Big symplectic or orthogonal monodromy modulo ℓ

Chris Hall *

April 23, 2007

Abstract

Let k be a field not of characteristic two and Λ be a set consisting of almost all rational primes invertible in k. Suppose we have a variety X/k and strictly compatible system $\{\mathcal{M}_\ell \to X : \ell \in \Lambda\}$ of constructible $\mathbb{F}_\ell$-sheaves. If the system is orthogonally or symplectically self-dual, then the geometric monodromy group of $\mathcal{M}_\ell$ is a subgroup of a corresponding isometry group Γ_ℓ over $\mathbb{F}_\ell$, and we say it has big monodromy if it contains the derived subgroup $\mathcal{D}\Gamma_\ell$. We prove a theorem which gives sufficient conditions for $\mathcal{M}_\ell$ to have big monodromy. We apply the theorem to explicit systems arising from the middle cohomology of families of hyperelliptic curves and elliptic surfaces to show that the monodromy is uniformly big as we vary ℓ and the system. We also show how it leads to new results for the inverse Galois problem.

1 Introduction

Galois theory in its various forms is one of the main and most powerful tool of arithmeticians and geometers, and in particular the determination of the Galois group of some field extensions or coverings of algebraic varieties (or differential Galois group of some equations) is often both an important step in solving certain problems and a very interesting question of its own. Whereas finding "upper bounds" for those Galois groups can be relatively easy (coming from the existence of symmetries that must be preserved), it is usually quite challenging to compute exactly the Galois groups. What is expected is that, given the known symmetry constraints, the Galois group will "usually" be the largest group preserving those symmetries; indeed, this is often the desired conclusion for applications. There are many celebrated results of this type, among which are Serre's computations of Galois groups of torsion fields of elliptic curves over number fields [S2], Katz's monodromy computations in algebraic geometry leading to equidistribution statements for angles of Kloosterman sums [Ka1], and some cases of the inverse Galois problem [Hi], [Sha1].

It is desirable to have criteria to compute Galois groups and to show they are "as big as possible", and it is most important that those criteria involve conditions that can be checked in practice. This paper considers an important class of situations where the groups involved are finite orthogonal or symplectic groups over $\mathbb{F}_\ell$. There are quite a few applications where such groups arise, and we describe the motivating one in section 2. Here is the simplified (and weakened) statement of the group theoretical criterion we will prove:

*Department of Mathematics, University of Texas, Austin, TX 78712, USA, cjh@math.utexas.edu

Theorem 1.1. *Let V be an $\mathbb{F}_\ell$-vector space together with a perfect pairing $V \times V \to \mathbb{F}_\ell$ and let $G \leq \mathrm{GL}(V)$ be an irreducible primitive subgroup which preserves the pairing. If the pairing is symmetric, G contains a reflection and an isotropic shear, and $\ell \geq 5$, then G is one of the following:*

1. *the full orthogonal group $O(V)$;*
2. *the kernel of the spinor norm;*
3. *the kernel of the product of the spinor norm and the determinant.*

If the pairing is alternating, G contains a transvection, and $\ell \geq 3$, then G is all of the symplectic group $\mathrm{Sp}(V)$.

For group-theoretic terms (e.g. transvection or isotropic shear) see section 3. Rather than assuming G is primitive, in which case we could appeal to [Wa1] or [Wa2] (cf. section 6 of [DR]), we make explicit assumptions about a set of elements generating G and show that they (essentially) imply G is primitive. In section 3 we also give a full statement of the theorem and its proof, and in the last two sections we give applications. Among those we single out (because it is easy to state and to prove) the following (unpublished) theorem of J-K. Yu.

Theorem 1.2. *The mod-ℓ geometric monodromy of hyperelliptic curves is $\mathrm{Sp}(2g, \mathbb{F}_\ell)$ for $\ell > 2$.*

See [Yu] for the preprint containing Yu's original proof or [AP] for another recent independent proof. The theorem has been used in several contexts. Yu originally proved his theorem in order to study the Cohen-Lenstra heuristics over function fields. Chavdarov [C] applied the theorem to study the irreducibility of numerators of zeta functions of families of curves over finite fields and Kowalski used his results to study the torsion fields of an abelian variety over a finite field [Kow2]. Achter applied Yu's theorem in [Ac] to prove a conjecture of Friedman and Washington on class groups of quadratic function fields.

In the last section of the paper we give applications of our group theorem to families of quadratic twists of elliptic curves. In addition to solving the motivating problem described in 2 we derive new results for the inverse Galois problem. More precisely, in section 6.5 we show how big subgroups of orthogonal groups arise as Galois group over $\mathbb{Q}(t)$. Both this application and our application to Yu's theorem rely on Katz's theory of middle convolution, and we summarize the relevant results in section 4.

1.1 Acknowledgements

We would like to thank D. Allcock, N.M. Katz, M. Olsson, D. Ulmer, and J.F. Voloch for several helpful conversations during the course of research and for their interest in this work, and we would like to thank the anonymous referree for carefully reading the paper and making several helpful suggestions for improving the exposition. We would also like to thank E. Kowalski for asking the question which motivated this paper, for suggesting that we could extend our results, originally for orthogonal monodromy, to symplectic monodromy, and for his generous feedback on earlier drafts of this paper. Finally, we must acknowledge the enormous influence of our mentor N.M. Katz. This paper would not exist without [Ka3] and we hope that it will serve as a useful complement.

1.2 Notation

We use the notation $n \gg_{i_1,\ldots,i_m} 0$ to mean that there is a constant $n_0(i_1,\ldots,i_m)$ depending on the objects $i_1,\ldots,i_m$ such that $n \geq n_0(i_1,\ldots,i_m)$. In nearly every case the bound can be made explicit, but we usually do not because all that matters is to determine the input objects $i_1,\ldots,i_m$.

2 Motivation and Strategy

Let k be a field, C/k be a proper smooth geometrically-connected curve, $K = k(C)$, and E/K be an elliptic curve with non-constant j-invariant. In a recent paper [Kow1], E. Kowalski asked whether one could prove uniform big $\mathbb{F}_\ell$-monodromy results for certain sequences of quadratic twists of E when $k = \mathbb{F}_q$. He went on to show how a sufficiently strong uniform bound (as ℓ varies) would allow one to prove a previously untreated variant of Goldfeld's average-rank conjecture, although the type of bounds he required were well beyond known results. One piece of evidence in favor of the existence of sufficient bounds was theorem 1.2, an unpublished theorem due to J.-K. Yu. Roughly speaking, the key property both situations share is that the monodromy groups arise from middle cohomology of varieties. One goal of this paper is to complete Kowalski's proof by proving bounds of the sort he requires. We will also show how our methods can be used to reprove Yu's theorem.

A striking aspect of Kowalski's variant is that both q *and* the degree of the conductor of the twisted curve tend to infinity in constrast with [Ka3] where only q grows. Katz fixes the degree of the conductor for the very important reason that he wants to restrict to nice sequences of twists which are all elements of a *single* nice geometric family. This allows him to bring Deligne's equidistribution theorem to bear on a variant of Goldfeld's conjecture by phrasing it in terms of monodromy groups of $\mathbb{Q}_\ell$-sheaves. Kowalski, on the other hand, must contend with an infinite sequence of geometric families, and he uses monodromy groups of $\mathbb{F}_\ell$-sheaves and the Čebotarev density theorem as well as sieve techniques to prove his results. A key difference between the two approaches is that, for a fixed family of twists, the $\mathbb{Q}_\ell$-monodromy groups are algebraic and essentially independent of ℓ while the $\mathbb{F}_\ell$-monodromy groups are finite and vary with ℓ.

We fix a dense affine open $U \subset C$ and an algebraic closure $k \to \overline{k}$. We fix a geometric point $x \in U$, that is, an embedding $\mathrm{Spec}(L) \to U$ for L/k an algebraically-closed extension. We write $\pi_1(U) = \pi_1(U,x)$ for the étale fundamental group and $\pi_1^g(U)$ for the geometric fundamental group $\pi_1(U \times \overline{k}) \leq \pi_1(U)$. We fix a set Λ of almost all odd primes ℓ which are invertible in k. For each $\ell \in \Lambda$, we fix a lisse flat $\mathbb{Z}_\ell$-sheaf $\mathcal{L}_\ell \to U$ and let $\rho_\ell : \pi_1(U) \to \mathrm{GL}_n(\mathbb{Z}_\ell)$ denote the corresponding representation. A priori n depends on ℓ, but we assume the family of representations $\{\rho_{\ell,\eta} = \rho_\ell \otimes \mathbb{Q}_\ell\}$ is a strictly compatible system in the sense of Serre [S1]; that is, for every $\ell \in \Lambda$, the characteristic polynomials of the Frobenii in $\rho_{\ell,\eta}$ have coefficients in $\mathbb{Q}$ and are independent of ℓ. We write $\mathcal{M}_\ell \to U$ for the lisse $\mathbb{F}_\ell$-sheaf $\mathcal{L}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell \to U$ and say that the family $\{\mathcal{M}_\ell \to U\}$ is a *(strictly) compatible system.*

For each ℓ, we write $G_\ell^a \leq \mathrm{GL}_n(\mathbb{F}_\ell)$ for the image $(\rho_\ell \otimes \mathbb{F}_\ell)(\pi_1(U))$ and $G_\ell^g \leq G_\ell^a$ for the image of $\pi_1^g(U)$. A priori G_ℓ^a may be any subgroup of $\mathrm{GL}_n(\mathbb{F}_\ell)$, but if we consider additional arithmetic information, then we may be able to deduce that G_ℓ^a lies in a proper subgroup $\Gamma_\ell^a \leq \mathrm{GL}_n(\mathbb{F}_\ell)$. For example, if there is a non-degenerate pairing $\mathcal{M}_\ell \times \mathcal{M}_\ell \to \mathbb{F}_\ell(m)$ for some Tate twist $\mathbb{F}_\ell(m) \to U$, then we say $\mathcal{M}_\ell$ is *self dual* and we may define Γ_ℓ^a to be the subgroup of similitudes for the pairing

whose determinants are powers of q^m. One can prove a similar geometric statement: if $\mathcal{M}_\ell$ is self dual and we define $\Gamma_\ell^g \leq \Gamma_\ell^a$ to be the subgroup of isometries of the pairing, then G_ℓ^g lies in Γ_ℓ^g.

In this paper we will assume $\mathcal{M}_\ell$ is self dual and $\Gamma_\ell = \Gamma_\ell^g \leq \mathrm{GL}_n(\mathbb{F}_\ell)$ is the corresponding isometry group as above for every $\ell \in \Lambda$. We will also assume the pairing $\mathcal{M}_\ell \times \mathcal{M}_\ell \to \mathbb{F}_\ell(m)$ is either always symmetric or always anti-symmetric, hence Γ_ℓ is orthogonal or symplectic respectively; recall ℓ is odd. We say $\mathcal{M}_\ell$ has *big monodromy* if $n = \mathrm{rk}(\mathcal{M}_\ell) > 1$ and $G_\ell = G_\ell^g$ contains the derived group $\mathcal{D}\Gamma_\ell = [\Gamma_\ell, \Gamma_\ell]$. If Γ_ℓ is an orthogonal group, then $\mathcal{D}\Gamma_\ell$ is the intersection of the kernel of the determinant and the kernel of the spinor norm and has index four. If Γ_ℓ is a symplectic group, then $\Gamma_\ell = \mathcal{D}\Gamma_\ell$. In particular, if we write Λ_{big} for the $\ell \in \Lambda$ where $\mathcal{M}_\ell$ has big monodromy, then in either case the index of G_ℓ in Γ_ℓ is uniformly bounded for $\ell \in \Lambda_{\mathrm{big}}$ and $\Lambda - \Lambda_{\mathrm{big}}$ is finite, which are the sort of properties Kowalski wants (see (16) of [Kow1]).

Remark: A priori we could relax the definition of Λ_{big} to include all $\ell \in \Lambda$ such that G_ℓ has index at most b in Γ_ℓ for some fixed b, but we note that the two definitions are in fact the same for $\min\{\ell, n\} \gg_b 0$. More precisely, the index of the largest proper subgroup of $\mathcal{D}\Gamma_\ell$ grows with $\min\{\ell, n\}$ (see table 5.2.A of [KL]), so if $\min\{\ell, n\} \gg_b 0$, then there is no proper subgroup of $\mathcal{D}\Gamma_\ell$ of index at most b.

One of the simplest examples of a compatible system with big monodromy can be constructed from the ℓ-torsion of our elliptic curve E/K from above (cf. section 6.1). Then G_ℓ^a is the Galois group of $K(E[\ell])/K$, G_ℓ^g is the Galois group of $\overline{k}K(E[\ell])/\overline{k}K$, and the function-field analogue of Serre's theorem implies $G_\ell = \Gamma_\ell$ for almost all ℓ; note $\Gamma_\ell \simeq \mathrm{Sp}_2(\mathbb{F}_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$. If we write $g(C)$ for the genus of C and $\ell \gg_{g(C)} 0$, then $G_\ell = \Gamma_\ell$ by theorem 1.1 of [CH]. We note that this strong uniformity was a crucial ingredient in the proof of theorem 1.2 of that paper.

A more general example is to fix an abelian variety A/K of higher dimension with trivial K/k-trace and consider the compatible system constructed from the ℓ-torsion. If we restrict the endomorphism ring and dimension of A, then theorem 3 of [S3] implies $\ell \in \Lambda_{\mathrm{big}}$ for $\ell \gg_A 0$, but little seems to be known in general otherwise. In particular, if we fix the genus of C and bound the dimensions of A and its $\overline{K}$-endomorphism ring, then we do not know if Λ_{big} may be chosen independently of A. We suspect that already for $C = \mathbb{P}^1$ and $\dim(A) \gg 0$ that no uniform bound exists because, roughly speaking, the corresponding 'modular varieties' are large and for arbitrarily large ℓ could conceivably contain at least one line.

For general systems it is natural to ask how big Λ_{big} is (cf. 10.7? of [S4]). The answer is interesting only if the Zariski closure of $\rho_{\ell,\eta}(\pi_1^g(U))$ in $\mathrm{GL}_n(\mathbb{Q}_\ell)$ is itself big in an appropriate sense for any (and hence every) $\ell \in \Lambda$, so we assume it is. Then one can often use general methods to show that Λ_{big} has Dirichlet density one (see [L]) or even that it contains almost all ℓ (see [MVW], [N] or [S3]). However, the subset of $\ell \in \Lambda_{\mathrm{big}}$ which these methods yield can be difficult to describe or control, and in Kowalski's case they are insufficient (see discussion at end of section 5 of [Kow1]). In particular, if we let the rank n tend to infinity, then these methods force us to restrict to $\ell \gg_n 0$ where the implicit lower bound for ℓ tends to infinity with n (e.g. so that one can apply characteristic zero arguments).

The main goal of this paper is to demonstrate how one can prove lower bounds for Λ_{big} without this restriction. The strategy we use to achieve this is to show G_ℓ is an irreducible subgroup of Γ_ℓ and then to apply theorem 3.1 where we give sufficient criteria, in terms of a set of generators, for an irreducible subgroup to contain $\mathcal{D}\Gamma_\ell$. More precisely, we show that the subgroup $R_\ell \leq G_\ell$ generated by the pseudoreflections is also irreducible and use the classifications in [ZS1] and [ZS2]

to show that $\mathcal{D}\Gamma_\ell \leq R_\ell$.

For our first application we return to our last example from above and let Λ be the set of all odd primes ℓ which are invertible in K. We also let $C = \mathbb{P}^1$ and let A/K be the Jacobian of a curve in a special class of hyperelliptic curves constructed in section 5, and in theorem 5.1 we reprove Yu's theorem and show that $\Lambda = \Lambda_{\text{big}}$. Katz has pointed out that the key ideas used in the proof generalize to tamely ramified compatible systems arising from the middle cohomology of the fibers of a Lefschetz pencil $\mathcal{X} \to \mathbb{A}^1$ of odd relative dimension, where $\mathbb{A}^1 = \mathbb{P}^1 - \{\infty\}$. Moreover, in this case one does not need the full power of theorem 3.1 to show that $\Lambda_{\text{big}} = \Lambda$, but instead one can appeal directly to the main theorem of [ZS2].

The real power of theorem 3.1 emerges only when we consider more general compatible systems. For example, in section 6 we examine systems arising from families of quadratic twists of the elliptic curve E/K when $K = \mathbb{F}_q(t)$. We recall the construction due to Katz [Ka3] of an affine variety $F_d/\mathbb{F}_q$ which parametrizes quadratic twists of E/K by a 'dense open' subset of the square-free polynomials in $\overline{\mathbb{F}}_q[t]$ of degree d. We also construct, for each ℓ, the orthogonally self-dual lisse $\mathbb{F}_\ell$-sheaf $\mathcal{T}_{d,\ell} \to F_d$ whose fibers encode the reduction modulo ℓ of the (unitarized) L-function of the corresponding twists (cf. section 6.1); it corresponds to a Tate twist of the $\mathbb{Q}_\ell$-sheaf constructed by Katz. He proved that the $\mathbb{Q}_\ell$-monodromy is big if $d \gg_E 0$ (cf. theorem 1.4.3 of *loc. cit.*), and we prove something similar in theorem 6.3: if $\ell \geq 5$ and $d \gg_E 0$, then $\ell \in \Lambda_{\text{big}}$.

The strategy we follow to prove theorem 6.3 is to show that the monodromy of the restriction to some one-parameter family is big. More precisely, for each $g \in F_{d-1}$ we construct a dense open $U_g \subset \mathbb{A}^1$ and a non-constant map $j_g : U_g \to F_d$ for which the pullback $j_g^*\mathcal{T}_{d,\ell} \to U_g$ has big monodromy. Up to replacing E/K by the quadratic twist E_g/K and shrinking U_g, this reduction amounts to restricting to the one-parameter family of twists by $c - t$ where $c \in U_g$. We apply Katz's theory of middle convolution to analyze the monodromy of such a family, and in theorem 6.4 we show that $j_g^*\mathcal{T}_{d,\ell}$ has big monodromy if $\ell \geq 5$ and $d \gg_{j(E)} 0$, where $j(E)$ is the j-invariant of E. In particular, as we vary d, g the collection of compatible systems $\{j_g^*\mathcal{T}_{d,\ell} \to U_g\}$ suffices for Kowalski's purposes.

We note that one can prove similar results for quadratic twists of more general systems for C of arbitrary genus. Fix a dense open $V \subset C$ and a self-dual compatible system $\{\mathcal{K}_\ell \to V\}$ such that, for each $\ell \in \Lambda$, the sheaf $\mathcal{K}_\ell \to V$ is tame, irreducible, and the monodromy around at least one geometric point of $C - V$ is pseudoreflection. We can construct, for each divisor $D > 0$ supported on $C - V$, a parameter space $F_D/\mathbb{F}_q$ of functions which is a 'dense open' subset of the Riemann-Roch space of D (cf. section 5.0 of [Ka3]) and a corresponding compatible system $\{\mathcal{T}_{D,\ell} \to F_D\}$. The fibers of $\mathcal{T}_{D,\ell} \to F_D$ are the quadratic twists of $\mathcal{K}_\ell \to V$ and the system $\{\mathcal{T}_{D,\ell} \to F_D\}$ is self-dual of the symmetry type opposite that of $\{\mathcal{K}_\ell \to V\}$. If we fix a sufficiently nice map $t : C \to \mathbb{P}^1$ whose polar divisor is $[e]D$ for some e, then one can argue as above to show $\mathcal{T}_{[de]D,\ell} \to F_{[de]D}$ has big monodromy for $\ell, d \gg_D 0$.

3 Subgroups of Finite Symplectic and Orthogonal Groups

Throughout this section we fix an odd prime ℓ and a vector space V over $\mathbb{F}_\ell$ together with a non-degenerate bilinear pairing. We assume that the pairing is either symmetric or alternating, and in the first case we also add the assumption that $\ell \geq 5$. We write $\langle w, v \rangle$ for the pairing of $w, v \in V$

and for a subspace $W \leq V$ we write $W^\perp$ for the orthogonal complement of V and $\mathrm{Rad}(W)$ for the intersection $W \cap W^\perp$. We write $\Gamma \leq \mathrm{GL}(V)$ for the subgroup preserving the pairing. If the pairing is symmetric (resp. alternating), then we write $\Gamma = O(V)$ (resp. $\Gamma = \mathrm{Sp}(V)$).

Given an element $\gamma \in \Gamma$ we write $V^{\gamma=a}$ for the subspace of V on which γ acts as the scalar $a \in \mathbb{F}_\ell^\times$, V^γ for $V^{\gamma=1}$, and V_γ for $(\gamma - 1)V$. We define the *drop* of an element $\gamma \in \Gamma$ to be the codimension of the invariant subspace $V^{\gamma=1}$. If $\gamma \in \Gamma$ is an element of drop 1, we say it is a *reflection* if $\det(\gamma) = -1$ and a *transvection* if $\det(\gamma) = 1$. In either case we call γ a *pseudoreflection* and a non-zero element of $(V^{\gamma=1})^\perp$ a *root*; the latter spans $V_\gamma = (V^{\gamma=1})^\perp$. We call a non-trivial element $\sigma \in \Gamma$ an *isotropic shear* if it is unipotent and $(\sigma - 1)^2 = 0$, and we note that the image of $\sigma - 1$ is a non-trivial isotropic subspace of V and necessarily $\dim(V) \geq 4$ when the pairing on V is symmetric.

REMARK: If the pairing on V is symmetric and $\mathrm{drop}(\sigma) = 2$, then what we call an isotropic shear is sometimes called a Siegel transvection. We use the term shear in order to avoid confusion with what we call a transvection. It is an elementary exercise to show that there are no (usual) transvections in the case $\Gamma = O(V)$.

REMARK: What we call an isotropic shear is a quadratic element in the sense of Thompson [T].

We say a subgroup $G \leq \Gamma$ is *irreducible* if V is an irreducible G-representation. We say G is *imprimitive* if V, as a G-representation, is induced from a proper subgroup of G and otherwise we say G is *primitive*. We note G is imprimitive if and only if there is a non-trivial subspace $W < V$ such that V decomposes as a direct sum $\oplus_{G/H} gW$ of the G-translates gW over all cosets gH (cf. section 12.D of [CR]).

We devote the rest of this section to the proof of the following theorem.

Theorem 3.1. *Let $r \geq 1$ and suppose $G \leq \Gamma$ is an irreducible subgroup together with a set of generators $S \subset G$ and a subset $S_0 \subset S$ satisfying the following properties:*

1. $\mathrm{drop}(\gamma) \leq r$ *for every* $\gamma \in S$;
2. *every* $\gamma \in S - S_0$ *has order prime to* $(r+1)!$ *or is a pseudoreflection;*
3. $2(r+1)|S_0| \leq \dim(V)$.

If the pairing is symmetric and G contains a reflection and an isotropic shear, then G is one of the following:

1. *the full orthogonal group $O(V)$;*
2. *the kernel of the spinor norm;*
3. *the kernel of the product of the spinor norm and the determinant.*

If the pairing is alternating and G contains a transvection, then G is all of $\mathrm{Sp}(V)$.

REMARK: The subgroups of $O(V)$ enumerated above are the subgroups of index at most two excluding $SO(V)$.

If the pairing on V is symmetric, then G contains one or more reflections, each of which has determinant -1. Otherwise the pairing is alternating and G contains one or more transvections. We write $R \trianglelefteq G$ for the normal subgroup generated by all pseudoreflections. It is non-trivial, although a priori it might be a proper subgroup of G. Our proof will show that it satisfies the conclusions of the theorem, hence so does G.

While one can give explicit formulas for pseudoreflections in terms of the pairing and roots, it is not necessary for what follows. For a fixed pseudoreflection $\gamma \in R$ most of the information about γ is contained in the proper subspaces $V_\gamma, V^\gamma < V$. These spaces satisfy the key identity $V_\gamma^\perp = V^\gamma$ and $\langle\gamma\rangle \leq R$ contains every pseudoreflection in R with the same (one-dimensional) root subspace. If the pairing is symmetric, then γ is semisimple and $V_\gamma = V^{\gamma=-1}$, hence $V = V_\gamma \oplus V^\gamma$. Otherwise γ is unipotent and it preserves the flag $0 < V_\gamma \leq V^\gamma < V$; the same statement is true for an isotropic shear.

Lemma 3.2. *If $W \leq V$ is a non-trivial irreducible R-submodule and $H = N_G(W) \leq G$ is the stabilizer, then* $\mathrm{Rad}(W) = 0$ *and* $V = \bigoplus_{G/H} gW$.

Proof. Every G-translate gW is an R-submodule because R is a normal subgroup of G. Some pseudoreflection γ acts non-trivially on W because otherwise $R = gRg^{-1}$ would act trivially on gW, hence on all of $V = \sum gW$, which is impossible. Therefore the subspace of W spanned by the roots contained in W is non-trivial. It is also an R-submodule, hence must be all of W, because the conjugate of a pseudoreflection is a pseudoreflection and so R permutes the roots in W. Thus we may write $W = \sum_\gamma W_\gamma$ where γ varies over the pseudoreflections in R and $W_\gamma = W \cap V_\gamma$.

If γ acts non-trivially on W, then $W_\gamma^\perp = V_\gamma^\perp = V^\gamma$. Therefore, if we write $S \leq R$ for the subgroup generated by all pseudoreflections γ which act non-trivially on W, then $W = \sum_{\gamma\in S} W_\gamma$ and $W^\perp = \cap_\gamma V^\gamma = V^S$. In particular, $\mathrm{Rad}(W) = W \cap W^\perp = W \cap V^S$ is the proper, hence trivial, R-submodule W^S. This proves the first part of the lemma.

If $gW \neq W$ and γ is a pseudoreflection, then $W_\gamma \cap (gW)_\gamma = 0$ because $W \cap gW = 0$. Moreover, if γ acts non-trivially on W, then $W_\gamma = V_\gamma$ and gW lies in $V^\gamma = W_\gamma^\perp$. Therefore gW lies in $V^S = W^\perp$ because $W = \sum_\gamma W_\gamma$, hence in general $g_1W \perp g_2W$ if and only if $g_1W \neq g_2W$. In particular, the sum of any proper subset of G-translates lies in the complement of any unused G-translate, hence the sum cannot be all of V. Therefore V decomposes as the direct sum of all G-translates and, in particular, $V = \oplus_{G/H} gW$ because $g_1W = g_2W$ if and only if $g_1H = g_2H$. □

Our main interest in lemma 3.2 is that it allows us to prove the following lemma, which in turn will allow us to use classification results about irreducible subgroups of $\mathrm{GL}(V)$ generated by pseudoreflections.

Lemma 3.3. *R is irreducible.*

Remark: The argument we give below was inspired by an argument of Katz for $\mathbb{Q}_\ell$-monodromy (1.6.4 of [Ka3]).

Proof. Let $W \leq V$ and $H \leq G$ be as in the statement of lemma 3.2. If $\dim(W) \geq r + 1$, then, for every $\gamma \in S$, the intersection $V^\gamma \cap W$ is non-trivial because $\mathrm{drop}(\gamma) \leq r$, hence $\gamma W = W$; note, $\gamma_1 W = \gamma_2 W$ if and only if $\gamma_1 H = \gamma 2_2 H$, otherwise $\gamma_1 W \cap \gamma_2 W = 0$ (cf. (12.26) of [CR]).

Therefore W is stabilized by G because S generates G, hence $W = V$ by the irreducibility of G. On the other hand, we cannot have $\dim(W) \leq r$ because otherwise we will show that it would imply $\dim(V) < 2(r+1) \cdot |S_0|$, contrary to the hypotheses of theorem 3.1. To prove this we need two lemmas.

Lemma 3.4. *For every $\gamma \in S$, if $\{g_i W\}$ is a subset of at least $(r+1)/\dim(W)$ G-translates, then $\{g_i W\}$ contains a $\langle\gamma\rangle$-orbit.*

Proof. The subspace $\bigoplus_i g_i W$ is at least $(r+1)$-dimensional, so it intersects V^γ non-trivially. Suppose $v \neq 0$ lies in the intersection. The non-empty subset of translates in $\{g_i W\}$ such that the projection of v onto $g_i W$ is non-trivial is $\langle\gamma\rangle$-stable, hence it is a union of $\langle\gamma\rangle$-orbits. □

For any $\gamma \in S$ we say a $\langle\gamma\rangle$-orbit in $\{gW\}$ is non-trivial if it has at least two elements. If γ is a pseudoreflection, then every $\langle\gamma\rangle$-orbit is trivial because every G-translate gW is an R-module and $\gamma \in R$. If $\gamma \in S - S_0$ is not a pseudoreflection, then a non-trivial $\langle\gamma\rangle$-orbit would have to contain at least $r+2$ elements, which is impossible by lemma 3.4. Therefore $\langle\gamma\rangle$ acts trivially on $\{gW\}$ for every $\gamma \in S - S_0$.

Lemma 3.5. *Suppose $\dim(W) \leq r$ and $\gamma \in S_0$. If the ith $\langle\gamma\rangle$-orbit in $\{gW\}$ has e_i elements, then $\dim(W) \sum_i (e_i - 1) < r + 1$.*

Proof. This follows immediately by considering any subset of $\{gW\}$ containing at most $e_i - 1$ elements from the ith orbit. In particular, such a subset contains no $\langle\gamma\rangle$-orbit, hence lemma 3.4 implies it has less than $(r+1)/\dim(W)$ elements. □

By applying lemma 3.5 to $\gamma \in S_0$ and the set of non-trivial $\langle\gamma\rangle$-orbits in $\{gW\}$ we conclude that there are less than $(r+1)/\dim(W)$ non-trivial $\langle\gamma\rangle$-orbits and they have less than $2(r+1)/\dim(W)$ elements in total. In particular, the union of all such orbits for all $\gamma \in S_0$ has less than $2(r+1)|S_0|/\dim(W)$ elements. On the other hand, S generates G and G is irreducible, so every conjugate gW lies in a non-trivial orbit for some $\gamma \in S_0$, hence $\dim(V) < 2(r+1)|S_0|$. Therefore $W = V$. □

If the pairing on V is alternating, then lemma 3.2 together with the main theorem of [ZS2] imply that $R = \mathrm{Sp}(V)$; for $\dim(V) = 2$ this is a well-known result of [D]. Therefore we may assume R is generated by reflections and apply the classification of irreducible reflection groups in [ZS1]. There are a handful of exceptional groups, but the key to eliminating them is to find a pair of reflections such that the order of their product is sufficiently large.

Lemma 3.6. *There are conjugate reflections $\rho, \sigma\rho\sigma^{-1} \in R$ such that $[\rho, \sigma] = \rho\sigma\rho\sigma^{-1}$ has order at least ℓ.*

Proof. First, we claim that for every isotropic shear $\sigma \in G$ there is a reflection $\rho \in R$ such that $\rho\sigma \neq \sigma\rho$. For the roots of all reflections in R span V by the irreducibility of R and we claim $\rho\sigma = \sigma\rho$ if and only if $V_\rho \leq V^\sigma$. In particular, at least one root does not lie in V^σ and so the corresponding reflection satisfies $\rho\sigma \neq \sigma\rho$ as claimed. To prove the claim we observe that $V_\rho \leq V^\sigma$ and $V_\sigma \leq V^\rho$ are dual, with respect to the pairing, hence both statements hold or neither does. The first implies that $(\sigma - 1)(\rho - 1) = 0$ in $\mathrm{End}(V)$ and the second that $(\rho - 1)(\sigma - 1) = 0$. If both

hold, then clearly $\sigma\rho = \rho\sigma$. Conversely, if $\rho\sigma = \sigma\rho$, then $\rho\sigma(r) = -\sigma(r)$ for any root $r \in V_\rho$, hence σ stabilizes V_ρ and its restriction acts trivially, so $V_\rho \leq V^\sigma$.

Next, fix any pair ρ, σ which do not commute, a root z of ρ, and $y \in V^\sigma \backslash V^H$. Note, $z \notin V^\sigma$ because $V_\rho \not\leq V^\sigma$, so y, z are independent. Rescaling y if necessary we may assume $\rho y = y + z$. We claim that $x = \sigma z - z$ lies in V^H and hence x, y, z span a three-dimensional H-submodule W. By definition x lies in the isotropic subspace $V_\sigma \leq V^\sigma$, hence $\langle\, x\,,\, x\,\rangle = 0$, and to show that it lies in V^ρ it suffices to show $\langle\, x\,,\, z\,\rangle = 0$. Using the identities $\langle\, x\,,\, x\,\rangle = 0$ and $\langle\, \sigma z\,,\, \sigma z\,\rangle = \langle\, z\,,\, z\,\rangle$ one easily deduces that $\langle\, \sigma z\,,\, z\,\rangle = \langle\, z\,,\, z\,\rangle$, hence $\langle\, x\,,\, z\,\rangle = \langle\, \sigma z\,,\, z\,\rangle - \langle\, z\,,\, z\,\rangle = 0$ as claimed.

Finally, in terms of the ordered basis x, y, z of W we have

$$\rho = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \rho\sigma\rho\sigma^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(W).$$

Thus the restriction u of $[\rho, \sigma]$ to W satisfies $(u-1)^\ell = 0$, hence u has order ℓ and the lemma follows. □

Applying lemma 3.6 to the classification in [ZS1] we find either $[O(V) : R] \leq 2$ or R is imprimitive. In their notation the two families of imprimitive groups we must rule out are $G(m, m, n)$ and $G(2m, m, n)$, where $n = \dim(V)$. The first is the subgroup of $\mathrm{GL}(V)$ generated by the permutation matrices and the diagonal matrix with diagonal $(\zeta, 1/\zeta, \ldots, 1)$, where ζ is a primitive mth root of unity in $\mathbb{F}_\ell^\times$ and $m > 1$. The second is the group generated by $G(2m, 2m, n)$ and the diagonal matrix with diagonal $(-1, 1, \ldots, 1)$. We can eliminate all the imprimitive groups but $G(2, 2, n)$ and $G(2, 1, n)$ using the following lemma.

Lemma 3.7. *If $G(m, m, n) \leq O(V)$, then $m = 2$. If $G(2m, m, n) \leq O(V)$, then $m = 1$.*

Proof. $G(2m, 2m, n)$ is a subgroup of $G(2m, m, n)$, hence the first statement of the lemma implies the second. Let π be any permutation matrix in $O(V)$ relative to some basis $\{x_i\}$ of V. Then $\langle\, \pi x_i\,,\, \pi x_j\,\rangle = \langle\, x_i\,,\, x_j\,\rangle$, hence $\langle\, x_i\,,\, x_j\,\rangle = a\delta_{ij} + b(1 - \delta_{ij})$ for some constants $a, b \in \mathbb{F}_\ell$, where δ_{ij} is the Kronecker delta function. Let $M \in O(V)$ be a diagonal matrix whose diagonal is $(\zeta, 1/\zeta, 1, \ldots, 1)$, where ζ is a primitive mth root of unity. We see that $b = 0$ because $b = \langle\, Mx_1\,,\, Mx_3\,\rangle = \zeta\langle\, x_1\,,\, x_3\,\rangle = \zeta b$ and $\zeta^2 = 1$ because $a = \langle\, Mx_1\,,\, Mx_1\,\rangle = \zeta^2 a$. □

To eliminate the two remaining imprimitive groups we note that the product of any pair of rotations in either of these groups has order at most 4, hence we can eliminate them using lemma 3.6. Therefore the only possibilities for R remaining are the groups of index at most two in $O(V)$ which are not $SO(V)$, which completes the proof of the theorem.

4 Middle Convolution

Let $C = \mathbb{P}^1$, $K = k(x)$, and assume $k = \overline{k}$. Let $\mathcal{F} \to C$ be a tame quasi-finite étale sheaf with coefficients in $\mathbb{F}_\ell$. We say $\mathcal{F}$ is Néron if there is a dense open set $j : U \to C$ so that the restriction $\mathcal{F} \to U$ is lisse and the adjunction map $j_* j^* \mathcal{F} \to \mathcal{F}$ is an isomorphism. Let $\mathcal{M}$ denote the collection of irreducible Néron $\mathcal{F} \to C$ such that the generic rank of $\mathcal{F}$ is at least two or the restriction

$\mathcal{F} \to C - \{\infty\}$ has at least two ramified fibers. If $U \subset C - \{0, \infty\}$ is dense open, then let $\mathcal{M}_U$ denote the subset of $\mathcal{F} \in \mathcal{M}$ such that the restriction $\mathcal{F} \to U$ is lisse and let $\mathrm{rk}(\mathcal{F})$ denote the rank of $\mathcal{F} \to U$. Moreover, if $t \in C - U$, then let $\mathcal{F}(t)$ denote the representation of $I(t) \leq \pi_1^t(U)$ corresponding to $\mathcal{F} \to U$. We fix an ordering of $C - U$ and topological generators $\sigma_t \in I(t)$ for $t \in C - U$ so that the ordered product is the identity in $\pi_1^t(U)$.

If $\lambda \in \mathbb{F}_\ell^\times$ has order invertible in k and $t \in C - U$, then we write $\lambda : I(t) \to \mathbb{F}_\ell^\times$ for the representation $\sigma_t \mapsto \lambda$. Let $\mathcal{L}_\lambda = \mathcal{L}_{\chi(x)} \to C$ denote the Kummer sheaf whose restriction to $C - \{0, \infty\}$ is lisse and invertible and for which $\mathcal{L}_\lambda(0) = \lambda$; note, $\mathcal{L}_\lambda$ is tame and Néron but does not lie in $\mathcal{M}$. If $t \in C - \{\infty\}$ is a closed point and $\tau_t : C \to C$ is the involution $x \mapsto t - x$, then $\tau_t^* \mathcal{L}_\lambda$ is lisse over $C - \{t, \infty\}$. Moreover, if $\mathcal{F} \in \mathcal{M}_U$ and i denotes the open immersion $U - \{t\} \to C$, then the sheaf $i_* i^*(\mathcal{F} \otimes \tau_t^* \mathcal{L}_\lambda)$, the twist of $\mathcal{F}$ by $\tau_t^* \mathcal{L}_\lambda$, also lies in $\mathcal{M}$. In particular, the étale cohomology group $V_t = H^1(C, i_* i^*(\mathcal{F} \otimes \tau_t^* \mathcal{L}_\lambda))$ is the only non-vanishing group and its dimension is constant as $t \in U$ varies over the closed points.

The *middle convolution* of $\mathcal{F} \in \mathcal{M}_U$ by $\mathcal{L}_\lambda$, which we denote $\mathrm{MC}_\lambda(\mathcal{F})$, is the sheaf in $\mathcal{M}_U$ whose fiber over t is V_t. Katz defined it when the characteristic of k is positive (cf. [Ka2]), and one can use [DR] to extend the definition to characteristic zero (where everything is tame).

Lemma 4.1. *The 'functors'* $\mathrm{MC}_\lambda : \mathcal{M}_U \to \mathcal{M}_U$ *satisfy:*

1. $\mathrm{MC}_1(\mathcal{F}) \simeq \mathcal{F}$;
2. $\mathrm{MC}_{\lambda_1}(\mathrm{MC}_{\lambda_2}(\mathcal{F})) \simeq \mathrm{MC}_{\lambda_1 \lambda_2}(\mathcal{F})$;
3. $\mathrm{rk}(\mathrm{MC}_\lambda(\mathcal{F})) = \sum_{t \in \mathbb{A}^1 - U} \mathrm{codim}\left(\mathcal{F}(t)^{I(t)}\right) - \dim\left((\mathcal{F}(\infty) \otimes \lambda)^{I(\infty)}\right)$;
4. $\mathrm{MC}_\lambda(\mathcal{F})(t)/\mathrm{MC}_\lambda(\mathcal{F})(t)^{I(t)} \simeq \left(\mathcal{F}(t)/\mathcal{F}(t)^{I(t)}\right) \otimes \lambda$ *for* $t \in \mathbb{A}^1 - U$.

Proof. The first two statements show that MC_λ is 'multiplicative' in λ. See proposition 2.9.7 of [Ka2] or proposition 3.2 and theorem 3.5 of [DR]. Statements 3 and 4 follow from corollary 3.3.6 of [Ka2] or from lemma 2.7 and lemma 4.1 respectively of [DR]. □

If $t \in \mathbb{A}^1 - U$ and $F = \mathcal{F}(t)$, then the Jordan decomposition of F together with the above properties completely determines the decomposition of $M = \mathrm{MC}_\lambda(\mathcal{F})(t)$. Let U_n denote an irreducible unipotent Jordan block of size n. The number of unipotent (or trivial) blocks of the form U_1 in either F, M is the dimension of the respective space of $I(t)$-invariants, and there is a bijection between the non-trivial blocks of F and those of M:

$$U_n \mapsto U_{n-1} \otimes \lambda, \quad U_n \otimes 1/\lambda \mapsto U_{n+1}, \quad B \notin \{U_n, U_n \otimes 1/\lambda\} \mapsto B \otimes \lambda \notin \{U_n \otimes \lambda, U_n\}. \tag{4.1}$$

The dimension changes in the first two cases are due to the isomorphism $U_m \simeq U_{m+1}/U_{m+1}^{I(t)}$ applied to unipotent blocks of F, M respectively.

For example, let $g \geq 1$, $f(x) \in k[x]$ be square-free of degree $2g$, and $\mathcal{F} \in \mathcal{M}$ be the quadratic Kummer sheaf $\mathcal{L}_{\chi(f(x))}$. If we write $U = \mathbb{A}^1 - \deg_0(f)$, then $\mathcal{F} \in \mathcal{M}_U$ and the Tate twist $\mathrm{MC}_{-1}(\mathcal{F})(1)$ is the Néron sheaf $\mathcal{J}_\ell \to C$ of the previous section. More precisely, if $t \in U$ is a closed point, then the fiber of $\mathrm{MC}_{-1}(\mathcal{F})(-1)$ over t is $H^1(C, \mathcal{L}_{\chi(f(x)(t-x))}(1))$, and the latter is easily seen to be cohomology group $H^1(X_t, (\mathbb{Z}/\ell)(1))$ of the hyperelliptic curve X_t/k. For each $t \in \mathbb{A}^1 - U$, the quotient $\mathcal{F}(t)/\mathcal{F}(t)^{I(t)}$ is the scalar representation -1, so $\mathrm{MC}_{-1}(\mathcal{F})(t)/\mathrm{MC}_{-1}(\mathcal{F})(t)^{I(t)}$ is the

trivial representation $\mathbb{Z}/\ell$. Thus, $\mathrm{MC}_{-1}(\mathcal{F})(t)$ has one Jordan block of the form U_2 and the rest are all trivial, hence the monodromy is a transvection. From formula 3 of lemma 4.1 we see that $\mathrm{rk}(\mathrm{MC}_{-1}(\mathcal{F})) = 2g$; note, $I(\infty)$ acts trivially on $\mathcal{F}(\infty)$.

5 A Theorem of Yu

Let q be an odd prime power, $C = \mathbb{P}^1$ over $\mathbb{F}_q$ and K be the global field $\mathbb{F}_q(C) = \mathbb{F}_q(t)$. Fix $g \geq 1$ and a monic square-free $f(x) \in \mathbb{F}_q[x]$ of degree $2g$.

Let X/K be the hyperelliptic curve which is the natural (one-point) compactification of the affine curve $y^2 = (t-x)f(x)$. The Jacobian J/K of X is a g-dimensional abelian variety and for any rational prime ℓ not dividing q we write $J[\ell]$ for the subgroup of ℓ-torsion. The main goal of this section is to prove the following theorem due to Jiu-Kang Yu [Yu].

Theorem 5.1. *If ℓ is odd, then the group $G_\ell = \mathrm{Gal}(K(J[\ell])/K)$ is as big as possible. More precisely, there is a primitive ℓth root of unity $\zeta_\ell \in K(J[\ell])$ and $K(J[\ell])/K(\zeta_\ell)$ is a geometric extension with Galois group $\Gamma_\ell = \mathrm{Sp}(2g, \mathbb{F}_\ell)$.*

Remark: For $g = 1$ the theorem is equivalent to Igusa's theorem [I] for the so-called Legendre curve.

Our proof, which will occupy the remainder of this section, differs from the proof in [Yu] and has the advantage that the techniques used allow one to prove more general results.

By the existence of the Weil pairing we know that $\mu_\ell \subset K(J[\ell])$, so to prove the theorem we may make the finite scalar extension where we replace K by $K(\mu_\ell)$. If we fix an isomorphism $\mu_\ell \simeq \mathbb{F}_\ell$, then the group law together with the Weil pairing gives $J[\ell]$ the structure of a $2g$-dimensional $\mathbb{F}_\ell$-vector space together with a non-degenerate alternating pairing. Therefore if we choose a basis of $J[\ell]$, then we may identify G_ℓ with a subgroup of Γ_ℓ and we must show that $G_\ell = \Gamma_\ell$.

Let $\mathcal{X} \to C$ denote the minimal regular model of X/K and $\mathcal{J} \to C$ the Néron model of J/K. The fibers of $\mathcal{X} \to C$ are proper smooth curves of genus g over the open complement $j : U \to C$ of the finite subset $Z = \{\tau \in \overline{\mathbb{F}}_q : f(\tau) = 0\} \cup \{\infty\}$, and each fiber of $\mathcal{X} \to Z - \{\infty\}$ is smooth away from an ordinary double point (i.e. Lefschetz). In particular, the restriction of $\mathcal{J} \to C$ to $\mathbb{A}^1 = C - \{\infty\}$ has semistable reduction. Over ∞ the fibers of $\mathcal{X}, \mathcal{J}$ are more difficult to describe, but we will show they are sufficiently 'tame' and that we can ignore them.

Multiplication by ℓ on J extends to an isogeny of C-group schemes $\times\ell : \mathcal{J} \to \mathcal{J}$ and we define $\mathcal{J}_\ell \subset \mathcal{J}$ to be the kernel. The latter is a quasi-finite étale group scheme over C and the restriction $\mathcal{J}_\ell \to U$ is finite étale. If we write $\pi : \mathcal{X} \to U$ for the restriction of $\mathcal{X} \to C$, then (the sheaf of sections of) $\mathcal{J}_\ell \to C$ is isomorphic to the direct image sheaf $j_*\mathcal{R}^1\pi_*\mu_\ell$. More precisely, the fiber of $\mathcal{R}^1\pi_*\mu_\ell \to U$ over a geometric point $\overline{\tau} \in U$ is the étale cohomology group $H^1(C_{\overline{\tau}}, \mu_\ell) = \mathcal{J}_\ell(\mathbb{F}_q(\overline{\tau}))$ and the adjunction map $j_*\mathcal{R}^1\pi_*\mu_\ell \simeq j_*j^*\mathcal{J}_\ell \to \mathcal{J}_\ell$ is an isomorphism.

We fix a geometric generic point $\overline{\tau} \in U$ (i.e. an algebraic closure $\overline{K}/K$) and let $\pi_1(U) = \pi_1(U, \overline{\tau})$ denote the étale fundamental group. The lisse sheaf $\mathcal{J}_\ell \to U$ corresponds to a $\mathbb{F}_\ell$-representation of $\pi_1(U)$ on the fiber $(\mathcal{J}_\ell)_{\overline{\tau}} = J[\ell]$ (which is defined up to inner automorphism). More precisely, if we write $G_K = \mathrm{Gal}(\overline{K}/K)$, then the quotient $G_K \to G_\ell$ factors through $G_K \to \pi_1(U)$. In fact, the following lemma implies $\pi_1(U) \to G_\ell$ factors through the maximal tame quotient $\pi_1(U) \to \pi_1^{\mathrm{t}}(U)$.

Lemma 5.2. *$\mathcal{J}_\ell \to C$ is tamely ramified.*

Proof. The extension $K(J[2])/K$ is a scalar extension hence unramified and by Kummer theory $K(J[4])/K(J[2])$ is tamely ramified, hence $K(J[4])/K$ is tamely ramified. Raynaud's criterion for semi-stable reduction implies J has semi-stable reduction over $L = K(J[4])$ (cf. 4.7 of [G2]), hence $L(J[\ell])/L$ is tamely ramified and thus so is $K(J[\ell])/K$. □

We fix an algebraic closure $\mathbb{F}_q \to \overline{\mathbb{F}}_q$ and let $\pi_1^{\mathrm{t}}(U \times \overline{k}) \leq \pi_1^{\mathrm{t}}(U)$ denote the geometric subgroup. If we order the points in $Z \times \overline{k}$, then for each $c \in Z \times \overline{k}$ we may choose a topological generator σ_c of the inertia group $I(c) \leq \pi_1^{\mathrm{t}}(U \times \overline{k})$ so that the ordered product is the identity (cf. [G1] or [SGA1]). Moreover, $\pi_1^{\mathrm{t}}(U \times \overline{k})$ is topologically generated by σ_c for $c \in Z \times \overline{k} - \{\infty\}$, hence to prove the theorem it suffices to show that the images of these elements generate Γ_ℓ which we will do using theorem 3.1. We note that it follows $K(J[\ell])/K$ is geometric (i.e. $\overline{k} \cap K(J[\ell]) = k$) because the image of $\pi_1^{\mathrm{t}}(U)$ in Γ_ℓ lies between the image of $\pi_1^{\mathrm{t}}(U \times \overline{k})$ and Γ_ℓ, hence is Γ_ℓ.

The Picard-Lefschetz formulas imply that σ_c acts as a (symplectic) transvection on $J[\ell]$ for every $c \in Z \times \overline{k} - \{\infty\}$ (cf. theorem III.4.3 of [FK]). One can also use Katz's theory of middle convolution [Ka2] for $\mathbb{F}_\ell$-sheaves to deduce the same thing as well as to give another proof of lemma 5.2. More importantly, one can also show that $\mathcal{J}_\ell \to C$ is irreducible (i.e. $\pi_1^{\mathrm{t}}(U \times \overline{k})$ acts irreducibly on $J[\ell]$). The key is to identify $\mathcal{J}_\ell \to C$ with the middle convolution $\mathrm{MC}_{-1}(\mathcal{L}_{\chi(f(x))})$ which is irreducible (see section 4 for notation and details).

To complete the proof of theorem 5.1 we let $\Gamma = \Gamma_\ell$, $G = G_\ell$, $r = 1$, $S = \{\sigma_c : c \in Z \times \overline{k} - \{\infty\}\}$, and $S_0 = \emptyset$ and apply theorem 3.1. Note the image of σ_c in G_ℓ has prime order $\ell > 2$ for every $c \in Z \times \overline{k} - \{\infty\}$.

6 Quadratic Twists of Elliptic Curves

Let q be an prime power not divisible by 2,3 and fix an algebraic closure $\mathbb{F}_q \to \overline{\mathbb{F}}_q$, although we remark that most of the results in this section apply if we replace $\mathbb{F}_q$ by an arbitrary field of characteristic distinct from 2,3. We fix a proper smooth geometrically connected curve $C/\mathbb{F}_q$ and write $K = \mathbb{F}_q(C)$ for its function field.

6.1 Geometry of a Twisted Curve

We fix an elliptic curve E_1/K with non-constant j-invariant and write $\mathcal{E}_1 \to C$ for its Néron model. For every non-trivial coset $fK^{\times 2} \subset K^\times$ we write E_f/K for the so-called quadratic twist of E_1/K by f. It is the unique elliptic curve over K which is not K-isomorphic to E_1 but is $K(\sqrt{f})$-isomorphic. The Néron model $\mathcal{E}_f \to C$ of E_f/K is a smooth group scheme and the group of sections $\mathcal{E}_f(C)$ is canonically isomorphic to the Mordell-Weil group $E_f(K)$.

Let ℓ be a prime which is invertible in K. The multiplication by ℓ map on $E_f(K)$ extends to an isogeny $\times\ell : \mathcal{E}_f \to \mathcal{E}_f$ and we define $\mathcal{E}_{f,\ell} \subset \mathcal{E}_f$ to be the kernel. It is a quasi-finite étale group scheme over C which we call the Néron model of the ℓ-torsion $E_f[\ell]$. We note that if $j : U \to C$ is the inclusion of a non-empty open set, then $\mathcal{E}_{f,\ell}$ is canonically isomorphic to $j_* j^* \mathcal{E}_{f,\ell}$, hence is a

so-called middle extension. The fiber of $\mathcal{E}_{f,\ell}$ over a geometric generic point of C is $E_f[\ell]$ and over an arbitrary geometric point of C it is a subspace of $E_f[\ell]$.

Lemma 6.1. *Let v be a geometric point of C. If ℓ does not divide the order of the component group of the special fiber of $\mathcal{E}_f$ over v, then*

$$\dim(\mathcal{E}_{f,\ell}(v)) = \begin{cases} 2 & \text{if } \mathcal{E}_f \text{ has good reduction over } v \\ 1 & \text{if } \mathcal{E}_f \text{ has multiplicative reduction over } v \\ 0 & \text{if } \mathcal{E}_f \text{ has additive reduction over } v \end{cases}.$$

Proof. The assumption on the order of the component group over v ensures that all ℓ-torsion lies in the identity component of the special fiber. The lemma follows easily by observing that identity component is cyclic in the case of multiplicative reduction and ℓ-torsion free in the case of additive reduction (cf. proposition 5.1 of [Si]). □

For ℓ satisfying the hypothesis of the lemma we regard $\mathcal{E}_{f,\ell}$ as the $\mathbb{F}_\ell$-analogue of Kodaira's homological invariant (cf. section 7 of [Kod] and section 2 of [Shi]). In order to obtain a similar result for general ℓ one must restrict to the intersection of $\mathcal{E}_{f,\ell}$ with the identity component of $\mathcal{E}_f$. However, for ease of exposition we will assume $\ell \neq 2, 3$ and ℓ does not divide $\max\{1, -\mathrm{ord}_v(j(E_f))\}$ for every closed point $v \in C$, where $j(E_f) = j(E_1)$ is the j-invariant, so that $\mathcal{E}_{f,\ell}$ is 'connected'. We note that the set of exceptional ℓ is independent of f.

We say that $\mathcal{E}_{f,\ell}$ has big monodromy if the Galois group of $K(E_f[\ell])/K$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. For $\ell \geq 5$ we note that there are no index-two subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$, hence $K(E_f[\ell])$ and $K(\sqrt{f})$ are (geometrically) disjoint extensions, so $\mathcal{E}_{f,\ell}$ has big monodromy if and only if $\mathcal{E}_{1,\ell}$ does. In particular, after we expand the set of exceptional ℓ to include those such that $\mathcal{E}_{f,\ell}$ does *not* have big monodromy we obtain a finite set which is still independent of f, and we assume Λ is a subset of the complement.

Remark: If we write $g(C)$ for the genus of C, then theorem 1.1 of [CH] asserts $\mathcal{E}_{f,\ell}$ has big monodromy if $\ell \gg_{g(C)} 0$, hence the set of exceptional ℓ may even be taken to depend only on $g(C)$ and the primes dividing the coefficients of the divisor of poles of $j(E_1)$.

We write $M_f, A_f \subset C$ for the divisors of multiplicative and additive reduction respectively of $\mathcal{E}_{f,\ell} \to C$ and let $U_f = C - M_f - A_f$. By assumption $\mathcal{E}_{f,\ell}$ has big monodromy, and in particular, the restriction of $\mathcal{E}_{f,\ell}$ to U_f is an irreducible lisse $\mathbb{F}_\ell$-sheaf of rank two.

Lemma 6.2. *The étale cohomology groups of $\mathcal{E}_{f,\ell}$ over $C \times \overline{\mathbb{F}}_q$ are $\mathbb{F}_\ell$-vector spaces satisfying*

$$\dim(H^i(C \times \overline{\mathbb{F}}_q, \mathcal{E}_{f,\ell})) = \begin{cases} \deg(M_f) + 2 \cdot \deg(A_f) + 4 \cdot (\mathrm{genus}(C) - 1) & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Proof. The cohomology groups for $i \neq 0, 1, 2$ are trivial by the cohomological dimension of C. The groups are also trivial for $i = 0, 2$ because $\mathcal{E}_{f,\ell}$ is irreducible of rank two: these groups are the $\pi_1(U_f \times \overline{\mathbb{F}}_q)$-invariants and $\pi_1(U_f \times \overline{\mathbb{F}}_q)$-coinvariants respectively of $E_f[\ell]$ (because $\mathcal{E}_{f,\ell}$ is a middle extension and is irreducible of rank greater than one). Finally, the dimension for $i = 1$ follows from the (Néron–)Ogg–Shafarevich formula (see [O] or [Sha2]); note, $\mathcal{E}_{f,\ell}$ is tamely ramified because 6 is invertible in K. □

Let $V_{f,\ell}$ be the étale cohomology group $H^1(C \times \overline{\mathbb{F}}_q, \mathcal{E}_{f,\ell})$.

Frob_q acts on $V_{f,\ell}$ by functoriality, hence we may regard Frob_q as a conjugacy class of elements in $\mathrm{GL}(V_{f,\ell})$. On the other hand, if $L(T, E_f/K)$ is the L-function of E_f/K, which we note lies in $\mathbb{Z}[T]$ and has leading coefficient which is non-zero modulo ℓ, then

$$\det(1 - qT\mathrm{Frob}_q | H^1(C \times \overline{\mathbb{F}}_q, \mathcal{E}_{f,\ell})) \equiv L(T, E_f/K) \pmod{\ell}.$$

In particular, we obtain an upper bound on the order of vanishing of $L(T, E_f/K)$ at $T = 1/q$, the so-called analytic rank of E_f/K, by studying the order of vanishing modulo ℓ. In [H] we studied the reduction when $\mathcal{E}_{f,\ell}$ has 'small' monodromy instead.

The usual Weil pairing on $E_f[\ell] \times E_f[\ell]$ extends to a non-degenerate alternating pairing $\mathcal{E}_{f,\ell} \times \mathcal{E}_{f,\ell} \to \mathbb{F}_\ell(1)$, hence $\mathcal{E}_{f,\ell} \to C$ is self-dual. Together with Poincaré duality we obtain a non-degenerate *symmetric* pairing of cohomology groups

$$H^1(C \times \overline{\mathbb{F}}_q, \mathcal{E}_{f,\ell}) \times H^1(C \times \overline{\mathbb{F}}_q, \mathcal{E}_{f,\ell}) \longrightarrow H^2(C \times \overline{\mathbb{F}}_q, \mathbb{F}_\ell(1)).$$

That is, we have a non-degenerate orthogonal pairing of $\mathbb{F}_\ell$-vector spaces $V_{f,\ell} \times V_{f,\ell} \to \mathbb{F}_\ell$. We write $O(V_{f,\ell})$ for the subgroup of $\mathrm{GL}(V_{f,\ell})$ preserving the pairing and note that Frob_q preserves the pairing on $V_{f,\ell}$, so belongs to a well-defined conjugacy class in $O(V_{f,\ell})$.

6.2 Families of Twists

For ease of exposition we assume $C = \mathbb{P}^1$ and $K = \mathbb{F}_q(t)$. For general C one will have to increase the minimum value of ℓ required for a surjectivity statement of the form of theorem 6.3.

We fix an elliptic curve E_1/K such that $\mathcal{E}_1 \to C$ has at least one fiber of multiplicative reduction away from ∞. We also fix a non-zero polynomial $m \in \mathbb{F}_q[t]$ which vanishes at one or more finite points in M_1 in order that for every $f \in \mathbb{F}_q[t]$ which is relatively prime to m, the twist $\mathcal{E}_f \to C$ also has at least one fiber of multiplicative reduction away from ∞.

For every integer positive integer d we define the family of twisting polynomials

$$F_d = \left\{ f \in \overline{\mathbb{F}}_q[t] : f \text{ is square-free}, \deg(f) = d, \gcd(f, m) = 1 \right\}.$$

We may regard F_d as a $(d+1)$-dimensional affine space and we write $F_d(\mathbb{F}_{q^n})$ for the set of $\mathbb{F}_{q^n}$-valued points, i.e. the subset of f with coefficients in $\mathbb{F}_{q^n}$. Unless we restrict the leading coefficient of f, there will be many $g \in F_d$ which give rise to an isomorphic twist. However, for every $n \geq 1$, the number of twists $\mathcal{E}_g$ by $g \in F_d(\mathbb{F}_{q^n})$ isomorphic to $\mathcal{E}_f$ is independent of $f \in F_d(\mathbb{F}_{q^n})$.

Katz first suggested restricting to twists parametrized by a fixed F_d in part because the set of twists by $f \in F_d(\mathbb{F}_{q^n})$ satisfy a remarkable uniformity property: the degree of the L-function $L(T, E_f/K_n)$ is independent of f and n. In fact, this is a consequence of a deeper sheaf-theoretic statement: for every non-exceptional ℓ, there is a unique étale $\mathbb{F}_\ell$-lisse sheaf $\mathcal{T}_{d,\ell} \to F_d$ whose (geometric) fiber over any $f \in F_d(\mathbb{F}_{q^n})$ is the $\mathbb{F}_\ell$-vector space $H^1(C \times \overline{\mathbb{F}}_{q^n}, \mathcal{E}_{f,\ell})$.

We fix a geometric point $f \in F_d$ and let $\pi_1(F_d) = \pi_1(F_d, f)$ denote the étale fundamental group. Then $\mathcal{T}_{d,\ell}$ corresponds to a $\mathbb{F}_\ell$-representation $\rho : \pi_1(F_d) \to \mathrm{GL}(V_{f,\ell})$ and the image is well defined up to inner automorphism. We define the arithmetic monodromy group to be the image of $\pi_1(F_d)$

and the geometric monodromy group to be the image of $\pi_1(F_d \times \overline{\mathbb{F}}_q)$. If we take $\mathcal{T}_{d,\ell}$ together with its orthogonal pairing, then the results at the end of the previous section imply that both monodromy groups lie in $O(V_{f,\ell})$.

The main question of interest for us is to determine as precisely as possible the monodromy groups as d and ℓ vary. While we do not answer this question completely, the following theorem demonstrates that the monodromy is usually 'big' in a strongly uniform way.

Theorem 6.3. *If $\ell \geq 5$ and $\deg(f) \gg_E 0$, then the geometric monodromy group has index at most two in $O(V_{f,\ell})$ and is not $SO(V_{f,\ell})$. That is, G is one of the following:*

1. *the full orthogonal group $O(V_{f,\ell})$;*
2. *the kernel of the spinor norm;*
3. *the kernel of the product of the spinor norm and the determinant.*

In order to prove the theorem it suffices to restrict to one-parameter families parametrized by an affine curve $U \subset F_d$ and to show that the image of $\pi_1(U \times \overline{\mathbb{F}}_q)$ is already big. More precisely, fix any $g \in F_{d-1}$ and consider the one-parameter family of polynomials $(c-t) \cdot g(t)$. We let $U_g \subset \mathbb{P}^1$ be the open subset of $c \in \mathbb{A}^1$ such that $(c-t) \cdot g(t) \in F_d$. Then theorem 6.3 follows immediately from the following theorem whose proof we postpone until the next section.

Theorem 6.4. *If $\ell \geq 5$ and $\deg(g) \gg_E 0$, then the image of $\pi_1(U_g \times \overline{\mathbb{F}}_q)$ has index at most two in $O(V_{f,\ell})$ and is not $SO(V_{f,\ell})$.*

6.3 Katz One-Parameter Families of Twists

We fix $g \in F_{d-1}$ and let $U_g \subset F_d$ be as before. The key observation Katz makes to prove analogous ℓ-adic monodromy theorems is that the restriction of $\mathcal{T}_{d,\ell}$ to U_g is the middle convolution sheaf $\mathrm{MC}_{-1}(\mathcal{E}_g) \to C$ (cf. section 4). In particular, $\mathcal{T}_{d,\ell}$ is irreducible and tame and we can describe its monodromy around the points of $\mathbb{P}^1 - U_g$. We refer the reader to section 3 for the definition of a reflection and isotropic shear.

Lemma 6.5. *For every geometric point $c \in \mathbb{A}^1 - U_g$ fix a topological generator σ_c of the inertia group $I(c) \leq \pi_1^{\mathrm{t}}(U_g \times \overline{\mathbb{F}}_q)$ and let $V = V_{f,\ell}$.*

1. *If $\mathcal{E}_g \to C$ has good reduction over $t = c$, then σ_c acts trivially on V.*
2. *If $\mathcal{E}_g \to C$ has multiplicative reduction over $t = c$, then σ_c acts as a reflection on V.*
3. *If $\mathcal{E}_g \to C$ has additive reduction of Kodaira type I_0^* over $t = c$, then σ_c acts as an isotropic shear on V.*

For all other $c \in \mathbb{A}^1 - U_g$, σ_c acts as a non-scalar on the two-dimensional quotient $V/V^{\sigma_c=1}$.

Proof. We follow the notation of section 4. The fiber of the convolution $\mathrm{MC}_{-1}(\mathcal{E}_g)$ over a (geometric) closed point $c \in U_g$ is $H^1(C, i_* i^*(\mathcal{E}_g \otimes \tau_c^* \mathcal{L}_{-1}))$, where $i : U_g \to C$. One can easily show that

$i_*i^*(\mathcal{E}_g \otimes \tau_c^*\mathcal{L}_{-1})$ is the fiber of $\mathcal{E}_f$ over c, hence the restrictions $\mathcal{T}_{d,\ell} \to U_g$ and $\mathrm{MC}_{-1}(\mathcal{E}_g) \to U_g$ are isomorphic, so $\mathcal{T}_{d,\ell} \simeq \mathrm{MC}_{-1}(\mathcal{E}_g)$.

If $\mathcal{E}_g \to C$ has multiplicative reduction over $t = c$, then $\mathcal{E}_g(c)/\mathcal{E}_g(c)^{I(c)}$ is the trivial representation $\mathbb{F}_\ell$, so $\mathcal{T}_{d,\ell}(c)/\mathcal{T}_{d,\ell}(c)^{I(c)}$ is the scalar representation -1 and the monodromy is a reflection. If $\mathcal{E}_g \to C$ has additive reduction of Kodaira type I_0^* over $t = c$, then $\mathcal{E}_g(c)/\mathcal{E}_g(c)^{I(c)}$ is the two-dimensional representation $(\mathbb{F}_\ell \oplus \mathbb{F}_\ell) \otimes -1$, so $\mathcal{T}_{d,\ell}(c)/\mathcal{T}_{d,\ell}(c)^{I(c)}$ is $\mathbb{F}_\ell \oplus \mathbb{F}_\ell$. Thus $\mathcal{T}_{d,\ell}$ has two unipotent blocks of the form U_2 and all other blocks are trivial (cf. (4.1)). Finally, for all other types of (additive) reduction we see that $\mathcal{E}_g(c)/\mathcal{E}_g(c)^{I(c)}$ is two-dimensional and σ_c acts as a non-scalar, so the same is true for $\mathcal{T}_{d,\ell}(c)/\mathcal{T}_{d,\ell}(c)^{I(c)}$. □

The elements $S = \{\sigma_c : c \in \mathbb{A}^1 - U_g\}$ topologically generate $\pi_1^{\mathrm{t}}(U_g \times \overline{\mathbb{F}}_q)$, hence they generate the image G of $\pi_1^{\mathrm{t}}(U_g \times \overline{\mathbb{F}}_q)$ in $O(V)$. One implication is that we can ignore the monodromy around ∞ (which is more difficult to describe). More importantly, the codimension of $V^{\sigma=1}$ in V is at most 2 for every $\sigma \in S$, and this places severe restrictions on the monodromy when $|S| \gg 0$. In particular, as $\deg(g)$, hence $|S|$, tends to infinity, the complement of the subset of isotropic shears in S has bounded order. Therefore theorem 6.4 is a consequence of theorem 3.1, applied with $r = 2$ and S_0 the complement of the reflections and the elements with order prime to $(r+1)! = 6$.

6.4 Near Independence

In this section we assume k is finite or separably closed. Fix $g \in F_{d-1}(k)$ and let $\mathcal{T}_{d,\ell} \to U_g$ be as before. Let L denote the function field $k(U_g)$ and let L_ℓ denote the splitting field $L(V_{f,\ell})$. As the following theorem shows, up to replacing L by a finite extension, these extensions are nearly independent (cf. 10.1? of [S4]).

Theorem 6.6. *If $d \gg_E 0$, then there is a finite extension M/L so $L_{\ell_1} \cap L_{\ell_2} \leq M$ for $\ell_1 > \ell_2 \gg_E 0$.*

Proof. By the results in the previous section, if $d \gg_E 0$ and $\ell \gg_E 0$, then $G_\ell = \mathrm{Gal}(L_\ell/L)$ is a big subgroup of an orthogonal group Γ_ℓ and $Q_\ell = G_\ell/\mathcal{D}G_\ell$ is a subgroup of $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. Moreover, if $\ell_i \geq 5$ and $d \gg_E 0$ (so $\dim(V_{f,\ell_i}) \geq 5$ as well), then the quotients $\mathcal{D}G_{\ell_i}/Z(\mathcal{D}G_{\ell_i})$ are non-abelian, simple, and pairwise non-isomorphic for $i = 1, 2$ (cf. theorem 5.27 of [Ar]). Therefore Ribet's lemma (5.2.2 of [R]) implies $L_{\ell_1} \cap L_{\ell_2}$ is contained in the fixed fields of Q_{ℓ_1}, Q_{ℓ_2}. On the other hand, the fixed field of Q_ℓ corresponds to an unramified cover $V_{g,\ell} \to U_g$ of bounded degree. In particular, there are only finitely many covers which occur as we vary ℓ because of our assumptions on k, so we make take M to be the compositum of all the corresponding extensions. □

6.5 Example: Twists of the Legendre Curve

Let $K = k(\lambda)$ and let E/K be the elliptic curve with affine model $y^2 = x(x-1)(x-\lambda)$. We write F_d for the square-free polynomials in $\overline{k}[\lambda]$ of degree d which are relatively prime to $\lambda(\lambda-1)$ and $F_d(k)$ for the subset in $k[\lambda]$. For each $f \in F_d(k)$ we write M_f, A_f for the divisors of multiplicative, additive reduction of the Néron model $\mathcal{E}_f \to C$ and $\mathrm{div}_0(f)$ for the divisor of zeros of f.

Lemma 6.7. *Suppose $f \in F_d(k)$. Then*

$$M_f, A_f, \dim(V_{f,\ell}) \;=\; \begin{cases} \{0,1\}, & \mathrm{div}_0(f) \cup \{\infty\}, & 2d & \text{if } d \text{ is even} \\ \{0,1,\infty\}, & \mathrm{div}_0(f), & 2d-1 & \text{if } d \text{ is odd} \end{cases}.$$

Moreover, the support of the fibers of $\mathcal{E}_f \to C$ of Kodaira type I_0^* is $\mathrm{div}_0(f)$.

Proof. Everything except the dimension assertions are proved in lemma 7 of [H], while $\dim(V_{f,\ell})$ is given in lemma 6.2. □

By theorem 5.1 the sheaves $\mathcal{E}_{f,\ell} \to C$ have big monodromy for all $f \in F_d(k)$ and all odd ℓ, so for $g \in F_{d-1}(k)$, ℓ odd, and $U_g = C - M_g - A_g$, the restriction $\mathcal{T}_{d,\ell} \to U_g$ is irreducible and lisse. The monodromy about a geometric point in $M_g - \{\infty\}$ is a reflection and the monodromy about a geometric point in $A_g - \{\infty\}$ is an isotropic shear by lemma 6.5, so $S_0 = \emptyset$ (if $\ell > 3$) and theorem 6.3 holds for $d \geq 2$ and $\ell \geq 5$. This in turn implies that proposition 5.2 of [Kow1] is valid unconditionally.

One can derive similar results if we replace E/K by the twist E_λ/K. In particular, we can construct $V_{f,\ell}$ satisfying $\dim(V_{f,\ell}) = 2d+1 \equiv 3 \pmod 4$ for d odd. In order to construct examples with $\dim(V_{f,\ell}) \equiv 2 \pmod 4$ one should replace the Legendre curve by one of the curves denoted $X_{211}, X_{321}, X_{431}$ in [MP]. In particular, up to an automorphism of the base $C = \mathbb{P}^1$, we can assume $M_1 = \{0,1\}$ and $A_1 = \{\infty\}$ as before, but now the key difference is that $\infty \in A_f$ for every twist.

Remark: Together these examples increase the set of big subgroups of orthogonal groups which are known to occur as Galois groups over $\mathbb{Q}(t)$. It is difficult to say precisely which group occurs, but despite the ambiguity these extend previous results (cf. survey in [MM]).

6.6 Generalizing to Abelian Varieties

While the previous sections deal exclusively with twists of elliptic curves, both for ease of exposition and application, most of the results can be easily adapted to deal with twists of 'many' abelian varieties A_1/K of dimension g with trivial K/k-trace. The easiest is to assume that the Galois group G_ℓ of $K(A_1[\ell])/K$ is big for $\ell \gg_{A_1} 0$, but it suffices to assume it acts irreducibly on $A_1[\ell]$ for $\ell \gg_{A_1} 0$. Either way we must also assume that G_ℓ acts tamely on $A_1[\ell]$; this is automatic if the characteristic of K is sufficiently large with respect to the genus of C. We must also assume that A_1/K has at potentially semi-stable reduction with toric part of dimension one over some closed point $x \in C$. For example, we may take A_1/K to be any J/K from section 5.

Over almost all the closed points in C an arbitrary quadratic twist of A_1/K has either good reduction or totally additive reduction. In the latter case [LO] implies the component group of the fiber over x of the Néron model is uniformly bounded by a constant which depends only on the dimension of A_1. For each of the remaining closed points the component group of the special fiber belongs to a set of at most two finite groups. Therefore as we vary over the quadratic twists A_f/K of A_1/K, the set of primes dividing the order of the component group of the Néron model $\mathcal{A}_f \to C$ is finite. In particular, if Λ is sufficiently small, then for every $\ell \in \Lambda$, we may assume G_ℓ acts irreducibly on $A_1[\ell]$ and ℓ is relatively prime to the order of the component group of $\mathcal{A}_f \to C$ for every twist.

We make these assumptions because they imply the cohomology groups of the $\mathbb{Z}_\ell$-sheaf $T_\ell(\mathcal{A}_f) \to C$, the latter defined as the projective system of the étale sheaves $\mathcal{A}_{f,\ell^n}$ (cf. section 2.2 of [G2]), are sufficiently well behaved. In particular, the $\mathbb{Z}_\ell$-sheaf $\mathcal{T}_{d,\ell^\infty} \to C$, defined as the projective system of the generalized sheaves $\mathcal{T}_{d,\ell^n} \to C$, is torsion free and $\mathcal{T}_{d,\ell^\infty} \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ is isomorphic to $\mathcal{T}_{d,\ell}$. The key is to consider the Kummer sequence

$$0 \longrightarrow T_\ell(\mathcal{A}_f) \xrightarrow{\times \ell} T_\ell(\mathcal{A}_f) \longrightarrow \mathcal{A}_{f,\ell} \longrightarrow 0$$

which is defined as the projective system of the sequences

$$0 \longrightarrow \mathcal{A}_{f,\ell^n} \longrightarrow \mathcal{A}_{f,\ell^{n+1}} \xrightarrow{\times \ell^n} \mathcal{A}_{f,\ell} \longrightarrow 0, \qquad n \geq 0.$$

The corresponding cohomology sequence simplifies (cf. 2.1–2.4 of [Shi]) to

$$0 \longrightarrow H^1(C \times \overline{k}, T_\ell(\mathcal{A}_f)) \xrightarrow{\times \ell} H^1(C \times \overline{k}, T_\ell(\mathcal{A}_f)) \longrightarrow H^1(C \times \overline{k}, \mathcal{A}_{f,\ell}) \longrightarrow 0$$

because $H^i(C \times \overline{k}, \mathcal{A}_{f,\ell}) = 0$ for $i \neq 1$, which implies the claim.

References

[Ac] J.D. Achter, "The distribution of class groups of function fields," J. Pure Appl. Algebra, 204 (2), 316–333, 2006.

[AP] J.D. Achter, R. Pries, "The integral monodromy of hyperelliptic and trielliptic curves," to appear in Math. Annalen, 2007.

[Ar] E. Artin, *Geometric Algebra*, Interscience, New York, 1957; Wiley Classics Library Edition, 1988.

[C] N. Chavdarov, "The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy," Duke Math. J. 87 (1997), no. 1, 151–180.

[CH] A. Cojocaru, C. Hall, "Uniform results for Serre's theorem for elliptic curves," Int. Math. Res. Not. 2005 (2005), no. 50, 3065–3071.

[CR] C. Curtis, I. Reiner, *Methods of Representation Theory I*, John Wiley & Sons, Inc., New York, 1981.

[DR] M. Dettweiler, S. Reiter, "An algorithm of Katz and its application to the inverse Galois problem," Algorithmic methods in Galois theory, J. Symbolic Comput. 30 (2000), no. 6, 761–798.

[D] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1901.

[FK] E. Freitag, R. Kiehl, "Étale cohomology and the Weil conjecture," Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 13. Springer-Verlag, 1988.

[G1] A. Grothendieck, *Fondements de la Géométrie Algébrique*, Séminaire Bourbaki 1957–62, Secrétariat Mathematique, Paris, 1962.

[G2] A. Grothendieck, "Modèles de Néron et monodromie", SGA 7 Part I, exposé IX, Springer Lecture Notes in Mathematics, Vol. 288, 1972.

[H] C. Hall, "L-functions of twisted Legendre curves," J. of Number Theory, Vol. 119, No. 1, 2006, 128–147.

[Hi] D. Hilbert, "Über die Irreducibilität ganzer rationaler Functionen mit ganzahligen Coeffizienten," J. reine angew. Math. 110, 104–129.

[I] J.-I. Igusa, "Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves," Amer. J. Math. 81, 1959, 453–476.

[Ka1] N.M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, 116, Princeton University Press, 1988.

[Ka2] N.M. Katz, *Rigid local systems*, Annals of Mathematics Studies, 139. Princeton University Press, Princeton, NJ, 1996.

[Ka3] N.M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, 150, Princeton University Press, Princeton, NJ, 2002.

[KS] N.M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, 45, 1999.

[KL] P. Kleidman, M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, 129.

[Kod] K. Kodaira, "On compact analytic surfaces. II," Ann. of Math. (2) 77 (1963), 563–626.

[Kow1] E. Kowalski, "On the rank of quadratic twists of elliptic curves over function fields," International J. of Number Theory 2 (2006), pp. 267–288.

[Kow2] E. Kowalski, "Weil numbers generated by other Weil numbers and torsion fields of abelian varieties," J. London Math. Soc. (2) 74 (2006), no. 2, 273–288.

[L] M. Larsen, "Maximality of Galois actions for compatible systems," Duke Math. J. 80 (1995), no. 3, 601–630.

[LO] H.W. Lenstra Jr., F. Oort, "Abelian varieties having purely additive reduction," J. Pure Appl. Algebra 36 (1985), no. 3, 281–298.

[MM] G. Malle, B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, 1999.

[MVW] C.R. Matthews, L.N. Vaserstein, B. Weisfeiler, "Congruence properties of Zariski-dense subgroups I," Proc. London Math. Soc. (3) 48 (1984), no. 3, 514–532.

[MP] R. Miranda, U. Persson, "On extremal rational elliptic surfaces," Math. Z. 193 (1986), no. 4, 537–558.

[N] M.V. Nori, "On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$," Invent. math. 88 (1987), no. 2, 257–275.

[O] A. Ogg, "Cohomology of abelian varieties over function fields," Ann. of Math. 76 (1962), 185–212.

[R] K. Ribet, "Galois actions on division points of abelian varieties with real multiplications," Amer. J. Math. 98 (1976), no. 3, 751–804.

[SGA1] A. Grothendieck et al, *Revêtements étale et groupe fondamental (1960–61)*, Lecture Notes in Math. 24, Springer, Heidelberg, 1971.

[S1] J-P Serre, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, New York, 1968; second edition, Addison-Wesley, Redwood City, 1989.

[S2] J-P Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques," Invent. math. 15 (1972), no. 4, 259–331.

[S3] J-P Serre, *Résumés des cours au Collège de France*, Annuaire du Collège de France (1985–1986), 95–99.

[S4] J-P Serre, "Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques," Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., 55, Part 1, 377–400.

[Sha1] I.R. Shafarevich, "Construction of fields of algebraic numbers with given solvable Galois group," Izv. Akad. Nauk SSSR. Ser. Mat. 18 (1954), 525-578.

[Sha2] I.R. Shafarevich, "Principal homogeneous spaces defined over a function field," Trudy Mat. Inst. Steklov 64 (1961), 316–346.

[Shi] T. Shioda, "On elliptic modular surfaces," J. Math. Soc. Japan 24 (1972), 20–59.

[Si] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, 1986.

[T] J. Thompson, "Quadratic pairs," Actes du Congrés International des Mathèmaticiens (Nice, 1970), Tome 1, pp. 375–376.

[Wa1] A. Wagner, "Collineation groups generated by homologies of order greater than 2," *Geom. Ded.*, 7, 387–398.

[Wa2] A. Wagner, "Determination of finite primitive reflection groups over an arbitrary field of characteristic not 2," *Geom. Ded.*, 9, 239–253; ibid. 10, 183–189, ibid. 10, 475–523.

[Yu] J.-K. Yu, "Toward a proof of the Cohen-Lenstra conjecture in the function field case," preprint (1996).

[ZS1] A.E. Zalesskiĭ, V.N. Serežkin, "Finite linear groups generated by reflections. (Russian)," Izv. Akad. Nauk SSSR Ser. Mat. 44 (1980), no. 6, 1279–1307, 38; translation in Math. USSR Izvestija, Vol. 17 (1981), no. 3, 477–503.

[ZS2] A.E. Zalesskiĭ, V.N. Serežkin, "Linear groups generated by transvections," (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 40 (1976), no. 1, 26–49, 221; translation in Math. USSR Izvestija, Vol. 10 (1976), no. 1, 25–46.