathrm{Aut}(\mathrm{M}_{23}) = \mathrm{M}_{23}$ [GLS, §5.3] and $\mathbf{C}_{\mathsf{S}_{23}}(\mathrm{M}_{23}) = 1$. [Indeed, M_{23} is a double transitive subgroup of S_{23}, hence it acts irreducibly on the deleted permutation module of S_{23}, and so its centralizer must act via scalars on the module and therefore must be trivial.] It follows that $\mathbf{N}_{\mathsf{S}_{23}}(\mathrm{M}_{23}) = \mathrm{M}_{23}$ and so $G_{\mathrm{geom},\mathcal{H}} = \mathrm{M}_{23}$. $\square$

Corollary 14.3. *For $f(X) := X^{20}(X-1)^3 \in \mathbb{F}_2[X]$, the lisse sheaf*

$$\mathcal{H}_0 := (1/f)_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$$

on $\mathbb{G}_m/\mathbb{F}_2$ has $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{M}_{23}$.

Proof. We have $\mathrm{M}_{23} = G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} < \mathsf{S}_{23}$, and M_{23} is its own normalizer in S_{23}. ☐

15. The Mathieu group M_{24}

In this section, we consider the hypergeometric sheaf

$$\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{23}; \mathsf{Char}_3^\times)$$

in characteristic $p = 2$.

Lemma 15.1. *For $f(X) := X^{23}(X-1) \in \mathbb{F}_2[X]$, there exists a geometric isomorphism*

$$\mathcal{H} \cong f_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}.$$

Proof. This is a particular case of Sawin's result [KT5, Lemma 9.2 (i)], applied with $A = 23, B = 1$ in characteristic $p = 2$. ☐

Theorem 15.2. *The geometric monodromy group G_{geom} of $\mathcal{H}$ is the Mathieu group M_{24} in its 23-dimensional irreducible representation.*

Proof. Exactly as in the proof of Theorem 14.2, we see that $G_{\mathrm{geom},\mathcal{H}}$ is the Galois group of the equation

$$X^{23}(X-1) = t$$

in $\overline{\mathbb{F}_2}(t)[X]$, and that it is a subgroup of S_{24}. We again pass to the Kummer pullback $[23]^\star\mathcal{H}$ to see that $G_{\mathrm{geom},[23]^\star\mathcal{H}} \lhd G_{\mathrm{geom},\mathcal{H}}$. Now $G_{\mathrm{geom},[23]^\star\mathcal{H}}$ is the Galois group of

$$X^{23}(X-1) = t^{23}.$$

Divide through by t^{23}, and write $Y := X/t$. Then our equation becomes

$$Y^{23}(tY-1) = 1.$$

Now write $Z := 1/Y$. The equation becomes

$$(1/Z)^{23}(t/Z-1) = 1.$$

Multiply through by Z^{24}, the equation becomes

$$t - Z = Z^{24},$$

which Abhyankar and Yie [AY, Theorem (1.1)] proved has Galois group M_{24}. Thus

$$\mathrm{M}_{24} = G_{\mathrm{geom},[23]^\star\mathcal{H}} \lhd G_{\mathrm{geom},\mathcal{H}} \le \mathsf{S}_{24}.$$

As in the proof of Theorem 14.2, we also have $\mathbf{C}_{\mathsf{S}_{24}}(\mathrm{M}_{24}) = 1$ and $\mathrm{Aut}(\mathrm{M}_{24}) = \mathrm{M}_{24}$. It follows that $\mathbf{N}_{\mathsf{S}_{24}}(\mathrm{M}_{24}) = \mathrm{M}_{24}$ and so $G_{\mathrm{geom},\mathcal{H}} = \mathrm{M}_{24}$. ☐

Corollary 15.3. *For $f(X) := X^{23}(X-1) \in \mathbb{F}_2[X]$, the lisse sheaf*

$$\mathcal{H}_0 := f_\star\overline{\mathbb{Q}_\ell}/\overline{\mathbb{Q}_\ell}$$

on $\mathbb{G}_m/\mathbb{F}_2$ has $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{M}_{24}$.

Proof. We have $\mathrm{M}_{24} = G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} < \mathsf{S}_{24}$, and M_{24} is its own normalizer in S_{24}. ☐

16. The MacLaughlin group McL

Theorem 16.1. *The local system $\mathcal{H}(22,5) = \mathcal{H}yp(\mathsf{Char}_{22}; \mathsf{Char}_5^\times)$ in characteristic 3 has finite monodromy.*

Proof. We need to show:

$$V(22x) + V(-5x) - V(-x) \geq 0.$$

Using the fact that $V(\frac{i}{22}) = V(\frac{11i}{3^5-1}) = \frac{1}{10}[11i]$ for $1 \leq i \leq 21$ and that $V(\frac{i}{5}) = V(\frac{16i}{3^4-1}) = \frac{1}{8}[16i]$ we check that the inequality holds for $22x \in \mathbb{Z}$ and for $5x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \neq 0$ and $V(5x) = \sum_{i \bmod 5} V(x + \frac{i}{5}) - 2$ [Ka7, §13], we can rewrite the inequality as

$$V(22x) \leq V\left(x + \frac{1}{5}\right) + V\left(x + \frac{3}{5}\right) + V\left(x + \frac{4}{5}\right) + V\left(x + \frac{2}{5}\right) - 1$$

and, following §9, it suffices to prove

$$[22x] \leq \left[x + \frac{3^r-1}{5}\right] + \left[x + \frac{3(3^r-1)}{5}\right] + \left[x + \frac{4(3^r-1)}{5}\right] + \left[x + \frac{2(3^r-1)}{5}\right] - r + 1$$

for every $r \geq 1$ divisible by $r_0 = 4$ and every $0 \leq x \leq 3^r - 1$. Since multiplication by 3 permutes $\gamma_1 = \frac{1}{5}$, $\gamma_2 = \frac{3}{5}$, $\gamma_3 = \frac{4}{5}$ and $\gamma_4 = \frac{2}{5}$ cyclically modulo 1, we can take $r_1 = 1$. Then, with the notation of §9, we have $(3^4-1)\gamma_1 = 0121_3$; $h_j = 1, 2, 1, 0$; $h_{2,j} = 21_3, 12_3, 01_3, 10_3$ and $h_{3,j} = 121_3, 012_3, 101_3, 210_3$ for $j = 1, 2, 3, 4$ respectively. We will prove that

$$[22x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x + h_{r,4}] - r + 1$$

for every $r \geq 1$ and $0 \leq x \leq 3^r - 1$. For $r \leq 5$ we check it by computer. For $r > 5$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
0	1	0	3	0	0	3
01,21	1	1	1	≥ 0	0	≥ 1
011	2	11	4	≥ 0	0	≥ 4
111	1	1	1	≥ 1	1	≥ 1
0211,2211	2	11	4	≥ 0	1	≥ 2
002,202	2	02	0	≥ 0	0	≥ 0
0102	4	0102	2	≥ 0	0	≥ 2
1102	2	02	0	≥ 1	1	≥ 0
02102,22102	3	102	-1	≥ 2	1	≥ 1
012	2	12	4	≥ 0	0	≥ 4
112,022,222	1	2	-1	≥ 2	1	≥ 1
2212	2	12	4	≥ 0	1	≥ 2
00122,20122	4	0122	2	≥ 1	0	≥ 4
01122	5	01122	5	≥ 0	0	≥ 5
11122,21122	2	22	2	≥ 1	2	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table.

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1=b'_1$	$c_1=c'_1$	$c_2=c'_2$	$c_3=c'_3$	$c_4=c'_4$
1211	4	122	3	4	1	111	0	1	1	1
12102	5	122	3	3	1	111	1	1	1	0
0212	4	022	3	6	3	20	0	0	1	0
1212	4	122	3	4	1	111	0	1	1	1
10122	5	102	3	1	-1	22	0	1	1	0
2122	4	22	2	4	2	201	1	1	1	1

$\square$

Theorem 16.2. *The local system $\mathcal{H}(22,3)=\mathcal{H}yp(\mathsf{Char}_{22};\mathsf{Char}_3^{\times})$ in characteristic 5 has finite monodromy.*

Proof. We need to show:

$$V(22x)+V(-3x)-V(-x)\geq 0.$$

Using the fact that $V(\frac{i}{22})=V(\frac{142i}{5^5-1})=\frac{1}{20}[142i]$ for $1\leq i\leq 21$ and that $V(\frac{i}{3})=V(\frac{8i}{5^2-1})=\frac{1}{8}[8i]$ for $i=1,2$ we check that the inequality holds for $22x\in\mathbb{Z}$ and for $3x\in\mathbb{Z}$. For all other values of x, using that $V(x)+V(-x)=1$ if $x\neq 0$ and $V(3x)=\sum_{i \bmod 3}V(x+\frac{i}{3})-1$ [Ka7, §13], we can rewrite the inequality as

$$V(22x)\leq V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right)$$

and, after a change of variable $x\mapsto x+\frac{2}{3}$, as

$$V\left(22x+\frac{2}{3}\right)\leq V\left(x+\frac{1}{3}\right)+V(x).$$

Following §9, it suffices to prove

$$\left[22x+\frac{2(5^r-1)}{3}\right]\leq\left[x+\frac{5^r-1}{3}\right]+[x]+4$$

for every $r\geq 1$ divisible by $r_0=2$ and every $0\leq x\leq 5^r-1$. For $r\leq 6$ we check it by computer. For $r>6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. Note that $\frac{5^r-1}{3}=1313\ldots13_5$. We also use the notation $\Sigma:=\Delta(s,z)-4\sum_j v_j+4\sum_i u_i$.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	Σ
$00,\ldots,31$	2	$00,\ldots,31$	≥ 0	≥ 0	0	≥ 0
$x32,\ldots,x44$, $x\neq 1$	2	$32,\ldots,44$	≥ 0	≥ 0	0	≥ 0
$x132,\ldots,x144$, $x\neq 3,4$	4	$x132,\ldots,x144$	≥ 0	≥ 0	0	≥ 0
04132,24132,34132,44132	4	4132	-4	≥ 1	0	≥ 0
014132,114132,214132	6	014132,114132,214132	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the c_2 corresponding to $\gamma_2=0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$
$3132,\ldots,3144$	4	32	2	≥ 0	0	30	1
314132	6	3133	4	0	0	30	1
414132	6	4133	4	-4	-4	34	1
$4133,\ldots,4144$	4	4132	4	≥ -4	-4	34	1

$\square$

Theorem 16.3. *Each of the two hypergeometric sheaves $\mathcal{H}(22,3) = \mathcal{H}yp(\mathsf{Char}_{22}; \mathsf{Char}_3^\times)$ in characteristic $p = 5$ and $\mathcal{H}(22,5) = \mathcal{H}yp(\mathsf{Char}_{22}; \mathsf{Char}_5^\times)$ in characteristic $p = 3$ has geometric monodromy group $G_{\mathrm{geom}} = \mathrm{McL}\cdot 2$, the full automorphism group of the MacLaughlin sporadic simple group* McL*. Each of these sheaves $\mathcal{H}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_p$, such that, over any finite extension k of $\mathbb{F}_{p^2}$, $\mathcal{H}'$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.*

Proof. (i) By Theorems 16.1 and 16.2, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G,V) satisfies ($\mathbf{S}+$). As $D = \dim(V) = 22$, G must be almost quasisimple by Lemma 3.1.

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma, and furthermore $\mathbf{Z}(G) \leq C_2$ since $\mathbb{Q}(\varphi) = \mathbb{Q}$. Furthermore, $\bar{\mathsf{o}}(g_0) = 22$ for a generator g_0 of the image of $I(0)$, whence 22 divides the order of $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. If $p = 3$, then $\dim \mathsf{Wild} = 18$, and so the image Q of $P(\infty)$ must admit an irreducible complex representation of dimension 9, whence 3^5 divides $|Q|$, and so also divides $|G/\mathbf{Z}(G)|$ by Proposition 5.6(i). Likewise, if $p = 5$, then $\dim \mathsf{Wild} = 20$, and so the image Q of $P(\infty)$ must admit an irreducible complex representation of dimension 5, whence 5^3 divides $|Q|$, and so also divides $|G/\mathbf{Z}(G)|$.

In the case $p = 3$, by Proposition 5.8, a p'-generator g_∞ must interchange the two simple $P(\infty)$-submodules in Wild, each of dimension 9, and there is some root of unity ζ such that the spectrum of g_∞^2 on each summand is $\zeta \cdot (\mu_{10} \smallsetminus \{1\})$. Besides, g_∞ has all four nontrivial 5th roots of unity as eigenvalues on Tame. It follows that $20|\bar{\mathsf{o}}(g_\infty)$. Next, if we write $\mathsf{o}(\zeta) = 2^b \cdot m$ with $a \in \mathbb{Z}_{\geq 0}$ and $2 \nmid m$, then $\Phi(g_\infty^{2^{b+2}})$ has spectrum

$$\underbrace{\beta \cdot (\mu_5 \smallsetminus \{1\})}_{4 \text{ times}},\ \beta, \beta, \mu_5 \smallsetminus \{1\},$$

where $\beta := \zeta^{2^{b+1}}$ has odd order m. It follows that

$$\varphi(g_\infty^{2^{b+2}}) = -1 - 2\beta. \tag{16.3.1}$$

Now we can apply the main result of [HM] to arrive at the following possibilities for (S,L).

- $S = \mathrm{PSL}_2(23)$, PSL_{43}, or M_{23}. This is impossible, since $\mathrm{Aut}(S) = \mathrm{PGL}_2(23)$, $\mathrm{PGL}_2(43)$, or M_{23} does not have order divisible by 3^5 or 5^3.
- $S = \mathrm{HS}$. This case is ruled by [KT5, Lemma 9.7].
- $S = \mathrm{PSU}_6(2)$. Since 5^3 does not divide $|\mathrm{Aut}(S)|$, we must have that $p = 3$. In the latter case, as $20|\bar{\mathsf{o}}(g_\infty)$, C_{20} embeds in $\mathrm{Aut}(S)$, which is impossible.
- $S = L = \mathsf{A}_{23}$, and $V|_L$ is just the deleted permutation module $S^{(22,1)}|_L$. In this case, the Sylow 5-subgroups of $\mathrm{Aut}(S) = \mathsf{S}_{23}$ are elementary abelian of order 5^4. Now if $p = 5$, then by Proposition

5.6(i), Q embeds in $\mathrm{Aut}(S)$ and so is abelian, contradicting $\dim \mathsf{Wild} = 20$. Hence $p = 3$. As $\mathbf{Z}(G) \leq C_2$ and $\mathrm{Aut}(S)/S \cong C_2$, the element $g_\infty^{2^{b+2}}$ must belong to $\mathbf{O}^2(G) = S = \mathsf{A}_{23}$, and so $\varphi(g_\infty^{2^{b+2}})$, the trace of $g_\infty^{2^{b+2}}$ on $S^{(22,1)}$, must be an integer ≥ -1. By (16.3.1), this means that the root of unity β satisfies $\beta \in \mathbb{Z}_{\leq 0}$. But this is impossible, since $\mathsf{o}(\beta) = m$ is odd.

- $S = L = \mathrm{McL}$. Since $\mathrm{meo}(S) = 11$ but $\bar{\mathsf{o}}(g_0) = 22$, we must have that

$$G/\mathbf{Z}(G) \cong \mathrm{Aut}(S) = S \cdot C_2.$$

If $\mathbf{Z}(G) = 1$, then $G \cong \mathrm{McL} \cdot 2$ as stated. Otherwise we have $\mathbf{Z}(G) = C_2$, and $S = \mathbf{O}^2(G)$. In this case, S contains the p-subgroup Q, and so G/S is cyclic by Theorem 5.3, of order 4. Recall [Atlas] that $\mathrm{Aut}(S)$ is a split extension of S by C_2. Hence we can find an element $x \in G$ such that x^2, but not x, centralizes S; say x induces the outer automorphism x_0 of S of class $2b$ in the notation of [GAP]. If $x^2 = 1$, then $\langle S, x\rangle \cong \mathrm{Aut}(S)$ and $\mathbf{Z}(G) \cap \langle S, x\rangle = 1$, whence $G = \mathbf{Z}(G) \times \langle S, x\rangle$ and $G/S \cong C_2^2$, a contradiction. Thus $1 \neq x^2 \in \mathbf{C}_G(S) = \mathbf{Z}(G)$, whence $\Phi(x^2) = -\mathrm{Id}$.

Consider an extension of $\Phi|_S$ to $\mathrm{Aut}(S)$ which we also denote by Φ. Since x and x_0 induce the same automorphism on S, $\Phi(x) = \alpha\Phi(x_0)$ for some $\alpha \in \mathbb{C}^\times$. As $\mathsf{o}(x_0) = 2$, we then have

$$-\mathrm{Id} = \Phi(x^2) = \alpha^2\Phi(x_0^2) = \alpha^2 \cdot \mathrm{Id},$$

whence $\alpha = \pm i$. The coset Sx_0 also contains an element sx_0 that belongs to class $4b$ in the notation of [GAP], for some $s \in S$, and $\mathrm{Tr}(\Phi(sx_0)) = \pm 4$ (see [GAP]). It follows that

$$\varphi(sx) = \mathrm{Tr}(\Phi(sx)) = \mathrm{Tr}(\Phi(s)\Phi(x)) = \alpha\mathrm{Tr}(\Phi(s)\Phi(x_0)) = \alpha\mathrm{Tr}(\Phi(sx_0)) = \pm 4i,$$

with $sx \in G$, contradicting $\mathbb{Q}(\varphi) = \mathbb{Q}$.

(ii) We use $\mathcal{H}' = \mathcal{H}_{00}$ as constructed in Theorem 7.5 (with $\mathcal{H}_0$ given in Table 4, lines 9 and 10), for which, over any finite extension k of $\mathbb{F}_{p^2}$, the field of traces of elements in $G_{\mathrm{arith},k}$ is still $\mathbb{Q}$, and so we still have

$$\mathbf{Z}(G_{\mathrm{arith},k}) = \mathbf{C}_{G_{\mathrm{arith},k}}(S) \leq C_2.$$

Now, if $G_{\mathrm{arith},\mathbb{F}_p} = G_{\mathrm{geom}}$ then we are done. Consider the case where $G_{\mathrm{arith},\mathbb{F}_p} > G_{\mathrm{geom}}$. As $G_{\mathrm{arith},\mathbb{F}_p}/\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_p})$ embeds in $\mathrm{Aut}(S) = S \cdot 2 \cong G_{\mathrm{geom}}$, we must then have that $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_p}) = C_2$ and $G_{\mathrm{arith},\mathbb{F}_p} = \langle G_{\mathrm{geom}}, h\rangle$ with $h^2 \in G_{\mathrm{geom}}$. Thus modulo G_{geom}, any element in $G_{\mathrm{arith},k}$ is $h^{\deg/\mathbb{F}_p}$. Hence $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ when $k \supseteq \mathbb{F}_{p^2}$. □

17. The Janko group J_2

Theorem 17.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{28} \smallsetminus \mathsf{Char}_{14}; \xi_8, \bar{\xi}_8)$ in characteristic $p = 5$ has finite geometric monodromy group.*

Proof. We need to show that

$$V(28x) - V(14x) + V\left(-x + \frac{1}{8}\right) + V\left(-x - \frac{1}{8}\right) \geq \frac{1}{2}$$

or

$$V(28x) - V(14x) + V\left(-x + \frac{3}{8}\right) + V\left(-x - \frac{3}{8}\right) \geq \frac{1}{2}$$

depending on the choice of χ. These inequalities are equivalent via the change of variable $x \mapsto 5x$, so it suffices to prove the first one. Using the fact that

$$V(\frac{i}{56}) = V(\frac{279i}{5^6 - 1}) = \frac{1}{24}[279i]$$

for $1 \leq i \leq 55$, we check that the inequality holds for $28x \in \mathbb{Z}$ and for $8x \in \mathbb{Z}$. For all other values of x, using that $V(x)+V(-x) = 1$ if $x \neq 0$ and $V(28x) = V(14x)+V(14x+\frac{1}{2})-\frac{1}{2}$ [Ka7, §13], we can rewrite the inequality via the change of variable $x \mapsto x+\frac{1}{8}$ as

$$V\left(14x+\frac{1}{4}\right) \leq V\left(x+\frac{1}{4}\right)+V(x)$$

and, following §9, it suffices to prove

$$\left[14x+\frac{5^r-1}{4}\right] \leq \left[x+\frac{5^r-1}{4}\right]+[x]$$

for every $r \geq 1$ and every $0 \leq x \leq 5^r-1$. For $r \leq 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-4\sum_j v_j+4\sum_i u_i$
0,1,2,3	1	0,1,2,3	0	≥ 0	0	≥ 0
04,14,24,44	1	4	0	≥ 0	0	≥ 0
034,134,234	3	034,134,234	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c_2'$ corresponding to $\gamma_2 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$
334	3	34	2	0	0	20	1
434	3	44	2	0	0	23	1

□

Theorem 17.2. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{28} \smallsetminus \mathsf{Char}_{14}; \xi_8, \bar{\xi}_8)$ in characteristic $p = 5$ has geometric monodromy group $G_{\rm geom} = 2\mathrm{J}_2{\cdot}2$. Furthermore, $\mathcal{H}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_{25}$ with arithmetic monodromy group $G_{{\rm arith},k} = G_{\rm geom}$ over any finite extension k of $\mathbb{F}_{25}$.*

Proof. By Theorem 17.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains $\sqrt{2}$; indeed, a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has trace $\zeta_8+\bar{\zeta}_8 = \sqrt{2}$ on Tame and 0 on Wild, whence $\varphi(g_\infty) = \sqrt{2}$. In fact, by Corollary 6.2(i) we have $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{2})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G,V) satisfies (**S**+). As $D = \dim(V) = 14$, G must be almost quasisimple by Lemma 3.1. Furthermore, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{2})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \qquad (17.2.1)$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\mathsf{o}(g_0) = 14$ for a generator g_0 of the image of $I(0)$, whence $C_{14} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is elementary abelian of order 25 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S,L).

• $S = L = \mathsf{A}_{15}$, and $V|_L$ is just the deleted permutation module $S^{(14,1)}|_L$. In this case, $\mathbb{Q}(\varphi)$ would have been equal to $\mathbb{Q}$ by Lemma 3.8, a contradiction.

• $S = L = \mathrm{J}_2$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, again a contradiction.

• $(S, L) = (\mathrm{J}_2, 2 \cdot \mathrm{J}_2)$. Now we have $\mathbf{Z}(G) = \mathbf{Z}(L) = \mathbf{C}_G(L) = C_2$ by (17.2.1). Furthermore, the element g_0 of central order 14 does not lie in $L \lhd G$, hence $G > L$. Now

$$S \cong L/\mathbf{Z}(L) < G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 2,$$

and we conclude that $G_{\rm geom} = 2\mathrm{J}_2 \cdot 2$.

By Theorem 7.7, $\mathcal{H}$ has a descent $\mathcal{H}' = \mathcal{H}_{00}$ to $\mathbb{F}_{25}$ for which any element in $G_{{\rm arith},k}$ still has trace in $\mathbb{Q}(\sqrt{2})$ when $k \supseteq \mathbb{F}_{25}$, with $\mathcal{H}_0$ given on line 11 of Table 4. Since any element in $\mathbf{C}_{G_{{\rm arith},k}}(L) = \mathbf{Z}(G_{{\rm arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{2})$, we see that

$$\mathbf{C}_{G_{{\rm arith},k}}(L) = C_2 = \mathbf{Z}(L).$$

Since $G_{\rm geom}$ already induces the full automorphism group $\mathrm{J}_2 \cdot 2$ of L, we conclude that $G_{{\rm arith},k} = G_{\rm geom}$. $\square$

Theorem 17.3. *The local system* $\mathcal{K} := \mathcal{K}l(\mathsf{Char}_{12}^{\times} \sqcup \mathsf{Char}_{3}^{\times}\})$ *in characteristic* $p = 5$ *has finite monodromy.*

Proof. We need to show:

$$V\left(x+\frac{1}{12}\right)+V\left(x+\frac{5}{12}\right)+V\left(x+\frac{7}{12}\right)+V\left(x+\frac{11}{12}\right)+V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right) \geq \frac{5}{2}.$$

Following §9, it suffices to prove

$$0 \leq \left[x+\frac{5^r-1}{12}\right]+\left[x+\frac{5(5^r-1)}{12}\right]+\left[x+\frac{7(5^r-1)}{12}\right]+$$
$$+\left[x+\frac{11(5^r-1)}{12}\right]++\left[x+\frac{5^r-1}{3}\right]+\left[x+\frac{2(5^r-1)}{3}\right]-10r$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 5^r - 1$. Notice that, in this case, multiplication by 5 permutes $\gamma_1 = \frac{1}{12}$ and $\gamma_2 = \frac{5}{12}$, $\gamma_3 = \frac{7}{12}$ and $\gamma_4 = 1112$; and $\gamma_5 = \frac{1}{3}$ and $\gamma_6 = \frac{2}{3}$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2-1)\gamma_1 = 02_5$, $(5^2-1)\gamma_3 = 24_5$, $(5^2-1)\gamma_5 = 13_5$, $h_j = 2, 0, 4, 2, 3, 1$ and $h_{2,j} = 02_5, 20_5, 24_5, 42_5, 13_5, 31_5$ for $j = 1, \ldots, 6$ respectively. We will prove that

$$0 \leq [x+h_{r,1}]+[x+h_{r,2}]+[x+h_{r,3}]+[x+h_{r,4}]+[x+h_{r,5}]+[x+h_{r,6}]-12r$$

for every $r \geq 1$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. We don't write the $\sum u_i$ since there are none in this case.

last digits of x	s	z	$\Delta(s,z)$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j$
0	1	0	2	0	≥ 2
$a1; a \neq 2$	1	1	4	0	≥ 4
$a21; a \neq 0$	1	1	4	1	≥ 0
$a2; a \neq 2, 3$	1	2	6	0	≥ 6
$a22; a \neq 0$	1	2	6	1	≥ 2
$a32; a \neq 1$	1	2	6	1	≥ 2
13	1	3	4	0	≥ 4
$ab3; ab \neq 02, 13, 20, 24$	1	4	6	1	≥ 2
1203,4203	3	203	4	0	≥ 4
$a133; a \neq 3$	2	33	4	1	≥ 0
$ab4; ab \neq 02, 13, 20, 24, 31$	1	3	4	1	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$c_1=c'_1$	$c_2=c'_2$	$c_3=c'_3$	$c_4=c'_4$	$c_5=c'_5$	$c_6=c'_6$
021,022,023,024	3	03	2	≥ 4	2	0	0	1	0	0	0
132,134	3	14	2	6	6	0	0	1	0	1	0
3133,3203,3243	4	333	3	4	4	0	1	1	1	1	1
0203,0243	4	033	3	2	2	0	0	0	1	0	0
2203	4	204	3	6	6	0	0	1	1	0	1
1243	4	103	3	8	6	0	0	0	1	0	0
2243	4	233	3	6	6	0	0	1	1	0	1
4243	4	433	3	6	6	1	1	1	1	1	1
204	3	21	2	6	6	0	0	1	1	0	1
244	3	3	1	6	4	0	1	1	1	0	1
314	3	32	2	6	6	0	1	1	1	1	1

□

Theorem 17.4. *The local system $\mathcal{K} := \mathcal{K}l(\mathsf{Char}_{12}^{\times} \sqcup \mathsf{Char}_3^{\times})$ in characteristic $p=5$ has $G_{\mathrm{geom}} = 2{\cdot}\mathrm{J}_2$. Furthermore, $\mathcal{K}$ has a descent $\mathcal{K}'$ to $\mathbb{F}_p$, which over any extension k of $\mathbb{F}_p$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.*

Proof. Because $\mathcal{K}$ is Kloosterman, it is not Belyi induced, and it is visibly not Kummer induced. Hence, it is $(\mathbf{S}+)$ by Theorem 3.3. By Theorem 17.3, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{K}$. By the construction of $\mathcal{H}$ and Corollary 6.2(ii), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}(\sqrt{5})$. Moreover, the representation is symplectic by [Ka4, 8.8.2], and

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{17.4.1}$$

As $\dim(V) = 6$, G is almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma, and furthermore $\mathbf{Z}(G) \leq C_2$ by (25.5.1). Moreover, the image Q of $P(\infty)$ is elementary abelian of order 25 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to see that $S = \mathrm{J}_2$ and $L = 2 \cdot S$; in particular, $\mathbf{Z}(G) = \mathbf{Z}(L) = C_2$ by (17.4.1). Note that $\varphi|_L$ is not fixed by any outer automorphism of L. Hence $G = L$.

A descent $\mathcal{K}'$ of $\mathcal{K}$ over $\mathbb{F}_p$ is constructed using Theorem 7.5(i), and listed on line 39 in Table 4. By Theorem 7.5(iii), the field of traces is still $\mathbb{Q}(\sqrt{5})$; hence (17.4.1) also holds for $G_{\mathrm{arith},k}$. Thus $\mathbf{Z}(G_{\mathrm{arith},k}) = C_2 = \mathbf{Z}(G_{\mathrm{geom}})$ over any extension k of $\mathbb{F}_p$. Since $\varphi|_L$ is not invariant under any automorphism of L, we conclude that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. □

18. The Janko group J_3

In this section, let $\mathcal{H} := \mathcal{H}yp(\xi_3 \cdot \mathsf{Char}_{19}^{\times}; \mathbb{1}, \xi_5, \bar{\xi}_5)$ be the hypergeometric sheaf in characteristic $p=2$, with 18 "upstairs" characters $\xi_3 \cdot \mathsf{Char}_{19}^{\times}$, and 3 "downstairs" characters $\mathbb{1}$, ξ_5, and $\bar{\xi}_5$.

Theorem 18.1. *The hypergeometric sheaf $\mathcal{H} = \mathcal{H}yp(\xi_3 \cdot \mathsf{Char}_{19}^{\times}; \mathbb{1}, \xi_5, \bar{\xi}_5)$ in characteristic $p=2$ has finite geometric monodromy group G_{geom}.*

Proof. We need to show:

$$V\left(19x + \frac{1}{3}\right) - V\left(x + \frac{1}{3}\right) + V(-x) + V\left(-x - \frac{1}{5}\right) + V\left(-x + \frac{1}{5}\right) \geq 1,$$

$$V\left(19x-\frac{1}{3}\right)-V\left(x-\frac{1}{3}\right)+V(-x)+V\left(-x-\frac{1}{5}\right)+V\left(-x+\frac{1}{5}\right)\geq 1,$$
$$V\left(19x+\frac{1}{3}\right)-V\left(x+\frac{1}{3}\right)+V(-x)+V\left(-x-\frac{2}{5}\right)+V\left(-x+\frac{2}{5}\right)\geq 1$$

and

$$V\left(19x-\frac{1}{3}\right)-V\left(x-\frac{1}{3}\right)+V(-x)+V\left(-x-\frac{2}{5}\right)+V\left(-x+\frac{2}{5}\right)\geq 1.$$

The change of variable $x\mapsto 2x$ interchanges the first and fourth and the second and third inequalities, so it suffices to prove the last two. Using the fact that $V(\frac{i}{15})=V(\frac{i}{2^4-1})=\frac{1}{4}[i]$ for $1\leq i\leq 14$ we check that the inequalities hold for $3x\in\mathbb{Z}$ and for $5x\in\mathbb{Z}$. For all other values of x, using that $V(x)+V(-x)=1$ if $x\neq 0$ we can rewrite the fourth inequality as

$$V\left(19x+\frac{1}{3}\right)\leq V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{5}\right)+V\left(x-\frac{2}{5}\right)+V(x)-1$$

and, via the change of variable $x\mapsto x+\frac{2}{3}$, this is equivalent to

$$V(19x)\leq V\left(x+\frac{2}{3}\right)+V\left(x+\frac{1}{15}\right)+V\left(x+\frac{4}{15}\right)+V(x)-1.$$

Following §9, it suffices to prove

$$[19x]\leq\left[x+\frac{2(2^r-1)}{3}\right]+\left[x+\frac{2^r-1}{15}\right]+\left[x+\frac{4(2^r-1)}{15}\right]+[x]-r$$

for every $r\geq 1$ divisible by $r_0=4$ and every $0\leq x\leq 2^r-1$. Notice that, in this case, multiplication by 2^2 fixes $\gamma_1=\frac{2}{3}$ and $\gamma_4=0$ and permutes $\gamma_2=\frac{1}{15}$ and $\gamma_3=\frac{4}{15}$, so we can take $r_1=2$. Then, with the notation of §9, we have $(2^4-1)\gamma_1=1010_2$, $(2^4-1)\gamma_2=0001_2$, $h_1=10_2$, $h_2=01_2$, $h_3=00_2$ and $h_{2,j}=1010_2,0001_2,0100_2$ for $j=1,2,3$ respectively. For $\gamma_4=0$ it is clear that $h_4=h_{r,4}=0$ for every r. We will prove that

$$[19x]\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x]-r$$

for every $r=2k\geq 1$ and every $0\leq x\leq 2^r-1$. For $r\leq 10$ we check it by computer. For $r>10$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-\sum_j v_j+\sum_i u_i$
00,01	2	00,01	0	≥ 0	0	≥ 0
010,011	2	11	1	≥ 0	0	≥ 1
1110	2	10	0	≥ 1	1	≥ 0
00110,00111	4	0110,0111	≥ 0	≥ 0	0	≥ 0
0010111	6	010111	0	≥ 0	0	≥ 0
011010111	8	11010111	0	≥ 0	0	≥ 0
110111	4	0111	2	≥ 0	1	≥ 1
001111	4	1111	2	≥ 0	1	≥ 1
0101111	6	101111	0	≥ 0	0	≥ 0
111111	2	11	1	≥ 2	3	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4=c'_4$ corresponding to $\gamma_4=0$, since it is always 0):

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1=b'_1$	$c_1=c'_1$	$c_2=c'_2$	$c_3=c'_3$
01010111	8	010111	6	0	0	110	1	0	0
0111010111	10	01110010	8	2	2	1000	1	0	0
1111010111	10	11111000	8	4	4	10010	1	1	1
010110	6	010111	6	1	0	110	1	0	0
110110	6	1110	4	6	4	10000	1	1	0
01101111	8	011100	6	2	2	1000	1	0	0
11101111	8	111100	6	2	2	10001	1	1	1
011111	6	1000	4	2	0	1001	1	0	0

The third inequality can be rewritten as

$$V\left(19x+\frac{2}{3}\right)\leq V\left(x+\frac{2}{3}\right)+V\left(x+\frac{2}{5}\right)+V\left(x+\frac{3}{5}\right)+V(x)-1$$

and following §9, it suffices to prove

$$\left[19x+\frac{2(2^r-1)}{3}\right]\leq\left[x+\frac{2(2^r-1)}{3}\right]+\left[x+\frac{2(2^r-1)}{5}\right]+\left[x+\frac{3(2^r-1)}{5}\right]+[x]-r+1$$

for every $r\geq 1$ divisible by $r_0=4$ and every $0\leq x\leq 2^r-1$. Notice that, in this case, multiplication by 2^2 fixes $\gamma_1=\frac{2}{3}$ and $\gamma_4=0$ and permutes $\gamma_2=\frac{2}{5}$ and $\gamma_3=\frac{3}{5}$, so we can take $r_1=2$. Then, with the notation of §9, we have $(2^4-1)\gamma_1=1010_2, (2^4-1)\gamma_2=0110_2$, $h_1=h_2=10_2$, $h_3=01_2$ and $h_{2,j}=1010_2, 0110_2, 1001_2$ for $j=1,2,3$ respectively. For $\gamma_4=0$ it is clear that $h_4=h_{r,4}=0$ for every r. We will prove that

$$\left[19x+\frac{2(2^r-1)}{3}\right]\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x]-r+1$$

for every $r=2k\geq 1$ and every $0\leq x\leq 2^r-1$. For $r\leq 8$ we check it by computer. For $r>8$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. In fact, we will prove the following sharper inequality:

$$\left[19x+\frac{2(2^r-1)}{3}\right]\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x]-r$$

whenever, if we split the r digits of x in k blocks of 2, the last block different from 00 is not 11. If we split x as p^sy+z then, for the induction step to work in the proof of the sharper inequality, we need $\Delta(s,z)-\sum_j v_j+\sum_i u_i\geq 1$ instead of 0 if the last two-digit block of y different from 00 is 11, unless the same is true for z (or $z=0$). Moreover, if the last two-digit block of z different from 00 is 11 but it is not the case for y, then it suffices with $\Delta(s,z)-\sum_j v_j+\sum_i u_i\geq -1$.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
00	2	00	0	0	0	≥ 0
01	2	01	1	≥ 0	0	≥ 1
0010	4	0010	1	≥ 0	0	≥ 1
000110	6	000110	2	≥ 0	0	≥ 2
100110	4	0110	0	≥ 0	0	≥ 0
110110	4	0110	0	≥ 3	1	≥ 2
01001010,10001010	6	001010	0	≥ 0	0	≥ 0
00001010,00111010	8	00001010,00111010	1	≥ 0	0	≥ 1
11001010,1111010	4	1010	1	2	≤ 2	≥ 1
1110	2	10	1	≥ 1	1	≥ 1
0011,1111	2	11	0	≥ 3	≤ 2	≥ 1
00000111,01000111	8	00000111,01000111	0	≥ 0	0	≥ 0
10000111	6	000111	-1	0	0	≥ -1
11000111	6	000111	-1	≥ 1	0	≥ 0
00110111	8	00110111	1	≥ 0	0	≥ 1
11110111	6	110111	2	≥ 0	2	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4 = c_4'$ corresponding to $\gamma_4 = 0$, since it is always 0). Here, in order to prove the sharper inequality, if the last two-digit block of z different from 00 is 11 but that of z' is not 11, we need $\Delta(s', z') \leq \Delta(s, z) + 1$. If the last two-digit block of z' different from 00 is 11 but that of z is not 11, we need $\Delta(s', z') \leq \Delta(s, z) - 1$.

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
010110	6	0110	4	2	0	111	1	0	0
011010	6	0111	4	1	0	1000	1	1	0
101010	6	1011	4	1	0	1101	1	1	1
10111010	8	110000	6	1	0	1110	1	1	1
010111	6	011000	6	-1	0	111	1	0	0
100111	6	1010	4	0	1	1100	1	1	1
01110111	8	01111010	8	0	1	1001	1	0	1
10110111	8	10111010	8	1	1	1110	1	1	1
001011	6	001010	6	-1	0	11	0	0	0
011011	6	011100	6	1	0	1000	1	1	0
101011	6	101100	6	0	0	1101	1	1	1
111011	6	111100	6	4	3	10010	1	1	1

$\square$

Theorem 18.2. *The hypergeometric sheaf* $\mathcal{H} = \mathcal{H}yp(\xi_3 \cdot \mathsf{Char}_{19}^{\times}; \mathbb{1}, \xi_5, \bar{\xi}_5)$ *in characteristic* $p = 2$ *has geometric monodromy group* $G_{\mathrm{geom}} = 3 \cdot \mathrm{J}_3$*, the triple cover of the third Janko sporadic simple group* J_3*. Conversely, if* $\mathcal{H}'$ *is an irreducible hypergeometric sheaf in some characteristic* r *with finite geometric monodromy group* H *which is almost quasisimple with* $S = \mathrm{J}_3$ *as its non-abelian composition factor, then* $\mathrm{rank}(\mathcal{H}') = 18$*,* $r = 2$*, and the* 18 *"upstairs" characters of* $\mathcal{H}'$ *are* $\chi \cdot \mathsf{Char}_{19}^{\times}$ *for some multiplicative character* χ*.*

Proof. (i) By Theorem 18.1, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}(\sqrt{5}, \zeta_3)$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 18$, G must be almost quasisimple by Lemma 3.1.

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\bar{\mathsf{o}}(g_0) = 19$ for a generator g_0 of the image of $I(0)$, and $5|\bar{\mathsf{o}}(g_\infty)$ for a p'-element g_∞ that generates $I(\infty)$ modulo $P(\infty)$, whence $19 \cdot 5$ divides the order of $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = L = \mathsf{A}_{19}$, and $V|_L$ is just the deleted permutation module $S^{(18,1)}|_L$. In this case, $\mathbb{Q}(\varphi)$ must be $\mathbb{Q}(\zeta_3)$ by Lemma 3.8, which is a contradiction since $\sqrt{5} \in \mathbb{Q}(\varphi)$.
- $S = \mathrm{PSL}_2(19)$. Since $p = 2$ and $\dim \mathsf{Wild} = 15$, by Proposition 5.8(iv) the image Q of $P(\infty)$ in G is an elementary abelian 2-group of order 2^4; furthermore, $Q \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. This is impossible, since $\mathrm{Aut}(S) = \mathrm{PGL}_2(19)$.
- $(S, L) = (\mathrm{J}_3, 3 \cdot \mathrm{J}_3)$. Since any outer automorphism of L does not preserve $\varphi|_L$, we have that $G = \mathbf{Z}(G)L$. Note that any element of $\mathbf{Z}(G)$ must act on V as a scalar z which is a root of unity in $\mathbb{Q}(\varphi)$, whence $z^6 = 1$ and $|\mathbf{Z}(G)|$ divides 6. In particular, L is a normal subgroup of index ≤ 2 in G. As $\mathsf{o}(g_0) = 57$, L contains both g_0 and its normal closure in G. Hence $G_{\mathrm{geom}} = G = L$ by Theorem 5.1.

(ii) For the converse, let $\langle h_0 \rangle$ be the image of $I(0)$ in H. Then $S \lhd H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$. As h_0 has simple spectrum on $\mathcal{H}'$, $D := \mathrm{rank}\mathcal{H}' \leq \bar{\mathsf{o}}(h_0) \leq \mathrm{meo}(\mathrm{Aut}(S)) = 34$. Using [GAP], we can see that $D = 18$ and $H/\mathbf{Z}(H) = S$, and furthermore $H = \mathbf{Z}(H)L$ with $L := H^{(\infty)} \cong 3 \cdot S$. Let ς denote the character of the representation of H underlying $\mathcal{H}'$. Again using [GAP] we can check that $|\varsigma(h)|/\varsigma(1) \leq 1/6$ for all $h \in H \smallsetminus \mathbf{Z}(H)$. Assume now that $r \neq 2$. Then the image Q of $P(\infty)$ has order at least 3. Applying [KT5, (7.2.2)], we get that $W \geq 18 \cdot (1 - 1/6) \cdot (1 - 1/3) = 10$ for the dimension of the wild part of $\mathcal{H}'$. On the other hand, note that $L = 3 \cdot \mathrm{J}_3$ has an irreducible 9-dimensional representation over $\overline{\mathbb{F}_2}$ which certainly extends to an irreducible representation $\Lambda : H \to \mathrm{GL}_9(\overline{\mathbb{F}_2})$. Hence, by [KT5, Theorem 4.14], $\Lambda(H)$ is cyclic, a contradiction. Thus $r = 2$. Finally, as h_0 has simple spectrum on $\mathcal{H}$, it must have order 19 modulo $\mathbf{Z}(H)$ [GAP], and we can then read off the "upstairs" characters of $\mathcal{H}'$ by inspecting the eigenvalues of such an element on $\mathcal{H}'$. $\square$

Corollary 18.3. *The hypergeometric sheaf $\mathcal{H} = \mathcal{H}yp(\xi_3 \cdot \mathsf{Char}_{19}^{\times}; \mathbb{1}, \xi_5, \bar{\xi}_5)$ in characteristic $p = 2$ has a descent $\mathcal{H}^\sharp$ to $\mathbb{F}_4$, with arithmetic monodromy group $G_{\mathrm{arith},k} = 3 \cdot \mathrm{J}_3$ over any finite extension k of $\mathbb{F}_{16}$.*

Proof. By Theorem 7.7, $\mathcal{H}$ has a descent $\mathcal{H}^\sharp = \mathcal{H}_{00}$ to $\mathbb{F}_4$ for which any element in $G_{\mathrm{arith},\mathbb{F}_k}$ still has trace in $\mathbb{Q}(\sqrt{5}, \zeta_3)$ for any finite extension k of $\mathbb{F}_4$, with $\mathcal{H}_0$ given on line 12 of Table 4. Recall from Theorem 18.2 that $L := G_{\mathrm{geom}} = 3 \cdot \mathrm{J}_3$. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{5}, \zeta_3)$, we see that

$$C_3 = \mathbf{Z}(L) \leq \mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k}) \leq C_6.$$

Since no outer automorphism of L can preserve the equivalence class of the representation of L on $\mathcal{H}$, we must have that $G_{\mathrm{arith},k} = \mathbf{Z}(G_{\mathrm{arith},k})L$. Now if $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_4}) = \mathbf{Z}(L)$ then $G_{\mathrm{arith},k} = L$ and we are done. Consider the case $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_4}) = C_6$. In this case $G_{\mathrm{arith},\mathbb{F}_4} = G_{\mathrm{geom}} \times \langle z \rangle$ for some central involution z, and so modulo G_{geom} every element in $G_{\mathrm{arith},\mathbb{F}_4}$ is $z^{\deg/\mathbb{F}_4}$. In particular, $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ when $k \supseteq \mathbb{F}_{16}$. $\square$

19. The Rudvalis group Ru

In this section, let $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{29}^{\times}; \xi_{12}, \xi_{12}^3, \xi_{12}^5, \xi_{12}^9)$ be the hypergeometric sheaf in characteristic $p = 5$, with 28 "upstairs" characters $\mathsf{Char}_{29}^{\times}$, and 4 "downstairs" characters $\xi_{12}, \xi_{12}^3, \xi_{12}^5, \xi_{12}^9$.

Theorem 19.1. *The hypergeometric sheaf* $\mathcal{H} = \mathcal{H}yp(\mathsf{Char}_{29}^{\times}; \xi_{12}, \xi_{12}^3, \xi_{12}^5, \xi_{12}^9)$ *in characteristic* $p = 5$ *has finite geometric monodromy group* G_{geom}.

Proof. We need to show:

$$V(29x) - V(x) + V\left(-x + \frac{1}{12}\right) + V\left(-x + \frac{5}{12}\right) + V\left(-x + \frac{1}{4}\right) + V\left(-x - \frac{1}{4}\right) \geq \frac{3}{2}$$

or

$$V(29x) - V(x) + V\left(-x - \frac{1}{12}\right) + V\left(-x - \frac{5}{12}\right) + V\left(-x + \frac{1}{4}\right) + V\left(-x - \frac{1}{4}\right) \geq \frac{3}{2}$$

depending on the choice of χ. Using the fact that

$$V(\frac{i}{348}) = V(\frac{17538838i}{5^{14}-1}) = \frac{1}{56}[17538838i]$$

for $1 \leq i \leq 347$, we check that the inequality holds for $29x \in \mathbb{Z}$ and for $12x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ for $x \neq 0$, we can rewrite the first inequality as

$$V(29x) \leq V(x) + V\left(x + \frac{1}{12}\right) + V\left(x + \frac{5}{12}\right) + V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right) - \frac{3}{2}$$

and, following §9, it suffices to prove

$$[29x] \leq \left[x + \frac{5^r - 1}{12}\right] + \left[x + \frac{5(5^r-1)}{12}\right] + \left[x + \frac{5^r - 1}{4}\right] + \left[x + \frac{3(5^r-1)}{4}\right] + [x] - 6r$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 2^r - 1$. Notice that, in this case, multiplication by 5 permutes $\gamma_1 = \frac{1}{12}$ and $\gamma_2 = \frac{5}{12}$ and fixes $\gamma_3 = \frac{1}{4}$, $\gamma_4 = \frac{3}{4}$ and $\gamma_5 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2-1)\gamma_1 = 02_5, (5^2-1)\gamma_3 = 11_5, (5^2-1)\gamma_4 = 33_5$, $h_j = 2, 0, 1, 3$ and $h_{2,j} = 02, 20, 11, 33$ for $j = 1, 2, 3, 4$ respectively. We will prove that

$$[29x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x + h_{r,4}] + [x] - 6r$$

for every $r \geq 1$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 5$ we check it by computer. For $r > 5$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1	1	0,1	0	≥ 0	0	≥ 0
$a2; a \neq 1$	1	2	0	≥ 0	0	≥ 0
03,23,33	1	3	0	≥ 0	0	≥ 0
04,24	1	4	0	≥ 0	0	≥ 0
$a12, a13, a14; a \neq 1$	2	12,13,14	≥ 0	≥ 0	0	≥ 0
$a112, a113, a114; a \neq 1$	3	112,113,114	0	≥ 0	0	≥ 0
043	2	43	4	≥ 0	0	≥ 4
0243,2243,3243	3	243	0	≥ 0	0	≥ 0
0343,2343	3	343	0	≥ 0	0	≥ 0
0443	3	443	1	≥ 4	0	≥ 4
034,234	2	34	4	≥ 0	0	≥ 4
0334,2334	3	334	4	≥ 0	0	≥ 4
044	2	44	4	≥ 0	0	≥ 4
03343,23343	4	3343	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_5 = c_5'$ corresponding to $\gamma_5 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$	$c_4 = c_4'$
1112,1113,1114	4	112	3	0	0	12	0	0	0	1
143,144	3	20	2	4	0	21	0	0	0	1
1243	4	130	3	0	0	14	0	0	0	1
4243	4	430	3	4	4	101	1	1	1	1
1343	4	140	3	4	4	20	0	0	0	1
13343	5	1343	4	4	4	20	0	0	0	1
33343	5	3343	4	0	0	41	1	0	1	1
43343	5	4343	4	4	4	102	1	1	1	1
4343	4	440	3	4	4	102	1	1	1	1
1443	4	200	3	4	0	21	0	0	0	1
2443	4	300	3	4	0	32	0	1	0	1
3443	4	400	3	4	0	43	0	1	1	1
4443	4	444	3	4	4	103	1	1	1	1
134	3	14	2	8	4	20	0	0	0	1
1334	4	134	3	8	8	20	0	0	0	1
3334	4	334	3	4	4	41	0	1	1	1
4334	4	434	3	8	8	102	1	1	1	1
434	3	44	2	8	4	102	1	1	1	1
244	3	30	2	4	0	32	1	0	0	1
344	3	343	3	0	0	42	1	0	1	1
444	3	443	3	4	4	103	1	1	1	1

For $29x \notin \mathbb{Z}$ and $12x \notin \mathbb{Z}$, the second inequality can be rewritten as

$$V(29x) \leq V(x) + V\left(x - \frac{1}{12}\right) + V\left(x - \frac{5}{12}\right) + V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right) - \frac{3}{2}$$

and, via the change of variable $x \mapsto x + \frac{1}{2}$, as

$$V\left(29x+\frac{1}{2}\right) \le V\left(x+\frac{1}{12}\right)+V\left(x+\frac{5}{12}\right)+V\left(x+\frac{1}{4}\right)+V\left(x+\frac{3}{4}\right)+V\left(x+\frac{1}{2}\right)-\frac{3}{2}.$$

Following §9, it suffices to prove

$$\left[29x+\frac{5^r-1}{2}\right] \le \left[x+\frac{5^r-1}{12}\right]+\left[x+\frac{5(5^r-1)}{12}\right]+\left[x+\frac{5^r-1}{4}\right]$$
$$+\left[x+\frac{3(5^r-1)}{4}\right]+\left[x+\frac{5^r-1}{2}\right]-6r+4$$

for every $r \ge 1$ divisible by $r_0 = 2$ and every $0 \le x \le 2^r - 1$. Again, multiplication by 5 permutes $\gamma_1 = \frac{1}{12}$ and $\gamma_2 = \frac{5}{12}$ and fixes $\gamma_3 = \frac{1}{4}$, $\gamma_4 = \frac{3}{4}$ and $\gamma_5 = \frac{1}{2}$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2-1)\gamma_1 = 02_5, (5^2-1)\gamma_3 = 11_5, (5^2-1)\gamma_4 = 33_5, (5^2-1)\gamma_5 = 22_5$, $h_j = 2, 0, 1, 3, 2$ and $h_{2,j} = 02, 20, 11, 33, 22$ for $j = 1, \dots, 5$ respectively. We will prove that

$$\left[29x+\frac{5^r-1}{2}\right] \le [x+h_{r,1}]+[x+h_{r,2}]+[x+h_{r,3}]+[x+h_{r,4}]+[x+h_{r,5}]-6r+4$$

for every $r \ge 1$ and every $0 \le x \le 2^r - 1$. For $r \le 5$ we check it by computer. For $r > 5$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1	1	0,1	≥ 0	≥ 0	0	≥ 0
$a2; a \ne 1$	1	2	4	≥ 0	0	≥ 4
$a12; a \ne 1$	2	12	4	≥ 0	0	≥ 4
$a112; a \ne 1$	3	112	4	≥ 0	0	≥ 4
003,303,403	2	03	-4	≥ 1	0	≥ 0
103	3	103	0	≥ 0	0	≥ 0
$a203; a \ne 1$	3	203	0	≥ 0	0	≥ 0
013,313,413	2	13	-4	≥ 1	0	≥ 0
$a113, a213; a \ne 1$	3	113,213	0	≥ 0	0	≥ 0
$a1113; a \ne 1$	4	1113	0	≥ 0	0	≥ 0
023,323,423	2	23	0	≥ 0	0	≥ 0
33	1	3	-4	≥ 1	0	≥ 0
043	2	43	1	≥ 0	0	≥ 0
$a143; a \ne 1$	3	143	0	≥ 0	0	≥ 0
443	1	3	-4	≥ 2	1	≥ 0
04	2	04	4	≥ 0	0	≥ 4
$a14; a \ne 1$	2	14	0	≥ 0	0	≥ 0
$a24; a \ne 1, 2$	2	24	0	≥ 0	0	≥ 0
034	1	4	-4	≥ 2	1	≥ 0
044	2	44	0	≥ 0	0	≥ 0
444	1	4	-4	≥ 2	1	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table, in which we have $b_1 = b_1'$, $c_1 = c_1'$, $c_2 = c_2'$, $c_3 = c_3'$, $c_4 = c_4'$, and $c_5 = c_5'$.

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	b_1	c_1	c_2	c_3	c_4	c_5
1112	4	112	3	4	4	12	0	0	0	1	0
1203, 1213, 1143	4	114	3	0	0	13	0	0	0	1	0
11113	5	1113	4	0	0	12	0	0	0	1	0
123,124	3	13	2	0	-4	14	0	0	0	1	0
223,224	3	23	2	4	0	30	0	0	0	1	1
243,244	3	30	2	-4	-4	32	1	0	0	1	1
343,344	3	40	2	-4	-4	43	1	0	1	1	1
114	3	113	3	0	0	13	0	0	0	1	0
134	3	14	2	0	0	20	0	0	0	1	0
234	3	24	2	0	0	31	0	0	0	1	1
334	3	34	2	-4	-4	42	1	0	1	1	1
434	3	44	2	0	0	103	1	1	1	1	1
144	3	143	3	0	0	21	0	0	0	1	0

□

Theorem 19.2. *The following statements hold.*

(i) *The hypergeometric sheaf* $\mathcal{H} = \mathcal{H}yp(\mathsf{Char}_{29}^{\times}; \xi_{12}, \xi_{12}^3, \xi_{12}^5, \xi_{12}^9)$ *in characteristic* $p = 5$ *has geometric monodromy group* $G_{\mathrm{geom}} = 2 \cdot \mathrm{Ru}$*, the double cover of the Rudvalis sporadic simple group* Ru*.*

(ii) *The sheaf* $\tilde{\mathcal{H}} := \mathcal{H} \otimes \mathcal{L}_{\xi_4}$ *has geometric monodromy group* $\tilde{G}_{\mathrm{geom}} = G_{\mathrm{geom}} \circ C_4$*, the central product of* $G_{\mathrm{geom}} = 2\cdot\mathrm{Ru}$ *with the cyclic scalar subgroup* C_4*. Furthermore,* $\tilde{\mathcal{H}}$ *has a descent* $\tilde{\mathcal{H}}'$ *to* $\mathbb{F}_5$ *with arithmetic monodromy group* $\tilde{G}_{\mathrm{arith},k} = \tilde{G}_{\mathrm{geom}}$ *over any finite extension* k *of* $\mathbb{F}_{25}$*.*

Proof. (i) By Theorem 19.1, $G := G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}(i)$ with $i = \zeta_4$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G,V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 28$, G must be almost quasisimple by Lemma 3.1. Furthermore, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(i)$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_4. \tag{19.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\mathsf{o}(g_0) = 29$ for a generator g_0 of the image of $I(0)$, and $24|\mathsf{o}(g_\infty)$ for a p'-element g_∞ that generates $I(\infty)$ modulo $P(\infty)$, whence both cyclic groups C_{29} and C_{24} embed in $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to arrive at the following possibilities for (S,L).

• $S = L = \mathsf{A}_{29}$, and $V|_L$ is just the deleted permutation module $S^{(28,1)}|_L$. In this case, since $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = \mathsf{S}_{29}$, the element g_0 of order 29 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G. Using (19.2.1), we see that in fact $g_0 \in S$, hence $G = S$ by Theorem 5.1. But this is a contradiction, since $\mathbb{Q}(\varphi)$ would have been equal to $\mathbb{Q}$.

• $S = \mathrm{PSL}_2(29)$. This is impossible, since C_{24} does not embed in $\mathrm{Aut}(S) = \mathrm{PGL}_2(29)$.

• $(S,L) = (\mathrm{Ru}, 2 \cdot \mathrm{Ru})$. Since $\mathrm{Aut}(L) = L$, we have that $G = \mathbf{Z}(G)L$. Again using (19.2.1) we see that $g_0 \in L$, whence $G_{\mathrm{geom}} = G = L$ by Theorem 5.1.

(ii) By Theorem 7.5, $\tilde{\mathcal{H}}$ has a descent $\tilde{\mathcal{H}}' = (\tilde{\mathcal{H}})_{00}$ to $\mathbb{F}_5$, for which any element in $\tilde{G}_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(i)$ over any finite extension k of $\mathbb{F}_{25}$, with $(\tilde{\mathcal{H}})_0$ given in Table 4, line 13. It follows that $\mathbf{Z}(\tilde{G}_{\rm geom}) \leq \mathbf{Z}(\tilde{G}_{{\rm arith},k}) \leq C_4$. Next, if $\tilde{g}_0$ generates the image of $I(0)$ in $\tilde{G} := \tilde{G}_{\rm geom}$, then note that $\tilde{g}_0^{29}$ acts as the scalar i on $\tilde{\mathcal{H}}$, whence we now have

$$\mathbf{Z}(\tilde{G}_{\rm geom}) = \mathbf{Z}(\tilde{G}_{{\rm arith},k}) = C_4. \tag{19.2.2}$$

By Lemma 5.12, $\tilde{G}/\mathbf{Z}(\tilde{G}) \cong G/\mathbf{Z}(G) = S$, and $\tilde{G}^{(\infty)} \cong G^{(\infty)} = L$. Next, since L already induces the full automorphism group Ru of $L \lhd \tilde{G}_{{\rm arith},k}$, we conclude that

$$\tilde{G}_{{\rm arith},k} = \tilde{G}_{\rm geom} = \mathbf{Z}(\tilde{G}_{\rm geom})L = (2 \cdot {\rm Ru}) \circ C_4.$$

[Note that $(2 \cdot {\rm Ru}) \circ C_4$ is the automorphism group of a certain 28-dimensional lattice over Gaussian integers, see [Atlas]]. □

20. The special linear group $\mathrm{PSL}_3(4)$

Theorem 20.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{14} \smallsetminus \{\mathbb{1}, \xi_7, \xi_7^2, \xi_7^4\}; \xi_4, \bar{\xi}_4)$ in characteristic $p = 3$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(14x) - V(x) - V\left(x + \frac{1}{7}\right) - V\left(x + \frac{2}{7}\right) - V\left(x + \frac{4}{7}\right) + V(-4x) - V(-2x) + 2 \geq 0$$

and

$$V(14x) - V(x) - V\left(x - \frac{1}{7}\right) - V\left(x - \frac{2}{7}\right) - V\left(x - \frac{4}{7}\right) + V(-4x) - V(-2x) + 2 \geq 0$$

which are equivalent via the change of variable $x \mapsto 3x$. Using the fact that

$$V(\frac{i}{28}) = V(\frac{26i}{3^6 - 1}) = \frac{1}{12}[26i]$$

for $1 \leq i \leq 13$, we check that the first inequality holds for $28x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$ and $V(2x) = V(x) + V(x + \frac{1}{2}) - \frac{1}{2}$ [Ka7, §13], as

$$V(14x) \leq V\left(x - \frac{1}{7}\right) + V\left(x - \frac{2}{7}\right) + V\left(x - \frac{4}{7}\right) + V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right) + V(x) - 2$$

and, via the change of variable $x \mapsto x + \frac{1}{4}$, as

$$V\left(14x + \frac{1}{2}\right) \leq V\left(x + \frac{3}{28}\right) + V\left(x + \frac{27}{28}\right) + V\left(x + \frac{19}{28}\right) + V\left(x + \frac{1}{4}\right) + V\left(x + \frac{1}{2}\right) + V(x) - 2$$

Following §9, it suffices to prove

$$\left[14x + \frac{3^r - 1}{2}\right] \leq \left[x + \frac{3(3^r - 1)}{28}\right] + \left[x + \frac{27(3^r - 1)}{28}\right] + \left[x + \frac{19(3^r - 1)}{28}\right] + \left[x + \frac{3^r - 1}{4}\right] + \left[x + \frac{3^r - 1}{2}\right] + [x] - 4r$$

for every $r \geq 1$ multiple of $r_0 = 6$ and every $0 \leq x \leq 3^r - 1$. Notice that, in this case, multiplication by 3^2 permutes $\gamma_1 = \frac{3}{28}$, $\gamma_2 = \frac{27}{28}$ and $\gamma_3 = \frac{19}{28}$ cyclically and fixes $\gamma_4 = \frac{1}{4}$, $\gamma_5 = \frac{1}{2}$ and $\gamma_6 = 0$, so we can take $r_1 = 2$. Then, with the notation of §9, we have $(3^6 - 1)\gamma_1 = 002220_3$, $h_j = 20_3, 22_3, 00_3, 02_3, 11_3$, $h_{2,j} = 2220_3, 0022_3, 2000_3, 0202_3, 1111_3$ and $h_{3,j} = 002220_3, 200022_3, 222000_3, 020202_3, 111111_3$ for $j = 1, \ldots, 5$ respectively. We will prove that

$$\left[14x + \frac{3^r - 1}{2}\right] \leq [x + h_{k,1}] + [x + h_{k,2}] + [x + h_{k,3}] + [x + h_{k,4}] + [x + h_{k,5}] + [x] - 4r$$

for every $r = 2k \geq 2$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
00	2	00	0	0	0	0
$a01, a02; a \neq 2$	2	01,02	≥ 0	≥ 0	0	≥ 0
$a201; a \neq 2$	2	01	0	1	1	0
$a202; a \neq 2$	2	02	2	0	1	0
012201,102201,122201,212201	4	2201	6	≥ 0	≤ 1	≥ 4
110,111	2	10,11	≥ 0	≥ 0	0	≥ 0
0210,1010,1210,2010	2	10	0	≥ 1	≤ 1	≥ 0
0211,1011,1211,2011	2	11	2	≥ 0	≤ 1	≥ 0
00010,10010	4	0010	0	≥ 0	0	≥ 0
020010,120010	4	0010	0	≥ 1	1	≥ 0
$ab12, ab20; ab \neq 00, 11, 22$	2	12,20	≥ 2	≥ 0	≤ 1	≥ 0
$ab1112; ab \neq 00, 11, 22$	4	1112	2	≥ 0	≤ 1	≥ 0
$ab21, ab22; ab \neq 00, 11, 20, 22$	2	21,22	≥ 4	≥ 0	≤ 1	≥ 2
$ab2221; ab \neq 00, 11, 20, 22$	4	2221	10	≥ 0	≤ 1	≥ 8

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_6 = c'_6$ corresponding to $\gamma_6 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	c_1	c_2	c_3	c_4	c_5
002201	6	0022	4	0	0	1	0	0	1	0	0
022201	6	1000	4	6	0	12	0	1	1	0	0
112201	6	1122	4	6	6	22	0	1	1	0	1
202201	6	2022	4	6	6	102	0	1	1	1	1
222201,222221	6	2222	4	≥ 10	10	112	1	1	1	1	1
2202,2210,2211	4	2201	4	6	6	111	1	1	1	1	1
220010	6	2201	4	6	6	111	1	1	1	1	1
0011,0012,0020,0021,0022	4	0010	4	≥ 0	0	1	1	0	0	0	0
001112	6	0011	4	0	0	1	0	0	1	0	0
111112	6	1112	4	2	2	21	0	1	1	0	1
221112	6	2212	4	8	8	111	1	1	1	1	1
2212,2220	4	2211	4	≥ 6	6	111	1	1	1	1	1
1120,1121	4	1112	4	2	2	21	1	0	1	0	1
1122	4	12	2	6	2	22	1	0	1	0	1
2021,2022	4	21	2	6	4	102	1	0	1	1	1
002221	6	01	2	8	0	2	0	0	1	0	0
112221	6	12	2	10	2	22	0	1	1	0	1
202221	6	21	2	12	4	102	0	1	1	1	1
2222	4	2221	4	10	10	112	1	1	1	1	1

□

Theorem 20.2. *The local system* $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{14} \smallsetminus \{\mathbb{1}, \xi_7, \xi_7^2, \xi_7^4; \xi_4, \bar{\xi}_4)$ *in characteristic* $p = 3$ *has geometric monodromy group* $G_{\mathrm{geom}} = 2 \cdot \mathrm{PSL}_3(4) \cdot 2_2$. *Moreover,* $\mathcal{H}$ *has a descent* $\mathcal{H}'$ *to* $\mathbb{F}_9$*, with arithmetic monodromy group* $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ *for any finite extension* k *of* $\mathbb{F}_9$.

Proof. (i) By Theorem 20.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(ii), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}(\sqrt{-7})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 10$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{20.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, for a generator g_0 of the image of $I(0)$ in G we have $\bar{\mathsf{o}}(g_0) = 14$, and so $C_{14} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is elementary abelian of order 3^2 by Proposition 5.8(iv), and a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has central order divisible by 8 by Proposition 5.9(iii). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = L = \mathsf{A}_{11}$, and $V|_L$ is just the deleted permutation module $S^{(10,1)}|_L$. This case is however impossible, since otherwise we would have $\mathbb{Q}(\varphi) = \mathbb{Q}$ by Lemma 3.8.
- $S = L = \mathsf{A}_7$. Since $\varphi|_S$ is not stable under outer automorphisms of S, we have that $G = \mathbf{Z}(G) \times S$. But this is a contradiction, since S contains no element of order 8.
- $(S, L) = (\mathrm{M}_{22}, 2\mathrm{M}_{22})$. Using [GAP] we can check that the restriction of $\varphi|_L$ to $2'$-elements yields an irreducible 2-Brauer character of L. In other words, a reduction modulo 2 of Φ is an absolutely irreducible 2-modular representation of G. However, this is impossible: applying Theorem 6.13 with $\ell = 2$ we see that such a reduction of Φ must admit a trivial composition factor over G.
- $(S, L) = (\mathrm{PSL}_3(4), 2 \cdot \mathrm{PSL}_3(4))$. Now we have $\mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L) = C_2$ by (20.2.1). Recall that $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot (C_2 \times \mathsf{S}_3)$, G admits an irreducible representation of degree 10, and contains the g_0 element of central order 14. Hence we see by [Atlas] that $G/\mathbf{Z}(G) = S \cdot 2_2$. It follows that $G_{\rm geom} = L \cdot 2_2 = 2 \cdot \mathrm{PSL}_3(4) \cdot 2_2$.

(ii) By Theorem 7.7, $\mathcal{H}$ has a descent $\mathcal{H}' = \mathcal{H}_{00}$ to $\mathbb{F}_9$, for which any element in $\tilde{G}_{{\rm arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-7})$ over any finite extension k of $\mathbb{F}_9$, with $\mathcal{H}_0$ either of the two choices given in Table 4, line 14. Since any element in $\mathbf{C}_{G_{{\rm arith},k}}(L) = \mathbf{Z}(G_{{\rm arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{-7})$, we see that $\mathbf{C}_{G_{{\rm arith},k}}(L) = C_2 = \mathbf{Z}(L)$. Hence, if $G_{{\rm arith},k} > G_{\rm geom}$, we see that some element of $G_{{\rm arith},k}$ must induce an outer automorphism of L lying outside of $S \cdot 2_2$, which is impossible under the condition that it acts on $L = 2 \cdot S$, see [Atlas]. Therefore we must have that $G_{{\rm arith},k} = L = G_{\rm geom}$. ☐

Theorem 20.3. *The local system $\mathcal{H}_2 := \mathcal{H}yp(\{\xi_{20}^i \mid i = 1, 3, 5, 7, 9, 13, 15, 17\}; \xi_3, \xi_3^2)$ in characteristic $p = 7$ has finite geometric monodromy group.*

Proof. We need to show:

$$V\left(10x + \frac{1}{2}\right) - V\left(x + \frac{11}{20}\right) - V\left(x + \frac{19}{20}\right) + V\left(-x + \frac{1}{3}\right) + V\left(-x + \frac{2}{3}\right) \geq 0,$$

$$V\left(10x + \frac{1}{2}\right) - V\left(x + \frac{13}{20}\right) - V\left(x + \frac{17}{20}\right) + V\left(-x + \frac{1}{3}\right) + V\left(-x + \frac{2}{3}\right) \geq 0,$$

$$V\left(10x + \frac{1}{2}\right) - V\left(x + \frac{1}{20}\right) - V\left(x + \frac{9}{20}\right) + V\left(-x + \frac{1}{3}\right) + V\left(-x + \frac{2}{3}\right) \geq 0,$$

and

$$V\left(10x+\frac{1}{2}\right)-V\left(x+\frac{3}{20}\right)-V\left(x+\frac{7}{20}\right)+V\left(-x+\frac{1}{3}\right)+V\left(-x+\frac{2}{3}\right)\geq 0.$$

The first two and the last two are equivalent via the change of variable $x\mapsto 7x$. Using the fact that $V(\frac{i}{60})=V(\frac{40i}{7^4-1})=\frac{1}{24}[40i]$ for $1\leq i\leq 59$ we check that the inequalities hold for $20x\in\mathbb{Z}$ and for $3x\in\mathbb{Z}$. For all other values of x we can rewrite the first inequality, using that $V(x)+V(-x)=1$ for $x\neq 0$, as

$$V\left(10x+\frac{1}{2}\right)\leq V\left(x+\frac{1}{20}\right)+V\left(x+\frac{9}{20}\right)+V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right)-1$$

and, following §9, it suffices to prove

$$\left[10x+\frac{7^r-1}{2}\right]\leq\left[x+\frac{7^r-1}{20}\right]+\left[x+\frac{9(7^r-1)}{20}\right]+\left[x+\frac{7^r-1}{3}\right]+\left[x+\frac{2(7^r-1)}{3}\right]-6r$$

for every $r\geq 1$ multiple of $r_0=4$ and every $0\leq x\leq 7^r-1$. Notice that, in this case, multiplication by 7^2 permutes $\gamma_1=\frac{1}{20}$ and $\gamma_2=\frac{9}{20}$ and fixes $\gamma_3=\frac{1}{3}$ and $\gamma_4=\frac{2}{3}$, so we can take $r_1=2$. Then, with the notation of §9, we have $(7^4-1)\gamma_1=0231_7$, $h_j=31_7,02_7,22_7,44_7$, $h_{2,j}=0231_7,3102_7,2222_7,4444_7$ for $j=1,\dots,4$ respectively. We will prove that

$$\left[10x+\frac{7^r-1}{2}\right]\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x+h_{k,4}]-6r$$

for every $r=2k\geq 2$ and every $0\leq x\leq 7^r-1$. For $r\leq 4$ we check it by computer. For $r>4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-6\sum_j v_j+6\sum_i u_i$
$00,\dots,22$	2	$00,\dots,22$	≥ 0	≥ 0	0	≥ 0
$a23,\dots,a35; a\neq 2$	2	$23,\dots,35$	≥ 0	≥ 0	0	≥ 0
$a36,\dots,a64; a\neq 2,4$	2	$36,\dots,44$	≥ 0	≥ 0	0	≥ 0
$a65,a66; a\neq 2,4,5$	2	$65,66$	≥ 0	≥ 0	0	≥ 0
$0abc, 1abc$	4	$0abc,1abc$	≥ 0	≥ 0	0	≥ 0
$a436,\dots,a443; a\neq 6$	2	$36,\dots,43$	≥ 0	≥ 1	1	≥ 0
$ab44; ab\neq 22,64$	2	44	18	≥ 0	1	≥ 12

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$	$c_3 = c'_3$	$c_4 = c'_4$
$2223,\ldots,2266$	4	23	2	≥ 0	0	3	0	0	0	1
$3223,\ldots,3266$	4	33	2	≥ 6	6	5	0	0	0	1
$4223,\ldots,4266$	4	43	2	≥ 0	0	6	0	1	0	1
$5223,\ldots,5266$	4	53	2	≥ 6	6	11	0	1	1	1
$6223,\ldots,6266$	4	63	2	≥ 6	6	12	0	1	1	1
$2445,\ldots,2466$	4	25	2	≥ 0	0	4	0	0	0	1
$3445,\ldots,3466$	4	35	2	≥ 0	0	5	0	0	0	1
$4445,\ldots,4466$	4	45	2	≥ 0	0	10	0	1	1	1
$5445,\ldots,5466$	4	55	2	≥ 0	0	11	0	1	1	1
$6436,\ldots,6466$	4	65	2	≥ 0	0	13	1	1	1	1
$2565, 2566$	4	26	2	≥ 0	0	4	0	0	0	1
$3565, 3566$	4	36	2	≥ 0	0	6	0	1	0	1
$4565, 4566$	4	46	2	≥ 0	0	10	0	1	1	1
$5565, 5566$	4	56	2	≥ 0	0	11	0	1	1	1
$6565, 6566$	4	66	2	≥ 0	0	13	1	1	1	1

The third inequality can be rewritten, using that $V(x)+V(-x)=1$ for $x\neq 0$, as

$$V\left(10x+\frac{1}{2}\right)\leq V\left(x+\frac{11}{20}\right)+V\left(x+\frac{19}{20}\right)+V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right)-1$$

and, via the change of variable $x\mapsto x+\frac{1}{2}$, as

$$V\left(10x+\frac{1}{2}\right)\leq V\left(x+\frac{1}{20}\right)+V\left(x+\frac{9}{20}\right)+V\left(x+\frac{1}{6}\right)+V\left(x+\frac{5}{6}\right)-1.$$

Following §9, it suffices to prove

$$\left[10x+\frac{7^r-1}{2}\right]\leq\left[x+\frac{7^r-1}{20}\right]+\left[x+\frac{9(7^r-1)}{20}\right]+\left[x+\frac{7^r-1}{6}\right]+\left[x+\frac{5(7^r-1)}{6}\right]-6r$$

for every $r\geq 1$ multiple of $r_0=4$ and every $0\leq x\leq 7^r-1$. Notice that, in this case, multiplication by 7^2 permutes $\gamma_1=\frac{1}{20}$ and $\gamma_2=\frac{9}{20}$ and fixes $\gamma_3=\frac{1}{6}$ and $\gamma_4=\frac{5}{6}$, so we can take $r_1=2$. Then, with the notation of §9, we have $(7^4-1)\gamma_1=0231_7$, $h_j=31_7,02_7,11_7,55_7$, $h_{2,j}=0231_7,3102_7,1111_7,5555_7$ for $j=1,\ldots,4$ respectively. We will prove that

$$\left[10x+\frac{7^r-1}{2}\right]\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x+h_{k,4}]-6r$$

for every $r=2k\geq 2$ and every $0\leq x\leq 7^r-1$. For $r\leq 6$ we check it by computer. For $r>6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-6\sum_j v_j+6\sum_i u_i$
$00,\ldots,11$	2	$00,\ldots,11$	≥ 0	≥ 0	0	≥ 0
$a12,\ldots,a35; a\neq 1$	2	$12,\ldots,35$	≥ 0	≥ 0	0	≥ 0
$a36,\ldots,a55; a\neq 1,4$	2	$36,\ldots,55$	≥ 0	≥ 0	0	≥ 0
$a56,\ldots,a66; a\neq 1,4,5$	2	$56,\ldots,66$	≥ 0	≥ 0	0	≥ 0
$0abc$	4	$0abc$	≥ 0	≥ 0	0	≥ 0
$a3556; a\neq 1$	4	3556	0	≥ 0	0	≥ 0
013556	6	013556	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$	$c_3 = c'_3$	$c_4 = c'_4$
$1112, \ldots, 1166$	4	12	2	≥ 0	0	2	0	0	0	1
$2112, \ldots, 2166$	4	22	2	≥ 0	0	3	0	0	0	1
$3112, \ldots, 3166$	4	32	2	≥ 6	6	5	0	0	0	1
$4112, \ldots, 4166$	4	42	2	≥ 0	0	6	0	1	0	1
$5112, \ldots, 5151$	4	51	2	≥ 6	6	10	0	1	0	1
$5152, \ldots, 5166$	4	52	2	≥ 12	12	11	0	1	0	1
$6112, \ldots, 6166$	4	62	2	≥ 6	6	12	0	1	1	1
$1436, \ldots, 1466$	4	15	2	≥ 0	0	2	0	0	0	1
$2436, \ldots, 2466$	4	25	2	≥ 6	6	4	0	0	0	1
$3436, \ldots, 3466$	4	35	2	≥ 6	6	5	0	0	0	1
$4436, \ldots, 4466$	4	45	2	≥ 12	12	10	0	1	0	1
$5436, \ldots, 5466$	4	55	2	≥ 12	12	11	0	1	0	1
$6436, \ldots, 6466$	4	65	2	≥ 6	6	13	1	1	1	1
$1556, \ldots, 1566$	4	16	2	≥ 0	0	3	0	0	0	1
$2556, \ldots, 2566$	4	26	2	≥ 0	0	4	0	0	0	1
113556	6	12	2	0	0	2	0	0	0	1
213556	6	22	2	0	0	3	0	0	0	1
313556	6	32	2	6	6	5	0	0	0	1
413556	6	42	2	0	0	6	0	1	0	1
513556	6	51	2	6	6	10	0	1	0	1
613556	6	62	2	6	6	12	0	1	1	1
$3560, \ldots, 3564$	4	35	2	≥ 6	6	5	0	0	0	1
$3565, 3566$	4	36	2	≥ 0	0	6	0	1	0	1
$4556, \ldots, 4566$	4	46	2	≥ 6	6	10	0	1	0	1
$5556, \ldots, 5566$	4	56	2	≥ 0	0	11	0	1	1	1
$6556, \ldots, 6566$	4	66	2	≥ 0	0	13	1	1	1	1

□

Theorem 20.4. *The local system $\mathcal{H}_2 := \mathcal{H}yp(\xi_{20}^i,\ i = 1,3,5,7,9,13,15,17; \xi_3, \bar{\xi}_3)$ in characteristic $p = 7$ has geometric monodromy group $G_{\rm geom} = 4_1 \cdot \mathrm{PSL}_3(4) \cdot 2_3$. Moreover, $\mathcal{H}_2$ has a descent $\mathcal{H}'_2$ to $\mathbb{F}_{49}$, with arithmetic monodromy group $G_{{\rm arith},k} = G_{\rm geom}$ for any finite extension k of $\mathbb{F}_{49}$.*

Proof. (i) By Theorem 20.3, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}_2$, and let g_0 denote a generator of the image of $I(0)$ in G. By the construction of $\mathcal{H}$, we may assume that the spectrum of g_0 on V consists of ζ_{20}^i, $i = 1,3,5,7,9,13,15,17$. In particular, $\varphi(g_0^5) = 2\sqrt{-1}$ and

$$\varphi(g_0^4) = -(\zeta_5 + \bar{\zeta}_5), \tag{20.4.1}$$

and thus the field of traces $\mathbb{Q}(\varphi)$ contains both $\sqrt{-1}$ and $\sqrt{5}$. On the other hand, each of the set of "upstairs" characters and the set of "downstairs" characters of $\mathcal{H}_2$ is fixed by the Galois automorphisms $\zeta_{60} \mapsto \zeta_{60}^{41}$ and $\zeta_{60} \mapsto \zeta_{60}^{49}$ of $\mathbb{Q}(\zeta_{60})/\mathbb{Q}$. It follows from Corollary 6.2(ii) that $\mathbb{Q}(\varphi) := \mathbb{Q}(\sqrt{-1}, \sqrt{5})$.

It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Also, it is tensor indecomposable by [KRLT3, Corollary 10.4]. Now, if it is tensor induced, then, since

$D = \dim(V) = 8$, it is 3-tensor induced, and G acts transitively on the 3 tensor factors of a decomposition $V = V_1 \otimes V_2 \otimes V_3$ with $\dim(V_i) = 2$, with kernel say K. By Proposition 5.8, the image Q of $P(\infty)$ in G has order 7, which is coprime to $|\mathsf{S}_3|$, and so Q and its normal closure $G_{P(\infty)}$ are contained in K. By Theorem 5.3, $G/G_{P(\infty)}$, hence G/K, is cyclic, and thus $G/K \cong C_3$. (Alternatively, we can also use [KT5, Corollary 3.3] to deduce that $G/K \cong C_3$.) As $\mathsf{o}(g_0) = 20$ is coprime to 3, $g_0 \in K$, and so the normal closure of the image $\langle g_0 \rangle$ of $I(0)$ is contained in K, contradicting Theorem 5.1. Hence, (G, V) satisfies $(\mathbf{S}+)$.

Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_4. \tag{20.4.2}$$

Suppose we are in the extraspecial case (c) of Lemma 3.1. Then G has a normal 2-subgroup R which acts irreducibly on V, and $\mathbf{Z}(R) \leq \mathbf{C}_G(R) = \mathbf{Z}(G) \leq 4$. Furthermore, $R = \mathbf{Z}(R)E$ with $E = 2^{1+6}_\epsilon$ for some $\epsilon = \pm$, and, using Φ to identify R and G with their images under Φ, we have

$$R \lhd G \leq \mathbf{N}_{\mathrm{GL}(V)}(R) \leq \mathbf{Z}(\mathrm{GL}(V)) \circ (C_4 \circ 2^{1+6}_\epsilon) \cdot \mathrm{Sp}_6(2)$$

(cf. [KT8, §8] and [NRS, §6]). Now, the element g_0^4 of order 5 cannot centralize R and so induces a nontrivial automorphism of R, where $\mathrm{Aut}(R) \cong 2^6 \cdot (2 \times \mathrm{Sp}_6(2))$ by [Gri, Corollary 2]. As the Sylow 5-subgroups of $(C_4 \circ 2^{1+6}_\epsilon) \cdot \mathrm{Sp}_6(2) > 2^{1+6}_+ \cdot \Omega^+_6(2)$ are of order 5, we can find an element $h \in 2^{1+6}_+ \cdot \Omega^+_6(2)$ of order 5 and a scalar $\alpha \in \mathbb{C}^\times$ such that $g_0^5 = \alpha h$. It follows that $\alpha^5 = 1$. On the other hand, $\mathrm{Trace}(h) \in \mathbb{Z}[\sqrt{2}]$ by [NRS, Theorem 2.2], and this contradicts (20.4.1).

We have shown that G is almost quasisimple. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, since $\bar{\mathsf{o}}(g_0) = 10$, we have $C_{10} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ has order 7 as mentioned above, and so $C_7 \hookrightarrow \mathrm{Aut}(S)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $(S, L) = (\mathsf{A}_9, 2\mathsf{A}_9)$ or $(\mathrm{Sp}_6(2), 2 \cdot \mathrm{Sp}_6(2))$. In these cases, we can check using [Atlas] that $G/\mathbf{Z}(G) = L/\mathbf{Z}(L)$, $G^{(\infty)} = L = L^{(\infty)}$, and $\mathbb{Q}(\varphi|_L) = \mathbb{Q}$, which is a contradiction by Lemma 3.9, since $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$.
- $(S, L) = (\mathsf{A}_8, 2\mathsf{A}_8)$, $(\mathsf{A}_9, \mathsf{A}_9)$, $(\Omega^+_8(2), 2 \cdot \Omega^+_8(2))$. In these two cases, we can find using [GAP] an almost quasisimple group $L \cdot 2$ and a faithful character ψ of $L \cdot 2$ such that $(L \cdot 2)/\mathbf{Z}(L) \geq G/\mathbf{Z}(G)$, $(L \cdot 2)^{(\infty)} = L = G^{(\infty)}$, $\psi|_L = \varphi|_L$, but $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\sqrt{-1}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{5}) = \mathbb{Q}(\varphi)$. The latter again contradicts Lemma 3.9.
- $(S, L) = (\mathrm{PSL}_3(4), 4_1 \cdot \mathrm{PSL}_3(4))$. Now we have $C_4 = \mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L)$ by (20.4.2). Recall that $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot (C_2 \times \mathsf{S}_3)$, $G \rhd L$ admits an irreducible representation of degree 8, and contains the g_0 element of central order 10. Hence we see by [Atlas] that $G/\mathbf{Z}(G) = S \cdot 2_3$. It follows that $G_{\mathrm{geom}} = L \cdot 2_3 = 4_1 \cdot \mathrm{PSL}_3(4) \cdot 2_3$.

(ii) By Theorem 7.5, $\mathcal{H}_2$ has a descent $\mathcal{H}_2' = (\mathcal{H}_2)_{00}$ to $\mathbb{F}_{49}$, for which any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ over any finite extension k of $\mathbb{F}_{49}$, with $(\mathcal{H}_2)_0$ given in Table 4, line 15. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$, we see that $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_4 = \mathbf{Z}(L)$. Hence, if $G_{\mathrm{arith},k} > G_{\mathrm{geom}}$, we see that some element of $G_{\mathrm{arith},k}$ must induce an outer automorphism of S lying outside of $S \cdot 2_3$, which is impossible under the condition that it fixes $L = 4_1 \cdot S$ and $\varphi|_L$, see [Atlas]. Therefore we must have that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. $\square$

Theorem 20.5. *The local system $\mathcal{H}_3 := \mathcal{H}yp(\mathsf{Char}_7^\times; \xi_3)$ in characteristic $p = 2$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(7x) - V(x) + V\left(-x + \frac{1}{3}\right) \geq 0$$

and

$$V(7x) - V(x) + V\left(-x - \frac{1}{3}\right) \geq 0$$

which are equivalent via the change of variable $x \mapsto 2x$. Using the fact that $V(\frac{i}{21}) = V(\frac{3i}{2^6-1}) = \frac{1}{6}[3i]$ for $1 \leq i \leq 20$ we check that the first inequality holds for $7x \in \mathbb{Z}$ and for $3x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$, as

$$V(7x) \leq V\left(x + \frac{1}{3}\right) + V(x)$$

and, following §9, it suffices to prove

$$[7x] \leq \left[x + \frac{2^r - 1}{3}\right] + [x] + 1$$

for every $r \geq 1$ multiple of $r_0 = 2$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
00,10	2	00,10	≥ 0	≥ 0	0	≥ 0
0001,0011	4	0001,0011	0	≥ 0	0	≥ 0
001001,001011	6	001001,001011	≥ 0	≥ 0	0	≥ 0
101001	4	1001	-1	≥ 1	0	≥ 0
11001	4	1001	-1	≥ 2	0	≥ 1
101	2	01	-1	≥ 1	0	≥ 0
11011	4	1011	0	≥ 0	0	≥ 0
111	2	11	0	≥ 0	0	≥ 0

The remaining case is proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c_2'$ corresponding to $\gamma_2 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$
101011	6	1011	4	0	0	100	1

□

Theorem 20.6. *The local system $\mathcal{H}_3 := \mathcal{H}yp(\mathsf{Char}_7^\times; \xi_3)$ in characteristic $p = 2$, has geometric monodromy group $G_{\mathrm{geom}} = 6 \cdot \mathrm{PSL}_3(4)$. Moreover, $\mathcal{H}_3$ has a descent $\mathcal{H}_3'$ to $\mathbb{F}_4$, with arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ for any finite extension k of $\mathbb{F}_4$.*

Proof. (i) By Theorem 20.5, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}_3$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, (G,V) satisfies ($\mathbf{S}$+) by Theorem 3.6. Next, $\mathbb{Q}(\varphi) := \mathbb{Q}(\sqrt{-3})$ by Corollary 6.2(i). By Theorem 7.5, $\mathcal{H}_3$ has a descent $\mathcal{H}_3' = (\mathcal{H}_3)_{00}$ to $\mathbb{F}_4$, for which any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-3})$ over any finite extension k of $\mathbb{F}_4$, with $(\mathcal{H}_3)_0$ given in Table 4, line 16. Since the cyclic group $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_4})$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3})$, we have that

$$\mathbf{Z}(G) \leq \mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_4}) \hookrightarrow C_6. \tag{20.6.1}$$

As $D = \dim(V) = 6$, G is almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, since $\bar{\mathsf{o}}(g_0) = 7$ for a generator g_0 of the image of $I(0)$ in G, we have $C_7 \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is an elementary abelian group of order 2^4 by Proposition 5.8, whence $2^4 \hookrightarrow \mathrm{Aut}(S)$ by Proposition 5.6(i). Also, a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ has trace 0 on the wild part Wild and eigenvalue of the tame part Tame of dimension 1; in particular, $\bar{\mathsf{o}}(g_\infty) = 5$ and $C_5 \hookrightarrow \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = \mathsf{A}_7$. This is impossible, since 2^4 does not embed in $\mathrm{Aut}(S) = \mathsf{S}_7$.
- $(S, L) = (\mathrm{J}_2, 2\mathrm{J}_2)$. This case is rule out since otherwise we would have that $\mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$.
- $(S, L) = (\mathrm{PSU}_4(3), 6_1 \cdot \mathrm{PSU}_4(3))$. In this case, using [GAP] we can check that $\varphi|_L$ has $M_{6,0} = 2$, and so φ has $M_{6,0} \leq 2$. Now we apply Theorem 6.5, with $(a, b) = (6, 0)$, and $C = 6666$, $B \leq 9333$, $A \leq 2667$ (according to Lemmas 6.6, 6.7, and Remark 6.8), which implies that the approximation of $M_{6,0}$ at most 4.6135 over $\mathbb{F}_{2^{20}}$. However, a calculation with [Mag], for which we thank Andrew Sutherland, yields an approximation of (at least) 6.8996 over $\mathbb{F}_{2^{20}}$, a contradiction. [In this calculation, we use the trace function of $\mathcal{H}_3' \otimes \mathcal{L}_{\xi_3}$, which has the same $(6,0)$ moment as $\mathcal{H}_3'$,

$$u \in E^\times \mapsto \frac{1}{\#E} \sum_{x \in E,\ 0 \neq t \in E} \psi\Big(\frac{x^7}{t} + x + \frac{t}{u}\Big)\xi_3(t)$$

for any finite extension E of $\mathbb{F}_4$.]
- $(S, L) = (\mathrm{PSL}_3(4), 6 \cdot \mathrm{PSL}_3(4))$. Now we have $C_6 = \mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L)$ by (20.6.1). As $\mathrm{Out}(S) = C_2 \times \mathsf{S}_3$ (see [Atlas]) and $\bar{\mathsf{o}}(g_0) = 7$, we see that $g_0 \in L$ and so $G_{\mathrm{geom}} = L$ by Theorem 5.1.

(ii) Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k})$ acts via scalars, we see by (20.6.1) that $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_6 = \mathbf{Z}(L)$. Let φ also denote the character of $G_{\mathrm{arith},\mathbb{F}_4}$ on the representation realizing $\mathcal{H}_3'$, and assume that $G_{\mathrm{arith},\mathbb{F}_4} > G_{\mathrm{geom}}$. Then the outer automorphism of L induced by any element in $G_{\mathrm{arith},k} \smallsetminus L$ must fix $\varphi|_L$, and so it belongs to $S \cdot 2_1$, see [Atlas]. Therefore we must have that $G_{\mathrm{arith},k} = 6 \cdot \mathrm{PSL}_3(4) \cdot 2_1$. One such extension, call it H, is given in [GAP], with a faithful character $\varsigma : H \to \mathrm{GL}(V)$ and an element h (of class $8c$), where $\varsigma|_L = \varphi|_L$ and $\mathbb{Q}(\varsigma) = \mathbb{Q}(\sqrt{-3}, \sqrt{2}) \supseteq \mathbb{Q}(\varphi)$. By Lemma 3.9, there is a root of unity $\gamma \in \mathbb{C}$ such that $\mathbb{Q}(\varsigma) = \mathbb{Q}(\varphi)(\gamma)$. Clearly, $\gamma \notin \mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\varsigma)$ has degree 2 over $\mathbb{Q}(\sqrt{-3})$. It follows that $\mathbb{Q}(\varsigma) = \mathbb{Q}(\sqrt{-3}, \gamma)$ is a cyclotomic extension of degree 4 over $\mathbb{Q}$, and so it must be either $\mathbb{Q}(\zeta_8)$ or $\mathbb{Q}(\zeta_{12})$. Both of these cases are however impossible since $\mathbb{Q}(\varsigma)$ contains both $\sqrt{2}$ and $\sqrt{-3}$. Consequently, $G_{\mathrm{arith},\mathbb{F}_4} = G_{\mathrm{geom}}$. □

21. The special unitary group $\mathrm{PSU}_4(3)$

Theorem 21.1. *The local system $\mathcal{H}yp(\mathsf{Char}_7^\times; \xi_2)$ in characteristic $p = 3$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(7x) + V(-2x) \geq \frac{1}{2}.$$

Using the fact that $V(\frac{i}{14}) = V(\frac{13i}{3^6-1}) = \frac{1}{12}[13i]$ for $1 \leq i \leq 27$ we check that the inequality holds for $28x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$ and

$V(2x) = V(x) + V(x + \frac{1}{2}) - \frac{1}{2}$ [Ka7, §13], as

$$V(7x) \le V\left(x + \frac{1}{2}\right) + V(x).$$

Following §9, it suffices to prove

$$[7x] \le \left[x + \frac{3^r - 1}{2}\right] + [x] + 2$$

for every $r \ge 1$ and every $0 \le x \le 3^r - 1$. For $r \le 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
0,1	1	0,1	≥ 0	≥ 0	0	≥ 0
02	2	02	0	≥ 0	0	≥ 0
012,022	3	012,022	1	≥ 0	0	≥ 0
00212	5	00212	0	0	0	0
010212	6	010212	0	0	0	0
110212,210212	5	10212	-1	≥ 1	0	≥ 0
020212,220212	5	20212	0	≥ 0	0	≥ 0
02212,22212	4	2212	1	≥ 0	0	≥ 1

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c_2'$ corresponding to $\gamma_2 = 0$, since it is always 0).

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$
112	3	12	2	-1	-1	10	1
120212	6	12112	5	2	0	11	1
1212	4	201	3	0	0	11	1
12212	5	1212	4	1	0	11	1
122	3	20	2	2	0	11	1
222	3	22	2	3	2	20	1

□

Theorem 21.2. *The local system $\mathcal{H} = \mathcal{H}yp(\mathsf{Char}_7^\times; \xi_2)$ in characteristic $p = 3$ has geometric monodromy group $G_{\rm geom} = 6_1 \cdot \mathrm{PSU}_4(3)$. Furthermore, over any finite extension k of $\mathbb{F}_3$, the descent $\mathcal{S}_{7,2}$ of $\mathcal{H}$, see Proposition 7.2, has arithmetic monodromy group $G_{{\rm arith},k}$ equal to $G_{\rm geom}$ if $2|\deg(k/\mathbb{F}_3)$ and $G_{\rm geom} \cdot 2_2$ if $2 \nmid \deg(k/\mathbb{F}_3)$.*

Proof. (i) By Theorem 21.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(ii), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}(\sqrt{-3})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G,V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 6$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_6. \tag{21.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma.

Furthermore, as $\mathsf{o}(g_0) = 7$ for a p'-generator g_0 of the image of $I(0)$ in G, we have $C_7 \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is elementary abelian of order 3^4 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Also by Proposition 5.8(iii), a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has central order divisible by 5, i.e. $C_5 \hookrightarrow G/\mathbf{Z}(G)$. Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = \mathsf{A}_7$ or $\mathrm{PSL}_2(7)$. This case is ruled out since $\mathrm{Aut}(S) = S \cdot 2$ contains no subgroup of order 3^4.
- $(S, L) = (\mathrm{PSL}_3(4), 6 \cdot \mathrm{PSL}_3(4))$. This case is again ruled out since $\mathrm{Aut}(S)$ contains no subgroup of order 3^4.
- $(S, L) = (\mathrm{J}_2, 2 \cdot \mathrm{J}_2)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, a contradiction.
- $(S, L) = (\mathrm{PSU}_4(3), 6_1 \cdot \mathrm{PSU}_4(3))$. In this case, we have $\mathbf{Z}(G) = \mathbf{Z}(L) = C_6$ by (21.2.1). Since $7 \nmid |\mathrm{Out}(S)|$, the element g_0 of order 7 lies in the inverse image L of S in G, hence $G_{\mathrm{geom}} = L$ by Theorem 5.1.

(ii) Now we turn our attention to $H := G_{\mathrm{arith},k}$ of $\mathcal{S}_{7,2}$ (also see line 17 of Table 4). By Proposition 7.1(i), the field of traces for elements in H is still $\mathbb{Q}(\sqrt{-3})$ and so $\mathbf{Z}(H) = \mathbf{C}_H(G) = \mathbf{Z}(G) = C_6$. Recall that $H/\mathbf{Z}(H) \hookrightarrow \mathrm{Aut}(S) = S \cdot D_8$. Furthermore, if $H > G$ then $H = G \cdot 2_2$ since the central involution 2_1 of $\mathrm{Out}(S) = D_8$ does not preserve $\varphi|_G$, see [Atlas], and any subgroup of order 4 of $\mathrm{Out}(S)$ must contain 2_1. Thus $H/G \hookrightarrow C_2$. Next, Proposition 7.2 shows that $G_{\mathrm{arith},k}$ has determinant $(-1)^{\deg}$ while acting on $\mathcal{S}_{7,2}$. It follows that $H = G$ if $2|\deg(k/\mathbb{F}_3)$ and $H = G \cdot 2_2$ otherwise. ☐

Theorem 21.3. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_7^\times; \mathsf{Char}_4 \smallsetminus \{\mathbb{1}\})$ in characteristic $p = 3$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(7x) + V(-4x) \geq \frac{1}{2}.$$

Using the fact that $V(\frac{i}{28}) = V(\frac{26i}{3^6-1}) = \frac{1}{12}[26i]$ for $1 \leq i \leq 27$ we check that the inequality holds for $28x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$ and $V(2x) = V(x) + V(x + \frac{1}{2}) - \frac{1}{2}$ [Ka7, §13], as

$$V(7x) \leq V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right) + V\left(x + \frac{1}{2}\right) + V(x) - 1.$$

Following §9, it suffices to prove

$$[7x] \leq \left[x + \frac{3^r - 1}{4}\right] + \left[x + \frac{3(3^r - 1)}{4}\right] + \left[x + \frac{3^r - 1}{2}\right] + [x] - 2r + 1$$

for every $r \geq 1$ multiple of $r_0 = 2$ and every $0 \leq x \leq 3^r - 1$. Notice that, in this case, multiplication by 3 permutes $\gamma_1 = \frac{1}{4}$ and $\gamma_2 = \frac{1}{4}$ and fixes $\gamma_3 = \frac{1}{2}$ and $\gamma_4 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(3^2 - 1)\gamma_1 = 02_3$, $h_j = 2_3, 0_3, 1_3$ and $h_{2,j} = 02_3, 20_3, 11_3$ for $j = 1, 2, 3$ respectively. We will prove that

$$[7x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - 2r + 1$$

for every $r = 2k \geq 2$ and every $0 \leq x \leq 2^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. We will actually prove the following sharper inequality

$$[7x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - 2r$$

as long as the last two digits of x are not 12. If we split x as $3^s y + z$ then, for the induction step to work in the proof of the sharper inequality, we need $\Delta(s, z) - 2\sum_j v_j + 2\sum_i u_i \geq 1$ instead of 0 if the last two digits of y are 12 but the last two digits of x are not. Moreover, if the last two digits of x are 12 but those of y are not, then it suffices with $\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i \geq -1$.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
0	1	0	1	0	0	1
01,11	1	1	0	≥ 0	0	≥ 0
02	1	2	1	≥ 0	0	≥ 1
0021,1021	3	021	0	≥ 0	0	≥ 0
012	3	012	2	≥ 0	0	≥ 2
0112	3	112	1	≥ 0	0	≥ 1
01212,12212,21212,22212	3	212	0	≥ 1	≤ 1	≥ 0
00212	5	00212	0	0	0	0
010212	6	010212	0	0	0	0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4 = c_4'$ corresponding to $\gamma_6 = 0$, since it is always 0). Here, in order to prove the sharper inequality, if the last two digits of z are 12 but those of z' are not, we need $\Delta(s', z') \leq \Delta(s,z) + 1$. If the last two digits of z' are 12 but those of z are not, we need $\Delta(s', z') \leq \Delta(s,z) - 1$.

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
2021	4	212	3	1	0	12	1	1	1
121	3	20	2	3	2	11	1	0	1
0221	4	1	1	3	0	2	0	1	0
1221	4	20	2	4	2	11	0	1	1
2221	4	221	3	5	4	20	1	1	1
1112	4	112	3	1	1	10	0	1	1
2112	4	212	3	0	0	12	1	1	1
110212	6	11021	5	3	4	10	0	1	0
210212	6	21021	5	0	1	12	1	1	1
20212	5	2021	4	0	1	12	1	1	1
11212	5	1120	4	2	2	10	1	0	1
02212	5	1000	4	2	3	2	1	0	0
022	3	10	2	3	1	2	1	0	0
122	3	20	2	4	2	11	1	0	1
222	3	221	3	5	4	20	1	1	1

□

Theorem 21.4. *The local system $\mathcal{H} = \mathcal{H}yp(\mathsf{Char}_7^\times; \mathsf{Char}_4 \smallsetminus \{\mathbb{1}\})$ in characteristic $p = 3$ has geometric monodromy group $G_{\mathrm{geom}} = 6_1 \cdot \mathrm{PSU}_4(3)$. Furthermore, over any finite extension k of $\mathbb{F}_3$, the descent $\mathcal{S}_{7,4}$ of $\mathcal{H}$, see Proposition 7.2, has arithmetic monodromy group $G_{\mathrm{arith},k}$ equal to G_{geom} if $2|\deg(k/\mathbb{F}_3)$ and $G_{\mathrm{geom}} \cdot 2_2$ if $2 \nmid \deg(k/\mathbb{F}_3)$.*

Proof. (i) By Theorem 21.3, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(ii), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}(\sqrt{-3})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies ($\mathbf{S}$+). As $D = \dim(V) = 6$, G

must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3})$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_6. \tag{21.4.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 7$ for a p'-generator g_0 of the image of $I(0)$ in G, we have $C_7 \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is non-abelian of order divisible by 3^3 by Proposition 5.9(ii), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

• $S = \mathsf{A}_7$ or $\mathrm{PSL}_2(7)$. This case is ruled out since $\mathrm{Aut}(S) = S \cdot 2$ contains no subgroup of order 3^3.

• $S = L = \mathrm{SU}_3(3)$. Since $7 \nmid |\mathrm{Out}(S)|$, the element g_0 of order 7 lies in the inverse image $S \times \mathbf{Z}(G)$ of S in G, whence $g_0 \in S$ by (21.4.1). It follows that $G_{\mathrm{geom}} = S$ by Theorem 5.1. But this is a contradiction since $\mathbb{Q}(\varphi)$ would have been $\mathbb{Q}$ in this case.

• $(S, L) = (\mathrm{PSL}_3(4), 6 \cdot \mathrm{PSL}_3(4))$. In this case, we have $\mathbf{Z}(G) = \mathbf{Z}(L) = C_6$ by (21.4.1). Since $7 \nmid |\mathrm{Out}(S)|$, the element g_0 of order 7 lies in the inverse image L of S in G, hence $G_{\mathrm{geom}} = L$ by Theorem 5.1. Now using [GAP] we can check that the restriction of φ to $2'$-elements of G yields a reducible 2-Brauer character. But this is a contradiction, since a reduction modulo $\ell = 2$ of the representation Φ is absolutely irreducible by Theorem 6.12.

• $(S, L) = (\mathrm{J}_2, 2 \cdot \mathrm{J}_2)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, a contradiction.

• $(S, L) = (\mathrm{PSU}_4(3), 6_1 \cdot \mathrm{PSU}_4(3))$. In this case, we have $\mathbf{Z}(G) = \mathbf{Z}(L) = C_6$ by (21.4.1). Since $7 \nmid |\mathrm{Out}(S)|$, the element g_0 of order 7 lies in the inverse image L of S in G, hence $G_{\mathrm{geom}} = L$ by Theorem 5.1.

(ii) To determine $G_{\mathrm{arith},k}$ we can use the same arguments of the final paragraph of Theorem 21.2, with either one of the two descents listed in Table 4, line 18. ☐

22. The symplectic group $\mathrm{Sp}_6(2)$

Theorem 22.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_5 \sqcup \mathsf{Char}_3^\times; \xi_2)$ in characteristic $p = 7$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(3x) + V(5x) - V(x) + V\left(-x - \frac{1}{2}\right) \geq \frac{1}{2}.$$

Using the fact that $V(\frac{i}{30}) = V(\frac{80i}{7^4-1}) = \frac{1}{24}[80i]$ for $1 \leq i \leq 29$ we check that the inequality holds for $30x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$, as

$$V(3x) + V(5x) \leq V\left(x + \frac{1}{2}\right) + V(x) + \frac{1}{2}.$$

Following §9, it suffices to prove

$$[3x] + [5x] \leq \left[x + \frac{7^r - 1}{2}\right] + [x] + 3r + 6$$

for every $r \geq 1$ and every $0 \leq x \leq 7^r - 1$. For $r \leq 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x:

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 6\sum_j v_j + 6\sum_i u_i$
0,1,2,3	1	0,1,2,3	≥ 0	≥ 0	0	≥ 0
$a4, a5, a6; a = 0, 1, 2$	2	$a4, a5, a6$	≥ 0	≥ 0	0	≥ 0
44	1	4	-6	≥ 1	0	≥ 0
$a54, a64; a = 0, 1, 2$	3	$a54, a64$	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c'_2$ corresponding to $\gamma_2 = 0$, since it is always 0).

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$b_2 = b'_2$	$c_1 = c'_1$
34,35,36	2	4	1	≥ -6	-6	1	2	1
354,364	3	34	2	-6	-6	1	2	1
454,464	3	51	2	0	0	2	3	1
554,564,654,664	3	64	2	≥ -6	-6	2	4	1
45,46	2	5	1	6	0	2	3	1
55,56,65,66	2	6	1	≥ 0	0	2	4	1

$\square$

Theorem 22.2. (i) *The local system $\mathcal{H} = \mathcal{H}yp(\mathsf{Char}_5 \sqcup \mathsf{Char}_3^\times; \xi_2)$ in characteristic $p = 7$ has geometric monodromy group $G_{\mathrm{geom}} = \mathrm{Sp}_6(2)$.*

(ii) *The sheaf $\mathcal{H}_1 := \mathcal{H} \otimes \mathcal{L}_{\xi_2}$ has geometric monodromy group $G_{\mathrm{geom},\mathcal{H}_1} = \mathrm{Sp}_6(2) \times C_2$. Furthermore, $\mathcal{H}_1$ has a descent $\mathcal{H}'_1$ to $\mathbb{F}_7$ with arithmetic monodromy group $G_{\mathrm{arith},k,\mathcal{H}'_1} = G_{\mathrm{geom},\mathcal{H}_1}$ over any finite extension k of $\mathbb{F}_7$.*

Proof. (i) By Theorem 22.1, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies ($\mathbf{S}+$). Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{22.2.1}$$

Also, $\bar{\mathsf{o}}(g_0) = 15$ for a p'-generator g_0 of the image of $I(0)$ in G, and so $C_{15} \hookrightarrow G/\mathbf{Z}(G)$. Now, if we are in case (c) of Lemma 3.1, then G contains an irreducible 7-subgroup E of order 7^3 with $\mathbf{C}_G(E) = \mathbf{Z}(G)$ and $G/\mathbf{Z}(G)$ embeds in $7^2 \cdot \mathrm{SL}_2(7)$. It follows from (22.2.1) that $5 \nmid |G|$, a contradiction. Hence, G must be almost quasisimple by Lemma 3.1.

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Now we can apply the main result of [HM] to arrive at the following two possibilities for (S, L).

- $S = L = \mathsf{A}_8$. Since $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(S)$ and 15 is coprime to $|\mathrm{Out}(S)|$, the element g_0 of order 15 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G. Using (22.2.1), we then see that $g_0 \in S$, and so $G = S$ by Theorem 5.1. Thus $G \cong \mathrm{SL}_4(2)$, and so $\dim \mathsf{Wild} \leq 4$ by [KT5, Theorem 4.14], a contradiction.
- $S = L = \mathrm{Sp}_6(2)$. Again, since 15 is coprime to $|\mathrm{Out}(S)|$ and $|\mathbf{Z}(G)|$, the element g_0 of order 7 must lie in S, hence $G_{\mathrm{geom}} = S$ by Theorem 5.1.

(ii) By Theorem 7.5, $\mathcal{H}_1$ has a descent $\mathcal{H}'_1 = (\mathcal{H}_1)_{00}$ to $\mathbb{F}_7$, for which any element in $G_{\mathrm{arith},k,\mathcal{H}'_1}$ still has trace in $\mathbb{Q}$ over any finite extension k of $\mathbb{F}_7$, with $(\mathcal{H}_1)_0$ given in Table 4, line 19. Hence,

$\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_1}) \le \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_1'}) \le C_2$. Next, if $\tilde{g}_0$ generates the image of $I(0)$ in $G_1 := G_{\mathrm{geom},\mathcal{H}_1}$, then note that $\tilde{g}_0^{15}$ acts as the scalar -1 on $\mathcal{H}_1$, whence we now have

$$\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_1}) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_1'}) = C_2.$$

By Lemma 5.12, $G_1/\mathbf{Z}(G_1) \cong G/\mathbf{Z}(G) = S$, and $G_1^{(\infty)} = G^{(\infty)} \cong S$. Next, since S already induces the full automorphism group of $S \lhd G_{\mathrm{arith},k,\mathcal{H}_1'}$, we conclude that

$$G_{\mathrm{arith},k,\mathcal{H}_1'} = G_{\mathrm{geom},\mathcal{H}_1} = \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_1})S = \mathrm{Sp}_6(2) \times C_2.$$

□

Theorem 22.3. *The local system $\mathcal{H}_2 := \mathcal{H}yp(\mathsf{Char}_{15}^{\times}; \mathsf{Char}_2)$ in characteristic $p = 7$ has geometric monodromy group $G_{\mathrm{geom},\mathcal{H}_2} = 2 \cdot \mathrm{Sp}_6(2)$. Moreover, $\mathcal{H}_2$ has a descent $\mathcal{H}_2'$ to $\mathbb{F}_7$ with arithmetic monodromy group $G_{\mathrm{arith},k,\mathcal{H}_2'} = G_{\mathrm{geom},\mathcal{H}_2}$ over any finite extension k of $\mathbb{F}_7$.*

Proof. (i) The sheaf $\mathcal{H}$ in Theorem 22.2 gives rise to a surjection $\phi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow S = \mathrm{Sp}_6(2)$ together with an irreducible representation $\Phi : S \to \mathrm{GL}_6(\overline{\mathbb{Q}_\ell})$. Also, consider the surjection

$$\pi : \hat{S} = 2 \cdot \mathrm{Sp}_6(2) \twoheadrightarrow S$$

with kernel $\mathrm{Ker}(\pi) \cong C_2$. The obstruction to lifting ϕ to a homomorphism $\varpi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \to \hat{S}$ lies in the group $H^2(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathrm{Ker}(\pi)) = 0$, the vanishing because open curves have cohomological dimension ≤ 1, cf. [SGA, Cor. 2.7, Exp. IX and Thm. 5.1, Exp. X]. Since $\hat{S}$ contains no subgroup isomorphic to S, we conclude that ϖ is also surjective. Now we can inflate Φ to a representation $\hat{\Phi}$ of $\hat{S}$ with kernel C_2. We also consider the faithful 8-dimensional representation $\Psi : \hat{S} \to \mathrm{GL}_8(\overline{\mathbb{Q}_\ell})$ and note that

$$\mathrm{Trace}(\Psi(h)) = 1 + \mathrm{Trace}(\hat{\Phi}(h))$$

for all 7-elements $h \in \hat{S}$. Applying [KT5, Theorem 5.1], we now see that $\Psi \circ \varpi$ gives rise to a hypergeometric sheaf $\tilde{\mathcal{H}}$ of type $(8, 2)$, still in characteristic $p = 7$, with C_7 being the image of $P(\infty)$, and with

$$G_{\mathrm{geom},\tilde{\mathcal{H}}} \cong \Psi(\hat{S}) \cong \hat{S}. \tag{22.3.1}$$

Let g_0 be a p'-generator of the image of $I(0)$ in S and let g_∞ be a p'-generator of $I(\infty)$ modulo $P(\infty)$ in S. Also, let $h_0 \in \hat{S}$, respectively $h_\infty \in \hat{S}$ be an inverse image of g_0, respectively of g_∞. The shape of $\mathcal{H}$ tells us by Proposition 5.8 that the spectrum of $\hat{\Phi}(h_\infty) = \Phi(g_\infty)$ consists of all 6^{th} roots of some $\alpha \in \mathbb{C}^\times$ and -1 (counting multiplicities). Thus $6|\mathsf{o}(h_\infty)$ and it has trace -1 in $\hat{\Phi}$. It follows that h_∞ belongs to class $6g$ or $6h$ in the notation of [GAP]. Likewise, the spectrum of $\Psi(h_\infty)$ consists of all 6^{th} roots of some $\beta \in \mathbb{C}^\times$ and two more roots of unity $\gamma \ne \delta \in \mathbb{C}^\times$ (counting multiplicities). Using [GAP] we can now see that $\beta = 1$ and $\{\gamma, \delta\} = \{1, -1\}$, which means that the two "downstairs" characters of $\tilde{\mathcal{H}}$ are $\mathbb{1}$ and ξ_2. Next, $15|\mathsf{o}(h_0)$, so h_0 belongs to class $15a$ or $30a$ in the notation of [GAP], and so inspecting the spectrum of $\Psi(h_0)$ we see that the "upstairs" characters of $\tilde{\mathcal{H}}$ are either $X_1 := \mathsf{Char}_{15}^{\times}$, or $X_2 := \mathsf{Char}_{30}^{\times} = \xi_2 \cdot X_1$. We conclude that either

$$\tilde{\mathcal{H}} \cong \mathcal{H}_2, \tag{22.3.2}$$

or

$$\tilde{\mathcal{H}} \cong \mathcal{H}_2 \otimes \mathcal{L}_{\xi_2}. \tag{22.3.3}$$

Because of (22.3.1), we are certainly done in the case of (22.3.2). Suppose we are in the case of (22.3.3) and thus $G_{\mathrm{geom},\mathcal{H}_2 \otimes \mathcal{L}_{\xi_2}} = \hat{S}$ by (22.3.1). Now we consider $H := G_{\mathrm{geom},\mathcal{H}_2}$. By Lemma 5.12, $H/\mathbf{Z}(H) \cong \hat{S}/\mathbf{Z}(\hat{S}) = S$ and $H^{(\infty)} \cong \hat{S}^{(\infty)} = \hat{S}$. Also, the field of traces for $\mathcal{H}_2$ is again $\mathbb{Q}$ by

Corollary 6.2(i), hence we have $\mathbf{Z}(H) \le C_2$. We conclude that $H \cong 2 \cdot \mathrm{Sp}_6(2)$, and so we again have $G_{\mathrm{geom},\mathcal{H}_2} \cong 2 \cdot \mathrm{Sp}_6(2)$.

(ii) By Theorem 7.5, $\mathcal{H}_2$ has a descent $\mathcal{H}_2' = (\mathcal{H}_2)_{00}$ to $\mathbb{F}_7$, for which any element in $G_{\mathrm{arith},k,\mathcal{H}_2'}$ still has trace in $\mathbb{Q}$ over any finite extension k of $\mathbb{F}_7$, with $(\mathcal{H}_2)_0$ given in Table 4, line 20. Hence, $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_2'}) = \mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_2'}}(G_{\mathrm{geom},\mathcal{H}_2}) = \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_2}) = C_2$. As $\mathrm{Out}(S) = 1$ [Atlas], we conclude that $G_{\mathrm{arith},k,\mathcal{H}_2'} = G_{\mathrm{geom},\mathcal{H}_2}$. □

23. The orthogonal group $\Omega_8^+(2)$

Theorem 23.1. *The local system* $\mathcal{K}l(\mathsf{Char}_9^\times \sqcup \mathsf{Char}_2)$ *in characteristic* $p = 5$ *has finite geometric monodromy group.*

Proof. We need to show:
$$V(2x) + V(9x) - V(3x) \ge 0.$$
Using the fact that $V(\frac{i}{18}) = V(\frac{868i}{5^6-1}) = \frac{1}{24}[868i]$ for $1 \le i \le 17$ we check that the inequality holds for $18x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \ne 0$ and $V(3x) = V(x) + V(x + \frac{1}{3}) + V(x + \frac{2}{3}) - 1$ [Ka7, §13], as
$$V(2x) + V(9x) \le V\left(x + \frac{1}{3}\right) + V\left(x + \frac{2}{3}\right) + V(x).$$
Following §9, it suffices to prove
$$[2x] + [9x] \le \left[x + \frac{5^r - 1}{3}\right] + \left[3x + \frac{2(5^r - 1)}{3}\right] + [x]$$
for every $r \ge 1$ multiple of $r_0 = 2$ and every $0 \le x \le 5^r - 1$. Notice that, in this case, multiplication by 5 permutes $\gamma_1 = \frac{1}{3}$ and $\gamma_2 = \frac{2}{3}$ and fixes $\gamma_3 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2 - 1)\gamma_1 = 13_5$, $h_1 = 3$, $h_2 = 1$ and $h_{2,j} = 13_2, 31_2$ for $j = 1, 2$ respectively. For $\gamma_3 = 0$ it is clear that $h_3 = h_{r,3} = 0$ for every r. We will prove that
$$[2x] + [9x] \le [x + h_{r,1}] + [x + h_{r,2}] + [x]$$
for every $r \ge 1$ and every $0 \le x \le 5^r - 1$. For $r \le 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x:

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1	1	0,1	≥ 0	≥ 0	0	≥ 0
$a2, a3; a \ne 3$	1	2,3	0	≥ 0	0	≥ 0
$a4; a \ne 1, 3$	1	4	4	≥ 0	0	≥ 4
$a32, a33, a34; a \ne 1, 3$	2	32,33,34	8	≥ 0	0	≥ 8

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_3 = c_3'$ corresponding to $\gamma_3 = 0$, since it is always 0).

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$b_2 = b_2'$	$c_1 = c_1'$	$c_2 = c_2'$
132,133,134	3	14	2	8	4	0	3	1	0
332,333,334	3	33	2	12	8	1	11	1	1
14	2	2	1	4	0	0	3	0	1

□

Theorem 23.2. *The local system $\mathcal{K}l(\mathsf{Char}_7 \sqcup \{\xi_2\})$ in characteristic $p = 5$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(2x) + V(7x) - V(x) \geq 0.$$

Using the fact that $V(\frac{i}{14}) = V(\frac{1116i}{5^6-1}) = \frac{1}{24}[1116i]$ for $1 \leq i \leq 13$ we check that the inequality holds for $14x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$, as

$$V(2x) + V(7x) \leq V(x) + 1.$$

Following §9, it suffices to prove

$$[2x] + [7x] \leq [x] + 4r + 4$$

for every $r \geq 1$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 5$ we check it by computer. For $r > 5$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x:

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1,3,4	1	0,1,3,4	≥ 0	≥ 0	0	≥ 0
02,42	2	02,42	0	≥ 0	0	≥ 0
012	3	012	0	≥ 0	0	≥ 0
0412,3412	4	0412,3412	0	≥ 0	0	≥ 0
$a2412; a \neq 3$	5	$a2412$	0	≥ 0	0	≥ 0
04412,24412,34412	5	04412,24412,34412	0	≥ 0	0	≥ 0
22	1	2	-4	≥ 1	0	≥ 0
32	3	$a32$	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_1 = c_1'$ corresponding to $\gamma_1 = 0$, since it is always 0).

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$b_2 = b_2'$
112	3	12	2	-4	-4	0	1
212	3	22	2	-4	-4	0	3
312	3	32	2	-4	-4	1	4
1412	4	202	3	-4	-4	0	2
32412	5	3222	4	-4	-4	1	4
14412	5	1412	4	-4	-4	0	2
44412	5	4412	4	-4	-4	1	11

□

Theorem 23.3. *Each of the two hypergeometric sheaves $\mathcal{K}_1 := \mathcal{K}l(\mathsf{Char}_9^\times \sqcup \mathsf{Char}_2)$ and $\mathcal{K}_2 := \mathcal{K}l(\mathsf{Char}_7 \sqcup \{\xi_2\})$, both in characteristic $p = 5$, has geometric monodromy group $G_{\mathrm{geom}} = 2 \cdot \Omega_8^+(2) \cdot 2$, with $G_{\mathrm{geom}}/\mathbf{Z}(G_{\mathrm{geom}}) \cong \mathrm{O}_8^+(2)$. Furthermore, each $\mathcal{K}_i$ with $i = 1, 2$ has a descent $\mathcal{K}_i'$ to $\mathbb{F}_5$ with arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ over any finite extension k of $\mathbb{F}_5$.*

Proof. (i) By Theorems 23.1 and 23.2, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{K}_i$ with $i = 1$ or 2. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, since $\mathcal{K}_i$ is Kloosterman, it is not Belyi induced. Hence, by Theorem 3.3, (G,V) satisfies $(\mathbf{S}+)$. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi)=\mathbb{Q}$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{23.3.1}$$

Also, $e := \bar{\mathsf{o}}(g_0) = 18$, respectively 14, for a p'-generator g_0 of the image of $I(0)$ in G, and so $C_e \hookrightarrow G/\mathbf{Z}(G)$. Moreover, the image Q of $P(\infty)$ is elementary abelian of order 5^2 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(ii). Now, if we are in case (c) of Lemma 3.1, then G contains an irreducible 2-subgroup E of order 2^7 with $\mathbf{C}_G(E) = \mathbf{Z}(G)$ and $G/\mathbf{Z}(G)$ embeds in $2^6 \cdot \mathrm{Sp}_6(2)$. It follows from (23.3.1) that $5^2 \nmid |G|$, a contradiction. Hence, G must be almost quasisimple by Lemma 3.1.

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma, and furthermore $\mathbf{Z}(G) \leq C_2$ by (23.3.1). Now we can apply the main result of [HM] to arrive at the only possibility $(S,L) = (\Omega_8^+(2), 2\cdot\Omega_8^+(2))$; in particular $\mathbf{Z}(G) = \mathbf{C}_G(L) = \mathbf{Z}(L) = C_2$ by (23.3.1). Using [GAP] we can now check that no element of central order divisible by 7 in L can have simple spectrum in Φ. Hence, when $i=2$ we must have that $g_0 \notin L$. Furthermore, if $u \in L$ has central order divisible by 9 and simple spectrum in Φ, then it has trace ± 1. As $\mathrm{Trace}(\Phi(g_0)) = 0$ for $i=1$, we also have $g_0 \notin L$ when $i=1$ as well. Thus in both cases, $g_0 \notin L$ and so $G > L$. In particular, the subgroup $G/\mathbf{Z}(G)$ of $\mathrm{Aut}(S) = S \cdot \mathsf{S}_3$ contains S properly. As the (unique) 8-dimensional faithful representation of L is not invariant under an outer automorphism of order 3, we conclude that $G = L\cdot 2$, with $G/\mathbf{Z}(G) = S\cdot 2 \cong \mathrm{O}_8^+(2)$, as stated.

(ii) By Theorem 7.5, $\mathcal{K}_i$ has a descent $\mathcal{K}'_i = (\mathcal{K}_i)_{00}$ to $\mathbb{F}_5$, for which any element in $G_{\mathrm{arith},k,\mathcal{K}'_i}$ still has trace in $\mathbb{Q}$ over any finite extension k of $\mathbb{F}_5$, with $(\mathcal{K}_i)_0$ given in Table 4, line 21 (where we can use either one of the two given choices) for $i=1$ and line 22 for $i=2$. Hence, we now have $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{K}'_i}) = \mathbf{C}_{G_{\mathrm{arith},k,\mathcal{K}'_i}}(L) = \mathbf{Z}(L) = C_2$. As $\mathrm{Out}(S) = \mathsf{S}_3$ [Atlas] and the (unique) 8-dimensional faithful representation of L is not invariant under any outer automorphism of order 3, we have that $G_{\mathrm{arith},k,\mathcal{K}'_i}/\mathbf{Z}(L) = S\cdot 2 = G_{\mathrm{geom}}/\mathbf{Z}(L)$, and so $G_{\mathrm{arith},k,\mathcal{K}'_i} = G_{\mathrm{geom}}$. $\square$

24. The exceptional group $G_2(3)$

Theorem 24.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{18} \smallsetminus \{\mathbb{1}, \xi_6, \xi_6^2, \xi_6^3\}; \xi_4, \bar{\xi}_4)$ in characteristic $p = 13$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(18x) - V(x) - V\left(x+\frac{1}{6}\right) - V\left(x+\frac{2}{6}\right) - V\left(x+\frac{3}{6}\right) + V(-4x) - V(-2x) + 2 \geq 0$$

and

$$V(18x) - V(x) - V\left(x-\frac{1}{6}\right) - V\left(x-\frac{2}{6}\right) - V\left(x-\frac{3}{6}\right) + V(-4x) - V(-2x) + 2 \geq 0.$$

The change of variable $x \mapsto x + \frac{1}{2}$ interchanges both inequalities, so it is enough to prove the second one. Using the fact that $V(\frac{i}{18}) = V(\frac{122i}{13^3-1}) = \frac{1}{36}[122i]$ for $1 \leq i \leq 17$ we check that the inequality holds for $18x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x)+V(-x)=1$ for $x \neq 0$ and $V(2x) = V(x) + V(x+\frac{1}{2}) - \frac{1}{2}$ [Ka7, §13], as

$$V(18x) \leq V\left(x+\frac{1}{6}\right) + V\left(x+\frac{2}{6}\right) + V\left(x+\frac{3}{6}\right) + V\left(x+\frac{1}{4}\right) + V\left(x+\frac{3}{4}\right) + V(x) - 2$$

and, following §9, it suffices to prove

$$[18x] \le \left[x + \frac{13^r-1}{6}\right] + \left[x + \frac{2(13^r-1)}{6}\right] + \left[x + \frac{3(13^r-1)}{6}\right] + \left[x + \frac{13^r-1}{4}\right] + \left[x + \frac{3(13^r-1)}{4}\right] + [x] - 24r$$

for every $r \ge 1$ and every $0 \le x \le 13^r - 1$. For $r \le 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. We denote the 13-adic digits by 0,1,2,3,4,5,6,7,8,9,A,B,C.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 12\sum_j v_j + 12\sum_i u_i$
0,1,2,3	1	0,1,2,3	≥ 0	≥ 0	0	≥ 0
$a4, a5, a6; a \ne 3$	1	4,5,6	≥ 0	≥ 0	0	≥ 0
$a34; a \ne 3$	2	34	0	≥ 0	0	≥ 0
$a7, a8; a \ne 3, 6$	1	7,8	≥ 0	≥ 0	0	≥ 0
$a9; a \ne 3, 6, 8$	1	9	0	≥ 0	0	≥ 0
$a\mathrm{A}; a \ne 3, 6, 8, 9$	1	A	0	≥ 0	0	≥ 0
$a\mathrm{B}, a\mathrm{C}; a \ne 3, 6, 8, 9, \mathrm{A}$	1	B,C	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_6 = c_6'$ corresponding to $\gamma_3 = 6$, since it is always 0; also we have $b_1 = b_1'$, $c_1 = c_1'$, $c_2 = c_2'$, $c_3 = c_3'$, $c_4 = c_4'$, and $c_5 = c_5'$):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	b_1	c_1	c_2	c_3	c_4	c_5
334	3	34	2	0	0	4	0	0	0	0	1
35,36,37	2	34	2	≥ 0	0	4	0	0	0	0	1
38,39,3A,3B,3C	2	4	1	≥ 0	0	5	0	0	0	0	1
67,68,69,6A,6B,6C	2	7	1	≥ 0	0	9	0	0	1	0	1
89,8A,8B,8C	2	9	1	≥ 0	0	C	0	1	1	0	1
9A,9B,9C	2	A	1	0	0	10	0	1	1	1	1
AB,AC	2	B	1	0	0	12	1	1	1	1	1

□

Theorem 24.2. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{18} \smallsetminus \{\mathbb{1}, \xi_6, \xi_6^2, \xi_6^3\}; \xi_4, \bar{\xi}_4)$ in characteristic $p = 13$ has geometric monodromy group $G_{\mathrm{geom}} = \mathrm{Aut}(G_2(3)) = G_2(3) \cdot 2$. Furthermore, $\mathcal{H}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_{13}$, which over any extension k of $\mathbb{F}_{13^4}$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.*

Proof. (i) By Theorem 24.1, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains $\sqrt{-3}$; indeed, a generator g_0 of the image of $I(0)$ in G has trace

$$\varphi(g_0) = -(1 + \zeta_6 + \zeta_6^2 + \zeta_6^3) = -\sqrt{-3}.$$

In fact, applying Proposition 6.1(iii) we see that $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G, V) satisfies ($\mathbf{S}$+). As $D = \dim(V) = 14$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$

acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-3})$, we have that $\mathbf{Z}(G) \hookrightarrow C_6$. In fact, as $\mathcal{H}$ has rank 14 and geometric determinant $\mathcal{L}_{\xi_2}$, it follows that

$$\mathbf{Z}(G) \hookrightarrow C_2, \text{ and } G \neq [G,G]. \tag{24.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 18$ we have $C_{18} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is cyclic of order 13 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = L = \mathsf{A}_{15}$, and $V|_L$ is just the deleted permutation module $S^{(14,1)}|_L$. Since $\varphi(g_0) = -\sqrt{-3}$, not an integer multiple of a root of unity, this case is rule out by Lemma 3.8.
- $S = \mathrm{PSL}_2(13)$ or $\mathrm{PSL}_2(27)$. These two cases are impossible since $\mathrm{Aut}(S)$ contains no element of order 18.
- $S = L = {}^2B_2(8)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(i)$, again a contradiction.
- $(S, L) = (\mathrm{PSp}_6(3), \mathrm{Sp}_6(3)$. Here we have that $\mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L) = C_2$ by (24.2.1). Furthermore, $G/\mathbf{Z}(G) = S$ since the outer automorphism of S does not fix the equivalence of any irreducible Weil representation of degree 14 of L. Thus $G = L$. Now, using [GAP] we can check that any element of order 18 in L with trace $\pm\sqrt{-3}$ belongs to classes $18q$, $18r$, $18s$, and $18t$ in the notation of [GAP], and no such element can have simple spectrum in the underlying representation. This contradicts the existence of the element g_0.
- $S = L = G_2(3)$. Recall that we have $\mathbf{Z}(G) = \mathbf{C}_G(S) \leq C_2$ by (24.2.1). Furthermore, the element g_0 of central order 18 does not lie in $\mathbf{Z}(G)S \lhd G$, hence $G > L$. Now $S < G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 2$, and so $G = (\mathbf{Z}(G) \times S) \cdot 2$. Now, $Q \cong C_{13}$ is contained in S, and so G/S is cyclic by Theorem 5.3. It follows that $\mathbf{Z}(G) = 1$ and $G_{\mathrm{geom}} = G_2(3) \cdot 2$.

(ii) For $\mathcal{H}'$, by Theorem 7.5 we can take the sheaf listed in Table 4, line 23. Over any finite extension k of $\mathbb{F}_{13^2}$, it has $\mathbb{Q}(\sqrt{-3})$ as the field of traces, hence $\mathbf{Z}(G_{\mathrm{arith},k}) \hookrightarrow C_6$. Next, $\mathbf{C}_{G_{\mathrm{arith},k}}(S) = \mathbf{Z}(G_{\mathrm{arith},k})$, and G_{geom} already induces the full automorphism group of S and has trivial center. Hence $G_{\mathrm{arith},k}/\mathbf{Z}(G_{\mathrm{arith},k}) \cong G_{\mathrm{geom}}$, and so $G_{\mathrm{arith},k} = \mathbf{Z}(G_{\mathrm{arith},k})G_{\mathrm{geom}}$ and $G_{\mathrm{arith},k}/G_{\mathrm{geom}} \cong \mathbf{Z}(G_{\mathrm{arith},k})$. Thus, modulo G_{geom}, any element in $G_{\mathrm{arith},k}$ is $z^{\deg(k/\mathbb{F}_{13^2})}$ for some generator z of $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_{13^2}})$. In particular, if $v \in \mathbb{F}_{13^2}$, then $Frob_{v,\mathbb{F}_{13^2}} = zh_v$ for some $h_v \in G_{\mathrm{geom}}$. Now, a computation using [Mag] reveals that, for some $v \in \mathbb{F}_{13^2}$, $Frob_{v,\mathbb{F}_{13^2}}$ has trace 2. On the other hand, z acts on $\mathcal{H}'$ as a 6^{th} root of unity $\alpha \in \mathbb{C}$, and the only such α for which $2\alpha^{-1}$ occurs as the trace of $h_v \in G_{\mathrm{geom}}$ is ± 1, see [GAP]. It follows that $\mathsf{o}(z) = \mathsf{o}(\alpha) \leq 2$. In particular, $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$ when $k \supseteq \mathbb{F}_{13^4}$. $\square$

25. The exceptional group $G_2(4)$ and its subgroup $\mathrm{SU}_3(4)$

Theorem 25.1. *The local system $\mathcal{H}yp(\mathsf{Char}_{13}^{\times}; \mathsf{Char}_3^{\times})$ in characteristic $p = 2$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(13x) + V(-3x) \geq \frac{1}{2}$$

Using the fact that $V(\frac{i}{39}) = V(\frac{105i}{2^{12}-1}) = \frac{1}{12}[105i]$ for $1 \leq i \leq 38$ we check that the inequality holds for $39x \in \mathbb{Z}$. For all other values of x, we can rewrite it as

$$V(13x) \leq V\left(x + \frac{1}{3}\right) + V\left(x + \frac{2}{3}\right) + V(x) - \frac{1}{2}$$

and, following §9, it suffices to prove

$$[13x] \le \left[x + \frac{2^r - 1}{3}\right] + \left[x + \frac{2(2^r - 1)}{3}\right] + [x] - \frac{r}{2} + \frac{3}{2}$$

for every $r \ge 1$ divisible by $r_0 = 2$ and every $0 \le x \le 2^r - 1$. Notice that, in this case, multiplication by 2 permutes $\gamma_1 = \frac{1}{3}$ and $\gamma_2 = \frac{2}{3}$ and fixes $\gamma_3 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(2^2 - 1)\gamma_1 = 01_2$, $h_j = 1, 0$ and $h_{2,j} = 01, 10$ for $j = 1, 2$ respectively. We will prove that

$$[13x] \le [x + h_{r,1}] + [x + h_{r,2}] + [x] - \frac{r}{2} + \frac{3}{2}$$

for every $r \ge 1$ and every $0 \le x \le 2^r - 1$. For $r \le 12$ we check it by computer. For $r > 12$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
0	1	0	$1/2$	0	0	$\ge 1/2$
01	2	01	0	≥ 0	0	≥ 0
0011	4	0011	0	≥ 0	0	≥ 0
00011011	8	00011011	0	≥ 0	0	≥ 0
0010011011	10	0010011011	0	≥ 0	0	≥ 0
1010011011	8	10011011	-1	≥ 2	0	≥ 1
1011011	2	11	0	≥ 2	2	≥ 0
0000111011	10	0000111011	0	≥ 0	0	≥ 0
1000111011,1100111011	8	00111011	-1	≥ 1	0	≥ 0
000100111011	12	000100111011	0	≥ 0	0	≥ 0
$ab0100111011; ab \ne 00$	10	0100111011	-1	≥ 3	0	≥ 2
10111011,11111011	4	1011	0	≥ 1	1	≥ 0
00111	5	00111	$1/2$	≥ 0	0	$\ge 1/2$
1111	2	11	0	≥ 2	1	≥ 1

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_3 = c_3'$ corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$
01011	5	011	3	$-1/2$	$-1/2$	100	1	0
110011011	9	1101011	7	$3/2$	$-1/2$	1010	1	1
01111011	8	1000011	7	1	$1/2$	110	0	1
010111	6	011	3	1	$-1/2$	100	0	1
110111	6	111	3	2	$1/2$	1011	1	1

□

Theorem 25.2. *The local system* $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{13}^{\times}; \mathsf{Char}_3^{\times})$ *in characteristic* $p = 2$ *has geometric monodromy group* $G_{\rm geom} = 2 \cdot G_2(4)$*. Moreover, over any finite extension* k *of* $\mathbb{F}_4$*, the descent* $\mathcal{S}_{13,3}$ *of* $\mathcal{H}$ *has arithmetic monodromy group* $G_{{\rm arith},k} = G_{\rm geom}$*.*

Proof. (i) By Theorem 25.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(ii), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}$, and φ has Frobenius-Schur indicator -1 by [Ka4, 8.8.1, 8.8.2] (i.e. $\mathcal{H}$ is symplectically self-dual). It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.6, (G, V) satisfies $(\mathbf{S}+)$. As $D = \dim(V) = 12$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{25.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, for a generator g_0 of the image of $I(0)$ in G we have $\bar{\mathsf{o}}(g_0) = 13$, and so $C_{13} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is elementary abelian of order 2^4 by Proposition 5.8(iv), and a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has central order divisible by 5 by Proposition 5.9(iii). In fact, since g_∞ has eigenvalues ζ_3 and $\bar{\zeta}_3$ on the tame part Tame, we have that $\bar{\mathsf{o}}(g_\infty) = 15$. Furthermore, $\varphi|_L$ is irreducible, rational-valued, and of Frobenius-Schur indicator -1. Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = L = \mathsf{A}_{13}$, and $V|_L$ is just the deleted permutation module $S^{(12,1)}|_L$. This case is however impossible, since $\varphi|_L$ has Frobenius-Schur indicator 1. Likewise, we can rule out the cases of $L = 6 \cdot \mathrm{Suz}$ and $\mathrm{Sp}_4(5)$.
- $(S, L) = (\mathrm{PSL}_2(25), \mathrm{SL}_2(25))$. In this case, $\mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L) = C_2$ by (25.2.1). Since $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 2^2$, we see that the element g_∞ of order 15 lies in L. But this is a contradiction, since $\mathrm{SL}_2(25)$ contains no element of order 15.
- $S = L = \mathrm{SU}_3(4)$. Here, since S has index 4 in $\mathrm{Aut}(S)$ and $\mathbf{Z}(G) = \mathbf{C}_G(S) \leq C_2$ by (25.2.1), G/S is a 2-group, and so the element g_0 of order 13 lies in S. It follows from Theorem 5.1 that $G = S$. Now, using [GAP] we can check that any element of order divisible by 15 in S has trace 0, whereas the element g_∞ has trace 0 on Wild and -1 on Tame, i.e. $\varphi(g_\infty) = -1$, a contradiction.
- $(S, L) = (G_2(4), 2 \cdot G_2(4))$. Recall that we have $\mathbf{Z}(L) = \mathbf{Z}(G) = \mathbf{C}_G(L) = C_2$ by (24.2.1). As $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 2$, we see that the element g_0 of order 13 lies in L. It follows from Theorem 5.1 that $G_{\mathrm{geom}} = L = 2 \cdot G_2(4)$.

(ii) Next, by Proposition 7.2, $\mathcal{S}_{13,3}$ is a descent of $\mathcal{H}$ to $\mathbb{F}_2$ (see also Table 4, line 24), and over any finite extension k of $\mathbb{F}_4$, any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}$. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith},k})$ acts via scalars, which are then roots of unity in $\mathbb{Q}$, we see that $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_2 = \mathbf{Z}(L)$. Hence, if $G_{\mathrm{arith},k} > L = G_{\mathrm{geom}}$, we see that some element of $G_{\mathrm{arith},k}$ must induce an outer automorphism of L. In particular, some element $g \in G_{\mathrm{arith},k}$ induces the same automorphism as an element h of class $16a$ of $L \cdot 2$ (as listed in [GAP]). Let Φ denote the representation of $G_{\mathrm{arith},k}$ on V, and extend $\Phi|_L$ to a representation $\tilde{\Phi}$ of $L \cdot 2$. Then $\tilde{\Phi}(h^{-1})\Phi(g)$ centralizes $\Phi(L)$, whence $\Phi(g) = \alpha\tilde{\Phi}(h)$ for some $\alpha \in \mathbb{C}^\times$. As both g and h have finite order, α is a root of unity. Hence $|\mathrm{Trace}(\Phi(g))| = |\mathrm{Trace}(\tilde{\Phi}(h))| = \sqrt{2}$, contradicting the fact that $\varphi(g) \in \mathbb{Q}$. Therefore we must have that $G_{\mathrm{arith},k} = L = G_{\mathrm{geom}}$. □

Theorem 25.3. *The local system $\mathcal{K}_5 = \mathcal{K}l(\mathsf{Char}_{16} \smallsetminus \{\mathbb{1}, \xi_8^4, \xi_8, \xi_8^{-1}\})$ in characteristic $p = 5$ has finite monodromy.*

Proof. We need to show:

$$V(16x) - V(x) - V\left(x + \frac{1}{2}\right) - V\left(x + \frac{1}{8}\right) - V\left(x - \frac{1}{8}\right) \geq -2$$

and

$$V(16x) - V(x) - V\left(x + \frac{1}{2}\right) - V\left(x + \frac{3}{8}\right) - V\left(x - \frac{3}{8}\right) \geq -2.$$

These inequalities are equivalent via the change of variable $x \mapsto 5x$, so we will focus on the first one.

Using the fact that $V(\frac{i}{16}) = V(\frac{39i}{5^4-1}) = \frac{1}{16}[39i]$ for $1 \le i \le 15$ we check that the inequality holds for $16x \in \mathbb{Z}$. For all other values of x, we can rewrite it as

$$V(16x) \le V\left(x + \frac{1}{2}\right) + V\left(x + \frac{1}{8}\right) + V\left(x - \frac{1}{8}\right) + V(x) - 1$$

and, via the change of variable $x \mapsto x + \frac{1}{8}$, as

$$V(16x) \le V\left(x + \frac{1}{8}\right) + V\left(x + \frac{5}{8}\right) + V\left(x + \frac{1}{4}\right) + V(x) - 1.$$

Following §9, it suffices to prove

$$[16x] \le \left[x + \frac{5^r-1}{8}\right] + \left[x + \frac{5(5^r-1)}{8}\right] + \left[x + \frac{5^r-1}{4}\right] + [x] - 4r$$

for every $r \ge 1$ divisible by $r_0 = 2$ and every $0 \le x \le 5^r - 1$. Notice that, in this case, multiplication by 5 permutes $\gamma_1 = \frac{1}{8}$ and $\gamma_2 = \frac{5}{8}$ and fixes $\gamma_3 = \frac{1}{4}$ and $\gamma_4 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2-1)\gamma_1 = 03_5$, $(5^2-1)\gamma_3 = 11_5$, $h_j = 3, 0, 1$ and $h_{2,j} = 03_5, 30_5, 11_5$ for $j = 1, 2, 3$ respectively. We will prove that

$$[16x] \le [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - 4r$$

for every $r \ge 1$ and every $0 \le x \le 5^r - 1$. For $r \le 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1	1	0,1	0	≥ 0	0	≥ 0
$a2, a3; a \ne 4$	1	2,3	0	≥ 0	0	≥ 0
$a4; a \ne 3, 4$	1	4	0	≥ 0	0	≥ 0
042,242	2	42	0	≥ 0	0	≥ 0
044,244	2	44	4	≥ 0	0	≥ 4

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4 = c_4'$ corresponding to $\gamma_4 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
142,144	3	20	2	4	0	11	1	0	0
342,344	3	40	2	4	0	22	1	0	1
442,444	3	44	2	4	4	30	1	1	1
43	2	42	2	0	0	24	1	1	1
34	2	4	1	4	0	22	0	1	1

□

Theorem 25.4. *The local system $\mathcal{K}_{13} = \mathcal{K}l(\mathsf{Char}_{16} \smallsetminus \{\mathbb{1}, \xi_8^4, \xi_8, \xi_8^{-1}\})$ in characteristic $p = 13$ has finite monodromy.*

Proof. We need to show:

$$V(16x) - V(x) - V\left(x + \frac{1}{2}\right) - V\left(x + \frac{1}{8}\right) - V\left(x - \frac{1}{8}\right) \ge -2$$

and

$$V(16x) - V(x) - V\left(x + \frac{1}{2}\right) - V\left(x + \frac{3}{8}\right) - V\left(x - \frac{3}{8}\right) \ge -2.$$

These inequalities are equivalent via the change of variable $x \mapsto 13x$, so we will focus on the first one.

Using the fact that $V(\frac{i}{16}) = V(\frac{1785i}{13^4-1}) = \frac{1}{48}[1785i]$ for $1 \le i \le 15$ we check that the inequality holds for $16x \in \mathbb{Z}$. For all other values of x, we can rewrite it as

$$V(16x) \le V\left(x+\frac{1}{2}\right) + V\left(x+\frac{1}{8}\right) + V\left(x-\frac{1}{8}\right) + V(x) - 1$$

and, via the change of variable $x \mapsto x + \frac{1}{8}$, as

$$V(16x) \le V\left(x+\frac{1}{8}\right) + V\left(x+\frac{5}{8}\right) + V\left(x+\frac{1}{4}\right) + V(x) - 1.$$

Let us denote the 13-adic digits by 0,1,2,3,4,5,6,7,8,9,A,B,C. Following §9, it suffices to prove

$$[16x] \le \left[x+\frac{13^r-1}{8}\right] + \left[x+\frac{5(13^r-1)}{8}\right] + \left[x+\frac{13^r-1}{4}\right] + [x] - 12r$$

for every $r \ge 1$ divisible by $r_0 = 2$ and every $0 \le x \le 13^r - 1$. Notice that, in this case, multiplication by 13 permutes $\gamma_1 = \frac{1}{8}$ and $\gamma_2 = \frac{5}{8}$ and fixes $\gamma_3 = \frac{1}{4}$ and $\gamma_4 = 0$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(13^2-1)\gamma_1 = 18_{13}$, $(13^2-1)\gamma_3 = 33_{13}$, $h_j = 8, 1, 3$ and $h_{2,j} = 18_{13}, 81_{13}, 33_{13}$ for $j = 1, 2, 3$ respectively. We will prove that

$$[16x] \le [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - 12r$$

for every $r \ge 1$ and every $0 \le x \le 13^r - 1$. For $r \le 2$ we check it by computer. For $r > 2$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 12\sum_j v_j + 12\sum_i u_i$
0,1,2,3,4	1	0,1,2,3,4	0	≥ 0	0	≥ 0
$a5, a6, a7, a8, a9; a \ne$B	1	5,6,7,8,9	≥ 0	≥ 0	0	≥ 0
aA, aB; $a \ne$ 9,B	1	A,B	≥ 0	≥ 0	0	≥ 0
aC; $a \ne$ 4,9,B	1	C	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4 = c_4'$ corresponding to $\gamma_4 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
B5, . . . ,BC	2	C	1	≥ 0	0	11	1	1	1
9A,9B,9C	2	A	1	≥ 0	0	C	0	1	1
4C	2	5	1	0	0	6	0	1	0

□

Theorem 25.5. *For $p = 5$ and $p = 13$, the local system $\mathcal{K}_p = \mathcal{K}l(\mathsf{Char}_{16} \smallsetminus \{\mathbb{1}, \xi_8^4, \xi_8, \xi_8^{-1}\})$ in characteristic p has $G_{\mathrm{geom}} = (2 \times \mathrm{SU}_3(4)) \cdot 4$, a maximal subgroup of $2 \cdot G_2(4) \cdot 2$. Furthermore, $\mathcal{K}_p$ has a descent $\mathcal{K}_p'$ to $\mathbb{F}_{p^2}$, which over any extension k of $\mathbb{F}_{p^2}$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.*

Proof. Because $\mathcal{K} = \mathcal{K}_p$ is Kloosterman, it is not Belyi induced, and it is visibly not Kummer induced. Hence, it is $(\mathbf{S}+)$ by Theorem 3.3. By Theorems 25.3 and 25.4, $G = G_{\mathrm{geom}}$ is finite. Let φ denote the character of the representation $\Phi : G \to \mathrm{GL}(V)$ of G realizing $\mathcal{K}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is precisely $\mathbb{Q}(\sqrt{2})$. Moreover, the representation is symplectic by [Ka4, 8.8.2], and

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{25.5.1}$$

Also, $\bar{\mathsf{o}}(g_0) = 16$ for a p'-generator g_0 of the image of $I(0)$ in G, and so

$$C_{16} \hookrightarrow G/\mathbf{Z}(G). \tag{25.5.2}$$

As $\dim(V) = 12$, G is almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma, and furthermore $\mathbf{Z}(G) \leq C_2$ by (25.5.1). Using (25.5.2), we can apply the main result of [HM] to arrive at the following two possibilities.

• $(S, L) = (G_2(4), 2 \cdot G_2(4))$ and $\mathbf{Z}(G) = C_2$. Since L contains no element of central order 16, (25.5.2) implies that $G/\mathbf{Z}(G) \cong \mathrm{Aut}(S)$, and so $G = L \cdot 2$; in paricular, G has no subgroup of index 4. On the other hand, Theorem 6.10(e) and Corollary 6.11 (with $(N, D) = (4, 3)$), shows that G has a subgroup of index 4, a contradiction.

• $S = L = \mathrm{SU}_3(4)$. Since $G/\mathbf{Z}(G)$ contains elements of order 16 by (25.5.1), $G/\mathbf{Z}(G) \cong \mathrm{Aut}(S) \cong S \cdot 4$. If $\mathbf{Z}(G) = 1$, then $G \cong \mathrm{Aut}(S)$ has no symplectic irreducible representation of degree 12. So $\mathbf{Z}(G) \cong C_2$, and $G \cong (2 \times \mathrm{SU}_3(4)) \cdot 4$, which is a maximal subgroup of $2 \cdot G_2(4) \cdot 2$.

A descent $\mathcal{K}'_p$ of $\mathcal{K}_p$ over $\mathbb{F}_{p^2}$ is constructed using Theorem 7.7(i), and listed on line 40 for $p = 5$ and line 41 for $p = 13$ in Table 4. By Theorem 7.7(ii), the field of traces is still $\mathbb{Q}(\sqrt{2})$; hence (25.5.1) also holds for $G_{\mathrm{arith},k}$. Thus $\mathbf{Z}(G_{\mathrm{arith},k}) = C_2 = \mathbf{Z}(G_{\mathrm{geom}})$ over any extension k of $\mathbb{F}_{p^2}$. Since G_{geom} already induces the full automorphism group of $L = \mathrm{SU}_3(4)$, we conclude that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. $\square$

In light of Theorem 25.2, one may wonder if finite almost quasisimple groups with $S = G_2(4)$ can admit hypergeometric sheaves in characteristic $\neq 2$. Our next result shows that this is impossible, and thus [KT5, Theorem 7.3] holds for these groups.

Theorem 25.6. *Let $\mathcal{H}$ be hypergeometric sheaf of type (D, m) with $D > m$ in characteristic p, with finite geometric monodromy group $G = G_{\mathrm{geom}}$. Suppose G is almost quasisimple, with $S = G_2(4)$ as the unique non-abelian composition factor. Then $p = 2$ and $D = 12$.*

Proof. (i) Let $V = \mathbb{C}^D$ denote the representation realizing $\mathcal{H}$, with G-character φ. By [KT5, Theorem 6.6], $D = 12$, and φ is irreducible over $L := G^{(\infty)} \cong 2S$. This implies that $\mathbf{C}_G(L) = \mathbf{Z}(G)$, and $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(S) = S \cdot 2$. As usual, let Q denote the image of $P(\infty)$ in G, and let g_0 be a generator of the image of $I(0)$ in G.

Assume now that $p \neq 2, 5, 13$. By Proposition 5.6(iii), p divides $|G/\mathbf{Z}(G)|$, hence $p = 3$ or $p = 7$. Now, $\mathbf{Z}(G)L$ is a normal subgroup of index ≤ 2 in G (as $|\mathrm{Out}(S)| = 2$), so we may assume that

$$Q \leq C \times R, \tag{25.6.1}$$

where $C = \mathbf{O}_p(\mathbf{Z}(G))$ and R is a Sylow p-subgroup of L. Note that $Q \not\leq \mathbf{Z}(G)$ by Proposition 5.6, hence Q contains some element $g = zh$ with $z \in C$ and $1 \neq h \in R$.

Consider the case $p = 7$. Then $R = \langle h \rangle \cong C_7$, and the spectrum of h on V consists of all nontrivial 7^{th} roots of unity, each with multiplicity 2, see [GAP]. It follows that the tame part has dimension $m \leq 2$. This implies by Proposition 5.6(iv) that $p \nmid |\mathbf{Z}(G)|$, i.e. $C = 1$, and $Q \cong C_7$. But this is a contradiction, because Q admits $W = D - m \geq 10$ distinct linear characters on Wild by Proposition 5.8.

Assume now that $p = 3$. Note that $R \cong 3^{1+2}_+$ (see [Atlas]), and $V|_R$ is the sum of the two faithful irreducible representations of R, each with multiplicity 2. As C acts via scalars on V, the same is true for $C \times R$. Restricting further down to Q, we see that each irreducible constituent of $V|_Q$ has *even* multiplicity. On the other hand, the Q-module Wild is multiplicity-free by Propositions 5.8 and 5.9, a contradiction.

(ii) The rest of the proof is to deal with the case where $p \in \{5, 13\}$. First we show that $Q < L$ and that $\mathcal{H}$ must be Kloosterman. Indeed, $Q \not\leq \mathbf{Z}(G)$ by Proposition 5.6. Next, $\mathbf{C}_G(L) = \mathbf{Z}(G)$ as L is irreducible on V, and so $G/\mathbf{Z}(G)L \hookrightarrow \mathrm{Out}(L) \cong C_2$ and henc $Q \leq \mathbf{Z}(G)L$. Using [GAP] we can check that any nontrivial p-element in L admits all $p-1$ nontrivial $p^{\rm th}$ roots of unity as eigenvalues on V. This implies that any $g \in Q \smallsetminus \mathbf{Z}(G)$ admits at least $p-2 \geq 3$ distinct eigenvalues on Wild, and so $D-m \geq 3$. Hence $p \nmid |\mathbf{Z}(G)|$ by Proposition 5.6(iv), implying $Q \leq L$. Now, if $p=13$, then $Q \cong C_{13}$ and $W=12$, meaning $\mathcal{H}$ is Kloosterman. Suppose $p=5$, so that $|Q|=5$ or 5^2. If Q contains an element g belonging to class $5C$ or $5D$ (in the notation of [Atlas]), then g has no fixed point on V, again showing $W=12$. If Q contains no such elements, then Q cannot be a full Sylow 5-subgroup of L, whence $Q \cong C_5$ is generated by an element of class $5A$ or $5B$. In this case, $W=8$, which contradicts Proposition 5.8, since Q cannot admit 8 distinct linear characters on Wild.

Now we will determine the set of 12 "upstairs" characters $\chi_1, \ldots, \chi_{12}$ of the Kloosterman sheaf $\mathcal{H}$, by inspecting possible ss-elements in G. Note that $\mathrm{Sp}(V)$ contains a finite group $H \cong L \cdot 2$ (the one listed in [Atlas] and [GAP]), and $G < \mathbf{Z}(\mathrm{GL}(V))H$. We note that the representation of L on V is $(\mathbf{S}+)$, whence $\mathcal{H}$ is $(\mathbf{S}+)$ as well; in particular, it is primitive. Next, using [GAP], we find 20 conjugate classes of ss-elements in H. Two of them (classes $15b$ and $30b$ in [GAP]) has spectrum $\epsilon(\mu_{15} \smallsetminus \mu_3)$ with $\epsilon = \pm$ on V, which is invariant under multiplication by ζ_3 and so $\mathcal{H}$ would be Kummer induced, a contradiction. The four classes $24ab$ and $14bc$ are ruled out for the same reason, since their spectra are $\mu_{24} \smallsetminus \mu_{12}$, respectively $\mu_{14} \smallsetminus \mu_2$. The two classes $24cd$ are also ruled out, since they have spectrum invariant under multiplication by -1.

This leaves 12 classes. Two of them have representatives x_{13} and $\boldsymbol{z}x_{13}$, with x_{13} in class $13a$ and $\mathbf{Z}(L) = \langle \boldsymbol{z} \rangle$. Now, if g_0 is a scalar multiple of one of them, then $p=5$ and, after tensoring, we may assume that $\mathcal{H} = \mathcal{K}l(\mathsf{Char}_{13}^{\times})$. However, as shown in [KT1, Theorem 17.1], the Kummer pullback by $[13]^\star$ of the latter sheaf has $G_{\rm geom} = \mathrm{SL}_2(25)$. The next two have representatives x_{21} and $\boldsymbol{z}x_{21}$, with x_{21} in class $21a$. If g_0 is a scalar multiple of one of them, then, after tensoring, we may assume that $\mathcal{H} = \mathcal{K}l(\mathsf{Char}_{21}^{\times})$. However, the latter sheaf fails the V-test for both $p=5$ and $p=13$. The next four are $24efgh$, and a generator of a cyclic subgroup generated by any of their representatives has spectrum

$$\{\zeta_{24}^j \mid j = 1,2,4,7,8,10,14,16,17,20,22,23\}$$

on V, Hence, if g_0 is a scalar multiple of one of them, then, after tensoring and taking Galois conjugate, we may assume that

$$\mathcal{H} = \mathcal{K}l\big(\xi_{24}^j \mid j = 1,2,4,7,8,10,14,16,17,20,22,23\big).$$

Again, the latter sheaf fails the V-test for both $p=5$ and $p=13$.

The remaining four classes are $16abcd$, and a generator of a cyclic subgroup generated by any of their representatives has spectrum $\mu_{16} \smallsetminus \{\zeta_8^{0,1,4,7}\}$ on V. Hence, if g_0 is a scalar multiple of one of them, then, after tensoring and taking Galois conjugate, we may assume that $\mathcal{H} = \mathcal{K}l\big(\mathsf{Char}_{16} \smallsetminus \{\xi_8^{0,1,4,7}\}\big)$. As shown in Theorems 25.3 and 25.4, this sheaf has finite $G_{\rm geom}$ for both $p=5$ and $p=13$. However, Theorem 25.5 shows that this sheaf has $G_{\rm geom} = (2 \times \mathrm{SU}_3(4)) \cdot 4$. $\square$

Corollary 25.7. *Let $\mathcal{H}$ be hypergeometric sheaf of type (D,m) with $D > m$ in characteristic p, with finite geometric monodromy group $G = G_{\rm geom}$. Suppose G is almost quasisimple, with $S = \mathrm{SU}_3(4)$ as the unique non-abelian composition factor. Then one of the following statements holds.*

(i) *$D = 12$, $p = 2$, 5, or 13, and all these cases occur.*
(ii) *$D = 13$, $G = \mathbf{Z}(G)S$, and $p = 2$, and this case occurs.*

Proof. Note that $\mathrm{SU}_3(4)$ has trivial Schur multiplier and $\mathrm{Out}(S) = C_4$. Moreover, $\mathrm{meo}(\mathrm{Aut}(S)) = 16$ [Atlas]. Hence, checking [GAP], we see that either $D = 12$, or $G = \mathbf{Z}(G)S$ and $D = 13$. In particular, $G_{\rm geom} \cong S$ is irreducible on the underlying representation $V_{\mathcal{H}} \cong \mathbb{C}^D$, with character φ.

(i) Suppose $D = 12$. Then $\mathrm{Aut}(S)$ embeds in $G_2(4) \cdot 2 = \mathrm{Aut}(G_2(4))$, and the S-representation on V extends to the subgroup $H = (2 \cdot G_2(4)) \cdot 2 < \mathrm{Sp}(V)$ mentioned in the proof of Theorem 25.6.

Now the analysis in part (i) of the proof of Theorem 25.6 rules out the case $p = 3$. The case $p = 2$ is realized by the sheaf $\mathcal{K}l(\mathsf{Char}_{13}^{\times})$, whose Kummer pullback by $[13]^{\star}$ has $G_{\mathrm{geom}} = \mathrm{SU}_3(4)$, see [KT1, Theorem 19.1] with $q := 4$ there. The cases $p = 5$ and $p = 13$ are shown to occur by Theorem 25.5.

(ii) Assume now that $D = 13$, so that $G = \mathbf{Z}(G)S$, but $p \neq 2$. Then $G \twoheadrightarrow S$ and $S = \mathrm{SU}_3(4)$ is an irreducible subgroup of $\mathrm{GL}_3(\overline{\mathbb{F}_2})$. Applying [KT5, Theorem 4.14], we see that $D - m = \dim \mathsf{Wild} \leq 3$. On the other hand, since $G = \mathbf{Z}(G)S$, it is easy to verify using [GAP] that any non-central p-element $g \in G$ can have a fixed point subspace of dimension at most 5 on $V_{\mathcal{H}}$, and thus $D - m \geq 13 - 5 = 8$, a contradiction.

Finally, the case $p = 2$ is realized by a sheaf of type $(13, 1)$, whose Kummer pullback by $[13]^{\star}$ has $G_{\mathrm{geom}} = \mathrm{SU}_3(4)$, see [KT1, Theorem 19.1] again with $q := 4$. $\square$

26. The "exceptional" group $\mathrm{SU}_3(3) \cdot 2 \cong G_2(2)$

Theorem 26.1. *The local system $\mathcal{K} := \mathcal{K}l(\mathsf{Char}_{12}^{\times} \cup \{\xi_6, \xi_6^3\})$ in characteristic $p = 7$ has finite geometric monodromy group.*

Proof. We need to show:

$$V\left(x+\frac{1}{12}\right)+V\left(x+\frac{5}{12}\right)+V\left(x+\frac{7}{12}\right)+V\left(x+\frac{11}{12}\right)+V\left(x+\frac{1}{6}\right)+V\left(x+\frac{1}{3}\right)\geq\frac{5}{2}.$$

and

$$V\left(x+\frac{1}{12}\right)+V\left(x+\frac{5}{12}\right)+V\left(x+\frac{7}{12}\right)+V\left(x+\frac{11}{12}\right)+V\left(x+\frac{5}{6}\right)+V\left(x+\frac{2}{3}\right)\geq\frac{5}{2}.$$

which are equivalent via the change of variable $x \mapsto x + \frac{1}{2}$. Using the fact that $V(\frac{i}{12}) = V(\frac{4i}{7^2-1}) = \frac{1}{12}[4i]$ for $1 \leq i \leq 11$ we check that the inequality holds for $12x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$ and $V(Nx) = \sum_{i \bmod N} V(x + \frac{i}{N}) - \frac{N-1}{2}$ [Ka7, §13], as

$$V\left(4x+\frac{1}{3}\right)+V\left(4x+\frac{2}{3}\right)\leq\left(x+\frac{1}{6}\right)+V\left(x+\frac{1}{3}\right)+\frac{1}{2}.$$

Following §9, it suffices to prove

$$\left[4x+\frac{7^r-1}{3}\right]+\left[4x+\frac{2(7^r-1)}{3}\right]\leq\left[x+\frac{7^r-1}{6}\right]+\left[x+\frac{7^r-1}{3}\right]+3r+6$$

for every $r \geq 1$ and every $0 \leq x \leq 7^r - 1$. For $r \leq 2$ we check it by computer. For $r > 2$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x:

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 6\sum_j v_j + 6\sum_i u_i$
0,1,2,3,4	1	0,1,2,3,4	≥ 0	≥ 0	0	≥ 0
$a5; a \neq 4$	1	5	0	≥ 0	0	≥ 0
06,16,26,66	1	6	-6	≥ 1	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table.

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$b_2 = b_2'$	$c_1 = c_1'$	$c_2 = c_2'$
45,46	2	5	1	≥ 0	0	3	3	0	1
36	2	4	1	0	0	2	2	0	0
56	2	6	1	-6	-6	3	4	1	1

$\square$

Theorem 26.2. *Each of the two local systems*

$$\mathcal{K} := \mathcal{K}l(\mathsf{Char}_{12}^{\times} \cup \{\xi_6, \xi_6^3\}) \text{ and } \mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{12}^{\times} \cup \mathsf{Char}_3; \xi_2)$$

in characteristic $p = 7$ has geometric monodromy group $G_{\mathrm{geom}} = \mathrm{SU}_3(3) \cdot 2 \cong G_2(2)$. Furthermore, $\mathcal{H}$ has a descent $\mathcal{H}'$ to $\mathbb{F}_{49}$, such that over any finite extension k of $\mathbb{F}_{49}$, $\mathcal{H}'$ has arithmetic monodromy group $G_{\mathrm{arith},k,\mathcal{H}'} = G_2(2)$. Also, $\mathcal{K}$ has a descent $\mathcal{K}'$ to $\mathbb{F}_7$, which over any finite extension k of $\mathbb{F}_{7^{36}}$ has arithmetic monodromy group $G_{\mathrm{arith},k,\mathcal{K}'} = G_2(2)$.

Proof. (i) By Theorem 26.1, $G = G_{\mathrm{geom}}$ for $\mathcal{K}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{K}$. By the construction of $\mathcal{K}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}(\sqrt{-3})$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, since it is Kloosterman, it is not Belyi induced. Hence (G, V) satisfies $(\mathbf{S}+)$ by Theorem 3.3. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars, we have that

$$\mathbf{Z}(G) \hookrightarrow C_6. \tag{26.2.1}$$

As $D = \dim(V) = 6$, G must be almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\bar{\mathsf{o}}(g_0) = 12$ for a generator g_0 of the image of $I(0)$, whence $C_{12} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is cyclic of order 7 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(ii). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = \mathrm{PSL}_2(7)$. These two cases are ruled out since $\mathrm{Aut}(S)$ contains no element of order 12.
- $(S, L) = (\mathrm{PSL}_2(13), \mathrm{SL}_2(13))$. In this case, G can induce only inner automorphisms of L, and this yields a contradiction since $G/\mathbf{Z}(G) \cong S$ contains no element of order 12.
- $S = \mathsf{A}_7$. Here, if $L = S$, then $V|_L$ is just the deleted permutation module $S^{(6,1)}|_S$, and so by Lemma 3.8, $\varphi(g_0)$ is an integer multiple of a a root of unity, contradicting the fact that $\varphi(g_0) = \sqrt{-3}$. Thus $L \neq S$, i.e. $L = 3 \cdot S$ or $6 \cdot S$. Since $\varphi|_L$ is not fixed by any outer automorphism of L, we have that $G/\mathbf{Z}(G) \cong S$, which is again a contradiction since S contains no element of order 12.
- $(S, L) = (\mathrm{PSL}_3(4), 6 \cdot \mathrm{PSL}_3(4))$. Since 2_1 is the only outer automorphism that fixes $\varphi|_L$, we now have that $G/\mathbf{Z}(G) \leq S \cdot 2_1$, which is a contradiction since $S \cdot 2_1$ contains no element of order 12.
- $(S, L) = (\mathrm{J}_2, 2 \cdot \mathrm{J}_2)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{5})$, again a contradiction.
- $(S, L) = (\mathrm{PSU}_4(3), 6_1 \cdot \mathrm{PSU}_4(3))$. In this case, $(\varphi + \bar{\varphi})|_L$ takes odd values ± 1, ± 3. On the other hand, applying Proposition 6.3(ii) with $r = 3$, $A = \mathsf{Char}_{12}^{\times}$, $B = \emptyset$, we see that $\varphi + \bar{\varphi}$ can take only even values, a contradiction.
- $S = L = \mathrm{SU}_3(3)$. In this case, any element of central order 12 in $\mathbf{Z}(G)S$ has trace being a root of unity, see [GAP]. On the other hand, $\varphi(g_0) = \sqrt{-3}$, so $G > \mathbf{Z}(G)S$ and hence $G/\mathbf{Z}(G) \cong \mathrm{Aut}(S) = S \cdot 2$ and $G = (\mathbf{Z}(G) \times S) \cdot 2$. In fact, we may assume that g_0 acts via conjugation as some element $h \in \mathrm{Aut}(S)$, of class $12b$ or $12c$ in the notation of [GAP]. Note that $\Phi|_S$ extends to a representation $\tilde{\Phi}$ of $\mathrm{Aut}(S)$. As $\Phi|_S$ is irreducible, by Schur's lemma we have that $\Phi(g_0) = \alpha\tilde{\Phi}(h)$ for some $\alpha \in \mathbb{C}^{\times}$. Now we have

$$\sqrt{-3} = \varphi(g_0) = \mathrm{Trace}(\Phi(g_0)) = \alpha \cdot \mathrm{Trace}(\tilde{\Phi}(h)) = \pm\alpha\sqrt{-3},$$

i.e. $\alpha = \pm 1$. Since $|\mathrm{Aut}(S)/S| = 2$, it is now easy to see that

$$\langle \Phi(S), \Phi(g_0) \rangle = \langle \Phi(S), \alpha\tilde{\Phi}(h) \rangle$$

is isomorphic to $\mathrm{Aut}(S)$ and normalized by $\Phi(G) = \langle \Phi(S), \Phi(g_0), \Phi(\mathbf{Z}(G)) \rangle$. It follows by Theorem 5.1 that $G \cong \Phi(G) = \langle \Phi(S), \Phi(g_0) \rangle \cong \mathrm{Aut}(S)$.

(ii) Let $G := \mathrm{Aut}(S) \cong G_2(2)$ as in (i). As shown in (i), the Kloosterman sheaf $\mathcal{K}$ gives rise to a surjection $\phi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow G$, together with a faithful irreducible representation $\Phi : G \to \mathrm{GL}_6(\overline{\mathbb{Q}_\ell})$.

We also consider an irreducible representation $\Psi : G \to \mathrm{GL}_7(\overline{\mathbb{Q}_\ell})$. Note that, for any p-element $v \in G$,

$$\mathrm{Trace}(\Psi(v)) = \mathrm{Trace}(\Phi(v)) + 1.$$

It follows from [KT5, Theorem 5.1] that $\Psi \circ \phi$ gives rise to a hypergeometric sheaf $\mathcal{H}'$, of type $(7, 1)$ and with geometric monodromy group $G_{\mathrm{geom},\mathcal{H}'} = \Psi(G) \cong G$. Furthermore, as shown above, g_0 is an element of order 12 and class $12b$ or $12c$ in G, hence the spectrum of $\Psi(g_0)$ is either

$$X := \{\zeta_{12}^i \mid i = 1, 5, 7, 11, 0, 4, 8\} \tag{26.2.2}$$

or

$$-X = (-1) \cdot X = \{\zeta_{12}^i \mid i = 1, 5, 7, 11, 2, 6, 10\}. \tag{26.2.3}$$

Let g_∞ be a p'-generator of the image of $I(\infty)$ modulo $P(\infty)$ in $G_{\mathrm{geom},\mathcal{H}'}$. By Proposition 5.8, the spectra of g_∞ on the wild part of $\mathcal{H}'$ is $\{\beta\zeta_6^j \mid 0 \le j \le 5\}$ and on the tame part is $\{\gamma\}$ for some $\beta, \gamma \in \mathbb{C}^\times$.

Suppose we are in the case of (26.2.2). Using [GAP], we can check that the only elements (of order divisible by 6) in G that can have the prescribed for g_∞ spectrum in Ψ are the ones in class $6b$ (in the notation of [GAP]), and for them we have $\gamma = -1$. This implies that the "upstairs" characters of $\mathcal{H}'$ are $\mathsf{Char}_{12}^\times \cup \mathsf{Char}_3$ and the "downstairs" character is ξ_2. In other words, $\mathcal{H}'$ is geometrically isomorphic to $\mathcal{H}$, and we are done.

Suppose now that we are in the case of (26.2.3). Again using [GAP], we can check that the only elements (of order divisible by 6) in G that can have the prescribed for g_∞ spectrum in Ψ are the ones in class $6b$ (in the notation of [GAP]), and for them we have $\gamma = 1$. This implies that the "upstairs" characters of $\mathcal{H}'$ are $\mathsf{Char}_{12}^\times \cup \mathsf{Char}_6$ and the "downstairs" character is $\mathbb{1}$. In other words, $\mathcal{H}'$ is geometrically isomorphic to $\mathcal{H} \otimes \mathcal{L}_{\xi_2}$. By Lemma 5.12, for $H := G_{\mathrm{geom},\mathcal{H}}$ we now have that $H/\mathbf{Z}(H) \cong G/\mathbf{Z}(G) \cong \mathrm{Aut}(S)$ and $H^{(\infty)} \cong G^{(\infty)} = S$. Furthermore, the field of traces of all elements in H is $\mathbb{Q}$ by Corollary 6.2(i), which implies that $\mathbf{Z}(H) \le C_2$. But $\mathrm{rank}\mathcal{H} = 7$ and $\mathcal{H}$ has trivial geometric determinant, so in fact $\mathbf{Z}(H) = 1$ and $H \cong \mathrm{Aut}(S)$.

(iii) For $\mathcal{K}'$, we can use $\mathcal{K}' = \mathcal{K}_{00}$ constructed by Theorem 7.5 and listed in Table 4, line 25. Over any finite extension k of $\mathbb{F}_{7^6}$, it still has $\mathbb{Q}(\sqrt{-3})$ as the field of traces, and so $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{K}'}) \hookrightarrow C_6$. Now we can argue as in part (ii) of the proof of Theorem 24.2.

For $\mathcal{H}'$, we can take $\mathcal{H}_{00}$, with $\mathcal{H}_0$ listed in Table 4, line 26. By [Ka4, 8.12.2], $\mathcal{H}'$ has trivial arithmetic determinant over any finite extension k of $\mathbb{F}_{49}$, and furthermore any element in $G_{\mathrm{arith},k,\mathcal{H}'}$ still has rational traces by Proposition 6.1. As $\mathrm{rank}\mathcal{H}' = 7$, it follows that $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}'}) = 1$, and we obtain $G_{\mathrm{arith},k,\mathcal{H}'} \cong H \cong \mathrm{Aut}(S)$ as above. $\square$

Remark 26.3. The statements in Theorem 26.2 concerning $\mathcal{H}$ were established in [Ka7] in a different way.

27. The Suzuki group ${}^2B_2(8)$

Theorem 27.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{15} \smallsetminus \{\mathbb{1}\}; \xi_{12}, \xi_{12}^5)$ in characteristic $p = 13$ has finite geometric monodromy group.*

Proof. We need to show that

$$V(15x) - V(x) + V\left(-x + \frac{1}{12}\right) + V\left(-x + \frac{5}{12}\right) \ge \frac{1}{2}$$

and

$$V(15x) - V(x) + V\left(-x - \frac{1}{12}\right) + V\left(-x - \frac{5}{12}\right) \ge \frac{1}{2}.$$

Using the fact that $V(\frac{i}{12}) = \frac{i}{12}$ for $1 \leq i \leq 11$ and that $V(\frac{i}{60}) = V(\frac{476i}{13^4-1}) = \frac{1}{48}[476i]$ for $1 \leq i \leq 59$ we check that the inequalities hold for $12x \in \mathbb{Z}$ and $15x \in \mathbb{Z}$. For all other values of x we can rewrite the first inequality as

$$V(15x) \leq V\left(x + \frac{1}{12}\right) + V\left(x + \frac{5}{12}\right) + V(x) - \frac{1}{2}$$

and, following §9, it suffices to prove

$$[15x] \leq \left[x + \frac{13^r - 1}{12}\right] + \left[x + \frac{5(13^r - 1)}{12}\right] + [x] - 6r$$

for every $r \geq 1$ and every $0 \leq x \leq 13^r - 1$. For $r \leq 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x. We denote the 13-adic digits by 0,1,2,3,4,5,6,7,8,9,A,B,C.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 12\sum_j v_j + 12\sum_i u_i$
0,1,2,3,4,5,6,7	1	0,1,2,3,4,5,6,7	≥ 0	≥ 0	0	≥ 0
$a8, a9, a\mathrm{A}, a\mathrm{B}; a \neq 7$	1	8,9,A,B	0	≥ 0	0	≥ 0
$a\mathrm{C}; a \neq$ 7,B	1	C	0	≥ 0	0	≥ 0
$a78, a79, a7\mathrm{A}; a \neq 7$	2	78,79,7A	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_3 = c_3'$ corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$
7B,7C	2	8	1	≥ 0	0	9	0	1
778,779,77A	3	78	2	0	0	8	0	1
BC	2	C	1	0	0	10	1	1

The second inequality can be rewritten, for $12x \notin \mathbb{Z}$ and $15x \notin \mathbb{Z}$, as

$$V(15x) \leq V\left(x - \frac{1}{12}\right) + V\left(x - \frac{5}{12}\right) + V(x) - \frac{1}{2}$$

which, via the change of variable $x \mapsto x + \frac{1}{2}$, is equivalent to

$$V\left(15x + \frac{1}{2}\right) \leq V\left(x + \frac{1}{12}\right) + V\left(x + \frac{5}{12}\right) + V\left(x + \frac{1}{2}\right) - \frac{1}{2}$$

and, following §9, it suffices to prove

$$\left[15x + \frac{13^r - 1}{2}\right] \leq \left[x + \frac{13^r - 1}{12}\right] + \left[x + \frac{5(13^r - 1)}{12}\right] + \left[x + \frac{13^r - 1}{2}\right] - 6r + 12$$

for every $r \geq 1$ and every $0 \leq x \leq 13^r - 1$. For $r \leq 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 12\sum_j v_j + 12\sum_i u_i$
0,1,2,3,4,5,6	1	0,1,2,3,4,5,6	≥ 0	≥ 0	0	≥ 0
$a7; a \neq 6$	1	7	0	≥ 0	0	≥ 0
$a8; a \neq 4, 5, 6, 7$,A,B	1	8	-12	≥ 1	0	≥ 0
$a9; a \neq 4, 6, 7$,A,B	1	9	-12	≥ 1	0	≥ 0
aA, aB; $a \neq 6, 7$	1	A,B	≥ 0	≥ 0	0	≥ 0
aC; $a \neq 6, 7$,B	1	C	0	≥ 0	0	≥ 0
48,49,58	2	48,49,58	0	≥ 0	0	≥ 0
aA8; $a \neq 6, 7$,A	2	A8	-12	≥ 1	0	≥ 0
aB8; $a \neq 6, 7$	2	B8	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$	$c_3 = c_3'$
67,68,69,6A,6B,6C	2	7	1	≥ 0	0	8	0	0	1
78,79,7A,7B,7C	2	8	1	≥ -12	-12	9	0	1	1
BC	2	C	1	0	0	11	1	1	1
6A8,6B8	3	69	2	0	0	8	0	0	1
7A8,7B8	3	79	2	-12	-12	9	0	1	1
AA8	3	A9	2	-12	-12	C	0	1	1
A9	2	A8	2	-12	-12	C	0	1	1
B9	2	B8	2	0	0	10	0	1	1

$\square$

Theorem 27.2. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{15} \smallsetminus \{\mathbb{1}\}; \xi_{12}, \xi_{12}^5)$ in characteristic $p = 13$ has geometric monodromy group $G_{\rm geom} = \mathrm{Aut}(^2B_2(8)) = {}^2B_2(8) \cdot 3$. Furthermore, the local system $\mathcal{H} \otimes \mathcal{L}_{\xi_4}$ has a descent $\tilde{\mathcal{H}}$ to $\mathbb{F}_{13}$, which over any finite extension k of $\mathbb{F}_{13^2}$ has geometric and arithmetic monodromy group $\tilde{G}_{{\rm arith},k} = \tilde{G}_{\rm geom} = \mathrm{Aut}(^2B_2(8)) \times C_4$.*

Proof. (i) By Theorem 27.1, $G = G_{\rm geom}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$, the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ contains $i = \sqrt{-1}$; indeed, a p'-generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has trace $\zeta_1 2 + \bar{\zeta}_1 2^5 = i$ on Tame and 0 on Wild, whence $\varphi(g_\infty) = i$. In fact, applying Proposition 6.1(iii) we see that $\mathbb{Q}(\varphi) = \mathbb{Q}(i)$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G, V) satisfies ($\mathbf{S}+$). As $D = \dim(V) = 14$, G must be almost quasisimple by Lemma 3.1. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(i)$, we have that $\mathbf{Z}(G) \hookrightarrow C_4$. In fact, as $\mathcal{H}$ has rank 14 and trivial geometric determinant, it follows that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{27.2.1}$$

Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, $\bar{\mathsf{o}}(g_0) = 15$ for a generator g_0 of the image of $I(0)$, whence $C_{15} \hookrightarrow G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Moreover, the image Q of $P(\infty)$ is cyclic of order 13 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(i). Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

- $S = L = \mathsf{A}_{15}$, and $V|_L$ is just the deleted permutation module $S^{(14,1)}|_L$. In this case, since $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = \mathsf{S}_{15}$, the element g_0 of order 15 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G. Using (27.2.1), we see that in fact $g_0 \in S$, hence $G = S$ by Theorem 5.1. But this is a contradiction, since $\mathbb{Q}(\varphi)$ would have been equal to $\mathbb{Q}$.
- $(S, L) = (\mathrm{PSp}_6(3), \mathrm{Sp}_6(3)$. In this case, $\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi|_L) = \mathbb{Q}(\sqrt{-3})$, again a contradiction.
- $S = L = {}^2B_2(8)$. Recall that we have $\mathbf{Z}(G) = \mathbf{C}_G(S) \leq C_2$ by (27.2.1). Furthermore, the element g_0 of central order 15 does not lie in $\mathbf{Z}(G)S \lhd G$, hence $G > S \times \mathbf{Z}(G)$. Now $S < G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 3$, and so $G = (\mathbf{Z}(G) \times S) \cdot 3$. We also note that G/S contains the central subgroup $\mathbf{Z}(G)$ of order ≤ 2 and of index 3, hence it is abelian. Thus G contains a subgroup $H = S \cdot 3$ of index ≤ 2, hence $H \lhd G$ and H contains the element g_0 of order 15. It now follows from Theorem 5.1 that $G = H$, and we conclude that $G_{\mathrm{geom}} = {}^2B_2(8) \cdot 3$.

(ii) First we note by Theorem 7.5 that $\mathcal{H}$ has a descent $\mathcal{H}_{00}$ (listed in Table 4, line 27) to $\mathbb{F}_{13}$, for which over any extension $k \supseteq \mathbb{F}_{13^2}$, any element in its arithmetic monodromy groups still has trace in $\mathbb{Q}(i)$. Now we can take $\tilde{\mathcal{H}} = \mathcal{H}_{00} \otimes \mathcal{L}_{\xi_4}$ and have that every element in $\tilde{G}_{\mathrm{arith},k}$ has trace in $\mathbb{Q}(i)$ whenever $k \supseteq \mathbb{F}_{13^2}$. It follows for $\tilde{\mathcal{H}}$ that $\mathbf{Z}(\tilde{G}_{\mathrm{geom}}) \leq \mathbf{Z}(\tilde{G}_{\mathrm{arith},k}) \leq C_4$. Next, if $\tilde{g}_0$ generates the image of $I(0)$ in $\tilde{G} := \tilde{G}_{\mathrm{geom}}$, then note that $\tilde{g}_0^{15}$ acts as the scalar $-i$ on $\tilde{\mathcal{H}}$, whence we now have

$$\mathbf{Z}(\tilde{G}_{\mathrm{geom}}) = \mathbf{Z}(\tilde{G}_{\mathrm{arith},k}) = C_4. \tag{27.2.2}$$

By Lemma 5.12,

$$\tilde{G}/\mathbf{Z}(\tilde{G}) \cong G/\mathbf{Z}(G) = \mathrm{Aut}(S) \text{ and } \tilde{G}^{(\infty)} \cong G^{(\infty)} = S. \tag{27.2.3}$$

Together with (27.2.2), we now have that $\tilde{G}/S$ is $C_4 \rtimes C_3$, with C_4 being central. Hence $\tilde{G}/S = C_4 \times C_3$, and so $\tilde{G}$ contains a normal subgroup N with $N/S \cong C_3$. Note that $\mathbf{Z}(\tilde{G})N = \tilde{G}$, $\mathbf{Z}(\tilde{G}) \cap N = 1$, and so $N \cong \tilde{G}/\mathbf{Z}(\tilde{G}) \cong \mathrm{Aut}(S)$ by (27.2.3). Thus $\tilde{G} = N \times \mathbf{Z}(\tilde{G}) = \mathrm{Aut}(S) \times C_4$. Finally, as $\mathbf{C}_{\tilde{G}_{\mathrm{arith},k}}(S) = \mathbf{Z}(\tilde{G}_{\mathrm{arith},k}) = \mathbf{Z}(\tilde{G})$ and $\tilde{G}$ already induces the full automorphism group of S, we also have that $\tilde{G}_{\mathrm{arith},k} = \tilde{G}$. $\square$

28. The "exceptional" group $\mathrm{SL}_2(8) \cdot 3 \cong {}^2G_2(3)$

Theorem 28.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_9^\times \sqcup \{\mathbb{1}\}; \xi_2)$ in characteristic $p = 7$ has finite geometric monodromy group.*

Proof. We need to show:

$$V(9x) + V(x) - V(3x) + V(-2x) - V(-x) \geq 0.$$

Using the fact that $V(\frac{i}{18}) = V(\frac{19i}{7^3-1}) = \frac{1}{18}[19i]$ for $1 \leq i \leq 17$ we check that the inequality holds for $18x \in \mathbb{Z}$. For all other values of x we can rewrite it, using that $V(x) + V(-x) = 1$ for $x \neq 0$, $V(2x) = V(x) + V(x + \frac{1}{2}) - \frac{1}{2}$ and $V(3x) = V(x) + V(x + \frac{1}{3}) + V(x + \frac{2}{3}) - 1$ [Ka7, §13], as

$$V\left(3x + \frac{1}{3}\right) + V\left(3x + \frac{2}{3}\right) + V(x) \leq V\left(x + \frac{1}{2}\right) + \frac{3}{2}$$

and, via the change of variable $x \mapsto x + \frac{1}{2}$, this is equivalent to

$$V\left(3x + \frac{1}{6}\right) + V\left(3x + \frac{5}{6}\right) + V\left(x + \frac{1}{2}\right) \leq V(x) + \frac{3}{2}.$$

Following §9, it suffices to prove

$$\left[3x + \frac{7^r - 1}{6}\right] + \left[3x + \frac{5(7^r - 1)}{6}\right] + \left[x + \frac{7^r - 1}{2}\right] \leq [x] + 9r$$

for every $r \geq 1$ and every $0 \leq x \leq 7^r - 1$. For $r = 1$ we check it by hand. For $r > 1$ we proceed by induction as described in §9, by splitting off the last digit of x. In this case, since $\Delta(1, z) = 0$ for every $z = 0, \ldots, 6$ and $\sum_j v_j$ is always 0, the induction step is automatically true. $\square$

Lemma 28.2. *The local system $\mathcal{H}' := \mathcal{H}yp(\mathsf{Char}_9 \smallsetminus \{\mathbb{1}\}; \mathsf{Char}_2)$ in characteristic $p = 7$ has geometric third moment $M_3 \geq 1$.*

Proof. First we note that $\mathcal{H}'$ is Sawin-like by [KT5, Lemma 9.2(ii)] (with $A = 7$ and $B = 2$). Hence its geometric monodromy group G_{geom} is contained in S_9 in its deleted natural permutation module $S^{(8,1)}$. Since the latter has nontrivial determinant, but $\mathcal{H}'$ has trivial geometric determinant, we have $G_{\mathrm{geom}} \leq \mathsf{A}_9$. Now, using [GAP] we can check that A_7 has $M_3 = 1$ on $S^{(8,1)}$, whence the statement follows. $\square$

Theorem 28.3. *The following statements hold.*

(a) *The local systems $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_9^\times \sqcup \{\mathbb{1}\}; \xi_2)$ and $\mathcal{H}' := \mathcal{H}yp(\mathsf{Char}_9 \smallsetminus \{\mathbb{1}\}; \mathsf{Char}_2)$ in characteristic $p = 7$ both have geometric monodromy group*

$$G_{\mathrm{geom},\mathcal{H}} \cong G_{\mathrm{geom},\mathcal{H}'} \cong \mathrm{SL}_2(8) \cdot 3 \cong {}^2G_2(3).$$

(b) *$\mathcal{H} \otimes \mathcal{L}_{\xi_2}$ has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_7$, which over any finite extension k of $\mathbb{F}_{49}$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = {}^2G_2(3) \times C_2$.*

(c) *$\mathcal{H}' \otimes \mathcal{L}_{\xi_2}$ has a descent $\mathcal{H}'_\sharp$ to $\mathbb{F}_7$, which over any finite extension k of $\mathbb{F}_{49}$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}'_\sharp} = G_{\mathrm{geom},\mathcal{H}'_\sharp} = {}^2G_2(3) \times C_2$.*

Proof. (i) By Theorem 28.1, $G = G_{\mathrm{geom},\mathcal{H}}$ is finite. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G realizing $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}$. It is clear that $\mathcal{H}$ is not Kummer induced. Furthermore, the shape of the "upstairs" and "downstairs" characters of $\mathcal{H}$ shows by Proposition 3.7(ii) that it is not Belyi induced. Hence, by Theorem 3.5, (G, V) satisfies $(\mathbf{S}+)$. Furthermore, $\mathsf{o}(g_0) = \bar{\mathsf{o}}(g_0) = 9$ for a generator g_0 of the image of $I(0)$, whence 9 divides $|G/\mathbf{Z}(G)|$. We also note by Proposition 5.6(iii) that $p = 7$ also divides $|G/\mathbf{Z}(G)|$. Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}$, we have that

$$\mathbf{Z}(G) \hookrightarrow C_2. \tag{28.3.1}$$

Suppose that G satisfies condition (c) of Lemma 3.1. Then $G \lhd R \cong 7^{1+2}$, and $G/\mathbf{Z}(G)$ embeds in $C_7^2 \rtimes \mathrm{Sp}_2(7)$, whence $9 \nmid |G/\mathbf{Z}(G)|$, a contradiction.

(ii) We have therefore shown that G is almost quasisimple by Lemma 3.1. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Hence, both C_9 and C_7 embed in $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to arrive at the following possibilities for (S, L).

• $S = L = \mathsf{A}_8$, and $V|_L$ is just the deleted permutation module $S^{(7,1)}|_L$. In this case, since $S \lhd G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = \mathsf{S}_8$, the element g_0 of order 9 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G. Using (28.3.1), we see that in fact $g_0 \in S$, hence $G = S$ by Theorem 5.1. Now $G \cong \mathrm{SL}_4(2)$ admits a faithful representation of degree 4 over $\mathbb{F}_2$. It follows from [KT5, Theorem 4.14] that $\dim \mathsf{Wild} \leq 4$, a contradiction.

• $S = L = \mathrm{Sp}_6(2)$. As in the previous case, we see that the element g_0 of order 9 must belong to the inverse image $S \times \mathbf{Z}(G)$ of S in G, and using (28.3.1), we then see that $g_0 \in S$, and so $G = S$ by Theorem 5.1. Now, the sheaf $\mathcal{H}$ gives rise to a surjection $\phi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow S$. Also, consider the surjection $\pi : \hat{S} = 2\mathrm{Sp}_6(2) \twoheadrightarrow S$ with kernel $\mathrm{Ker}(\pi) \cong C_2$. The obstruction to lifting ϕ

to a homomorphism $\varpi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \to \hat{S}$ lies in the group $H^2(\mathbb{G}_m/\overline{\mathbb{F}_p}, \mathrm{Ker}(\pi)) = 0$, the vanishing because open curves have cohomological dimension ≤ 1, cf. [SGA, Cor. 2.7, Exp. IX and Thm. 5.1, Exp. X]. Since $\hat{S}$ contains no subgroup isomorphic to S, we conclude that ϖ is also surjective. Now we can inflate Φ to a representation $\hat{\Phi}$ of $\hat{S}$ with kernel C_2. We also consider the faithful 8-dimensional representation $\Psi : \hat{S} \to \mathrm{GL}_8(\mathbb{C})$ and note that

$$\mathrm{Trace}(\Psi(h)) = 1 + \mathrm{Trace}(\hat{\Phi}(h))$$

for all 7-elements $h \in \hat{S}$. Applying [KT5, Theorem 5.1], we now see that $\Psi \circ \varpi$ gives rise to a hypergeometric sheaf $\tilde{\mathcal{H}}$ of type $(8, 2)$, still in characteristic $p = 7$ and with C_7 being the image of $P(\infty)$. Let g_∞ be a p'-generator of $I(\infty)$ modulo $P(\infty)$ in S, and let $h_0 \in \hat{S}$, respectively $h_\infty \in \hat{S}$ be an inverse image of g_0, respectively of g_∞. The shape of $\mathcal{H}$ tells us by Proposition 5.8 that the spectrum of $\hat{\Phi}(h_\infty) = \Phi(g_\infty)$ consists of all 6^{th} roots of some $\alpha \in \mathbb{C}^\times$ and -1 (counting multiplicities). Thus $6|\mathsf{o}(h_\infty)$ and it has trace -1 in $\hat{\Phi}$. It follows that h_∞ belongs to class $6g$ or $6h$ in the notation of [GAP]. Likewise, the spectrum of $\Psi(h_\infty)$ consists of all 6^{th} roots of some $\beta \in \mathbb{C}^\times$ and two more roots of unity $\gamma \neq \delta \in \mathbb{C}^\times$ (counting multiplicities). Using [GAP] we can now see that $\beta = 1$ and $\{\gamma, \delta\} = \{1, -1\}$, which means that the two "downstairs" characters of $\tilde{\mathcal{H}}$ are $\mathbb{1}$ and ξ_2. Next, $9|\mathsf{o}(h_0)$, so h_0 belongs to class $9a$ or $18a$ in the notation of [GAP], and so inspecting the spectrum of $\Psi(h_0)$ we see that the "upstairs" characters of $\tilde{\mathcal{H}}$ are either $X_1 := \mathsf{Char}_9 \smallsetminus \{\mathbb{1}\}$, or $X_2 := \xi_2 \cdot X_1$. We conclude that either

$$\tilde{\mathcal{H}} \cong \mathcal{H}', \tag{28.3.2}$$

or

$$\tilde{\mathcal{H}} \cong \mathcal{H}' \otimes \mathcal{L}_{\xi_2}. \tag{28.3.3}$$

In the case of (28.3.2), Lemma 28.2 tells us that $\tilde{\mathcal{H}} = \mathcal{H}'$ has $M_3 \geq 1$, whereas Ψ has $M_3 = 0$ (indeed, $\mathbf{Z}(\hat{S}) \cong C_2$ acts faithfully in Ψ), a contradiction. Hence (28.3.3) must occur, and thus $G_{\mathrm{geom},\mathcal{H}'\otimes\mathcal{L}_{\xi_2}} = \hat{S}$. Now we consider $H := G_{\mathrm{geom},\mathcal{H}'}$. By Lemma 5.12, $H/\mathbf{Z}(H) \cong \hat{S}/\mathbf{Z}(\hat{S}) = S$ and $H^{(\infty)} \cong \hat{S}^{(\infty)} \cong \hat{S}$. In particular, $\mathbf{Z}(H) \geq \mathbf{Z}(H^{(\infty)}) = C_2$, and so H has $M_3 = 0$, again contradicting Lemma 28.2.

- $S = L = \mathrm{SL}_2(8)$. Recall that we have $\mathbf{Z}(G) = \mathbf{C}_G(S) \leq C_2$ by (28.3.1). We again look at a p'-generator g_∞ of $I(\infty)$ modulo $P(\infty)$ in G, and note by Proposition 5.8(iii) that $6|\bar{\mathsf{o}}(g_\infty)$. As $S\mathbf{Z}(G)$ does not contain any element of order 6, we have that $G > \mathbf{Z}(G) \times S$. Now $S < G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 3$, and so $G = (\mathbf{Z}(G) \times S) \cdot 3$. We also note that G/S contains the central subgroup $\mathbf{Z}(G)$ of order ≤ 2 and of index 3, hence it is abelian. Thus G contains a subgroup $H = S \cdot 3$ of index ≤ 2, hence $H \lhd G$ and H contains the element g_0 of order 9. It now follows from Theorem 5.1 that $G = H$, and we conclude that $G_{\mathrm{geom},\mathcal{H}} = \mathrm{SL}_2(8) \cdot 3$.

(iii) The result of (ii) yields a surjection $\phi : \pi_1(\mathbb{G}_m/\overline{\mathbb{F}_p}) \twoheadrightarrow G$ with $G = G_{\mathrm{geom},\mathcal{H}} = \mathrm{SL}_2(8)\cdot 3$. Note that G admits a unique 8-dimensional irreducible representation Θ with rational-valued character, and moreover

$$\mathrm{Trace}(\Theta(v)) = 1 + \mathrm{Trace}(\Phi(v))$$

for all 7-elements $v \in G$. Applying [KT5, Theorem 5.1], we again see that $\Theta \circ \phi$ gives rise to a hypergeometric sheaf $\mathcal{H}''$ of type $(8, 2)$, still in characteristic $p = 7$ and with C_7 being the image of $P(\infty)$. By Theorem 5.1, the normal closure of g_0 in G equals G, so $g_0 \notin \mathrm{SL}_2(8)$, and thus the element g_0 must belong to class $9b$ or $9c$ in the notation of [GAP]. Inspecting the spectrum of $\Theta(g_0)$, we see that the "upstairs" characters of $\mathcal{H}''$ are $\mathsf{Char}_9 \smallsetminus \{\mathbb{1}\}$. Likewise, a p'-generator g_∞ of $I(\infty)$ modulo $P(\infty)$ in G has order divisible by 6, and so must belong to class $6a$ or $6b$ in the notation of [GAP]. Inspecting the spectrum of $\Theta(g_\infty)$, we see that the "downstairs" characters of $\mathcal{H}''$ are Char_2. Thus $\mathcal{H}'' \cong \mathcal{H}'$, and so $G_{\mathrm{geom},\mathcal{H}'} \cong \Theta(G) \cong G$.

(iv) Now we note by Theorem 7.5 that $\mathcal{H}$ has a descent $\mathcal{H}_{00}$ (listed in Table 4, line 28) to $\mathbb{F}_7$, for which over any extension $k \supseteq \mathbb{F}_{49}$, any element in its arithmetic monodromy groups still has rational trace. Now we can take $\mathcal{H}_\sharp = \mathcal{H}_{00} \otimes \mathcal{L}_{\xi_2}$ and have that every element in $\tilde{G}_{\mathrm{arith},k}$ has trace in $\mathbb{Q}$ whenever $k \supseteq \mathbb{F}_{49}$. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \leq \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \leq C_2$. Next, if v_0 generates the image of $I(0)$ in $G_{\mathrm{geom},\mathcal{H}_\sharp}$, then note that v_0^9 acts as the scalar -1 on $\mathcal{H}_\sharp$, whence we now have

$$\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = C_2 = \langle v_0^9 \rangle. \tag{28.3.4}$$

By Lemma 5.12,

$$G_{\mathrm{geom},\mathcal{H}_\sharp}/\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \cong G/\mathbf{Z}(G) = \mathrm{Aut}(S) \text{ and } (G_{\mathrm{geom},\mathcal{H}_\sharp})^{(\infty)} \cong G^{(\infty)} = S. \tag{28.3.5}$$

Together with (28.3.4), we now have that $G_{\mathrm{geom},\mathcal{H}_\sharp}/S$ is $C_2 \rtimes C_3$, with C_2 being central. Hence $G_{\mathrm{geom},\mathcal{H}_\sharp}/S = C_2 \times C_3$, and so $G_{\mathrm{geom},\mathcal{H}_\sharp}$ contains a normal subgroup N with $N/S \cong C_3$. Note that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp})N = G_{\mathrm{geom},\mathcal{H}_\sharp}$, $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \cap N = 1$, and so $N \cong G_{\mathrm{geom},\mathcal{H}_\sharp}/\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \cong \mathrm{Aut}(S)$ by (28.3.4). Thus $G_{\mathrm{geom},\mathcal{H}_\sharp} = N \times \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) = \mathrm{Aut}(S) \times C_2$. Finally, as

$$\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(S) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp})$$

and $G_{\mathrm{geom},\mathcal{H}_\sharp}$ already induces the full automorphism group of S, we also have that

$$G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp}.$$

The same arguments apply to the case of $\mathcal{H}'$, by taking $\mathcal{H}'_\sharp = (\mathcal{H}')_{00} \otimes \mathcal{L}_{\xi_2}$, with $(\mathcal{H}')_{00}$ either one of the two sheaves given in Table 4, line 29. $\square$

Remark 28.4. Given a finite group G and a finite-dimensional $\mathbb{C}G$-module V, even in the case (G, V) satisfies $(\mathbf{S}+)$ and V is orthogonally self-dual, the third moment $M_3(G, V)$ can be 0 (as in the case of the 8-dimensional faithful module for $2 \cdot \mathrm{Sp}_6(2)$ as we saw above), 1 (as in the case of the 8-dimensional faithful module for A_9-module), 2 (as in the case of the 12-dimensional module for $\mathrm{SL}_3(3)$), or even 35 (as in the case of the 189-dimensional faithful module for A_9-module). Note that, in addition to $(\mathbf{S}+)$, the first three cases share the common property of having an element with a simple spectrum.

29. The Conway group Co_1 and the Suzuki group Suz

Theorem 29.1. *The local system $\mathcal{H} := \mathcal{H}yp(\mathsf{Char}_{39}^\times; \mathbb{1})$ in characteristic $p = 2$ has a descent $\mathcal{H}'$ to $\mathbb{F}_2$ which over any finite extension k of $\mathbb{F}_2$ has geometric and arithmetic monodromy groups $G_{\mathrm{geom}} = G_{\mathrm{arith},k} = 2 \cdot \mathrm{Co}_1$, the double cover of the Conway sporadic simple group Co_1.*

Proof. The statement about G_{geom} is [KRLT3, Theorem 8.1]. We will use the descent $\mathcal{H}' = \mathcal{H}_{00}$ constructed in Theorem 7.5 and listed in Table 4, line 30, which also has $\mathbb{Q}$ as the field of traces of all elements in $G_{\mathrm{arith},k}$, whence

$$\mathbf{Z}(G_{\mathrm{arith},k}) = \mathbf{C}_{G_{\mathrm{arith},k}}(G_{\mathrm{geom}}) = \mathbf{Z}(G_{\mathrm{geom}}) = C_2.$$

Now,

$$S \lhd G_{\mathrm{arith},k}/\mathbf{Z}(G_{\mathrm{arith},k}) \leq \mathrm{Aut}(S) = S$$

for $S := G_{\mathrm{geom}}/\mathbf{Z}(G_{\mathrm{geom}}) = \mathrm{Co}_1$, and so $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. $\square$

Theorem 29.2. *Each of the two local systems*

$$\mathcal{H}_1 := \mathcal{H}yp(\mathsf{Char}_{20} \smallsetminus (\mathsf{Char}_4 \cup \mathsf{Char}_5); \mathbb{1}) \text{ and } \mathcal{H}_2 := \mathcal{H}yp(\mathsf{Char}_{28}^{\times}; \mathbb{1})$$

in characteristic $p = 3$ has a descent $\mathcal{H}'$ to $\mathbb{F}_3$, which over any finite extension k of $\mathbb{F}_3$ has geometric and arithmetic monodromy groups $G_{\mathrm{geom}} = G_{\mathrm{arith},k} = 6 \cdot \mathrm{Suz}$, the sixth cover of the Suzuki sporadic simple group Suz.

Proof. The statement about G_{geom} is [KRLT3, Theorem 8.2]. We will use the descent $\mathcal{H}' = \mathcal{H}_{00}$ constructed in Theorem 7.5 and listed in Table 4, lines 31 and 32, which also has $\mathbb{Q}(\sqrt{-3})$ as the field of traces of all elements in G_{arith}, whence

$$\mathbf{Z}(G_{\mathrm{arith},k}) = \mathbf{C}_{G_{\mathrm{arith},k}}(G_{\mathrm{geom}}) = \mathbf{Z}(G_{\mathrm{geom}}) = C_6.$$

Now,

$$S \lhd G_{\mathrm{arith},k}/\mathbf{Z}(G_{\mathrm{arith},k}) \le \mathrm{Aut}(S) = S \cdot 2$$

for $S := G_{\mathrm{geom}}/\mathbf{Z}(G_{\mathrm{geom}}) = \mathrm{Suz}$, and no outer automorphism of S can fix the equivalence class of a 12-dimensional faithful complex representation of G_{geom}. It follows that $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$. $\square$

30. Complex reflection groups

Theorem 30.1. *The local system $\mathcal{H}yp(\mathsf{Char}_{15}^{\times}; \mathsf{Char}_9 \smallsetminus \mathsf{Char}_3^{\times})$ in characteristic 2 has finite monodromy.*

Proof. We need to show:

$$V(15x) - V(3x) - V(5x) + V(x) + V(-9x) - V(-3x) + V(-x) \ge 0.$$

Using the fact that $V(\frac{i}{9}) = V(\frac{7i}{2^6-1}) = \frac{1}{6}[7i]$ for $1 \le i \le 8$ we check that the inequality holds for $9x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \neq 0$ and $V(Nx) = \sum_{i \bmod N} V(x + \frac{i}{N}) - \frac{N-1}{2}$ [Ka7, §13], we can rewrite the inequality as

$$V(9x) \le V\left(x + \frac{1}{15}\right) + V\left(x + \frac{2}{15}\right) + V\left(x + \frac{4}{15}\right) + V\left(x + \frac{8}{15}\right) + V\left(x + \frac{5}{15}\right) + V\left(x + \frac{10}{15}\right) +$$
$$+ V\left(x + \frac{7}{15}\right) + V\left(x + \frac{14}{15}\right) + V\left(x + \frac{13}{15}\right) + V\left(x + \frac{11}{15}\right) - 4$$

and, following §9, it suffices to prove

$$[9x] \le \left[x + \frac{2^r-1}{15}\right] + \left[x + \frac{2(2^r-1)}{15}\right] + \left[x + \frac{4(2^r-1)}{15}\right] + \left[x + \frac{8(2^r-1)}{15}\right] + \left[x + \frac{5(2^r-1)}{15}\right]$$
$$\left[x + \frac{10(2^r-1)}{15}\right] + \left[x + \frac{7(2^r-1)}{15}\right] + \left[x + \frac{14(2^r-1)}{15}\right] + \left[x + \frac{13(2^r-1)}{15}\right] + \left[x + \frac{11(2^r-1)}{15}\right] - 4r$$

for every $r \ge 1$ divisible by $r_0 = 4$ and every $0 \le x \le 2^r - 1$. Since multiplication by 2 permutes $\gamma_1 = \frac{1}{15}$, $\gamma_2 = \frac{2}{15}$, $\gamma_3 = \frac{4}{15}$ and $\gamma_4 = \frac{8}{15}$; $\gamma_5 = \frac{5}{15}$ and $\gamma_6 = \frac{10}{15}$; and $\gamma_7 = \frac{7}{15}$, $\gamma_8 = \frac{14}{15}$, $\gamma_9 = \frac{13}{15}$ and $\gamma_{10} = \frac{11}{15}$ cyclically modulo 1, we can take $r_1 = 1$. Then, with the notation of §9, we have

$$(2^4-1)\gamma_1 = 0001_2,\ (2^4-1)\gamma_5 = 0101_2,\ (2^4-1)\gamma_7 = 0111_2;$$

$$h_j = 1,0,0,0,1,0,1,1,1,0;\ h_{2,j} = 01_2, 00_2, 00_2, 10_2, 01_2, 10_2, 11_2, 11_2, 01_2, 10_2;$$

$$h_{3,j} = 001_2, 000_2, 100_2, 010_2, 101_2, 010_2, 111_2, 011_2, 101_2, 110_2;$$

and

$$h_{4,j} = 0001_2, 1000_2, 0100_2, 0010_2, 0101_2, 1010_2, 0111_2, 1011_2, 1101_2, 1110_2$$

for $j = 1, \dots, 10$ respectively. We will prove that

$$[9x] \le \sum_{i=1}^{10} [x + h_{r,i}] - 4r$$

for every $r \ge 1$ and $0 \le x \le 2^r - 1$. For $r \le 8$ we check it by computer. For $r > 8$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - \sum_j v_j + \sum_i u_i$
0	1	0	1	0	0	1
0001,1101,0111	1	1	4	≥ 0	≤ 4	≥ 0
000011,110011	4	0011	1	≥ 0	≤ 1	≥ 0
11011	3	011	2	≥ 2	2	≥ 2
00001111	8	00001111	4	0	0	4

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	b_1	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}
1001	4	101	3	7	6	101	0	0	0	1	0	1	1	1	1	1
10101	5	1010	4	7	7	101	1	0	0	0	1	0	1	1	1	1
00101	5	0011	4	3	1	1	0	0	0	0	0	0	0	0	1	1
0010011	7	001011	6	2	2	1	0	0	0	0	0	0	1	1	0	0
1010011	7	100111	6	6	5	101	0	0	1	0	1	0	1	1	1	1
$\{$ 00100011, 00101111	8	0011	4	1	1	1	0	0	0	0	0	0	0	1	1	0
10100011	8	100111	6	5	5	101	0	0	0	1	0	1	1	1	1	1
1100011	7	101111	6	5	5	110	0	1	1	0	1	1	1	1	1	1
01011	5	0110	4	3	3	11	0	0	0	0	1	0	1	0	1	1
10001111	8	1001011	7	7	6	101	0	0	0	1	0	1	1	1	1	1
1001111	7	100111	6	6	5	101	0	0	1	0	1	0	1	1	1	1
10101111	8	10111	5	6	6	110	0	0	0	1	1	1	1	1	1	1
01101111	8	0101111	7	2	2	11	0	0	0	0	0	1	0	1	1	1
11101111	8	1111111	7	8	8	1000	1	1	1	1	1	1	1	1	1	1
11111	5	1111	4	8	8	1000	1	1	1	1	1	1	1	1	1	1

□

Theorem 30.2. *The local system $\mathcal{H}yp(\mathsf{Char}_9^\times; \mathsf{Char}_5)$ in characteristic 2 has finite monodromy.*

Proof. We need to show:

$$V(9x) - V(3x) + V(-5x) \ge 0.$$

Using the fact that $V(\frac{i}{9}) = V(\frac{7i}{2^6-1}) = \frac{1}{6}[7i]$ for $1 \le i \le 8$ we check that the inequality holds for $9x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \ne 0$ and $V(Nx) = \sum_{i \bmod N} V(x + \frac{i}{N}) - \frac{N-1}{2}$ [Ka7, §13], we can rewrite the inequality as

$$\begin{aligned} V\left(3x + \frac{1}{3}\right) + V\left(3x + \frac{2}{3}\right) &\le V(5x) + 1 \\ &= V\left(x + \frac{1}{5}\right) + V\left(x + \frac{4}{5}\right) + V\left(x + \frac{2}{5}\right) + V\left(x + \frac{3}{5}\right) + V(x) - 1 \end{aligned}$$

and, following §9, it suffices to prove

$$\left[3x+\frac{2^r-1}{3}\right]+\left[3x+\frac{2(2^r-1)}{3}\right]\leq\left[x+\frac{2^r-1}{5}\right]+\left[x+\frac{4(2^r-1)}{5}\right]+ \\ +\left[x+\frac{2(2^r-1)}{5}\right]+\left[x+\frac{3(2^r-1)}{5}\right]+[x]-r$$

for every $r\geq 1$ divisible by $r_0=4$ and every $0\leq x\leq 2^r-1$. Since multiplication by 2^2 permutes $\gamma_1=\frac{1}{5}$ and $\gamma_2=\frac{4}{5}$, and $\gamma_3=\frac{2}{5}$ and $\gamma_4=\frac{3}{5}$ cyclically modulo 1, we can take $r_1=2$. Then, with the notation of §9, we have $(2^4-1)\gamma_1=0011_2$; $h_1=11_2$, $h_2=0$; $h_{2,j}=0011_2,1100_2$ for $j=1,2$ respectively. We will prove that

$$\left[3x+\frac{2^r-1}{3}\right]+\left[3x+\frac{2(2^r-1)}{3}\right]\leq[x+h_{r,1}]+[x+h_{r,2}]+[x+h_{r,3}]+[x+h_{r,4}]+[x]-r$$

for every $r=2k\geq 1$ and $0\leq x\leq 2^r-1$. For $r\leq 8$ we check it by computer. For $r>8$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-\sum_j v_j+\sum_i u_i$
00	2	00	0	0	0	0
0001,1001,0101	2	01	1	≥ 0	≤ 1	≥ 0
0010,0110	2	10	1	≥ 0	≤ 1	≥ 0
0001110	6	001110	0	≥ 0	0	≥ 0
01001110	6	001110	0	1	1	0
0011	2	11	2	≥ 0	1	≥ 1
000111	6	000111	0	0	0	0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_5=c_5'$ corresponding to $\gamma_5=0$, since it is always 0):

$z=$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1=b_1'$	$b_2=b_2'$	$c_1=c_1'$	$c_2=c_2'$	$c_3=c_3'$	$c_4=c_4'$
1010	4	11	2	3	2	10	10	0	1	1	1
11001110	8	110111	6	2	2	10	11	1	1	1	1
101110,100111	6	1100	4	2	2	10	10	1	0	1	1
011110	6	1000	4	3	1	1	10	1	0	1	0
111110,111111	6	1111	4	≥ 4	3	11	11	1	1	1	1
1101	4	1110	4	3	2	10	11	1	1	1	1
010111	6	0110	4	1	1	1	1	1	0	0	0
110111	6	1110	4	2	2	10	11	1	1	1	1
1011	4	11	2	3	2	10	10	0	1	1	1
001111	6	01	2	3	1	1	1	1	0	0	0
101111	6	11	2	4	2	10	10	1	0	1	1
011111	6	10	2	4	1	1	10	1	0	1	0

□

Theorem 30.3. *The local system* $\mathcal{H}yp(\mathsf{Char}_7^\times;\mathsf{Char}_3^\times\sqcup\{\xi_9,\xi_9^4,\xi_9^7\})$ *in characteristic* 2 *has finite monodromy.*

Proof. We need to show:

$$V(7x)-V(x)+V(-3x)-V(-x)+V\left(-x+\frac{1}{9}\right)+V\left(-x+\frac{4}{9}\right)+V\left(-x+\frac{7}{9}\right)\geq 1$$

and

$$V(7x)-V(x)+V(-3x)-V(-x)+V\left(-x+\frac{2}{9}\right)+V\left(-x+\frac{8}{9}\right)+V\left(-x+\frac{5}{9}\right)\geq 1.$$

Since these inequalities are equivalent via the change of variable $x\mapsto 2x$, we will focus on the first one. Using the fact that $V(\frac{i}{63})=V(\frac{i}{2^6-1})=\frac{1}{6}[i]$ for $1\leq i\leq 62$ we check that the inequality holds for $7x\in\mathbb{Z}$. For all other values of x, using that $V(x)+V(-x)=1$ if $x\neq 0$ and $V(3x)=V(x)+V(x+\frac{1}{3})+V(x+\frac{2}{3})-1$ [Ka7, §13], we can rewrite the inequality as

$$V(7x)\leq V\left(x+\frac{1}{3}\right)+V\left(x+\frac{2}{3}\right)+V\left(x+\frac{1}{9}\right)+V\left(x+\frac{4}{9}\right)+V\left(x+\frac{7}{9}\right)+V(x)-2$$

and, following §9, it suffices to prove

$$[7x]\leq\left[x+\frac{2^r-1}{3}\right]+\left[x+\frac{2(2^r-1)}{3}\right]+\left[x+\frac{2^r-1}{9}\right]+\left[x+\frac{4(2^r-1)}{9}\right]+\left[x+\frac{7(2^r-1)}{9}\right]+[x]-2r$$

for every $r\geq 1$ divisible by $r_0=6$ and every $0\leq x\leq 2^r-1$. Since multiplication by 2^2 fixes $\gamma_1=\frac{1}{3}$ and $\gamma_2=\frac{2}{3}$ and permutes $\gamma_3=\frac{1}{9}$, $\gamma_4=\frac{4}{9}$ and $\gamma_5=\frac{7}{9}$ cyclically modulo 1, we can take $r_1=2$. Then, with the notation of §9, we have $(2^4-1)\gamma_1=0001_2$, $(2^6-1)\gamma_1=010101_2$, $(2^6-1)\gamma_2=101010_2$, $(2^6-1)\gamma_3=000111_2$; $h_j=01_2,10_2,11_2,01_2,00_2$; $h_{2,j}=0101_2,1010_2,0111_2,0001_2,1100_2$ and $h_{3,j}=010101_2,101010_2,000111_2,110001_2,011100_2$ for $j=1,\dots,5$ respectively. We will prove that

$$0\leq[x+h_{k,1}]+[x+h_{k,2}]+[x+h_{k,3}]+[x+h_{k,4}]+[x+h_{k,5}]+[x]-2r$$

for every $r=2k\geq 1$ and $0\leq x\leq 2^r-1$. For $r\leq 12$ we check it by computer. For $r>12$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z)-\sum_j v_j+\sum_i u_i$
00	2	00	1	0	0	1
101	2	01	0	≥ 0	0	≥ 0
0001	4	0001	0	0	0	0
001001	6	001001	0	0	0	0
00101001	8	00101001	3	≥ 0	0	≥ 3
00011001	8	00011001	0	0	0	≥ 0
0011011001	10	0011011001	1	≥ 0	0	≥ 1
001011011001	12	001011011001	1	≥ 0	0	≥ 1
0010,1110,01010,00110	2	10	2	≥ 0	≤ 2	≥ 0
0011,00111,11111	2	11	3	≥ 0	≤ 3	≥ 0
001011	6	001011	2	≥ 0	0	≥ 2

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_6=c_6'$ corresponding to $\gamma_6=0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	c_1	c_2	c_3	c_4	c_5
10101001	8	101001	6	5	3	100	0	1	1	0	1
01101001	8	011011	6	1	1	10	0	1	1	0	1
11101001	8	111011	6	4	4	110	1	1	1	1	1
01011001	8	011001	6	0	0	10	0	1	1	0	0
10011001	8	101001	6	3	3	100	0	1	1	0	1
101011011001	12	1011011001	10	2	2	100	1	1	0	1	1
011011011001	12	011001001	10	0	0	10	0	1	0	0	1
111011011001	12	1110010001	10	3	3	110	1	1	1	1	1
0111011001	10	01111001	8	2	2	11	0	1	0	1	0
1111011001	10	11111001	8	4	4	110	1	1	1	1	1
00111001	8	010001	6	0	0	1	0	0	1	0	0
10111001	8	110001	6	3	3	101	1	1	1	0	1
01111001	8	100001	6	2	2	11	0	1	1	0	0
11111001	8	111011	6	4	4	110	1	1	1	1	1
011010,010110,010111	6	0110	4	≥ 3	3	10	0	1	0	0	1
111010	6	1111	4	6	5	110	1	1	1	1	1
110110	6	1101	4	5	4	101	1	1	0	1	1
110111	6	1110	4	8	7	110	1	1	0	1	1
011011	6	011001	6	1	0	10	0	1	0	0	1
101011	6	1011	4	3	3	100	1	1	0	1	1
111011	6	111001	6	4	3	110	1	1	1	1	1
001111	6	0100	4	2	1	1	0	0	0	0	1
101111	6	1100	4	5	4	101	1	1	0	1	1

□

Theorem 30.4. *The local system* $\mathcal{H}yp(\mathsf{Char}_5^\times; \mathsf{Char}_4 \setminus \{\mathbb{1}\})$ *in characteristic* 3 *has finite monodromy.*

Proof. We need to show:

$$V(5x) - V(x) + V\left(-x + \frac{1}{4}\right) + V\left(-x + \frac{1}{2}\right) + V\left(-x + \frac{3}{4}\right) \geq 1.$$

Using the fact that $V(\frac{i}{20}) = V(\frac{4i}{3^4-1}) = \frac{1}{8}[4i]$ for $1 \leq i \leq 19$ we check that the inequality holds for $5x \in \mathbb{Z}$. For other values of x, using that $V(x) + V(-x) = 1$ if $x \neq 0$, we can rewrite the inequality as

$$V(5x) \leq V\left(x + \frac{1}{4}\right) + V\left(x + \frac{1}{2}\right) + V\left(x + \frac{3}{4}\right) + V(x) - 1$$

and, following §9, it suffices to prove

$$[5x] \leq \left[x + \frac{3^r - 1}{4}\right] + \left[x + \frac{3(3^r - 1)}{4}\right] + \left[x + \frac{3^r - 1}{2}\right] + [x] - 2r + 1$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 3^r - 1$. Since multiplication by 3 permutes $\gamma_1 = \frac{1}{4}$ and $\gamma_2 = \frac{3}{4}$ and fixes $\gamma_3 = \frac{1}{2}$ modulo 1, we can take $r_1 = 1$. Then, with the notation of §9, we have $(3^2-1)\gamma_1 = 02_3$, $(3^2-1)\gamma_3 = 11_3$, $h_i = 2, 0, 1$ and $h_{2,i} = 02_3, 20_3, 11_3$ for $i = 1, 2, 3$ respectively. We will prove that

$$[x] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x + h_{r,3}] + [x] - 2r + 1$$

for every $r \geq 1$ and $0 \leq x \leq 3^r - 1$. For $r \leq 6$ we check it by computer. For $r > 6$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
0	1	0	1	0	0	1
01,11	1	1	0	≥ 0	0	≥ 0
$a021$, $a \neq 2$	3	021	0	≥ 0	0	≥ 0
$a02021$, $a \neq 2$	5	02021	0	≥ 0	0	≥ 0
0121	4	0121	0	≥ 0	0	≥ 0
02	2	02	4	≥ 0	0	≥ 4
012	3	012	2	≥ 0	0	≥ 2

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_4 = c'_4$ corresponding to $\gamma_5 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$	$c_3 = c'_3$
202021	6	2021	4	1	1	10	1	1	1
12021	5	1121	4	-1	-1	2	1	0	1
22021	5	2121	4	2	2	11	1	1	1
1121	4	121	3	-1	-1	2	0	1	1
2121	4	221	3	2	2	11	1	1	1
0221	4	021	3	1	0	1	0	1	0
1221	4	201	3	4	4	10	0	1	1
2221	4	221	3	3	2	11	1	1	1
112	3	12	2	1	1	2	1	0	1
212,222	3	22	2	≥ 4	4	11	1	1	1
022	3	10	2	3	1	1	1	0	0
122	3	20	2	6	4	10	1	0	1

$\square$

Theorem 30.5. *The local system $\mathcal{H}yp(\mathsf{Char}_3^\times; \xi_2)$ in characteristic 5 has finite monodromy.*

Proof. We need to show:

$$V(3x) - V(x) + V\left(-x + \frac{1}{2}\right) \geq 0.$$

For $3x \in \mathbb{Z}$ it is clearly true, since $V(\frac{i}{6}) = \frac{1}{2}$ for $i = 1, \ldots, 5$. For other values of x, Using the fact that $V(x) + V(-x) = 1$ if $x \neq 0$, we can rewrite the inequality as

$$V(3x) \leq V\left(x + \frac{1}{2}\right) + V(x)$$

and, following §9, it suffices to prove

$$[3x] \leq \left[x + \frac{5^r - 1}{2}\right] + [x] + 1$$

for every $r \geq 1$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 2$ we check it by computer. For $r > 2$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1,2	1	0,1,2	≥ 1	≥ 0	0	≥ 1
03,13	2	03,13	≥ 0	≥ 0	0	≥ 0
$a43$, $a \neq 2$	2	43	1	≥ 0	0	≥ 1
04,14	2	04,14	≥ 4	≥ 0	0	≥ 4

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c_2'$ corresponding to $\gamma_2 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$
23,24	2	3	1	≥ -1	-1	1	1
33,34,44	2	4	1	≥ 2	2	2	1
243	3	30	2	1	1	1	1

□

Theorem 30.6. *The local system $\mathcal{H}yp(\mathsf{Char}_4^\times; \mathbb{1})$ in characteristic 3 has finite monodromy.*

Proof. We need to show:

$$V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right) + V(-x) \geq 1.$$

Using the fact that $V(x) + V(-x) = 1$ if $x \neq 0$, we can rewrite the inequality as

$$V(x) \leq V\left(x + \frac{1}{4}\right) + V\left(x + \frac{3}{4}\right)$$

and, following §9, it suffices to prove

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

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 3^r - 1$. Since multiplication by 3 permutes $\gamma_1 = \frac{1}{4}$ and $\gamma_2 = \frac{3}{4}$ modulo 1, we can take $r_1 = 1$. Then, with the notation of §9, we have $(3^2 - 1)\gamma_1 = 02_3$, $h_1 = 2$, $h_2 = 0$, $h_{2,1} = 02_3$, $h_{2,2} = 20_3$. We will prove that

$$[x] \leq [x + h_{r,1}] + [x + h_{r,2}]$$

for every $r \geq 1$ and $0 \leq x \leq 3^r - 1$. For $r \leq 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 2\sum_j v_j + 2\sum_i u_i$
0	1	0	2	0	0	2
01,11	1	1	1	0	0	1
0021,1021	3	021	1	0	0	1
02,12	1	2	2	0	0	2
122,222	1	2	2	0	1	0

The remaining cases are proved by substitution of the last digits, as specified in the following table:

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$	$c_2 = c_2'$
2021	4	221	3	1	1	0	1	1
121,022	3	11	2	2	2	0	1	0
221	3	21	2	1	1	0	1	1

$\square$

Theorem 30.7. *The following statements hold.*

(i) *The sheaf* $\mathcal{H}_8 := \mathcal{H}yp(\mathsf{Char}_{15}^{\times}; \mathsf{Char}_9 \smallsetminus \mathsf{Char}_3^{\times})$ *in characteristic* 2 *has* $G = G_{\rm geom} = W(E_8)$ *in its reflection representation. Conversely, if* $\mathcal{H}$ *is a geometrically irreducible hypergeometric sheaf of type* $(8,7)$ *in some characteristic* p *with* $G_{\rm geom} = W(E_8)$ *in its reflection representation, then* $p = 2$ *and* $\mathcal{H}' \cong \mathcal{H}_8$.

(ii) *The sheaf* $\mathcal{H}_6 := \mathcal{H}yp(\mathsf{Char}_9^{\times}; \mathsf{Char}_5)$ *in characteristic* 2 *has* $G = G_{\rm geom} = W(E_6) \cong \mathrm{SU}_4(2)\cdot 2$ *in its reflection representation. Conversely, if* $\mathcal{H}'$ *is a geometrically irreducible hypergeometric sheaf of type* $(6,5)$ *in some characteristic* p *with* $G_{\rm geom} = W(E_6)$ *in its reflection representation, then* $p = 2$ *and* $\mathcal{H}' \cong \mathcal{H}_6$.

(iii) *The sheaf* $\mathcal{H}_6' := \mathcal{H}yp(\mathsf{Char}_7^{\times}; \xi_9^{1,3,4,6,7})$ *in characteristic* 2 *has* $G = G_{\rm geom} \cong 6_1\cdot \mathrm{PSU}_4(3)\cdot 2_2$, *the Mitchell group, in its reflection representation.*

(iv) *The sheaf* $\mathcal{H}_4 := \mathcal{H}yp(\mathsf{Char}_5^{\times}; \mathsf{Char}_4 \smallsetminus \{\mathbb{1}\})$ *in characteristic* 3 *has* $G = G_{\rm geom} \cong 3\times \mathrm{Sp}_4(3)$ *in its reflection representation.*

(v) *The sheaf* $\mathcal{H}_2 := \mathcal{H}yp(\mathsf{Char}_3^{\times}; \xi_2)$ *in characteristic* 5 *has* $G = G_{\rm geom} \cong \mathrm{SL}_2(5)\times 5$ *in its reflection representation.*

(vi) *The sheaf* $\mathcal{H}_2' := \mathcal{H}yp(\mathsf{Char}_4^{\times}; \mathbb{1})$ *in characteristic* 3 *has* $G = G_{\rm geom} \cong \mathrm{SL}_2(3)$ *in its reflection representation.*

Proof. (i) By Theorem 30.1, G is finite. Moreover, the shape of $\mathcal{H}_8$ shows by Proposition 3.7 that it is primitive, and the field of traces is $\mathbb{Q}$ by Proposition 6.1(iii). In particular, $\mathbf{Z}(G) \le C_2$. Next, by [KT9, Theorem 5.6], $G = \mathbf{Z}(G)G_0$, where $G_0 = W(E_8)$ in its reflection representation. As $\mathbf{Z}(G_0) = C_2$ is central in G, we conclude that $\mathbf{Z}(G) \le G_0$ and hence $G = G_0$, as stated.

Conversely, we consider $\mathcal{H}$ with geometric monodromy group $H = G_{\rm geom} \cong W(E_8)$ in its reflection representation. Every complex reflection in H has order 2. Hence any non-identity element h in the image of $P(\infty)$ in H has order 2, and thus $p = 2$. Next, h is a $2F$-involution, in the notation of [GAP]. As usual, let h_0 generate the image of $I(0)$ in H, and let h_∞, of p'-order, generate the image of $I(\infty)$ modulo $P(\infty)$ in H. As $2 \nmid \mathsf{o}(h_\infty)$,h_∞ has simple spectrum on Tame (of dimension 7) and centralizes h, we see using [GAP] that h_∞ has order 7 (of class $7A$), 9 (of class $9A$), or 15 (of class $15A$). Inspecting the spectrum of h_∞, we see that in each of these three cases, 1 is an eigenvalue of multiplicity 2, hence it must occur on both Wild and Tame. It follows that the set of "downstairs" characters of $\mathcal{H}$ is

$$\mathsf{Char}(7),\ \{\xi_9^i \mid i = 0,1,2,4,5,7,8\},\ \mathsf{Char}_{\rm ntriv}(3) \sqcup \mathsf{Char}(5), \tag{30.7.1}$$

respectively. On the other hand, h_0 can belong to either class $9B$ or $15B$, and so the set of "upstairs" characters of $\mathcal{H}$ is $\mathsf{Char}_{\rm ntriv}(9)$ or $\mathsf{Char}^{\times}(15)$, respectively. If the "upstairs" set is $\mathsf{Char}_{\rm ntriv}(9)$, then the "downstairs" set must be $\mathsf{Char}(7)$, in which case $G_{\rm geom} = \mathsf{S}_9$ by [KT5, Theorem 9.3]. Hence the "upstairs" set is $\mathsf{Char}^{\times}(15)$. The first and the third of the three possibilities listed in (30.7.1) for the "downstairs" set lead to local systems that fail the V-test and thus have infinite $G_{\rm geom}$. The middle candidate gives rise to $\mathcal{H} \cong \mathcal{H}_8$.

(ii) By Theorem 30.2, G is finite. Moreover, the shape of $\mathcal{H}_6$ shows by Proposition 3.7 that it is primitive, and the field of traces is $\mathbb{Q}$ by Proposition 6.1(iii). In particular, $\mathbf{Z}(G) \le C_2$. Next, by [KT9, Theorem 4.8], $G = \mathbf{Z}(G)G_0$ where G_0 is the normal closure of the image of $P(\infty)$ in G and

$G_0 = W(E_6)$ in its reflection representation (note that G_0 cannot be the Mitchell group because $\mathbf{Z}(G) \leq C_2$). As $\mathbf{Z}(G_0) \leq C_2$, G/G_0 is a 2-group. On the other hand, G/G_0 has odd order by Theorem 5.3. Hence $G = G_0$, as stated.

Conversely, we consider $\mathcal{H}$ with geometric monodromy group $H = G_{\rm geom} \cong W(E_6)$ in its reflection representation. Every complex reflection in H has order 2. Hence any non-identity element h in the image of $P(\infty)$ in H has order 2, and thus $p = 2$. Next, h is a $2C$-involution, in the notation of [GAP]. With h_0 and h_∞ as defined in (i), $2 \nmid \mathsf{o}(h_\infty)$, h_∞ has simple spectrum on Tame (of dimension 5) and centralizes h. Using [GAP] we see that h_∞ belongs to class $5A$, and so the set of "downstairs" characters of $\mathcal{H}$ is Char_5. On the other hand, as h_0 has odd order and has simple spectrum on $\mathcal{H}$, it can belong to class $9A$, and so the set of "upstairs" characters of $\mathcal{H}$ is $\mathsf{Char}_9^\times$, showing $\mathcal{H} \cong \mathcal{H}_6$.

(iii) By Theorem 30.3, G is finite. Moreover, the shape of $\mathcal{H}_6'$ shows by Proposition 3.7 that it is primitive, and the field of traces is contained in $\mathbb{Q}(\zeta_3)$ by Proposition 6.1(iii). In particular, $\mathbf{Z}(G) \leq C_6$. Next, by [KT9, Theorem 4.8], $G = \mathbf{Z}(G)G_0$ where G_0 is the normal closure of the image of $P(\infty)$ in G, and G_0 is either $W(E_6)$ or the Mitchell group in their reflection representations. Since g_0 has central order 7, $G_0 \neq W(E_6)$, and thus $G_0 = 6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$, the Mitchell group. As $\mathbf{Z}(G_0) = C_6$ centralizes G, we conclude that $\mathbf{Z}(G) \leq G$ and $G = G_0$, as stated.

(iv) By Theorem 30.4, G is finite. Moreover, the shape of $\mathcal{H}_4$ shows by Proposition 3.7 that it is primitive, and the field of traces is $\mathbb{Q}(\zeta_3)$ by Corollary 6.2(ii). In particular, $\mathbf{Z}(G) \leq C_6$. Recall that any element $1 \neq h$ in the image of $P(\infty)$ in G acts a complex reflection of order 3. Hence, by Bagnera's theorem, see [Mit, Theorem 2], $G/\mathbf{Z}(G) \cong S = \mathrm{PSp}_4(3)$. Since irreducible projective representations of degree 4 of S can only lift to linear representations of $L = \mathrm{Sp}_4(3)$, which are not stable under outer automorphisms of L, we have that $G = \mathbf{Z}(G)L$. Now $\mathbf{Z}(G) \geq \mathbf{Z}(L) \cong C_2$. But L does not contain complex reflections (of order 3), we must have $\mathbf{Z}(G) = C_6$ and thus $G = 3 \times L$, as stated.

(v) By Theorem 30.5, G is finite. Moreover, the shape of $\mathcal{H}_2$ shows by Proposition 3.7 that it is primitive, and the field of traces is contained in $\mathbb{Q}(\zeta_5)$ by Proposition 6.1(iii). In particular, $\mathbf{Z}(G) \leq C_{10}$. Since $D = 2$, G satisfies $(\mathbf{S}+)$, and the existence of a non-trivial element h in the image of $P(\infty)$, which acts as the scalar ζ_5 on Wild and 1 on Tame rules out the extraspecial normalizer case of Lemma 3.1. Thus G is almost quasisimple, and one quickly deduces that $G = \mathbf{Z}(G)\mathrm{SL}_2(5)$; in particular $2 \mid |\mathbf{Z}(G)|$. The existence of h now implies that in fact $|\mathbf{Z}(G)| = 10$ and $G = \mathrm{SL}_2(5) \times 5$.

(vi) By Theorem 30.6, G is finite. Moreover, the shape of $\mathcal{H}_2'$ shows by Proposition 3.7 that it is primitive, and the field of traces is $\mathbb{Q}(\zeta_3)$ by Corollary 6.2(ii). In particular,

$$\mathbf{Z}(G) \leq C_6. \tag{30.7.2}$$

Since $D = 2$, G satisfies $(\mathbf{S}+)$, and the trace field $\mathbb{Q}(\zeta_3)$ rules out the almost quasisimple extraspecial case of Lemma 3.1 (which would imply $G \rhd \mathrm{SL}_2(5)$ with $\mathbb{Q}(\sqrt{5})$ contained in the trace field), as well as the case of $R = E * C_4$ in the extraspecial normalizer case (which would imply the existence of a trace $2\sqrt{-1}$). Thus $R \lhd G \leq \mathbf{N}_{\mathrm{GL}(V)}(R)$, where $V = \mathbb{C}^2$, and $R \cong D_8 = 2_+^{1+2}$ or $R \cong Q_8 = 2_-^{1+2}$. Next, a nontrivial element h in the image of $P(\infty)$ acts on V with eigenvalues 1 and ζ_3, hence inducing an automorphism of order 3 of R. As $\mathrm{Aut}(D_8)$ is a 2-group, it follows that $R \cong Q_8$. Since R is irreducible on V, we have that $\mathbf{C}_G(R) = \mathbf{Z}(G)$, and so $G/\mathbf{Z}(G) \hookrightarrow \mathrm{Aut}(R) \cong \mathsf{S}_4$.

Suppose that $G/\mathbf{Z}(G) \cong \mathsf{S}_4$. Then the representation Φ of G on V gives a degree 2 irreducible projective representation of S_4, which is realized by a degree 2 irreducible representation Ψ of a double cover $H = 2 \cdot \mathsf{S}_4$. Furthermore, the induced projective representation $\overline{\Phi} : G \to \mathrm{PGL}(V)$ is faithful on $R/\mathbf{Z}(R) \cong C_2^2$. Hence, Ψ cannot be a linear representation of S_4 (otherwise its image would be $\cong \mathsf{S}_3$), and so it must be a faithful representation of H. Using the character table of H given in [GAP], we can find an element $g \in G$ and a root of unity γ with $\mathrm{Tr}(\gamma\Phi(g)) = \sqrt{-2}$. On the other hand, $\mathrm{Tr}(\Phi(g)) = a+b\zeta_3$ for some $a, b \in \mathbb{Z}$. It follows that $2 = |\mathrm{Tr}(\gamma\Phi(g))|^2 = |\mathrm{Tr}(g)|^2 = a^2-ab+b^2$, i.e. $(2a-b)^2+3b^2 = 8$, a contradiction.

As both $R/\mathbf{Z}(R) \cong C_2^2$ and C_3 inject in $G/\mathbf{Z}(G)$, we conclude that $G/\mathbf{Z}(G) \cong \mathsf{A}_4$. Suppose $\mathbf{Z}(G) > \mathbf{Z}(R)$. Then (30.7.2) implies that $\mathbf{Z}(G) = C_3 \times \mathbf{Z}(R)$. It follows that R is a normal subgroup of index 9 in G. As a generator g_0 of the image of $I(0)$ in G has order 4, the normal closure G_0 of the image of $I(0)$ in G is contained in R, and so 9 divides $|G/G_0|$, contradicting Theorem 5.2. Thus $\mathbf{Z}(G) = \mathbf{Z}(R) \cong C_2$. Note that the representation $\Phi|_R : R \to \mathrm{GL}(V)$ extends to a symplectic, faithful representation $\Theta : L \to \mathrm{GL}(V)$, with $R \lhd L \cong \mathrm{SL}_2(3) \cong 2 \cdot \mathsf{A}_4$. In particular, an element $t \in L$ of order 3 induces on R the same automorphism as the one induced by h, and $\mathrm{Tr}(\Theta(h)) = -1$. Thus $\Phi(g) = \xi\Theta(h)$ for some root of unity ξ, and, since $1+\zeta_3 = \mathrm{Tr}(\Phi(g)) = \xi\mathrm{Tr}(\Theta(h))$, we get $\xi = \zeta_3^2$, i.e. $\Phi(g) = \zeta_3^2\Theta(h)$. Now we have

$$G = \langle R, g\rangle \cong \langle \Phi(R), \Phi(g)\rangle \cong \langle \Theta(R), \Theta(h)\rangle \cong \mathrm{SL}_2(3).$$

[In fact, Φ is Θ tensored with the faithful linear character of L/R sending h to ζ_3^2.] $\square$

Theorem 30.8. *For the hypergeometric sheaves listed in Theorem 30.7, the following statements hold.*

(i) *$\mathcal{H} = \mathcal{H}_8$ in Theorem* 30.7(i) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_2$, which over any finite extension k of $\mathbb{F}_2$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = W(E_8)$.*

(ii) *$\mathcal{H} = \mathcal{H}_6$ in Theorem* 30.7(ii) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_2$, which over any finite extension k of $\mathbb{F}_4$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = W(E_6)$.*

(iii) *$\mathcal{H} = \mathcal{H}'_6$ in Theorem* 30.7(iii) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_4$, which over any finite extension k of $\mathbb{F}_4$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = 6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$.*

(iv) *$\mathcal{H} = \mathcal{H}_4$ in Theorem* 30.7(iv) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_3$, which over any finite extension k of $\mathbb{F}_3$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = 3 \times \mathrm{Sp}_4(3)$.*

(v) *$\mathcal{H} = \mathcal{H}_2$ in Theorem* 30.7(v) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_5$, which over any finite extension k of $\mathbb{F}_5$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = 5 \times \mathrm{SL}_2(5)$.*

(vi) *$\mathcal{H} = \mathcal{H}'_2$ in Theorem* 30.7(vi) *has a descent $\mathcal{H}_\sharp$ to $\mathbb{F}_3$, which over any finite extension k of $\mathbb{F}_3$ has arithmetic and geometric monodromy groups $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp} = \mathrm{SL}_2(3)$.*

Proof. (i) Note by Theorem 7.5 that $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 33) to $\mathbb{F}_2$, for which over any extension $k \supseteq \mathbb{F}_2$, any element in its arithmetic monodromy group still has rational trace. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \le \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \le C_2$. Since $G_{\mathrm{geom},\mathcal{H}_\sharp} = W(E_8)$ by Theorem 30.7(i), we have $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = C_2$. Next, $G_{\mathrm{geom},\mathcal{H}_\sharp}$ induces a subgroup C_2 of $\mathrm{Out}(L)$ for $L := [W(E_8), W(E_8)] \cong 2 \cdot \Omega^+8(2)$, and the representation of L on $\mathbb{C}^8$ is not stable under any outer automorphism of order 3 in $\mathrm{Out}(L)$. As $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(L) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$, we conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = W(E_8)$.

(ii) Note by Theorem 7.5 that $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 34) to $\mathbb{F}_2$, for which over any extension $k \supseteq \mathbb{F}_2$, any element in its arithmetic monodromy group still has rational trace. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \le \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \le C_2$. Next, $G_{\mathrm{geom},\mathcal{H}_\sharp} = W(E_6)$ induces the full group $\mathrm{Out}(L) \cong C_2$ for $L := [W(E_6), W(E_6)] \cong \mathrm{SU}_4(2)$, and $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(L) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$. Hence, we conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = W(E_6)\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$, and $W(E_6)$ has index ≤ 2 in it. In particular, if $k \supseteq \mathbb{F}_4$, then $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = W(E_6)$.

(iii) Note by Theorem 7.7 that $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 35) to $\mathbb{F}_4$, for which over any extension $k \supseteq \mathbb{F}_4$, any element in its arithmetic monodromy group still has trace in $\mathbb{Q}(\zeta_3)$. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \le \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \le C_6$. Since $G_{\mathrm{geom},\mathcal{H}_\sharp} = 6_1 \cdot \mathrm{PSU}_4(3) \cdot 2_2$, the Mitchell group, by Theorem 30.7(iii), we have $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = C_6$. Next, $G_{\mathrm{geom},\mathcal{H}_\sharp}$ induces a subgroup 2_2 of $\mathrm{Out}(L)$ for $L := [G_{\mathrm{geom},\mathcal{H}_\sharp}, G_{\mathrm{geom},\mathcal{H}_\sharp}] \cong 6_1 \cdot \mathrm{PSU}_4(3)$, and the representation of L on $\mathbb{C}^6$ is not stable under any larger subgroup of $\mathrm{Out}(L)$. As $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(L) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$, we conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp}$.

(iv) By Theorem 7.5, $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 36) to $\mathbb{F}_3$, for which over any extension $k \supseteq \mathbb{F}_3$, any element in its arithmetic monodromy group still has trace in $\mathbb{Q}(\zeta_3)$. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \leq \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \leq C_6$. Since $G_{\mathrm{geom},\mathcal{H}_\sharp} = 3 \times \mathrm{Sp}_4(3)$ by Theorem 30.7(iv), we have $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = C_6$. Next, the representation of $L := [G_{\mathrm{geom},\mathcal{H}_\sharp}, G_{\mathrm{geom},\mathcal{H}_\sharp}] \cong \mathrm{Sp}_4(3)$ on $\mathbb{C}^4$ is not stable under any outer automorphism of L, and $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(L) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$. We conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp}$.

(v) By Theorem 7.5, $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 37) to $\mathbb{F}_5$, for which over any extension $k \supseteq \mathbb{F}_5$, any element in its arithmetic monodromy group still has trace in $\mathbb{Q}(\zeta_5)$. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \leq \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \leq C_{10}$. Since $G_{\mathrm{geom},\mathcal{H}_\sharp} = 5 \times \mathrm{SL}_2(5)$ by Theorem 30.7(v), we have $\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) = C_{10}$. Next, the representation of $L := [G_{\mathrm{geom},\mathcal{H}_\sharp}, G_{\mathrm{geom},\mathcal{H}_\sharp}] \cong \mathrm{SL}_2(5)$ on $\mathbb{C}^2$ is not stable under any outer automorphism of L, and $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(L) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$. We conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp}$.

(vi) By Theorem 7.5, $\mathcal{H}$ has a descent $\mathcal{H}_\sharp = \mathcal{H}_{00}$ (listed in Table 4, line 38) to $\mathbb{F}_3$, for which over any extension $k \supseteq \mathbb{F}_3$, any element in its arithmetic monodromy group still has trace in $\mathbb{Q}(\zeta_3)$. It follows for $\mathcal{H}_\sharp$ that $\mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \leq \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \leq C_6$. Since $G_{\mathrm{geom},\mathcal{H}_\sharp} = \mathrm{SL}_2(3)$ by Theorem 30.7(v), we have

$$C_2 = \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp}) \leq \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp}) \leq C_6. \tag{30.8.1}$$

Let $R := \mathbf{O}_2(G_{\mathrm{geom},\mathcal{H}_\sharp}) \cong Q_8$. Then $G_{\mathrm{geom},\mathcal{H}_\sharp}$ induces the subgroup A_4 of $\mathrm{Aut}(R) \cong \mathsf{S}_4$, and $\mathbf{C}_{G_{\mathrm{arith},k,\mathcal{H}_\sharp}}(R) = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$. If $G_{\mathrm{arith},k,\mathcal{H}_\sharp}/\mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})$ induces the full group $\mathrm{Aut}(R)$, then the automorphisms of R outside of A_4 fuse the two conjugacy classes of elements of order 3 in $\mathrm{SL}_2(3)$ and force them to have the same rational trace -1, which is a contradiction since they actually have traces $1+\zeta_3$ and $1+\zeta_3^2$ on $\mathbb{C}^2$. Hence we must have that

$$G_{\mathrm{arith},k,\mathcal{H}_\sharp} = \mathbf{Z}(G_{\mathrm{arith},k,\mathcal{H}_\sharp})G_{\mathrm{geom},\mathcal{H}_\sharp}. \tag{30.8.2}$$

Suppose $\mathbf{Z}(G_{\mathrm{arith},\mathbb{F}_3,\mathcal{H}_\sharp}) \neq \mathbf{Z}(G_{\mathrm{geom},\mathcal{H}_\sharp})$. It follows from (30.8.1) and (30.8.2) that

$$G_{\mathrm{arith},\mathbb{F}_3,\mathcal{H}_\sharp} = \langle \boldsymbol{z} \rangle \times G_{\mathrm{geom},\mathcal{H}_\sharp},$$

where $\boldsymbol{z}$ acts via scalar ζ_3 on $\mathbb{C}^2$. In this case, we may assume that modulo $G_{\mathrm{geom},\mathcal{H}_\sharp} = \mathrm{SL}_2(3)$, any element in $G_{\mathrm{arith},\mathbb{F}_3,\mathcal{H}_\sharp}$ is $\boldsymbol{z}^{\deg}$. Recall from Theorem 30.7(vi) that $G_{\mathrm{geom},\mathcal{H}_\sharp}$ acts on $\mathbb{C}^2$ via one of its non-self-dual irreducible representations of degree 2. Hence, any element $Frob_{u,\mathbb{F}_{81}}$ has trace $\pm 2\zeta_3$ or of absolute value 0 or 1. However, a computation using [Mag] shows that some elements $Frob_{u,\mathbb{F}_{81}}$ have trace 2 and -2, a contradiction. We conclude that $G_{\mathrm{arith},k,\mathcal{H}_\sharp} = G_{\mathrm{geom},\mathcal{H}_\sharp}$. □

31. Further local systems for $\mathrm{Sp}_6(2)$, $\mathrm{SU}_3(3)$, ${}^2G_2(3)$, and $2\mathsf{A}_7$

In this section, we obtain new local systems realizing $\mathrm{Sp}_6(2)$ and its subgroups $G_2(2)' \cong \mathrm{SU}_3(3)$ and ${}^2G_2(3) \cong \mathrm{SL}_2(8) \rtimes C_2$. We also obtain new local systems realizing $2\mathsf{A}_7$. These are "exotic" exponential sums with finite monodromy, exotic in the sense that the finiteness of their monodromy does not result from van der Geer-van der Vlugt, cf. [KT9].

Theorem 31.1. *The local system $\mathcal{H}(\mathsf{Char}_7; \xi_6, \xi_6^5, \xi_2)$ in characteristic $p = 5$ has finite monodromy.*

Proof. We need to show:

$$V(7x) + V\left(-x + \frac{1}{2}\right) + V\left(-x + \frac{1}{6}\right) + V\left(-x - \frac{1}{6}\right) \geq \frac{3}{2}.$$

Using the fact that $V(\frac{i}{42}) = V(\frac{372i}{5^6-1}) = \frac{1}{24}[372i]$ for $1 \leq i \leq 41$ we check that the inequality holds for $7x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \neq 0$, we can rewrite the inequality as

$$V(7x) \leq V\left(x + \frac{1}{2}\right) + V\left(x + \frac{5}{6}\right) + V\left(x + \frac{1}{6}\right) - \frac{1}{2}$$

and, via the change of variable $x \mapsto x + \frac{1}{2}$, as

$$V\left(7x + \frac{1}{2}\right) \leq V\left(x + \frac{1}{3}\right) + V\left(x + \frac{2}{3}\right) + V(x) - \frac{1}{2}.$$

Following §9, it suffices to prove

$$\left[7x + \frac{5^r - 1}{2}\right] \leq \left[x + \frac{5^r - 1}{3}\right] + \left[x + \frac{2(5^r - 1)}{3}\right] + [x] - 2r$$

for every $r \geq 1$ divisible by $r_0 = 2$ and every $0 \leq x \leq 5^r - 1$. Notice that, in this case, multiplication by 5 permutes $\gamma_1 = \frac{1}{3}$ and $\gamma_2 = \frac{2}{3}$, so we can take $r_1 = 1$. Then, with the notation of §9, we have $(5^2 - 1)\gamma_1 = 13_5$, $h_1 = 3$, $h_2 = 1$. We will prove that

$$\left[7x + \frac{5^r - 1}{2}\right] \leq [x + h_{r,1}] + [x + h_{r,2}] + [x] - 2r$$

for every $r \geq 1$ and every $0 \leq x \leq 5^r - 1$. For $r \leq 4$ we check it by computer. For $r > 4$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 4\sum_j v_j + 4\sum_i u_i$
0,1	1	0,1	0	≥ 0	0	≥ 0
$a2, a3; a \neq 3$	1	2,3	0	≥ 0	0	≥ 0
$a4; a \neq 1, 3$	1	4	4	≥ 0	0	≥ 4
$a32; a \neq 1, 3$	2	32	4	≥ 0	0	≥ 4
$a132; a \neq 3$	3	132	0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_3 = c'_3$ corresponding to $\gamma_3 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b'_1$	$c_1 = c'_1$	$c_2 = c'_2$
3132	4	320	3	4	4	10	1	1
332	3	33	2	4	4	10	1	1
33,34	2	32	2	4	4	10	1	1
14	2	2	1	4	0	3	0	1

□

Theorem 31.2. (a) *The local system $\mathcal{H} := \mathcal{H}(\mathsf{Char}_7; \xi_6, \xi_6^5, \xi_2)$ in characteristic $p = 5$ has geometric monodromy group $G_{\mathrm{geom}} = \mathrm{Sp}_6(2)$. Furthermore, $\mathcal{H}$ has a descent $\mathcal{H}_{00}$ to $\mathbb{F}_5$, whose arithmetic monodromy group $G_{\mathrm{arith},k}$ over any finite extension k of $\mathbb{F}_5$ is $2 \times \mathrm{Sp}_6(2)$ if $2 \nmid [k : \mathbb{F}_5]$ and $\mathrm{Sp}_6(2)$ is $2|[k : \mathbb{F}_5]$.*

(b) *The local system* $\mathcal{F}$ *on* $\mathbb{A}^1$ *with trace function* $t \mapsto -\sum_x \psi(x^7 + tx^3)\xi_2(x)$ *in characteristic* $p = 5$ *has geometric monodromy group* $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_6(2)$. *Over a finite extension* k *of* $\mathbb{F}_5$, *the arithmetic monodromy group* $G_{\mathrm{arith},k,\mathcal{G}}$ *of* $\mathcal{G} := \mathcal{F} \otimes (-\mathsf{Gauss})^{-\deg}$ *is* $2 \times \mathrm{Sp}_6(2)$ *if* $2 \nmid [k : \mathbb{F}_5]$ *and* $\mathrm{Sp}_6(2)$ *is* $2|[k : \mathbb{F}_5]$.

Proof. (a) By Theorem 31.1, $G = G_{\mathrm{geom}}$ is finite. Furthermore, G is primitive by [KT9, Lemma 12.8], but the rank is 7, so it satisfies ($\mathbf{S}+$). Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G underlying $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}$. Moreover, a generator g_0 of the image $I(0)$ in G has central order 7, and the image Q of $P(\infty)$ is of order 5 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(ii). Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars, $\mathbb{Q}(\varphi) = \mathbb{Q}$, and the geometric determinant is trivial [Ka4, Lemma 8.11.6], we have that

$$\mathbf{Z}(G) = 1. \tag{31.2.1}$$

Suppose G satisfies conclusion (c) of Lemma 3.1. Then G contains an irreducible normal 7-subgroup R, and

$$G/\mathbf{C}_G(R)R \hookrightarrow \mathrm{Out}(R) \hookrightarrow \mathrm{Sp}_2(7).$$

But this is a contradiction, since $\mathbf{C}_G(R) = \mathbf{Z}(G) = 1$ by (31.2.1), and 5 divides $|G|$ but not $|\mathrm{Sp}_2(7)|$.

Thus G is almost quasisimple. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G) = 1$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 7$ and $|Q| = 5$ we have that $5 \cdot 7$ divides the order of $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to see that either $S = L = \mathsf{A}_8$ or $S = L = \mathrm{Sp}_6(2)$. In either case, since $7 \nmid |\mathrm{Out}(S)|$, g_0 must lie in S, whence $G_{\mathrm{geom}} = S$ by Theorem 5.1. We also note that a generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has central order divisible by 4 while acting on Wild, see Proposition 5.8(iii), and by 3 while acting on Tame, hence $12|\bar{\mathsf{o}}(g_\infty)$. This rules out the possibility $G = \mathsf{A}_8$, and we conclude that $G = \mathrm{Sp}_6(2)$.

Next we consider $\mathcal{H}_{00}$, with $\mathcal{H}_0$ given on line 42 of Table 4. To identify $G_{\mathrm{arith},k}$, since the representation is orthogonal and the geometric determinant is trivial, we know that the arithmetic determinant is either trivial or $(-1)^{\deg}$. Note $\mathcal{G}$ (with ψ replaced by $x \mapsto \psi(-7x)$) is the $[7]^\star$ Kummer pullback of $\mathcal{H}_{00}$ by [KT6, Corollary 3.10]. By [KT1, Theorem 2.5(4)], $\mathcal{G}$ has arithmetic determinant $(-1)^{\deg}$, therefore the same holds for $\mathcal{H}_{00}$. On the other hand, $\mathbf{Z}(G_{\mathrm{arith},k}) \leq C_2$, so $\mathrm{Sp}_6(2) = G_{\mathrm{geom}} \lhd G_{\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2)$, and the statement for $G_{\mathrm{arith},k}$ follows.

(b) Since $\mathcal{G}$ is the $[7]^\star$ Kummer pullback of $\mathcal{H}_{00}$ by [KT6, Corollary 3.10], we have that $1 \neq G_{\mathrm{geom},\mathcal{F}} \lhd G_{\mathrm{geom}} = \mathrm{Sp}_6(2)$, whence $G_{\mathrm{geom},\mathcal{F}} = \mathrm{Sp}_6(2)$. Now,

$$\mathrm{Sp}_6(2) = G_{\mathrm{geom},\mathcal{F}} \lhd G_{\mathrm{arith},k,\mathcal{G}} \leq G_{\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2),$$

and, as mentioned above, the arithmetic determinant of $\mathcal{G}$ is $(-1)^{\deg}$. Hence we conclude that $G_{\mathrm{arith},k,\mathcal{G}} = G_{\mathrm{arith},k}$. □

Remark 31.3. Let us consider the local system on $\mathbb{A}^2/\mathbb{F}_5$ with coordinates (t,u)

$$\mathcal{F}_{t,u} : (t,u) \mapsto -\sum_x \psi(x^7 + tx^3 + ux)\xi_2(x).$$

By Theorem 31.2, the pullback $\mathcal{F}_{t,0}$ has $G_{\mathrm{geom}} = \mathrm{Sp}_6(2)$. One knows [Ka5, Theorem 4.12] that the pullback $\mathcal{F}_{0,u}$ has $G_{\mathrm{geom}} = G_2(\mathbb{C})$. The group G_{geom} for $\mathcal{F}_{t,u}$ on $\mathbb{A}^2$ lies in SO_7 (it a priori lies in O_7, but its geometric determinant, having order dividing 2, is geometrically constant on $\mathbb{A}^2$; being trivial on the line $u = 0$, it is trivial). It follows that the group G_{geom} for $\mathcal{F}_{t,u}$ on $\mathbb{A}^2$ is all of SO_7, as it lies in SO_7 and contains both $\mathrm{Sp}_6(2)$ and $G_2(\mathbb{C})$. We now apply Pink's specialization theorem

[Ka4, Theorem 8.18.2] to $\mathcal{F}_{t,u}$ and the projections onto the t and u lines respectively. We find that for all but finitely many $t_0 \in \overline{\mathbb{F}_5}$, $\mathcal{F}_{t_0,u}$ on the u line has group SO_7, but that at time $t_0 = 0$ it has group $G_2(\mathbb{C})$. Similarly, we find that for all but finitely many $u_0 \in \overline{\mathbb{F}_5}$, $\mathcal{F}_{t,u_0}$ on the t line has group SO_7, but that at time $u_0 = 0$ it has group $\mathrm{Sp}_6(2)$. Are there other curves in (t,u) space along which $\mathcal{F}$ has group G_2? Along which $\mathcal{F}$ has group $\mathrm{Sp}_6(2)$?

Theorem 31.4. *The local system $\mathcal{F}$ on $\mathbb{A}^2$ with trace function $(s,t) \mapsto -\sum_x \psi(x^7 + sx^5 + tx)\xi_2(x)$ in characteristic $p = 3$ has finite monodromy.*

Proof. By [KRLT1, Theorem 2.12], it suffices to prove

$$\left[7a + 5b + \frac{3^r - 1}{2}\right] \leq [a] + [b] + r + 2$$

for every $r \geq 1$ and every $a, b \in \{0, 1, \ldots, 3^r - 1\}$, where $[x] := [x]_3$ denotes the sum of the 3-adic digits of x. We proceed by induction on r. For $r \leq 3$, we check it by computer. For $r > 3$ we distinguish the following cases (where, for each case, it is implicitly assumed that the previous cases do not apply).

Case 1: The last (3-adic) digits of a and b are not $(1,0)$. Write $a = 3 \cdot a_1 + a_0$ and $b = 3 \cdot b_1 + b_0$ with $(a_0, b_0) \in \{0,1,2\}^2 \smallsetminus \{(1,0)\}$. Then it is easily checked by computer that $[7a_0 + 5b_0 + 1] \leq [a_0] + [b_0] + 1$, so

$$\begin{aligned}
\left[7a + 5b + \frac{3^r - 1}{2}\right] &= \left[3 \cdot \left(7a_1 + 5b_1 + \frac{3^{r-1} - 1}{2}\right) + (7a_0 + 5b_0 + 1)\right] \\
&\leq \left[7a_1 + 5b_1 + \frac{3^{r-1} - 1}{2}\right] + [7a_0 + 5b_0 + 1] \\
&\leq [a_1] + [b_1] + (r-1) + 2 + [a_0] + [b_0] + 1 \\
&= [a] + [b] + r + 2
\end{aligned}$$

by induction hypothesis.

Case 2: The last two digits of a and b are not $(01_3, 10_3)$ or $(21_3, 00_3)$. Write $a = 3^2 \cdot a_1 + a_0$ and $b = 3^2 \cdot b_1 + b_0$ with $a_0, b_0 < 3^2$ and $(a_0, b_0) \notin \{(01_3, 10_3), (21_3, 00_3)\}$. Then it is easily checked by computer that $[7a_0 + 5b_0 + 4] \leq [a_0] + [b_0] + 2$, so

$$\begin{aligned}
\left[7a + 5b + \frac{3^r - 1}{2}\right] &= \left[3^2 \cdot \left(7a_1 + 5b_1 + \frac{3^{r-2} - 1}{2}\right) + (7a_0 + 5b_0 + 4)\right] \\
&\leq \left[7a_1 + 5b_1 + \frac{3^{r-2} - 1}{2}\right] + [7a_0 + 5b_0 + 4] \\
&\leq [a_1] + [b_1] + (r-2) + 2 + [a_0] + [b_0] + 2 \\
&= [a] + [b] + r + 2
\end{aligned}$$

by induction hypothesis.

Case 3: The last three digits of a and b are not $(001_3, 110_3)$ or $(201_3, 010_3)$. Write $a = 3^3 \cdot a_1 + a_0$ and $b = 3^3 \cdot b_1 + b_0$ with $a_0, b_0 < 3^3$ and $(a_0, b_0) \notin \{(001_3, 110_3), (201_3, 010_3)\}$. Then it is easily checked by computer that $[7a_0+5b_0+13] \le [a_0]+[b_0]+3$, so

$$\begin{aligned}\left[7a+5b+\frac{3^r-1}{2}\right] &= \left[3^3\cdot\left(7a_1+5b_1+\frac{3^{r-3}-1}{2}\right)+(7a_0+5b_0+13)\right]\\ &\le \left[7a_1+5b_1+\frac{3^{r-3}-1}{2}\right]+[7a_0+5b_0+13]\\ &\le [a_1]+[b_1]+(r-3)+2+[a_0]+[b_0]+3\\ &= [a]+[b]+r+2\end{aligned}$$

by induction hypothesis.

Case 4: The last three digits of a and b are $(001_3, 110_3)$ or $(201_3, 010_3)$. Write $a = 3^2\cdot a_1+1$ and $b = 3^2\cdot b_1+3$, and let $a' = 3\cdot a_1+1$ and $b' = 3\cdot b_1$. Then the last digit of $7a_1+5b_1+\frac{3^{r-2}-1}{2}$ is 0, and $7\cdot 1+5\cdot 3+\frac{3^2-1}{2} = 26 = 222_3$ and $7\cdot 1+5\cdot 0+\frac{3-1}{2} = 8 = 22_3$, so there are no digit carries in either of the sums

$$7a+5b+\frac{3^r-1}{2} = 3^2\cdot\left(7a_1+5b_1+\frac{3^{r-2}-1}{2}\right)+\left(7\cdot 1+5\cdot 3+\frac{3^2-1}{2}\right)$$

and

$$7a'+5b'+\frac{3^{r-1}-1}{2} = 3\cdot\left(7a_1+5b_1+\frac{3^{r-2}-1}{2}\right)+\left(7\cdot 1+5\cdot 0+\frac{3^1-1}{2}\right).$$

Therefore,

$$\begin{aligned}\left[7a+5b+\frac{3^r-1}{2}\right] &= \left[7a_1+5b_1+\frac{3^{r-2}-1}{2}\right]+[26]\\ &= \left[7a_1+5b_1+\frac{3^{r-2}-1}{2}\right]+[8]+2\\ &= \left[7a'+5b'+\frac{3^{r-1}-1}{2}\right]+2\\ &\le [a']+[b']+(r-1)+2+2\\ &= [a]+[b]+r+2\end{aligned}$$

by induction hypothesis. ☐

Theorem 31.5. *The local system $\mathcal{F}|_{s=-1}$ on $\mathbb{A}^1$ with trace function $t \mapsto -\sum_x \psi(x^7-x^5+tx)\xi_2(x)$ in characteristic $p=3$, has fifth moment $M_{5,0}\neq 0$ and third moment $M_{3,0}\neq 1$.*

Proof. We apply Theorem 6.9, with $(a,b) := (5,0)$, and $q = 3^{11}$, to

$$\mathcal{G} := \mathcal{F}|_{s=-1}\otimes(-\mathsf{Gauss}_{\mathbb{F}_3}(\psi,\xi_2))^{-\deg/\mathbb{F}_3}.$$

A calculation by Magma shows that the traces attained, with their multiplicities, are

$$(-2, \text{mult. } 6534), (-1, \text{mult. } 66430), (0, \text{mult. } 25411), (1, \text{mult. } 78651), (7, \text{mult. } 121).$$

Thus the empirical $M_{5,0}$ computed over $\mathbb{F}_{3^{11}}$ is approximately 10.368676861589527341699266 7107. On the other hand, $\mathcal{G}$ has highest ∞-slope $7/6$, cf. [KRLT1, §1]. So if $M_{5,0}$ were 0, then (conservatively) taking $m := 0$ in Theorem 6.9, we would have its $H_{5,0} = 7^5/6$, so that the empirical $M_{5,0}$ computed over $\mathbb{F}_{3^{11}}$ would be

$$\le 7^5/(6\cdot 3^{11/2}) = 6.6553676092387107161215 7994094.$$

This contradiction shows that $M_{5,0}\neq 0$.

We now show that $M_{3,0} \neq 1$. We argue by contradiction. Because $\mathcal{G}$ has integer traces, if $M_{3,0}$ were one, then $\det(1-TFrob_{\mathbb{F}_3}|H^2_c(\mathbb{A}^1/\overline{\mathbb{F}_3}, \mathcal{G}^{\otimes 3}))$ is an integer polynomial (being the denominator of the L function) of degree one which, by purity, is either $1-3T$ or $1+3T$. Thus the empirical third moment $M_{3,0}$ over $\mathbb{F}_{3^{11}}$ is within $H_{3,0}/3^{11/2} = (1+7^3/6)/3^{11/2} = 0.13819975579367585172406922112 1$ of either 1 or -1. But this empirical moment is 0.0081965824992802587681417128147 8, contradiction. $\square$

Theorem 31.6. *For the local system $\mathcal{G}$ on $\mathbb{A}^2/k$ with trace function*

$$(s,t) \in k \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi_k(x^7 + sx^5 + tx)\xi_2(x)$$

in characteristic $p = 3$, we have the following results.

(a) *The system $\mathcal{G}|_{t=0}$ and the system $\mathcal{H} := \mathcal{H}(\mathsf{Char}_7; \xi_2\mathsf{Char}_5)$ both have geometric monodromy group $G_{t=0,\mathrm{geom}} = \mathrm{Sp}_6(2)$. Next, $\mathcal{H}$ has a descent $\mathcal{H}_{00}$, whose arithmetic monodromy group $G_{t=0,\mathrm{arith},k}$ over any finite extension k of $\mathbb{F}_3$ is $2 \times \mathrm{Sp}_6(2)$ when $2 \nmid [k : \mathbb{F}_3]$ and $\mathrm{Sp}_6(2)$ when $2|[k : \mathbb{F}_3]$. Furthermore, over any finite extension k of $\mathbb{F}_3$, the arithmetic monodromy group of $\mathcal{G}|_{t=0}$ is equal to $G_{t=0,\mathrm{arith},k}$.*

(b) *The system $\mathcal{G}$ has geometric monodromy group $G_{2\text{-}param,\mathrm{geom}} = \mathrm{Sp}_6(2)$. Over any finite extension k of $\mathbb{F}_3$, it has the same arithmetic monodromy group as $\mathcal{G}|_{t=0}$.*

(c) *The system $\mathcal{G}|_{s=0}$ has geometric monodromy group $G_{s=0,\mathrm{geom}} = \mathrm{SU}_3(3)$. Over any finite extension k of $\mathbb{F}_9$, it has arithmetic monodromy group $G_{s=0,\mathrm{arith},k} = \mathrm{SU}_3(3)$. Over $\mathbb{F}_3$, it has arithmetic monodromy group $G_{s=0,\mathrm{arith},\mathbb{F}_3} = \mathrm{SU}_3(3) \cdot 2 \cong G_2(2)$.*

(d) *The system $\mathcal{G}|_{s=-1}$ has geometric monodromy group $G_{s=-1,\mathrm{geom}} = {}^2G_2(3) \cong \mathrm{SL}_2(8) \rtimes C_3$. Over any finite extension k of $\mathbb{F}_3$, it has arithmetic monodromy group $G_{s=-1,\mathrm{arith},k} = 2 \times G_{s=-1,\mathrm{geom}}$ if $2 \nmid [k : \mathbb{F}_3]$ and $G_{s=-1,\mathrm{geom}}$ if $2|[k : \mathbb{F}_3]$.*

Proof. (a) By Theorem 31.4, $\mathcal{G}|_{t=0}$ has finite monodromy, and it is the $[7]^\star$ Kummer pullback of $\mathcal{H}$ by [KT6, Corollary 3.10]. Hence $\mathcal{H}$ also has finite geometric monodromy group H, which is primitive by [KT9, Lemma 12.8]. But the rank is 7, so H satisfies ($\mathbf{S}$+). Let φ denote the character of the representation $H \to \mathrm{GL}(V)$ of H underlying $\mathcal{H}$. By the construction of $\mathcal{H}$ and Corollary 6.2(i), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}$. Next, a generator g_0 of the image $I(0)$ in H has central order 7. Moreover, a generator g_∞ of the image of $I(\infty)$ modulo $P(\infty)$ in G has central order divisible by 2 while acting on Wild, see Proposition 5.8(iii), and by 5 while acting on Tame, hence $10|\bar{\mathsf{o}}(g_\infty)$. Since the cyclic group $\mathbf{Z}(H)$ acts via scalars, $\mathbb{Q}(\varphi) = \mathbb{Q}$, and the geometric determinant is trivial [Ka4, Lemma 8.11.6], we have that

$$\mathbf{Z}(H) = 1. \tag{31.6.1}$$

Suppose H satisfies conclusion (c) of Lemma 3.1. Then H contains an irreducible normal 7-subgroup R, and

$$H/\mathbf{C}_H(R)R \hookrightarrow \mathrm{Out}(R) \hookrightarrow \mathrm{Sp}_2(7).$$

But this is a contradiction, since $\mathbf{C}_H(R) = \mathbf{Z}(H) = 1$ by (31.6.1), and 5 divides $|H|$ but not $|\mathrm{Sp}_2(7)|$.

Thus H is almost quasisimple. Let S denote the unique non-abelian composition factor of H, so that $S = L/\mathbf{Z}(L)$ for $L := E(H) = H^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_H(L) = \mathbf{Z}(H) = 1$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_\infty) = 10$, we have that 10 divides the order of $H/\mathbf{Z}(H) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to see that either $S = L = \mathsf{A}_8$ or $S = L = \mathrm{Sp}_6(2)$. In either case, since $7 \nmid |\mathrm{Out}(S)|$, g_0 must lie in S, whence $H = S$ by Theorem 5.1. Noting that A_8 contains no element of order 10, we conclude that $H = \mathrm{Sp}_6(2)$. Now, the geometric monodromy group $G_{t=0,\mathrm{geom}}$ of $\mathcal{G}|_{t=0}$ is a normal subgroup of index dividing 7 in H, hence it must be equal to H.

Next we identify the arithmetic monodromy group $H_{\mathrm{arith},k}$ of $\mathcal{H}_{00}$ (note $\mathcal{H}_0$ is listed on line 43 of Table 4). Since the representation is orthogonal and the geometric determinant is trivial, we know that the arithmetic determinant of $\mathcal{H}$ is either trivial or $(-1)^{\mathrm{deg}}$. Note $\mathcal{G}$ (with ψ replaced by $x \mapsto \psi(-7x)$) is the $[7]^\star$ Kummer pullback of $\mathcal{H}_{00}$ by [KT6, Corollary 3.10]. By [KT1, Theorem 2.5(4)], $\mathcal{G}$ has arithmetic determinant $(-1)^{\mathrm{deg}}$, therefore the same holds for $\mathcal{H}_{00}$. On the other hand, $\mathbf{Z}(H_{\mathrm{arith},k}) \leq C_2$, so $\mathrm{Sp}_6(2) = H \lhd H_{\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2)$, and the stated structure for $H_{\mathrm{arith},k}$ follows.

Since $\mathcal{G}$ is the $[7]^\star$ Kummer pullback of $\mathcal{H}_{00}$ by [KT6, Corollary 3.10], we have

$$\mathrm{Sp}_6(2) = G_{t=0,\mathrm{geom}} \lhd G_{t=0,\mathrm{arith},k} \leq H_{\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2),$$

and, as mentioned above, the arithmetic determinant of $\mathcal{G}$ is $(-1)^{\mathrm{deg}}$. Hence we conclude that $G_{t=0,\mathrm{arith},k} = H_{\mathrm{arith},k}$.

(b) By Theorem 31.4, $\mathcal{G}$ has finite geometric monodromy group $G = G_{2\text{-param},\mathrm{geom}}$. We first note that its field of traces is $\mathbb{Q}$; indeed over any extension of $\mathbb{F}_3$, the substitution $x \mapsto -x$ shows that the traces of $\mathcal{G}$, a priori in $\mathbb{Q}(\zeta_3)$, are real. Thus the traces lie in $\mathbb{Z}$; and furthermore $\mathcal{G}$ is arithmetically orthogonal. We next note that $\det(\mathcal{G})$ is geometrically trivial. Indeed, the geometric determinant has order dividing 2, but $\mathcal{G}$ lives over $\mathbb{A}^2$, so any such character of G is geometrically trivial. Hence, in parallel to (31.6.1) now we have $\mathbf{Z}(G) = 1$. Furthermore, G contains $G_{t=0,\mathrm{geom}} = \mathrm{Sp}_6(2)$, so it also satisfies ($\mathbf{S}$+), and, as in (a), it cannot satisfy Lemma 3.1(c) since 5 divides $|H|$. Again applying [HM] and using $\mathrm{Sp}_6(2) \leq G$, we see that $G \rhd S \cong \mathrm{Sp}_6(2)$, and $\mathbf{C}_G(S) = \mathbf{Z}(G) = 1$. It follows that $G = S$.

Now, the arithmetic determinant of $\mathcal{G}$ is either trivial, or $(-1)^{\mathrm{deg}}$ by arithmetic orthogonality. According to (a), $\mathcal{G}|_{t=0}$ already has arithmetic determinant $(-1)^{\mathrm{deg}}$, so the same holds for $\mathcal{G}$. Note that the arithmetic monodromy group $G_{2\text{-param},\mathrm{arith},k}$ of $\mathcal{G}$ has center of order ≤ 2 (again by orthogonality), we have

$$\mathrm{Sp}_6(2) \lhd G_{2\text{-param},\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2).$$

Using the determined arithmetic determinant, we conclude that $G_{2\text{-param},\mathrm{arith},k} = G_{t=0,\mathrm{arith},k}$.

(c) It was shown in [KT1, Theorem 19.1] that the geometric monodromy group, as well as the arithmetic monodromy group of $\mathcal{G}|_{s=0}$ over any finite extension k of $\mathbb{F}_9$, is $\mathrm{SU}_3(3)$. Also, [KT8, Theorem 7.9] shows that the arithmetic monodromy group of $\mathcal{G}|_{s=0}$ over $\mathbb{F}_3$ is $\mathrm{SU}_3(3) \cdot 2$.

(d) Part (c) implies by specializing $s = -1$ that $\mathcal{G}|_{s=-1}$ has finite geometric monodromy group $K := G_{s=-1,\mathrm{geom}}$ which is a subgroup of $G = G_{2\text{-param},\mathrm{geom}} = \mathrm{Sp}_6(2)$. Note that, since the wild part has dimension 6, the image of $P(\infty)$ is non-abelian, and so the Sylow 3-subgroups of K are also non-abelian, hence of order at least 3^3, and certainly $7 = \mathrm{rank}(\mathcal{G}|_{s=-1})$ divides $|K|$. Thus $3^3 \cdot 7$ divides $|K|$, and, furthermore, $K = \mathbf{O}^{3'}(K)$ as $\mathcal{G}|_{s=-1}$ lives on $\mathbb{A}^1$. Checking the subgroups of $\mathrm{Sp}_6(2)$ [Atlas] that satisfy these conditions, we now see that either $K = G$, or $K \leq \mathrm{SU}_3(3)$, or $K \leq {}^2G_2(3) \cong \mathrm{SL}_2(8) \rtimes C_3$. Since $M_{5,0} = 0$ for $\mathrm{Sp}_6(2)$, Theorem 31.5 shows $K \neq G$. Again checking these conditions on the subgroups of $\mathrm{SU}_3(3)$ and ${}^2G_2(3)$, we see that $K = \mathrm{SU}_3(3)$ or $K = {}^2G_2(3)$. Since $M_{3,0} = 1$ for $\mathrm{SU}_3(3)$, Theorem 31.5 implies that $K = {}^2G_2(3)$.

To determine $G_{s=-1,\mathrm{arith},k}$, we note that $K \lhd G_{s=-1,\mathrm{arith},k} \leq G_{2\text{-param},\mathrm{arith},k} \leq 2 \times \mathrm{Sp}_6(2)$, and K is maximal in $\mathrm{Sp}_6(2)$. By [Ka5, Theorem 1.7], $\mathcal{G}|_{s=-1}$ has arithmetic determinant $(-1)^{\mathrm{deg}}$. Hence $G_{s=-1,\mathrm{arith},k}$ has the described structure. $\square$

As a consequence of Theorem 31.6, we now prove Conjectures 7.2 and 7.3 of [Ka9]:

Corollary 31.7. *The local system $\mathcal{G}_3$ on $\mathbb{A}^1/\mathbb{F}_3$ with trace function*

$$t \in k \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi_k\big((x^7 + 2x^5 + 2x^3 + 2x) + tx\big)\xi_2(x)$$

has geometric and arithmetic monodromy groups $G_{\mathrm{geom},\mathcal{G}_3} = G_{\mathrm{arith},\mathcal{G}_3} = {}^2G_2(3)$. *Furthermore, the pullback* $\mathcal{H}_3$ *of* $\mathcal{G}_3$ *by* $t \mapsto t^3 - t$ *has geometric monodromy group* $G_{\mathrm{geom},\mathcal{H}_3} = \mathrm{SL}_2(8)$. *Over any finite extension* k *of* $\mathbb{F}_3$, $\mathcal{H}_3$ *has arithmetic monodromy group* $G_{\mathrm{arith},k,\mathcal{H}_3} = {}^2G_2(3)$ *if* $3 \nmid [k:\mathbb{F}_3]$ *and* $\mathrm{SL}_2(8)$ *if* $3|[k:\mathbb{F}_3]$.

Proof. In characteristic $p = 3$, the above trace function reduces to

$$t \in k \mapsto \frac{1}{\overline{\mathsf{Gauss}_k}} \sum_{x \in k} \psi_k\big(x^7 - x^5 + (t+1)x\big)\xi_2(x),$$

hence $\mathcal{G}_3$ is the pullback by $t \mapsto t+1$ of the system $\mathcal{G}|_{s=-1}$ considered in Theorem 31.6, but with Gauss_k replaced by $\overline{\mathsf{Gauss}_k}$. By this replacement, $\mathcal{G}_3$ has arithmetically trivial determinant, cf. [Ka5, Theorem 1.7]; in particular, $\mathbf{Z}(G_{\mathrm{arith}}) = 1$. Now the proof of Theorem 31.6(d) shows that $G_{\mathrm{geom},\mathcal{G}_3} = G_{\mathrm{arith},\mathcal{G}_3} = {}^2G_2(3)$.

We next show that $G_{\mathrm{geom},\mathcal{H}_3} = \mathrm{SL}_2(8)$. Consider the quotient $G_{\mathrm{geom},\mathcal{G}_3}/\mathrm{SL}_2(8) = G_{\mathrm{arith},\mathcal{G}_3}/\mathrm{SL}_2(8)$. This is a cyclic group of order 3, given by a lisse rank one sheaf $\mathcal{L}$ on $\mathbb{A}^1/\mathbb{F}_3$ which is a quotient of $\mathcal{G}_3$. The ∞-slopes of $\mathcal{G}_3$ are 0 once and $7/6$ with multiplicity 6. Therefore our $\mathcal{L}$, whose integer ∞-slope is $\le 7/6$, is either tame at ∞, in which case it is geometrically trivial, or it has ∞-slope 1. Our $\mathcal{L}$ is not geometrically trivial, as it is a nontrivial quotient of $G_{\mathrm{geom},\mathcal{G}_3}$. Therefore our $\mathcal{L}$ is geometrically of the form $\mathcal{L}_{\psi(at+b)}$ for some $a \in \overline{\mathbb{F}_3}^\times$ and some $b \in \overline{\mathbb{F}_3}$. But this $\mathcal{L}$ lives on $\mathbb{A}^1/\mathbb{F}_3$ (being a quotient of $G_{\mathrm{arith},\mathcal{G}_3}$). So its arithmetic isomorphism class is $\mathrm{Gal}(\overline{\mathbb{F}_3}/\mathbb{F}_3)$-invariant. This forces $a \in \mathbb{F}_3^\times = \pm 1$ and $b \in \mathbb{F}_3$. The $t \mapsto t^3 - t$ pullback trivializes both $\mathcal{L}_{\psi(t)}$ and $\mathcal{L}_{\psi(-t)}$. Thus after this pullback the group $G_{\mathrm{geom},\mathcal{H}_3}$ has indeed shrunk to $\mathrm{SL}_2(8)$. Moreover, the group $G_{\mathrm{arith},\mathcal{G}_3}/G_{\mathrm{geom},\mathcal{H}_3}$ is now the geometrically trivial rank one sheaf $\psi(b)^{\deg}$, of order either 1 (if $b = 0$) or 3 (if $b = \pm 1$).

A calculation using Magma shows that $Frob_{0,\mathbb{F}_3}$ has order 6 and trace -1, and no such element exists in $\mathrm{SL}_2(8)$ [GAP]. As $\mathrm{SL}_2(8) \lhd G_{\mathrm{arith},\mathbb{F}_3,\mathcal{H}_3} \le G_{\mathrm{arith}} = {}^2G_2(3)$, we conclude that $G_{\mathrm{arith},\mathbb{F}_3,\mathcal{H}_3} = {}^2G_2(3)$. $\square$

Remark 31.8. It would be interesting to have a conceptual proof of part (d) of Theorem 31.6. The argument above shows that for any given specializations $s = s_0$, the resulting monodromy group K_{s_0} is one of the three groups $\mathrm{Sp}_6(2)$, $\mathrm{SU}_3(3)$, ${}^2G_2(3)$. So far we have shown that $K_0 = \mathrm{SU}_3(3)$ and $K_{-1} = {}^2G_2(3)$. A Magma calculation over $\mathbb{F}_{3^8}$ for $s = 1$ shows that both 3 and -3 occur as traces; this eliminates both $\mathrm{SU}_3(3)$ and ${}^2G_2(3)$, and hence $K_1 = \mathrm{Sp}_6(2)$. What about other values of $s_0 \in \overline{\mathbb{F}_3}$?

There is one general statement we can make along these lines. By Pink's specialization theorem [Ka4, Theorem 8.18.2], applied to $\mathcal{F}$ on $X := \mathbb{A}^2$ the (s,t)-plane, $S = \mathbb{A}^1$ the s-line, and $X \to S$ the map $(s,t) \mapsto s$, we see that $K_{s_0} = \mathrm{Sp}_6(2)$ for all but finitely many values of of $s_0 \in \overline{\mathbb{F}_3}$.

Theorem 31.9. *The local system* $\mathcal{H}(\mathsf{Char}_5^\times; \xi_2)$ *in characteristic* $p = 7$ *has finite monodromy.*

Proof. We need to show:

$$V(5x) - V(x) + V\left(-x + \frac{1}{2}\right) \ge 0.$$

Using the fact that $V(\frac{i}{10}) = V(\frac{240i}{7^4-1}) = \frac{1}{24}[240i]$ for $1 \le i \le 9$ we check that the inequality holds for $5x \in \mathbb{Z}$. For all other values of x, using that $V(x) + V(-x) = 1$ if $x \ne 0$, we can rewrite the inequality as

$$V(5x) \le V\left(x + \frac{1}{2}\right) + V(x).$$

Following §9, it suffices to prove

$$[5x] \le \left[x + \frac{7^r - 1}{2}\right] + [x] + 3$$

for every $r \ge 1$ and every $0 \le x \le 7^r - 1$. For $r \le 3$ we check it by computer. For $r > 3$ we proceed by induction as described in §9, proving first the following cases by splitting off the last digits of x.

last digits of x	s	z	$\Delta(s,z)$	$\sum_i u_i$	$\sum_j v_j$	$\Delta(s,z) - 6\sum_j v_j + 6\sum_i u_i$
0,1,2,3	1	0,1,2,3	≥ 0	≥ 0	0	≥ 0
04,14,24	2	04,14,24	≥ 0	≥ 0	0	≥ 0
$a44, a64; a \ne 3$	2	44,64	0	≥ 0	0	≥ 0
054,154,254	3	054,154,254	≥ 0	≥ 0	0	≥ 0
$a5, a6; a \ne 3$	1	5,6	≥ 0	≥ 0	0	≥ 0

The remaining cases are proved by substitution of the last digits, as specified in the following table (we do not include the $c_2 = c_2'$ corresponding to $\gamma_2 = 0$, since it is always 0):

$z =$ last digits of x	s	z'	s'	$\Delta(s,z)$	$\Delta(s',z')$	$b_1 = b_1'$	$c_1 = c_1'$
34,35,36	2	4	1	≥ -3	-3	2	1
344	3	35	2	0	0	2	1
354	3	34	2	-3	-3	2	1
454	3	44	2	0	0	3	1
554	3	61	2	3	3	4	1
654	3	64	2	0	0	4	1
364	3	40	2	0	0	2	1

□

Theorem 31.10. (a) *The local system $\mathcal{H} = \mathcal{H}(\mathsf{Char}_5^\times; \xi_2)$ in characteristic $p = 7$ has geometric monodromy group $G_{\mathrm{geom}} = 2\mathsf{A}_7$. Furthermore, $\mathcal{H}$ has a descent $\mathcal{H}_{00}$ to $\mathbb{F}_7$, whose arithmetic monodromy group $G_{\mathrm{arith},k}$ over any finite extension k of $\mathbb{F}_7$ is equal to G_{geom}.*

(b) *The local system $\mathcal{F}$ on $\mathbb{A}^1$ with trace function*

$$t \in k \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi(x^5 + tx^2)$$

in characteristic $p = 7$ has geometric monodromy group $G_{\mathrm{geom}} = 2\mathsf{A}_7$, which is also its arithmetic monodromy group over any finite extension k of $\mathbb{F}_7$.

Proof. By Theorem 31.9, $G = G_{\mathrm{geom}}$ is finite. Furthermore, G satisfies (**S**+) by [KT5, Theorem 1.9]. Let φ denote the character of the representation $G \to \mathrm{GL}(V)$ of G underlying $\mathcal{H}$. By the construction of $\mathcal{H}$ and Proposition 6.1(iii-bis), the field of values $\mathbb{Q}(\varphi) := \mathbb{Q}(\varphi(g) \mid g \in G)$ is $\mathbb{Q}(\sqrt{-7})$. Moreover, a generator g_0 of the image $I(0)$ in G has central order 5, and the image Q of $P(\infty)$ is of order 7 by Proposition 5.8(iv), and $Q \hookrightarrow G/\mathbf{Z}(G)$ by Proposition 5.6(ii). Next, since the cyclic group $\mathbf{Z}(G)$ acts via scalars and $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{-7})$, we have that

$$\mathbf{Z}(G) \le C_2. \tag{31.10.1}$$

Suppose G satisfies conclusion (c) of Lemma 3.1. Then G contains an irreducible normal 2-subgroup R, and

$$G/\mathbf{C}_G(R)R \hookrightarrow \mathrm{Out}(R) \hookrightarrow \mathrm{Sp}_4(2) \cong \mathsf{S}_6.$$

But this is a contradiction, since $\mathbf{C}_G(R) = \mathbf{Z}(G) \le C_2$ by (31.10.1), and 7 divides $|G|$ but not $|\mathsf{S}_6|$.

Thus G is almost quasisimple. Let S denote the unique non-abelian composition factor of G, so that $S = L/\mathbf{Z}(L)$ for $L := E(G) = G^{(\infty)}$. Then $V|_L$ is irreducible by Lemma 3.1, and so $\mathbf{C}_G(L) = \mathbf{Z}(G)$ by Schur's lemma. Furthermore, as $\bar{\mathsf{o}}(g_0) = 5$ and $|Q| = 7$ we have that $5 \cdot 7$ divides the order of $G/\mathbf{Z}(G) \leq \mathrm{Aut}(S)$. Now we can apply the main result of [HM] to see that $S = \mathsf{A}_7$ and $L = 2\mathsf{A}_7$. In this case we also have that $\mathbf{Z}(G) = \mathbf{Z}(L) = C_2$ by (31.10.1). Since $7 \nmid |\mathrm{Out}(S)|$, g_0 must lie in the inverse image L of S in G, whence $G_{\mathrm{geom}} = L$ by Theorem 5.1.

By Theorem 7.5, $\mathcal{H}$ has a descent $\mathcal{H}_{00}$ to $\mathbb{F}_7$ for which any element in $G_{\mathrm{arith},k}$ still has trace in $\mathbb{Q}(\sqrt{-7})$ whenever $k \supseteq \mathbb{F}_7$, with $\mathcal{H}_0$ given on line 44 of Table 4. Since any element in $\mathbf{C}_{G_{\mathrm{arith},k}}(L) = \mathbf{Z}(G_{\mathrm{arith}})$ acts via scalars, which are then roots of unity in $\mathbb{Q}(\sqrt{-7})$, we see that

$$\mathbf{C}_{G_{\mathrm{arith},k}}(L) = C_2 = \mathbf{Z}(L).$$

Since no outer automorphism of L can fix the character $\varphi|_L$, we conclude that $G_{\mathrm{arith},k} = L = G_{\mathrm{geom}}$.

The statements in (b) now follow, since $\mathcal{F}$ is the $[5]^\star$ Kummer pullback of $\mathcal{H}$ by [KT6, Corollary 3.10]. ☐

32. Further multi-parameter local systems

Theorem 32.1. *The local system on $\mathbb{A}^3$ with trace function $(s,t,u) \mapsto -\sum_x \psi(x^7 + sx^4 + tx^2 + ux)$ in characteristic $p = 3$ has finite monodromy.*

Proof. By [KRLT1, Theorem 2.12], it suffices to prove

$$[7a + 4b + 2c] \leq [a] + [b] + [c] + r + 1$$

for every $r \geq 1$ and every $a, b \in \{0, 1, \dots, 3^r - 1\}$, where $[x] := [x]_3$ denotes the sum of the 3-adic digits of x. We proceed by induction on r. For $r \leq 3$, we check it by computer. For $r > 3$ we distinguish the following cases.

Case 1: The last (3-adic) digits of a, b and c are not $(0,2,0)$, $(1,0,0)$ or $(2,0,0)$. Write $a = 3 \cdot a_1 + a_0$, $b = 3 \cdot b_1 + b_0$ and $c = 3 \cdot c_1 + c_0$ with $(a_0, b_0, c_0) \in \{0,1,2\}^3 \smallsetminus \{(0,2,0),(1,0,0),(2,0,0)\}$. Then it is easily checked by computer that $[7a_0 + 4b_0 + 2c_0] \leq [a_0] + [b_0] + [c_0] + 1$, so

$$\begin{aligned}
[7a + 4b + 2c] &= [3 \cdot (7a_1 + 4b_1 + 2c_1) + (7a_0 + 4b_0 + 2c_0)] \\
&\leq [7a_1 + 4b_1 + 2c_1] + [7a_0 + 4b_0 + 2c_0] \\
&\leq [a_1] + [b_1] + [c_1] + (r-1) + 1 + [a_0] + [b_0] + [c_0] + 1 \\
&= [a] + [b] + [c] + r + 1
\end{aligned}$$

by induction hypothesis.

Case 2: The last digits of a, b and c are $(0,2,0)$, $(1,0,0)$ or $(2,0,0)$, except if the last two digits are $(02, 10, 00)$. Write $a = 3^2 \cdot a_1 + a_0$, $b = 3^2 \cdot b_1 + b_0$ and $c = 3^2 \cdot c_1 + c_0$ with $a_0, b_0, c_0 < 3^2$ and $(a_0, b_0, c_0) \neq (02_3, 10_3, 00_3)$. Then it is easily checked by computer that $[7a_0 + 4b_0 + 2c_0] \leq [a_0] + [b_0] + [c_0] + 2$, so

$$\begin{aligned}
[7a + 4b + 2c] &= [3^2 \cdot (7a_1 + 4b_1 + 2c_1) + (7a_0 + 4b_0 + 2c_0)] \\
&\leq [7a_1 + 4b_1 + 2c_1] + [7a_0 + 4b_0 + 2c_0] \\
&\leq [a_1] + [b_1] + [c_1] + (r-2) + 1 + [a_0] + [b_0] + [c_0] + 2 \\
&= [a] + [b] + [c] + r + 1
\end{aligned}$$

by induction hypothesis.

Case 3: The last two digits of a, b and c are $(02_3, 10_3, 00_3)$. Write $a = 3^3 \cdot a_1 + a_0$, $b = 3^3 \cdot b_1 + b_0$ and $c = 3^3 \cdot c_1 + c_0$ with $a_0, b_0, c_0 < 3^3$ and $(a_0, b_0, c_0) \equiv (02_3, 10_3, 00_3) \bmod 9$. Then it is easily checked by computer that $[7a_0 + 4b_0 + 2c_0] \leq [a_0] + [b_0] + [c_0] + 3$, so

$$\begin{aligned}[7a + 4b + 2c] &= [3^3 \cdot (7a_1 + 4b_1 + 2c_1) + (7a_0 + 4b_0 + 2c_0)] \\ &\leq [7a_1 + 4b_1 + 2c_1] + [7a_0 + 4b_0 + 2c_0] \\ &\leq [a_1] + [b_1] + [c_1] + (r - 3) + 1 + [a_0] + [b_0] + [c_0] + 3 \\ &= [a] + [b] + [c] + r + 1\end{aligned}$$

by induction hypothesis. □

Theorem 32.2. *The local system $\mathcal{G}$ on $\mathbb{A}^3$ with trace function*

$$(s, t, u) \in k^3 \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi(x^7 + sx^4 + tx^2 + ux)$$

in characteristic $p = 3$ has geometric monodromy group $G = G_{\mathrm{geom}} = 6_1 \cdot \mathrm{PSU}_4(3)$. Over any finite extension k of $\mathbb{F}_3$, the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{G}$ is $\big(6_1 \cdot \mathrm{PSU}_4(3)\big) \cdot 2_2 = G \cdot 2$ if $2 \nmid [k : \mathbb{F}_3]$ and G if $2 | [k : \mathbb{F}_3]$.

Proof. By Theorem 32.1, G is finite. Next, the sheaf $\mathcal{G}|_{t=u=0}$ is the $[7]^\star$ Kummer pullback of the sheaf $\mathcal{H}yp(\mathsf{Char}_{\mathrm{ntriv}}(7), \mathsf{Char}_{\mathrm{ntriv}}(4))$, and so it has geometric monodromy group $H = 6_1 \cdot \mathrm{PSU}_4(3)$ by Theorem 21.4. Since $H \leq G$ and H is $(\mathbf{S}+)$, G is also $(\mathbf{S}+)$, and therefore it is almost quasisimple by Lemma 3.1; also, $|G/\mathbf{Z}(G)|$ is divisible by $|H/\mathbf{Z}(H)| = |\mathrm{PSU}_4(3)|$. Using this information and [HM], we see that the only non-abelian composition factor S of G is $S \cong \mathrm{PSU}_4(3)$ and $G^{(\infty)} = 6_1 \cdot \mathrm{PSU}_4(3) = H$. Since the field of traces is $\mathbb{Q}(\zeta_3)$, $|\mathbf{Z}(G)| \leq 6$, and so $\mathbf{Z}(G) = \mathbf{Z}(H)$. Finally, $G = \mathbf{O}^{3'}(G)$ and $\mathrm{Out}(S)$ is a $3'$-group, implying $G/\mathbf{C}_G(H) = G/\mathbf{Z}(G) = S$, and hence $G = H$.

To determine the arithmetic monodromy group over any finite extension k of $\mathbb{F}_3$, it suffices by Lemma 4.2 to show that $\tilde{G} := G_{\mathrm{arith},\mathbb{F}_3} = \big(6_1 \cdot \mathrm{PSU}_4(3)\big) \cdot 2_2$. Note that the field of traces is still $\mathbb{Q}(\zeta_3)$, so $\mathbf{C}_{\tilde{G}}(G) = \mathbf{Z}(\tilde{G})$ has order at most 6, and so $\mathbf{C}_{\tilde{G}}(G) = \mathbf{Z}(G)$. Next, the only nontrivial element of $\mathrm{Out}(G) = D_8$ that preserves the character of G on $\mathcal{G}$ is 2_2, see [Atlas]; hence either $\tilde{G} = G$ or $\tilde{G} = G \cdot 2_2$. Suppose we are in the former case. Then the arithmetic monodromy group of $\mathcal{G}|_{s=t=0}$ over k is contained in G. This specialization is just the local system $\mathcal{W}^{3,1,0}$ in [KT8, Corollary 7.10], according to which it has arithmetic monodromy group $\mathrm{SU}_3(3) \cdot 2 \cong G_2(2)$. The latter group is *not* a subgroup of $G = 6_1 \cdot \mathrm{PSU}_4(3)$, see [Atlas], a contradiction. Hence $\tilde{G} = G \cdot 2_2$ as stated. □

Theorem 32.3. *The local system on $\mathbb{A}^2$ with trace function $(s, t) \mapsto -\sum_x \psi(x^{13} + sx^3 + tx)$ in characteristic $p = 2$ has finite monodromy.*

Proof. By [KRLT1, Theorem 2.12], it suffices to prove

$$[13a + 3b] \leq [a] + [b] + \frac{r}{2} + \frac{3}{2}$$

for every $r \geq 1$ and every $a, b \in \{0, 1, \ldots, 2^r - 1\}$, where $[x] := [x]_2$ denotes the sum of the 2-adic digits of x. We proceed by induction on r. For $r \leq 4$, we check it by computer. For $r > 4$ we distinguish the following cases (where, for each case, it is implicitly assumed that the previous cases do not apply).

Case 1: The last (2-adic) digits of a and b are not $(1, 0)$ or $(0, 1)$. Write $a = 2 \cdot a_1 + a_0$ and $b = 2 \cdot b_1 + b_0$ with $(a_0, b_0) \in \{(0, 0), (1, 1)\}$. Then it is easily checked by computer that

$[13a_0 + 3b_0] \le [a_0] + [b_0] + \frac{1}{2}$, so

$$\begin{aligned}[13a + 3b] &= [2 \cdot (13a_1 + 3b_1) + (13a_0 + 3b_0)] \\ &\le [13a_1 + 3b_1] + [13a_0 + 3b_0] \\ &\le [a_1] + [b_1] + \frac{r-1}{2} + \frac{3}{2} + [a_0] + [b_0] + \frac{1}{2} \\ &= [a] + [b] + \frac{r}{2} + \frac{3}{2}\end{aligned}$$

by induction hypothesis.

Case 2: The last two digits of a and b are not $(01_2, 00_2)$, $(10_2, 01_2)$ or $(11_2, 00_2)$. Write $a = 2^2 \cdot a_1 + a_0$ and $b = 2^2 \cdot b_1 + b_0$ with

$$a_0, b_0 < 2^2,\ (a_0, b_0) \notin \{(01_2, 00_2), (10_2, 01_2), (11_2, 00_2)\}.$$

Then it is easily checked by computer that $[13a_0 + 3b_0] \le [a_0] + [b_0] + 1$, so

$$\begin{aligned}[13a + 3b] &= [2^2 \cdot (13a_1 + 3b_1) + (13a_0 + 3b_0)] \\ &\le [13a_1 + 3b_1] + [13a_0 + 3b_0] \\ &\le [a_1] + [b_1] + \frac{r-2}{2} + \frac{3}{2} + [a_0] + [b_0] + 1 \\ &= [a] + [b] + \frac{r}{2} + \frac{3}{2}\end{aligned}$$

by induction hypothesis.

Case 3: The last three digits of a and b are not $(001_2, 000_2)$, $(010_2, 001_2)$, $(011_2, 000_2)$ or $(111_2, 000_2)$. Write $a = 2^3 \cdot a_1 + a_0$ and $b = 2^3 \cdot b_1 + b_0$ with

$$a_0, b_0 < 2^3,\ (a_0, b_0) \notin \{(001_2, 000_2), (010_2, 001_2), (011_2, 000_2), (111_2, 000_2)\}.$$

Then it is easily checked by computer that $[13a_0 + 3b_0] \le [a_0] + [b_0] + \frac{3}{2}$, so

$$\begin{aligned}[13a + 3b] &= [2^3 \cdot (13a_1 + 3b_1) + (13a_0 + 3b_0)] \\ &\le [13a_1 + 3b_1] + [13a_0 + 3b_0] \\ &\le [a_1] + [b_1] + \frac{r-3}{2} + \frac{3}{2} + [a_0] + [b_0] + \frac{3}{2} \\ &= [a] + [b] + \frac{r}{2} + \frac{3}{2}\end{aligned}$$

by induction hypothesis.

Case 4: The last four digits of a and b are not $(0011_2, 1000_2)$ or $(1001_2, 0000_2)$. Write $a = 2^4 \cdot a_1 + a_0$ and $b = 2^4 \cdot b_1 + b_0$ with $a_0, b_0 < 2^4$ and $(a_0, b_0) \notin \{(0011_2, 1000_2), (1001_2, 0000_2)\}$. Then it is easily checked by computer that $[13a_0 + 3b_0] \le [a_0] + [b_0] + 2$, so

$$\begin{aligned}[13a + 3b] &= [2^4 \cdot (13a_1 + 3b_1) + (13a_0 + 3b_0)] \\ &\le [13a_1 + 3b_1] + [13a_0 + 3b_0] \\ &\le [a_1] + [b_1] + \frac{r-4}{2} + \frac{3}{2} + [a_0] + [b_0] + 2 \\ &= [a] + [b] + \frac{r}{2} + \frac{3}{2}\end{aligned}$$

by induction hypothesis.

Case 5: The last four digits of a and b are $(0011_2, 1000_2)$. Write $a = 2^4 \cdot a_1 + 3$ and $b = 2^4 \cdot b_1 + 8$, and let $a' = 2^2 \cdot a_1 + 1$ and $b' = 2^2 \cdot b_1$. Since $13 \cdot 3 + 3 \cdot 8 = 111111_2$ and $13 \cdot 1 + 3 \cdot 0 = 1101_2$ have the same first two digits, the number of digit carries in the sums $13a + 3b = 2^4 \cdot (13a_1 + 3b_1) + (13 \cdot 3 + 3 \cdot 8)$ and $13a' + 3b' = 2^2 \cdot (13a_1 + 3b_1) + (13 \cdot 1 + 3 \cdot 0)$ is the same. In particular,

$$[13a + 3b] - [13a_1 + 3b_1] - [13 \cdot 3 + 3 \cdot 8] = [13a' + 3b'] - [13a_1 + 3b_1] - [13 \cdot 1 + 3 \cdot 0].$$

Therefore,

$$\begin{aligned}
[13a + 3b] &= [13a_1 + 3b_1] + [13 \cdot 3 + 3 \cdot 8] + ([13a + 3b] - [13a_1 + 3b_1] - [13 \cdot 3 + 3 \cdot 8]) \\
&= [13a_1 + 3b_1] + [13 \cdot 3 + 3 \cdot 8] + ([13a' + 3b'] - [13a_1 + 3b_1] - [13 \cdot 1 + 3 \cdot 0]) \\
&= [13a' + 3b'] + 3 \le [a'] + [b'] + \frac{r-2}{2} + \frac{3}{2} + 3 \\
&= [a] + [b] - 2 + \frac{r-2}{2} + \frac{3}{2} + 3 \\
&= [a] + [b] + \frac{r}{2} + \frac{3}{2}
\end{aligned}$$

by induction hypothesis.

Case 6: The last four digits of a and b are $(1001_2, 0000_2)$. Write $a = 2^4 \cdot a_1 + 9$ and $b = 2^4 \cdot b_1$, and let $a' = 2^2 \cdot a_1 + 2$ and $b' = 2^2 \cdot b_1 + 1$. Since $13 \cdot 9 + 3 \cdot 0 = 1110101_2$ and $13 \cdot 2 + 3 \cdot 1 = 11101_2$ have the same first three digits, the number of digit carries in the sums $13a + 3b = 2^4 \cdot (13a_1 + 3b_1) + (13 \cdot 9 + 3 \cdot 0)$ and $13a' + 3b' = 2^2 \cdot (13a_1 + 3b_1) + (13 \cdot 2 + 3 \cdot 1)$ is the same. In particular,

$$[13a + 3b] - [13a_1 + 3b_1] - [13 \cdot 9 + 3 \cdot 0] = [13a' + 3b'] - [13a_1 + 3b_1] - [13 \cdot 2 + 3 \cdot 1].$$

Therefore,

$$\begin{aligned}
[13a + 3b] &= [13a_1 + 3b_1] + [13 \cdot 9 + 3 \cdot 0] + ([13a + 3b] - [13a_1 + 3b_1] - [13 \cdot 9 + 3 \cdot 0]) \\
&= [13a_1 + 3b_1] + [13 \cdot 9 + 3 \cdot 0] + ([13a' + 3b'] - [13a_1 + 3b_1] - [13 \cdot 2 + 3 \cdot 1]) \\
&= [13a' + 3b'] + 1 \le [a'] + [b'] + \frac{r-2}{2} + \frac{3}{2} + 1 \\
&= [a] + [b] + \frac{r-2}{2} + \frac{3}{2} + 1 \\
&= [a] + [b] + \frac{r}{2} + \frac{3}{2}
\end{aligned}$$

by induction hypothesis. $\square$

Theorem 32.4. *The local system $\mathcal{F}$ on $\mathbb{A}^2$ with trace function*

$$(s,t) \in k \mapsto \frac{-1}{\sqrt{2}^{\deg(k/\mathbb{F}_2)}} \sum_{x \in k} \psi(x^{13} + sx^3 + tx)$$

in characteristic $p = 2$ has geometric monodromy group $G = G_{\mathrm{geom}} = 2 \cdot G_2(4)$. Over any finite extension k of $\mathbb{F}_2$, the arithmetic monodromy group $G_{\mathrm{arith},k}$ of $\mathcal{F}$ is $\big(2 \cdot G_2(4)\big) \cdot 2 = G \cdot 2$ if $2 \nmid [k : \mathbb{F}_2]$ and G if $2 | [k : \mathbb{F}_2]$.

Proof. By Theorem 32.3, G is finite. Next, the sheaf $\mathcal{G}|_{t=0}$ is the $[13]^\star$ Kummer pullback of the sheaf $\mathcal{H}yp(\mathsf{Char}_{\mathrm{ntriv}}(13), \mathsf{Char}_{\mathrm{ntriv}}(3))$, and so it has geometric monodromy group $H = 2 \cdot G_2(4)$ by Theorem 25.2. Since $H \le G$ and H is $(\mathbf{S}+)$, G is also $(\mathbf{S}+)$, and therefore it is almost quasisimple by Lemma 3.1; also, $|G/\mathbf{Z}(G)|$ is divisible by $|H/\mathbf{Z}(H)| = |G_2(4)|$, and the field of traces is $\mathbb{Q}$. Using this information and [HM], we see that the only non-abelian composition factor S of G is $S \cong G_2(4)$ and $G^{(\infty)} = 2 \cdot G_2(4) = H$. Since the field of traces over any finite extension of $\mathbb{F}_4$ is $\mathbb{Q}$, $|\mathbf{Z}(G)| \le 2$, and so $\mathbf{Z}(G) = \mathbf{Z}(H)$. Next, $G/\mathbf{C}_G(H) = G/\mathbf{Z}(G) \le \mathrm{Aut}(S) = S \cdot 2$, but $2 \cdot S \cdot 2$ does not rational characters of degree 12 [Atlas], so $G = H$.

To determine the arithmetic monodromy group over any finite extension k of $\mathbb{F}_2$, it suffices to show that $\tilde{G} := G_{\mathrm{arith},\mathbb{F}_2} = (2 \cdot G_2(4)) \cdot 2$. Note that the field of traces over $\mathbb{F}_2$ is contained in $\mathbb{Q}(\sqrt{2})$, so $\mathbf{C}_{\tilde{G}}(G) = \mathbf{Z}(\tilde{G})$ has order at most 2, and so $\mathbf{C}_{\tilde{G}}(G) = \mathbf{Z}(G)$. Since $\mathrm{Out}(G) = C_2$ [Atlas], either $\tilde{G} = G$ or $\tilde{G} = G \cdot 2$. Suppose we are in the former case. Then the trace of any $Frob_{(s,t),\mathbb{F}_2}$ with $s, t \in \mathbb{F}_2$ is rational. On the other hand, $Frob_{(1,0),\mathbb{F}_2}$ has trace $-\sqrt{2}$, a contradiction. Hence $\tilde{G} = G \cdot 2$ as stated. $\square$

Theorem 32.5. *The local system on $\mathbb{A}^3$ with trace function $(s,t,u) \mapsto -\sum_x \psi(x^5 + sx^4 + tx^2 + ux)$ in characteristic $p = 3$ has finite monodromy.*

Proof. By [KRLT1, Theorem 2.12], it suffices to prove

$$[5a + 4b + 2c] \le [a] + [b] + [c] + r + 1$$

for every $r \ge 1$ and every $a, b, c \in \{0, 1, \ldots, 3^r - 1\}$, where $[x] := [x]_3$ denotes the sum of the 3-adic digits of x. We proceed by induction on r. For $r \le 2$, we check it by computer. For $r > 3$ we distinguish the following cases.

Case 1: The last (3-adic) digits of a, b and c are not $(0, 2, 0)$ or $(1, 0, 0)$. Write $a = 3 \cdot a_1 + a_0$, $b = 3 \cdot b_1 + b_0$ and $c = 3 \cdot c_1 + c_0$ with $(a_0, b_0, c_0) \notin \{(0, 2, 0), (1, 0, 0)\}$. Then it is easily checked by computer that $[5a_0 + 4b_0 + 2c_0] \le [a_0] + [b_0] + [c_0] + 1$, so

$$\begin{aligned}
[5a + 4b + 2c] &= [3 \cdot (5a_1 + 4b_1 + 2c_1) + (5a_0 + 4b_0 + 2c_0)] \\
&\le [5a_1 + 4b_1 + 2c_1] + [5a_0 + 4b_0 + 2c_0] \\
&\le [a_1] + [b_1] + [c_1] + (r - 1) + 1 + [a_0] + [b_0] + [c_0] + 1 \\
&= [a] + [b] + [c] + r + 1
\end{aligned}$$

by induction hypothesis.

Case 2: The last digits of a, b and c are $(0, 2, 0)$ or $(1, 0, 0)$, except when their last two digits are $(01_3, 10_3, 00_3)$ or $(11_3, 00_3, 10_3)$. Write $a = 3^2 \cdot a_1 + a_0$, $b = 3^2 \cdot b_1 + b_0$ and $c = 3^2 \cdot c_1 + c_0$ with $(a_0, b_0, c_0) \equiv (0, 2, 0)$ or $(1, 0, 0) \bmod 3$ but $(a_0, b_0, c_0) \notin \{(01_3, 10_3, 00_3), (11_3, 00_3, 10_3)\}$. Then it is easily checked by computer that $[5a_0 + 4b_0 + 2c_0] \le [a_0] + [b_0] + [c_0] + 2$, so

$$\begin{aligned}
[5a + 4b + 2c] &= [3^2 \cdot (5a_1 + 4b_1 + 2c_1) + (5a_0 + 4b_0 + 2c_0)] \\
&\le [5a_1 + 4b_1 + 2c_1] + [5a_0 + 4b_0 + 2c_0] \\
&\le [a_1] + [b_1] + [c_1] + (r - 2) + 1 + [a_0] + [b_0] + [c_0] + 2 \\
&= [a] + [b] + [c] + r + 1
\end{aligned}$$

by induction hypothesis.

Case 3: The last two digits of a, b and c are $(01_3, 10_3, 00_3)$. Write $a = 3^2 \cdot a_1 + 1$, $b = 3^2 \cdot b_1 + 3$ and $c = 3^2 \cdot c_1$, and let $a' = 3 \cdot a_1 + 1$, $b' = 3 \cdot b_1$ and $c' = 3 \cdot c_1$. Since $5 \cdot 1 + 4 \cdot 3 + 2 \cdot 0 = 122_3$ and $5 \cdot 1 + 4 \cdot 0 + 2 \cdot 0 = 12_2$ have the same first digit, the number of digit carries in the sums $5a + 4b + 2c = 3^2 \cdot (5a_1 + 4b_1 + 2c_1) + (5 \cdot 1 + 4 \cdot 3 + 2 \cdot 0)$ and $5a' + 4b' + 2c' = 3 \cdot (5a_1 + 4b_1 + 2c_1) + (5 \cdot 1 + 4 \cdot 0 + 2 \cdot 0)$ is the same. In particular,

$$[5a + 4b + 2c] - [5a_1 + 4b_1 + 2c_1] - [5 \cdot 1 + 4 \cdot 3 + 2 \cdot 0] = [5a' + 4b' + 2c'] - [5a_1 + 4b_1 + 2c_1] - [5 \cdot 1 + 4 \cdot 0 + 2 \cdot 0].$$

Therefore,

$$\begin{aligned}
&[5a+4b+2c]\\
&=[5a_1+4b_1+2c_1]+[5\cdot 1+4\cdot 3+2\cdot 0]+([5a+4b+2c]-[5a_1+4b_1+2c_1]-[5\cdot 1+4\cdot 3+2\cdot 0])\\
&=[5a_1+4b_1+2c_1]+[5\cdot 1+4\cdot 3+2\cdot 0]+([5a'+4b'+2c']-[5a_1+4b_1+2c_1]-[5\cdot 1+4\cdot 0+2\cdot 0])\\
&=[5a'+4b'+2c']+2\\
&\le [a']+[b']+[c']+(r-1)+1+2\\
&=[a]+[b]+[c]+r+1
\end{aligned}$$

by induction hypothesis.

Case 4: The last two digits of a, b and c are $(11_3, 00_3, 10_3)$. Write $a = 3^2\cdot a_1 + 4$, $b = 3^2 \cdot b_1$ and $c = 3^2 \cdot c_1 + 3$, and let $a' = 3\cdot a_1$, $b' = 3\cdot b_1 + 2$ and $c' = 3\cdot c_1$. Since $5\cdot 4+4\cdot 0+2\cdot 3 = 222_3$ and $5\cdot 0+4\cdot 2+2\cdot 0 = 22_2$ have the same first digit, the number of digit carries in the sums $5a+4b+2c = 3^2\cdot(5a_1+4b_1+2c_1)+(5\cdot 4+4\cdot 0+2\cdot 3)$ and $5a'+4b'+2c' = 3\cdot(5a_1+4b_1+2c_1)+(5\cdot 0+4\cdot 2+2\cdot 0)$ is the same. In particular, $[5a+4b+2c]-[5a_1+4b_1+2c_1]-[5\cdot 4+4\cdot 0+2\cdot 3] = [5a'+4b'+2c']-[5a_1+4b_1+2c_1]-[5\cdot 0+4\cdot 2+2\cdot 0]$. Therefore,

$$\begin{aligned}
&[5a+4b+2c]\\
&=[5a_1+4b_1+2c_1]+[5\cdot 4+4\cdot 0+2\cdot 3]+([5a+4b+2c]-[5a_1+4b_1+2c_1]-[5\cdot 4+4\cdot 0+2\cdot 3])\\
&=[5a_1+4b_1+2c_1]+[5\cdot 4+4\cdot 0+2\cdot 3]+([5a'+4b'+2c']-[5a_1+4b_1+2c_1]-[5\cdot 0+4\cdot 2+2\cdot 0])\\
&=[5a'+4b'+2c']+2\\
&\le [a']+[b']+[c']+(r-1)+1+2\\
&=[a]+[b]+[c]+r+1
\end{aligned}$$

by induction hypothesis. □

Theorem 32.6. *The local system $\mathcal{F}$ on $\mathbb{A}^3$ with trace function*

$$(s,t,u)\mapsto \frac{1}{\mathsf{Gauss}_k}\sum_{x\in k}\psi(x^5+sx^4+tx^2+ux)$$

in characteristic $p=3$ has geometric monodromy group $G = G_{\mathrm{geom}} = 3\times \mathrm{Sp}_4(3)$. Over any finite extension k of $\mathbb{F}_3$, $\mathcal{F}$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.

Proof. By Theorem 32.5, G is finite. Next, the sheaf $\mathcal{F}|_{t=u=0}$ is the $[5]^\star$ Kummer pullback of $\mathcal{H}yp(\mathsf{Char}_{\mathrm{ntriv}}(5), \mathsf{Char}_{\mathrm{ntriv}}(4))$, and so it has geometric monodromy group $H = 3\times \mathrm{Sp}_4(3)$ by Theorem 30.7(iv). Since $H \le G$ and H is $(\mathbf{S}+)$, G is also $(\mathbf{S}+)$, and in fact it is almost quasisimple; also, $|G/\mathbf{Z}(G)|$ is divisible by $|H/\mathbf{Z}(H)| = |\mathrm{PSp}_4(3)|$, and the field of traces is $\mathbb{Q}(\zeta_3)$. Using this information and [HM], we see that the only non-abelian composition factor S of G is $S\cong \mathrm{PSp}_4(3)$ and $G^{(\infty)} = \mathrm{Sp}_4(3)$. Since the field of traces is $\mathbb{Q}(\zeta_3)$, $|\mathbf{Z}(G)|\le 6$, and so $\mathbf{Z}(G) = \mathbf{Z}(H)$. Next, $G/\mathbf{C}_G(H) = G/\mathbf{Z}(G) \le \mathrm{Aut}(S) = S\cdot 2$, but $2\cdot S\cdot 2$ does not irreducible characters of degree 4 [Atlas], so $G = H$.

To determine $G_{\mathrm{arith},k}$, we note that the field of traces is still $\mathbb{Q}(\zeta_3)$, and repeat the above arguments verbatim. □

Theorem 32.7. *The local system $\mathcal{F}$ on $\mathbb{A}^2$ with trace function $(s,t)\mapsto -\sum_x \psi(x^3+sx^2+tx)$ in characteristic $p=5$ has finite monodromy.*

Proof. By [KRLT1, Theorem 2.12], it suffices to prove

$$[3a+2b]\le [a]+[b]+2r$$

for every $r \geq 1$ and every $a, b \in \{0, 1, \ldots, 5^r - 1\}$, where $[x] := [x]_5$ denotes the sum of the 5-adic digits of x. We proceed by induction on r. For $r = 1$ we check it by computer.

For $r > 1$, write $a = 5 \cdot a_1 + a_0$ and $b = 5 \cdot b_1 + b_0$ with $(a_0, b_0) \in \{0, 1, 2, 3, 4\}$. Then

$$\begin{aligned}[3a + 2b] &= [5 \cdot (3a_1 + 2b_1) + (3a_0 + 2b_0)] \\ &\leq [3a_1 + 2b_1] + [3a_0 + 2b_0] \\ &\leq [a_1] + [b_1] + 2(r - 1) + [a_0] + [b_0] + 2 \\ &= [a] + [b] + 2r\end{aligned}$$

by induction hypothesis. □

Theorem 32.8. *The local system $\mathcal{F}$ on $\mathbb{A}^2$ with trace function*

$$(s, t) \mapsto \frac{1}{\mathsf{Gauss}_k} \sum_{x \in k} \psi(x^3 + sx^2 + tx)$$

in characteristic $p = 5$ has finite geometric monodromy group $G = G_{\mathrm{geom}} = 5 \times \mathrm{SL}_2(5)$. Over any finite extension k of $\mathbb{F}_5$, $\mathcal{F}$ has arithmetic monodromy group $G_{\mathrm{arith},k} = G_{\mathrm{geom}}$.

Proof. By Theorem 32.7, G is finite. Next, the sheaf $\mathcal{F}|_{t=0}$ is the $[3]^\star$ Kummer pullback of $\mathcal{H}yp(\mathsf{Char}_3^\times, \xi_2)$, and so it has geometric monodromy group $H = 5 \times \mathrm{SL}_2(5)$ by Theorem 30.7(v). Since $H \leq G$ and H is $(\mathbf{S}+)$, G is also $(\mathbf{S}+)$ and in fact it is almost quasisimple; also, the field of traces is $\mathbb{Q}(\zeta_5)$. Using this information and [HM], we see that the only non-abelian composition factor S of G is $S \cong \mathsf{A}_5$ and $G^{(\infty)} = \mathrm{SL}_2(5)$. Since the field of traces is $\mathbb{Q}(\zeta_5)$, $|\mathbf{Z}(G)| \leq 10$, and so $\mathbf{Z}(G) = \mathbf{Z}(H)$. Next, $G/\mathbf{C}_G(H) = G/\mathbf{Z}(G) \leq \mathrm{Aut}(S) = S \cdot 2$, but $2 \cdot S \cdot 2$ does not irreducible characters of degree 2 [Atlas], so $G = H$.

To determine $G_{\mathrm{arith},k}$, we note that the field of traces is still $\mathbb{Q}(\zeta_5)$, and repeat the above arguments verbatim. □

References

[Abh1] Abhyankar, S., Coverings of algebraic curves, *Amer. J. Math.* **79** (1957), 825–856.

[Abh2] Abhyankar, S., Mathieu group coverings in characteristic two, *C. R. Acad. Sci. Paris* Sér. I Math. **316** (1993), 267–271.

[AY] Abhyankar, S., and Yie, I., Some more Mathieu group coverings in characteristic two, *Proc. Amer. Math. Soc.* **122** (1994), 1007–1014.

[Asch] Aschbacher, M., Maximal subgroups of classical groups, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[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.

[Bor] Borel, A., Linear Algebraic Groups, Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991. xii+288 pp.

[BH] Beukers, F., Heckman, G., Monodromy for the hypergeometric function ${}_nF_{n-1}$, *Invent. Math.* **95** (1989), 325–354.

[De] Deligne, P., La conjecture de Weil II, *Publ. Math. IHES* **52** (1981), 313–428.

[GAP] The GAP group, GAP - groups, algorithms, and programming, Version 4.4, 2004, `http://www.gap-system.org`.

[GLS] Gorenstein, D., Lyons, R., and Solomon, R.M., The Classification of the finite simple groups, Number 3. Part I. Chapter A, volume **40** of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 1998.

[Gri] Griess, R.L., Automorphisms of extra special groups and nonvanishing degree 2 cohomology, *Pacif. J. Math.* **48** (1973), 403–422.

[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.

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

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

[Har] Harbater, D., Abhyankar's conjecture on Galois groups over curves, *Invent. Math.* **117** (1994), 1–25.

[HM] Hiss, G. and Malle, G., Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4** (2001), 22–63; Corrigenda: Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **5** (2002), 95–126.

[Is] Isaacs, I. M., Character theory of finite groups, AMS-Chelsea, Providence, 2006.

[Is-FGT] Isaacs, I. M., Finite group theory, Graduate Studies in Mathematics Volume 92, AMS, Providence, 2008.

[Ka1] Katz, N., Local-to-global extensions of representations of fundamental groups, *Annales de L'Institut Fourier* **36** (1986), 59–106.

[Ka2] Katz, N., On the monodromy groups attached to certain families of exponential sums, *Duke Math. J.* **54** (1987), 41–56.

[Ka3] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies, **116**. Princeton Univ. Press, Princeton, NJ, 1988. ix+246 pp.

[Ka4] Katz, N., Exponential sums and differential equations. Annals of Mathematics Studies, **124**. Princeton Univ. Press, Princeton, NJ, 1990. xii+430 pp.

[Ka5] Katz, N., Notes on G_2, determinants, and equidistribution, *Finite Fields Appl.* **10** (2004), 221–269.

[Ka6] Katz, N., Moments, monodromy, and perversity. Annals of Mathematics Studies, **159**. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[Ka7] Katz, N., G_2 and hypergeometric sheaves, *Finite Fields Appl.* **13** (2007), 175–223; Corrigendum to: "G_2 and hypergeometric sheaves", *Finite Fields Appl.* **14** (2008), 847.

[Ka8] Katz, N., From Clausen to Carlitz: low-dimensional spin groups and identities among character sums, *Mosc. Math. J.* **9** (2009), 57–89.

[Ka9] Katz, N., Exponential sums, Ree groups and Suzuki groups: conjectures, *Exp. Math.* **28** (2019), 49–56.

[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 $2.\mathsf{Co}_1$ and two others with monodromy group the Suzuki group $6.\mathsf{Suz}$, *Trans. Amer. Math. Soc.* **373** (2020), 2007–2044.

[KS] Katz, N., and Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, **45**. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[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., Rigid local systems and finite general linear groups, *Math. Z.* **298** (2021), 1293–1321.

[KT5] Katz, N., and Tiep, P.H., Monodromy groups of Kloosterman and hypergeometric sheaves, *Geom. Funct. Analysis* **31** (2021), 562–662.

[KT6] Katz, N., and Tiep, P.H., Exponential sums and total Weil representations of finite symplectic and unitary groups, *Proc. Lond. Math. Soc.* **122** (2021), 745–807.

[KT7] Katz, N., and Tiep, P.H., Hypergeometric sheaves and finite symplectic and unitary groups, *Cambridge J. Math.* **9** (2021), 577–691.

[KT8] Katz, N., and Tiep, P.H., Local systems, extraspecial groups, and finite unitary groups in characteristic 2, (in preparation).

[KT9] Katz, N., and Tiep, P.H., Character sums, hypergeometric sheaves, and monodromy groups, (in preparation).

[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.

[Ku] Kubert, D., Lectures at Princeton University, May 1986.

[Mag] Bosma, W., Cannon, J., Fieker, C., Steel, A. (editors), Handbook of Magma functions, Version 2.19, Sydney, April 24, 2013; `http://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf`.

[Mit] Mitchell, H. H., Determination of the finite quaternary linear groups, *Trans. Amer. Math. Soc.* **14** (1913), 123–142.

[NRS] Nebe, G., Rains, E., and Sloane, N.J.A., The invariants of the Clifford groups, *Des. Codes Crypt.* **24** (2001), 99–122.

[Pop] Pop, F., Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture, *Invent. Math.* **120** (1995), 555–578.

[Ray] Raynaud, M. Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar, *Invent. Math.* **116** (1994), 425–462.

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

[SGA] A. Grothendieck et al, Séminaire de Géometrie Algébrique du Bois-Marie, SGA 4, Part III, Springer Lecture Notes in Math. **305**, Springer, 1973.

[vdG-vdV] van der Geer, G., van der Vlugt, M., Reed-Muller codes and supersingular curves. I, *Compos. Math.* **84** (1992), 333–367.

Department of Mathematics, Princeton University, Princeton, NJ 08544
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
E-mail address: `tiep@math.rutgers.edu`