RIGID LOCAL SYSTEMS ON $\mathbb{A}^1$ WITH FINITE MONODROMY

NICHOLAS M. KATZ, WITH AN APPENDIX BY PHAM HUU TIEP

Abstract. We formulate some conjectures about the precise determination of the monodromy groups of certain rigid local systems on $\mathbb{A}^1$ whose monodromy groups are known, by results of Kubert, to be finite. We prove some of them.

Contents

1. Introduction

The solution [Ray] of Abhyankar's Conjecture for the affine line in finite characteristic p tells us that any finite group which is generated by its p-Sylow subgroups occurs as a quotient of the geometric fundamental group. In a series of papers, Abhyankar has written down explicit equations which realize many finite groups of Lie type as such quotients. Here our concern is with certain local systems which arise as very simple one-parameter families of exponential sums.

Namely, we start with a finite field $\mathbb{F}_q$ of characteristic p, a prime number $\ell \neq p$, a nontrivial $\overline{\mathbb{Q}_\ell}$-valued additive character ψ of $\mathbb{F}_q$, and a $\overline{\mathbb{Q}_\ell}^\times$-valued multiplicative character χ of $\mathbb{F}_q^\times$ (with the convention that for χ the trivial character $\mathbb{1}$, $\mathbb{1}(0) = 1$, otherwise $\chi(0) = 0$), and an integer $D \geq 3$. Then we form the local system $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ on $\mathbb{A}^1/\mathbb{F}_q$ whose trace function(at $\mathbb{F}_q$-valued points $t \in \mathbb{F}_q = \mathbb{A}^1(\mathbb{F}_q)$) is given by

$$t \mapsto -\sum_{x \in \mathbb{F}_q} \chi(x)\psi(x^D + tx),$$

with an analogous formula for the trace at k-valued points $t \in k$, for $k/\mathbb{F}_q$ a finite extension.

As we recall in Theorem 3.1, these local systems have long been known to have huge geometric monodromy groups when the characteristic p is large compared to D. In our earlier work, we had also encountered some situations where p was small compared to D and where we showed that the geometric monodromy group was a finite group. Here are some of them.

(1) $\mathcal{F}(\mathbb{F}_2, \psi, \mathbb{1}, 3)$.
(2) $\mathcal{F}(\mathbb{F}_2, \psi, \mathbb{1}, 5)$.
(3) $\mathcal{F}(\mathbb{F}_3, \psi, \mathbb{1}, 4)$.
(4) $\mathcal{F}(\mathbb{F}_3, \psi, \mathbb{1}, 5)$.
(5) $\mathcal{F}(\mathbb{F}_5, \psi, \mathbb{1}, 3)$.
(6) $\mathcal{F}(\mathbb{F}_3, \psi, \chi_2, 5)$, $G_{geom} = A_5$.
(7) $\mathcal{F}(\mathbb{F}_{13}, \psi, \chi_2, 7)$, $G_{geom} = PSL(3, 13)$.
(8) $\mathcal{F}(\mathbb{F}_3, \psi, \chi_2, 7)$, $G_{geom} = SU(3, 3)$.

See [Ka-MMP, 3.8.4] for the first five, and [Ka-NG2, 3.9,4.13,4.14] for the last three.

Theorems of Kubert [Kubert] from May,1986 gave whole families of local systems $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ with finite geometric monodromy groups. The numerology of some of the Kubert families matches the numerology of the representation theory of the groups $SL(2, q)$ for $q \geq 5$ a power of an odd prime p. The numerology of other Kubert families matches the numerology of the representation theory of the groups $SU(n, q)$ for

$n \geq 3$ odd and q any power of p (with the proviso that $q \geq 3$ if $n = 3$). In section 9, we formulate the natural conjectures which arise form this agreement of numerology.

We were led to formulate these conjectures when we realized, only recently, that all of the eight examples of finite geometric monodromy listed above fit into the framework of Kubert's theorems. One of his results (Theorem 4.1) was that for q any power of p, $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, q+1)$ has finite geometric monodomy, which Pink [Pink] the next week (!) showed to be a p-group, see the Appendix for Pink's proof. Sawin has recently shown that when q is odd, this group is in fact a Heisenberg group of order pq^2 and exponent p. See the second appendix for Sawin's proof. This explains examples (1) through (5) above. Items (6) and (7) result from another Kubert theorem (Theorem 4.2,(2)), that $\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ has finite geometric monodromy, which we conjecture always to be the image of $SL(2,q)$ in one of its irreducible representations of dimension $(q+1)/2$, so long as $q \geq 5$ is odd. Item (6) falls under this rubric with $q = 9$ if we remember that A_5 is also $PSL(2,5)$. Item (7) is the case $q = p = 13$. The final case results from yet another Kubert result (Theorem 4.3,(2)), that for $n \geq 3$ odd, $\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q^n+1)/(q+1))$ has finite geometric monodromy, which we conjecture to be the image of $SU(n,q)$ in its unique orthogonal representation of dimension $(q^n+1)/(q+1)$, so long as $q \geq 3$ is odd. Item (8) confirms this to be the case for $n = q = 3$.

We prove these conjectures in the case of $SL(2,p)$ using classical group theory results of Brauer [Brauer], [Brauer2], Feit [Feit] and Tuan [Tuan]. We then treat all cases of the conjectures for $SL(2,q)$ and many (but not all) for $SU(3,q)$ by using the beautiful work of Dick Gross [Gross] and the ideas underlying that work, which Gross generously explained to us. We identify the local systems in question as Kummer pullbacks of local systems on $\mathbb{G}_m/\mathbb{F}_q$, respectively on $\mathbb{G}_m/\mathbb{F}_{q^2}$, which are themselves pushouts of G-torsors when G is $PSL(2,q)$, respectively $PU(3,q)$. These G-torsors are themselves certain Deligne-Lusztig curves, which Gross explains how to view as G-torsors for G either $PSL(2,q)$ or $PU(3,q)$

It is a pleasure to acknowledge Dick Gross's essential contribution to this work. It is a pleasure to thank Ron Evans, for providing the proofs of Theorem 16.3 and of Theorem 19.4, Richard Pink for providing, in 1986, the proof of Theorem 20.1 and its corollaries, and Will Sawin for providing the proof of Theorem 21.1.

In a first version of this paper, the $SU(3,q)$ discussion required q to be odd, because it used explicit facts about the representation theory of finite Heisenberg groups, which for q odd occurs as certain unipotent

radicals. Pham Huu Tiep explained to me that in the q even case, the representation theory of these unipotent radicals was no different, and kindly added an appendix showing this.

2. The local systems

Fix a prime p, a finite field $\mathbb{F}_q$ of characteristic p, and a nontrivial additive character

$$\psi : (\mathbb{F}_q, +) \to \mu_p(\mathbb{Z}[\zeta_p]).$$

Denote by χ a nontrivial multiplicative character

$$\chi : \mathbb{F}_q^\times \to \mu_{q-1}(\mathbb{Z}[\zeta_{q-1}]).$$

We extend χ to a function on all of $\mathbb{F}_q$ by defining $\chi(0) = 0$.

We choose a prime number $\ell \neq p$, and an embedding of $\overline{\mathbb{Q}}$, say viewed as the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, into an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$. This allows us to speak of the lisse, rank one $\overline{\mathbb{Q}_\ell}$ Artin-Schreier sheaf $\mathcal{L}_\psi$ on $\mathbb{A}^1/\mathbb{F}_q$ and of the lisse, rank one $\overline{\mathbb{Q}_\ell}$ Kummer sheaf $\mathcal{L}_\chi$ on $\mathbb{G}_m/\mathbb{F}_q$. For $j : \mathbb{G}_m \subset \mathbb{A}^1$ the inclusion, the extension by zero $j_!\mathcal{L}_\chi$ on $\mathbb{A}^1$ will also be denoted $\mathcal{L}_\chi$ when no ambiguity can result. We denote by $\mathbb{1}$ the trivial multiplicative character, and adopt the convention that $\mathcal{L}_{\mathbb{1}}$ is the constant sheaf $\overline{\mathbb{Q}_\ell}$ on $\mathbb{A}^1$. We write FT for FT_ψ, the Fourier Transform using $\mathcal{L}_{\psi(xy)}$ as the kernel.

Given an integer $D \geq 2$ which is prime to p, we denote by

$$\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D) := FT(\mathcal{L}_{\psi(x^D)}),$$

and, for each nontrvial χ,

$$\mathcal{F}(\mathbb{F}_q, \psi, \chi, D) := FT(\mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)}).$$

These Fourier Transform sheaves are lisse on $A^1/\mathbb{F}_q$, pure of weight one, and geometrically irreducible. They are cohomologically rigid, being the Fourier Transforms of rank one objects, cf. [Ka-RLS, 3.0.2]. Their ranks are

$$\operatorname{rank}(\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)) = D - 1,$$
$$\operatorname{rank}(\mathcal{F}(\mathbb{F}_q, \psi, \chi, D) = D \quad \text{for } \chi \neq \mathbb{1}.$$

Their trace functions are given as follows. For $k/\mathbb{F}_q$ a finite extension, define

$$\psi_{k/\mathbb{F}_q} := \psi \circ \operatorname{Trace}_{k/\mathbb{F}_q}, \quad \chi_{k/\mathbb{F}_q} := \chi \circ \operatorname{Norm}_{k/\mathbb{F}_q}.$$

Then for $t \in k$, we have

$$\operatorname{Trace}(Frob_{t,k} | \mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)) = -\sum_{x \in k} \psi_{k/\mathbb{F}_q}(x^D + tx),$$

$$\operatorname{Trace}(Frob_{t,k} | \mathcal{F}(\mathbb{F}_q, \psi, \chi, D)) = -\sum_{x \in k^\times} \chi_{k/\mathbb{F}_q}(x)\psi_{k/\mathbb{F}_q}(x^D + tx).$$

When D is odd, $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ is symplectically self-dual toward $\overline{\mathbb{Q}_\ell}(-1)$. When D is even, $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ has no autoduality.

When D is odd, p is odd, and χ is the quadratic character χ_2, then $\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, D)$ is orthogonally self-dual toward $\overline{\mathbb{Q}_\ell}(-1)$. No other $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ with nontrivial χ is autodual.

Given a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{F}$ on $\mathbb{A}^1/\mathbb{F}_q$ of rank r, we choose a geometric point $\overline{\eta}$ of $\mathbb{A}^1$ and view $\mathcal{F}$ as a representation of the fundamental group

$$\pi_1^{arith}(\mathbb{A}^1/\mathbb{F}_q, \overline{\eta}) := \pi_1(\mathbb{A}^1/\mathbb{F}_q, \overline{\eta}),$$

$$\rho_{\mathcal{F}} : \pi_1^{arith}(\mathbb{A}^1/\mathbb{F}_q, \overline{\eta}) \to GL(\mathcal{F}_{\overline{\eta}}) \cong GL(r, \overline{\mathbb{Q}_\ell}).$$

The Zariski closure of the image of π_1^{arith} is the arithmetic monodromy group $G_{arith,\mathcal{F}}$ of $\mathcal{F}$. The Zariski closure of the image of its normal subroup

$$\pi_1^{geom}(\mathbb{A}^1/\mathbb{F}_q, \overline{\eta}) := \pi_1(\mathbb{A}^1/\overline{\mathbb{F}_q}, \overline{\eta})$$

is the geometric monodromy group $G_{geom,\mathcal{F}}$ of $\mathcal{F}$.

For $\mathcal{F}$ a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{A}^1/\mathbb{F}_q$ of rank r which is geometrically irreducible, if $p > 2r + 1$, then $\mathcal{F}$ is Lie-irreducible, i.e., the identity component G^0_{geom} of G_{geom} acts irreducibly, cf [Ka-MG, Prop. 5]. Below we will be interested in situations where $p \leq 2r + 1$.

Geometrically, i.e. on $\mathbb{A}^1/\overline{\mathbb{F}_q}$, the (restrictions to $\mathbb{G}_m$ of the) local systems $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ and $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D))$ are Kummer pullbacks, by the D'th power map, of certain Kloosterman, respectively hypergeometric, sheaves, cf.[Ka-ESDE, 9.2.3 and 9.2.2]. The precise statement is this.

Theorem 2.1. *We have the following results.*

(1) *Denote by $\rho_1, ..., \rho_{D-1}$ all but one of the multipicative characters of order dividing D (of a suitably large extension of $\mathbb{F}_q$, say $\mathbb{F}_q[\mu_D]$). Then $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)|\mathbb{G}_m$ is geometrically isomorphic to a multiplicative translate of*

$$[D]^\star Kl(!, \psi; \rho_1, ..., \rho_{D-1}) = [D]^\star \mathcal{H}(!, \psi; \rho_1, ..., \rho_{D-1}; \emptyset).$$

(2) *Denote by $\rho_1, ..., \rho_D$ all the multipicative characters of order dividing D (of a suitably large extension of $\mathbb{F}_q$, say $\mathbb{F}_q[\mu_D]$). Choose a multiplicative character Λ (of a suitably large extension of $\mathbb{F}_q$) such that*

$$\Lambda^D = \overline{\chi}.$$

Then $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)|\mathbb{G}_m$ is geometrically isomorphic to a multiplicative translate of

$$[D]^\star \mathcal{H}(!, \psi; \rho_1, ..., \rho_D; \Lambda).$$

Corollary 2.2. *We have the following results.*

(1) *For $D \geq 3$, the determinants $\det(\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D))$ and $\det(\mathcal{F}(\mathbb{F}_q, \psi, \chi, D))$ are everywhere tame, hence geometrically constant on $\mathbb{A}^1/\mathbb{F}_q$.*

(2) *The I_∞ representation of $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ is totally wild, with all slopes $D/(D-1)$. The I_∞ representation of $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ is the direct sum of a totally wild summand of rank $D-1$ with all slopes $D/(D-1)$ and a rank one summand which is the restriction to I_∞ of the Kummer sheaf $\mathcal{L}_\chi$.*

(3) *For $j : \mathbb{A}^1 \subset \mathbb{P}^1$ the inclusion, we have*

$$j_!\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D) \cong j_\star\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D),$$

$$j_!\mathcal{F}(\mathbb{F}_q, \psi, \chi, D) \cong j_\star\mathcal{F}(\mathbb{F}_q, \psi, \chi, D).$$

(4) *For $\mathcal{F}$ either $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ or $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$, and $i \neq 1$, we have*

$$H^i_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{F}) = H^i(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}) = 0.$$

(5) *We have*

$$H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)) = H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)) = \overline{\mathbb{Q}_\ell}(-1).$$

(6) *For χ nontrivial, we have*

$$H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{F}(\mathbb{F}_q, \psi, \chi, D)) = H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)) = 0.$$

Proof. Assertion (1) results from the corresponding fact for the hypergeometric sheaves in question. They are tame at 0, and at ∞ all their nonzero ∞ slopes are $1/(D-1) < 1$ (because $D \geq 3$), so their determinants are tame at both 0 and ∞. The pullbacks of their determinants by $[D]$ are lisse on $\mathbb{A}^1$ and tame at ∞, so geometrically constant. Assertion (2) results by pullback from the corresponding facts about hypergemetric sheaves. Assertion (3) is then immediate from (2), according to which both $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ and $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ are totally ramified at ∞. Assertion (4) results from (3) and the fact that the $\mathcal{F}$'s in question are geometrically irreducible of rank ≥ 2. Assertions (5) and (6) result from Fourier inversion. □

We have the following more precise information about determinants.

Theorem 2.3. *For $D \geq 3$, both $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, D)$ and $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ have geometrically trivial determinants, so of the form α^{deg} for some scalar $\alpha(\mathbb{F}_q, \psi, \chi, D) \in \overline{\mathbb{Q}_\ell}^\times$. The scalar $\alpha(\mathbb{F}_q, \psi, \chi, D)$ is given as follows, where for $m \in \mathbb{F}_q$ we write ψ_m for the additive character $x \mapsto \psi(mx)$.*

(1) *If $D = 2d$ is even, then for $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, 2d)$ we have*

$$\alpha(\mathbb{F}_q, \psi, \mathbb{1}, D) = (-g(\psi_d, \chi_2))q^{d-1}.$$

(2) *If $D = 2d$ is even, then for $\mathcal{F}(\mathbb{F}_q, \psi, \chi, 2d)$ with χ nontrivial we have*

$$\alpha(\mathbb{F}_q, \psi, \chi, D) = (-g(\psi_{-D}, \chi))(-g(\psi_d, \chi_2))q^{d-1}.$$

(3) *If $D = 2d+1$ is odd, then for $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, 2d+1)$ we have*

$$\alpha(\mathbb{F}_q, \psi, \mathbb{1}, 2d+1) = q^d.$$

(4) *If $D = 2d+1$ is odd, then for $\mathcal{F}(\mathbb{F}_q, \psi, \chi, 2d+1)$ with χ nontrivial we have*

$$\alpha(\mathbb{F}_q, \psi, \chi, 2d+1) = (-g(\psi_D, \chi))q^d.$$

Proof. As shown in 2.2 part(1), the determinants in question are geometrically trivial, so each is of the form α^{deg} for some scalar $\alpha \in \overline{\mathbb{Q}_\ell}^\times$. This scalar is then the common value of $\det(Frob_{\mathbb{F}_q,t}|\mathcal{F})$ at points $t \in \mathbb{F}_q$. Taking $t = 0$, the scalar is

$$\det(Frob_{\mathbb{F}_q}|H^1_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)})),$$

for χ either $\mathbb{1}$ or nontrivial.

Here is a simple trick which "unites" these cases. When χ is the trivial character $\mathbb{1}$, replace it by $j_!$ of itself; in other words, consider instead the cohomology group $H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)})$. When χ is nontrivial, this is the same group as before; when $\chi = \mathbb{1}$, the cohomology group grows in dimension by one, adding an eigenvalue 1. So in both cases the determinant does not change.

To compute the determinant, we use the Hasse-Davenport method, cf. [Ka-MG, page 53] and [Ka-NG2, 2.2-2.3]. In terms of the elementary symmetric functions S_i, the Newton symmetric functions N_i are $\mathbb{Z}$-polynomials in the S_j. Then

$$\det(-Frob_{\mathbb{F}_q}|H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, \mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)})) =$$

$$= \sum_{S_1,...,S_D \in \mathbb{F}_q, S_D \neq 0} \chi(S_D)\psi(N_D(S_1, ..., S_D)).$$

The polynomial $N_D(S_1, ..., S_D)$ is of the form

$$N_D = (-1)^{D+1} D S_D + (-1)^D \sum_{i=1}^{D-1} i S_i S_{D-i} + R,$$

where R is a polynomial in the S_i which is isobaric of degree D and in which every monomial has usual degree at least 3.

[To see this, begin with the identity

$$\log(1/(1 - S_1 T + S_2 T^2 + ...)) = \sum_{i \geq 1} N_i T^i / i,$$

apply Td/dT to get

$$\frac{\sum_{i\geq 1}(-1)^{i+1}iS_iT^i}{1-S_1T+S_2T^2+..} = \sum_{i\geq 1} N_iT^i,$$

and expand the denominator by the geometric series.]

When $D = 2d+1$ is odd, this expression is of the form

$$N_D = DS_D - D\sum_{i=1}^{d} S_iS_{2d+1-i} + R.$$

When $D = 2d$ is even, it is of the form

$$N_D = -DS_D + dS_d^2 + D\sum_{i=1}^{d-1} S_iS_{2d-i} + R.$$

Exactly as in [Ka-NG2, 2.2-2.3], using this expression for N_D we see that when $D = 2d+1$ is odd, then $\det(-Frob)$ is equal to

$$g(\psi_D,\chi)q^d,$$

and that when $D = 2d$ is even, then $\det(-Frob)$ is equal to

$$g(\psi_{-D},\chi)g(\psi_d,\chi_2)q^{d-1}.$$

Thus when $D = 2d+1$ is odd, $\det(Frob)$ is given by

$$-g(\psi_D,\chi)q^d,$$

and when $D = 2d$, $\det(Frob)$ is given by

$$(-g(\psi_{-D},\chi))(-g(\psi_d,\chi_2))q^{d-1}$$

With our $j_!$ convention, $-g(\psi_D,\mathbb{1}) = 1$. □

Remark 2.4. The attentive reader may be disturbed by the presence of the quadratic Gauss sum in the statements of parts (1) and (2) of the previous theorem, as they make no sense in characteristic 2. But these cases concern D even, which is not allowed in characteristic 2.

3. Review of the situation in large characteristic

Suppose we fix an integer $D \geq 3$. In large (compared to D) characteristic p, the local systems $\mathcal{F}(\mathbb{F}_q,\psi,\chi,D)$ have very large geometric monodromy groups G_{arith}. Here is a precise statement.

Theorem 3.1. *Fix $D \geq 3$. We have the following results.*

(1) *If $p > 2D-1$, then for any finite field $\mathbb{F}_q$ of characteristic p and any nontrivial additive character ψ of $\mathbb{F}_q$, the local system $\mathcal{F}(\mathbb{F}_q,\psi,\mathbb{1},D)$ has $G_{geom} = Sp(D-1,\overline{\mathbb{Q}_\ell})$ if D is odd, and it has $G_{geom} = SL(D-1,\overline{\mathbb{Q}_\ell})$ if D is even.*

(2) *There is an explicit integer $M(D)$ (the integer $2DN_1(D-1)N_2(D-1)$ in* [Ka-ESDE, 7.1.1]*) such that if $p > M(D)$, then for any finite field $\mathbb{F}_q$ of characteristic p, any nontrivial additive character ψ of $\mathbb{F}_q$, and any nontrivial character χ of $\mathbb{F}_q^\times$, the local system $\mathcal{F}(\mathbb{F}_q, \psi, \chi, D)$ has G_{geom} either $SO(D, \overline{\mathbb{Q}_\ell})$ or $SL(D, \overline{\mathbb{Q}_\ell})$ or, if $D = 7$, the group $G_2(\overline{\mathbb{Q}_\ell})$ in its 7-dimensional irreducible representation.*

Proof. Case (1) is proven in [Ka-MG, Thm. 19]. For case (2), we argue as follows. Because $p > 2D$, $\mathcal{F}$ on $\mathbb{A}^1/\mathbb{F}_q$ is geometrically Lie-irreducible. Because its determinant is geometrically trivial, its G_{geom} is connected, cf. [Ka-MG, Prop. 5]. Because $\mathcal{F}$ is pure of weight one, its G_{geom} is a semisimple group. Therefore

$$G_{geom} = G^0_{geom} = (G^0_{geom})^{der}.$$

Its highest ∞-slope is $D/(D-1)$, which occurs with multiplicty $D-1$. Applying [Ka-ESDE, 7.2.7], which lists the possible $(G^0_{geom})^{der}$, we see that G_{geom} is one of the listed groups, except that we must show that if D is even, we cannot have Sp. In fact, when D is even, no $\mathcal{F}$ is self dual. Indeed, the dual of a Fourier Transform is given geometrically by

$$(FT(\mathcal{A}))^\vee \cong FT([x \mapsto -x]^\star((\mathcal{A})^\vee)).$$

So by Fourier inversion, $FT(\mathcal{A})$ is geometrically self dual if and only if there is a geometrtic isomorphism

$$\mathcal{A} \cong [x \mapsto -x]^\star((\mathcal{A})^\vee).$$

Here our $\mathcal{A}$ is $\mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)}$, so the requirement is

$$\mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D)} \cong \mathcal{L}_{\chi^{-1}(-x)} \otimes \mathcal{L}_{\psi(-(-x)^D)},$$

which is equivalent to having

$$\mathcal{L}_{\chi(x)} \otimes \mathcal{L}_{\psi(x^D+(-x)^D)} \cong \mathcal{L}_{\chi^{-1}(-x)}.$$

This is nonsense, because D is even and $p > D > 2$, so the left side has $\mathrm{Swan}_\infty = D$, while the right side is tame at ∞. □

4. Kubert's finiteness theorems: statements

In the Spring of 1986, Kubert lectured in my graduate course, proving that various Kloosterman and hypergeometric sheaves had finite geometric monodromy.

Theorem 4.1. *For any prime power q, $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, q+1)$ has finite geometric monodromy.*

Theorem 4.2. *Suppose q is odd. Then we have the following results.*

(1) $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$ *has finite geometric monodromy.*
(2) $\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ *has finite geometric monodromy.*

Theorem 4.3. *Let $n \geq 3$ be odd, q an arbitrary prime power. Then we have the following results.*

(1) $\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, (q^n+1)/(q+1))$ *has finite geometric monodromy.*
(2) *For any nontrivial multiplicative character χ of $F_{q^2}^\times$ of order dividing $q+1$, $\mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi, (q^n+1)/(q+1))$ has finite geometric monodromy.*

5. Proofs of Kubert's theorems

As explained in 2.1 above, each local system $\mathcal{F}$ on $\mathbb{A}^1$ in question is geometrically, when restricted to $\mathbb{G}_m$, the pullback by the D'th power map of an explicit hypergeometric sheaf. So to prove the theorems, it suffices to show in each case that the relevant hypergeometric sheaf has finite G_{geom}.

The proofs of Theorem 4.1 and part (1) of 4.2 are given in [Ka-G2hyper, 13.3]. To give the remaining proofs, we will make use of Kubert's V function [Ka-G2hyper, & 13]

$$V : (\mathbb{Q}/\mathbb{Z})_{\text{prime to p}} \to [0, 1),$$

giving the suitably normalized p-adic ord's of gauss sums. As explained in [Ka-G2hyper, & 13], this function has the following properties.

(1) $V(x) = 0$ if and only if $x = 0$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$.
(2) For x nonzero in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, $V(x) + V(-x) = 1$.
(3) $V(1/2) = 1/2$.
(4) For any x in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, $V(x) = V(px)$.
(5) For any x and y in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, $V(x) + V(y) \geq V(x+y)$.
(6) For any x in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, and any integer $N \geq 1$ prime to p, $\sum_{i \bmod N} V(x + i/N) = V(Nx) + (N-1)/2$.

The application of this V function to showing that a hypergeometric sheaf $\mathcal{H}$ has finite geometric monodromy (or equivalently [Ka-ESDE, 8.14.4] that after a constant α^{deg} twist to produce an $\mathcal{F}$ whose determinant is arithmetically of finite order, the resulting $\mathcal{F}$ has finite G_{arith}) is given by the following proposition, quoted from [Ka-G2hyper, 13.2].

Proposition 5.1. *Given the hypergeometric sheaf $\mathcal{H} := \mathcal{H}(\psi; \chi_i\,'s; \rho_j\,'s)$ on $\mathbb{G}_m/k$ and its twist $\mathcal{F}$, pick any multiplicative character $Teich_k$ of $k^\times$ which is faithful, i.e., has order $\#k - 1$. Define a list of $n+m$ elements $(a_1, ..., a_n, b_1, ..., b_m)$ of $(1/(\#k-1))\mathbb{Z}/\mathbb{Z}$ by*

$$\chi_i = Teich_k^{-a_i(\#k-1)}, \ \rho_j = Teich_k^{-b_j(\#k-1)}.$$

Then $\mathcal{F}$ has finite G_{arith} if and only if the following conditions hold. For every $N \in (\mathbb{Z}/(\#k-1)\mathbb{Z})^\times$, and for every $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, we have the inequality

$$\sum_i V(Na_i+x)+\sum_j V(-Nb_j-x) \geq (n-1)/2+(1/n)\sum_{i,j} V(Na_i-Nb_j).$$

When $\mathcal{H}$ is a Kloosterman sheaf of the form

$$Kl(\psi; \text{all nontrivial } \chi \text{ of order dividing } D)$$

for some prime to p integer D, the criterion is that for all $x \in (\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, we have

$$V(Dx) + 1/2 \geq V(x).$$

When $\mathcal{H}$ is a hypergeometric sheaf of the form

$$\mathcal{H}(\psi;\ \text{all } \chi \text{ of order dividing } D; \text{a single } \rho \text{ of order } M)$$

for D and M prime to p integers such that $V(aD/M) = 1/2$ for all integers a prime to M, the criterion is that

$$V(Dx) + V(a/M - x) \geq 1/2$$

for every integer a prime to M.

To prove part (2) of 4.2, we take $D = (q+1)/2$ and $M = q+1$. Here $D/M = 1/2$, so the condition $V(D/M) = 1/2$ is met. We have

$$V((q+1)/2)x) + V(a/(q+1) - x) \geq V(((q-1)/2)x + a/(q+1)),$$

by property (5) of V. Using property (4), we have

$$V(a/(q+1) - x) = V(aq/(q+1) - qx) = V(-a/(q+1) - qx),$$

the second equality because q is -1 mod $q+1$. So we also have the inequality

$$V(((q+1)/2)x)+V(a/(q+1)-x) = V(((q+1)/2)x)+V(-a/(q+1)-qx)$$
$$\geq V(((1-q)/2)x - a/(q+1).$$

Adding these inequalities, we get

$$2(V((q+1)/2)x) + V(a/(q+1) - x))$$
$$\geq V(((q-1)/2)x + a/(q+1)) + V(((1-q)/2)x - a/(q+1)).$$

For x such that $((q-1)/2)x + a/(q+1) \neq 0$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, the two arguments are nonzero negatives of each other, and by property (2) of V, they sum to 1 and we are done.

In the remaining case,

$$((q+1)/2)x = x + ((q-1)/2)x = x - a/(q+1),$$

and hence

$$V((q+1)/2)x)+V(a/(q+1)-x) = V(x-a/(q+1))+V(a/(q+1)-x),$$

which is ≥ 1 unless $x = a/(q+1)$. In that case $((q+1)/2)x = 0$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$, but this is impossible, since $a/(q+1)$ has full order $q+1$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$.

To prove part (1) of 4.3, we take $D = (q^n+1)/(q+1)$ with $n \geq 3$ odd. We must show

$$V(((q^n+1)/(q+1))x) + 1/2 \geq V(x).$$

This trivially holds for $x = 0$. For $x \neq 0$, use $V(x) = 1 - V(-x)$ to write the criterion as

$$V(((q^n+1)/(q+1))x) + V(-x) \geq 1/2, \text{ for all } x \neq 0.$$

This sum is

$$\geq V(((q^n+1)/(q+1)-1)x).$$

Replacing$V(((q^n+1)/(q+1))x)$ by $V(q((q^n+1)/(q+1))x)$, and replacing $V(-x)$ by $V(-q^n x)$, this same sum is

$$\geq V((q(q^n+1)/(q+1)-q^n)x).$$

The two quantities $((q^n+1)/(q+1)-1)x$ and $(q(q^n+1)/(q+1)-q^n)x$ are negative of each other, i.e. they sum to

$$((q+1)(q^n+1)/(q+1)-1-q^n)x = 0.$$

So we are done, unless x is such that $((q^n+1)/(q+1))x = x$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$. In that case,

$$V(((q^n+1)/(q+1))x) + V(-x) = V(x) + V(-x) = 1,$$

as $x \neq 0$.

To prove part (2) of 4.3, we take $D = (q^n+1)/(q+1)$ and we take $M = D(q+1)/m$, for m some proper divisor m of $q+1$. Then $D/M = m/(q+1)$. For any a prime to M, we have $V(aD/M) = V(am/(q+1)) = 1/2$, thanks to the Stickelberger identity [Be-Ev-Wi, 11.6.1]. We must show that

$$V(Dx) + V(a/M - x) \geq 1/2$$

for all a prime to M. This sum is

$$\geq V((D-1)x + a/M).$$

Replacing $V(Dx)$ by $V(qDx)$ and $V(a/M - x)$ by $V(q^n a/M - q^n x)$, this same sum is

$$\geq V((qD-q^n)x + q^n a/M).$$

The two quantities $(D-1)x + a/M$ and $(qD - q^n)x + q^n a/M$ are negatives of each other; they sum to

$$((q+1)D - 1 - q^n)x + (q^n+1)a/M = (q^n+1)a/M$$

$$= (q^n+1)am/(D(q+1)) = am = 0 \text{ in } (\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}.$$

So we are done unless x is such that $Dx = x - a/M$ in $(\mathbb{Q}/\mathbb{Z})_{\text{prime to p}}$. In that case,

$$V(Dx) = V(x - a/M),$$

and thus

$$V(Dx) + V(a/M - x) = V(x - a/M) + V(a/M - x).$$

So we are done unless $x = a/M$. But $Dx - a/M$, so $Dx = 0$, i.e., $D(a/M) = 0$. But

$$D(a/M) = D(am/(D(q+1))) = am/(q+1)$$

is nonzero.

This completes the proofs of Kubert's theorems.

6. Some numerology for $SL(2, \mathbb{F}_q)$

Suppose $q \geq 5$ is odd. The group $PSL(2,q) := PSL(2, \mathbb{F}_q)$ is simple, and, with the exception of $q = 9$, its Schur cover group is the double cover $SL(2,q) := SL(2, \mathbb{F}_q)$. The group $SL(2,q)$ has two irreducible representations of degree $(q-1)/2$, and two of degree $(q+1)/2$. The characters of these four representations all take values in the (ring of integers of the) field $\mathbb{Q}(\sqrt{\epsilon q})$, with $\epsilon = (-1)^{(q-1)/2}$. When q is an odd power of p, the characters of the two representations of each of the degrees $(q \pm 1)/2$ are algebraically conjugate, by the galois group of $\mathbb{Q}(\sqrt{\epsilon q})/\mathbb{Q}$.

If q is 1 mod 4, the two representations of even degree $(q-1)/2$ are both symplectically self-dual, and the two of odd degree $(q+1)/2$ are both orthogonally self-dual. Those of odd degree $(q+1)/2$ factor through $PSL(2,q)$, but not those of even degree $(q-1)/2$

If q is 3 mod 4, none of these four representations is self-dual. Those of odd degree $(q-1)/2$ factor through $PSL(2,q)$, but not those of even degree $(q+1)/2$.

7. Some numerology for $SU(\text{odd n}, \mathbb{F}_q)$

In this SU discussion, we assume throughout that $n \geq 3$ is odd. We assume further that either $q > 2$ or $n > 3$, i.e., we rule out the case of $SU(3, \mathbb{F}_2)$. The group $PSU(n,q) := PSU(n, \mathbb{F}_q)$ is simple.

The group $SU(n,q) := SU(n,\mathbb{F}_q)$ has one representation of degree $(q^n+1)/(q+1)-1$, and it has q representations of degree $(q^n+1)/(q+1)$, cf. [Hiss-Malle, Thm. 16]. The representation of degree

$$(q^n+1)/(q+1)-1$$

is symplectically self-dual. When q is odd, precisely one of the q representations of degree $(q^n+1)/(q+1)$ is self-dual, and its autoduality is orthogonal. If q is even, none of the q representations of degree $(q^n+1)/(q+1)$ is self-dual.

The representation of degree $(q^n+1)/(q+1)-1$ factors through $PSU(n,q)$. When q is odd, the unique self-dual representation of degree $(q^n+1)/(q+1)$ also factors through $PSU(n,q)$.

The order of the center of $SU(n,q)$ is $\gcd(n,q+1)$. Of the $q+1$ representations of degree either $(q^n+1)/(q+1)-1$ or $(q^n+1)/(q+1)$, precisely $(q+1)/gcd(n,q+1)$ of them factor through $PSU(n,q)$. [Notice that if $n=q+1$, then q must be even (as n is odd), and none of the q representations of of degree $(q^n+1)/(q+1)$ factors through $PSU(n,q)$.]

8. The conjectures: preparations

In this section, we refine our determinant calculations for the local systems which will figure in the conjectures.

We begin with the $SL(2)$ case.

Lemma 8.1. *Suppose q is odd. Denote by ψ_{-2} the additive character $\psi_{-2} : x \mapsto \psi(-2x)$, and define*

$$\beta := \beta(\mathbb{F}_q, \psi, (q+1)/2) := -g(\psi_{-2}, \chi_2).$$

(1) *Suppose q is 1 mod 4. Then the twisted local system*

$$\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) := (\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset Sp((q-1)/2, \overline{\mathbb{Q}_\ell}),$$

and the twisted local system

$$\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2) := \mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset SO((q+1)/2, \overline{\mathbb{Q}_\ell}).$$

(2) *Suppose q is 3 mod 4. Then the twisted local system*

$$\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) := \mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset SL((q-1)/2, \overline{\mathbb{Q}_\ell}),$$

and the twisted local system

$$\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2) := \mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset SL((q+1)/2, \overline{\mathbb{Q}_\ell}).$$

Proof. That the $\mathcal{G}$'s have arithemtically trivial determinants results from the determinant calculation, using the quadratic character of 2 to simplify the expressions. When q is 1 mod 4, the $\mathcal{G}$'s have real traces (see the lemma below) and, being pure of weight zero, are self-dual. As the $\mathcal{G}$ are irreducible, the autoduality is unique up to a scalar factor, so its sign may be read from that of its restriction to $\mathcal{F}$. Hence for $\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$, its G_{arith} lies in the symplectic group Sp, and for $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$, its G_{arith} lies in the orthogonal group O. In this latter case, because the determinant is arithemtically trivial, G_{arith} lies in the special orthogonal group SO. □

Lemma 8.2. *The trace functions of the above local systems $\mathcal{G}$ take values in $\mathbb{Q}(\sqrt{\epsilon_q q})$ for $\epsilon_q = (-1)^{(q-1)/2}$.*

Proof. For p the characteristic of $\mathbb{F}_q$, all traces a priori lie in $\mathbb{Q}(\zeta_p)$. The galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $\mathbb{F}_p^\times$, and the galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{\epsilon_p p})$ is the subgroup of squares in $\mathbb{F}_p^\times$. For χ either $\mathbb{1}$ or χ_2, and $k/\mathbb{F}_q$ a finite extension, the trace at $t \in k$ is

$$(1/g)\sum_{x\in k} \chi(x)\psi(x^{(q+1)/2} + tx),$$

with g the gauss sum $g := g(\psi_{-2}, \chi_2)$. Each of these sums is invariant under the effect of a^2, for any $a \in \mathbb{F}_p^\times$, the "trick" being that $a^2 = (a^2)^{(q+1)/2}$. Indeed, the effect of a^2 is to map this sum to

$$(1/g)\sum_{x\in k} \chi(x)\psi(a^2x^{(q+1)/2}+ta^2x) = (1/g)\sum_{x\in k} \chi(x)\psi((a^2x)^{(q+1)/2}+ta^2x) =$$

$$= (1/g)\sum_{x\in k} \chi(a^2x)\psi((a^2x)^{(q+1)/2}+ta^2x) = (1/g)\sum_{x\in k} \chi(x)\psi(x^{(q+1)/2}+tx).$$

When q is an even power of p, then any $a \in \mathbb{F}_p^\times$ becomes a square b^2 for some $b \in \mathbb{F}_q^\times$, and then each sum is invariant under a, by the substitution $x \mapsto b^2x$ (now because $b^2 = (b^2)^{(q+1)/2}$). □

We now turn to the SU(odd n) case. We assume that $n \geq 3$ is odd, and that either $q > 2$ or $n > 3$.

Lemma 8.3. *Let ψ be a nontrivial additive character of $\mathbb{F}_{q^2}$ which is obtained from a nontrivial additive character ot $\mathbb{F}_q$ by composition with* $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$.

(1) *With*

$$\beta := -q,$$

the twisted local system

$$\mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^n+1)/(q+1)) := \mathcal{F}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^n+1)/(q+1)) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset Sp((q^n+1)/(q+1)-1, \overline{\mathbb{Q}_\ell}).$$

(2) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_{q^2}^\times$ whose order m divides $q+1$. Then for*

$$\beta := -q \text{ if } q \text{ is even }, \beta := -(-1)^{(q+1)/m} q \text{ if } q \text{ is odd},$$

the twisted local system

$$\mathcal{G}(\mathbb{F}_{q^2}, \psi, \chi, (q^n+1)/(q+1)) := \mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi, (q^n+1)/(q+1)) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset SL((q^n+1)/(q+1), \overline{\mathbb{Q}_\ell}).$$

(3) *In the special case when q is odd and χ is χ_2, then β is $-(-1)^{(q+1)/2} q$ and the twisted local system*

$$\mathcal{G}(\mathbb{F}_{q^2}, \psi, \chi_2, (q^n+1)/(q+1)) := \mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi_2, (q^n+1)/(q+1)) \otimes \beta^{-deg}$$

has

$$G_{geom} \subset G_{arith} \subset SO((q^n+1)/(q+1), \overline{\mathbb{Q}_\ell}).$$

Proof. Parts (1) and (3) result from the D odd case of the determinant lemma. Here

$$D = (q^n+1)/(q+1) = 1 + q(q-1) \sum_{i=0}^{(n-3)/2} q^{2i}$$

is odd, and D is 1 mod p. In both cases, the trace function of $\mathcal{G}$ has real (in fact, integer, because $a^D = a$ for $a \in \mathbb{F}_p^\times$ and such an a is a square, indeed a $q+1$'st power, in $\mathbb{F}_{q^2}$) values. As $\mathcal{G}$ is pure of weight zero, it is self-dual, and we argue as in the proof of Lemma 8.1.

To prove (2), for ψ a nontrivial additive character of $\mathbb{F}_q$ and χ a nontrivial multiplicative character of $\mathbb{F}_{q^2}^\times$ of order m dividing $q+1$, we have the Stickelberger determination [Be-Ev-Wi, Thm. 11.6.1] of $g(\psi, \chi)$ over $\mathbb{F}_{q^2}$; it is equal to q if q is even, and to $(-1)^{(q+1)/m} q$ if q is odd. [In the cited reference, the ψ is a Ψ that comes from $\mathbb{F}_p$. So our ψ is of the form Ψ_λ for some $\lambda \in \mathbb{F}_q^\times$. But any such λ is a $q+1$'st power in $\mathbb{F}_{q^2}$ (surjectivity of the norm), so $g(\psi, \chi) = g(\Psi, \chi)$.] $\square$

9. The conjectures

Conjecture 9.1. *Suppose $q \geq 5$ is odd. Then*

(1) *For*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$$

we have $G_{geom} = G_{arith}$, and this group is the image [1] of $SL(2,q)$ in one of its irreducible representations of degree $(q-1)/2$. If we choose a nonsquare $\lambda \in \mathbb{F}_q^\times$, and replace ψ by $\psi_\lambda : x \mapsto \psi(\lambda x)$, then the group G_{geom} for

$$\mathcal{G}(\mathbb{F}_q, \psi_\lambda, \mathbb{1}, (q+1)/2)$$

is the image of $SL(2,q)$ in its other representation of degree $(q-1)/2$.

(2) *For*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$$

we have $G_{geom} = G_{arith}$, and this group is the image [2] of $SL(2,q)$ in one of its irreducible representations of degree $(q+1)/2$, If we choose a nonsquare $\lambda \in \mathbb{F}_q^\times$, and replace ψ by $\psi_\lambda : x \mapsto \psi(\lambda x)$, then the group G_{geom} for

$$\mathcal{G}(\mathbb{F}_q, \psi_\lambda, \chi_2, (q+1)/2)$$

is the image of $SL(2,q)$ in its other irreducible representation of degree $(q+1)/2$.

Conjecture 9.2. *Suppose $n \geq 3$ is odd. Then*

(1) *For*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^n+1)/(q+1))$$

we have $G_{geom} = G_{arith}$, and this group is the image[3] of $SU(n,q)$ in its unique irreducible representation of degree

$$(q^n+1)/(q+1) - 1.$$

(2) *If q is odd, then for*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \chi_2, (q^n+1)/(q+1))$$

---

[1] This image is $PSL(2,q)$ if the dimension $(q-1)/2$ is odd, otherwise it is $SL(2,q)$.

[2] This image is $PSL(2,q)$ if the dimenision $(q+1)/2$ is odd, otherwise it is $SL(2,q)$.

[3] Except in the case of $SU(3,2)$, the image group is the simple group $PSU(n,q)$. In the case of $SU(3,2)$, the group $PSU(3,2)$ is not simple, and has a quotient Q_8, the quaternion group of order eight, which is the image group.

we have $G_{geom} = G_{arith}$, and this group is the image $PSU(n,q)$ of $SU(n,q)$ in its unique self-dual irreducible representation of degree

$$(q^n+1)/(q+1).$$

(3) *Let χ be one of the q nontrivial characters χ of $\mathbb{F}_{q^2}^\times$ of order dividing $q+1$. For*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \chi, (q^n+1)/(q+1))$$

we have $G_{geom} = G_{arith}$, and this group is the image [4] of $SU(n,q)$ in precisely one of its q irreducible representations of degree

$$(q^n+1)/(q+1).$$

10. Comments on the conjectures

Suppose we use a nontrivial additive character ψ of $\mathbb{F}_q$ which comes (by composition with the trace) from a character of the prime field $\mathbb{F}_p$. Then both the local systems

$$\mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) \text{ and } \mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$$

on $\mathbb{A}^1/\mathbb{F}_q$ come, by extension of scalars, from the local systems

$$\mathcal{F}(\mathbb{F}_p, \psi, \mathbb{1}, (q+1)/2) \text{ and } \mathcal{F}(\mathbb{F}_p, \psi, \chi_2, (q+1)/2)$$

on $\mathbb{A}^1/\mathbb{F}_p$. Moreover, if we use the gauss sum $-g(\psi_{-2}, \chi_2)$ over $\mathbb{F}_p$ as the twisting factor, we get descents

$$\mathcal{G}(\mathbb{F}_p, \psi, \mathbb{1}, (q+1)/2) \text{ and } \mathcal{G}(\mathbb{F}_p, \psi, \chi_2, (q+1)/2)$$

to $\mathbb{A}^1/\mathbb{F}_p$ of the corresponding $\mathcal{G}$'s on $\mathbb{A}^1/\mathbb{F}_q$. The G_{geom} groups for the descents do not change, but their G_{arith} groups can grow. A natural guess for what they are is the following. The galois group of $\mathbb{F}_q/\mathbb{F}_p$ acts coefficientwise on the group $SL(2,q)$ and fixes the isomorphism classes of both representations of degree $(q-1)/2$ and of both representations of degree $(q+1)/2$ (because the galois action preserves each of the two conjugacy classes of unipotent elements, which are distinguished by whether the upper right entry is a square or not). So each of these representations extends to the semidirect product of $SL(2,q)$ with $Gal(\mathbb{F}_q/\mathbb{F}_p)$. The natural guess is that G_{arith} for the descended $\mathcal{G}$ is the image of this semidirect product in the corresponding representation.

[4] If $\gcd(n, q+1) = 1$, then $SU(n,q) = PSU(n,q)$ is simple, so this image is $PSU(n,q)$. When $\gcd(n, q+1) = N > 1$, so that $PSU(n,q) = SU(n,q)/\mu_N$, we conjecture the following exact determination of this image: for M the largest divisor of N for which the order of χ divides $(q+1)/M$, this image is the quotient $SU(n,q)/\mu_M$.

Similarly, when ψ starts life over $\mathbb{F}_p$, for each odd $n \geq 3$ the local system

$$\mathcal{F}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^n+1)/(q+1))$$

and, if q is odd, the local system

$$\mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi_2, (q^n+1)/(q+1))$$

descend to $\mathbb{A}^1/\mathbb{F}_p$; just replace $\mathbb{F}_{q^2}$ by $\mathbb{F}_p$ in the name. In the q odd case, using $-g(\psi_{(-1)^{(n-1)/2}}, \chi_2)$ over $\mathbb{F}_p$ as the twisting factor, we get a descent $\mathcal{G}(\mathbb{F}_p, \psi, \chi_2, (q^n+1)/(q+1))$ to $\mathbb{A}^1/\mathbb{F}_p$ of the corresponding $\mathcal{G}$. When q is 3 mod 4, this same twisting factor (or any quadratic gauss sum over $\mathbb{F}_p$) gives a descent $\mathcal{G}(\mathbb{F}_p, \psi, \mathbb{1}, (q^n+1)/(q+1))$. We do not know the "right"[5] twisting factor to use when q is not 3 mod 4. Just as in the paragraph above, the G_{geom} groups for the descents do not change, but their G_{arith} groups can grow. The galois group of $\mathbb{F}_{q^2}/\mathbb{F}_p$ acts coefficientwise on the group $SU(n,q)$ and fixes the isomorphism class of its unique irreducible representation of degree

$$(q^n+1)/(q+1) - 1$$

(precisely by the uniqueness). When q is odd, the galois action also fixes the isomorphism class of the unique orthogonal irreducible representation of degree $(q^n+1)/(q+1)$ (again by uniqueness). So each of these representations extends to the semidirect product of $SU(n,q)$ with $Gal(\mathbb{F}_q/\mathbb{F}_p)$. The natural guess is that G_{arith} for the descended $\mathcal{G}$ is the image of this semidirect product in the corresponding representation.

Once we think in terms of these descents, the following question arises. Suppose we are in a given characteristic p, and are told that one of the conjectures applies to $\mathcal{F}(\mathbb{F}_p, \mathbb{1},\ D)$ (in which case it also applies to $\mathcal{F}(\mathbb{F}_p, \chi_2, D)$ when p is odd). Can we be sure which conjecture?

Can there be more than one way of writing D as $(q^n+1)/(q+1)$ for q some power of p and n some odd integer ≥ 3. The answer is no. Begin with the identity

$$(q^n+1)/(q+1) = 1 - q + q^2 ... + q^{n-1} = 1 + q(q-1)[1 + q^2 + ... + q^{n-3}].$$

When q is p^r, the base p expansion of $q-1$ is a sequence of r digits, each $p-1$. So the base p digit expression of $(q^n+1)/(q+1) - 1$ is $(n-1)/2$ successive strings, each consisting of r digits $p-1$ followed by r digits 0. For example, in base p we have

$$(p^{15}+1)/(p^3+1) - 1 = XXX000XXX000 \text{ with } X = p-1.$$

[5]If q is p^a, we can use any $2a$'th root of $-q$ as the twisting factor, but this seems ad hoc at best.

So both r and n are determined by the base p expression of $D-1$.

When p is odd, we must also distinquish $(q^n+1)/(q+1)$, q some power of p and $n \geq 3$ odd, from $(p^a+1)/2$, $a \geq 1$. If $p \geq 5$, two such expressions can never be equal, because the first is 1 mod p and the second is $1/2$ mod p. To do the general case, subtract 1 from each and compare the base p expressions. That of $(p^a-1)/2$ consists of a sequence of a digits, each $(p-1)/2$. We must also note that if $D = (p^a + 1/2$, then p^a is determined, it is $2D-1$.

A slight variant on this question is this. Still in a fixed characteristic p, can there be more than one local system of a given rank R to which one of the conjectures applies? If R is to be either $(q^n+1)/(q+1)$ or $(q_1^m+1)/(q_1+1)-1$, we can tell which of the two, because the first is 1 mod p and the second is 0 mod p. Then looking at the base p expansion of R tells the rest. Similarly, looking at the base p expansions of $(p^a+1)/2 = (p^a-1)/2+1$ and of $(p^a-1)/2/$ allows us to separate these cases from each other and from the SU cases.

On the other hand, for a given rank, different characteristics can give rise to cases of the conjectures. For example, any time we have twin primes or twin prime powers (e.g. $9, 11$ or $23, 25$ or $27, 29$ or $79, 81$ or $81, 83$), say $q_2 = q_1 + 2$, then $\mathcal{F}(\mathbb{F}_{q_1}, \psi, \chi_2, (q_1+1)/2)$ in characteristic p_1 and $\mathcal{F}(\mathbb{F}_{q_2}, \psi, \mathbb{1}, (q_2+1)/2$ in characteristic p_2 are local systems of the same rank $(q_1+1)/2 = (q_2-1)/2$.

More interesting examples involve ranks having SL conjectures in some characteristics and SU conjectures in others. For example, with rank 6 we have

$$\mathcal{F}(\mathbb{F}_3, \psi, \mathbb{1}, (3^3+1)/(3+1))$$

in characteristic 3, and the two SL cases for the twin primes $11, 13$.

For rank 7, we have

$$\mathcal{F}(\mathbb{F}_3, \psi, \chi_2, (3^3+1)/(3+1)),$$

which has G_{geom} the image of $SU(3,3)$ in its unique orthogonal irreducible representation of degree 7, cf. [Ka-NG2, 4.15], and we have

$$\mathcal{F}(\mathbb{F}_{13}, \psi, \chi_2, (13+1)/2)$$

which has $G_{geom} = PSL(2, 13)$, cf. [Ka-NG2, 4.13]. In both of these rank 7 cases, G_{geom} is a subgroup of the exceptional group G_2.

For rank 10, we have

$$\mathcal{F}(\mathbb{F}_2, \psi, \mathbb{1}, (2^5+1)/(2+1))$$

in characteristic 2, and we have

$$\mathcal{F}(\mathbb{F}_{19}, \psi, \chi_2, (19+1)/2).$$

in characteristic 19.

For rank 11, we have

$$\mathcal{F}(\mathbb{F}_2, \psi, \chi_3, (2^5+1)/(2+1))$$

in characteristic 2, with χ_3 either of the two characters of $\mathbb{F}_4^\times$ of order 3, and we have

$$\mathcal{F}(\mathbb{F}_{23}, \psi, \mathbb{1}, (23+1)/2)$$

in characteristic 23.

For rank 12 we have

$$\mathcal{F}(\mathbb{F}_2, \psi, \mathbb{1}, (4^3+1)/(4+1))$$

in characteristic 2, and the two SL cases for the twin prime powers $23, 25$.

For rank 13 we have

$$\mathcal{F}(\mathbb{F}_2, \psi, \chi_5, (4^3+1)/(4+1))$$

in characteristic 2, with χ_5 any of the four characters of order 5 of $\mathbb{F}_{4^2}^\times$, and the two SL cases for the twin prime powers $25, 27$.

For rank 20 we have

$$\mathcal{F}(\mathbb{F}_5, \psi, \mathbb{1}, (5^3+1)/(5+1))$$

in characteristic 5, and we have

$$\mathcal{F}(\mathbb{F}_{41}, \psi, \mathbb{1}, (41+1)/2)$$

in characteristic 41.

For rank 21, we have

$$\mathcal{F}(\mathbb{F}_5, \psi, \chi_2, (5^3+1)/(5+1))$$

in characteristic 5, and the two SL cases for the twin primes $41, 43$.

For rank 993, we have

$$\mathcal{F}(\mathbb{F}_2, \psi, \chi_2, (2^{15}+1)/(2^5+1))$$

in characteristic 2, and we have

$$\mathcal{F}(\mathbb{F}_{1987}, \psi, \mathbb{1}, (1987+1)/2)$$

in characteristic 1987.

11. Verification, for $SL(2,p)$

Theorem 11.1. *Suppose q is an odd prime $p \geq 5$. Then Conjecture 9.1 for p is correct.*

Proof. Let $\mathcal{G}$ be one of the local systems in question, i.e., either

$$\mathcal{G}(\mathbb{F}_p, \psi, \mathbb{1}, (p+1)/2) \text{ or } \mathcal{G}(\mathbb{F}_p, \psi, \chi_2, (p+1)/2).$$

Its G_{geom} has order divisible by p (the wild inertia group P_∞ acts nontrivially on $\mathcal{G}$), its determinant is trivial, and it is a primitive irreducible subgroup of $SL(n, \overline{\mathbb{Q}_\ell})$ with n one of $(p\pm 1)/2$. [It is primitive because if the representation were induced, $\mathcal{G}$ would be, geometrically, the direct image of a local system on a finite etale connected covering of $\mathbb{A}^1/\overline{\mathbb{F}_p}$ of some degree $d > 1$ dividing n. But $n < p$, hence $d < p$, and $\mathbb{A}^1/\overline{\mathbb{F}_p}$ has no finite etale connected covers of degree $1 < d < p$.] The larger group G_{arith} has the same properties.

We have already seen that the trace functions of both these local systems take values in $\mathbb{Q}(\sqrt{\epsilon p})$ for $\epsilon = (-1)^{(p-1)/2}$. Because $p \geq 5$, the only roots of unity in this field are ± 1. So the only scalars which can possibly lie in G_{geom} or G_{arith} are among ± 1. As these groups are irreducible subgroups of the ambient $SL(n, \overline{\mathbb{Q}_\ell})$, we conclude that

$$Z(G_{arith}) = Z(G_{geom}) = \{1\}, \text{ if } n \text{ is odd},$$

$$Z(G_{arith}) \subset Z(G_{geom}) \subset \pm 1, \text{ , if } n \text{ is even}.$$

Consider first the case of $\mathcal{G} := \mathcal{G}(\mathbb{F}_p, \psi, \mathbb{1}, (p+1)/2)$. Here the representation has dimension $n = (p-1)/2$, and so $p = 2n+1$. By [Brauer, (2**B**),(2**C**)], both $G_{geom}/Z(G_{geom})$ and $G_{arith}/Z(G_{arith})$ are isomorphic to $PSL(2,p)$. If $n = (p-1)/2$ is odd, then the centers are trivial, and we are done. If $n = (p-1)/2$ is even, then neither center can be trivial, since $PSL(2,p)$ has no irreducible representation of degree $n = (p-1)/2$. Thus both G_{geom} and G_{arith} contain ± 1, and their quotients by ± 1 are $PSL(2,p)$. Neither G_{geom} or G_{arith} can be isomorphic to the product $\pm 1 \times PSL(2,p)$, again because $PSL(2,p)$ has no irreducible representation of degree $n = (p-1)/2$. So both G_{geom} and G_{arith} are isomorphic to the Schur double cover of $PSL(2,p)$, which is $SL(2,p)$, and again we are done.

In the case of $\mathcal{G} := \mathcal{G}(\mathbb{F}_p, \psi, \chi_2, (p+1)/2)$, the representation dimension is $n = (p+1)/2$. In this case $p = 2n-1 > n+1$ (because $p \geq 5$), and Brauer, cf. [Brauer, (2**B**)] and [Brauer2], tells us that, by a theorem of Feit [Feit], only the first power of p divides $\#G_{arith}/Z(G_{arith})$ or divides $\#G_{geom}/Z(G_{geom})$. As the centers have order dividing 2, only the first power of p divides either $\#G_{arith}$ or divides $\#G_{geom}$. Furthermore, the p-Sylow sugroups of G_{geom} are not normal subgroups. Otherwise the quotient of G_{geom} by the p-Sylow subgroup would be a prime to p quotient of $\pi_1(\mathbb{A}^1/\overline{\mathbb{F}_p})$, so trivial, hence G_{geom} would be a p-group, in fact of order p, which is nonsense, as it has an irreducible representation of degree $1 < n < p$. Because p only divides $\#G_{arith}$ to

the first power, its p-Sylows are conjugate to p-Sylows of of G_{geom}, so they are certainly not normal subgroups of G_{arith}.

This information allows us to apply a theorem of Tuan [Tuan, p. 111, first four paragraphs], which tells us that for $p > 7$, both $G_{geom}/Z(G_{geom})$ and $G_{arith}/Z(G_{arith})$ are isomorphic to $PSL(2,p)$. For $p = 5$ (respectively $p = 7$) we could also have the alternating group A_6 (respectively A_7) in addition to $PSL(2,p)$.

In the case $p = 5$, we have shown in [Ka-NG2, 3.9] that G_{geom} is $PSL(2,5) = A_5$. The group A_5 is its own normalizer in $SO(3,\overline{\mathbb{Q}_\ell})$, hence we have $G_{arith} = A_5$ as well.

In the case $p = 7$, we invoke an extraordinary isomorphism [6], where we exploit the fact that for the rank three local system

$$\mathcal{G}_3 := \mathcal{G}(\mathbb{F}_7, \psi, \mathbb{1}, 4),$$

we already know that $G_{geom} = G_{arith} = PSL(2,7)$. We wish to prove that for

$$\mathcal{G}_4 := \mathcal{G}(\mathbb{F}_7, \psi, \chi_2, 4),$$

both $G_{geom}/Z(G_{geom})$ and $G_{arith}/Z(G_{arith})$ are isomorphic to $PSL(2,7)$. The extraordinary isomorphism is

$$Sym^2(\mathcal{G}_3) \cong \Lambda^2(\mathcal{G}_4).$$

Granting this, which we will prove below, we argue as follows. The images of both $\pi_1^{geom}(\mathbb{A}^1/\mathbb{F}_7)$ and of $\pi_1^{arith}(\mathbb{A}^1/\mathbb{F}_7)$ acting on $\mathcal{G}_3$ are $PSL(2,7)$, so this is also their image acting on $Sym^2(\mathcal{G}_3)$ (the homomorphism

$$Sym^2 : SL(3,\overline{\mathbb{Q}_\ell}) \to SL(6,\overline{\mathbb{Q}_\ell})$$

is injective). Therefore their images acting on $\Lambda^2(\mathcal{G}_4)$ are also $PSL(2)$. The homomorphism

$$\Lambda^2 : SL(4,\overline{\mathbb{Q}_\ell}) \to SO(6,\overline{\mathbb{Q}_\ell})$$

(which is the spin double cover of $SO(6)$) has kernel ± 1, so the images of both $\pi_1^{geom}(\mathbb{A}^1/\mathbb{F}_7)$ and of $\pi_1^{arith}(\mathbb{A}^1/\mathbb{F}_7)$ acting on $\mathcal{G}_4$ have $G_{geom}/Z(G_{geom}) = G_{arith}/Z(G_{arith}) = PSL(2,7)$.

Once we know that both $G_{geom}/Z(G_{geom})$ and $G_{arith}/Z(G_{arith})$ are isomorphic to $PSL(2,p)$, we argue as follows.

If p is 1 mod 4, then $(p+1)/2$ is odd, and the ambient group $SO((p+1)/2,\overline{\mathbb{Q}_\ell})$ contains no scalars other than 1. So in this case the centers $Z(G_{geom})$ and $Z(G_{arith})$ are trivial, and we conclude that $G_{geom} = G_{arith} = PSL(2,p$.

[6] We will see later, in Theorem 16.4, that this isomorphism is one a panoply of such isomorphisms

If p is 3 mod 4, then $(p+1)/2$ is even, and $PSL(2,p)$ has no irreducible representation of dimension $(p+1)/2$. Therefore neither of the groups G_{geom} or G_{arith} can be either $PSL(2,p)$ or the product $\pm 1 \times PSL(2,p)$. Therefore each of these groups is the Schur double cover of $PSL(2,p)$, which is $SL(2,p)$.

It remains to show that when we choose a nonsquare $\lambda \in \mathbb{F}_p^\times$, and replace ψ by $\psi_\lambda : x \mapsto \psi(\lambda x)$, then in both cases we replace G_{geom} by the image of $SL(2,p)$ in its other representation of the same dimension. In both cases the trace functions of the two representations of the given dimension (either $(p-1)/2$ or $(p+1)/2$) are known to be galois conjugates of each other, by $Gal(\mathbb{Q}(\sqrt{\epsilon p})/Q)$. The replacement of ψ by ψ_λ performs the conjugation by the nontrivial element in this galois group. □

12. Existence of the extraordinary isomorphism

We first show the existence of a geometric isomorphism between $Sym^2(\mathcal{G}_3)$ and $\Lambda^2(\mathcal{G}_4)$. For this, we use the following.

Lemma 12.1. *Suppose $\mathcal{A}$ and $\mathcal{B}$ are $\overline{\mathbb{Q}_\ell}$ local systems on $\mathbb{A}^1/\mathbb{F}_q$ which are both pure of weight zero, and of the same rank r. Let $\lambda \in \mathbb{R}$ be an upper bound for the ∞ slopes which occur in either $\mathcal{A}$ or $\mathcal{B}$. Suppose that $\mathcal{A}$ is geometrically irreducible. Denote by $\overline{\mathcal{A}}$ the dual of $\mathcal{A}$. Then we have the following results.*

(1) *There exists a geometric isomorphism between $\mathcal{A}$ and $\mathcal{B}$ if and only the cohomology group*

$$H_c^2(\mathbb{A}^1/\overline{\mathbb{F}_q}, \overline{\mathcal{A}} \otimes \mathcal{B})$$

is nonzero, in which case it is of dimension one.

(2) *If this H_c^2 vanishes, then*

$$\dim(H_c^1(\mathbb{A}^1/\overline{\mathbb{F}_q}, \overline{\mathcal{A}} \otimes \mathcal{B})) \leq (\lambda - 1)r^2,$$

and for every finite extension field k of $\mathbb{F}_q$, we have the estimate

$$|\sum_{t \in k} \mathrm{Trace}(Frob_{t,k}|\overline{\mathcal{A}})\mathrm{Trace}(Frob_{t,k}|\mathcal{B})| \leq (\lambda - 1)r^2\sqrt{\#k}.$$

Proof. Because $\mathcal{A}$ and $\mathcal{B}$ and $\overline{\mathcal{A}} \otimes \mathcal{B}$ are pure, they are geometrically semisimple, hence the H_c^2 in question is the group $\mathrm{Hom}_{geom}(\mathcal{A}, \mathcal{B})$. Because $\mathcal{A}$ is geometrically irreducible and of the same rank as $\mathcal{B}$, any nonzero hom is automatically an isomorphism. So if this H_c^2 is nonzero, $\mathcal{B}$ is also geometrically irreducible. The one-dimensionality then follows from Schur's lemma.

If the H^2_c vanishes, then the Euler-Poincaré formula gives

$$\dim H^1_c = -\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_q}, \overline{\mathcal{A}} \otimes \mathcal{B}) = Swan(\overline{\mathcal{A}} \otimes \mathcal{B}) - \text{rank}(\overline{\mathcal{A}} \otimes \mathcal{B})$$
$$\leq \lambda r^2 - r^2 = (\lambda - 1)r^2.$$

The sum of traces

$$\sum_{t \in k} \text{Trace}(Frob_{t,k}|\overline{\mathcal{A}})\text{Trace}(Frob_{t,k}|\mathcal{B})$$

is minus the trace of $Frob_k$ on the H^1_c, so by Deligne's Weil II estimate, its absolute value is bounded by $\dim(H^1_c)\sqrt{\#k}$. □

We now apply this lemma, with $\mathcal{A} = Sym^2(\mathcal{G}_3)$ and with $\mathcal{B} = \Lambda^2(\mathcal{G}_4)$. Both are of rank 6, pure of weight zero, and with ∞-slopes $\leq 4/3$. The quantity $(\lambda - 1)r^2$ is thus 12.

To see that $Sym^2(\mathcal{G}_3)$ is geometrically irreducible, we argue as follows. We already know that G_{geom} for $\mathcal{G}_3$ is $PSL(2,7)$ in one of its three-dimensional irreducible representations, call it ρ_3. The character table of $PSL(2,7)$ shows that $Sym^2(\rho_3)$ is the unique irreducible six-dimensional representation of $PSL(2,7)$.

Calculation in Magma shows that the sum of traces over the field $k = GF(7^3)$ is approximately

$$18.466264252736530243909236483 2\sqrt{7^3}.$$

This shows that the H^2_c cannot vanish, and hence we have the asserted geometric isomorphism. Because both sides are geometrically irreducible, there exists a lisse rank one $\mathcal{L}$ on $\mathbb{A}^1/\mathbb{F}_7$ for which there exists an arithmetic isomorphism of $Sym^2(\mathcal{G}_3)$ with $\mathcal{L} \otimes \Lambda^2(\mathcal{G}_4)$. The Swan conductor at ∞ of $\mathcal{L}$ is $\leq 4/3$, hence either 0 or 1. Thus $\mathcal{L}$ is of the form $\alpha^{degree} \otimes \mathcal{L}_{\psi(at)}$ for some scalar $\alpha \in \overline{\mathbb{Q}_\ell}^\times$, and some $a \in \mathbb{F}_7$. At both the points $t = 0$ and $t = 1$, $Sym^2(\mathcal{G}_3)$ and $\Lambda^2(\mathcal{G}_4)$ have equal $\mathbb{F}_7$ traces, namely 2 and -1 respectively. So we have two equalities

$$\alpha\psi(0) = 1, \quad \alpha\psi(a) = 1.$$

Thus $\alpha = 1$ and $a = 0$, i.e., $\mathcal{L}$ is arithmetically trivial.Thus there exists an arithmetic isomorphism of $Sym^2(\mathcal{G}_3)$ with $\Lambda^2(\mathcal{G}_4)$.

13. $PGL(2,q)$ d'apres Gross, and hypergeometric sheaves

We write $PGL(2,\mathbb{F}_q) := PGL(2,q)$, q any prime power, though later we will specialize to the case q odd. In [Gross], Gross, using results of Lusztig [Lusztig], explains how to view the Deligne-Lusztig curve as a $PGL(2,q)$ torsor $\mathcal{T}$ on $\mathbb{G}_m/\mathbb{F}_q$. On $\mathcal{T}$, the inertia and wild inertia groups at 0 and ∞ are given explicitly in terms of the Borel B, its

unipotent radical U, the split torus T_{spl}, of order $q-1$, and the nonsplit torus T_{nspl}, of order $q+1$. We have

$$I_\infty = B \rhd P_\infty = U, \quad I_\infty/P_\infty = T_{spl},$$
$$I_0 = T_{nspl}, \quad P_0 = \{1\}.$$

[Concretely, the complete Deligne-Lusztig curve in this case is $\mathbb{P}^1/\mathbb{F}_q$, on which $PGL(2,q)$ acts in the usual way by fractional linear transformation. This action is free on $\mathbb{P}^1 \setminus \mathbb{P}^1(\mathbb{F}_{q^2})$. The quotient of $\mathbb{P}^1/\mathbb{F}_q$ by $PGL(2,q)$ is $\mathbb{P}^1/\mathbb{F}_q$. The map to the quotient is given explicitly, in terms of a coordinate x upstairs, by

$$x \mapsto \frac{((x^{q^2}-x)/(x^q-x))^{q+1}}{(x^q-x)^{q(q-1)}} = \frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}}.$$

It maps $\mathbb{P}^1(\mathbb{F}_q)$ to ∞, and it maps $\mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ to 0. Using the fact that $PGL(2,q)$ is generated by the transformations $x \mapsto ax, a \in \mathbb{F}_q^\times$, $x \mapsto 1/x$, and by the translations $x \mapsto x+b, b \in \mathbb{F}_q$, one checks that the map is $PGL(2,q)$-equivariant. For t in an overfield of $\mathbb{F}_q$, the fibre over t consists of the roots of the polynomial

$$f(x) := (x^q-x)^{q-1}+1)^{q+1} - t(x^q-x)^{q(q-1)}.$$

Its derivative is easily computed to be

$$f'(x) = [(x^q-x)^{q-1}+1)]^q (x^q-x)^{q-2},$$

whose only zeroes lie in $\mathbb{F}_{q^2}$, all points of which map to either ∞ (for $x \in \mathbb{F}_q$) or to 0 (for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$). Thus the map makes $\mathbb{P}^1 \setminus \mathbb{P}^1(\mathbb{F}_{q^2})$ into a finite étale covering of $\mathbb{G}_m/\mathbb{F}_q$ of degree $q(q-1)(q+1) = \#PGL(2,q)$. As the map is $PGL(2,q)$-equivariant, it must be the quotient map.]

Now take an irreducible $\overline{\mathbb{Q}_\ell}$-representation

$$\rho : PGL(2,q) \to GL(\dim(\rho), \overline{\mathbb{Q}_\ell}),$$

of dimension > 1, and denote by $\mathcal{W}_\rho$ the local system on $G_m/\mathbb{F}_q$ obtained by "pushing out" the torsor $\mathcal{T}$ by ρ. Thanks to [Gross, Corollary page 2537], we have a great deal of information. First of all, $\mathrm{Swan}_\infty(\mathcal{W}_\rho) = 1$. This fact implies that $\mathcal{W}_\rho$ is, geometrically (i.e. on $\mathbb{G}_m/\overline{\mathbb{F}_q}$), a multiplicative translate of a hypergeometric sheaf, cf. [Ka-ESDE, 8.5.3.1].

In what follows, we fix a choice of additive character ψ of $\mathbb{F}_q$, and write simply

$$\mathcal{H}(\text{character data})$$

for the hypergeometric sheaf

$$\mathrm{Hyp}(!, \psi, \text{the same character data})$$

in the notation of [Ka-ESDE, 8.2.2].

For the Steinberg representation, St of dimension q, we have $\dim((\mathcal{W}_{St})^{I_\infty}) = 1$ and $\dim((\mathcal{W}_{St})^{I_0}) = 0$. For all other irreducibles ρ of dimension > 1, we have $\dim((\mathcal{W}_\rho)^{I_\infty}) = 0$ and $\dim((\mathcal{W}_\rho)^{I_0}) = 1$.

The irreducible ρ of dimension > 1 have dimension either $q-1$, q, or $q+1$. Looking at the character table of $PGL(2,q)$, we see that the trace of a nontrivial unipotent element in one of these representations is

$$-1, \text{if } \dim(\rho) = q-1,$$
$$0, \text{if } \dim(\rho) = q,$$
$$1, \text{if } \dim(\rho) = q+1.$$

This means that, writing Reg for the regular representation of P_∞, the action of $\rho|P_\infty$ is given by

$$\mathrm{Reg} - \mathbb{1}, \text{if } \dim(\rho) = q-1,$$
$$\mathrm{Reg}, \text{if } \dim(\rho) = q,$$
$$\mathrm{Reg} + \mathbb{1}, \text{if } \dim(\rho) = q+1.$$

This in turn means that the I_∞-representation is of the form

$$\mathrm{Wild}_{q-1}, \text{if } \dim(\rho) = q-1,$$
$$\mathrm{Wild}_{q-1} \oplus (1 \text{ dim tame}),$$
$$\text{if } \dim(\rho) = q,$$
$$\mathrm{Wild}_{q-1} \oplus (2 \text{ dim tame}), \text{if } \dim(\rho) = q+1,$$

where we write Wild_{q-1} for a totally wild I_∞-representation of dimension $q-1$ and Swan 1.

The I_0-representation, being tame, consists of various characters of order dividing $q+1$. No character can occur more than once, otherwise the local monodromy at 0 will not be of finite order, cf. [Ka-ESDE, 8.4.5 (5)]. Thus our hypergeometric must be a multiplicative translate of

$$\mathcal{H}(\text{all but two char.}'\text{s of order dividing } q+1; \emptyset),$$
$$\text{if } \dim(\rho) = q-1,$$
$$\mathcal{H}(\text{all but one char. of order dividing } q{+}1; \text{one char. of order dividing } q{-}1),$$
$$\text{if } \dim(\rho) = q,$$
$$\mathcal{H}(\text{all char.}'\text{s of order dividing } q{+}1; \text{two char.}'\text{s of order dividing } q{-}1),$$
$$\text{if } \dim(\rho) = q+1.$$

These facts, together with what we already know about $\mathcal{W}_{St}$, show that $\mathcal{W}_{St}$ is, geometrically, a multiplicative translate of

$$\mathcal{H}(\text{all nontriv. char.}'\text{s of order dividing } q+1; \mathbb{1}).$$

We now bring to bear the fact that every irreducible ρ is orthogonally self-dual. Then from [Ka-ESDE, 8.8.1 and 8.8.2] we see that for any other (i.e., other than Steinberg) irreducible ρ of dimension > 1, its $\mathcal{H}$ must have

(1) In dimension $q-1$, the two omitted characters are χ, $\overline{\chi}$ with $\chi \neq \overline{\chi}$, and χ of order dividing $q+1$.
(2) in dimension q, with q odd, the omitted character is the quadratic character χ_2, and the bottom character is χ_2. [If q is even, St is the only irreducble of dimension q.]
(3) In dimension $q+1$, the two "downstairs" characters must be χ, $\overline{\chi}$ with $\chi \neq \overline{\chi}$ and χ of order dividing $q-1$.

When q is odd, there are precisely $(q-1)/2$ unordered pairs χ, $\overline{\chi}$ as in [(1)] above, and there are precisely $(q-3)/2$ unordered pairs χ, $\overline{\chi}$ as in [(3)] above. When q is even, there are $q/2$ unordered pairs χ, $\overline{\chi}$ as in [(1)] above, and there are precisely $(q-2)/2$ unordered pairs χ, $\overline{\chi}$ as in [(3)] above. These are precisely the number of irreducible ρ of dimensions $q-1$ and $q+1$ respectively. So each $\mathcal{W}_\rho$ with ρ an irreducible of dimension > 1 is, geometrically, a multiplicative translate of a hypergeometric of specified form, and every hypergeometric of that specified form is, geometrically, a multiplicative translate of a $\mathcal{W}_\rho$.

14. Descent of hypergeometric sheaves

Let us denote by

$$\mathcal{H}_{\rho-\mathrm{data}}$$

the hypergeometric sheaf

$$\mathrm{Hyp}(!, \psi, \text{character data determined by } \rho)$$

which occurs geometrically as a multiplicative translate of $\mathcal{W}_\rho$. Each such has a canonical descent to $\mathbb{G}_m/\mathbb{F}_q$, the point being that in all cases both the "upstairs" characters and the "downstairs" characters are $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-stable sets of characters. Let us call any such hypergeometric "descendable to $\mathbb{F}_q$". In the description [Ka-ESDE, 8.2] of a hypergeometric as the multiplicative convolution of a Kloosterman sheaf Kl_{up} with the "upstairs" characters with the $[x \mapsto 1/x]$ pullback of a Kloosterman sheaf $\mathrm{Kl}_{\mathrm{down}}$ with the inverses of the "downstairs" characters (and the additive character $\overline{\psi}$), both factors have canonical descents, cf. [Ka-GKM, 8.8], and the convolution of these descents is the desired descent

$$\mathcal{H}_{\rho-\mathrm{data,desc}}$$

of our $\mathcal{H}_{\rho-\mathrm{data}}$.

Lemma 14.1. *Given a hypergeometric $\mathcal{H}$ on $\mathbb{G}_m/\overline{\mathbb{F}_q}$ which is descendable to $\mathbb{F}_q$ and a character χ of $\mathbb{F}_q^\times$, the formation of the canonical descent commutes with the operation of tensoring with $\mathcal{L}_\chi$:*

$$(\mathcal{H}\otimes\mathcal{L}_\chi)_{desc}\cong\mathcal{H}_{desc}\otimes\mathcal{L}_\chi \text{ on } \mathbb{G}_m/\mathbb{F}_q.$$

In particular, if $\mathcal{H}$ is geometrically isomorphic to $\mathcal{H}\otimes\mathcal{L}_\chi$, then

$$\mathcal{H}_{desc}\cong\mathcal{H}_{desc}\otimes\mathcal{L}_\chi \text{ on } \mathbb{G}_m/\mathbb{F}_q.,$$

Proof. The second assertion is a special case of the first. The first is clear from the explicit description of the canonical descent of a descendable $\mathcal{H}$, which separately breaks the upstairs and downstairs characters into orbits under $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, and then reduces to the case of Kloosterman sheaves formed on single orbit, i.e., those of the form

$$\mathrm{Kl}(\Lambda,\Lambda^q,...,\Lambda^{q^{r-1}})$$

for some $r\geq 1$ and some character Λ of $\mathbb{F}_{q^r}$ which has r distinct galois conjugates under the action of $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$. □

At the same time, we have the local system $\mathcal{W}_\rho$ on $\mathbb{G}_m/\mathbb{F}_q$ with which we began. It is geometrically isomorphic to a multiplicative translate of $\mathcal{H}_{\rho-\mathrm{data},desc}$. Recall from [Ka-ESDE, 8.5.4] that a hypergeometric sheaf is isomorphic to no nontrivial translate of itself. That the translation is by a point of $\mathbb{G}_m(\mathbb{F}_q)$ results from the following rationality lemma.

Lemma 14.2. *Let k be a perfect field, G/k a smooth, geometrically connected group scheme, ℓ a prime invertible in k, and $\mathcal{A}$ and $\mathcal{B}$ two $\overline{\mathbb{Q}_\ell}$ local systems on G which are both geometrically irreducible. Suppose that*

1. *The local system $\mathcal{B}$ is not geometrically isomorphic to any nontrivial (i.e. by a point of $G(\overline{k})$ other than the identity) translate of itself.*
2. *The local system $\mathcal{A}$ is geometrically isomorphic to a translate of $\mathcal{B}$.*

Then there is a unique point $\gamma\in G(\overline{k})$ such $\mathcal{A}$ is geometrically isomorphic to the translate $[g\mapsto\gamma g]^\star(\mathcal{B})$, and this point γ lies in $G(k)$.

Proof. The uniqueness is obvious, from condition (1). Now consider the local system $\mathcal{C}$ on $G\times_k G$, coordinates (t,g), given by

$$\mathcal{C}(t,g)=(\mathcal{A}(g))^\vee\otimes\mathcal{B}(tg).$$

In fancier terms, we have the multiplication map $m: G\times_k G\to G, (t,g)\mapsto tg$, and our $\mathcal{C}$ is

$$\mathcal{C}:=pr_2^\star(\mathcal{A}^\vee)\otimes m^\star(\mathcal{B}).$$

For d the relative dimension of G over k, the sheaf $R^{2d}(pr_1)_!(\mathcal{C})$ on G is supported at γ. Therefore γ is rational over the perfection of k. As k is perfect, γ lies in $G(k)$. □

Thus there exists a unique $a_\rho \in k^\times$ such that there exists a geometric isomorphism

$$\mathcal{W}_\rho \cong [x \mapsto a_\rho x]_\star \mathcal{H}_{\rho-\mathrm{data},desc} := \mathcal{H}_{a_\rho,\rho-\mathrm{data},desc}.$$

As both are geometrically isomorphic, there exists a unique $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$ such that on $\mathbb{G}_m/\mathbb{F}_q$ we have an arithmetic isomorphism

$$\mathcal{W}_\rho \cong \mathcal{H}_{a_\rho,\rho-\mathrm{data},desc} \otimes \alpha_\rho^{deg}.$$

Theorem 14.3. *For each irreducible representation ρ of $PGL(2,q)$ of dimension > 1, the local system*

$$\mathcal{H}_\rho := \mathcal{H}_{a_\rho,\rho-\mathrm{data},desc} \otimes \alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ has $G_{geom} = G_{arith} =$ the image of $PGL(2,q)$ *in the corresponding representation ρ.*

Proof. The statement is tautologically true for the local system $\mathcal{W}_\rho$. □

15. Pulling back from $PGL(2,q)$ to $PSL(2,q)$

In this section, we assume that q is odd. Then $PSL(2,q)$ is a subgroup of index two in $PGL(2,q)$. If we think of the Galois theory diagram of the geometric covering $\mathcal{T} \to \mathbb{G}_m/\mathbb{F}_q$ as a finite etale covering with group $PGL(2,q)$, then we have a diagram

$$\mathcal{T} \to S \to \mathbb{G}_m/\mathbb{F}_q$$

in which $\mathcal{T} \to S$ is a $PSL(2,q)$ torsor, and $S \to \mathbb{G}_m/\mathbb{F}_q$ is a finite etale covering of degree two. As Gross explains in [Gross, bottom of p. 2537], this last covering is the squaring map

$$[2] : x \mapsto x^2$$

of $\mathbb{G}_m/\mathbb{F}_q$ as a covering of itself. What this means concretely is that for ρ an irreducible representation of $PGL(2,q)$ of dimension > 1, its restriction to $PSL(2,q)$ is given by the local system on $\mathbb{G}_m/\mathbb{F}_q$ which is the pullback $[2]^\star\mathcal{W}_\rho$.

Let us recall the following irreducibility lemma, which we will apply both with $k = \overline{\mathbb{F}_q}$ and with $k = \mathbb{F}_q$.

Lemma 15.1. *Let $\ell \neq p$, p odd, k a field of characteristic p, and $\mathcal{H}$ a lisse $\overline{\mathbb{Q}_\ell}$-sheaf on $\mathbb{G}_m/k$ which is irreducible. Then*

(1) *$[2]^\star\mathcal{H}$ is irreducible if and only if $\mathcal{H}$ is not isomorphic to $\mathcal{H}\otimes\mathcal{L}_{\chi_2}$.*

(2) *If $\mathcal{H}$ is isomorphic to $\mathcal{H}\otimes\mathcal{L}_{\chi_2}$, then $[2]^\star\mathcal{H}$ is isomorphic to a direct sum $\mathcal{A}\oplus\mathcal{B}$, with $\mathcal{B}=[x\mapsto -x]^\star\mathcal{A}$.*

Proof. We use Frobenius reciprocity to compute

$$< [2]^\star\mathcal{H}, [2]^\star\mathcal{H} >=< \mathcal{H}, [2]_\star[2]^\star\mathcal{H} >=< \mathcal{H}, \mathcal{H}\otimes [2]_\star\overline{\mathbb{Q}_\ell} >=$$

$$=< \mathcal{H}, \mathcal{H}\otimes(\overline{\mathbb{Q}_\ell}\oplus\mathcal{L}_{\chi_2}) >=< \mathcal{H}, \mathcal{H} > + < \mathcal{H}, \mathcal{H}\otimes\mathcal{L}_{\chi_2} > .$$

This makes (1) obvious. If we are in situation (2), then $< [2]^\star\mathcal{H}, [2]^\star\mathcal{H} >= 2$, hence $[2]^\star\mathcal{H}$ is $\mathcal{A}\oplus\mathcal{B}$ with $\mathcal{A}$ not isomorphic to $\mathcal{B}$ (otherwise $[2]^\star\mathcal{H}$ is $\mathcal{A}\oplus\mathcal{A}$, in which case $< [2]^\star\mathcal{H}, [2]^\star\mathcal{H} >$ would be 4). Let $\mathcal{A}$ have $\mathrm{rank}(\mathcal{A})\leq\mathrm{rank}(\mathcal{B})$. Then

$$< \mathcal{H}, [2]_\star\mathcal{A} >=< [2]^\star\mathcal{H}, \mathcal{A} >= 1,$$

so $\mathcal{H}$ occurs in $[2]_\star\mathcal{A}$. But as $\mathrm{rank}(\mathcal{A})\leq\mathrm{rank}(\mathcal{B})$, we have $\mathrm{rank}(\mathcal{H})\geq\mathrm{rank}([2]_\star\mathcal{A})$. Therefore we have $\mathcal{H}\cong[2]_\star\mathcal{A}$. In particular, $\mathcal{H}$ has even rank and $\mathcal{A}$ has rank half that of $\mathcal{H}$. [The same argument then applies to $\mathcal{B}$, and so $\mathcal{H}\cong[2]_\star\mathcal{B}$.] Then

$$[2]^\star\mathcal{H}\cong[2]^\star[2]_\star\mathcal{A}\cong\mathcal{A}\oplus[x\mapsto -x]^\star\mathcal{A}.$$

□

We now apply this to the hypegeometric sheaves

$$\mathcal{H}_\rho := \mathcal{H}_{a_\rho,\rho-\mathrm{data},desc}\otimes\alpha_\rho^{deg},$$

which give the $\mathcal{W}_\rho$.

Those of rank $q-1$ are, geometrically,

$$\mathcal{H}_{a_\rho}(\text{all char.}'\text{s of order dividing } q+1 \text{ save } \chi,\overline{\chi})$$

with $\chi\neq\overline{\chi}$ of order dividing $q+1$. This will have its [2] pullback irreducible unless the unordered pair $\{\chi,\overline{\chi}\}$ is equal to the unordered pair $\{\chi\chi_2,\overline{\chi}\chi_2\}$. This equality can only hold if χ has order 4, which is only allowed if q is 3 mod 4.

Those of rank $q+1$ are, geometrically,

$$\mathcal{H}_{a_\rho}(\text{all char.}'\text{s of order dividing } q+1;\chi,\overline{\chi})$$

with $\chi\neq\overline{\chi}$ of order dividing $q-1$. This will have its [2] pullback irreducible unless the unordered pair $\{\chi,\overline{\chi}\}$ is equal to the unordered pair $\{\chi\chi_2,\overline{\chi}\chi_2\}$. This equality can only hold if χ has order 4, which is only allowed if q is 1 mod 4.

Thus we have the following theorem.

Theorem 15.2. *For q odd, we have the following results.*

(1a) *Suppose q is 1 mod 4. Then the* [2] *pullback of*

$$\mathcal{H}_{a_\rho,desc}(\text{all char.'s of order dividing } q+1;\chi_4,\overline{\chi}_4)\otimes\alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ is the direct sum $\mathcal{A}\oplus[x\mapsto -x]^\star\mathcal{A}$ with $\mathcal{A}$ geometrically a unique multiplicative translate (necessarily by a point of $\mathbb{G}_m(\mathbb{F}_q)$, cf. 14.2) of the hypergeometric sheaf

$$\mathcal{H}(\text{all char.'s of order dividing } (q+1)/2;\chi_2).$$

$\mathcal{A}$ and $[x\mapsto -x]^\star\mathcal{A}$ are local systems on $\mathbb{G}_m/\mathbb{F}_q$ giving the two representations of $PSL(2,q)$ of dimension $(q+1)/2$. Each has $G_{geom}=G_{arith}=PSL(2,q)$.

(1b) *Suppose q is 1 mod 4. Then every other W_ρ of rank >1 pulls back by* [2] *to an irreducible local system. Of these, $\mathcal{W}_\rho$ and $\mathcal{W}_\rho\otimes\mathcal{L}_{\chi_2}$ have the same pullback. So we get $(q-5)/4$ irreducible pullbacks of rank $q+1$, we get $(q-1)/4$ irreducible pullbacks of rank $q-1$, and we get one irreducible pullback of rank q. These local systems give all the irreducible representations of $PSL(2,q)$ of dimension $q+1, q-1,$ or q.*

(2a) *Suppose q is 3 mod 4. Then the* [2] *pullback of*

$$\mathcal{H}_{a_\rho,desc}(\text{all char.'s of order dividing } q+1 \text{ save } \chi_4,\overline{\chi_4})\otimes\alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ is the direct sum $\mathcal{A}\oplus[x\mapsto -x]^\star\mathcal{A}$ with $\mathcal{A}$ geometrically a unique multiplicative translate (necessarily by a point of $\mathbb{G}_m(\mathbb{F}_q)$, cf. 14.2) of the hypergeometric sheaf

$$\mathcal{H}(\text{all char.'s of order dividing } (q+1)/2 \text{ save } \chi_2).$$

$\mathcal{A}$ and $[x\mapsto -x]^\star\mathcal{A}$ are local systems giving the two representations of $PSL(2,q)$ of dimension $(q-1)/2$ Each has $G_{geom}=G_{arith}=PSL(2,q)$..

(2b) *Suppose q is 3 mod 4. Then every other W_ρ of rank >1 pulls back by* [2] *to an irreducible local system. Of these, $\mathcal{W}_\rho$ and $\mathcal{W}_\rho\otimes\mathcal{L}_{\chi_2}$ have the same pullback. So we get $(q-3)/4$ irreducible pullbacks of rank $q+1$, we get $(q-3)/4$ irreducible pullbacks of rank $q-1$, and we get one irreducible pullback of rank q. These local systems give all the irreducible representations of $PSL(2,q)$ of dimension $q+1, q-1,$ or q.*

Taking into account [Ka-ESDE, 9.3.2], we get the following theorem. Let us write $\mathrm{Kl}(\chi,\overline{\chi})$ for the Kloosterman sheaf $\mathrm{Kl}(!,\psi;\chi,\overline{\chi})$

Theorem 15.3. *Suppose $q>3$ (so that $PSL(2,q)$ is a simple group). We have the following results.*

(1) *Let $\chi \neq \overline{\chi}$ be characters of order dividing $q+1$, with $\chi^4 \neq \mathbb{1}$. Then*

$$FT([q+1]^\star \mathrm{Kl}(\chi, \overline{\chi}))$$

is an irreducible rigid local system of rank $q-1$ on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose G_{geom} is the group $PSL(2,q)$. For a unique $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$, the local system

$$FT([q+1]^\star \mathrm{Kl}(\chi, \overline{\chi})_{desc}) \otimes \alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ has $G_{geom} = G_{arith} = PSL(2,q)$.

(2) *The irreducible rigid local system of rank q on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ given by*

$$FT([q+1]^\star \mathrm{Kl}(\mathbb{1}, \mathbb{1}))$$

has G_{geom} the group $PSL(2,q)$ in the Steinberg representation. For s unique $\alpha_{St} \in \overline{\mathbb{Q}_\ell}^\times$, the local system

$$FT([q+1]^\star \mathrm{Kl}(\mathbb{1}, \mathbb{1})_{desc}) \otimes \alpha_{St}^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ has $G_{geom} = G_{arith} = PSL(2,q)$.

(3) *Let $\chi \neq \overline{\chi}$ be characters of order dividing $q-1$, with $\chi^4 \neq \mathbb{1}$. Then*

$$FT([q+1]^\star \mathrm{Kl}(\chi, \overline{\chi}))$$

is an irreducible rigid local system of rank $q+1$ on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose G_{geom} is the group $PSL(2,q)$. For s unique $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$, the local system

$$FT([q+1]^\star \mathrm{Kl}(\chi, \overline{\chi}))_{desc}) \otimes \alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ has $G_{geom} = G_{arith} = PSL(2,q)$.

(4) *If q is 1 mod 4, then*

$$FT([(q+1)/2]^\star \mathrm{Kl}(\chi_2)) = FT(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(x^{(q+1)/2})})$$

is an irreducible rigid local system of rank $(q+1)/2$ on $\mathbb{A}^1/\overline{\mathbb{F}_q}$ whose G_{geom} is the group $PSL(2,q)$. For s unique $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$, the local system

$$FT(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(x^{(q+1)/2})}) \otimes \alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ has $G_{geom} = G_{arith} = PSL(2,q)$.

(5) *If q is 3 mod 4, so that $(q+1)/2$ is even and hence*

$$[(q+1)/2]^\star \mathrm{Kl}(\chi_2) = [(q+1)/2]^\star \mathrm{Kl}(\mathbb{1}),$$

then

$$FT([(q+1)/2]^\star \mathrm{Kl}(\chi_2)) = FT([(q+1)/2]^\star \mathrm{Kl}(\mathbb{1})) = FT(\mathcal{L}_{\psi(x^{(q+1)/2})})$$

is an irreducible rigid local system of rank $(q-1)/2$ *on* $\mathbb{A}^1/\overline{\mathbb{F}_q}$ *whose* G_{geom} *is the group* $PSL(2,q)$. *For* s *unique* $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$, *the local system*

$$FT(\mathcal{L}_{\psi(x^{(q+1)/2})}) \otimes \alpha_\rho^{deg}$$

on $\mathbb{G}_m/\mathbb{F}_q$ *has* $G_{geom} = G_{arith} = PSL(2,q)$.

(6) *If in (4) and (5) we replace* ψ *by* $\psi_a : x \mapsto \psi(ax)$ *with* $a \in \mathbb{F}_q^\times$ *a non-square, then we obtain a local system whose monodromy representation is the other irreducible of dimension* $(q+1)/2$ *if* q *is* 1 *mod* 4 *(respectively of dimension* $(q-1)/2$ *if* q *is* 3 *mod* 4*).*

(7) *The monodromy representations of the aforementioned local systems provide all the irreducible representations of* $PSL(2,q)$ *of dimension* > 1.

Proof. If we translate a local system on $\mathbb{G}_m/\mathbb{F}_q$ by a point of $\mathbb{G}_m(\mathbb{F}_q)$, we change neither G_{geom} nor G_{arith}. This allows us to ignore the the unique translations by points of $\mathbb{G}_m(\mathbb{F}_q)$ in the statement of the previous theorem. Assertions (1) through (5), and (7), then result from the previous theorem, together with [Ka-ESDE, 9.3.2 (1)], according to which

$$FT([q+1]^\star \mathrm{Kl}(\chi, \overline{\chi}))$$

is a multiplicative translate (by a point of $\mathbb{G}_m(\mathbb{F}_p)$) of

$$[q+1]^\star \mathbf{Cancel}(\mathcal{H}(\text{all char.}'\text{s of order divding } q+1; \chi, \overline{\chi})),$$

and, when q is odd,

$$FT([(q+1)/2]^\star \mathrm{Kl}(\chi_2))$$

is a multiplicative translate (by a point of $\mathbb{G}_m(\mathbb{F}_p)$) of

$$[(q+1)/2]^\star \mathbf{Cancel}(\mathcal{H}(\text{all char.}'\text{s of order divding } (q+1)/2; \chi_2)).$$

When q is even, the groups $PGL(2,q)$, $PSL(2,q)$, and $SL(2,q)$ all coincide, and the pullback by $[q+1]^\star$ can only shrink G_{geom} to a normal subgroup of itself of index dividing $q+1$. But for $q \geq 4$, $PGL(2,q)$ is simple, of order $(q-1)q(q+1) > q+1$.

When q is odd, then already in the first case

$$[2]^\star \mathbf{Cancel}(\mathcal{H}(\text{all char.}'\text{s of order divding } q+1; \chi, \overline{\chi}))$$

has $PSL(2,q)$ as its G_{geom}, and its further pullback by [(q+1)/2] can only shrink G_{geom} to a normal subgroup of $PSL(2,q)$ of index dividing $(q+1)/2$. But for $q > 3$, $PSL(2,q)$ is simple, of order $(q-1)q(q+1)/2 > (q+1)/2$. In the second case, we know that

$$\mathbf{Cancel}(\mathcal{H}(\text{all char.}'\text{s of order divding } (q+1)/2; \chi_2))$$

has $G_{geom} = PSL(2,q)$, and just as above the pullback by [(q+1)/2] can shrink it no more.

It remains to explain, in (6), why replacing ψ by $\psi_a : x \mapsto \psi(ax)$ with $a \in \mathbb{F}_q^\times$ a non-square provides the other representation of dimension equal to whichever of $(q \pm 1)/2$ is odd. For this, we may suppose ψ is a character of $\mathbb{F}_p$.

Suppose first that q is not a square, i.e., that q is an odd power of p. Then we may take for a a nonsquare in $\mathbb{F}_p^\times$. In this case, the trace function using ψ_a will be the galois conjugate, by the nontrivial element of $Gal(\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})/\mathbb{Q})$ of the trace function using ψ. One knows that this galois conjugation interchanges the two representations of dimension equal to whichever of $(q \pm 1)/2$ is odd.

Suppose now that q is a square. Then $(q+1)/2$ is odd, and both representations of dimension $(q+1)/2$ have $\mathbb{Z}$-valued trace functions, so galois conjugation is not available. But recall that the two representations of this dimension are given by the local systems

$$\mathcal{A} \cong \mathcal{H}(\text{all char.'s of order dividing } (q+1)/2; \chi_2)$$

and $[x \mapsto -x]^\star \mathcal{A}$. Because $(q+1)/2$ is odd, the two pullbacks $[(q+1)/2]^\star$ and $[x \mapsto -x]^\star$ commute with each other, i.e.,

$$(-x)^{(q+1)/2} = -x^{(q+1)/2}.$$

Consider now the local systems

$$\mathcal{K} := FT_\psi(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(x^{(q+1)/2})}) = [(q+1)/2]^\star \mathcal{A}$$

and

$$\mathcal{K}_a := FT_{\psi_a}(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi_a(x^{(q+1)/2})}).$$

Over extension fields $k/\mathbb{F}_q$ in which a is a square, the trace function of $\mathcal{K}$ is given by

$$t \mapsto -\sum_{x \in k^\times} \chi_2(x)\psi(x^{(q+1)/2} + tx).$$

The trace function of $\mathcal{K}_a$ is given by

$$t \mapsto -\sum_{x \in k^\times} \chi_2(x)\psi(ax^{(q+1)/2} + tax) =$$

(making the substitution $x \mapsto x/a$, which turns $ax^{(q+1)/2}$ into $-x^{(q+1)/2}$)

$$= -\sum_{x \in k^\times} \chi_2(x)\psi(-x^{(q+1)/2} + tx) =$$

(making the substitution $x \mapsto -x$)

$$= -\sum_{x \in k^\times} \chi_2(x)\psi(x^{(q+1)/2} - tx),$$

which is the trace function of

$$[t \mapsto -t]^\star[(q+1)/2]^\star\mathcal{A} = [(q+1)/2]^\star[x \mapsto -x]^\star\mathcal{A},$$

the pullback by $[(q+1)/2]$ of the other representation of the same dimension. □

16. Transition from $PSL(2,q)$ to $SL(2,q)$

In this section, we return to our focus on the local systems

$$\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) \text{ and } \mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$$

on $\mathbb{A}^1/\mathbb{F}_q$. We begin by applying the relevant result of the previous section.

Theorem 16.1. *Suppose $q > 3$. Then we have the following results.*

(1) *If q is 1 mod 4, the local system $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ has*

$$G_{geom} = G_{arith} = PSL(2,q)$$

in one of the irreducible representations of $PSL(2,q)$ of dimension $(q+1)/2$. If we replace ψ by ψ_a for $a \in \mathbb{F}_q^\times$ a nonsquare, we get the other irreducible representations of $PSL(2,q)$ of dimension $(q+1)/2$.

(2) *If q is 3 mod 4, the local system $\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$ has*

$$G_{geom} = G_{arith} = PSL(2,q).$$

in one of the irreducible representations of $PSL(2,q)$ of dimension $(q-1)/2$. If we replace ψ by ψ_a for $a \in \mathbb{F}_q^\times$ a nonsquare, we get the other irreducible representations of $PSL(2,q)$ of dimension $(q-1)/2$.

Proof. The statements about G_{geom} were proven in 15.3, parts (4) and (5), as are the statements about the effect on G_{geom} of replacing ψ by ψ_a. What remains to show is that the scaling factor α_ρ in the statement of 15.3 is the same scaling factor used in defining $\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$ and $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$. In other words, we know that, in each of (1) and (2), there is a unique scalar α such that $\mathcal{G} \otimes \alpha^{deg}$ has $G_{geom} = G_{arith} = PSL(2,q)$. What we must show is that in each case that scalar is 1.

We begin with case (1). Here G_{arith} for $\mathcal{G}$ lies in $SO((q+1)/2, \overline{\mathbb{Q}_\ell})$, as does $G_{arith} = PSL(2,q)$ for $\mathcal{G} \otimes \alpha^{deg}$ in either of its irreducible representations of dimension $(q+1)/2$. Therefore the scalar α itself lies in $SO((q+1)/2, \overline{\mathbb{Q}_\ell})$. But as $(q+1)/2$ is odd in this case, the only such scalar is 1.

In case (2), G_{arith} for $\mathcal{G}$ lies in $SL((q-1)/2, \overline{\mathbb{Q}_\ell})$, as does $G_{arith} = PSL(2,q)$ for $\mathcal{G} \otimes \alpha^{deg}$ in one of its irreducible representations of dimension $(q-1)/2$. Therefore the scalar α itself lies in $SL((q+1)/2, \overline{\mathbb{Q}_\ell})$. The only such scalars are roots of unity of order dividing the odd integer $(q-1)/2$. The only scalar in (the image of) $G_{arith} = PSL(2,q)$ for $\mathcal{G} \otimes \alpha^{deg}$ (in either of the irreducible representations of dimension $(q-1)/2$ of $PSL(2,q)$) is 1.Therefore α lies in the image of G_{arith} for $\mathcal{G}$.

Because q is 3 mod 4, q is an odd power of a prime p which is 3 mod 4. The representation for $\mathcal{G}$ has its character with values in $\mathbb{Q}(\sqrt{-p})$, so the only scalars in the image of G_{arith} for $\mathcal{G}$ are roots of unity in this field. If $p \geq 5$, the only roots of unity in this field are ± 1. Of these, only 1 has order dividing the odd integer $(q-1)/2$, If $p = 3$, the roots of unity in this field are μ_6. For $q = 3^{2k+1}$ (with $k \geq 1$ because $q > 3$ by hypothesis), we have $\gcd(6, (q-1)/2) = 1$. □

$$Sym^2(\mathcal{G}(\mathbb{F}_q, \psi_a, \mathbb{1}, (q+1)/2)) \cong \Lambda^2(\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)).$$

The situation now is that for each odd $q > 3$, we have proven the $SL(2,q)$ conjecture for whichever of the two local systems

$$\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2) \text{ and } \mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$$

has odd rank. However, there is a simple relation between these two local systems, which will, in the next section, allow us to prove the $SL(2,q)$ conjecture for the one of even rank. We state this relation in the following two theorems. The proof of the second is due to Ron Evans.

Theorem 16.2. *Let q be odd. Suppose q is ± 1 mod 8, i.e., that 2 is a square in $\mathbb{F}_q^\times$. Then there exists an isomorphism of local systems on $\mathbb{G}_m/\mathbb{F}_q$*

$$Sym^2(\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)) \cong \Lambda^2(\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)).$$

Theorem 16.3. (Evans)*Let q be odd. Suppose 2 is not a square in $\mathbb{F}_q^\times$. Then for any nonsquare $a \in \mathbb{F}_q^\times$, there exists an isomorphism of local systems on $\mathbb{G}_m/\mathbb{F}_q$*

$$Sym^2(\mathcal{G}(\mathbb{F}_q, \psi_a, \mathbb{1}, (q+1)/2)) \cong \Lambda^2(\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)).$$

Remark 16.4. The formulation of the above theorems is motivated by the following facts. The group $SL(2,q)$, $q > 3$ odd, has two irreducible representations of dimension $(q-1)/2$, Small_1 and Small_2, and two irreducible representations of dimension $(q+1)/2$, Large_1 and Large_2.

They can be numbered so that on nontrivial unipotent elements $g \in SL(2,q)$, we have

$$\mathrm{Trace}(\mathrm{Small}_1(g)) = -\mathrm{Trace}(\mathrm{Large}_1(g)),$$
$$\mathrm{Trace}(\mathrm{Small}_2(g)) = -\mathrm{Trace}(\mathrm{Large}_2(g)).$$

With this numbering, it is easy to see from the character table that there exist isomorphisms of representations

$$Sym^2(\mathrm{Small}_i) \cong \Lambda^2(\mathrm{Large}_i)$$

for $i = 1$ and for $i = 2$. Moreover, if 2 is a square in $\mathbb{F}_q^\times$, so that squaring maps each of the two unipotent conjugacy classes to itself (rather than to the other one), then there exist isomorphisms of representations

$$Sym^2(\mathrm{Small}_i) \cong \Lambda^2(\mathrm{Large}_j)$$

for any choices of i, j in $\{1,2\}$. In all these cases, the isomorphism exists (only) because the characters coincide. A beautiful generalization of this result to $Sp(2n,q)$ is due to Guralnick, Maagard, and Tiep [GMT].

Proof of Theorem 16.2 Let us recall the statement. Suppose q is ± 1 mod 8. Then there exists an isomorphism of local systems on $\mathbb{G}_m/\mathbb{F}_q$

$$Sym^2(\mathcal{G}(\mathbb{F}_q,\psi,\mathbb{1},(q+1)/2)) \cong \Lambda^2(\mathcal{G}(\mathbb{F}_q,\psi,\chi_2,(q+1)/2)).$$

Proof. Because both inputs are irreducible, their Λ^2 and Sym^2 are semisimple, so by Chebotarev it suffices to show that both sides have the same trace function. Thus k is a finite extension of $\mathbb{F}_q$, and k_2/k is its quadratic extension. Let us denote

$$\mathcal{G}_{sm} := (\mathcal{G}(\mathbb{F}_q,\psi,\mathbb{1},(q+1)/2)), \quad \mathcal{G}_{lg} := \mathcal{G}(\mathbb{F}_q,\psi,\chi_2,(q+1)/2).$$

Then for $t \in k$,

$$2\times\mathrm{Trace}(Frob_{k,t}|Sym^2(\mathcal{G}_{sm})) = (\mathrm{Trace}(Frob_{k,t}|\mathcal{G}_{sm}))^2 + \mathrm{Trace}(Frob_{k_2,t}|\mathcal{G}_{sm}),$$
$$2\times\mathrm{Trace}(Frob_{k,t}|\Lambda^2(\mathcal{G}_{lg})) = (\mathrm{Trace}(Frob_{k,t}|\mathcal{G}_{lg}))^2 - \mathrm{Trace}(Frob_{k_2,t}|\mathcal{G}_{lg}).$$

The local systems $\mathcal{G}_{sm}$ and $\mathcal{G}_{lg}$ have the same twisting factor $\beta = -g(\psi_{-2},\chi_2)$ in their definitions, so it suffices to prove this equality with $\mathcal{G}_{sm}$ replaced by

$$\mathcal{F}_{sm} := FT_\psi(\mathcal{L}_{\psi(x^{(q+1)/2})})$$

and with $\mathcal{G}_{lg}$ replaced by

$$\mathcal{F}_{lg} := FT_\psi(\mathcal{L}_{\chi_2(x)} \otimes \mathcal{L}_{\psi(x^{(q+1)/2})}).$$

Thus we must show that

$$(-\sum_{x\in k}\psi_k(x^{(q+1)/2}+tx))^2 + (-\sum_{x\in k_2}\psi_{k_2}(x^{(q+1)/2}+tx)) =$$

$$= (-\sum_{x\in k} \chi_{2,k}(x)\psi_k(x^{(q+1)/2}+tx))^2 - (-\sum_{x\in k_2} \chi_{2,k_2}(x)\psi_{k_2}(x^{(q+1)/2}+tx)).$$

For this, we break the sum $\sum_{x\in k} \chi_{2,k}(x)\psi_k(x^{(q+1)/2}+tx)$ into the two obvious pieces

$$\sum_{x\in k} \chi_{2,k}(x)\psi_k(x^{(q+1)/2}+tx) =$$

$$= \sum_{x\in k^\times \text{ a square}} \psi_k(x^{(q+1)/2}+tx) - \sum_{x\in k^\times \text{ a nonsquare}} \psi_k(x^{(q+1)/2}+tx).$$

Choose a nonsquare $\delta \in k^\times$. Then the squares are of the form x^2 and the nonsquares of the form δx^2, with $x \in k^\times$. So this difference is

$$(1/2)\sum_{x\in k} \psi(x^{q+1}+tx^2) - (1/2)\sum_{x\in k} \psi(\delta^{(q+1)/2}x^{q+1}+t\delta x^2),$$

the $x=0$ terms cancelling. Let us name these sums. We define

$$S(a,b) := \sum_{x\in k} \psi(ax^{q+1}+bx^2).$$

So this difference is

$$(1/2)S(1,t) - (1/2)S(\delta^{(q+1)/2},\delta t).$$

On the other hand, the sum $-\sum_{x\in k} \psi_k(x^{(q+1)/2}+tx)$ is equal to

$$(1/2)S(1,t) + (1/2)S(\delta^{(q+1)/2},\delta t).$$

So what we must show is

$$((1/2)S(1,t) + (1/2)S(\delta^{(q+1)/2},\delta t))^2 - \sum_{x\in k_2} \psi_{k_2}(x^{(q+1)/2}+tx) =$$

$$= ((1/2)S(1,t) - (1/2)S(\delta^{(q+1)/2},\delta t))^2 + \sum_{x\in k_2} \chi_{2,k_2}(x)\psi_{k_2}(x^{(q+1)/2}+tx).$$

Moving the terms around, this is the same as showing

$$((1/2)S(1,t)+(1/2)S(\delta^{(q+1)/2},\delta t))^2-((1/2)S(1,t)-(1/2)S(\delta^{(q+1)/2},\delta t))^2 =$$

$$\sum_{x\in k_2} (1+\chi_{2,k_2}(x))\psi_{k_2}(x^{(q+1)/2}+tx).$$

The first expression is simply

$$S(1,t)S(\delta^{(q+1)/2},\delta t).$$

The second sum picks out the squares in k_2, so it is

$$\sum_{x\in k_2} \psi_{k_2}(x^{q+1}+tx^2) = \sum_{x\in k_2} \psi_k(\mathrm{Trace}_{k_2/k}(x^{q+1}+tx^2)).$$

Because δ is a nonsquare in $k^\times$, k_2 is $k(\sqrt{\delta})$. Let us write $x \in k_2$ as $u + v\sqrt{\delta}$, with $u, v \in k$. Then

$$x^{q+1} = (u + v\sqrt{\delta})^{q+1} = (u^q + v^q\sqrt{\delta}^q)(u + v\sqrt{\delta}) =$$
$$= (u^{q+1} + \delta^{(q+1)/2}v^{q+1}) + (u^q v + uv^q\delta^{(q-1)/2})\sqrt{\delta}.$$

Thus we see that

$$\mathrm{Trace}_{k_2/k}(x^{q+1}) = 2u^{q+1} + 2\delta^{(q+1)/2}v^{q+1}.$$

We have $x^2 = (u + v\sqrt{\delta})^2 = (u^2 + \delta v^2) + 2uv\sqrt{\delta}$, so

$$\mathrm{Trace}_{k_2/k}(x^2) = 2u^2 + 2\delta v^2,$$

Thus

$$\sum_{x\in k_2} \psi_k(\mathrm{Trace}_{k_2/k}(x^{q+1} + tx^2)) =$$
$$= \sum_{u,v\in k} \psi_k(2u^{q+1} + 2\delta^{(q+1)/2}v^{q+1} + 2tu^2 + 2t\delta v^2) =$$
$$= S(2, 2t)S(2\delta^{(q+1)/2}, 2t\delta).$$

So the needed equality of traces is equivalent to the identity

$$S(1, t)S(\delta^{(q+1)/2}, \delta t) = S(2, 2t)S(2\delta^{(q+1)/2}, 2\delta t).$$

Because 2 is a square in $\mathbb{F}_q^\times$, say

$$2 = A^2,\ A \in \mathbb{F}_q,$$

for any nonzero $a, b \in k$, we will have

$$S(2a, 2b) = S(a, b).$$

Indeed, $2 = A^2 = A^{q+1}$, so

$$S(2a, 2b) := \sum_{x\in k} \psi_k(2ax^{q+1} + 2bx^2) =$$
$$= \sum_{x\in k} \psi_k(A^{q+1}ax^{q+1} + A^2bx^2) = S(a, b),$$

by the change of variable $x \mapsto x/A$. □

Remark 16.5. Suppose that 2 is not a square in $\mathbb{F}_q$, i.e., that q is ± 3 mod 8. Then the identity, for all $k/\mathbb{F}_q$ and all $t \in k$,

$$S(1, t)S(\delta^{(q+1)/2}, \delta t) = S(2, 2t)S(2\delta^{(q+1)/2}, 2\delta t)$$

does not hold. Indeed, it already fails in the special case $k = \mathbb{F}_q$ and $t = 1$. To see this, note that q must be an odd power of an odd prime p (otherwise q would be 1 mod 8) with p congruent to q mod 8 and 2 a nonsquare in $\mathbb{F}_p^\times$. The quantities $S(a, b)$ lie in $\mathbb{Q}(\sqrt{\epsilon p}), \epsilon := (-1)^{(p-1)/2}$.

For any a, b, the quantities $S(a,b)$ and $S(2a,2b)$ are galois conjugates of each other, by $Gal(\mathbb{Q}(\sqrt{\epsilon p})/\mathbb{Q})$. So the equality

$$S(1,t)S(\delta^{(q+1)/2},\delta t) = S(2,2t)S(2\delta^{(q+1)/2},2\delta t)$$

is an equality of galois conjugates. It can hold if and only if $S(1,t)S(\delta^{(q+1)/2},\delta t)$ lies in $\mathbb{Q}$. Taking $k := \mathbb{F}_q$, and δ a nonsquare in $\mathbb{F}_q^\times$, we have

$$\delta = -\delta^{(q+1)/2}$$

and

$$x^{q+1} = x^2 \text{ for all } x \in \mathbb{F}_q.$$

Thus

$$S(1,1) = \sum_{x\in\mathbb{F}_q} \psi(x^2+x^2)$$

is a gauss sum which, having absolute value $\sqrt{q}$, does not lie in $\mathbb{Q}$. and

$$S(\delta^{(q+1)/2},\delta) = \sum_{x\in\mathbb{F}_q} \psi(\delta^{(q+1)/2}x^2+\delta x^2) = \sum_{x\in\mathbb{F}_q} \psi(0) = q.$$

Thus the product $S(1,t)S(\delta^{(q+1)/2},\delta t)$ does not lie in $\mathbb{Q}$.

Evans' Proof of Theorem 16.3 When $a \in \mathbb{F}_q^\times$ is a nonsquare, for any nontrivial additive character of $\mathbb{F}_q$ and for any finite extension $k/\mathbb{F}_q$, we have the identity

$$\sum_{x\in k} \psi_k(ax^{(q+1)/2}+atx) = \sum_{x\in k} \psi_k(-x^{(q+1)/2}+tx);$$

simply use the fact that $a = -a^{(q+1)/2}$ and make the substitution $x \mapsto x/a$. So the explicit identity to be proven is that for any $k/\mathbb{F}_q$, with k_2/k its quadratic extension, we have

$$(-\sum_{x\in k} \psi_k(-x^{(q+1)/2}+tx))^2 + (-\sum_{x\in k_2} \psi_{k_2}(-x^{(q+1)/2}+tx)) =$$

$$= (-\sum_{x\in k} \chi_{2,k}(x)\psi_k(x^{(q+1)/2}+tx))^2 - (-\sum_{x\in k_2} \chi_{2,k_2}(x)\psi_{k_2}(x^{(q+1)/2}+tx)).$$

If we expand out both sides and fix the trace, call it A, ($x+y$ for $k\times k$ as a k-algebra, $\mathrm{Trace}_{k_2/k}$ for k_2 as a k-algebra), we reduce (by Fourier inversion with respect to A) to the following identities: for each $A \in k$, we are to have

$$\sum_{x\in k} \chi_{2,k}(x(A-x))\psi_k(x^{(q+1)/2}+(A-x)^{(q+1)/2}) +$$

$$\sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \chi_{2,k}(\mathrm{Norm}_{k_2/k}(x))\psi_k(\mathrm{Trace}_{k_2/k}(x^{(q+1)/2})) =$$

$$= \sum_{x\in k} \psi_k(-x^{(q+1)/2} - (A-x)^{(q+1)/2})$$
$$- \sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \psi_k(-\mathrm{Trace}_{k_2/k}(x^{(q+1)/2})).$$

In fact, Evans shows [Evans] that for **any** nontrivial additive character ψ of k, and any $A \in k$, we have the identity

$$\sum_{x\in k} \chi_{2,k}(x(A-x))\psi(x^{(q+1)/2} + (A-x)^{(q+1)/2}) +$$
$$\sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \chi_{2,k}(\mathrm{Norm}_{k_2/k}(x))\psi(\mathrm{Trace}_{k_2/k}(x^{(q+1)/2})) =$$
$$= \sum_{x\in k} \psi(-x^{(q+1)/2} - (A-x)^{(q+1)/2})$$
$$- \sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \psi(-\mathrm{Trace}_{k_2/k}(x^{(q+1)/2})).$$

We will give his proof only in the case when 2 is a not square in $\mathbb{F}_q^\times$, see [Evans] for the general case.

Choose a nonsquare $\delta \in k^\times$. Then k_2 is $k[\sqrt{\delta}]$, and the elements $u \in k_2$ with $\mathrm{Trace}_{k_2/k}(a) = A$ are those of the form

$$A/2 + b\sqrt{\delta},$$

$b \in k$ arbitrary. Let us also write

$$n := (q+1)/2.$$

We first treat the case $A = 0$. Here the elements $u \in k_2$ with $\mathrm{Trace}_{k_2/k}(a) = 0$ are $x\sqrt{\delta}$, $x \in k$ arbitrary. So the identity to be proved is

$$\sum_{x\in k} \chi_{2,k}(-x^2)\psi(x^n + (-x)^n) +$$
$$\sum_{x\in k} \chi_{2,k}(\mathrm{Norm}_{k_2/k}(x\sqrt{\delta}))\psi(\mathrm{Trace}_{k_2/k}((x\sqrt{\delta})^n)) =$$
$$= \sum_{x\in k} \psi(-x^n - (-x)^n)$$
$$- \sum_{x\in k} \psi(-\mathrm{Trace}_{k_2/k}((x\sqrt{\delta})^n)).$$

If n is odd, then $x^n + (-x)^n = 0$, $\mathrm{Trace}_{k_2/k}((x\sqrt{\delta})^n) = 0$, and $\mathrm{Norm}_{k_2/k}(x\sqrt{\delta}) = -x^2\delta$. As δ is a nonsquare in $k^\times$, both sides of the asserted identity vanish.

Suppose now that n is even, i.e. that q is 3 mod 4, or equivalently that -1 is not a square in $\mathbb{F}_q$. Then $\sqrt{\delta}^n = \delta^{n/2}$ lies in k, and the identity to be proven (still in the $A = 0$ case) is

$$\sum_{x\in k} \chi_{2,k}(-x^2)\psi(2x^n)+$$

$$\sum_{x\in k} \chi_{2,k}(-x^2\delta))\psi(2x^n\delta^{n/2})) =$$

$$= \sum_{x\in k} \psi(-2x^n)$$

$$- \sum_{x\in k} \psi(-2x^n\delta^{n/2})).$$

Because δ is a nonsquare in $k^\times$, the first term is (the terms $x = 0$ cancelling)

$$\chi_{2,k}(-1)(\sum_{x\in k} \psi(2x^n) - \sum_{x\in k} \psi(2x^n\delta^{n/2})),$$

and the second term is

$$\sum_{x\in k} \psi(-2x^n) - \sum_{x\in k} \psi(-2x^n\delta^{n/2}),$$

If the degree of $k/\mathbb{F}_q$ is even, then -1 is a square in k, and indeed -1 is an $2n$'th power in k: this is already true in $\mathbb{F}_{q^2}$, as $(q^2-1)/(2n) = (q^2-1)/((q+1)2) = q-1$, and hence

$$(-1)^{(q^2-1)/(2n)} = (-1)^{q-1} = 1.$$

So in the asserted identity, the factor $\chi_{2,k}(-1) = 1$, and as -1 is an n'th power in $k^\times$, say $-1 = a^n$, the change of variable $x \mapsto x/a$ turns the second sum into the first.

If the degree of $k/\mathbb{F}_q$ is odd, then -1 is a nonsquare in k, but $\gcd(n, \#k^\times) = 2$. Indeed, if $\#k = q^s$ with s odd, then $\gcd(q+1, q^s - 1) = 2$ (write $q^s - 1 = ((q+1)-1)^s - 1 \equiv (-1)^s - 1 = -2 \bmod q+1$). So in this case, sums over n'th powers in k are sums over square in k, and our alleged identity is

$$-(\sum_{x\in k} \psi(2x^2) - \sum_{x\in k} \psi(2x^2\delta^{n/2})),$$

and the second term is

$$\sum_{x\in k} \psi(-2x^2) - \sum_{x\in k} \psi(-2x^2\delta^{n/2}),$$

In terms of the Gauss sum

$$g := \sum_{x\in k^\times} \chi_{2,k}(x)\psi(x),$$

we have, for any $a \in k^\times$, the identity

$$\sum_{x\in k} \psi(ax^2) = \chi_{2,k}(a)g,$$

so the identity in question is g times the identity

$$-(\chi_{2,k}(2) - \chi_{2,k}(2\delta^{n/2}) = \chi_{2,k}(-2) - \chi_{2,k}(-2\delta^{n/2}).$$

As -1 is a nonsquare in k, this identity holds. This concludes the treatment of the $A = 0$ case.

Now we treat the case when $A \neq 0$. We first rewrite the identity to be proven as

$$\sum_{x\in k} \psi(-x^n - (A-x)^n) -$$
$$\sum_{x\in k} \chi_{2,k}(x(A-x))\psi(x^n + (A-x)^n) =$$
$$= \sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \chi_{2,k}(\mathrm{Norm}_{k_2/k}(x))\psi(\mathrm{Trace}_{k_2/k}(x^n)) +$$
$$\sum_{x\in k_2, \mathrm{Trace}_{k_2/k}(x)=A} \psi(-\mathrm{Trace}_{k_2/k}(x^n)).$$

In the left hand side, Evans makes the substitution

$$x \mapsto (1+x)A/2,$$

under which, one readily computes,

$$x(A-x) \mapsto (A/2)^2(1-x^2),$$
$$x^n + (A-x)^n \mapsto (A/2)^n((1+x)^n + (1-x)^n).$$

The polynomial $(1+X)^n + (1-X)^n$ is visibly a polynomial in x^2. So there is a unique integer polynomial $f(X) \in \mathbb{Z}[X]$ such that

$$f(X^2) = (1+X)^n + (1-X)^n.$$

Thus the left hand side becomes

$$\sum_{x\in k} \psi(-(A/2)^n f(x^2)) - \sum_{x\in k} \chi_{2,k}(1-x^2))\psi((A/2)^n f(x^2)).$$

On the right hand side, write elements $u \in k_2$ with $\mathrm{Trace}_{k_2/k}(x) = A$ of as $u = (A/2)(1 + x\sqrt{\delta})$. Then

$$\mathrm{Norm}_{k_2/k}((A/2)(1+x\sqrt{\delta})) = (A/2)^2(1-x^2\delta),$$

and

$$\mathrm{Trace}_{k_2/k}(((A/2)(1+x\sqrt{\delta}))^n) =$$
$$= (A/2)^n((1+x\sqrt{\delta}))^n + (1-x\sqrt{\delta}))^n) = (A/2)^n f(x^2\delta).$$

So the right hand side becomes

$$= \sum_{x\in k} \chi_{2,k}(1-x^2\delta)\psi((A/2)^n f(x^2\delta)) +$$
$$\sum_{x\in k} \psi(-(A/2)^n f(x^2\delta)).$$

For the nontrivial additive character $\psi_{(A/2)^n}$, the identity to be proven thus becomes

$$\sum_{x\in k} \psi(-f(x^2)) - \sum_{x\in k} \chi_{2,k}(1-x^2))\psi(f(x^2)) =$$
$$= \sum_{x\in k} \chi_{2,k}(1-x^2\delta)\psi(f(x^2\delta)) + \sum_{x\in k} \psi(-f(x^2\delta)).$$

We now rewrite this as

$$\sum_{x\in k} \psi(-f(x^2)) - \sum_{x\in k} \psi(-f(x^2\delta)) =$$
$$= \sum_{x\in k} \chi_{2,k}(1-x^2))\psi(f(x^2)) + \sum_{x\in k} \chi_{2,k}(1-x^2\delta)\psi(f(x^2\delta)).$$

The key point now is that as x runs over $k^\times$, x^2 runs twice over the squares, and $x^2\delta$ runs twice over the nonsquares. The left side (in which the $x=0$ terms cancel) is thus equal to

$$2\sum_{x\in k^\times} \chi_{2,k}(x)\psi(-f(x)),$$

itself equal to the same sum over all $x \in k$:

$$2\sum_{x\in k} \chi_{2,k}(x)\psi(-f(x)).$$

The right side is

$$2\psi(f(0)) + 2\sum_{x\in k^\times} \chi_{2,k}(1-x))\psi(f(x)),$$

itself equal to

$$2\sum_{x\in k} \chi_{2,k}(1-x))\psi(f(x)).$$

Making the substitution $x \mapsto 1-x$, the right side becomes

$$2\sum_{x\in k} \chi_{2,k}(x))\psi(f(1-x)).$$

That the two sides are equal when 2 is not a square in $\mathbb{F}_q$ results immediately from the following miraculous lemma of Evans.

Lemma 16.6. (Evans)*Let p be an odd prime, $\mathbb{F}_q$ a finite extension of $\mathbb{F}_p$,. $n := (q+1)/2$, and $f(X) \in \mathbb{F}_q[X]$ the unique polynomial such that*

$$f(X^2) = (1+X)^n + (1-X)^n.$$

Then we have the identity

$$f(1-X) = \chi_{2,\mathbb{F}_q}(2) f(X).$$

In particular, if 2 is not a square in $\mathbb{F}_q$, then $f(1-X) = -f(X)$.

Proof. The polynomial $f(X)$ has degree $[n/2]$.

We first claim that $f(X)^2 = f(1-X)^2$. Each of these polynomials has degree $2[n/2] \leq n < q$, so it suffices to show that $f(x)^2 = f(1-x)^2$ for every $x \in \mathbb{F}_q$. For $x = 0$, $f(0) = f(0^2) = 2$ and $f(1) = f(1^2) = 2^n = \chi_{2,\mathbb{F}_q}(2)2$ (because $n := (q+1)/2$). So we do have $f(x)^2 = f(1-x)^2$ for x either 0 or 1. For $x \neq 0$, choose a square root of x in $\mathbb{F}_{q^2}$, call it $\sqrt{x}$. Then

$$f(x) = f((\sqrt{x})^2) = (1+\sqrt{x})^n + (1-\sqrt{x})^n.$$

Thus for $x \neq 0$, we have

$$f(x)^2 = 2(1-x)^n + (1+\sqrt{x})^{q+1} + (1-\sqrt{x})^{q+1} =$$

$$= 2(1-x)^n + (1+\sqrt{x}^q)(1+\sqrt{x}) + (1-\sqrt{x}^q)(1-\sqrt{x}) =$$

$$= 2(1-x)^n + 2 + 2x^n.$$

This expression is visibly invariant under $x \mapsto 1-x$. Thus we have the polynomial identity $f(X)^2 = f(1-X)^2$ in $\mathbb{F}_q[X]$. Therefore $f(X) = \epsilon f(1-X)$ for some $\epsilon \in \{\pm 1\}$. Evaluating at $X = 0$, as we have done above, we see that the sign is $\chi_{2,\mathbb{F}_q}(2)$. □

Remark 16.7. Using Evans' polynomial $f(X)$ and his lemma above, one also gets a proof of Theorem 16.2 along these same lines, simply replace every occurrence of $\psi(-f)$ in the above proof by $\psi(f)$.

For ease of reference, we combine the statements of Theorems 16.2 and 16.3.

Theorem 16.8. (joint with Evans)*Let q be odd. For any nontrivial additive character ψ of $\mathbb{F}_q$, with $\psi_2(x) := \psi(2x)$, there exists an isomorphism of local systems on $\mathbb{G}_m/\mathbb{F}_q$*

$$Sym^2(\mathcal{G}(\mathbb{F}_q, \psi_2, \mathbb{1}, (q+1)/2)) \cong \Lambda^2(\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)).$$

17. The situation for $SL(2,q)$

Theorem 17.1. *Suppose $q > 3$. Then we have the following results.*

(1) *If q is 1 mod 4, the local system $\mathcal{G}(\mathbb{F}_q, \psi, \mathbb{1}, (q+1)/2)$ has*

$$G_{geom} = G_{arith} = SL(2,q)$$

in one of the irreducible representations of $SL(2,q)$ of dimension $(q-1)/2$. If we replace ψ by ψ_a for $a \in \mathbb{F}_q^\times$ a nonsquare, we get the other irreducible representations of $SL(2,q)$ of dimension $(q-1)/2$.

(2) *If q is 3 mod 4, the local system $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ has*

$$G_{geom} = G_{arith} = SL(2,q)$$

in one of the irreducible representations of $SL(2,q)$ of dimension $(q+1)/2$. If we replace ψ by ψ_a for $a \in \mathbb{F}_q^\times$ a nonsquare, we get the other irreducible representations of $SL(2,q)$ of dimension $(q+1)/2$.

Proof. When q is 1 mod 4, $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ has odd rank $(q+1)/2$ and $\mathcal{G}(\mathbb{F}_q, \psi_2, \mathbb{1}, (q+1)/2)$ have even rank $(q-1)/2$. When q is 3 mod 4, $\mathcal{G}(\mathbb{F}_q, \psi_2, \mathbb{1}, (q+1)/2)$ has odd rank $(q-1)/2$ and $\mathcal{G}(\mathbb{F}_q, \psi, \chi_2, (q+1)/2)$ has even rank $(q+1)/2$. Let us denote these local systems

$$\mathcal{G}_{odd} \text{ and } \mathcal{G}_{even}$$

respectively.

We have proven that $\mathcal{G}_{odd}$ has $G_{geom} = G_{arith} = PSL(2,q)$ for all odd $q > 3$. Therefore we have

$$G_{geom} = G_{arith} = PSL(2,q)$$

for

$$\Lambda^2(\mathcal{G}_{odd}), \text{ when } q \text{ is } 1 \mod 4,$$

and for

$$Sym^2(\mathcal{G}_{odd}), \text{ when } q \text{ is } 3 \mod 4.$$

We have proven the existence of isomorphisms

$$\Lambda^2(\mathcal{G}_{odd}) \cong Sym^2(\mathcal{G}_{even}), \text{ when } q \text{ is } 1 \mod 4,$$

$$Sym^2(\mathcal{G}_{odd}) \cong \Lambda^2(\mathcal{G}_{even}), \text{ when } q \text{ is } 3 \mod 4.$$

Therefore we know that

$$G_{geom} = G_{arith} = PSL(2,q)$$

for

$$Sym^2(\mathcal{G}_{even}), \text{ when } q \text{ is } 1 \mod 4,$$

and for

$$\Lambda^2(\mathcal{G}_{even}), \text{ when } q \text{ is } 3 \mod 4.$$

Passing from $\mathcal{G}_{even}$ to either $\Lambda^2(\mathcal{G}_{even})$ or to $Sym^(\mathcal{G}_{even})$ either leaves G_{geom} (respectively G_{arith}) unchanged, or it divides that group by ± 1. These groups cannot remain unchanged, because $PSL(2,q)$ does not have an irreducible representation of this degree. Therefore both G_{geom} and G_{arith} are double covers of $PSL(2,q)$. Neither can be the product of ± 1 with $PSL(2,q)$, again because $PSL(2,q)$ does not have an irreducible representation of this degree. Therefore each is the Schur double cover of $PSL(2,q)$, which is $SL(2,q)$. □

For ease of later reference, we combine the statements of this last theorem and of Theorem 16.1.

Theorem 17.2. *Suppose $q > 3$ is odd. In the notation $\mathcal{G}_{odd}$ and $\mathcal{G}_{even}$ of the proof of the theorem above, we have the following results.*

(1) *For every odd $q > 3$, $\mathcal{G}_{odd}$ has $G_{arith} = G_{geom} = PSL(2,q)$.*
(2) *For every odd $q > 3$, $\mathcal{G}_{even}$ has $G_{arith} = G_{geom} = SL(2,q)$.*

18. Representations of $PU(3,q)$, d'apres Gross

Gross has constructed a $PU(3,q)$-torsor $\mathcal{T}$ on $\mathbb{G}_m/\mathbb{F}_{q^2}$ with the following properties. On $\mathcal{T}$, the inertia and wild inertia groups at 0 and ∞ are given explicitly in terms of the Borel B, its unipotent radical R_u, the quasisplit torus T_{qspl}, cyclic of order q^2-1, and the Coxeter torus T_{cxt}, cyclic of order q^2-q+1. We have

$$I_\infty = B \rhd P_\infty = R_u, \quad I_\infty/P_\infty = T_{qspl},$$
$$I_0 = T_{cxt}, \quad P_0 = \{1\}.$$

[Over finite fields, there is only one isomorphism class of nondegenerate hermitian form in each dimension, cf. [Grove, Thm. 10.3]. The complete Deligne-Lusztig curve for $PU(3,q)$ can therefore be seen either as the Hermitian curve

$$XY^q + X^qY = Z^{q+1},$$

or as the Fermat curve of degree $q+1$,

$$X^{q+1} + Y^{q+1} + Z^{q+1} = 0.$$

The action of $PU(3,q)$ on the Fermat curve is perhaps most visible. The quotient is $\mathbb{P}^1/\mathbb{F}_{q^2}$, and the torsor $\mathcal{T}$ is the restriction to $\mathbb{G}_m$ of the projection to $\mathbb{P}^1/\mathbb{F}_{q^2}$ of the Fermat curve onto its quotient.]

When q is odd, the group R_u is a Heisenberg group of exponent p and order q^3, whose center $Z(R_u)$, which is also its derived group, is noncanonically the additive group of $\mathbb{F}_q$. When p is odd, one knows

(Stone-von Neumann theorem, cf. [Ga]) that the irreducible representations of R_u are as follows.

(1) Those trivial on $Z(R_u)$; the quotient $R_u/Z(R_u)$ is abelian of order q^2, and hence has q^2 linear characters.
(2) For each nontrivial character ψ of $Z(R_u)$, there is an irreducible representation H_ψ of dimension q having ψ as its central character. The character of H_ψ vanishes on $R_u \setminus Z(R_u)$, and is equal to $q\psi$ on $Z(R_u)$.

In the Appendix, Tiep shows (Theorem 22.2) that for **any** prime power q, the irreducible representations of R_u are as described in (1) and (2) above.

As I learned from Dick Gross, the action of B/R_u on $Z(R_u)$ by conjugation cyclically permutes the $q-1$ nontrivial characters of $Z(R_u)$. Indeed, in the matrix picture given by Ennola [Enn, bottom of page 30], B is the subgroup $c=1$, R_u is the subgroup $a=c=1$, its center $Z(R_u)$ is the further subgroup $b=e=0$, with parameter d, the lowermost left corner, which is any element of $\mathbb{F}_{q^2}$ with $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(d)=0$. The quotient $B/R_u = T_{qspl}$ is the $\mathbb{F}_{q^2}^\times$ of diagonal matrices $\mathrm{Diag}(a,1,1/a^q), a \in \mathbb{F}_{q^2}^\times$, which acts on $Z(R_u)$ by multiplication by $1/\mathrm{Norm}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a)$.

Lemma 18.1. *Suppose $q \geq 3$. The group $PU(3,q)$ has $\gcd(3,q+1)$ irreducible representations of dimension $q(q-1)$, and it has $q+1-\gcd(3,q+1)$ irreducible representations of dimension $1+q(q-1)$.*

Proof. This is most easily seen from the character table of $U(3,q)$ due to Ennola [Enn, pp. 29-31]. In that table, the irreducible representations of dimension $q(q-1)$ are denoted $\chi^{(t)}_{q^2-q}$, with t an integer mod $q+1$; those trivial on the center of $U(3,q)$ are those whose parameter t satisfies $3t=0$ in $\mathbb{Z}/(q+1)\mathbb{Z}$. The irreducible representations of dimension $1+q(q-1)$ are denoted $\chi^{(t,u)}_{q^2-q+1}$, with t,u mod $q+1$ and $t \neq u$. Those trivial on the center of $U(3,q)$ are those of the form $\chi^{(-2u,u)}_{q^2-q+1}$ with $3u \neq 0$ mod $q+1$. □

Remark 18.2. When $q=2$, the group $PU(3,2)$ has $\gcd(q+1,3) = 3$ irreducible representations of dimension $q(q-1)=2$, but rather than having $q+1-\gcd(3,q+1)=0$ irreducible representations of dimension $1+q(q-1)=3$, it has one such. This "exotic" one is the representation labeled $\chi^{(t,u,v)}_{(q-1)(q^2-q+1)}$ in Ennola's table, with (t,u,v) taken to be $(1,2,3)$.

Theorem 18.3. (Gross) *We have the following results.*

(1) *In each of the irreducible representations of $PU(3,q)$ of dimension $q(q-1)$, the action of R_u is by the direct sum*

$$\bigoplus_{\text{nontriv. } \psi} H_\psi$$

of the $(q-1)$ irreducible representations of R_u with nontrivial central character. These $q-1$ summands are cyclically permuted by a generator of $B/R_u = T_{qspl}$.

(2) *In each of the irreducible representations of $PU(3,q)$ of dimension $q(q-1)$, the group T_{cxt} acts by*

$$\mathrm{Reg} - \rho,$$

with Reg *the regular representation and ρ a character of order dividing $q+1$ having ρ^3 trivial. [Unless $q \equiv 2 \bmod 3$, the only such ρ is $\mathbb{1}$. If $q \equiv 2 \bmod 3$, then $3|q^2-q+1$, and there are 3 such ρ.]*

(3) *Suppose $q \neq 2$. In each of the irreducible representations of $PU(3,q)$ of dimension $1+q(q-1)$, the action of R_u is by the direct sum*

$$\mathbb{1} \oplus \bigoplus_{\text{nontriv. } \psi} H_\psi.$$

The $q-1$ summands H_ψ are cyclically permuted by a generator of $B/R_u = T_{qspl}$. The group B/R_u acts on the line of R_u-invariants by a character ρ of order dividing $q+1$ with ρ^3 nontrivial.

(4) *Suppose $q \neq 2$. In each of the irreducible representations of $PU(3,q)$ of dimension $1+q(q-1)$, the group T_{cxt} acts by the regular representation.*

Proof. (1) In the tables of Ennola, nontrivial elements of the center $Z(R_u)$ lie in the conjugacy class $C_2^{(q+1)}$, and these elements all have trace $-q$ in each of the ireducible representations of $PU(3,q)$ of dimension $q(q-1)$. Elements of $R_u \setminus Z(R_u)$ lie in the conjugacy class $C_3^{(q+1)}$, and have trace 0 in each of these representationa. In other words, the character of $Z(R_u)$ is equal to q times the sum of the $q-1$ nontrivial linear characters of $Z(R_u)$, and the character of R_u is equal to the sum of the characters of the $q-1$ distinct q-dimensional irreducible representations H_ψ of R_u. Because the nontrivial characters of $Z(R_u)$ are cyclically permuted by a generator of $B/R_u = T_{qspl}$, the summands H_ψ must themselves be cyclically permuted by a generator of $B/R_u = T_{qspl}$.

(2) A generator of the group T_{cxt} is the image in $PU(3,q)$ of an element in the conjugacy class $C_8^{(1)}$. Its k'th power, for $1 \leq k < q^2-q+1$, lies in the image in $PU(3,q)$ of the conjugacy class $C_8^{(k)}$. Its trace in $\chi_{q^2-q}^{(t)}$ is $-\epsilon^{tk}$, ϵ being a chosen $q+1$'st root of unity. As $3t = 0 \mod q+1$, the assertion follows.

(3) Again looking at the tables of Ennola, the nontrivial elements of $Z(R_u)$ all have trace $1-q$ in any of the ireducible representations of $PU(3,q)$ of dimension $1+q(q-1)$, and the elements of $R_u \setminus Z(R_u)$ all have trace 1 in any of these representations. Therefore the representation of R_u is

$$\mathbb{1} \oplus \bigoplus_{\text{nontriv. } \psi} H_\psi.$$

Because R_u is a normal subgroup of B, B/R_u acts on the line of R_u-invariants by a linear character, call it ρ. A generator of $B/R_u = T_{qspl}$ permutes cyclically the H_ψ, so it has trace zero on $\bigoplus_{\text{nontriv. } \psi} H_\psi$, and hence the value of ρ on a generator γ of T_{qspl} is the trace of γ in the representation. A generator of T_{qspl} is the image in $PU(3,q)$ of an element in the conjugacy class $C_7^{(q+1,1)}$, and such an element has trace ϵ^{-u} in $\chi_{q^2-q+1}^{(-2u,u)}$. As $3u \neq 0 \mod q+1$, the assertion follows.

(4) Exactly as in part (2), it suffices now to remark that the nontrivial elements of T_{cxt} lie in the (images in $PU(3,q)$ of) conjugacy classes $C_8^{(k)}$, for $1 \leq k < q^2-q+1$, and that all these classes have trace zero in any of the irreducible representations of dimension $1+q(q-1)$. □

Corollary 18.4. (Gross) *The pushout of the Gross $PU(3,q)$-torsor on $\mathbb{G}_m/\mathbb{F}_{q^2}$ by any of the irreducible representations of $PU(3,q)$ of dimension either $q(q-1)$ or, if $q \neq 2$, of dimension $1+q(q-1)$ is tame at 0 and has $\mathrm{Swan}_\infty = 1$.*

Proof. In all cases, the tameness at 0 is obvious, since I_0 acts through T_{cxt}, a group of order prime to p.

The irreducible representation $\chi_{q^q-q}^{(q+1)}$ is the only one of the irreducible representations of dimension $q(q-1)$ whose character is $\mathbb{R}$-valued, so is the only one of them which is self dual. Therefore it is the irreducible unipotent cuspidal representation of dimension $q(q-1)$, and for this representation the statement is given in [Gross, Cor. part (c), top of page 2537].

For V the pushout by any of the other representations, its L-function is known to be the constant 1, of degree 0 [Gross, Cor. part (c), bottom of page 2536], and we have the formula [Gross, middle of page 2536]

$$\mathrm{Swan}_\infty(V) = \mathrm{degree}(L) + \dim(V^{I_0}) + \dim(V^{I_\infty}).$$

[This is the Euler-Poincaré formula, applied to the geometrically irreducible and nonconstant lisse sheaf V on $\mathbb{G}_m/\mathbb{F}_q$, the inclusion

$$j : \mathbb{G}_m \subset \mathbb{P}^1,$$

the short exact sequence of sheaves on $\mathbb{P}^1$,

$$0 \to j_!V \to j_\star V \to V^{I_0} \otimes \delta_0 \bigoplus V^{I_\infty} \otimes \delta_\infty \to 0,$$

and the piece of the long exact cohomology sequence

$$0 \to V^{I_0} \oplus V^{I_\infty} \to H^1_c(\mathbb{G}_m/\overline{\mathbb{F}_q}, V) \to H^1(\mathbb{P}^1/\overline{\mathbb{F}_q}, j_\star V) \to 0.$$

Because V is tame at 0, the middle term has dimesion $\mathrm{Swan}_\infty(V)$, and the last term has dimension equal to the degree of the L function.]

For the other, if any, irreducible representations of dimension $q(q-1)$, I_0 acts as $\mathrm{Reg} - \rho$ with ρ nontrivial, so has a one-dimensional space of invariants, while the I_∞-representation is totally wild.

For the irreducible representations of dimension $1 + q(q-1)$, we suppose $q \neq 2$. Then I_0 acts as the regular representation, so has a one-dimensional space of invariants. The I_∞-representation is the direct sum of a totally wild representation and a tame line on which I_∞/P_∞ acts through a nontrivial character (one of order dividing $q+1$ whose cube is nontrivial). So again in this case there are no nonzero I_∞-invariants. □

It is known [Ka-ESDE, 8.5.3] that a geometrically irreducible local system on $\mathbb{G}_m/\mathbb{F}_{q^2}$ which is tame at 0 and has $\mathrm{Swan}_\infty = 1$ is, geometrically, a hypergeometric sheaf, and is determined [Ka-ESDE, 8.5.6 (2)] by the semisimplifications of its I_0 and I_∞ representations. So we get the following, in which the subscript *desc* denotes the canonical descent to $\mathbb{G}_m/\mathbb{F}_{q^2}$.

Corollary 18.5. *We have the following results.*

(1) *There are* $\gcd(3, q+1)$ *irreducible representations of* $PU(3,q)$ *of dimension* $q(q-1)$*. Their pushouts of the Gross torsor are, geometrically, unique multiplicative translates of the Kloosterman sheaves*

$$Kl_{desc}(!, \psi; \text{all char.}'\text{s of order dividing } q^2 - q + 1 \text{ save } \rho),$$

with ρ *of order dividing* $q+1$ *and having* $\rho^3 = \mathbb{1}$*.*

(2) *Suppose* $q \neq 2$*. There are* $q + 1 - gcd(3, q+1)$ *irreducible representations of* $PU(3,q)$ *of dimension* $1+q(q-1)$*. Their pushouts of the Gross torsor are, geometrically, unique multiplicative translates of the hypergeometric sheaves of type* $(1+q(q-1), 1)$

$$\mathcal{H}_{desc}(!, \psi; \text{all char.}'\text{s of order dividing } q^2 - q + 1; \rho),$$

with ρ a character of order dividing $q+1$ with ρ^3 nontrivial.

Remark 18.6. When q is not 2 mod 3, then the only ρ in part (1) is $\mathbb{1}$, and all nontrivial ρ occur in (2). When q is 2 mod 3, then 3 also divides q^2-q+1, and there are three ρ in part (1) and $q+1-3 = q-2$ ρ in part (2).

If we now pay attention to rationality questions, we get

Corollary 18.7. *We have the following results.*

(1) *For each character ρ of order dividing $q+1$ and having $\rho^3 = \mathbb{1}$, there exists $a_\rho \in \mathbb{G}_m(\mathbb{F}_{q^2})$ and $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$ such that the corresponding pushout of the Gross torsor is arithmetically isomorphic to*

$$\mathcal{H}_\rho :=$$

$$[x \mapsto a_\rho x]_\star Kl_{desc}(!, \psi; \text{all char.}'\text{s of order dividing } q^2-q+1 \text{ save } \rho) \otimes \alpha_\rho^{deg}.$$

(2) *Suppose $q \neq 2$. For each character ρ of order dividing $q+1$ and having ρ^3 nontrivial, there exists $a_\rho \in \mathbb{G}_m(\mathbb{F}_{q^2})$ and $\alpha_\rho \in \overline{\mathbb{Q}_\ell}^\times$ such that the corresponding pushout of the Gross torsor is arithmetically isomorphic to*

$$\mathcal{H}_\rho :=$$

$$[x \mapsto a_\rho x]_\star \mathcal{H}_{desc}(!, \psi; \text{all char.}'\text{s of order dividing } q^2-q+1; \rho) \otimes \alpha_\rho^{deg}.$$

(3) *These local systems $\mathcal{H}_\rho$ in parts (1) and (2) have $G_{geom} = G_{arith} =$* the image of $PU(3,q)$ *in the corresponding representation.*

19. Passage to $PSU(3,q)$

In general, $PSU(3,q)$ is a subgroup of $PU(3,q)$ and a quotient of $SU(3,q)$. When $\gcd(3, q+1) = 1$, all these groups coincide. When 3 divides $q+1$, then $PSU(3,q)$ has index 3 in $PU(3,q)$, and $SU(3,q)$ has a center μ_3 of order 3. In this latter case (which of course does not occur when q is a power of 3), restricting one of the irreducible representations of the previous section to $PSU(3,q)$ is achieved by the cubic pullback $[t \mapsto t^3]^\star$ of the pushout local system, cf. [Gross, bottom of page 2537], just as in the discussion of pullback from $PGL(2,q)$ to $PSL(2,q)$, where it was the pullback by squaring of the local system. From the identity

$$q^2-q+1 = (q-2)(q+1)+3$$

we see that 3 divides $q+1$ if and only if it divides q^2-q+1. So in all cases, the $[t \mapsto t^{q^2-q+1}]^\star$ pullback of any of the local systems $\mathcal{H}_\rho$ of the

last section are then local systems with $G_{geom} = G_{arith} = PSU(3,q)$. Taking into account [Ka-GKM, 9.3.2], we get the following theorems.

Theorem 19.1. *Suppose that* 3 *does not divide* $q+1$. *Then the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ *has* $G_{geom} = SU(3,q)$. *When pulled back to* $\mathbb{G}_m/\mathbb{F}_{q^4}$, *it has* $G_{geom} = G_{arith} = SU(3,q)$ $(= PSU(3,q))$. *For each of the* q *nontrivial characters* ρ *of order dividing* $q+1$, *the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho^3, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ *has* $G_{geom} = G_{arith} = SU(3,q)$ $(= PSU(3,q))$.

Proof. By [Ka-GKM, 9.3.2], for each character ρ of order dividing $q+1$, the $[t \mapsto t^{q^2-q+1}]^\star$ pullback of $\mathcal{H}_\rho$ is geometrically isomorphic to a $\mathbb{G}_m(\mathbb{F}_{q^2})$-translate (cf. 14.2) of

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho^{-3}, (q^3+1)/(q+1)).$$

Therefore there exists $\beta_\rho \in \overline{\mathbb{Q}_\ell}^\times$ such that this pullback is arithmetically isomorphic to a $\mathbb{G}_m(\mathbb{F}_{q^2})$-translate of $\mathcal{G} \otimes \beta_\rho^{deg}$. As translation by a rational point does not affect either G_{arith} or G_{geom}, the local system

$$\mathcal{G} \otimes \beta_\rho^{deg}$$

itself has $G_{geom} = G_{arith} = SU(3,q)$ $(= PSU(3,q))$ and has the same field of traces as $[t \mapsto t^{q^2-q+1}]^\star \mathcal{H}_\rho$.

It suffices to show $\beta_\rho = 1$ when ρ is nontrivial, and that $\beta_{\mathbb{1}} \in \pm 1$.

As one sees from Ennola's character table, the character of $\mathcal{H}_\rho$ takes values in the field $\mathbb{Q}(\rho)$, the field generated over $\mathbb{Q}$ by the values of ρ. The character of

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho^{-3}, (q^3+1)/(q+1))$$

also takes values in this field. Therefore the scalar β_ρ must lie in $\mathbb{Q}(\rho)$. Both $\mathcal{G}$ and $\mathcal{H}_\rho$ have their G_{arith} lying in $Sp(q(q-1), \overline{\mathbb{Q}_\ell})$ if $\rho^3 = \mathbb{1}$ (respectively in $SL(q^2-q+1, \overline{\mathbb{Q}_\ell})$ if ρ^3 is nontrivial). Therefore β_ρ is a root of unity. The only roots of unity in $\mathbb{Q}(\rho) \subset \mathbb{Q}(\mu_{q+1})$ lie in $\mu_{2(q+1)}$.

If ρ is nontrivial, β_ρ lies in $SL(q^2-q+1, \overline{\mathbb{Q}_\ell})$, so is a root of unity of order dividing $\gcd(2(q+1), q^2-q+1) = \gcd(q+1, q^2-q+1) = 1$ (the first equality because q^2-q+1 is odd). If $\rho = \mathbb{1}$, $\beta_{\mathbb{1}}$ is a root of unity in $\mathbb{Q}$, so is ± 1.

□

Theorem 19.2. *Suppose that* 3 *divides* $q+1$. *Then we have the following results.*

(1) *For $q \neq 2$, the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ has $G_{geom} = PSU(3,q)$, and after pullback to $\mathbb{G}_m/\mathbb{F}_{q^4}$ it has

$$G_{geom} = G_{arith} = PSU(3,q).$$

For $q = 2$, replace $PSU(3,2)$ in the above statement by its quotient Q_8, the quaternion group of order 8, which is the image of $PSU(3,2)$ in its unique irreducible representation of dimension two.

(2) *If q is odd, the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \chi_2, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ has $G_{geom} = G_{arith} = PSU(3,q)$

(3) *For any nontrivial character ρ of order dividing $(q+1)/3$ whose order is prime to 3, the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ has $G_{geom} = G_{arith} = PSU(3,q)$.

(4) *For any nontrivial character ρ of order dividing $(q+1)/3$, the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho, (q^3+1)/(q+1))$$

has $G_{geom} = PSU(3,q)$. After pullback to $\mathbb{G}_m/\mathbb{F}_{q^6}$ it has

$$G_{geom} = G_{arith} = PSU(3,q).$$

Proof. Statement (2) is a special case of (3), but seems worth stating separately.

Exactly as in the proof of the previous theorem, for each ρ of order dividing $q+1$, there exists $\beta_\rho \in \overline{\mathbb{Q}_\ell}^\times$ such that for

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho^{-3}, (q^3+1)/(q+1)),$$

the local system

$$\mathcal{G} \otimes \beta_\rho^{deg}$$

itself has $G_{geom} = G_{arith} = SU(3,q)$ $(= PSU(3,q))$ and has the same field of traces as $[t \mapsto t^{q^2-q+1}]^\star \mathcal{H}_\rho$.

(1) In this case of $\rho = \mathbb{1}$, both $\mathcal{G}$ and $\mathcal{G} \otimes \beta_{\mathbb{1}}^{deg}$ have their $G_{arith} \subset Sp(q(q-1), \overline{\mathbb{Q}_\ell})$. Therefore the scalar $\beta_{\mathbb{1}}$ lies in $Sp(q(q-1), \overline{\mathbb{Q}_\ell})$, hence is ± 1.

(2)In this case of $\rho = \chi_2$, both $\mathcal{G}$ and $\mathcal{G} \otimes \beta_{\chi_2}^{deg}$ have their $G_{arith} \subset SO(1+q(q-1), \overline{\mathbb{Q}_\ell})$. Therefore the scalar $\beta_{\chi_2} = 1$.

(3) If ρ is nontrivial of order dividing $(q+1)/3$ and prime to 3, then we can write $\rho = \Lambda^{-3}$ for a unique nontrivial character Λ of order dividing $(q+1)/3$ and prime to 3. Then for

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \rho, (q^3+1)/(q+1)) = \mathcal{G}(\mathbb{F}_{q^2}, \psi, \Lambda^{-3}, (q^3+1)/(q+1))$$

the local system

$$\mathcal{G} \otimes \beta_\Lambda^{deg}$$

has $G_{geom} = G_{arith} = PSU(3,q)$. The field of traces of $\mathcal{G} \otimes \beta_\Lambda^{deg}$ lies in $\mathbb{Q}(\Lambda) = \mathbb{Q}(\zeta_d)$ for d the order of Λ. The field of traces of $\mathcal{G}$ also lies in this field. Therefore the scalar β_Λ must lie in $\mathbb{Q}(\zeta_d)$. All roots of unity in this field lie in μ_{2d}. Both $\mathcal{G}$ and $\mathcal{G} \otimes \beta_\Lambda^{deg}$ have their G_{arith} lying in $SL(1+q(q-1), \overline{\mathbb{Q}_\ell})$. Therefore the scalar β_Λ lies in this SL group, so is a root of unity of order dividing $\gcd(q^2-q+1, 2d) = \gcd(q^2-q+1, d) = 1$ (the first equality because q^2-q+1 is odd, the second equality because $d|q+1$ and $\gcd(q^2-1+1, q+1) = 3$ while d is prime to 3).

(4)In this case, write ρ as Λ^{-3} for some character Λ of order dividing $q+1$.The same sort of argument only shows that β_Λ is a root of unity of order dividing $\gcd(q^2-1+1, q+1) = 3$. □

Remark 19.3. In part (1) of both Theorem 19.1 and 19.2, the possibility is left open that for

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^3+1)/(q+1)),$$

it is $\mathcal{G} \otimes (-1)^{deg}$ rather than $\mathcal{G}$ on $\mathbb{G}_m/\mathbb{F}_{q^2}$ which has $G_{arith} = PSU(3,q)$. Computer experiments suggested that it was indeed $\mathcal{G}$ which has $G_{arith} = PSU(3,q)$. The idea behind the experiments was to exploit the fact that for any $q > 3$, the character of the irreducible representation of $PSU(3,q)$ of dimension $q(q-1)$ takes the value 2, but never takes the value -2. [The reason $q = 3$ is an exception is that the value $1-q$ is always taken. For $q = 3$, one can show that $\mathcal{G}$ has the correct G_{arith} by checking that over the odd degree extension $\mathbb{F}_{3^6}$ of $\mathbb{F}_{3^2}$, we have $\mathrm{Trace}(Frob_{\mathbb{F}_{3^6},0}|\mathcal{G}) = 6$ $(= q(q-1))$, another character value whose negative does not occur as a character value. The reason $q = 2$ is an exception is that both 2 and -2 occur as traces equally often, and the only other trace attained is 0.] Therefore to show that $\mathcal{G}$ has $G_{arith} = PSU(3,q)$ for odd $q > 3$, it sufficed to exhibit a value $t \in \mathbb{F}_{q^2}$ at which

$$\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = 2,$$

simply because for this t, $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G} \otimes (-1)^{deg}) = -2$, a value that does not occur as a character value.

Let us make explicit the simple formula for this trace. Here ψ is any nontrivial additive character of $\mathbb{F}_{q^2}$ which comes from $\mathbb{F}_q$ by composition with the trace, and $t \in \mathbb{F}_{q^2}$.

$$\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = (1/q)\sum_{x\in\mathbb{F}_{q^2}} \psi(x^{1+q(q-1)} + tx).$$

Extensive computer experiments led us to conjecture the following theorem, whose proof is due to Ron Evans.

Theorem 19.4. (Evans) *We have the following determinations of the trace when q is odd.*

1. *If $q \equiv 2 \bmod 3$, then for $t = 0$ we have* $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},0}|\mathcal{G}) = 2$.
2. *If $q \equiv 3 \bmod 4$, then for $t = 1$ we have* $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},1}|\mathcal{G}) = 2$.
3. *If $q \equiv 1 \bmod 12$ and q is a nonsquare mod 5, then for $t = -2$ we have* $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},-2}|\mathcal{G}) = 2$.
4. *For any odd q, there exists $t \in \mathbb{F}_q$ with* $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = 2$.
5. *If q is an odd power of p, there exists $t \in \mathbb{F}_p$ with* $\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = 2$.

Proof. Because q is odd, we may view $\mathbb{F}_{q^2}$ as obtained from $\mathbb{F}_q$ by adjoining

$$\delta := \sqrt{A},$$

for $A \in \mathbb{F}_q^\times$ a nonsquare. Thus

$$\mathbb{F}_{q^2} = \mathbb{F}_q[\delta], \quad \delta^q = -\delta.$$

For $t \in \mathbb{F}_q$, we have

$$q\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = \sum_{x\in\mathbb{F}_{q^2}} \psi(x^{1+q(q-1)} + tx) =$$

$$= 1 + \sum_{x\in\mathbb{F}_{q^2}^\times} \psi(x^{2-q} + tx) = 1 + \sum_{(a,b)\in\mathbb{F}_q^2,(a,b)\neq(0,0)} \psi((a+b\delta)^2/(a-b\delta) + t(a+b\delta)).$$

Break the sum into two pieces, the first with $a = 0$. We get

$$= 1 + \sum_{b\in\mathbb{F}_q^\times} \psi((b\delta)^2/(-b\delta) + tb\delta) + \sum_{a\neq 0, b\in\mathbb{F}_q} \psi((a+b\delta)^2/(a-b\delta) + t(a+b\delta)) =$$

$$= \sum_{b\in\mathbb{F}_q} \psi((t-1)b\delta) + \sum_{a\neq 0, b\in\mathbb{F}_q} \psi((a+b\delta)^2/(a-b\delta) + t(a+b\delta)).$$

Remember that our ψ is of the form $\psi_{\mathbb{F}_q} \circ \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ for $\psi_{\mathbb{F}_q}$ a nontrivial additive character of $\mathbb{F}_q$. The first sum is q, because t, b both lie in $\mathbb{F}_q$

and δ has $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\delta) = 0$. Making the change of variable $(a,b) \mapsto (a, ab)$, the second sum becomes

$$\sum_{a\neq 0, b\in\mathbb{F}_q} \psi(a(1+b\delta)^2/(1-b\delta) + at(1+b\delta)) =$$

$$= \sum_{a\neq 0, b\in\mathbb{F}_q} \psi(a[(1+b\delta)^2 + t(1-b^2\delta^2)]/(1-b\delta)) =$$

$$= \sum_{a\neq 0, b\in\mathbb{F}_q} \psi(a\frac{[(1+b\delta)^2 + t(1-b^2\delta^2)](1+b\delta)}{1-b^2\delta^2}).$$

Expanding out the numerator, this is

$$= \sum_{a\neq 0, b\in\mathbb{F}_q} \psi(a\frac{Xb\delta + 1 + t + (3-t)b^2\delta^2}{1-b^2\delta^2}),$$

with $X \in \mathbb{F}_q$. As $\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\delta) = 0$, this is

$$\sum_{a\neq 0, b\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(2a\frac{1 + t + (3-t)b^2\delta^2}{1-b^2\delta^2}).$$

The denominator $1 - b^2\delta^2 = 1 - b^2A$ never vanishes for $b \in \mathbb{F}_q$, so adding back the $a = 0$ terms this sum is

$$-q + \sum_{a,b\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(2a\frac{1 + t + (3-t)b^2\delta^2}{1-b^2\delta^2}).$$

Recalling that the first sum was q, we end up with the formula

$$q\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = \sum_{a,b\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(2a\frac{1 + t + (3-t)b^2A}{1-b^2A}) =,$$

for $t \neq 3$,

$$= \sum_{b\in\mathbb{F}_q}\sum_{a\in\mathbb{F}_q} \psi_{\mathbb{F}_q}(2a(\frac{(3-t)A}{1-b^2A})(b^2 - \frac{t+1}{(t-3)A})).$$

Suppose now that $t \neq -1, 3$ is chosen so that $\frac{t+1}{(t-3)A}$ is a nonzero square in $\mathbb{F}_q$. Then there are exactly 2 values of b for which the factor $b^2 - \frac{1+t}{(t-3)A}$ vanishes. For each of these, the sum over a gives q. For the other values of b, the sum over a vanishes. So for such a value of $t \neq -1, 3$ in $\mathbb{F}_q$, we have

$$\mathrm{Trace}(Frob_{\mathbb{F}_{q^2},t}|\mathcal{G}) = 2.$$

Because A is a nonsquare, the requirement is that $\frac{1+t}{t-3}$ be a nonzero nonsquare. If $q \equiv 2 \bmod 3$, then by quadratic reciprocity -3 is a

nonsquare in $\mathbb{F}_q$, and we take $t = 0$. This proves (1). If $q \equiv 3 \bmod 4$, then -1 is a nonsquare in $\mathbb{F}_q$, and we take $t = 1$, proving (2). If q is a nonsquare mod 5, then by quadratic reciprocity 5 (and hence 1/5) is nonsquare in $\mathbb{F}_q$ and we take $t = -2$, proving (3). In general, the fraction $\frac{1+t}{t-3}$ assumes $q-2$ nonzero values in $\mathbb{F}_q$, so for $q \geq 5$ at least one of them is a nonsquare. The case $q = 3$ is handled by case (2), where $t = 1$ "works". This proves (4). If q is an odd power of p, the same argument shows that there exists $t \in \mathbb{F}_p$ for which $\frac{t+1}{t-3}$ is a nonsquare in $\mathbb{F}_p$ and hence in $\mathbb{F}_q$. This proves (5). □

Corollary 19.5. *For any odd q, the local system*

$$\mathcal{G} := \mathcal{G}(\mathbb{F}_{q^2}, \psi, \mathbb{1}, (q^3+1)/(q+1))$$

on $\mathbb{G}_m/\mathbb{F}_{q^2}$ has

$$G_{geom} = G_{arith} = PSU(3, q).$$

20. Supplement: Proof of Pink's theorem

Let us recall the situation. For q a power of p, Kubert proved (Theorem 9.1) that

$$\mathcal{F} := \mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, q+1)$$

has finite G_{geom}.

Theorem 20.1. (Pink) *On $\mathbb{A}^1/\mathbb{F}_{q^4}$, we have an isomorphism*

$$End(\mathcal{F}) := \mathcal{F} \otimes \mathcal{F}^\vee \cong \bigoplus_{\alpha \in F_{q^4}, \alpha^{q^2} = -\alpha} \mathcal{L}_{\psi(\alpha x)}.$$

Proof. Fix a choice of $\alpha \in F_{q^4}, \alpha^{q^2} = -\alpha$. [So $\alpha \in \mathbb{F}_{q^2}$ if q is even.] We first construct an isomorphism

$$\mathcal{F} \otimes \mathcal{L}_{\psi(\alpha x)} \cong \mathcal{F}$$

on $\mathbb{A}^2/\mathbb{F}_{q^4}$. The target is the Fourier Transform of $\mathcal{L}_{\psi((x-\alpha)^{q+1})}$, so it is equivalent to construct an isomorphism

$$\mathcal{L}_{\psi((x-\alpha)^{q+1})} \cong \mathcal{L}_{\psi(x^{q+1})}$$

on $\mathbb{A}^2/\mathbb{F}_{q^4}$. For this, we use the identity

$$(x-\alpha)^{q+1} = (x-\alpha)^q(x-\alpha) = (x^q - \alpha^q)(x-\alpha) = x^{q+1} - \alpha x^q - \alpha^q x + \alpha^{q+1} =$$

$$= x^{q+1} + \alpha^{q^2} x^q - \alpha x^q + \alpha^{q+1} = x^{q+1} + [(\alpha x^q)^q - \alpha x^q] + +\alpha^{q+1}.$$

The bracketed term is visibly Artin-Schreir equivalent to zero. The constant α^{q+1} is also of the form $\beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^4}$, simply because $\mathrm{Trace}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(\alpha^{q+1}) = 0$, as one easily checks. [When q is even, $\alpha^{q+1} \in \mathbb{F}_{q^2}$, so already $\mathrm{Trace}_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}(\alpha^{q+1}) = 0$ in this q even case.]

Now we use the fact $End(\mathcal{F})$ has a direct sum decomposition

$$End(\mathcal{F}) = End_0(\mathcal{F}) \oplus \overline{\mathbb{Q}_\ell},$$

with $End_0(\mathcal{F})$ the endomorphisms of trace zero.

Using the (inverse of the) isomorphism $\mathcal{F} \otimes \mathcal{L}_{\psi(\alpha x)} \cong \mathcal{F}$ constructed above, we get

$$End(\mathcal{F}) \cong End(\mathcal{F}) \otimes \mathcal{L}_{\psi(\alpha x)} \cong (End_0(\mathcal{F}) \oplus \overline{\mathbb{Q}_\ell}) \otimes \mathcal{L}_{\psi(\alpha x)},$$

which exhibits $\mathcal{L}_{\psi(\alpha x)}$ as a direct factor of $End(\mathcal{F})$.

Using all the α together, we get a morphism of local systems on $\mathbb{A}^2/\mathbb{F}_{q^4}$,

$$End(\mathcal{F}) \to \bigoplus_{\alpha \in F_{q^4}, \alpha^{q^2} = -\alpha} \mathcal{L}_{\psi(\alpha x)}.$$

This map is a geometric isomorphism. Indeed $End(\mathcal{F})$ is geometrically semisimple (by purity), the various $\mathcal{L}_{\psi(\alpha x)}$ are pairwise not geometrically isomorphic, and the number of them is q^2, the rank of $End(\mathcal{F})$. Being π_1^{arith}-equivariant, this map is an arithmetic isomorphism as well. □

Denote by $\mathbb{W}_q$ the one-dimensional $\mathbb{F}_{q^2}$-vector space

$$\mathbb{W}_q := \{\alpha \in \mathbb{F}_{q^4} | \alpha + \alpha^{q^2} = 0\}.$$

Corollary 20.2. (Pink) *On $\mathbb{A}^1/\mathbb{F}_{q^4}$, the sheaf $End(\mathcal{F})$ has $G_{geom} = G_{arith} = \mathbb{W}_q$.*

Proof. Indeed, for

$$\pi : \mathbb{A}^1 \to \mathbb{A}^1, t \mapsto t + t^{q^2},$$

we have

$$\pi_\star \overline{\mathbb{Q}_\ell} \cong \bigoplus_{\alpha \in \mathbb{W}_q} \mathcal{L}_{\psi(\alpha x)} \cong End(\mathcal{F}).$$

□

Corollary 20.3. (Pink) *The group $G_{geom,\mathcal{F}}$ for $\mathcal{F}$ is a finite p-group.*

Proof. As noted in Theorem 2.3, $\mathcal{F}$ has a geometrically trivial determinant. Therefore $G_{geom,\mathcal{F}}$ lies in $SL(q, \overline{\mathbb{Q}_\ell})$. Passing to $End(\mathcal{F})$ gives an isomorphism

$$G_{geom,\mathcal{F}}/(\text{scalars} \cap G_{geom,\mathcal{F}}) \cong G_{geom,End(\mathcal{F})}.$$

The target group is $\mathbb{W}_q$. The group scalars $\cap\, G_{geom,\mathcal{F}}$ is a subgroup of μ_q, the scalars in the ambient $SL(q, \overline{\mathbb{Q}_\ell})$. □

21. Second Supplement: Proof of Sawin's theorem

Theorem 21.1. (Sawin) *Suppose q is odd. The group G_{geom} for*

$$\mathcal{F} := \mathcal{F}(\mathbb{F}_q, \psi, \mathbb{1}, q+1)$$

is "the" Heisenberg group of order pq^2 and exponent p.

Proof. We exploit the fact (cf. Theorem 20.1) that for each $\alpha \in \mathbb{W}_q$, we have

$$\mathcal{F} \cong \mathcal{F} \otimes \mathcal{L}_{\psi(\alpha x)}.$$

Hence for the q^2 fold direct sum of $\mathcal{F}$, which we denote $q^2\mathcal{F}$, we have

$$q^2\mathcal{F} \cong \bigoplus_{\alpha \in \mathbb{W}} \mathcal{F} \otimes \mathcal{L}_{\psi(\alpha x)} \ \cong \mathcal{F} \otimes \pi_\star \overline{\mathbb{Q}_\ell} \cong \pi_\star \pi^\star \mathcal{F}.$$

We also know that $\pi^\star End(\mathcal{F})$ is trivial, which implies that the action of G_{geom} on $\pi^\star\mathcal{F}$ is scalar. In other words, $\pi^\star\mathcal{F}$ is q copies of a one-dimensional representation, thus we have

$$\pi^\star \mathcal{F} \cong q\mathcal{L}$$

for some lisse, rank one sheaf $\mathcal{L}$ on the "upstairs" $\mathbb{A}^1$. Applying $\pi_\star$, we get

$$q\pi_\star\mathcal{L} \cong \pi_\star\pi^\star\mathcal{F} \cong q^2\mathcal{F},$$

and hence

$$\pi_\star\mathcal{L} \cong q\mathcal{F},$$

(here using Chebotarev, and the fact that $\mathcal{F}$ is geometrically and hence arithmetically irreducible).

Using this, we next show that the Euler characteristic $\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_{q^4}}, \mathcal{L}) = -q$. Indeed, we have

$$\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_{q^4}}, \mathcal{L}) = \chi_c(\mathbb{A}^1/\overline{\mathbb{F}_{q^4}}, \pi_\star\mathcal{L}) = q\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_{q^4}}, \mathcal{F}),$$

and

$$\chi_c(\mathbb{A}^1/\overline{\mathbb{F}_{q^4}}, \mathcal{F}) = \mathrm{rank}(\mathcal{F}) - \mathrm{Swan}_\infty(\mathcal{F}) = q - (q+1) = -1.$$

Therefore $\mathcal{L}$, being lisse of rank one on $\mathbb{A}^1$, has $\mathrm{Swan}_\infty(\mathcal{L}) = q+1$.

We next show that $\mathcal{L}$ is geometrically of the form $\mathcal{L}_{\psi(ct^{q+1})}$ for some nonzero constant $c \in \overline{\mathbb{F}_q}$. The morphism π is equivariant for the action of μ_{q+1} on $\mathbb{A}^1$ given by $t \mapsto \zeta t$. The sheaf $\mathcal{F}$ is visibly isomorphic to its pullback by any $\zeta \in \mu_{q+1}$, hence so is its pullback $\pi^\star\mathcal{F} \cong q\mathcal{F}$, hence also $\mathcal{L}$. The group μ_{q+1} being cyclic, the restriction of $\mathcal{L}$ to $\mathbb{G}_m$ descends through the $q+1$-power map, to a lisse rank one sheaf $\mathcal{L}_1$ on $\mathbb{G}_m$ which is tame at 0 and whose $\mathrm{Swan}_\infty(\mathcal{L}_1) = 1$. So geometrically $\mathcal{L}_1$ is of the form $\mathcal{L}_{\chi(x)}\mathcal{L}_{\psi(cx)}$ for some nonzero $c \in \overline{\mathbb{F}_q}$. Thus $\mathcal{L}$, being lisse at 0, is geometrically $\mathcal{L}_{\psi(ct^{q+1})}$.

We next show that the constant c figuring in $\mathcal{L}_{\psi(ct^{q+1})}$ lies in $\mathbb{F}_q$. For this, we use the fact that the morphism π is equivariant for the translation action of $\mathbb{W}_q$ on $\mathbb{A}^1$. We know that $\mathcal{F}$ is isomorphic to its additive pullback by any $\alpha \in \mathbb{W}_q$. Therefore so its its pullback $q\mathcal{L}$, and hence $\mathcal{L}$ is isomorphic to any additive translate of itself by $\alpha \in \mathbb{W}_q$. Thus

$$\mathcal{L}_{\psi(c(t+\alpha)^{q+1}-ct^{q+1})}$$

is geometrically trivial. Remembering that $(x+y)^{q+1} = (x^q+y^q)(x+y)$, we readily compute

$$c(t+\alpha)^{q+1} - ct^{q+1} = c(\alpha^q t + \alpha t^q + \alpha^{q+1}) =$$

$$= c(\alpha^q t - \alpha^{q^2} t^q + \alpha^{q+1}) = (c - c^{1/q})\alpha^q t + (c^{1/q}\alpha^q t) - (c^{1/q}\alpha^q t)^q + \alpha^{q+1}).$$

Thus we have a geometric isomorphism

$$\mathcal{L}_{\psi(c(t+\alpha)^{q+1}-cx^{q+1})} \cong \mathcal{L}_{\psi(c-c^{1/q})\alpha^q t)}.$$

Taking for α a nonzero element of $\mathbb{W}_q$, this has $\mathrm{Swan}_\infty = 1$ unless $c = c^{1/q}$, i.e., unless $c \in \mathbb{F}_q$.

In order to trivialize $\mathcal{F}$, we must first pull back by π, in order to trivialize $End(\mathcal{F})$, and then we must further pull back to trivialize $\mathcal{L}$ (or equivalently to trivialize $\pi^\star\mathcal{F}$). Choose a nontrivial additive character ψ_1 of $\mathbb{F}_p$, extend it to $\mathbb{F}_q$ by composition with the trace, and write our chosen ψ as $\psi_1(ax)$ for some $a \in \mathbb{F}_q^\times$. So $\mathcal{L}$ is $\mathcal{L}_{\psi_1(cat^{q+1})}$. Thus the finite etale galois covering of the x-line which trivializes $\mathcal{F}$ is the subscheme of $\mathbb{A}^3$ given by the two equations

$$t + t^{q^2} = x, \quad z^p - z = cat^{q+1},$$

and the Galois group of this covering is our G_{geom}.

This Galois group consists of pairs

$$(\alpha \in \mathbb{W}_q, \lambda \in \overline{\mathbb{F}_q}[t] \text{ such that } \lambda^p - \lambda = ca(t+\alpha)^{q+1} - cat^{q+1}),$$

acting as

$$t \mapsto t + \alpha, \quad z \mapsto z + \lambda.$$

Let us specify

$$q = p^n.$$

In any $\mathbb{F}_p$-algebra, we have the telescoping identity

$$A^q - A = (A^p - A) + (A^p - A)^p + (A^p - A)^{p^2} + ...(A^p - A)^{p^{n-1}}.$$

So in terms of the "mock trace" polynomial

$$T(X) := \sum_{i=0}^{i=n-1} X^{p^i},$$

which is an additive $\mathbb{F}_p$-linear polynomial, we have

$$A^q - A = T(A)^p - T(A).$$

We next observe that for $\alpha \in \mathbb{W}_q$, we have

$$(\alpha^{q+1})^q = \alpha^{q^2}\alpha^q = -\alpha^{q+1}.$$

Thus

$$(\alpha^{q+1})^q - \alpha^{q+1} = -2\alpha^{q+1},$$
$$(-ca\alpha^{q+1})^q - ca\alpha^{q+1} = -2ca\alpha^{q+1},$$

and hence

$$T(-ca\alpha^{q+1}/2)^p - T(-ca\alpha^{q+1}/2) = ca\alpha^{q+1}.$$

Expanding

$$ca(t+\alpha)^{q+1} - cat^{q+1} = ca\alpha^q t + ca\alpha t^q + ca\alpha^{q+1} = ca\alpha^q t - (ca\alpha^q t)^q + ca\alpha^{q+1} =$$
$$= T(-ca\alpha^q t)^p - T(-ca\alpha^q t) + T(-ca\alpha^{q+1}/2)^p - T(-ca\alpha^{q+1}/2) =$$
$$= T(-ca\alpha^{q+1}/2 - ca\alpha^q t)^p - T(-ca\alpha^{q+1}/2 - ca\alpha^q t).$$

Thus for each element $\alpha \in \mathbb{W}_q$, the pair

$$(\alpha, T(-ca\alpha^{q+1}/2 - ca\alpha^q t))$$

is an element of the Galois group, and the most general element of the Galois group with first coordinate α is

$$(\alpha, T(-ca\alpha^{q+1}/2 - ca\alpha^q t) + r),$$

with $r \in \mathbb{F}_p$. We denote this element as

$$[\alpha, r] := (\alpha, T(-ca\alpha^{q+1}/2 - ca\alpha^q t) + r).$$

A straightforward calculation shows that under composition, we have

$$[\beta, s] \circ [\alpha, r] = [\alpha + \beta, r + s + T(-ca(\alpha^q\beta - \alpha\beta^q))].$$

For $\alpha, \beta \in \mathbb{W}_q$, one checks that

$$\alpha^q\beta - \alpha\beta^q \in \mathbb{F}_q,$$

and hence

$$T(-ca(\alpha^q\beta - \alpha\beta^q)) = \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}(-ca(\alpha^q\beta - \alpha\beta^q)).$$

To show that we have the asserted Heisenberg group, it remains only to check that the alternating $\mathbb{F}_p$-valued bilinear form on $\mathbb{W}_q$ given by

$$<\alpha, \beta> := \mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}(-ca(\alpha^q\beta - \alpha\beta^q)),$$

is a perfect pairing. If we note that $\alpha^q\beta \in \mathbb{F}_{q^2}$, and that $\alpha^q\beta - \alpha\beta^q$ is its trace down to $\mathbb{F}_q$, then

$$\mathrm{Trace}_{\mathbb{F}_q/\mathbb{F}_p}(-ca(\alpha^q\beta - \alpha\beta^q)) = \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(-ca\alpha^q\beta).$$

If we choose a basis e of $\mathbb{W}_q$ as $\mathbb{F}_{q^2}$-vector space, and write $\alpha = A^q e, \beta = Be$, then our pairing is

$$\mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(-ca\alpha^q\beta) = \mathrm{Trace}_{\mathbb{F}_{q^2}/\mathbb{F}_p}(-caABe^{q+1}).$$

As $-cae^{q+1}$ is a nonzero element of $\mathbb{F}_{q^2}$, this is a perfect pairing, by nondegeneracy of the trace. □

22. Appendix, by Pham Huu Tiep

Let $q = p^f$ be a power of a prime p. The unitary group $U(3,q)$ is the automorphism group of a 3 dimensional $\mathbb{F}_{q^2}$-space W together with a nondegenerate Hermitian form $<,>$. We work with the projective unitary group $PU(3,q) = U(3,q)/Z$, for $Z = \mathbf{Z}(U(3,q))$.

It is convenient to choose a basis (e_1, e_2, e_3) of the space W with respect to which the Hermitian form $<,>$ is

$$< e_i, e_j >= \delta_{4,i+j},$$

i.e., has the Gram matrix $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Ennola calls this the hyperbolic basis, cf. [Enn, bottom of page 30]. Then the Borel subgroup B of $PU(3,q)$ is the group of matrices

$$\begin{pmatrix} a & 0 & 0 \\ b & 1 & 0 \\ d & e & 1/a^q \end{pmatrix}$$

with entries $a \in \mathbb{F}_{q^2}^\times$, $b, d, e \in \mathbb{F}_{q^2}$, satisfying

$$ae^q + b = 0, \quad ad^q + a^q d + bb^q = 0.$$

The quasisplit torus $T_{qspl} \subset B$ is the diagonal subgroup

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/a^q \end{pmatrix}.$$

The unipotent radical R_u of B is the subgroup $a = 1$, i.e., the group of matrices

$$(x,y) := \begin{pmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ y & -x^q & 1 \end{pmatrix}, \ x, y \in \mathbb{F}_{q^2}, \ y + y^q + x^{q+1} = 0,$$

with the multiplication

$$(x,y)(X,Y) = (x + X, y + Y - x^q X).$$

It is now easy to check that

$$\mathbf{Z}(R_u) = [R_u, R_u] = \{(0, y) \mid y \in \mathbb{F}_{q^2}, y + y^q = 0\}$$

is (non canonically, unless $p = 2$) isomorphic to the additive group $(\mathbb{F}_q, +)$; in particular, it is an elementary abelian p-group of order q.

The quotient $R_u/\mathbf{Z}(R_u)$ is isomorphic to the additive group $(\mathbb{F}_{q^2}, +)$ and so it is elementary abelian of order q^2. It follows that the Frattini subgroup $\Phi(R_u)$ (i.e. the intersection of all maximal subgroups of R_u) coincides with $\mathbf{Z}(R_u)$.

Lemma 22.1. *For any $g \in R_u \smallsetminus \mathbf{Z}(R_u)$, one has*

$$[g, R_u] = \mathbf{Z}(R_u).$$

Proof. Indeed, any element of $\mathbf{Z}(R_u)$ is of the form $(0, c - c^q)$ for some $c \in \mathbb{F}_{q^2}$. For $g = (a, b)$ with $a \neq 0$, the commutator $[(a, b), (X, 0)]$ is readily calculated to be $(0, aX^q - a^q X)$, so we have only to take $X = (c/a)^q$. □

Theorem 22.2. *Up to isomorphism, the group R_u has q^2+q-1 complex irreducible representations, namely*

(a) *q^2 of degree 1, and*
(b) *$q - 1$ irreducible representations H_ψ of degree q, one for each nontrivial linear character ψ of $\mathbf{Z}(R_u)$.*

Moreover, we have the following information about the representations H_ψ.

(c) *The character χ_ψ of H_ψ vanishes on $R_u \smallsetminus \mathbf{Z}(R_u)$ and equals $q\psi$ on $\mathbf{Z}(R_u)$.*
(d) *The characters $\{\chi_\psi\}_\psi$ of these $q-1$ irreducible representations H_ψ are transitively permuted by T_{qspl}.*

Proof. As mentioned above, $[R_u, R_u] = \mathbf{Z}(R_u)$ has index q^2 in R_u, whence $\mathrm{Irr}(R_u)$ contains exactly q^2 linear characters. Let $H \in \mathrm{Irr}(R_u)$ be an irreducible representation $H : R_u \to GL(d, \mathbb{C})$ with $d > 1$. The center $\mathbf{Z}(R_u)$ acts as scalars, and that action is nontrivial (otherwise H would be a representation of the abelian group $R_u/\mathbf{Z}(R_u)$). So there is a nontrivial linear character ψ of $\mathbf{Z}(R_u)$ such that for all $t \in \mathbf{Z}(R_u)$ and all $g \in R_u$ we have

$$H(tg) = H(gt) = \psi(t)H(g).$$

In particular,

$$H(t) = \psi(t)H(1), \text{ i.e., } H|_{\mathbf{Z}(R_u)} = d\psi.$$

Because ψ is nontrivial, there exists an element $z \in \mathbf{Z}(R_u)$ with $\psi(z) \neq 1$. For any $g \in R_u \smallsetminus \mathbf{Z}(R_u)$, there exists (by Lemma 22.1 applied to g^{-1}) an element $x \in R_u$ such that $x^{-1}gx = gz$. Then

$$H(x^{-1}gx) = H(gz) = \psi(z)H(g).$$

Taking traces, we obtain $\chi_H(g) = \psi(z)\chi_H(g)$, and so $\chi_H(g) = 0$. Thus

$$\chi_H = 0 \text{ on } R_u \smallsetminus \mathbf{Z}(R_u).$$

The orthogonality relation then gives

$$q^3 = \sum_{y \in R_u} |\chi_H(y)|^2 = \sum_{y \in \mathbf{Z}(R_u)} |\chi_H(y)|^2 = qd^2,$$

and so $d = q$.

We have shown that each non-linear character χ of R_u has degree q, whence there must be $(q^3 - q^2)/q^2 = q - 1$ of them. The above analysis shows that each of them is determined by its central character, which is one of the $q-1$ nontrivial characters of $\mathbf{Z}(R_u)$. Therefore there exists the asserted H_ψ for each nontrivial character ψ of $\mathbf{Z}(R_u)$, and these H_ψ give all the non-linear irreducible representations of R_u.

To prove the last assertion (d), pick an element $x \in \mathbb{F}_{q^2}^\times$ of full order $q^2 - 1$. Then T_{qspl} contains the element $h := \mathrm{diag}(x, 1, x^{-q})$ of order $q^2 - 1$. Since $h(0, b)h^{-1} = (0, x^{-q-1}b) = (0, b/\mathrm{Norm}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x))$, we conclude that h acts a cyclic permutation of length $q - 1$ on both the nontrivial elements of $\mathbf{Z}(R_u)$ and on the set of nontrivial characters of $\mathbf{Z}(R_u)$. □

References

[Be-Ev-Wi] Berndt, B.C., Evans, R.J., and Williams, K.S., Gauss and Jacobi Sums, Can. Math. Soc. Series of Monographs and Advanced Texts, Wiley, New York, 1998, xii+583 pp.

[Brauer] Brauer, R.,Über endliche lineare Gruppen von Primzahlgrad, Math. Ann. 169 (1967), 73-96.

[Brauer2] Brauer, R., On the order of finite projective groups in a given dimension, Nachr. Akad. Wiss. Göttingen Math-PhysKl. II (1969), 103-106.

[C-W] Cohen, A., Wales, D., Finite subgroups of G2(C). Comm. Algebra 11 (1983), no. 4, 441-459.

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

[De-Weil II] Deligne, P., La conjecture de Weil. II. Inst. Hautes Études Sci. Publ. Math. No. 52 (1980), 137-252.

[Enn] Ennola, V., On the characters of the finite unitary groups, Ann. Acad. Sci. Fenn. 323 (1963) 35 pp.

[Evans] Evans, Ron, notes available at `http://math.ucsd.edu/~revans/katzconj.pdf`, June, 2017.

[Feit] Feit, W., Groups which have a faithful representation of dimension $< p-1$, Trans. Am. Math. Soc. 112 (1964),287-303.

[F-T] Feit, W.,Thompson, J., Groups which have a faithful representation of degree less than (p-1/2). Pacific J. Math. 11 (1961), 1257-1262.

[Fu] Fu, L., Calculation of ℓ-adic local Fourier transformations. Manuscripta Math. 133 (2010), no. 3-4, 409-464.

[Ga] Garrett, P., Heisenberg groups over finite fields, 21014-2015 lecture notes available at `www.math.umn.edu/~garrett/m/repns/notes_2014-15/05_finite_heisenberg_ssw.pdf`.

[Grove] Grove, L., Classical Groups and Geometric Algebra, Grad. Studies in Math. 39, Amer. Math. Soc,., Providence, R.I., 2001, xi +169 pp.

[GMT] Guralnick, R., Maagard, K., Tiep, P.H., Symmetric and alternating powers of Weil representations of finite symplectic groups, preprint.

[Gross] Gross, B. H., Rigid local systems on $\mathbb{G}_m$ with finite monodromy. Adv. Math. 224 (2010), no. 6, 2531-2543.

[Gr-Lef] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L. Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, Paris, 1995.

[Hiss-Malle] Hiss, G., Malle, G., Low-dimensional representations of special unitary groups. J. Algebra 236 (2001), no. 2, 745-767.

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

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

[Ka-G2hyper] Katz, N., G_2 and hypergeometric sheaves, Finite Fields Appl. 13 (2007), no. 2, pp. 175-223.

[Ka-LFM] Katz, N., L-functions and monodromy: four lectures on Weil II. Adv. Math. 160 (2001), no. 1, 81-132

[Ka-MG] Katz, N., On the monodromy groups attached to certain familiies of exponential sums, Duke Math. J.,vol, 34, no. 1 (1987), 41-56.

[Kubert] Kubert, D.,Lectures at Princeton University, May 1986.

[Ka-MMP] Katz, N., Moments, monodromy, and perversity: a Diophantine perspective. Annals of Mathematics Studies, 159. Princeton University Press, Princeton, NJ, 2005. viii+475 pp.

[Ka-NG2] Katz, N., Notes on G2, determinants, and equidistribution. Finite Fields Appl. 10 (2004), no. 2, 221-269.

[Ka-RLS] Katz, N., Rigid Local Systems. Annals of Mathematics Studies 139, Princeton University Press, Princeton, NJ, 1996, viii+223 pp.

[Ka-WVQKR] Katz,N., Witt vectors and a question of Keating and Rudnick. Int. Math. Res. Not. IMRN (2013), no. 16, 3613-3638.

[Lau-FT] Laumon, G., Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil. Inst. Hautes Études Sci. Publ. Math. No. 65 (1987), 131-210.

[Pink] Pink, R., Lectures at Princeton University, May 1986.

[Ray] Raynaud, M. Revêtements de la droite affine en caractéristique p $>$ 0 et conjecture d'Abhyankar. Invent. Math. 116 (1994), no. 1-3, 425-462.

[Lusztig] Lusztig, G., Coxeter orbits and eigenspaces of Frobenius, Invent. Math. 38 (1976). 101-159.

[Tuan] Tuan, H.-F, On Groups Whose Orders Contain a Prime Number to the First Power, Ann. Math., Second Series, 45 (1944), pp.110-140.

Department of Mathematics, Princeton University, Princeton, NJ 08544

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

Department of Mathematics, Rutgers University, Piscataway, NJ 08904

E-mail address: tiep@math.rutgesr.edu