Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Finite Fields and Their Applications 10 (2004) 221–269
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Notes on G_2, determinants, and equidistribution

Nicholas M. Katz

Princeton University, Princeton, NJ, USA

Received 21 October 2003

Communicated by Daqing Wang

Abstract

We determine the exact shape of the G_2 equidistribution law for the one parameter family of exponential sums over $\mathbb{F}_p^\times$,

$$\sum_{x \bmod p,\ x\neq 0} \chi_2(x)\exp(2\pi i(x^7+tx)/p).$$

Here $\chi_2(x)$ denotes the quadratic character (x/p), t in $\mathbb{F}_p$ is the parameter, and p is any prime other than 2 or 7. This answers a question raised in Keating et al. (J. Phys. A Math. Gen. 36 (2003) 2943, footnote 3) and in Serre (pers. commun., March 7, 2002). We also analyze the analogous families when 7 is replaced by any odd integer $n\geqslant 3$.

Contents

E-mail address: nmk@math.princeton.edu.

1071-5797/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2003.11.002

0. Introduction

The present work grew out of independent email exchanges with Rudnick and with Serre about the exact shape of the G_2 equidistribution law for the sums in the abstract, and for their natural generalization to finite extensions of $\mathbb{F}_p$. One knew that in any characteristic $p>15$, after dividing these sums by a suitable normalizing factor, they were distributed like the traces of random elements of the compact form UG_2 of the exceptional group G_2. The initial problem was to determine precisely this normalizing factor. We carry out this determination (in Sections 1 and 2) using a method which goes back to Davenport and Hasse [Dav-Has], and which ultimately comes down to exploiting the exact shape of the relations between elementary symmetric functions and Newton symmetric functions. The same method works to determine the correct normalizing factor for the analogous sums, when 7 is replaced by any odd integer.

For a fixed odd n, the "geometric monodromy group" G_{geom} attached to this family of sums is the same in all large characteristics p: this "stable value" is G_2 for $n=7$, and $\mathrm{SO}(n)$ for other odd n, see Sections 3 and 4. In Section 4, we analyze the $n=7$ case in all characteristics p where the sums "make sense", i.e., for any p other than 2 or 7. We show that G_{geom} is G_2 except in characteristics 3 and 13, where we show it is a finite group, and determine which finite group it is.

In Section 5, we give the G_2 equidistribution consequences of our results in the $n=7$ case. In Section 6, we give the $\mathrm{SO}(n)$ equidistribution consequences of our results in the $n\neq 7$ case. In the final Section 7, we take the "large n limit" of the results of Section 6, and give applications to the Katz–Sarnak measures $\nu(-,c)$.

It is a pleasure to thank Rudnick and Serre for stimulating the work reported on here. It is also a pleasure to thank Chris Hall for computer computations over the fields of 3^{15} and 3^{16} elements which play an essential role in the analysis of the $n=7$ case in characteristic 3.

1. Determinant calculations

(1.1). We work over a finite field $k=\mathbb{F}_q$ of odd characteristic p. We fix a prime number $\ell\neq p$, an algebraic closure $\bar{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$, and a field embedding ι of $\bar{\mathbb{Q}}_\ell$ into $\mathbb{C}$. We denote by ψ a nontrivial additive character ψ of k, and by χ_2 the quadratic character of $k^\times$, both with values in $\bar{\mathbb{Q}}_\ell^\times$. For any finite extension field E/k, we denote by ψ_E (resp. χ_E) the additive (resp. multiplicative) character of k (resp. $k^\times$) defined by composition with the trace (resp. norm) of E/k.

(1.2). For any α in $k^\times$, we denote by ψ_α the additive character $\psi(\alpha x)$. We define the Gauss sum

$$G(\psi,\chi_2) := \sum_{x \text{ in } k^\times} \chi_2(x)\psi(x). \tag{1.2.1}$$

We have the well-known identities

$$G(\psi_\alpha, \chi_2) = \chi_2(\alpha) G(\psi, \chi_2), \tag{1.2.2}$$

$$G(\psi, \chi_2)^2 = \chi_2(-1)(\#k). \tag{1.2.3}$$

For E/k a finite extension, the Gauss sums for E and k are related by

$$-G(\psi_E, \chi_{2,E}) = (-G(\psi, \chi_2))^{\deg(E/k)}. \tag{1.2.4}$$

(1.3). For each odd integer $n = 2d + 1$ prime to p, there is on $\mathbb{A}^1/k$ a geometrically irreducible lisse $\bar{\mathbb{Q}}_\ell$-sheaf of rank n which is pure of weight one,

$$\mathscr{F}_n := \mathrm{NFT}_\psi(\mathscr{L}_{\chi_2(x)} \otimes \mathscr{L}_{\psi(x^n)}), \tag{1.3.1}$$

cf. [Ka-ESDE, 7.8.2.1], whose trace function is given as follows. For E/k a finite extension, and for t in $E = \mathbb{A}^1(E)$, we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_n) = -\sum_{x \text{ in } E^\times} \chi_{2,E}(x) \psi_E(x^n + tx). \tag{1.3.2}$$

In fact, the stalk at t in $E = \mathbb{A}^1(E)$ of $\mathscr{F}_n$ is the cohomology group

$$H^1_c(\mathbb{G}_m \otimes_E \bar{k}, \mathscr{L}_{\chi_{2,E}(x)} \otimes \mathscr{L}_{\psi(x^n + tx)}).$$

Let us define the sign $\varepsilon(n) = \pm 1$ in k by

$$\varepsilon(n) := (-1)^d \tag{1.3.3}$$

Denote by A_n the ℓ-adic unit in $\bar{\mathbb{Q}}_\ell$ defined by

$$A_n := -G(\psi_{e(n)n}, \chi_2), \tag{1.3.4}$$

and form the constant twist $\mathscr{G}_n$ of $\mathscr{F}_n$ defined by

$$\mathscr{G}_n := \mathscr{F}_n \otimes (A_n)^{-\deg}. \tag{1.3.5}$$

This is a lisse, rank n, $\mathbb{Q}_\ell$-sheaf on $\mathbb{A}^1/k$ which is now pure of weight zero. Its trace function is given as follows. For E/k a finite extension, and for t in $E = \mathbb{A}^1(E)$, we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_n) = \left(\sum_{x \text{ in } E^\times} \chi_{2,E}(x) \psi_E(x^n + tx) \right) / G(\psi_{e(n)n,E}, \chi_{2,E}). \tag{1.3.6}$$

We see easily (by $x \mapsto -x$) that the trace function of $\mathscr{G}_n$ on Frobenii is $\mathbb{R}$-valued (via ι). As $\mathscr{G}_n$ is pure of weight 0, its $\bar{\mathbb{Q}}_\ell$-dual $\mathscr{G}_n^\vee$ as lisse sheaf on $\mathbb{A}^1/k$ has the

complex conjugate trace function on Frobenii. Therefore $\mathscr{G}_n$ is self-dual, because it is absolutely irreducible, and has the same trace function (on Frobenii, and hence on all elements of $\pi_1(\mathbb{A}^1/k)$) as its dual. As $\mathscr{G}_n$ has odd rank n, the autoduality must be orthogonal. So the n-dimensional representation

$$\rho_n : \pi_1(\mathbb{A}^1/k) \to \mathrm{GL}(n, \bar{\mathbb{Q}}_\ell) \tag{1.3.7}$$

corresponding to the lisse sheaf $\mathscr{G}_n$ factors through the orthogonal group $O(n, \bar{\mathbb{Q}}_\ell)$:

$$\rho_n : \pi_1(\mathbb{A}^1/k) \to \mathrm{O}(n, \bar{\mathbb{Q}}_\ell). \tag{1.3.8}$$

(1.4) Theorem. *The representation ρ_n lands in $\mathrm{SO}(n, \bar{\mathbb{Q}}_\ell)$, i.e., for every finite extension E/k and for every t in $E = \mathbb{A}^1(E)$, we have*

$$\det(\mathrm{Frob}_{E,t} \mid \mathscr{G}_n) = 1.$$

(1.5). This theorem is a special case of the following more general result. Denote by $\mathscr{P}_{n,\mathrm{odd}}$ odd the space of monic polynomials of degree n which are odd. Thus for any k-algebra R, a point f in $\mathscr{P}_{n,\mathrm{odd}}(R)$ is a polynomial $f(X)$ in $R[X]$ of the form

$$f(X) = X^n + \sum_{i=1 \text{ to } d} a_{2i-1} X^{2i-1}.$$

Thus $\mathscr{P}_{n,\mathrm{odd}}$ is a d-dimensional affine space $\mathbb{A}^d$, with coordinates the coefficients a_{2i-1}. The lisse sheaf $\mathscr{F}_n$ is the restriction, to the $\mathbb{A}^1$ in $\mathscr{P}_{n,\mathrm{odd}}$ of polynomials of the form $x^n + tx$, of a lisse sheaf $\mathscr{F}_{n,\mathrm{odd}}$ on $\mathscr{P}_{n,\mathrm{odd}}/k$, whose trace function is given as follows. For E/k a finite extension, and for f in $\mathscr{P}_{n,\mathrm{odd}}(E)$, we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,f} \mid \mathscr{F}_{n,\mathrm{odd}}) = -\sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(f(x)). \tag{1.5.1}$$

In fact, the stalk at f in $\mathscr{P}_{n,\mathrm{odd}}(E)$ of $\mathscr{F}_{n,\mathrm{odd}}$ is the cohomology group

$$H^1_c(\mathbb{G}_m \otimes_E \bar{k}, \mathscr{L}_{\chi_{2,E}(x)} \otimes \mathscr{L}_{\psi(f(x))}).$$

(1.6). We form the constant twist $\mathscr{G}_{n,\mathrm{odd}}$ of $\mathscr{F}_{n,\mathrm{odd}}$ defined by

$$\mathscr{G}_{n,\mathrm{odd}} := \mathscr{F}_{n,\mathrm{odd}} \otimes (A_n)^{-\deg}. \tag{1.6.1}$$

This is a lisse, rank n, $\bar{\mathbb{Q}}_\ell$-sheaf on $\mathscr{P}_{n,\mathrm{odd}}/k$ which is now pure of weight zero. Its trace function is given as follows. For E/k a finite extension, and for f in $\mathscr{P}_{n,\mathrm{odd}}(E)$,

we have

$$\mathrm{Trace}(\mathrm{Frob}_{E,f} \mid \mathscr{G}_{n,\mathrm{odd}}) = \left(\sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(f(x)) \right) \Big/ G(\psi_{e(n)n,E}, \chi_{2,E}). \quad (1.6.2)$$

Exactly as above, $\mathscr{G}_{n,\mathrm{odd}}$ has real trace function on Frobenii, so is orthogonally self-dual. The corresponding representation $\rho_{n,\mathrm{odd}}$ lands in $O(n, \bar{\mathbb{Q}}_\ell)$:

$$\rho_{n,\mathrm{odd}} : \pi_1(\mathscr{P}_{n,\mathrm{odd}}/k) \to \mathrm{O}(n, \bar{\mathbb{Q}}_\ell). \quad (1.6.3)$$

(1.7) Theorem. *The representation* $\rho_{n,\mathrm{odd}}$ *lands in* $\mathrm{SO}(n, \bar{\mathbb{Q}}_\ell)$, *i.e., for every finite extension E|k and for every f in* $\mathscr{P}_{n,\mathrm{odd}}(E)$, *we have*

$$\det(\mathrm{Frob}_{E,f} \mid \mathscr{G}_{n,\mathrm{odd}}) = 1.$$

2. Proof of Theorem 1.7

(2.1). We first observe that $\det(\rho_{n,\mathrm{odd}})$ is geometrically trivial, i.e., its restriction to $\pi_1 \,\mathrm{geom}(\mathscr{P}_{n,\mathrm{odd}}/k) = \pi_1(\mathbb{A}^d \otimes_k \bar{k})$ is trivial. Indeed, this restriction is a homorphism from $\pi_1(\mathbb{A}^d \otimes_k \bar{k})$ to $\{\pm 1\} = \mu_2$, i.e., an element of $H^1(\mathbb{A}^d \otimes_k \bar{k}, \mu_2)$, and this last group vanishes, because $\mathrm{char}(k)$ is odd. Therefore $\det(\rho_{n,\mathrm{odd}})$ is a homomorphism

$$\det(\rho_{n,\mathrm{odd}}) : \pi_1(\mathscr{P}_{n,\mathrm{odd}}/k) \to \{\pm 1\} \quad (2.1.1)$$

which is geometrically constant, so necessarily of the form $B^{\deg}$ for some choice of B in $\{\pm 1\}$. For this B, we have

$$\det(\mathrm{Frob}_{E,f} \mid \mathscr{G}_{n,\mathrm{odd}}) = (B)^{\deg(E/k)}. \quad (2.1.2)$$

(2.2). We must show that $B = 1$. For this, it suffices to compute at a single k-valued point f. We take the point $f := x^n$.

We have

$$\begin{aligned} \det(1 - A_n T \,\mathrm{Frob}_{k,f} \mid \mathscr{G}_{n,\mathrm{odd}}) &= \det(1 - T \,\mathrm{Frob}_k \mid H^1_c(\mathbb{G}_m \otimes_k \bar{k}, \mathscr{L}_{\chi_2(x)} \otimes \mathscr{L}_{\psi(x^n)}) \\ &= L(\mathbb{G}_m/k, \mathscr{L}_{\chi_2(x)} \otimes \mathscr{L}_{\psi(x^n)}, T), \end{aligned} \quad (2.2.1)$$

the abelian L-function on $\mathbb{G}_m/k$ with coefficients in $\mathscr{L}_{\chi_2(x)} \otimes \mathscr{L}_{\psi(x^n)}$. The additive expression of this L-function as a sum over all effective divisors of $\mathbb{G}_m/k$, i.e. over all monic polynomials $h(X)$ in $k[X]$ with $h(0) \neq 0$, is

$$1 + \sum_{r \geqslant 1} c_r T^r,$$

where c_r is the sum

$$c_r = \sum_{\text{monic } h \text{ of degree } r \text{ with } h(0)\neq 0} \chi_2\left(\prod_{\text{roots } \alpha \text{ of } h} \alpha\right)\psi\left(\sum_{\text{roots } \alpha \text{ of } h} \alpha^n\right). \tag{2.2.1}$$

But this L-function is a polynomial of degree n. Comparing coefficients of T^n, we find

$$\begin{aligned}&\det(-A_n\text{Frob}_{k,f} \mid \mathscr{G}_{n,\text{odd}})\\ &= \det(-\text{Frob}_k \mid H^1_c(\mathbb{G}_m \otimes_k \bar{k}, \mathscr{L}_{\chi_2(x)} \otimes \mathscr{L}_{\psi(f(x))})\\ &= c_n,\end{aligned} \tag{2.2.2}$$

which we rewrite in the equivalent form

$$\det(\text{Frob}_{k,f} \mid \mathscr{G}_{n,\text{odd}}) = c_n/(-A_n)^n. \tag{2.2.3}$$

(2.3). We now compute c_n as an n-variable character sum. Write a monic h of degree n as

$$h(X) = X^n + \sum_{i=1 \text{ to } n} (-1)^i s_i X^{n-i}. \tag{2.3.1}$$

Then

$$\prod_{\text{roots } \alpha \text{ of } h} \alpha = s_n, \tag{2.3.2}$$

$$\sum_{\text{roots } \alpha \text{ of } h} \alpha^n = N_n, \tag{2.3.3}$$

where the N_n is the nth Newton symmetric function. We know that N_n is an isobaric polynomial of weight n in $s_1, \ldots, s_n$:

$$N_n = N_n(s_1, \ldots, s_n).$$

So the coefficient c_n is given by the n-variable character sum

$$c_n = \sum_{s_1,\ldots,s_n \text{ in } k, s_n\neq 0} \chi_2(s_n)\psi(N_n(s_1, \ldots, s_n)). \tag{2.3.4}$$

It remains only to establish the identity

$$c_n = (-A_n)^n, \tag{2.3.5}$$

i.e.,

$$c_n = G(\psi_{e(n)n}, \chi_2)^n. \tag{2.3.6}$$

Recall that $G(\psi_{e(n)n}, \chi_2)^2 = \chi_2(-1)q$, and $n = 2d+1$, so we have

$$\begin{aligned} G(\psi_{e(n)n}, \chi_2)^n &= (G(\psi_{e(n)n}, \chi_2)^2)^d G(\psi_{e(n)n}, \chi_2) \\ &= \chi_2((-1)^d) q^d G(\psi_{e(n)n}, \chi_2) \\ &= q^d G(\psi_n, \chi_2), \end{aligned} \tag{2.3.7}$$

the last identity because $\varepsilon(n)$ is $(-1)^d$. Thus we must show that

$$\sum_{s_1,\ldots,s_n \text{ in } k, s_n \neq 0} \chi_2(s_n)\psi(N_n(s_1, \ldots, s_n)) = q^d G(\psi_n, \chi_2). \tag{2.3.8}$$

The proof of this depends on the following lemma.

(2.4) Lemma. *For $n = 2d+1 \geqslant 3$, we have the identity*

$$\begin{aligned} &N_n(s_1, \ldots, s_n) \\ &\quad = (-1)^{n+1} n s_n + (-1)^n n \sum_{i=1 \text{ to } d} s_i s_{n-i} + R_n(s_1, \ldots, s_n), \end{aligned}$$

where every monomial in $R_n(s_1, \ldots, s_n)$ is isobaric of weight n and has usual degree $\geqslant 3$.

Proof. Applying $(Td/dT)\circ\log$ to the identity

$$\prod_{i=1 \text{ to } n} (1 - X_i T) = 1 + \sum_{i=1 \text{ to } n} (-1)^i s_i T^i, \tag{2.4.1}$$

we find

$$-\sum_{n \geqslant 1} N_n T^n = \left(\sum_{i=1 \text{ to } n} (-1)^i i s_i T^i \right) \Big/ \left(1 + \sum_{i=1 \text{ to } n} (-1)^i s_i T^i \right). \tag{2.4.2}$$

Cross-multiply and equate coefficients of like powers of T to obtain the identity, for each $i = 1$ to n,

$$(-1)^{i+1} i s_i = N_i + \sum_{a=1 \text{ to } i-1} (-1)^a s_a N_{i-a}. \tag{2.4.3}$$

Because N_i is isobaric of weight i, N_i involves only $s_1, \ldots, s_i$, and the involvement of s_i is of the form

$$N_i = (-1)^{i+1} i s_i + P_i(s_1, \ldots, s_{i-1}), \tag{2.4.4}$$

where every monomial in $P_i(s_1, \ldots, s_{i-1})$ is isobaric of weight i and has usual degree $\geqslant 2$. [Indeed, $P_i(s_1, \ldots, s_{i-1})$ is given explicitly as

$$P_i(s_1, \ldots, s_{i-1}) = -\sum_{a=1 \text{ to } i-1} (-1)^a s_a N_{i-a}, \tag{2.4.5}$$

but we will not use this more explicit information.] Take the formula (2.4.3) above for $i = n$,

$$(-1)^{n+1} n s_n = N_n + \sum_{a=1 \text{ to } n-1} (-1)^a s_a N_{n-a}, \tag{2.4.6}$$

and substitute for $N_i = (-1)^{i+1} i s_i + P_i(s_1, \ldots, s_{i-1})$. We obtain

$$\begin{aligned} N_n &= (-1)^{n+1} n s_n - \sum_{a=1 \text{ to } n-1} (-1)^a s_a N_{n-a} \\ &= (-1)^{n+1} n s_n - \sum_{a=1 \text{ to } n-1} (-1)^a s_a (-1)^{n-a+1} (n-a) s_{n-a} \\ &\quad - \sum_{a=1 \text{ to } n-1} (-1)^a s_a P_{n-a}(s_1, \ldots, s_{n-a-1}). \end{aligned} \tag{2.4.7}$$

The final term will be our $R_n(s_1, \ldots, s_n)$. In the sum

$$-\sum_{a=1 \text{ to } n-1} (-1)^a s_a (-1)^{n-a+1} (n-a) s_{n-a},$$

every term $s_i s_{n-i}$ with $1 \leqslant i \leqslant d$ occurs twice, first with coefficient $(-1)^n (n-i)$, and then again with coefficient $(-1)^n (i)$. □

(2.5) Corollary. *For $n = 2d+1 \geqslant 3$, if we write $N_n(s_1, \ldots, s_n)$ as a polynomial in $s_{d+1}, \ldots, s_n$, with coefficients in $\mathbb{Z}[s_1, \ldots, s_d]$, we have*

$$\begin{aligned} N_n(s_1, \ldots, s_n) &= (-1)^{n+1} n s_n \\ &\quad + (-1)^n n \sum_{i=1 \text{ to } d} s_{n-i}(s_i + Q_i(s_1, \ldots, s_{i-1})) + P_n(s_1, \ldots, s_d), \end{aligned}$$

where each $Q_i(s_1, \ldots, s_{i-1})$ is isobaric of weight i, and every monomial in it has usual degree at least two, and where $P_n(s_1, \ldots, s_d)$ is isobaric of weight n, and every monomial in it has usual degree at least three.

Proof. From the isobaricity of R_n, we see that each of $s_n, s_{n-1}, \ldots, s_{d+1}$, occurs at most linearly. If one of these, say $s_{n-i}, i \leqslant d$, occurs, its coefficient Q_i in R_n is isobaric of weight i, and every monomial in Q_i has usual degree at least two, so only involves those variables s_a with index $1 \leqslant a \leqslant i-1$. Those monomials in R_n which involve none of $s_n, s_{n-1}, \ldots, s_{d+1}$ comprise P_n. □

(2.6). With this corollary established, it is a simple matter to compute c_n. We have

$$\begin{aligned} c_n &= \sum_{s_1,\dots,s_n \text{ in } k,\ s_n\neq 0} \chi_2(s_n)\psi(N_n(s_1,\dots,s_n)) \\ &= \sum_{s_1,\dots,s_n \text{ in } k,\ s_n\neq 0} \\ &\quad \times\chi_2(s_n)\psi((-1)^{n+1}ns_n + (-1)^n n \sum_{i=1 \text{ to } d} s_{n-i}(s_i + Q_i(s_1,\dots,s_{i-1})) + P_n(s_1,\dots,s_d)) \\ &= \left(\sum_{s_n \text{ in } k^x} \chi_2(s_n)\psi((-1)^{n+1}ns_n)\right) \sum_{s_1,\dots,s_{n-1} \text{ in } k} \psi(P_n(s_1,\dots,s_d)) \\ &\quad \times \psi\left((-1)^n n \sum_{i=1 \text{ to } d} s_{n-i}(s_i + Q_i(s_1,\dots,s_{i-1}))\right). \end{aligned} \tag{2.6.1}$$

Remember that $n = 2d+1$ is odd, so the first sum is just $G(\psi_n, \chi_2)$. We claim the second sum is q^d. Write it as

$$\begin{aligned} &\sum_{s_1,\dots,s_d \text{ in } k} \psi(P_n(s_1,\dots,s_d)) \\ &\quad \times \sum_{s_{d+1},\dots,s_{n-1} \text{ in } k} \psi_{-n}\left(\sum_{i=1 \text{ to } d} s_{n-i}(s_i + Q_i(s_1,\dots,s_{i-1}))\right). \end{aligned} \tag{2.6.2}$$

The inner sum is of the form

$$\sum_{s_{d+1},\dots,s_{n-1} \text{ in } k} \psi(\text{a linear form in } s_{n-1},\dots,s_{d+1}), \tag{2.6.3}$$

so it vanishes unless all the coefficients of the linear form vanish, in which case it is q^d. But the coefficients are

$$s_1, s_2 + Q_2(s_1), \dots, s_i + Q_i(s_1,\dots,s_{i-1}), \dots, s_d + Q_d(s_1,\dots,s_{d-1}). \tag{2.6.4}$$

If they all vanish, then we see successively that $s_1 = 0, s_2 = 0, \dots, s_d = 0$. So the inner sum is nonzero precisely once, for $s_1 = \cdots = s_d = 0$, in which case it is q^d. Thus the second sum is $q^d\psi(P_n(0,\dots,0))$. Now P_n has no constant term, every monomial in it being of usual degree at least three, so $P_n(0,\dots,0) = 0$, and so

$$q^d\psi(P_n(0,\dots,0)) = q^d\psi(0) = q^d. \tag{2.6.5}$$

This concludes the proof of Theorem (1.7), and with it, Theorem (1.4). □

3. Monodromy of $\mathscr{G}_n$ for general odd n

(3.1). In [Ka-ESDE, 7.1.1], we defined, for each integer $b \geqslant 1$, nonzero integers $N_1(b)$ and $N_2(b)$, and showed that if a prime p does not divide $2N_1(b)N_2(b)$, then the relations in $\bar{\mathbb{F}}_p$ of the form

$$\alpha - \beta = \gamma - \delta$$

among elements α, β, γ, δ of $\mu_b(\bar{\mathbb{F}}_p) \cup \{0\}$ are, in a precise sense, "the same" as in characteristic zero.

(3.2) Theorem. *Fix an odd integer $n \geqslant 3$, $n \neq 7$. For any prime p such that*

$$p > 2n + 1,$$

and

$$p \text{ does not divide } 2nN_1(n-1)N_2(n-1),$$

for any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, the group G_{geom} for the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_n$ (or equivalently for the lisse sheaf $\mathscr{F}_n$) on $\mathbb{A}^1/k$ is $\mathrm{SO}(n)$.

Proof. The description of $\mathscr{F}_n$ as a Fourier Transform, together with Laumon's Stationary Phase, [Lau-TF] or [Ka-ESDE, 7.4.1, 7.5], shows that the $I(\infty)$-representation attached to $\mathscr{F}_n$ is the direct sum

$$\mathscr{L}_{\chi_2} \oplus \text{ (a totally wild representation of } \dim n-1, \text{ all breaks } n/(n-1)).$$

Because $p > 2n+1$, and $\mathscr{F}_n$ is lisse of rank n and geometrically irreducible on $\mathbb{A}^1$, it is Lie-irreducible [Ka-MG, Proposition 5]. We now apply [Ka-ESDE, 7.2.7], with a/b there taken to be $n/(n-1)$. Since we have an a priori inclusion of G_{geom} in $\mathrm{SO}(n)$, the only possibility among the choices offered there for $(G_{\text{geom}})^{0,\text{der}}$ is $\mathrm{SO}(n)$ itself. □

(3.3). For any given odd $n \geqslant 3$, we do not know the exact list of the exceptional primes, those p prime to $2n$ for which G_{geom} for $\mathscr{F}_n$ is smaller than $\mathrm{SO}(n)$. However, there is a general principle that it quite useful in thinking about such questions.

(3.4) Lemma. *Fix an odd integer $n \geqslant 3$, a characteristic p prime to $2n$, and a prime $\ell \neq p$. The group G_{geom} for $\mathscr{F}_n$ is independent of the auxiliary choice of (k, ψ) used to define $\mathscr{F}_n$.*

Proof. Given two data (k, ψ) to (k_1, ψ_1), denote by $\mathscr{F}_n(k, \psi)$ and $\mathscr{F}_n(k_1, \psi_1)$ the versions of $\mathscr{F}_n$ they give rise to. To compare them, we pass to a common finite extension E of both k and k_1. There the two nontrivial additive characters ψ_E and

$\psi_{1,E}$ are $E^\times$-proportional: there exists α in $E^\times$ such that for x in E we have

$$\psi_{1,E}(x) = \psi_E(\alpha x).$$

Passing to a further finite extension if necessary, we may assume that $\alpha = \beta^{2n}$ for some β in $E^\times$. Then we see that for any finite extension E_1 of E, and any t in E_1, we have

$$\begin{aligned}
&\mathrm{Trace}(\mathrm{Frob}_{E_1,t} \mid \mathscr{F}_n(k_1,\psi_1))\\
&= -\sum_{x \text{ in } E_1^\times} \chi_{2,E_1}(x)\psi_{E_1}(\beta^{2n}(x^n + tx))\\
&= -\sum_{x \text{ in } E_1^\times} \chi_{2,E_1}(\beta^{-2}x)\psi_{E_1}(\beta^{2n}((\beta^{-2}x)^n + t\beta^{-2}x))\\
&= -\sum_{x \text{ in } E_1^\times} \chi_{2,E_1}(x)\psi_{E_1}(x^n + t\beta^{2n-2}x))\\
&= \mathrm{Trace}(\mathrm{Frob}_{E_1,t\beta^{2n-2}} \mid \mathscr{F}_n(k,\psi)).
\end{aligned}$$

This means that after pullback to $\mathbb{A}^1/E$, the sheaves

$$\mathscr{F}_n(k_1,\psi_1) \quad \text{and} \quad [t \mapsto \beta^{2n-2}t]^*\mathscr{F}_n(k,\psi)$$

have the same trace function. As both are geometrically and hence arithmetically irreducible, by Chebotarev, they are isomorphic:

$$\mathscr{F}_n(k_1,\psi_1) \cong [t \mapsto \beta^{2n-2}t]^*\mathscr{F}_n(k,\psi) \quad \text{on } \mathbb{A}^1/E.$$

In particular, they are geometrically isomorphic. Now

$$[t \mapsto \beta^{2n-2}t]^*\mathscr{F}_n(k,\psi)$$

is the pullback of $\mathscr{F}_n(k,\psi)$ by an automorphism, so has the same G_{geom} as $\mathscr{F}_n(k,\psi)$. Thus $\mathscr{F}_n(k_1,\psi_1)$ and $\mathscr{F}_n(k,\psi)$ have the same G_{geom}.

(3.5) Lemma. *Suppose k is a finite field of characteristic p, C/k a smooth, geometrically connected affine curve, ℓ a prime invertible in k, and $\mathscr{F}$ a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on C which is geometrically irreducible, and whose rank n is a prime number. Then either $\mathscr{F}$ is Lie-irreducible, or $\mathscr{F}$ has finite G_{geom}. If in addition C is $\mathbb{A}^1$ and $p > n$, then either $\mathscr{F}$ is Lie-irreducible or G_{geom} is a finite primitive irreducible subgroup of* $\mathrm{GL}(n,\bar{\mathbb{Q}}_\ell)$.

Proof. If $\mathscr{F}$ is not Lie-irreducible, then [Ka-MG, Proposition 1] geometrically it is either induced, i.e. of the form $\pi_*\mathscr{H}$ for some finite etale covering $\pi : Z \to C/\bar{k}$ of degree $d > 1$, $d|n$, and some lisse $\mathscr{H}$ on Z of rank n/d, or it is a tensor product $\mathscr{A} \otimes \mathscr{B}$ with $\mathscr{B}$ Lie-irreducible of rank r a proper divisor r of n, and with $\mathscr{A}$ of rank n/r

having finite G_{geom}. Since n is prime, in the induced case $\mathscr{F}$ is $\pi_*\mathscr{L}$ for some $\mathscr{L}$ of rank one, and in the tensor product case $\mathscr{F}$ is $\mathscr{A}\otimes\mathscr{L}$ with $\mathscr{L}$ of rank one and $\mathscr{A}$ having finite G_{geom}. In either case, the pullback of $\mathscr{F}$ to a finite etale connected galois covering of $C/\bar{k}$ is the direct sum of n lisse sheaves, each of rank one. Therefore $(G_{\text{geom}})^0$ for $\mathscr{F}$ lies in a torus, so is a torus. But by Grothendieck's theorem [De-WeilII, 1.3.9], $(G_{\text{geom}})^0$ for $\mathscr{F}$ is semisimple. Therefore $(G_{\text{geom}})^0$ for $\mathscr{F}$ is trivial, i.e. G_{geom} for $\mathscr{F}$ is finite. If C is $\mathbb{A}^1$ and $p>n$, the induced case is impossible, because $\mathbb{A}^1/\bar{k}$ has no connected finite etale coverings of degree $<p$. □

(3.6). We now return to the sheaves $\mathscr{F}_n$. When n is prime, we have the following result.

(3.7) Theorem. *Fix an odd integer $n\geqslant 3$, $n\neq 7$, and suppose that n is prime. Then for any prime $p\geqslant 2n+1$, for any finite field k of characteristic p, for any prime $\ell\neq p$, and for any choice of nontrivial additive character ψ of k, the group G_{geom} for the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_n$ (or equivalently for the lisse sheaf $\mathscr{F}_n$) on $\mathbb{A}^1/k$ is* $\mathrm{SO}(n)$.

Proof. We first treat the case $p>2n+1$. Because $p>2n+1$, and $\det(\mathscr{F}_n)$ is geometrically trivial, $\mathscr{F}_n$ is Lie-irreducible, and G_{geom} is connected [Ka-MG, Proposition 5]. Thus G_{geom} is an irreducible connected subgroup of $\mathrm{SO}(n)$. Because n is an odd prime other than 7, it results from Gabber's theorem on prime-dimensional representations [Ka-ESDE, 1.6] that G_{geom} is either $\mathrm{SO}(n)$ or the faithful image $\mathrm{PSL}(2)$ of $\mathrm{SL}(2)$ in $\mathrm{Sym}^{n-1}(\mathrm{std}_2)$. If $n=3$, these two cases coincide. If $n\geqslant 5$, the second case cannot occur. Indeed, $\mathscr{F}_n$ has an ∞-break $n/(n-1)$, so by [Ka-GKM, 1.9], every faithful representation of its G_{geom} has dimension $\geqslant n-1$, compare [Ka-ESDE, proof of 9.1.1]. But $\mathrm{PSL}(2)\cong\mathrm{SO}(3)$ has a faithful three-dimensional representation.

It remains to treat the case $p=2n+1$. If $\mathscr{F}_n$ is Lie-irreducible, then the argument above applies.

Since n is prime, if $\mathscr{F}_n$ is not Lie-irreducible, then by Lemma (3.5) above, it has finite G_{geom}. We must show that G_{geom} for $\mathscr{F}_n$ is not finite, if $p=2n+1$. The key point is not the exact value of p, but rather that we have the congruence

$$p\equiv 1 \bmod 2n.$$

If G_{geom} is finite, then a power of every $\mathrm{Frob}_{E,t}\,|\,\mathscr{F}_n$ is scalar, cf. [Ka-ESDE, 8.14.3.1]. In particular, a power of $\mathrm{Frob}_{k,0}\,|\,\mathscr{F}_n$ is scalar, and hence in particular has equal eigenvalues.

To conclude the proof, we will now show that if $p\equiv 1 \bmod 2n$, then no power of $\mathrm{Frob}_{k,0}\,|\,\mathscr{F}_n$ has equal eigenvalues. We argue by contradiction. Since $p\equiv 1 \bmod 2n$, and n is an odd prime, already $\mathbb{F}_p$ and hence k contains all the $2n$th roots of unity. Enlarging k if necessary, we may assume that $\mathrm{Frob}_{k,0}\,|\,\mathscr{F}_n$ itself has all equal eigenvalues. Denote by $\{\Lambda_1,\ldots,\Lambda_n\}$ all the multiplicative characters of $k^\times$ of order

dividing n. We have

$$\begin{aligned}
&\mathrm{Trace}(\mathrm{Frob}_{k,0} \mid \mathscr{F}_n)\\
&= -\sum_{x\neq 0 \text{ in } k} \chi_2(x)\psi(x^n)\\
&= -\sum_{x\neq 0 \text{ in } k} \chi_2(x^n)\psi(x^n)\\
&= -\sum_{u\neq 0 \text{ in } k} \chi_2(u)\psi(u)\ (\text{number of } n\text{th roots of } u \text{ in } k)\\
&= -\sum_{u\neq 0 \text{ in } k} \chi_2(u)\psi(u)\sum_{i=1 \text{ to } n} \Lambda_i(u)\\
&= \sum_{i=1 \text{ to } n} -G(\psi,\chi_2\Lambda_i).
\end{aligned}$$

These same identities, but over all finite extensions of k, show that the eigenvalues of $\mathrm{Frob}_{k,0} \mid \mathscr{F}_n$ are precisely the $((-1)\times)$ Gauss sums

$$-G(\psi,\chi_2\Lambda_i),$$

for all the characters Λ_i of order dividing n. So it suffices to show that these n Gauss sums are all distinct. The key point is that the characters $\chi_2\Lambda_i$ are all distinct, all nontrivial, and they all have order dividing $p-1$. That they are all distinct results from the fact that the $p-2$ Gauss sums formed with *all* the nontrivial characters of order dividing $p-1$ are all distinct. This follows from (the most elementary case of) Stickelberger's theorem. These sums all lie in $\mathbb{Z}[\zeta_p,\zeta_{p-1}]$, and for any p-adic place $\mathscr{P}$ of $\mathbb{Q}(\zeta_p,\zeta_{p-1})$, these Gauss sums have all distinct $\mathscr{P}$-adic valuations. If we normalize $\mathrm{ord}_{\mathscr{P}}$ by $\mathrm{ord}_{\mathscr{P}}(\#k)=1$, the $p-2$ sums in question have as $\mathrm{ord}_{\mathscr{P}}$'s the $p-2$ fractions $a/(p-1)$, for $a=1$ to $p-2$, in some order. □

(3.8). For $n=3$, this result is sharp.

(3.9) Lemma. *In characteristic $p=5$, $\mathscr{F}_3$, or equivalently $\mathscr{G}_3$, has finite $G_{\mathrm{geom}}=A_5$, where A_5 is viewed as lying in* SO(3) *by one of its two irreducible three-dimensional representations.*

Proof. By Lemma (3.4) above, we may choose k to the prime field $\mathbb{F}_5$, and ψ to be (the image under ι of) the $\mathbb{C}$-valued additive character $x\mapsto\exp(2\pi ix/5)$. We know a priori that G_{geom} is a irreducible subgroup of SO(3), so it is either SO(3) itself, or it is one of A_4, S_4, or A_5.

We first show that G_{geom} is not SO(3). We argue by contradiction. Recall that SO(3) has a unique irreducible representation Λ_{2m+1} of each odd dimension $2m+1$. Since $\mathscr{G}_3$ has $\pi_1(\mathbb{A}^1/\mathbb{F}_5)$ landing in SO(3), we can form the lisse sheaf $\Lambda_{2m+1}(\mathscr{G}_3)$ on $\mathbb{A}^1/\mathbb{F}_5$. Each sheaf $\Lambda_{2m+1}(\mathscr{G}_3)$ is pure of weight zero and self-dual. If G_{geom} is SO(3),

then each is geometrically irreducible, and so we will have

$$H_c^2(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$$
$$\cong H_c{}^2(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,\ End(\Lambda_{2m+1}(\mathscr{G}_3)))=\bar{\mathbb{Q}}_\ell(-1).$$

So for any finite extension $E/\mathbb{F}_5$, the Lefschetz trace formula will give

$$\sum_{t\ \text{in}\ E}(\mathrm{Trace}(\mathrm{Frob}_{E,t}\mid\Lambda_{2m+1}(\mathscr{G}_3)))^2$$
$$=\#E-\mathrm{Trace}(\mathrm{Frob}_E\mid H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})).$$

By Deligne [De-WeilII, 3.3.1], $H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$ is mixed of weight $\leqslant 1$, and hence we have the estimate

$$\left|\#E-\sum_{t\ \text{in}\ E}(\mathrm{Trace}(\mathrm{Frob}_{E,t}\mid\Lambda_{2m+1}(\mathscr{G}_3)))^2\right|$$
$$\leqslant\dim H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})(\#E)^{1/2}.$$

Dividing through by $\#E$, we rewrite this in the form

$$\left|1-(1/\#E)\sum_{t\ \text{in}\ E}(\mathrm{Trace}(\mathrm{Frob}_{E,t}\mid\Lambda_{2m+1}(\mathscr{G}_3)))^2\right|$$
$$\leqslant\dim H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})/(\#E)^{1/2}.$$

We next note that

$$\dim H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})\leqslant 1+2m^2+2m.$$

To show this, we argue as follows. Because G_{geom} is SO(3),
$\dim H_c{}^2(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})=1$, so

$$1-\dim H_c{}^1(\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$$
$$=\chi((\mathbb{A}^1\otimes\bar{\mathbb{F}}_5,(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$$
$$=\mathrm{rank}((\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})-\mathrm{Swan}_\infty(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$$
$$=(2m+1)^2-\mathrm{Swan}_\infty(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}).$$

Now $\mathscr{G}_3$ has highest ∞-slope 3/2, so $(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$ has highest ∞-slope $\leqslant 3/2$, and so

$$\mathrm{Swan}_\infty(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})\leqslant(3/2)\mathrm{rank}(\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2})$$
$$\leqslant(3/2)(2m+1)^2.$$

Thus we have

$$(2m+1)^2 \geqslant \chi((\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) \geqslant (2m+1)^2 - (3/2)(2m+1)^2.$$

On the other hand, we have

$$1 - \dim H_c{}^1(\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) = \chi((\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}),$$

so we have

$$1 \geqslant \chi((\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}).$$

Thus we have

$$1 \geqslant \chi((\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) \geqslant -(1/2)(2m+1)^2,$$

and so

$$1 \geqslant 1 - \dim H_c{}^1(\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) \geqslant -(1/2)(2m+1)^2,$$

so finally

$$\dim H_c{}^1(\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) \leqslant 1 + (1/2)(2m+1)^2$$
$$\leqslant 1 + 2m^2 + 2m + 1/2.$$

Since dimensions are integers, we have

$$\dim H_c{}^1(\mathbb{A}^1 \otimes \bar{\mathbb{F}}_5, (\Lambda_{2m+1}(\mathscr{G}_3))^{\otimes 2}) \leqslant 1 + 2m^2 + 2m,$$

as asserted. Thus if G_{geom} is SO(3), we have the estimate, for every $m \geqslant 1$, and every finite extension $E/\mathbb{F}_5$,

$$\left| 1 - (1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \Lambda_{2m+1}(\mathscr{G}_3)))^2 \right|$$
$$\leqslant (1 + 2m^2 + 2m)/(\#E)^{1/2}.$$

We now take $m = 3$. Then a machine calculation over E the field of $5^5 = 3125$ elements gives

$$(1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \Lambda_7(\mathscr{G}_3)))^2 = 1.99872,$$

which is not within

$$(1 + 2m^2 + 2m)/(\#E)^{1/2} = 25/\text{Sqrt}(5^5) = 0.447214$$

of 1. Therefore G_{geom} for $\mathscr{G}_3$ is not SO(3).

The only other possibilities for G_{geom}, i.e., the only finite irreducible subgroups of SO(3), are A_4, S_4, and A_5. Denote by G_{arith} the Zariski closure of $\rho(\pi_1(\mathbb{A}^1/k))$ in SO(3), for ρ the representation corresponding to $\mathscr{G}_3$. Then G_{arith} is finite as well, cf. [Ka-ESDE, 8.14.3.1], and it contains G_{geom} as a normal irreducible subgroup. So G_{arith} is itself one of A_4, S_4, or A_5. But all the irreducible three-dimensional representations of A_4 and S_4 have trace functions which take values in the set $\{3,1,0,-1\}$. On the other hand, the traces of G_{arith} are all the numbers

$$\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_3) = (-1/G(\psi,\chi_2))^{\deg(E/\mathbb{F}_p)} \times \left(- \sum_{t \text{ in } E} \chi_{2,E}(x)\psi_E(x^3+tx) \right).$$

Taking for E the prime field $\mathbb{F}_5$, and $t=1$, we get 1.61803… as a trace, and hence G_{arith} can only be A_5. Since A_5 is simple, and G_{geom} is an irreducible normal subgroup of it, we have $G_{\text{geom}} = A_5$. □

(3.10). For general odd n, we have uniform results not for $\mathscr{F}_n$ but for its several parameter version $\mathscr{F}_{n,\text{odd}}$.

(3.11) Theorem. *Fix $p>5$. Then for any odd $n \geqslant 3$ prime to p, for any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, the group G_{geom} for the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_{n,\text{odd}}$ (or equivalently for the lisse sheaf $\mathscr{F}_{n,\text{odd}}$) on $\mathscr{P}_{n,\text{odd}}/k$ is* SO(n).

Proof. For $n=3$, $\mathscr{F}_{3,\text{odd}}$ is just $\mathscr{F}_3$, and the theorem is a special case of Theorem (3.7). We will handle the case $n \geqslant 5$ by a degeneration argument, which in fact proves a stronger result. Inside the space $\mathscr{P}_{n,\text{odd}}$ of monic odd polynomials of degree n, let us denote by $\mathscr{P}_{n,\text{odd},\leqslant 3}$ the closed subscheme whose R-valued points are all polynomials of the form

$$x^n + bx^3 + cx,$$

with b, c in R. We denote by $\mathscr{F}_{n,\text{odd},\leqslant 3}$ (respectively $\mathscr{G}_{n,\text{odd},\leqslant 3}$) the restriction of $\mathscr{F}_{n,\text{odd}}$ (respectively $\mathscr{G}_{n,\text{odd}}$) to this closed subspace. We know that G_{geom} for $\mathscr{F}_{n,\text{odd}}$ lies in SO(n). Since G_{geom} for a pullback is a subgroup, it suffices to prove that G_{geom} for $\mathscr{F}_{n,\text{odd},\leqslant 3}$ is SO(n). □

(3.12) Theorem. *Fix $p>5$. Then for any odd $n \geqslant 5$ prime to p, for any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, the group G_{geom} for the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_{n,\text{odd},\leqslant 3}$ (or equivalently for the lisse sheaf $\mathscr{F}_{n,\text{odd},\leqslant 3}$) on $\mathscr{P}_{n,\text{odd}}/k$ is* SO(n).

Proof. Exactly as in [Ka-LFM, pp. 115–119], we show that the fourth moment M_4 of G_{geom} for the lisse sheaf $\mathscr{F}_{n,\text{odd},\leqslant 3}$ is 3. Since G_{geom} is a priori a subgroup of SO(n),

it follows from Larsen's Alternative [Ka-LFM, p. 113] that G_{geom} is either $\mathrm{SO}(n)$, or is finite.

It remains to show that G_{geom} for $\mathscr{F}_{n,\text{odd},\leqslant 3}$ is not finite. Consider the following geometric situation. Over $\mathbb{A}^3/k$, with coordinates $a,\ b,\ c$ consider the product space $\mathbb{G}_m \times \mathbb{A}^3$, with coordinates $x,\ a,\ b,\ c$, endowed with the lisse sheaf

$$\mathscr{K} := \mathscr{L}_{\chi_2(x)}\mathscr{L}_{\psi(a^2x^n+bx^3+cx)}.$$

Via the projection

$$\begin{array}{c} \mathbb{G}_m \times \mathbb{A}^3 \\ \downarrow pr_2 \\ \mathbb{A}^3, \end{array}$$

we form the sheaf

$$\mathscr{M} := R^1(pr_2)_!\mathscr{K}$$

on the base $\mathbb{A}^3/k$. As explained in [Ka-SMD], $\mathscr{M}$ is a sheaf of perverse origin on $\mathbb{A}^3/k$. The restriction of $\mathscr{M}$ to the $\mathbb{A}^1$ of polynomials x^3+tx, i.e., the points $(0,1,t)$ in $\mathbb{A}^3$, is just the sheaf $\mathscr{F}_3$. The restriction of $\mathscr{M}$ to the open set $\mathbb{A}^3[1/a]$ is isomorphic to a pullback of the sheaf $\mathscr{F}_{n,\text{odd},\leqslant 3}$. [First pull back by the map

$$\mathbb{A}^3[1/a] \to \mathscr{P}_{n,\text{odd},\leqslant 3}.$$

$$(a,b,c) \to x^n + (b/a^6)x^3 + (c/a^2)x,$$

then do the $\mathbb{A}^3[1/a]$-automorphism of $\mathbb{G}_m \times \mathbb{A}^3[1/a]$

$$(x,a,b,c) \to (a^2x,a,b,c).]$$

So if $\mathscr{F}_{n,\text{odd},\leqslant 3}$ has finite G_{geom}, then $\mathscr{M}|\mathbb{A}^3[1/a]$ has finite G_{geom}. This implies, by [Ka-SMD], that $\mathscr{M}|$ (the $\mathbb{A}^1$ of $(0,1,t)$) has finite G_{geom}. But $\mathscr{M}|$ (the $\mathbb{A}^1$ of $(0,1,t)$) is $\mathscr{F}_3$, whose G_{geom} is not finite, being $\mathrm{SO}(3)$. Therefore $\mathscr{F}_{n,\text{odd},\leqslant 3}$ does not have finite G_{geom}. □

4. Monodromy of $\mathscr{G}_7$: the group G_2 and its finite subgroups

(4.1). Recall that G_2 is the automorphism group of Cayley's and Graves' octonions, cf. [Spr, 17.4], [Adams, 15.16]. By looking its action on the "purely imaginary" octonions, we obtain G_2 as a closed subgroup of $\mathrm{SO}(7)$. Let us denote by UG_2 a maximal compact subgroup of the complex Lie group $G_2(\mathbb{C})$. The following lemma is well known, we include it for ease of reference.

(4.2) Lemma. *Two elements of* UG_2 *are conjugate in* UG_2 *if and only if they have the same characteristic polynomial in the given seven-dimensional representation.*

Proof. Use the fact that the two fundamental representations ω_1 and ω_2 of G_2 are the given seven-dimensional one std_7, and the adjoint representation $\mathrm{Lie}(G_2)$. We have

$$\mathrm{std}_7 \oplus \mathrm{Lie}(G_2) \cong \Lambda^2(\mathrm{std}_7).$$

Fix an element g in UG_2. Given its characteristic polynomial on std_7, we know its characteristic polynomial also on $\Lambda^2(\mathrm{std}_7)$, and so by long division on $\mathrm{Lie}(G_2)$ as well. Once we know the characteristic polynomial of g in both fundamental representations, we know it in all irreducible representations. So we know the trace of g in all irreducible representations. By Peter–Weyl the conjugacy class of g is determined by all these traces. □

(4.3). Also standard is the following lemma.

(4.4) Lemma. *The normalizer of* G_2 *in* $\mathrm{SO}(7)$ *is* G_2.

Proof. Every automorphism of G_2 is inner, because its Dynkin diagram has no automorphisms. So if g in $\mathrm{SO}(7)$ normalizes G_2, there exists h in G_2 such conjugation by h has the same effect as conjugation by g, i.e., hg^{-1} is an element of $\mathrm{SO}(7)$ which commutes with G_2. But G_2 acts irreducibly in its seven-dimensional representation, so hg^{-1} must be a scalar. The only scalar in $\mathrm{SO}(7)$ is 1. Hence $g = h$ lies in G_2. □

(4.5). Another useful fact is this.

(4.6) Lemma. *Over* $\mathbb{C}$, let G *be a Zariski closed irreducible subgroup of* $\mathrm{SO}(7)$. *Then* G *lies in* (*some* $\mathrm{SO}(7)$*-conjugate of*) G_2 *inside* $\mathrm{SO}(7)$ *if and only if* $\Lambda^3(\mathrm{std}_7)$ *contains a nonzero* G*-invariant vector, in which case the space of* G*-invariants in* $\Lambda^3(\mathrm{std}_7)$ *has dimension one.*

Proof. As pointed out by [Co-Wa, p. 449], this follows from the classification of trilinear forms in seven variables [Sch]. For a later treatment, see [Asch, Theorem 5, parts (2) and (5) on p. 196]. □

(4.7). We now turn our attention to the lisse sheaf $\mathscr{G}_7$. Let p be a prime other than 2 or 7. For any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, we have the lisse sheaves $\mathscr{F}_7$ and $\mathscr{G}_7$ on $\mathbb{A}^1/k$. We denote by

$$\rho : \pi_1(\mathbb{A}^1/k) \to \mathrm{SO}(7, \bar{\mathbb{Q}}_\ell)$$

the representation which "is" $\mathscr{G}_7$, and by G_{arith} the Zariski closure of its image. Recall that G_{geom} is the normal subgroup of G_{arith} defined as the Zariski closure of the image by ρ of $\pi_1^{\text{geom}}(\mathbb{A}^1/k)$.

(4.8) G_2 Inclusion Theorem. *Let p be a prime other than 2 or 7. For any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, the group G_{arith} for the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/k$ lies in G_2.*

Proof. We know (1.3) that $\mathscr{G}_7$ is geometrically irreducible, i.e., that G_{geom} and hence a fortiori G_{arith} is an irreducible subgroup of SO(7). So by the previous lemma, it suffices to show that $\Lambda^3(\mathscr{G}_7)$ as a representation of G_{arith} has a nonzero space of invariants. It is proven in [Ka-ESDE, pp. 321–324] that $(\mathscr{G}_7)^{\otimes 3}$ has a one-dimensional space of invariants under G_{geom}. We will refine the argument given there to show that this one-dimensional space lies in $\Lambda^3(\mathscr{G}_7)$, and that G_{arith} acts trivially on this space. Since we know that G_{geom} is semisimple, it is equivalent to show that the space of G_{geom} co-invariants in $\Lambda^3(\mathscr{G}_7)$ is one-dimensional, and that Frob_k acts trivially on it, i.e., we must show

$$\dim H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1) = 1,$$

$$\text{Frob}_k \text{ acts as 1 on } H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1).$$

Let us first explain the idea. We already know from [Ka-ESDE, pp. 321–324] that

$$\dim H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 3})(-1) = 1.$$

Therefore since $\Lambda^3(\mathscr{G}_7)$ is a direct summand of $(\mathscr{G}_7)^{\otimes 3}$, we have the inequality

$$\dim H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1) \leqslant 1.$$

By the Lefschetz trace formula, we have, for every finite extension E/k,

$$\begin{aligned}&\text{Trace}(\text{Frob}_E \mid H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1))\\ &= \text{Trace}(\text{Frob}_E \mid H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1))\\ &\quad + (1/\#E) \sum_{t \text{ in } E} \text{Trace}(\text{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7)).\end{aligned}$$

By Deligne [De-WeilII, 3.3.1], $H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1)$ is mixed of weight $\leqslant -1$, so we have

$$|\text{Trace}(\text{Frob}_E \mid H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1))| \leqslant \dim(H_c^1)/\text{Sqrt}(\#E).$$

Thus for variable finite extensions E/k, we have

$$\begin{aligned}&\mathrm{Trace}(\mathrm{Frob}_E \mid H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1))\\ &= (1/\#E) \sum_{t \text{ in } E} \mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7)) + O(1/\mathrm{Sqrt}(\#E)).\end{aligned}$$

We will show that for variable finite extensions E/k, we have

$$(1/\#E) \sum_{t \text{ in } E} \mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7)) = 1 + O(1/\mathrm{Sqrt}(\#E)).$$

Let us temporarily admit this. Then we have

$$\mathrm{Trace}(\mathrm{Frob}_E \mid H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1)) = 1 + O(1/\mathrm{Sqrt}(\#E)).$$

From this we first conclude that $H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1) \neq 0$. Since it has dimension at most one, we must have

$$\dim H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, \Lambda^3(\mathscr{G}_7))(-1) = 1.$$

Denote by A the scalar by which Frob_k acts on this one-dimensional space. For variable integers $n \geqslant 1$, we have

$$A^n = 1 + O(1/\mathrm{Sqrt}(\#k)^n).$$

Writing A as A^{n+1}/A^n for large n, we conclude that $A = 1$, as required.

We now turn to proving that

$$(1/\#E) \sum_{t \text{ in } E} \mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7)) = 1 + O(1/\mathrm{Sqrt}(\#E)).$$

The third standard symmetric function S_3 is given in Newton symmetric functions N_i by

$$6S_3 = (N_1)^3 + 2N_3 - 3N_1N_2.$$

Thus for each t in E we have the identity

$$\begin{aligned}&6\,\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7))\\ &= (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))^3 + 2\,\mathrm{Trace}((\mathrm{Frob}_{E,t})^3 \mid \mathscr{G}_7)\\ &\quad - 3\,\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7)\mathrm{Trace}((\mathrm{Frob}_{E,t})^2 \mid \mathscr{G}_7).\end{aligned}$$

If we denote by E_n/E the extension of E of degree n, then

$$\mathrm{Trace}((\mathrm{Frob}_{E,t})^n \mid \mathscr{G}_7) = \mathrm{Trace}(\mathrm{Frob}_{E_n,t} \mid \mathscr{G}_7).$$

So we have the identity

$$\begin{aligned} &6\,\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \Lambda^3(\mathscr{G}_7)) \\ &\quad = (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))^3 + 2\,\mathrm{Trace}(\mathrm{Frob}_{E_3,t} \mid \mathscr{G}_7) \\ &\qquad - 3\,\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7)\,\mathrm{Trace}(\mathrm{Frob}_{E_2,t} \mid \mathscr{G}_7). \end{aligned}$$

So it suffices to show the following three statements:

(1) $(1/\#E)\sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))^3 = 1 + O(1/\mathrm{Sqrt}(\#E))$,
(2) $(1/\#E)\sum_{t \text{ in } E} \mathrm{Trace}(\mathrm{Frob}_{E_3,t} \mid \mathscr{G}_7) = 1 + O(1/\mathrm{Sqrt}(\#E))$,
(3) $(1/\#E)\sum_{t \text{ in } E} \mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7)\,\mathrm{Trace}(\mathrm{Frob}_{E_2,t} \mid \mathscr{G}_7) = -1 + O(1/\mathrm{Sqrt}(\#E))$.

With the finite extension E/k fixed, let us write

$$A := -G(\psi_{-7,E}, \chi_{2,E})$$

for the quantity "A_7" of 1.3.4, relative to the field E. Then for any t in E, and any integer $n \geqslant 1$, we have

$$\begin{aligned} &\mathrm{Trace}(\mathrm{Frob}_{E_n,t} \mathscr{G}_7) \\ &\quad = (1/A^n)\left(- \sum_{x \text{ in } E_n} \psi_E(\mathrm{Trace}_{E_n/E}(x^7 + tx))\chi_{2,E}(\mathrm{Norm}_{E_n/E}(x)) \right), \end{aligned}$$

with the convention that $\chi_{2,E}(0) = 0$.

Thus the sum in (1) is

$$(1/\#E)(-1/A)^3 \sum_{t \text{ in } E} \sum_{x,y,z \text{ in } E} \psi_E(x^7 + y^7 + z^7 + t(x + y + z))\chi_{2,E}(xyz).$$

The sum in (2) is

$$(1/\#E)(-1/A^3) \sum_{t \text{ in } E} \sum_{x \text{ in } E_3} \psi_E(\mathrm{Trace}_{E_3/E}(x^7 + tx))\chi_{2,E}(\mathrm{Norm}_{E_3/E}(x)).$$

The sum in (3) is

$$(1/\#E)(-1/A)(-1/A^2) \sum_{t \text{ in } E} \sum_{x \text{ in } E,\ y \text{ in } E_2} \psi_E(x^7 + tx + \mathrm{Trace}_{E_2/E}(y^7 + ty))\chi_{2,E}(x\,\mathrm{Norm}_{E_2/E}(y)).$$

In each of the three sums, we interchange the order of summation. Because the quantity t runs over the ground field E, and $\mathrm{Trace}_{E_n/E}$ is E-linear, we can use the usual orthogonality relations for the nontrivial additive character ψ_E of E. We find

that the sum in (1) is

$$(-1/A)^3 \sum_{x,y,z \text{ in } E,\ x+y+z=0} \psi_E(x^7+y^7+z^7)\chi_{2,E}(xyz).$$

The sum in (2) is

$$(-1/A^3) \sum_{x \text{ in } E_3, \mathrm{Trace}_{E_3/E}(x)=0} \psi_E(\mathrm{Trace}_{E_3/E}(x^7))\chi_{2,E}(\mathrm{Norm}_{E_3/E}(x)).$$

The sum in (3) is

$$(-1/A)(-1/A^2) \sum_{x \text{ in } E,\ y \text{ in } E_2,\ x+\mathrm{Trace}_{E_2/E}(y)=0} \psi_E(x^7+\mathrm{Trace}_{E_2/E}(y^7))\chi_{2,E}(x\,\mathrm{Norm}_{E_2/E}(y)).$$

Thus what we must show is that (for (1))

$$\sum_{x,y,z \text{ in } E,\ x+y+z=0} \psi_E(x^7+y^7+z^7)\chi_{2,E}(xyz) = (-A)^3 + O(\#E),$$

(for (2))

$$\sum_{x \text{ in } E_3, \mathrm{Trace}_{E_3/E}(x)=0} \psi_E(\mathrm{Trace}_{E_3/E}(x^7))\chi_{2,E}(\mathrm{Norm}_{E_3/E}(x)) = (-A)^3 + O(\#E),$$

(for (3))

$$\sum_{x \text{ in } E,\ y \text{ in } E_2,\ x+\mathrm{Trace}_{E_2/E}(y)=0} \psi_E(x^7+\mathrm{Trace}_{E_2/E}(y^7))\chi_{2,E}(x\,\mathrm{Norm}_{E_2/E}(y)) = (-A)^3 + O(\#E).$$

The common feature of these last sums is that, in each, we have one of the three finite etale three-dimensional E-algebras B/E, and the sum is

$$\sum_{x \text{ in } B,\ \mathrm{Trace}_{B/E}(x)=0} \psi_E(\mathrm{Trace}_{B/E}(x^7))\chi_{2,E}(\mathrm{Norm}_{B/E}(x)).$$

Indeed, in the first case B is $E \times E \times E$, in the second case it is E_3, and in the third case it is $E \times E_2$. Denote by $B_{tr=0}$ the set of elements in B whose trace to E vanishes. We must show that

$$\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(\mathrm{Trace}_{B/E}(x^7))\chi_{2,E}(\mathrm{Norm}_{B/E}(x)) = (-A)^3 + O(\#E).$$

Denote by s_1, s_2, s_3 the polynomial functions on B which are the trace functions of the exterior powers of the left regular representation of B on itself. Thus for x in B we have

$$\det(T - \mathrm{Reg}(x)|B) = T^3 - s_1(x)T^2 + s_2(x)T - s_3(x).$$

In particular, we have

$$s_1(x) = \mathrm{Trace}_{B/E}(x), \quad s_3(x) = \mathrm{Norm}_{B/E}(x).$$

(4.9) Key Lemma. *Let E be a field, B/E a finite etale E-algebra of dimension three.*

(1) *For x in B, we have the identity*

$$s_1(x^7) - s_1(x)^7 = -7(s_1(x)s_2(x) - s_3(x))((s_1(x)^2 - s_2(x))^2 + s_1(x)s_3(x)).$$

(2) *For x in B with $\mathrm{Trace}_{B/E}(x) = 0$, we have the identity*

$$\mathrm{Trace}_{B/E}(x^7) = 7\,\mathrm{Norm}_{B/E}(x)s_2(x)^2 = 7s_3(x)s_2(x)^2.$$

Proof of Key Lemma. Assertion (2) is the special case of (1) when $s_1(x) = 0$. To prove assertion (1), we may extend scalars from E to its algebraic closure, and so reduce to the case where B is $E \times E \times E$. For an element (x, y, z) in $E \times E \times E$, with elementary symmetric functions s_i, $i = 1$ to 3, we must show that

$$x^7 + y^7 + z^7 - (x + y + z)^7 = -7(s_1s_2 - s_3)((s_1^2 - s_2)^2 + s_1s_3).$$

In terms of the characteristic polynomial

$$P(T) := T^3 - s_1T^2 + s_2T - s_3 = (T - x)(T - y)(T - z),$$

we have

$$s_1s_2 - s_3 = P(s_1) = (s_1 - x)(s_1 - y)(s_1 - z) = (y + z)(x + z)(x + y).$$

So the asserted identity is the following polynomial identity

$$x^7 + y^7 + z^7 - (x + y + z)^7$$
$$= -7(y + z)(x + z)(x + y)((x^2 + y^2 + z^2 + xy + xz + yz)^2 + (x + y + z)xyz),$$

whose unenlightening verification we leave to the reader. □

View B as the E-points of the affine B-scheme $\mathscr{B}$, whose R-valued points, for any E-algebra R, are given by $\mathscr{B}(R) := B \otimes_E R$. As an E-scheme, $\mathscr{B}$ is noncanonically $\mathbb{A}^3$.

Denote by $B_{\mathrm{tr}=0} \subset B$ the E-subspace of elements of trace zero, and $\mathscr{B}_{\mathrm{tr}=0}$ the corresponding closed subscheme of $\mathscr{B}$: for any E-algebra R,

$$\mathscr{B}_{\mathrm{tr}=0}(R) = B_{\mathrm{tr}=0} \otimes_E R = \mathrm{Ker}(\mathrm{Trace}_{B\otimes_E R/R} : B \otimes_E R \to R).$$

Thus $\mathscr{B}_{\mathrm{tr}=0}$ is noncanonically $\mathbb{A}^2$ as an E-scheme.

(4.10) Lemma. *Over the algebraic closure $\bar{E}$ of E, the polynomial function on $\mathscr{B}_{\mathrm{tr}=0}$ given by $s_2(x)^2 s_3(x)$ is homogeneous of degree seven, and not a seventh power.*

Proof. Immediate reduction to the case $E = \bar{E}$, when B is $E \times E \times E$, with coordinates (x, y, z). Then $B_{\mathrm{tr}=0}$ is the subspace $x + y + z = 0$, which we endow with coordinates x and y. Then $s_2^2 s_3$ is the function

$$(xy + x(-y-x) + y(-x-y))^2 xy(-x-y) = -(x^2 + xy + y^2)^2 xy(x+y).$$

This polynomial is visibly not a seventh power in the UFD $E[x, y]$, since it is divisible just once by the irreducible polynomial x. □

(4.11) Uniformity Lemma. *Given integers $n \geqslant 1$ and $d \geqslant 1$, there exists a constant $C(n, d)$ such that for any algebraically closed field k, for any prime ℓ invertible in k, and for any polynomial f in n variables of degree $\leqslant d$ over k, we have* $\dim H_c^{n-1}((f = 0 \text{ in } \mathbb{A}^n), \bar{\mathbb{Q}}_\ell) \leqslant C(n, d)$.

Proof. This is a special case of [Ka-Betti, Theorem 1 on p. 31 and Corollary, p. 34]. □

We can now complete the proof of the theorem. We must show that

$$\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(\mathrm{Trace}_{B/E}(x^7))\chi_{2,E}(\mathrm{Norm}_{B/E}(x)) = (-A)^3 + O(\#E).$$

In view of the identity above, the sum in question is

$$\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(7 s_3(x) s_2(x)^2)\chi_{2,E}(s_3(x)).$$

If x has $s_2(x)$ nonzero, we can put $s_2(x)^2$ inside the $\chi_{2,E}$, so the sum is

$$\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(7 s_3(x) s_2(x)^2)\chi_{2,E}(s_3(x) s_2(x)^2) + \sum_{x \text{ in } B_{\mathrm{tr}=0},\ s_2(x)=0} \chi_{2,E}(s_3(x)).$$

The second sum is trivially $O(\#E)$. Indeed, each summand in it is either 0 or ± 1, and there are at most $27\#E$ summands, one for each element x of B which has $s_1(x) = s_2(x) = 0$. Such elements are solutions in B of an equation $x^3 = \alpha$ for some α

(namely $s_3(x)$) in E. Fix α in E. As B is a product of at most 3 fields, in each of which $x^3=\alpha$ has at most three solutions, the equation $x^3=\alpha$ has at most 27 solutions in B.

So we must show that

$$\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(7s_3(x)s_2(x)^2)\chi_{2,E}(s_3(x)s_2(x)^2) = (-A)^3 + O(\#E).$$

For this, we argue as follows. Consider the function

$$f := s_3 s_2^2 : \mathscr{B}_{\mathrm{tr}=0} \to \mathbb{A}^1.$$

Then

$$\begin{aligned}&\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(7s_3(x)s_2(x)^2)\chi_{2,E}(s_3(x)s_2(x)^2)\\ &\quad = \sum_{\alpha \text{ in } E^\times} \psi_E(7\alpha)\chi_{2,E}(\alpha)\#\{x \text{ in } B_{\mathrm{tr}=0} \text{ with } f(x)=\alpha\}.\end{aligned}$$

Because f is homogeneous of degree seven, and not a seventh power, for each $\alpha\neq 0$ in $\bar{E}$, $f=\alpha$ is a smooth, geometrically irreducible curve. So we have $R^2 f_!\bar{\mathbb{Q}}_\ell \mid \mathbb{G}_m \cong \bar{\mathbb{Q}}_\ell(-1)$, and $R^1 f_!\bar{\mathbb{Q}}_\ell \mid \mathbb{G}_m$ becomes constant after pullback by the seventh power map [7]: $\mathbb{G}_m \to \mathbb{G}_m$. In particular, $R^1 f_!\bar{\mathbb{Q}}_\ell \mid \mathbb{G}_m$ is lisse, and tamely ramified at both 0 and ∞, cf. [Ka-ESDE, pp. 322–323]. By the Lefschetz Trace formula, we have

$$\begin{aligned}&\sum_{\alpha \text{ in } E^\times} \psi_E(7\alpha)\chi_{2,E}(\alpha)\#\{x \text{ in } B_{\mathrm{tr}=0} \text{ with } f(x)=\alpha\}\\ &\quad = \sum_{\alpha \text{ in } E^\times} \psi_E(7\alpha)\chi_{2,E}(\alpha)(q - \mathrm{Trace}(\mathrm{Frob}_{E,\alpha} \mid R^1 f_!\bar{\mathbb{Q}}_\ell))\\ &\quad = qG(\psi_{7,E},\chi_{2,E})\\ &\qquad - \sum_{\alpha \text{ in } E^\times} \psi_E(7\alpha)\chi_{2,E}(\alpha)\,\mathrm{Trace}(\mathrm{Frob}_{E,\alpha} \mid R^1 f_!\bar{\mathbb{Q}}_\ell)\\ &\quad = -q\chi_{2,E}(-1)(-G(\psi_{-7,E},\chi_{2,E}))\\ &\qquad - \sum_{\alpha \text{ in } E^\times} \mathrm{Trace}(\mathrm{Frob}_{E,\alpha} \mid \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_!\bar{\mathbb{Q}}_\ell)\\ &\quad = -q\chi_{2,E}(-1)A\\ &\qquad - \mathrm{Trace}(\mathrm{Frob}_E \mid H_c^2(\mathbb{G}_m \otimes_E \bar{E}, \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_!\bar{\mathbb{Q}}_\ell))\\ &\qquad + \mathrm{Trace}(\mathrm{Frob}_E \mid H_c^1(\mathbb{G}_m \otimes_E \bar{E}, \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_!\bar{\mathbb{Q}}_\ell)).\end{aligned}$$

As noted above, $R^1 f_!\bar{\mathbb{Q}}_\ell \mid \mathbb{G}_m$ is lisse, and tamely ramified at both 0 and ∞. So the lisse sheaf $\mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_!\bar{\mathbb{Q}}_\ell$ on $\mathbb{G}_m$ is totally wild at ∞ (and tame at 0).

Therefore we have

$$H_c^2(\mathbb{G}_m \otimes_E \bar{E}, \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_! \bar{\mathbb{Q}}_\ell) = 0.$$

The group $H_c^1(\mathbb{G}_m \otimes_E \bar{E}, \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_! \bar{\mathbb{Q}}_\ell)$ is mixed of weight $\leqslant 2$, and its dimension is

$$\begin{aligned} &-\chi_c(\mathbb{G}_m \otimes_E \bar{E}, \mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_! \bar{\mathbb{Q}}_\ell) \\ &= \mathrm{Swan}_\infty(\mathscr{L}_{\psi_{7,E}} \otimes \mathscr{L}_{\chi_{2,E}} \otimes R^1 f_! \bar{\mathbb{Q}}_\ell) \\ &= \mathrm{rank}(R^1 f_! \bar{\mathbb{Q}}_\ell \mid \mathbb{G}_m) \leqslant C(2,7), \end{aligned}$$

for $C(2,7)$ the constant of the Uniformity Lemma above.

Thus we have

$$\begin{aligned} &\sum_{x \text{ in } B_{\mathrm{tr}=0}} \psi_E(7 s_3(x) s_2(x)^2) \chi_{2,E}(s_3(x) s_2(x)^2) \\ &= -q\chi_{2,E}(-1)A + O(\#E). \end{aligned}$$

But we have

$$A^2 = q\chi_{2,E}(-1),$$

cf. 1.2.3. This concludes the proof of the G_2 Inclusion Theorem. □

(4.12) G_2 Theorem ([Ka-ESDE, 9.1.1]). *Let p be a prime which is either* 5, 11, *or a prime $p > 15$. For any finite field k of characteristic p, for any prime $\ell \neq p$, and for any choice of nontrivial additive character ψ of k, the lisse sheaf $\mathscr{F}_7$ has*

$$G_{\mathrm{geom}} = G_2,$$

and the lisse sheaf $\mathscr{G}_7$ has

$$G_{\mathrm{geom}} = G_{\mathrm{arith}} = G_2.$$

Proof. We first note that the two assertions are equivalent. Indeed, since $\mathscr{F}_7$ and $\mathscr{G}_7$ have the same G_{geom}, the second assertion implies the first. Since G_{arith} for $\mathscr{G}_7$ lies in G_2 by Theorem (4.8), for $\mathscr{G}_7$ we have inclusions $G_{\mathrm{geom}} \subset G_{\mathrm{arith}} \subset G_2$. So the first assertion implies the second. We will prove the first.

For $p > 15$, this is proven in [Ka-ESDE, 9.1.1]. In fact, a slight modification of the argument given there divides into two parts. One first uses the hypothesis $p > 15$ to insure, via [Ka-MG, Proposition 5], that $\mathscr{F}_7$ is Lie-irreducible. One then shows, via Gabber's theorem on prime-dimensional representations [Ka-ESDE, 1.6], that in any characteristic $p \neq 2$, $p \neq 7$ for which $\mathscr{F}_7$ is Lie irreducible, G_{geom}^0 is either SO(7) or G_2 or the image PSL(2) of SL(2) in $\mathrm{Sym}^6(\mathrm{std}_2)$. Since G_{geom} lies in G_2 by the G_2 Inclusion Theorem (4.8), either G_{geom} is G_2, or G_{geom}^0 is the image PSL(2) of SL(2) in

$\mathrm{Sym}^6(\mathrm{std}_2)$, in which case G_{geom} lies in the normalizer in G_2 of this PSL(2). But PSL(2) is its own normalizer in G_2, indeed it is its own normalizer in SO(7) (because every automorphism of PSL(2) is inner, PSL(2) is an irreducible subgroup of SO(7), and SO(7) contains no nontrivial scalars). So either G_{geom} is G_2 or it is PSL(2). The PSL(2) case is ruled out just as in the proof of Theorem (3.7).

It remains to show that for $p = 5$ or 11, $\mathscr{F}_7$ is Lie-irreducible. By Lemma (3.4), we may take for k the prime field $\mathbb{F}_p$. By Lemma (3.5), if $\mathscr{F}_7$ is not Lie-irreducible, then it has finite G_{geom}, and a power of every $\mathrm{Frob}_{E,t} \mid \mathscr{F}_7$ is scalar. Suppose that G_{geom} is finite. Because $\mathscr{G}_7 := \mathscr{F}_7 \otimes (-G(\psi_{-7}, \chi_2))^{-\deg}$ has trivial determinant, every eigenvalue of $\mathrm{Frob}_{E,t} \mid \mathscr{F}_7$ will be of the form

$$(\text{a root of unity})(-G(\psi_{-7,E}, \chi_{2,E}))$$

$$= (\text{a root of unity})(\#E)^{1/2}.$$

Consequently, for every finite extension E of $\mathbb{F}_p$, and for every t in E, $\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7)$ is divisible by $(\#E)^{1/2}$ as an algebraic integer.

But the sum

$$\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7) = -\sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(x^7 + tx)$$

lies in the ring $\mathbb{Z}[\zeta_p]$, and the field $\mathbb{Q}(\zeta_p)$ has a unique p-adic valuation $\mathscr{P}$. If we normalize the valuation by

$$\mathrm{ord}_{\mathscr{P},E}(\#E) = 1,$$

then the finiteness of G_{geom} for $\mathscr{F}_7$ implies that for every (E, t) as above we have

$$\mathrm{ord}_{\mathscr{P},E}(\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7)) \geqslant 1/2.$$

In the case $p = 11$, one sees by a direct calculation that

$$\mathrm{ord}_{\mathscr{P},\mathbb{F}_{11}}(\mathrm{Trace}(\mathrm{Frob}_{\mathbb{F}_{11},1} \mid \mathscr{F}_7)) = 3/10.$$

In the case $p = 5$, one sees by a direct calculation that

$$\mathrm{ord}_{\mathscr{P},\mathbb{F}_{25}}(\mathrm{Trace}(\mathrm{Frob}_{\mathbb{F}_{25},1} \mid \mathscr{F}_7)) = 1/4.$$

In neither case do we have divisibility by $(\#E)^{1/2}$ in $\mathbb{Z}_p[\zeta_p]$, much less in the ring of algebraic integers. Therefore G_{geom} is not finite in either case, and hence $\mathscr{F}_7$ is Lie-irreducible in both characteristics 5 and 11, as required.

Let us explain briefly how to do such calculations. In $\mathbb{Z}_p[\zeta_p]$, the quantity $\pi := \zeta_p - 1$ is a uniformizing parameter, the residue field is $\mathbb{F}_p$, $\mathrm{ord}_{\mathscr{P},\mathbb{F}_p}(\pi) = 1/(p-1)$, and

$$\mathbb{Z}_p[\zeta_p]/(p) = \mathbb{Z}_p[\zeta_p]/(\pi^{p-1}) \cong \mathbb{F}_p[\pi]/(\pi^{p-1}).$$

For $\mathrm{ord}_\pi := (p-1)\mathrm{ord}_{\mathscr{P},\mathbb{F}_p}$ (i.e., $\mathrm{ord}_\pi(\pi) = 1$), we are to show that

$$\mathrm{ord}_\pi(\mathrm{Trace}(\mathrm{Frob}_{\mathbb{F}_{11},1} \mid \mathscr{F}_7)) = 3, \quad \text{for } p = 11,$$

$$\mathrm{ord}_\pi(\mathrm{Trace}(\mathrm{Frob}_{\mathbb{F}_{25},1} \mid \mathscr{F}_7)) = 2, \quad \text{for } p = 5.$$

Now for any element f in $\mathbb{Z}_p[\zeta_p]$, with image mod p

$$\sum_{i=0 \text{ to } p-2} a_i \pi^i, \text{ coefficients } a_i \text{ in } \mathbb{F}_p$$

in the ring $\mathbb{F}_p[\pi]/(\pi^{p-1})$, we have

$$\mathrm{ord}_\pi(f) \geqslant p-1 \text{ if and only if all } a_i = 0,$$

and, if some $a_i \neq 0$, then

$$\mathrm{ord}_\pi(f) = \text{Minimum } i \text{ such that } a_i \neq 0.$$

So the problem is to calculate the image in $\mathbb{Z}_p[\zeta_p]/(\pi^{p-1}) \cong \mathbb{F}_p[\pi]/(\pi^{p-1})$ of the sum

$$\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7) = -\sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(x^7 + tx).$$

We may assume that $\psi(1) = \zeta_p = 1 + \pi$. Then

$$\begin{aligned}
&\sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(x^7 + tx) \\
&= \sum_{x \text{ in } E^\times} \chi_2(N_{E/\mathbb{F}_p}(x))\psi(\mathrm{Trace}_{E/\mathbb{F}_p}(x^7 + tx)) \\
&= \sum_{x \text{ in } E^\times} \chi_2(N_{E/\mathbb{F}_p}(x))(1+\pi)^{(\mathrm{Trace}_{E/\mathbb{F}_p}(x^7+tx))} \\
&\equiv \sum_{x \text{ in } E^\times} x^{(\#E-1)/2} \sum_{i=0 \text{ to } p-2} \mathrm{Binom}(\mathrm{Trace}_{E/\mathbb{F}_p}(x^7 + tx), i)\pi^i,
\end{aligned}$$

in $\mathbb{Z}_p[\zeta_p]/(\pi^{p-1}) \cong \mathbb{F}_p[\pi]/(\pi^{p-1})$. We have written $\mathrm{Binom}(x,i)$ for the ith binomial coefficient as a function of its "numerator":

$$\begin{aligned}
\mathrm{Binom}(x,i) &:= 1, i = 0, \\
&:= x(x-1)\ldots(x-(i-1))/i!, \quad \text{for } 1 \leqslant i \leqslant p-2.
\end{aligned}$$

Thus the coefficients a_i in the expansion of $-\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7)$ are the quantities in $\mathbb{F}_p$ given by

$$a_i = \sum_{x \text{ in } E^\times} x^{(\#E-1)/2}\, \mathrm{Binom}(\mathrm{Trace}_{E/\mathbb{F}_p}(x^7 + tx), i).$$

But the power sums over $E^\times$ are given by

$$\sum_{x \text{ in } E^\times} x^k = -1 \text{ in } \mathbb{F}_p, \quad \text{if } k \equiv 0 \bmod (\#E-1),$$
$$= 0, \text{ otherwise.}$$

Thus $a_0 = 0$. To compute a_i for $1 \leqslant i \leqslant p-2$ we first write $\#E$ as p^d, second we expand

$$\text{Trace}_{E/\mathbb{F}_p}(x^7 + tx) = \sum_{k=0 \text{ to } d-1} (x^{7p^k} + t^{p^k} x^{p^k})$$

as a polynomial in x with coefficients in $\mathbb{F}_p[t]$, third we expand $\text{Binom}(\text{Trace}_{E/\mathbb{F}_p}(x^7 + tx), i)$ as a polynomial in x with coefficients in $\mathbb{F}_p[t]$, and finally we sum up the coefficients of all monomials of the form x^k, with k of the form

$$(\#E-1)/2 + r(\#E-1),$$

for $r = 0, 1, 2, \ldots$. We leave to the reader the verification that this calculation leads to the asserted conclusions

$$\text{ord}_\pi(\text{Trace}(\text{Frob}_{\mathbb{F}_{11},1} \mid \mathscr{F}_7)) = 3, \quad \text{for } p = 11,$$

$$\text{ord}_\pi(\text{Trace}(\text{Frob}_{\mathbb{F}_{25},1} \mid \mathscr{F}_7)) = 2, \quad \text{for } p = 5. \qquad \square$$

(4.13) Theorem. *For any finite field k of characteristic* 13, *for any prime $\ell \neq 13$, and for any choice of nontrivial additive character ψ of k, consider the lisse sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/k$ and its corresponding representation $\rho : \pi_1(\mathbb{A}^1/k) \to \text{SO}(7)$. Denote by G_{arith} the Zariski closure in* SO(7) *of $\rho(\pi_1(\mathbb{A}^1/k))$. Then*

$$G_{\text{arith}} = G_{\text{geom}} = \textit{the finite subgroup } \text{PSL}(2, \mathbb{F}_{13}) \textit{ of } G_2,$$

where $\text{PSL}(2, \mathbb{F}_{13})$ *is viewed inside G_2 by one of its two seven-dimensional irreducible representations* (*both of which have image in G_2*, cf. [Co-Wa]).

Proof. We first treat the case when k is the prime field $\mathbb{F}_{13}$, and ψ is (the image under ι of) the $\mathbb{C}$-valued additive character $x \mapsto \exp(2\pi i x/13)$. Because

$$p = 13 > 7 = \text{rank}(\mathscr{G}_7),$$

Lemma (3.5) tells us that either $\mathscr{G}_7$ is Lie-irreducible, or its G_{geom} is a finite primitive irreducible subgroup of SO(7), and indeed of G_2, by the G_2 Inclusion Theorem (4.8), As explained in the proof of Theorem (4.12) above, if $\mathscr{G}_7$ is Lie-irreducible, then its G_{geom} is G_2. If G_{geom} is G_2, then G_{arith} lies in the normalizer of G_2 inside SO(7), and

this normalizer is just G_2 itself, cf. Lemma (4.4). So if G_{geom} is not finite, we have

$$G_{\text{geom}} = G_{\text{arith}} = G_2.$$

If G_{geom} is finite, then G_{arith} is finite, by [Ka-ESDE, 8.14.3.1], and G_{geom} is a normal subgroup of G_{arith}. Therefore, if G_{geom} is finite, then G_{arith} is itself a finite primitive irreducible subgroup of G_2. Every $\rho(\text{Frob}_{E,t})$ then lies in G_{arith}, and, by Chebotarev, every element of G_{arith} is of this form. But

$$\begin{aligned}\text{Trace}(\rho(\text{Frob}_{E,t})) &\coloneqq \text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7)\\ &\coloneqq (1/G(\psi_{-7,E}, \chi_{2,E})) \sum_{x \text{ in } E^\times} \chi_{2,E}(x)\psi_E(x^7 + tx)\end{aligned}$$

visibly has values in the field $\mathbb{Q}(\zeta_{13})$ of 13th roots of unity. We claim that $\text{Trace}(\rho(\text{Frob}_{\mathbb{F}_{13},1}))$ does not lie in $\mathbb{Q}$. Indeed, using the fact that for x nonzero in $\mathbb{F}_{13}$, x is a square if and only if $x^6 = 1$ in $\mathbb{F}_{13}$, we readily compute

$$\begin{aligned}&\text{Trace}(\rho(\text{Frob}_{\mathbb{F}_{13},1}))\\ &= (-1/\text{Sqrt}(13)) \sum_{x \text{ in } \mathbb{F}_{13}^\times} \chi_2(x)\psi(x^7 + x)\\ &= (-1/\text{Sqrt}(13)) \sum_{x \text{ in } \mathbb{F}_{13}^\times} \chi_2(x)\psi((x^6 + 1)x)\\ &= (-1/\text{Sqrt}(13)) \sum_{x \text{ in } \mathbb{F}_{13}^\times, x \text{ a square}} \psi(2x)\\ &\quad + (-1/\text{Sqrt}(13)) \sum_{x \text{ in } \mathbb{F}_{13}^\times, x \text{ nonsquare}} (-1)\psi(0)\\ &= (-1/\text{Sqrt}(13))(1/2) \sum_{u \text{ in } \mathbb{F}_{13}^\times} \psi(2u^2) + 6/\text{Sqrt}(13)\\ &= (-1/2\,\text{Sqrt}(13))\left(-1 + \sum_{u \text{ in } \mathbb{F}_{13}} \psi(2u^2)\right) + 12/2\,\text{Sqrt}(13)\\ &= (-1/2\,\text{Sqrt}(13))(-1 + G(\psi_2, \chi_2)) + 12/2\,\text{Sqrt}(13)\\ &= (-1/2\,\text{Sqrt}(13))(-1 + \chi_2(2)G(\psi, \chi_2)) + 12/2\,\text{Sqrt}(13)\\ &= (-1/2\,\text{Sqrt}(13))(-1 - G(\psi, \chi_2)) + 12/2\,\text{Sqrt}(13)\\ &= (1/2\,\text{Sqrt}(13))(13 + \text{Sqrt}(13))\\ &= (1 + \text{Sqrt}(13))/2.\end{aligned}$$

Thus if G_{geom} is not G_2, then G_{arith} is a finite primitive irreducible subgroup of G_2, the character of whose given seven-dimensional representation has values in the field $\mathbb{Q}(\zeta_{13})$, and not all of the character values lie in $\mathbb{Q}$.

On the other hand, the finite primitive irreducible subgroups G of G_2 have been classified by Cohen–Wales [Co-Wa]. The list of possibilities, in Atlas notation, is

$$L_2(13) \text{ (i.e. } \mathrm{PSL}(2,\mathbb{F}_{13}))$$
$$L_2(8) \text{ (i.e. } \mathrm{PSL}(2,\mathbb{F}_8))$$
$$L_2(7).2 \text{ (i.e., } \mathrm{PGL}(2,\mathbb{F}_7))$$
$$U_3(3) \text{ or } U_3(3).2 \text{ (i.e. } U_3(3) \text{ or } G_2(2))$$

Of these, only the first has a seven-dimensional irreducible representation whose character takes values, some irrational, in the field $\mathbb{Q}(\zeta_{13})$. [In fact, $L_2(13)$ has two seven-dimensional irreducible representations, and both have this property.] Indeed, all seven-dimensional irreducible representations of the other groups have character values lying in the following fields:

$$L_2(8) \quad \mathbb{Q}(\zeta_9)$$
$$L_2(7).2 \quad \mathbb{Q}$$
$$U_3(3) \quad \mathbb{Q}(\zeta_4)$$
$$U_3(3).2 \quad \mathbb{Q}.$$

But the intersection of $\mathbb{Q}(\zeta_{13})$ with any of the fields $\mathbb{Q}$, $\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\zeta_9)$ is $\mathbb{Q}$ itself. So if G_{geom} is not G_2, then G_{arith} is the finite group $\mathrm{PSL}(2,\mathbb{F}_{13})$. Conveniently, this group is simple. As G_{geom} is an irreducible (and hence nontrivial) normal subgroup of G_{arith}, we see that if G_{arith} is $\mathrm{PSL}(2,\mathbb{F}_{13})$, then $G_{\text{geom}} = G_{\text{arith}} = \mathrm{PSL}(2,\mathbb{F}_{13})$.

To summarize our situation so far: with $k = \mathbb{F}_{13}$ and ψ the image under ι of $x \mapsto \exp(2\pi i x/13)$, G_{arith} and G_{geom} for the lisse sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/k$ are on a very short list:

$$\text{either } G_{\text{arith}} = G_{\text{geom}} = G_2,$$
$$\text{or } \quad G_{\text{arith}} = G_{\text{geom}} = \mathrm{PSL}(2,\mathbb{F}_{13}).$$

We now explain how to rule out the G_2 possibility. We do this through a consideration of fourth moments, cf. [Ka-LFM, 112–113]. For G_2 in its seven-dimensional representation std_7, we have

$$M_4(G_2, \mathrm{std}_7) = 4.$$

We focus on M_4 because for $\mathrm{PSL}(2,\mathbb{F}_{13})$, in either of its irreducible seven-dimensional representations, we have (using the ATLAS [CCNPW-Atlas] character tables available in GAP [GAP])

$$M_4(\mathrm{PSL}(2,\mathbb{F}_{13}), \mathrm{std}_7) = 5.$$

On the other hand, we have

$$M_4(G_{\text{geom}}, \mathscr{G}_7) = \dim H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})\,(-1).$$

Suppose now that $G_{\text{arith}} = G_{\text{geom}} = G_2$. Then

$$H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})\,(-1)$$

is four-dimensional, and Frob_k acts on it as the identity. Thus for any finite extension field E/k, we have

$$\text{Trace}(\text{Frob}_E, H_c^2(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})(-1)) = 4.$$

The group $H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})\,(-1)$ is mixed of weight $\leqslant -1$. Using the Euler–Poincare formula, we see that

$$\begin{aligned}\dim H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})\,(-1) &= 4 - \chi(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4}) \\ &= 4 + \text{Swan}_\infty((\mathscr{G}_7)^{\otimes 4}) - \text{rank}((\mathscr{G}_7)^{\otimes 4}).\end{aligned}$$

Because $\mathscr{G}_7$ has all ∞-slopes $\leqslant 7/6$, we have

$$\text{Swan}_\infty((\mathscr{G}_7)^{\otimes 4}) \leqslant (7/6)\,\text{rank}((\mathscr{G}_7)^{\otimes 4}).$$

Thus we have

$$\begin{aligned}\dim H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})(-1) &\leqslant 4 + (1/6)\,\text{rank}((\mathscr{G}_7)^{\otimes 4}) \\ &\leqslant 4 + 7^4/6 = 4 + 2401/6 = 404.166\ldots.\end{aligned}$$

Thus we have

$$\dim H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})(-1) \leqslant 404.$$

From the Lefschetz Trace formula, we now find that for any finite extension E/k, we have the estimate

$$\begin{aligned}&|4 - (1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7))^4| \\ &\quad = |\text{Trace}(\text{Frob}_E \mid H_c^1(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 4})(-1)| \leqslant 404/\text{Sqrt}(\#E),\end{aligned}$$

and consequently the upper bound

$$|(1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7))^4| \leqslant 4 + 404/\text{Sqrt}(\#E).$$

Since $\mathscr{F}_7$ is $\mathscr{G}_7 \otimes (-G(\psi_{-7}, \chi_2))^{\deg}$, we can rewrite this as

$$|(1/\#E)^3 \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7))^4| \leqslant 4 + 404/\mathrm{Sqrt}(\#E).$$

Taking for E the field of cardinality 13^5, we have $\mathrm{Sqrt}(\#E) = 609.338\ldots$, so for this field, we find the estimate

$$|(1/\#E)^3 \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7))^4| \leqslant 4.6631.$$

But machine calculation shows that for this field, we have

$$(1/\#E)^3 \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{F}_7))^4 = 4.9992\ldots\ .$$

This rules out the G_2 possibility, and so concludes the proof that for $(\mathbb{F}_{13}, x \mapsto \exp(2\pi i x/13))$, any $\ell \neq 13$ and any $\iota : \bar{\mathbb{Q}}_\ell \subset \mathbb{C}$, $\mathscr{G}_7$ has

$$G_{\mathrm{arith}} = G_{\mathrm{geom}} = \mathrm{PSL}(2, \mathbb{F}_{13}).$$

Once we have treated that case, we argue as follows. For any finite extension k of $\mathbb{F}_{13}$, any $\ell \neq 13$ and any nontrivial additive character ψ of k, $\mathscr{G}_7$ has the same G_{geom}, namely $\mathrm{PSL}(2, \mathbb{F}_{13})$, and its G_{arith} is a finite (by [Ka-ESDE, 8.14.3.1]) group inside G_2 (by (4.8)) which contains G_{geom} as a normal subgroup. Since G_{geom} is a finite primitive irreducible subgroup of G_2, a fortiori G_{arith} is itself a finite primitive irreducible subgroup of G_2. Every element of G_{arith} has trace in the field $\mathbb{Q}(\zeta_{13})$, and already $G_{\mathrm{geom}} = \mathrm{PSL}(2, \mathbb{F}_{13})$ contains elements whose trace does not lie in $\mathbb{Q}$. So by the previous classification argument, we conclude that $G_{\mathrm{arith}} = \mathrm{PSL}(2, \mathbb{F}_{13})$. □

(4.14) Theorem. *For k the prime field $\mathbb{F}_3$ of characteristic 3, for any prime $\ell \neq 3$, and for any choice of nontrivial additive character ψ of k, consider the lisse sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/k$ and its corresponding representation $\rho : \pi_1(\mathbb{A}^1/k) \to \mathrm{SO}(7)$. Denote by G_{arith} the Zariski closure in $\mathrm{SO}(7)$ of $\rho(\pi_1(\mathbb{A}^1/k))$. Then*

$$G_{\mathrm{arith}} = \textit{the finite subgroup } G_2(2) = U_3(3).2 \textit{ of } G_2,$$

$$G_{\mathrm{geom}} = \textit{the finite subgroup } U_3(3) \textit{ of } G_2.$$

Proof. Our first task is to prove that G_{geom} is finite. By Lemma (3.5), either G_{geom} is G_2, or it is a finite irreducible subgroup of G_2 (thanks to 4.8). We rule out the G_2 possibility by a consideration of sixth moments. For G_2 in its seven-dimensional representation std_7, simpLie [MPR] tells us that

$$M_6(G_2, \mathrm{std}_7) = 35.$$

[We focus on M_6 because for $U_3(3)$ in the unique seven-dimensional representation std_7 which lands it in G_2, we have (using the ATLAS [CCNPW-Atlas] character tables in GAP [GAP])

$$M_6(U_3(3), \mathrm{std}_7) = 41,$$

and this is the lowest moment that distinguishes $U_3(3)$ from G_2 itself.]

If G_{geom} is G_2, then, exactly as explained in the proof of Theorem (4.13) above, we have denoting by $[x]$ the integral part (floor) of the real number x,

$$\dim H^1_c(\mathbb{A}^1 \otimes_k \bar{k}, (\mathscr{G}_7)^{\otimes 6})(-1)$$

$$\leqslant [35 + (1/6)7^6] = [19643.1666...] = 19643,$$

and hence we have the estimate, for any finite extension $E/\mathbb{F}_3$,

$$|(1/\#E) \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))^6| \leqslant 35 + 19643/\mathrm{Sqrt}(\#E).$$

Taking E to be the field of 3^{16} elements, the error term is

$$19643/\mathrm{Sqrt}(\#E) = 19643/3^8 = 2.9939\ldots < 3.$$

So if G_{geom} is G_2, we have

$$|(1/\#E) \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))6| < 38,$$

for E the field of 3^{16} elements. But machine calculation, for which I am indebted to Chris Hall, shows that as t varies over this E, the values assumed by $\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7)$ and their frequencies are given by the following table:

Value	How many times assumed
−2	398763
−1	13899820
0	19474298
1	4782969
2	3586680
3	897080
7	7111.

Thus we find

$$(1/\#E) \sum_{t \text{ in } E} (\mathrm{Trace}(\mathrm{Frob}_{E,t} \mid \mathscr{G}_7))^6 = 1764324500/3^{16} = 40.98\ldots\ .$$

Therefore G_{geom} is not G_2, and hence is a finite irreducible subgroup of G_2. Then G_{arith} is also finite, so G_{arith} is itself a finite irreducible subgroup of G_2.

We now show that G_{geom} is a primitive irreducible subgroup of G_2 (i.e., primitive as a subgroup of GL(7)). Suppose not. By Cohen–Wales [Co-Wa, p. 448], an imprimitive irreducible finite subgroup of G_2 is either $L_2(7) \cong L_3(2) = \mathrm{GL}(3, \mathbb{F}_2)$, or a possibly nonsplit extension of a three-dimensional $\mathbb{F}_2$-space by some subgroup of $L_3(2)$. So we have a group homomorphism

$$G_{\text{geom}} \to L_2(7),$$

which is either injective, or whose kernel is a group of order prime to $p = 3$. This leads to a contradiction, as follows. The group $L_2(7)$ has two irreducible three dimensional representations, both of which are necessarily faithful (because $L_2(7)$ is a simple group). Pick one, say Λ, and consider the lisse sheaf $\mathscr{G}_7(\Lambda)$ of rank 3 on $\mathbb{A}^1/\bar{\mathbb{F}}_3$ corresponding to the composite homomorphism

$$\pi_1 \mathrm{geom}(\mathbb{A}^1/\mathbb{F}_3) \xrightarrow{\rho} G_{\text{geom}} \xrightarrow{\Lambda} \mathrm{GL}(3).$$

By [Ka-ESDE, 7.2.4], $\mathscr{G}_7(\Lambda)$ has the same highest ∞-slope as $\mathscr{G}_7$, namely $7/6$. But any ∞-slope occurs with multiplicity some multiple of its denominator, so an ∞-slope $7/6$ cannot occur in any lisse sheaf on $\mathbb{A}^1/\bar{\mathbb{F}}_3$ of rank less than six. Therefore G_{geom} is primitive.

Since G_{geom} is primitive, a fortiori G_{arith} is primitive. Already over the field of 3^4 elements, direct calculation shows that both ± 2 occur as traces of Frobenius elements. Of the primitive irreducible subgroups of G_2 [Co-Wa, Theorem p. 449], namely $L_2(13), L_2(8), L_2(7).2, U_3(3)$ and $U_3(3).2$, only the last two contain both elements of trace 2 and elements of trace -2 in a seven-dimensional representation which lands them in G_2. Therefore G_{arith} is either $U_3(3)$ or $U_3(3).2$. Now $U_3(3)$ is a simple group, and it is the only nontrivial proper normal subgroup of $U_3(3).2$. So we have either

$$G_{\text{geom}} = G_{\text{arith}} = U_3(3).2,$$

or

$$G_{\text{geom}} = G_{\text{arith}} = U_3(3),$$

or

$$G_{\text{geom}} = U_3(3), \quad G_{\text{arith}} = U_3(3).2.$$

We first show that G_{geom} cannot be $U_3(3).2$. Indeed, we have (using the ATLAS [CCNPW-Atlas] character tables available in GAP [GAP]) $\mathrm{M}_6(U_3(3).2, \mathrm{std}_7) = 36$, and the calculation over the field of 3^{16} elements which ruled out G_2 also rules out this possibility. Thus if G_{geom} is primitive, it is $U_3(3)$. Supposing this to be the case,

we next show $G_{\text{arith}} \neq G_{\text{geom}}$. For if not, then we would have

$$G_{\text{geom}} = G_{\text{arith}} = U_3(3).$$

In this case, we would have, for any finite extension $E/\mathbb{F}_3$, the estimate

$$|M_6(U_3(3), \text{std}_7) - (1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7))^6|$$
$$\leqslant [41 + (1/6)7^6]/\text{Sqrt}(\#E) = 19649/\text{Sqrt}(\#E).$$

Taking for E the field of 3^{15} elements, the error term is

$$19649/3^{7.5} = 5.187.... < 6,$$

and hence for this field we would have

$$(1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7))^6 > 35.$$

But machine calculation, for which I am indebted to Chris Hall, shows that as t varies over this E, the values assumed by $\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7)$ and their frequencies are given by the following table:

Value	How many times assumed
−1	5380840
0	4782969
1	3587227
3	597871

Thus we find

$$(1/\#E) \sum_{t \text{ in } E} (\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7))^6 = 444816026/3^{15} = 30.999\ldots\ .$$

Therefore we conclude that

$$G_{\text{geom}} = U_3(3), \quad G_{\text{arith}} = U_3(3).2. \qquad \square$$

(4.15) Corollary. *Let k be a finite field of characteristic 3, ℓ any prime $\ell \neq 3$, and ψ a nontrivial additive character ψ of k. Consider the lisse sheaf $\mathscr{G}_7 = \mathscr{G}_7(k, \psi)$ on $\mathbb{A}^1/k$. Then its G_{geom} and G_{arith} are given by the following recipe.*

(1) *If* $\deg(k/\mathbb{F}_3)$ *is odd, then*

$$G_{\text{arith}} = U_3(3).2,$$

$$G_{\text{geom}} = U_3(3).$$

(2) *If* $\deg(k/\mathbb{F}_3)$ *is even, then*

$$G_{\text{geom}} = G_{\text{arith}} = U_3(3).$$

Proof. First consider the case when ψ is obtained by composition with the trace from a nontrivial additive character of the prime field $\mathbb{F}_3$. Then $\mathscr{G}_7(k,\psi)$ on $\mathbb{A}^1/k$ is the pullback of the lisse sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/\mathbb{F}_3$ considered in the previous theorem, for which G_{geom} is $U_3(3)$, of index two in $G_{\text{arith}} = U_3(3).2$. So the assertion is obvious in this case.

In the general case, the nontrivial additive character is of the form ψ_α, with ψ as in the case above, and α some element of k^x. Consider first the case in which α is a seventh power in k^x, i.e., $\alpha = \beta^7$ for some β in k^x. We claim that there exists an isomorphism of lisse sheave on $\mathbb{A}^1/k$,

$$\mathscr{G}_7(\psi_{\beta^7},k) \cong [t \mapsto \beta^6 t]^* \mathscr{G}_7(\psi,k).$$

To show this, it suffices to show that both sides have the same trace function, since this by Chebotarev implies that they have isomorphic semisimplifications as $\pi_1(\mathbb{A}^1/k)$-representations, and both are $\pi_1(\mathbb{A}^1/k)$-irreducible. For E/k a finite extension, and t in E, we readily calculate

$$\begin{aligned}
&\text{Trace}(\text{Frob}_{E,t} \mid \mathscr{G}_7(\psi_{\beta^7},k)) \\
&= (1/G(\psi_{-7\beta^7,E},\chi_{2,E})) \sum_{x \text{ in } E} \psi(\beta^7 \text{Trace}_{E/k}(x^7 + tx))\chi_{2,E}(x) \\
&= \chi_{2,E}(\beta^7)\big(1/G(\psi_{-7,E},\chi_{2,E})\big) \\
&\quad \times \sum_{x \text{ in } E} \psi(\text{Trace}_{E/k}((\beta x)^7 + \beta^6 t(\beta x)))\chi_{2,E}(x) \\
&= \chi_{2,E}(\beta)\big(1/G(\psi_{-7,E},\chi_{2,E})\big) \\
&\quad \times \sum_{x \text{ in } E} \psi(\text{Trace}_{E/k}(x^7 + \beta^6 tx))\chi_{2,E}(\beta^{-1}x) \\
&= \big(1/G(\psi_{-7,E},\chi_{2,E})\big) \sum_{x \text{ in } E} \psi(\text{Trace}_{E/k}(x^7 + \beta^6 tx))\chi_{2,E}(x) \\
&= \text{Trace}(\text{Frob}_{E,\beta^6 t} \mid \mathscr{G}_7(\psi,k)) \\
&= \text{Trace}(\text{Frob}_{E,t} \mid [t \mapsto \beta^6 t]^* \mathscr{G}_7(\psi,k)).
\end{aligned}$$

Therefore there exists an isomorphism of lisse sheave on $\mathbb{A}^1/k$,

$$\mathscr{G}_7(\psi_{\beta^7},k) \cong [t \mapsto \beta^6 t]^* \mathscr{G}_7(\psi,k).$$

Now $\mathscr{G}_7(\psi,k)$ and $[t \mapsto \beta^6 t]^* \mathscr{G}_7(\psi,k)$ have the same G_{arith} as each other, and the same G_{geom} as each other. So the corollary holds for $\mathscr{G}_7(\psi_{\beta^7},k)$.

To treat the general case, we reduce to the previous case, as follows. By Lemma (3.4), we know that G_{geom} is $U_3(3)$. We also know that G_{arith} is a finite subgroup of G_2 which contains G_{geom}, and hence G_{arith} is either $U_3(3)$ or is $U_3(3).2$. Thus G_{arith} is either equal to G_{geom}, or G_{arith} contains G_{geom} with index two. To determine which case we are in, we may pass from k to any finite extension of odd degree, and look there. But any α in $k^\times$ becomes a seventh power in an odd degree extension of k. [If k contains no nontrivial seventh roots of unity, every element α of $k^\times$ is a seventh power. If k contains the seventh roots of unity, then either α is already a seventh power, or the polynomial $X^7-\alpha$ is irreducible over k, in which case α becomes a seventh power in an extension of odd degree seven.] So we are reduced to the previous case. □

(4.16) Remark. One cannot fail to be struck by the fact that in the two characteristics $p=3$ and $p=13$ for which $\mathscr{G}_7$ has a finite G_{geom}, that finite group is the $\mathbb{F}_p$ points of a Chevalley group, i.e., $U_3(3)=\mathrm{PSU}(3,\mathbb{F}_3)$ in characteristic 3, and $L_2(13)=\mathrm{PSL}(2,\mathbb{F}_{13})$ in characteristic 13. This raises two obvious questions.

(1) Can one give conceptual, rather than computational, proofs of the results for characteristics 3 and 13?

(2) Can one find a "diophantinely meaningful" lisse sheaf of rank seven on $\mathbb{A}^1/\mathbb{F}_8$ with $G_{\text{geom}}=L_2(8)$? On $\mathbb{A}^1/\mathbb{F}_7$ with $G_{\text{geom}}=L_2(7).2$?

5. Application to explicit G_2 equidistribution

(5.1). Given a finite field k of characteristic $p=5$, $p=11$, or $p>15$, a nontrivial $\mathbb{C}$-valued additive character of k, and an element t in k, we define a conjugacy class

$$\vartheta(k,\psi,t)$$

in UG_2 as follows. Pick any prime $\ell\neq p$, and any field embedding $\iota:\bar{\mathbb{Q}}_\ell\to\mathbb{C}$. Then ι induces an isomorphism $\mu_{\mathrm{p}}(\bar{\mathbb{Q}}_\ell)\cong\mu_p(\mathbb{C})$, so there is a unique $\bar{\mathbb{Q}}_\ell$-valued additive character $\tilde{\psi}$ of k which, after ι, becomes the chosen ψ. Using this $\tilde{\psi}$, we construct the lisse $\bar{\mathbb{Q}}_\ell$-sheaf $\mathscr{G}_7$ on $\mathbb{A}^1/k$, with its corresponding representation

$$\rho:\pi_1(\mathbb{A}^1/k)\to G_2(\bar{\mathbb{Q}}_\ell). \tag{5.1.1}$$

For t in $k=\mathbb{A}^1(k)$, the element $\rho(\mathrm{Frob}_{k,t})$ in $G_2(\bar{\mathbb{Q}}_\ell)$ is in fact semisimple [because $H^1_c(\mathbb{G}_m\otimes_k\bar{k},\mathscr{L}_{\chi_2(x)}\otimes\mathscr{L}_{\psi(x^7+tx)})$ is a direct factor of $H^1(C\otimes_k\bar{k},\bar{\mathbb{Q}}_\ell)$, for C the complete nonsingular model of the curve in $\mathbb{A}^3$ defined by $y^2=x, z^q-z=x^7+tx$]. The element $\iota\rho(\mathrm{Frob}_{k,t})$ in $G_2(\mathbb{C})$ has its eigenvalues on the unit circle, so, being semisimple lies in a compact subgroup of $G_2(\mathbb{C})$, and hence is conjugate to an element of the chosen maximal compact subgroup UG_2. There is a general argument

of Deligne, given in [Ka-GKM, 3.3], which assures us that the resulting element of UG_2 is itself unique up to UG_2-conjugacy. The resulting conjugacy class we define to be $\vartheta(k,\psi,t)$. In the case at hand, we can use Lemma (4.2) to give a more down to earth description of this conjugacy class. It is the unique conjugacy class whose characteristic polynomial is given by

$$\begin{aligned}&\det(1-T\vartheta(k,\psi,t))\\&\quad=\iota L(\mathbb{G}_m/k,\mathscr{L}_{\chi_2(x)}\otimes\mathscr{L}_{\psi(x^n+tx)},T/(-G(\tilde{\psi}_{-7},\chi_2)))\\&\quad=\exp\left(\sum_{m\geqslant 1}(S(m,k,\psi,t)/(-G(\psi_{-7},\chi_2))^m)T^m/m\right),\end{aligned}\tag{5.1.2}$$

where we write k_m/k for the extension of degree m, and where we write $S(m,k,\psi,t)$ for the complex number

$$S(m,k,\psi,t):=\sum_{x\ \text{in}\ k_m,\ x\neq 0}\chi_{2,k_m}(x)\psi_{k_m}(x^7+tx).\tag{5.1.3}$$

(5.2). Applying Deligne's general equidistribution theorem, in the form [Ka-GKM, 3.6], to this situation, and remembering that $\mathscr{G}_7$ has highest ∞-break $7/6$ at ∞, we get the following theorem.

(5.3) Theorem. *In any sequence of data* (k_i,ψ_i), with

k_i *a finite field of characteristic* $p=5$, $p=11$, *or* $p>15$,

ψ_i *a nontrivial* $\mathbb{C}$*-valued additive character of* k_i,

in which $\#k_i\to\infty$, *the* $\#k_i$ *conjugacy classes* $\{\vartheta(k_i,\psi_i,t)\}_{t\ \text{in}\ k_i}$ *become equidistributed for normalized* (*total mass one*) *Haar measure in the space* $\mathrm{UG}_2^{\#}$ *of conjugacy classes of* UG_2. *For any continuous central function*

$$h:\mathrm{UG}_2\to\mathbb{C},$$

we have the integration formula

$$\int_{\mathrm{UG}_2}h(A)\,dA=\lim_{i\to\infty}(1/\#k_i)\sum_{t\ \text{in}\ k_i}h(\vartheta(k_i,\psi_i,t)).$$

More precisely, for k *a finite field of characteristic* $p=5$, $p=11$, *or* $p>15$, ψ *a nontrivial* $\mathbb{C}$*-valued additive character of* k, *and* Λ *a nontrivial unitary representation of* UG_2, *we have the estimate*

$$|(1/\#k)\sum_{t\ \text{in}\ k}\mathrm{Trace}(\Lambda(\vartheta(k,\psi,t)))|\leqslant\dim(\Lambda)/6\,\mathrm{Sqrt}(\#k)$$

(5.4) Remark. We get the constant in this last estimate as follows. The representation Λ extends to a representation of G_2, so we can form the lisse sheaf $\Lambda(\mathscr{G}_7)$. It has $H^i_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))=0$ for $i\neq 1$, and

$$\begin{aligned}&\sum_{t\ \text{in}\ k}\operatorname{Trace}(\Lambda(\vartheta(k,\psi,t)))\\&\quad=\iota\sum_i(-1)^i\operatorname{Trace}(\operatorname{Frob}_k\mid H^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7)))\\&\quad=-\iota\operatorname{Trace}(\operatorname{Frob}_k\mid H^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))).\end{aligned}\tag{5.4.1}$$

By Deligne [De-WeilII, 3.3.1], we have

$$\begin{aligned}&|\iota\operatorname{Trace}(\operatorname{Frob}_k\mid H^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7)))|\\&\quad\leqslant h^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))\operatorname{Sqrt}(\#k)\\&\quad=-\chi_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))\operatorname{Sqrt}(\#k).\end{aligned}\tag{5.4.2}$$

By the Euler Poincare formula, we have

$$\chi_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))=\operatorname{rank}(\Lambda(\mathscr{G}_7))-\operatorname{Swan}_\infty(\Lambda(\mathscr{G}_7)),\tag{5.4.3}$$

i.e., we have

$$h^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))=\operatorname{Swan}_\infty(\Lambda(\mathscr{G}_7))-\operatorname{rank}(\Lambda(\mathscr{G}_7)).\tag{5.4.4}$$

Because $\mathscr{G}_7$ has highest ∞-break $7/6$ at ∞, we have

$$\operatorname{Swan}_\infty(\Lambda(\mathscr{G}_7))\leqslant(7/6)\dim(\Lambda).\tag{5.4.5}$$

So we have

$$h^1_c(\mathbb{A}^1\otimes_k\bar{k},\ \Lambda(\mathscr{G}_7))\leqslant(7/6)\dim(\Lambda)-\dim(\Lambda)=\dim(\Lambda)/6.\tag{5.4.6}$$

(5.5). We now take the "direct image" of this result by the trace (in the seven-dimensional representation)

$$\operatorname{Trace}:\operatorname{UG}_2\to[-7,7].$$

As I learned from Serre [Se], the traces of elements of UG_2 all lie in the closed interval $[-2,7]$. Indeed, from the known shape of a maximal torus in G_2, namely all matrices of the form $\operatorname{Diag}(1,a,1/a,b,1/b,ab,1/ab)$, these traces are precisely the image of the map

$$[0,2\pi]\times[0,2\pi]\to\mathbb{R},$$

$$(x,y)\mapsto 1+2\operatorname{Cos}(x)+2\operatorname{Cos}(y)+2\operatorname{Cos}(x+y).$$

It is then a calculus exercise to see that the maximum, 7, occurs at $(0,0)$, and that the minimum, -2, occurs at $(2\pi/3, 2\pi/3)$ and at $(4\pi/3, 4\pi/3)$.

(5.6). Denote by

$$\mu_{G_2,\,\mathrm{trace}} \coloneqq \mathrm{Trace}_*(\text{normalized Haar measure on } \mathrm{UG}_2) \tag{5.6.1}$$

the direct image probability measure on $[-2,7]$. Thus for $h(x)$ a continuous $\mathbb{C}$-valued function on $[-2,7]$,

$$\int_{[-2,7]} h(x)\, d\mu_{G_2,\,\mathrm{trace}} \coloneqq \int_{\mathrm{UG}_2} h(\mathrm{Trace}(A))\, dA. \tag{5.6.2}$$

(5.7) Corollary. *In any sequence of data* (k_i, ψ_i) *as in Theorem* (4.8) *above, the* $\#k_i$ *real numbers*

$$\{-S(1,k_i,\psi_i,t)/(-G(\psi_{-7},\ \chi_2))\}_{t \text{ in } k_i},$$

become equidistributed in $[-2,7]$ *for the measure* $\mu_{G_2,\,trace}$.

(5.8). For each prime $p=5$, $p=11$, or $p>15$, take for ψ the additive character of $\mathbb{F}_p$ given by

$$\psi(x) \coloneqq \exp(2\pi i x/p). \tag{5.8.1}$$

Then for t in $\mathbb{F}_p$, we have

$$\begin{aligned} &-S(1,\mathbb{F}_p,\psi,t)/(-G(\psi_{-7},\ \chi_2)) \\ &\quad = (1/G(\psi_{-7},\ \chi_2)) \sum_{x \text{ in } \mathbb{F}_p,\, x\neq 0} \chi_2(x)\psi(x^7+tx). \end{aligned} \tag{5.8.2}$$

On the other hand,

$$G(\psi_{-7},\ \chi_2) = \chi_2(-7)G(\psi,\chi_2). \tag{5.8.3}$$

In the classical notation, and using quadratic reciprocity, we have

$$\chi_2(-7) = (-7/p) = (p/7). \tag{5.8.4}$$

By Gauss, we have

$$\begin{aligned} G(\psi,\chi_2) &= \mathrm{Sqrt}(p), \quad \text{if } p \equiv 1 \bmod 4, \\ &= i\,\mathrm{Sqrt}(p), \ \text{if } p \equiv 3 \bmod 4. \end{aligned} \tag{5.8.5}$$

Thus for $p \equiv 1 \bmod 4$, we have

$$-S(1, \mathbb{F}_p, \psi, t)/(-G(\psi_{-7}, \chi_2)) = (p/7)p^{-1/2} \sum_{x \text{ in } \mathbb{F}_p^\times} (x/p)\,\mathrm{Cos}(2\pi(x^7 + tx)/p). \tag{5.8.6}$$

For $p \equiv 3 \bmod 4$, we have

$$-S(1, \mathbb{F}_p, \psi, t)/(-G(\psi_{-7}, \chi_2)) = (p/7)p^{-1/2} \sum_{x \text{ in } \mathbb{F}_p^\times} (x/p)\,\mathrm{Sin}(2\pi(x^7 + tx)/p). \tag{5.8.7}$$

(5.9) Corollary. *As $p \to \infty$, the p real numbers*

$$\{(p/7)p^{-1/2} \sum_{x \text{ in } \mathbb{F}_p^\times} (x/p)\,\mathrm{Cos}(2\pi(x^7 + tx)/p)\}_{t \bmod p}, \text{ if } p \equiv 1 \bmod 4,$$

$$\{(p/7)p^{-1/2} \sum_{x \text{ in } \mathbb{F}_p^\times} (x/p)\,\mathrm{Sin}(2\pi(x^7 + tx)/p)\}_{t \bmod p}, \text{ if } p \equiv 3 \bmod 4,$$

become equidistributed in $[-2, 7]$ for the measure $\mu_{G_2,trace}$ on the closed interval $[-2, 7]$.

(5.10). We do not know an explicit formula for the measure $\mu_{G_2,\,\mathrm{trace}}$ on $[-2, 7]$. However, most of its mass is concentrated in the interval $[-2, 2]$. More precisely, we have the following tail estimate.

(5.11) Tail Estimate. For any real t in $(0, 7]$, we have the estimate

$$\mu_{G_2,\,\mathrm{trace}}([t, 7]) \leqslant \mathrm{Min}(1/t^2, 4/t^4, 35/t^6, 455/t^8).$$

In particular, we have the estimates

$$\mu_{G_2,\,\mathrm{trace}}([2, 7]) \leqslant 1/2^2 < 1/4,$$

$$\mu_{G_2,\,\mathrm{trace}}([3, 7]) \leqslant 4/3^4 < 1/20,$$

$$\mu_{G_2,\,\mathrm{trace}}([4, 7]) \leqslant 455/4^8 < 1/144,$$

$$\mu_{G_2,\,\mathrm{trace}}([5, 7]) \leqslant 455/5^8 < 1/858,$$

$$\mu_{G_2,\,\mathrm{trace}}([6, 7]) \leqslant 455/6^8 < 1/3691.$$

Proof. The first few even moments $M_{2k} := M_{2k}(G_2, \mathrm{std}_7)$ of G_2 in its seven dimensional representation std_7 are given (with help from simpLie [MPR]) by

$$M_2 = 1,\ M_4 = 4,\ M_6 = 35,\ M_8 = 455.$$

By the unitarian trick, we have

$$M_{2k} = \int_{\mathrm{UG}_2} (\mathrm{Trace}(A))^{2k}\, dA = \int_{[-2,7]} x^{2k}\, d\mu_{G_2,\,\mathrm{trace}}.$$

Now for any probability measure μ on $\mathbb{R}$, with even moments

$$m_{2k}(\mu) := \int_{\mathbb{R}} x^{2k}\, d\mu,$$

and for any real $t>0$, we have the inequality

$$m_{2k}(\mu) := \int_{\mathbb{R}} x^{2k}\, d\mu \geqslant \int_{|x|\geqslant t} x^{2k}\, d\mu \geqslant t^{2k}\mu(\{x \text{ with } |x|\geqslant t\}),$$

and the consequent Chebychev inequality

$$\mu(\{x \text{ with } |x|\geqslant t\}) \leqslant m_{2k}(\mu)/t^{2k}.$$

Applying this with μ the measure $\mu_{G_2,\,\mathrm{trace}}$, we find the asserted inequality. □

6. Application to explicit SO(n) equidistribution

(6.1). The results are entirely analogous to those in the G_2 case. We state them explicitly for ease of later reference.

(6.2). Fix an odd integer $n = 2d+1 \geqslant 3,\ n \neq 7$. Recall that

$$\varepsilon(n) := (-1)^d. \tag{6.2.1}$$

A compact form of SO(n) is the real group $\mathrm{SO}(n,\mathbb{R})$ for the quadratic form $\sum_i (x_i)^2$. Because n is odd, conjugacy classes in $\mathrm{SO}(n,\mathbb{R})$ are determined by their characteristic polynomials.

(6.3). Let us say that a characteristic p is "good for n" if the following condition 6.3.1 holds.

(6.3.1). For any finite field k of characteristic p, for any prime $\ell \neq p$, and for any nontrivial $\mathbb{Q}_\ell$-valued additive character ψ of k, the lisse sheaf $\mathscr{F}_n$ on $\mathbb{A}^1/k$ has $G_{\mathrm{geom}} = \mathrm{SO}(n)$.

(6.4). We know that, given an odd $n \geqslant 3$, all but finitely many p are good for n, but in general we do not know exactly which are not.

(6.5). Given a finite field k of characteristic p which is good for n, a nontrivial $\mathbb{C}$-valued additive character of k, and an element t in k, we define a conjugacy class

$$\vartheta(k, \psi, t)$$

in $\mathrm{SO}(n, \mathbb{R})$ just as we did in the G_2 case. It is the unique conjugacy class whose characteristic polynomial is given by

$$\det(1 - T\vartheta(k, \psi, t))$$

$$= \exp\left(\sum_{m \geqslant 1} (S(m, k, \psi, t)/(-G(\psi_{\varepsilon(n)n},\ \chi_2))^m) T^m/m \right), \tag{6.5.1}$$

where we write k_m/k for the extension of degree m, and where we write $S(m, k, \psi, t)$ for the complex number

$$S(m, k, \psi, t) := \sum_{x \text{ in } k_m,\ x \neq 0} \chi_{2,k_m}(x) \psi_{k_m}(x^n + tx). \tag{6.5.2}$$

Applying Deligne's general equidistribution theorem to this situation in the form [Ka-GKM, 3.6], and remembering that $\mathscr{G}_n$ has highest ∞-break $n/(n-1)$ at ∞, we get the following theorem.

(6.6) Theorem. *In any sequence of data (k_i, ψ_i), with*

k_i a finite field of characteristic p which is good for n,

ψ_i a nontrivial $\mathbb{C}$-valued additive character of k_i,

in which $\#k_i \to \infty$, the $\#k_i$ conjugacy classes $\{\vartheta(k_i, \psi_i, t)\}_{t \text{ in } k_i}$ become equidistributed for normalized (total mass one) Haar measure in the space $\mathrm{SO}(n, \mathbb{R})^{\#}$ of conjugacy classes of $\mathrm{SO}(n, \mathbb{R})$. For any continuous central function

$$h : \mathrm{SO}(n, \mathbb{R}) \to \mathbb{C},$$

we have the integration formula

$$\int_{\mathrm{SO}(n,\ \mathbb{R})} h(A)\, dA = \lim_{i \to \infty} (1/\#k_i) \sum_{t \text{ in } k_i} h(\vartheta(k_i, \psi_i, t)).$$

More precisely, for k a finite field of characteristic $p > 2n + 1$ not dividing the integer $2nN_1(n-1)N_2(n-1)$, ψ a nontrivial $\mathbb{C}$-valued additive character of k, and Λ a

nontrivial unitary representation of $\mathrm{SO}(n)$ we have the estimate

$$\left|(1/\#k)\sum_{t\text{ in }k}\mathrm{Trace}(\Lambda(\vartheta(k,\psi,t)))\right|\leqslant \dim(\Lambda)/((n-1)\,\mathrm{Sqrt}(\#k)).$$

(6.7). We now take the "direct image" of this result by the trace

$$\mathrm{Trace}\ :\ \mathrm{SO}(n,\ \mathbb{R})\to[2-n,n],$$

and define

$$\mu_{\mathrm{SO}(n),\ \mathrm{trace}} \coloneqq \mathrm{Trace}_*(\text{normalized Haar measure on } \mathrm{SO}(n,\mathbb{R})). \tag{6.7.1}$$

(6.8) Corollary. *In any sequence of data* (k_i,ψ_i) *as in Theorem* (5.6) *above, the* $\#k_i$ *real numbers*

$$\{-S(1,k_i,\psi_i,t)/(-G(\psi_{-7},\chi_2))\}_{t\text{ in }k_i},$$

become equidistributed in $[2-n,n]$ *for the measure* $\mu_{\mathrm{SO}(n),\ \mathrm{trace}}$.

(6.9). For each prime p which is good for n, take for ψ the additive character of $\mathbb{F}_p$ given by

$$\psi(x) \coloneqq \exp(2\pi i x/p). \tag{6.9.1}$$

Then for t in $\mathbb{F}_p$, we have

$$\begin{aligned} &-S(1,\mathbb{F}_p,\psi,t)/(-G(\psi_{\varepsilon(n)n},\ \chi_2))\\ &\quad=(1/G(\psi_{\varepsilon(n)n},\ \chi_2))\sum_{x\text{ in }\mathbb{F}_p,\ x\neq 0}\chi_2(x)\psi(x^n+tx). \end{aligned} \tag{6.9.2}$$

On the other hand,

$$G(\psi_{\varepsilon(n)n},\ \chi_2)=\chi_2(\varepsilon(n)n)G(\psi,\ \chi_2). \tag{6.9.3}$$

In the classical notation, and using quadratic reciprocity, we have

$$\chi_2(\varepsilon(n)n)=(\varepsilon(n)n/p)=(p/n), \tag{6.9.4}$$

where (p/n) is the extended Jacobi symbol: for n with prime factorization $n=\prod_i(\ell_i)^{e(i)}$,

$$(p/n)\coloneqq\prod_i(p/\ell_i)^{e(i)}. \tag{6.9.5}$$

For $p \equiv 1 \bmod 4$, we have

$$-S(1,\mathbb{F}_p,\psi,t)/(-G(\psi_{\varepsilon(n)n},\chi_2)) = (p/n)p^{-1/2}\sum_{x \text{ in } \mathbb{F}_p^\times}(x/p)\,\mathrm{Cos}(2\pi(x^n+tx)/p). \tag{6.9.6}$$

For $p \equiv 3 \bmod 4$, we have

$$-S(1,\mathbb{F}_p,\psi,t)/(-G(\psi_{\varepsilon(n)n},\chi_2)) = (p/n)p^{-1/2}\sum_{x \text{ in } \mathbb{F}_p^\times}(x/p)\,\mathrm{Sin}(2\pi(x^n+tx)/p). \tag{6.9.7}$$

6.10. Corollary. *As $p\to\infty$, the p real numbers*

$$\left\{(p/n)p^{-1/2}\sum_{x \text{ in } \mathbb{F}_p^\times}(x/p)\,\mathrm{Cos}(2\pi(x^n+tx)/p)\right\}_{t \bmod p}, \quad \text{if } p \equiv 1 \bmod 4,$$

$$\left\{(p/n)p^{-1/2}\sum_{x \text{ in } \mathbb{F}_p^\times}(x/p)\,\mathrm{Sin}(2\pi(x^n+tx)/p)\right\}_{t \bmod p}, \quad \text{if } p \equiv 3 \bmod 4,$$

become equidistributed in $[2-n,n]$ for the measure $\mu_{\mathrm{SO}(n),\,trace}$.

(6.11). We do not know an explicit formula for the measure $\mu_{\mathrm{SO}}(n)$, trace on $[-2-n,n]$. However, most of its mass is concentrated in the interval $(-2,2)$. To formulate more precise tail estimates, recall that for an positive even integer $2k$, we define

$$(2k)!! := \prod_{\ell=1 \text{ to } k}(2k+1-2\ell) = (2k-1)(2k-3)\ldots(3)(1).$$

One knows [Rains, Theorem 3.4] that the even moments of $\mathrm{SO}(n)$ in its standard representation std_n are given by

$$M_{2k} := M_{2k}(\mathrm{SO}(n),\mathrm{std}_n) = (2k)!!, \quad \text{for } k \leqslant n.$$

[This is proven for $O(n)$ in [Rains, Theorem 3.4]; as n is odd, $O(n)$ is $\mathrm{SO}(n)\times\{\pm 1\}$, so the two groups have the same even moments.] By exactly the same Chebychev argument as in the proof of 5.11, we find

(6.12) Tail Estimate. For any odd $n \geqslant 3$, and any real $t>0$, we have the estimate

$$\mu_{\mathrm{SO}(n),\ \mathrm{trace}}(\{x \text{ with } |x| \geqslant t\}) \leqslant \operatorname*{Min}_{k=1 \text{ to } n}((2k)!!/t^{2k}).$$

In particular, for odd $n \geqslant 5$ we have the estimates

$$\mu_{\mathrm{SO}(n),\ \mathrm{trace}}(\{x \text{ with } |x| \geqslant 2\}) \leqslant 3/2^4 < 1/5,$$

$$\mu_{\mathrm{SO}(n),\ \mathrm{trace}}(\{x \text{ with } |x| \geqslant 3\}) \leqslant (3)(5)(7)/3^8 < 1/62,$$

$$\mu_{\mathrm{SO}(n),\ \mathrm{trace}}(\{x \text{ with } |x| \geqslant 4\}) \leqslant (3)(5)(7)(9)/4^{10} < 1/1109,$$

7. Application to the Katz–Sarnak measures $\nu(-, c)$

(7.1). A second flavor of application of our $\mathscr{F}_n$ results is to the eigenvalue location measures $\nu(-, c)$ of [Ka-Sar, 13.1]. Here $r \geqslant 1$ is an integer, $c\ (c(1), \ldots, c(r))$ in $\mathbb{Z}^r$ is an "offset vector", i.e.

$$0 < c(1) < c(2) < \cdots < c(r). \tag{7.1.1}$$

For $n = 2d + 1$ with $d \geqslant c(r)$, the eigenvalues of an element A of $\mathrm{SO}(n, \mathbb{R})$ are of the form

$$1, e^{\pm i\varphi(1)},\ e^{i\varphi(2)}, \ldots, e^{\pm i\varphi(d)}, \tag{7.1.2}$$

for a unique sequence of angles

$$0 \leqslant \varphi(1) \leqslant \varphi(2) \leqslant \cdots \leqslant \varphi(d) \leqslant \pi. \tag{7.1.3}$$

Formation of any given $\varphi(i)$ defines a continuous central function on $\mathrm{SO}(n, \mathbb{R})$,

$$A \mapsto \varphi(i)(A). \tag{7.1.4}$$

We rescale this function, and call it $\vartheta(i)$:

$$\vartheta(i)(A) := n\varphi(i)(A)/2\pi. \tag{7.1.5}$$

Given the offset vector c, we define the continuous central function

$$F_c : \mathrm{SO}(n, \mathbb{R}) \to \mathbb{R}^r,$$

$$F_c(A) := (\vartheta(c(1))(A), \ldots, \vartheta(c(r))(A)). \tag{7.1.6}$$

We then define the probability measure $\nu(c, \mathrm{SO}(n, \mathbb{R}))$ on $\mathbb{R}^v$ to be

$$\nu(c, \mathrm{SO}(n, \mathbb{R})) := (F_c)_*(\text{normalized Haarmeasure on } \mathrm{SO}(n, \mathbb{R})). \tag{7.1.7}$$

(7.2). Given a finite field k of characteristic p which is good for n, and a nontrivial $\mathbb{C}$-valued additive character ψ of k, we define the probability measure $\nu(c,k,\psi,\mathrm{SO}(n,\mathbb{R}))$ on $\mathbb{R}^r$ by averaging over the images, by F_c, of the conjugacy classes $\vartheta(k,\psi,t)$, t in k:

$$\nu(c,k,\psi,\mathrm{SO}(n,\mathbb{R})) := (1/\#k)\sum_{t\ \mathrm{in}\ k}\delta_{F_{c(\vartheta(k,\psi,t))}}. \tag{7.2.1}$$

As an immediate consequence of the general equi-distribution theorem, we find the following corollary.

7.3. Corollary. *Fix $r\geqslant 1$, and c an offset vector in $\mathbb{Z}^r$. Suppose $n=2d+1$ is an odd integer with $d\geqslant c(r)$. In any sequence of data (k_i,ψ_i) as in the theorem above, the $\#k_i$ points $\{F_c(\vartheta(k_i,\psi_i,t))\}_{t\ \mathrm{in}\ k_i}$ in $\mathbb{R}^r$ become equidistributed for the measure $\nu(c,\mathrm{SO}(n,\mathbb{R}))$. In other words, the measures $\nu(c,k_i,\psi_i,\mathrm{SO}(n,\mathbb{R}))$ tend weak $*$ to the measure $\nu(c,\mathrm{SO}(n,\mathbb{R}))$ as $i\to\infty$.*

(7.4). We now take the large n limits, cf. [Ka-Sar, 13.8].

7.5 Theorem. *In any sequence of pairs (k_i,ψ_i) in which $\mathrm{char}(k_i)\to\infty$, we have the following double limit formula for the probability measure $\nu(-,c)$ on $\mathbb{R}^r$. For any bounded continuous $\mathbb{C}$-valued function h on $\mathbb{R}^r$, we have the integration formula*

$$\int_{\mathbb{R}^r} h\,d\nu(-,c) = \lim_{\mathrm{odd}\ n\to\infty}\ \lim_{i\to\infty}\int_{\mathbb{R}^r} h\,d\nu(c,k_i,\psi_i,\mathrm{SO}(n,\mathbb{R})).$$

7.6. Remark. We need to have $\mathrm{char}(k_i)$ tending to ∞ to be sure that for each odd n, $\mathrm{char}(k_i)$ is "good for n" provided that i is sufficiently large. At present, we do not which, if any, primes p are good for every odd $n\geqslant 3$ which is prime to p. We could avoid these problems by working instead with the sheaves $\mathscr{F}_{n,\mathrm{odd}\leqslant 3}$ or $\mathscr{F}_{n,\mathrm{odd}}$, since, by Theorems (3.11) and (3.12), every prime $p>5$ not dividing n is good for them.

References

[Adams] J.F. Adams, Lectures on exceptional Lie groups, Chicago Lectures in Mathematics, University of Chicago Press, 1996.

[Asch] M. Aschbacher, Chevalley groups of type G_2 as the group of a trilinear form, J. Algebra 109 (1987) 193–259.

[Co-Wa] A. Cohen, D. Wales, Finite subgroups of $G_2(\mathbb{C})$, Comm. Algebra 11 (1983) 441–459.

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

[Dav-Has] H. Davenport, H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine Angew. Math. 172 (1934) 151–182.

[De-WeilII] P. Deligne, La conjecture de Weil II, Pub. Math. I.H.E.S. 52 (1981) 313–428.

[GAP] Lehrstuhl D für Mathematik, RWTH Aachen, GAP, computer program, available from http://www-gap.dcs.st-and.ac.uk/~gap.

[Ka-Betti] N. Katz, Sums of Betti numbers in arbitrary characteristic, Finite Fields Appl. 7 (2001) 29–44.

[Ka-ESDE] N. Katz, Exponential Sums and Differential Equations, Annals of Mathematic Studies, Vol. 124, Princeton University Press, Princeton, NJ, 1990.

[Ka-GKM] N. Katz, Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematic Studies, Vol. 116, Princeton University Press, Princeton, NJ, 1988.

[Ka-LFM] N. Katz, *L*-functions and monodromy: four lectures on Weil II, Adv. Math. 160 (1) (2001) 81–132.

[Ka-MG] N. Katz, On the monodromy groups attached to certain families of exponential sum, Duke Math J. 54 (1) (1987) 41–56.

[Ka-SMD] N. Katz, A semicontinuity result for monodromy under degeneration, Forum Math. 15 (2) (2003) 191–200.

[Ka-Sar] N. Katz, P. Sarnak, Random matrices, Frobenius eigenvalues, and monodromy, American Mathematical Society, Colloquium Publications, Vol. 45, American Mathematical Society, Providence, RI, 1999.

[Lau-TF] G. Laumon, Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil, Pub. Math. I.H.E.S. 65 (1987) 131–210.

[MPR] R.V. Moody, J. Patera, D.W. Rand, simpLie,Version 2.1, Macintosh Software for Representations of Simple Lie Algebras, December 2000, available from http://www.crm.umontreal.ca/~rand/simpLie.html

[Rains] E.M. Rains, Increasing subsequences and the classical groups, Electron. J. Combin. 5 (1) (1998) Research Paper 12, p. 9 (electronic).

[Sch] J.A. Schouten, Klassifigizierung der alternierenden Groszen dritten Grades in 7 Dimensionen, Rend. Circ. Matem. Palermo 55 (1931) 77–91.

[Se] J.-P. Serre, personal communication, March 7, 2002.

[Spr] T.A. Springer, Linear Algebraic Groups, 2nd Edition, Birkhauser, Basel, 1998.