

Galois Representations Attached to Picard Curves

M. G. Upton

September 17, 2009

1

Abstract

Let $J(C)$ be the Jacobian of a Picard curve C defined over a number field K containing $\mathbb{Q}(\zeta_3)$. We consider the family $(\tilde{\rho}_l)_l$ of l -adic representations defined by the natural action of the Galois group $\text{Gal}(\overline{K}/K)$ on the l -power torsion of $J(C)$.

We show that for a Picard curve C with endomorphism ring $\mathbb{Z}[\zeta_3]$ the images of these representations are full for all but finitely many primes l . We consider the reduction modulo l of the image of $\tilde{\rho}_l$, that is, the action of $\text{Gal}(\overline{K}/K)$ on the l -torsion of the Jacobian. This gives a representation ρ_l into either $\text{GL}_3(\mathbb{F}_l)$ or into a unitary group over

¹With thanks to my advisor, Don Blasius, for suggesting this line of research and for many fruitful discussions.

I would also like to thank the anonymous reviewer for his/her useful suggestions

\mathbb{F}_{l^2} , depending on the splitting behavior of l in $\mathbb{Q}(\zeta_3)$. It is sufficient to show that the image of ρ_l is full in order to show that the image of $\tilde{\rho}_l$ is full.

1 Introduction

Let A be an abelian variety defined over a number field K . The action of the absolute Galois group $\text{Gal}(\overline{K}/K)$ on the l -power torsion of A gives an l -adic Galois representation $\rho_{A,l}$ for each prime l . A classic result of Serre ([17]) states that the Galois representations attached to an elliptic curve E without complex multiplication are surjective for almost all l .

Let K be a number field containing $\mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive cube root of unity. Picard curves are smooth projective curves of genus three which are isomorphic to a curve whose affine equation is

$$Y^3 = X^4 + G_2X^2 + G_3X + G_4,$$

where the polynomial $X^4 + G_2X^2 + G_3X + G_4$ has no repeated roots. The map $Y \mapsto \zeta_3 Y$ is an automorphism of any Picard curve whose field of definition contains ζ_3 . Let C be a Picard curve such that $\text{End}(J(C)) = \mathbb{Z}[\zeta_3]$ where $J(C)$ is the Jacobian of C . This paper considers the family of Galois representations attached to $J(C)$.

Picard curves were introduced by Emile Picard in 1883 ([13]). Like elliptic curves, they can be used in discrete log based cryptography. Bauer, Teske

and Weng ([1]) give an algorithm for counting the points on certain Picard curves over a finite field in the context of cryptography. Koike and Weng ([10]) state that the highest genus of curves suitable for discrete log based cryptography appears to be 3.

The main result in this paper is that, for a fixed Picard curve C , the image of the representation $\rho_{J(C),l}$ can be identified with $\mathrm{GL}_3(\mathbb{Z}_l)$ for almost all primes $l \equiv 1 \pmod{3}$ or with the group $\mathrm{GU}_3(O_L)$ of unitary similitudes over O_L , where O_L is the ring of integers of the quadratic extension $L = \mathbb{Q}(\zeta_3) \otimes \mathbb{Q}_l$ of \mathbb{Q}_l , for almost all primes $l \equiv 2 \pmod{3}$.

We show that the reduction modulo l of $\rho_{J(C),l}$ is, for all but finitely many primes l , onto $\mathrm{GL}_3(\mathbb{F}_l)$ or $\mathrm{GU}_3(\mathbb{F}_{l^2})$, where \mathbb{F}_q is the finite field with q elements. Applying Mitchell's classification ([12]) of the subgroups of PSL_3 and PSU_3 over a finite field, we find that the list of possible images of the reduction of $\rho_{J(C),l}$ is finite. We then apply a theorem of Serre to one member of this list (the completely reducible subgroups). The other subgroups are considered using different methods.

Serre ([15]) investigated the case of curves C over a number field with genus $g(C)$ odd or equal to 2 or 6 and where $\mathrm{End}(C) = \mathbb{Z}$. He showed that the image of ρ_l in that case is $\mathrm{Sp}_{2g}(\mathbb{Z}_l)$ for almost all l . In the case studied in this paper, there is additional structure provided by the larger endomorphism ring. As one result of this, the splitting behavior of l in $\mathbb{Q}(\zeta_3)$ becomes important.

We begin in section 1.1 with some background on l -adic representations.

In section 1.2, we introduce certain characters and a theorem of Serre which will be used in the main body of the proof.

In section 1.3 we continue with a discussion of the groups $\mathrm{PSL}_3(\mathbb{F}_l)$ and $\mathrm{PSU}_3(\mathbb{F}_{l^2})$. Section 1.4 is a discussion of the justification for reducing ρ_l modulo l .

In section 2 we introduce the Picard curves.

In section 3 we begin the body of the proof of the main result of this paper with a discussion of the action of the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$. Section 4 continues this discussion by considering the possible images for the representations.

The main result is formally stated in Section 5.

In the final section, we give several explicit examples of Picard curves and specific primes l for which the representation $\rho_{J(C),l}$ is onto.

1.1 Background on l -adic representations

1.1.1 Definitions

Let l be a rational prime and F a number field. An l -adic Galois representation ρ is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{F}/F) \rightarrow \mathrm{GL}(V) \cong \mathrm{GL}_n(E_l)$ where E_l is a finite extension of \mathbb{Q}_l and V is an n -dimensional vector space over E . The group $\mathrm{Gal}(\overline{F}/F)$ has the Krull (profinite) topology. The fields F and E need not be related.

Let k be the residue field of F at the place v of F . Recall that the inertia

subgroup I_v of $\text{Gal}(\overline{F}/F)$ is the kernel of the map $\text{Gal}(\overline{F}/F) \rightarrow \text{Gal}(\overline{k}/k)$. We write Fr_v for the Frobenius element at a place v of F .

Suppose that ρ_l and τ_l are two semi-simple l -adic Galois representations over a number field F which are ramified at only finitely many places of F . Then if the characteristic polynomials of $\rho_l(\text{Fr}_v)$ and $\tau_l(\text{Fr}_v)$ are equal at all of the unramified places v of F , it follows that $\rho_l = \tau_l$. This is a consequence of the Chebotarev density theorem([16]). While in theory this allows the complete determination of the image of any semi-simple Galois representation, in practice an explicit determination of the image of a representation ρ_l is non-trivial.

Definition 1. For each prime l , let $\rho_l : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_n(E)$ be an l -adic representation. The system $(\rho_l)_l$ is said to be a *strictly compatible system of representations in the sense of Serre*([16]) if there is a finite set of places S of F such that:

1. For any l , ρ_l is unramified outside S and the primes v of F over l . That is, $\rho_l(I_v)$ is trivial for each place $v \notin S$ not over l .
2. The characteristic polynomials of $\rho_l(\text{Fr}_p)$ have rational coefficients for all places p of F such that $p \notin S$ and p is not over l .
3. For any l and l' and for $p \notin S$ and not over l or l' , the characteristic polynomials of $\rho_l(\text{Fr}_p)$ and $\rho_{l'}(\text{Fr}_p)$ agree.

1.1.2 Representations from geometry

Let \bar{F} be an algebraic closure of a number field F . For X any variety defined over F , let $H_{et}^i(\bar{X}, \mathbb{Z}_l) = \varprojlim H_{et}^i(\bar{X}, \mathbb{Z}/l^n\mathbb{Z})$ be the l -adic étale cohomology of $\bar{X} = X \times_F \bar{F}$. Let $H_{et}^i(\bar{X}, \mathbb{Q}_l) = H_{et}^i(\bar{X}, \mathbb{Z}_l) \otimes \mathbb{Q}_l$. If $F \subseteq \mathbb{C}$, then $H_{et}^i(\bar{X}, \mathbb{Q}_l) \cong H_B^i(X \times_F \mathbb{C}, \mathbb{Q}_l)$, the usual Betti cohomology. This is sometimes known as Artin's comparison theorem. The Galois group $\text{Gal}(\bar{F}/F)$ acts on the points of X through its action on the field \bar{F} . It therefore also acts on $H_{et}^i(\bar{X}, \mathbb{Q}_l)$. This natural action of the Galois group defines a strictly compatible system of l -adic Galois representations in the sense of Serre.

For an abelian variety A defined over an algebraically closed field F , let $A[n]$ be the kernel of multiplication by $n \in \mathbb{N}$. The Tate module is defined as $T_l(A) = \varprojlim A[l^n]$. If A is a curve, then $H_{et}^1(\bar{A}, \mathbb{Q}_l)$ is the dual of $T_l(J)$, where J is the Jacobian of A . The l -adic Galois representations are given in this case by the action of $\text{Gal}(\bar{F}/F)$ on $T_l(J)$. This case was first studied by Taniyama ([19]).

We write $P_v(T)$ for the characteristic polynomial of $\rho_{J(A),l}(\text{Fr}_v)$, v is a place of F not over l . As the representations $\rho_{J(A),l}$ form a strictly compatible system, $P_v(T)$ is independent of l and has rational coefficients for almost all places v . Recall that for a curve C the zeta function $Z_v(C, T)$ is $\frac{P_v(T)}{(1-T)(1-qT)}$ where the residue field at v is \mathbb{F}_q .

The algebraic envelopes of the images of each $\rho_{J(A),l}$, i.e. the smallest algebraic Lie algebra containing this image, were shown by Bogomolov ([2]) to contain the homotheties. The Mumford-Tate conjecture states that the

image of such a representation $\rho_{J(A),l}$ is equal to $\mathfrak{h}_l = \mathbb{Q}_l \otimes \mathfrak{h}_{\mathbb{Q}}$ where $\mathfrak{h}_{\mathbb{Q}}$ is the Hodge group ([18]). This conjecture has been shown to be true in many cases (see for example [3, 18]). The image of $\rho_{J(A),l}$ is known to be open in some algebraic subgroup of $\mathrm{GL}_{2g}(\mathbb{Q}_l)$ ([2]).

In the case of a curve C , it follows from theorems of Faltings ([7]), that the commutator of the image of $\rho_{J(C),l}$ in $\mathrm{End}_{\overline{\mathbb{Q}_l}}(T_l(J(C)))$ is the endomorphism ring of $J(C)$ tensored with \mathbb{Q}_l .

1.2 Characters of $S_{\mathfrak{m}}$

We now review Serre's construction of certain spaces and maps ([16, 17]).

Let F be a number field. Let S be a finite set of finite places of F . Then $\mathfrak{m} = (m_v)_{v \in S}$ with the m_v strictly positive integers is called a *modulus* of *support* for S and S is called the support of \mathfrak{m} .

For any place v of F , let U_v be the group of units of the ring of integers of F_v , the completion of F at v . For v an infinite place, let $U_{v,\mathfrak{m}}$ be the connected component of F_v^* containing the identity. For finite v , let $U_{v,\mathfrak{m}} = U_v$ if $v \notin S$ and $\{x \in U_v \mid v(1-x) \geq m_v\}$ if $v \in S$, where we also write v for the valuation at the place v . Let $U_{\mathfrak{m}} = \prod_v U_{v,\mathfrak{m}}$ where the product is taken over all places v of F .

Let T be the torus of the multiplicative group of F (so $T(\mathbb{Q}) = F^*$). Denote the group of units of F by E . We embed E in the adèles over F diagonally and define $E_{\mathfrak{m}} = E \cap U_{\mathfrak{m}}$. Let $\overline{E}_{\mathfrak{m}}$ be the Zariski closure of $E_{\mathfrak{m}}$. Regarding $E_{\mathfrak{m}}$ as a subgroup of E and hence of F^* , we define $T_{\mathfrak{m}} = T/\overline{E}_{\mathfrak{m}}$.

We then have a natural map $\epsilon : F^*/E_m \rightarrow T_m$ by identifying F^* with $T(\mathbb{Q})$.

Let Γ be the set of embeddings of F into $\overline{\mathbb{Q}}$, the algebraic closure of \mathbb{Q} . Then $\sigma \in \Gamma$ can be extended by linearity to

$$\sigma_l : \prod_{v|l} F_v = F \otimes \mathbb{Q}_l \rightarrow \overline{\mathbb{Q}}_l$$

where σ_l is trivial on all but one F_v .

A character $[\sigma]$ of T can be defined for any $\sigma \in \Gamma$ by defining $[\sigma](x)$ for all $x \in T(\mathbb{Q})$ by $[\sigma](x) = \sigma(x)$. These form a basis of the characters of T .

Let ϕ be a character of T . It can then be written $\phi = \prod [\sigma]^{n(\sigma)}$ and the characters of T_m are those ϕ where $\phi(x) = 1$ for all $x \in E_m$.

Let C_m be the quotient of the idele class group C by the image of U_m in C . Let I be the idele group and I_m be the quotient of I by U_m .

There is an exact sequence

$$1 \rightarrow F^*/E_m \rightarrow I_m \rightarrow C_m \rightarrow 1.$$

We extend C_m by T_m to get S_m . That is, S_m is constructed so that the diagram

$$\begin{array}{ccc} F^*/E_m & \xrightarrow{\epsilon} & T_m(F) \\ \downarrow & & \downarrow \\ I_m & \longrightarrow & S_m(F) \end{array} \quad (1)$$

commutes and so that S_m is “universal” with respect to this diagram. Suppose we have a group B and maps $T_m \rightarrow B$ and $I_m \rightarrow B$ such that the

diagram

$$\begin{array}{ccc} F^*/E_{\mathfrak{m}} & \xrightarrow{\epsilon} & T_{\mathfrak{m}}(F) \\ \downarrow & & \downarrow \\ I_{\mathfrak{m}} & \longrightarrow & B \end{array}$$

commutes. By “universal” we mean that the only such groups and maps are those where the maps $T_{\mathfrak{m}} \rightarrow B$ and $I_{\mathfrak{m}} \rightarrow B$ are defined from the diagram in equation (1) by composition with a morphism $S_{\mathfrak{m}} \rightarrow B$.

Such a group $S_{\mathfrak{m}}$ is constructed by defining a group law on the disjoint union $\cup A_y$, where A_y is a copy of $T_{\mathfrak{m}}$ and y runs over $C_{\mathfrak{m}}$. Let \bar{y} be a representative of y in $I_{\mathfrak{m}}$. We define a map $c : C_{\mathfrak{m}} \times C_{\mathfrak{m}} \rightarrow F^*/E_{\mathfrak{m}}$ by for y and y' in $C_{\mathfrak{m}}$, $\bar{y} + \bar{y}' = \overline{y + y'} + c(y, y')$. We compose with ϵ to get $\epsilon \circ c : C_{\mathfrak{m}} \times C_{\mathfrak{m}} \rightarrow T_{\mathfrak{m}}$. We define the group law on $S_{\mathfrak{m}} = \cup A_y$ by sending $(a, a') \in A_y \times A_{y'}$ to $a + a' + \epsilon(c(y, y')) \in A_{y+y'} \subseteq S_{\mathfrak{m}}$.

The characters of $S_{\mathfrak{m}}$ are given by pairs $\psi = (\phi, f)$ where ϕ is a character of T and $f \in \text{Hom}(I, \overline{\mathbb{Q}}^*)$ such that $f(x) = 1$ for $x \in U_{\mathfrak{m}}$ and $f(x) = \phi(x)$ for $x \in F^*$.

The characters ϕ and ψ extend to $\phi_l : T_{\mathfrak{m}} \rightarrow \mathbb{Q}_l$ and $\psi_l : S_{\mathfrak{m}} \rightarrow \mathbb{Q}_l^*$ through the extension of $\sigma \in \Gamma$ to T discussed earlier in this section. Define $\psi_l : I \rightarrow \overline{\mathbb{Q}}_l^*$ by $\psi_l(a) = f(a)\phi_l(a_l^{-1})$ for a in I .

The map ψ_l is trivial on F^* and thus defines a map on the idele class group C . By class field theory, we have a map

$$\phi_l : \text{Gal}(F^{ab}/F) \rightarrow \overline{\mathbb{Q}}_l^*$$

where F^{ab} is the maximal abelian extension of F .

Let α_l be the map $I \rightarrow T(\mathbb{Q}_l) \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_l)$ defined by projecting $I \rightarrow T(\mathbb{Q}_l)$ and then applying the map from equation (1). We define $\epsilon_l(a) = \epsilon(a)\alpha_l(a^{-1})$. Then ϕ_l is the composition of $\phi : S_{\mathfrak{m}} \rightarrow \overline{\mathbb{Q}_l}^*$ with ϵ_l ([16]).

The following theorem is due to Serre.

Theorem 1 (Serre [17]). *Let (τ_l) be a system of strictly compatible semi-simple l -adic representations in the sense of Serre of $\text{Gal}(\overline{F}/F)$.*

Let k_l be the residue field of F at l . Suppose that there is an integer N and an infinite subset L of the set P of primes such that the reduction of $\tau_l \bmod l$ is abelian for all $l \in L$, that is, $\tau_l \bmod l$ is diagonal and so given by three characters $\theta_l^{(i)} : I \rightarrow k_l^$. Suppose further that there exist integers $n(\sigma, l, i)_{\sigma \in \Gamma}$, with absolute value bounded by N , such that*

$$\theta_l^{(i)}(a_l) = \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{n(\sigma, l, i)} \pmod{\mathfrak{p}_l} \quad (2)$$

for $a_l \in I$.

Then τ_l is isomorphic to the system ϕ_l associated to some $S_{\mathfrak{m}}$.

In particular, for all $l \in P$, τ_l is abelian.

1.3 Subgroups of $\text{PSL}_3(\mathbb{F}_l)$ and $\text{PSU}_3(\mathbb{F}_{l^2})$

Let l be a rational prime. Let \mathbb{F}_q be the finite field with $q = l^k$ elements, $k \geq 1$. We define $\text{PSL}_3(\mathbb{F}_q)$ to be the quotient of $\text{SL}_3(\mathbb{F}_q)$ by its center. In the case that $l \equiv 2 \pmod{3}$, this center is trivial. When $l \equiv 1 \pmod{3}$, this

center is the subgroup of cube roots of unity realized as diagonal matrices.

The subgroups of $PSL_3(\mathbb{F}_q)$ were classified by Mitchell ([12]). We only need the case $q = l$.

Lemma 1 (Mitchell [12]). *Let H be a subgroup of $PSL_3(\mathbb{F}_l)$, $l \geq 7$. Then H is one of*

1. $PSL_3(\mathbb{F}_l)$.
2. *A subgroup of a proper parabolic subgroup. A parabolic group is a group which fixes a proper subspace of \mathbb{F}_l^3 .*
3. *A subgroup of the normalizer of a split Cartan subgroup. A split Cartan subgroup is a group conjugate over \mathbb{F}_l to a group generated by the diagonal elements. Its normalizer additionally contains the symmetric group on three elements. These groups have order prime to l .*
4. *A subgroup of the normalizer of a non-split Cartan subgroup. A non-split Cartan subgroup is conjugate to a group generated by diagonal elements but this conjugacy is over an extension of the field \mathbb{F}_l and not over \mathbb{F}_l itself. These groups have order prime to l .*
5. *A group isomorphic to A_6 (the alternating group on 6 letters which is of order 360), $PSL_2(\mathbb{F}_7)$ (with order 168) or the Hessian group or its subgroups of order 36 or 72. (Note that not all of these are possible for a given l .) The Hessian group is a classical group of order 216.*

6. A non-degenerate orthogonal group, a group which fixes a non-degenerate cone. That is, a group of elements of $PSL_3(\mathbb{F}_l)$ whose action is invariant on a quadratic form $\sum_{i,j=1}^3 a_{ij}x_i x_j$, with $a_{ij} \in \mathbb{F}_q$ and $\det(a_{ij}) \neq 0$ ([21]) where (a_{ij}) is the matrix of the a_{ij} .

Mitchell also classified the subgroups of the group $PSU_3(\mathbb{F}_{l^{2k}})$. We only need the case $k = 1$, where the result is as follows.

Lemma 2 (Mitchell [12]). *Let H be a subgroup of $PSU_3(\mathbb{F}_{l^2})$, $l \geq 7$. Then H is one of*

1. $PSU_3(\mathbb{F}_{l^2})$.
2. A subgroup of a proper parabolic subgroup.
3. A subgroup of the normalizer of a split or non-split Cartan subgroup.
These groups have order prime to l .
4. A group isomorphic to A_6 , $PSL_2(\mathbb{F}_7)$ or the Hessian group of order 216.
5. A non-degenerate orthogonal group.

1.4 Lifting

Let

$$r_m : \mathbb{Z}_l \rightarrow \mathbb{Z}/l^m\mathbb{Z}$$

be reduction modulo l^m for an integer $m \geq 1$. This map extends to any ring over \mathbb{Z}_l . We may also extend r_m to $GL_n(\mathbb{Z}_l)$ and to any of its subgroups.

Definition 2. For a ring R and any Hermitian form h on R^n , the special unitary group $SU_n(R, h)$ consists of those elements of $SL_n(R)$ which leave h invariant. The unitary group $U_n(R, h)$ is defined similarly as the group of those elements of $GL_n(R)$ which leave h invariant. The general unitary group or group of unitary similitudes, $GU_n(R, h)$, is the subgroup of $GL_n(R)$ which leaves h invariant up to multiplication by a constant.

We say that h represents 0 if there is a nonzero element $v \in R^n$ such that $h(v, v) = 0$.

In the case of a finite field, we may neglect the form h as all Hermitian forms are equivalent over a finite field and hence define identical groups ([4]). It is sometimes standard to write $SU_n(\mathbb{F}_l)$ for the group which we denote as $SU_n(\mathbb{F}_{l^2})$.

The goal of this section is to establish the following proposition.

Proposition 1. *Let $l \geq 5$ be a rational prime which does not divide n .*

- *Suppose that H is a subgroup of $GL_n(\mathbb{Z}_l)$. If $r_1(H) \cap SL_n(\mathbb{F}_l)$ projects onto $PSL_n(\mathbb{F}_l)$, then H contains the group $SL_n(\mathbb{Z}_l)$.*
- *Let L be a quadratic extension of \mathbb{Q}_l with ring of integers O_L and let h be a Hermitian form on O_L^n which represents 0. Suppose H is a subgroup of $GU_n(O_L, h)$. If $r_1(H) \cap SU_n(\mathbb{F}_{l^2})$ projects onto $PSU_3(\mathbb{F}_{l^2})$ then H contains the group $SU_3(O_L, h)$.*

We adapt Serre's argument for $GL_2(\mathbb{Z}_l)$ ([17]).

It is well known that $\mathrm{PSL}_n(\mathbb{F}_q)$ is simple for $n > 2$ or $q \geq 4$ and that $\mathrm{PSU}_n(\mathbb{F}_{l^2})$ is simple except when $n = 2$ and $l = 2$ or 3 or $n = 3$ and $l = 2$ ([8, 11]).

Lemma 3. *Let l be a prime not dividing n . Suppose that H is a subgroup of $\mathrm{SL}_n(\mathbb{F}_l)$ such that H maps surjectively to $\mathrm{PSL}_n(\mathbb{F}_l)$. Then $H = \mathrm{SL}_n(\mathbb{F}_l)$.*

Proof. Let Z be the center of $\mathrm{SL}_n(\mathbb{F}_l)$

Let d be the greatest common divisor of n and $l - 1$. Then Z is the subgroup of d -th roots of unity $\zeta \in \mathbb{F}_l$ realized as diagonal matrices. If $d = 1$, then $\mathrm{SL}_n(\mathbb{F}_l) = \mathrm{PSL}_n(\mathbb{F}_l)$ and the result is trivial.

Otherwise, we decompose $\mathrm{SL}_n(\mathbb{F}_l) = ZH$ as the hypothesis of the lemma state that $H/Z = \mathrm{PSL}_n(\mathbb{F}_l)$.

Recall that the elementary matrices are matrices of the form $I + E$ where I is the identity matrix and E is a matrix whose only nonzero entry is its ij^{th} entry with $i \neq j$. The elementary matrices are of order l and generate $\mathrm{SL}_n(\mathbb{F}_l)$ ([11]).

Fix a d^{th} root of unity ζ which generates Z . We write $I + E$ as $\zeta^a h$ where $h \in H$ and a is some integer. Let b be such that $db \equiv 1 \pmod{l}$. Consider $h^{db} \in H$. Then $h^{db} = (\zeta^{-a}(I + E))^{db} = \zeta^{-adb}(I + E)^{db} = I + E$ and hence $I + E \in H$. We conclude that H contains the elementary matrices and hence that $H = \mathrm{SL}_n(\mathbb{F}_l)$. □

Lemma 4. *Let l be an odd prime which does not divide n . Suppose that H is a subgroup of $\mathrm{SU}_n(\mathbb{F}_{l^2})$ such that H projects onto all of $\mathrm{PSU}_n(\mathbb{F}_{l^2})$. Then*

$$H = SU_n(\mathbb{F}_{l^2}).$$

Proof. If $l-1$ is relatively prime to n , there is nothing to show as $PSU_n(\mathbb{F}_{l^2}) = SU_n(\mathbb{F}_{l^2})$. So we assume that $l-1$ and n are not relatively prime. Let d be the greatest common divisor of $l-1$ and n .

Again, note that it is possible to write $SU_n(\mathbb{F}_{l^2}) = ZH$ where $Z = \{\zeta \in \mathbb{F}_{l^2} : \zeta^d = 1\}$ is the center of $SU_n(\mathbb{F}_{l^2})$. The ζ are realized as diagonal matrices.

Recall that a transvection on a space V is a map τ which fixes a subspace $W \subseteq V$ of codimension 1 and satisfies $\tau v - v \in W$ for all vectors $v \in V$ ([8]). Transvections have l power order ([8]).

Let $\tau \in SU_n(\mathbb{F}_{l^2})$ be a transvection with order l^a . As $H/Z = SU_n(\mathbb{F}_{l^2})$, there is some n -th root of unity ζ such that $\zeta\tau \in H$. As in the previous lemma, we take b such that $nb \equiv 1 \pmod{l^a}$. Therefore $\tau = (\zeta\tau)^{nb} \in H$.

The group $SU_n(\mathbb{F}_{l^2})$ is generated by its transvections([8]). Hence $H = SU_n(\mathbb{F}_{l^2})$.

□

Serre states the following lemma in [17], with a proof for the case $n = 2$. The general proof below is very similar.

Lemma 5. *Let $l \geq 5$ be prime. If $H \subseteq SL_n(\mathbb{Z}_l)$ is a topologically closed subgroup and $r_1(H) = SL_n(\mathbb{F}_l)$ then $H = SL_n(\mathbb{Z}_l)$.*

Proof. Consider the group $r_m(H) \subseteq SL_n(\mathbb{Z}/l^m\mathbb{Z})$. To show that $H = SL_n(\mathbb{Z}_l)$, it suffices to show $r_m(H) = SL_n(\mathbb{Z}/l^m\mathbb{Z})$ for all positive integers m .

We induct on m and show that, for $m > 1$, if $r_{m-1}(H) = \mathrm{SL}_n(\mathbb{Z}/l^{m-1}\mathbb{Z})$ then $r_m(H) = \mathrm{SL}_n(\mathbb{Z}/l^m\mathbb{Z})$.

Let $s \in \mathrm{SL}_n(\mathbb{Z}_l)$. We wish to show that there is an $s_1 \in H$ such that $s_1 \equiv s \pmod{l^m}$. By the induction hypothesis, there is an $x \in H$ such that $x \equiv s^{-1} \pmod{l^{m-1}}$. Hence it is enough to show the existence of such an element s_1 for $s \equiv 1 \pmod{l^{m-1}}$.

Write $s = 1 + l^{m-1}u$. The determinant of s is 1, so u has trace zero modulo l . Any such matrix u can be written as $u = \sum u_j$ where $u_j^2 \equiv 0 \pmod{l}$ and $\mathrm{Tr}u_j \equiv 0 \pmod{l}$. We write

$$s \equiv \prod_{j=1}^k (I + l^{m-1}u_j) \pmod{l^m}$$

as $m \geq 2$. It is enough to show that there are $h_j \in H$ such that $r_m(I + l^{m-1}u_j) = r_m(h_j)$ for each j , as then the product of such h_j is trivially an element of H .

We now assume therefore that $s = 1 + l^{m-1}u$ for some matrix u with zero trace and $u^2 = 0$.

Recall that the reduction of $H \pmod{l^{m-1}}$ is all of $\mathrm{SL}_n(\mathbb{Z}/l^{m-1}\mathbb{Z})$ by the induction hypothesis. Therefore there is an element $y \in H$ with $y \equiv 1 + l^{m-2}u \pmod{l^{m-1}}$.

Consider $y^l \in H$. We have

$$y^l = I + l(l^{m-2}u) + \frac{l(l-1)}{2}(l^{m-2}u)^2 + \cdots + (l^{m-2}u)^l \equiv I + l^{m-1}u \pmod{l^m}. \quad (3)$$

When $m \geq 3$, this congruence follows from $(l^{m-2})^k \equiv 0 \pmod{l^m}$ for $k \geq 3$ and $\frac{l(l-1)}{2}(l^{m-2})^2 \equiv 0 \pmod{l^m}$. When $m = 2$, the requirement that $u^2 = 0$ is necessary.

Hence, $y^l \equiv s \pmod{l^m}$ and $r_m(H) = \mathrm{SL}_n(\mathbb{Z}/l^m\mathbb{Z})$.

□

A similar lemma applies to the special unitary group.

Lemma 6. *Let $l \geq 5$ be a prime which does not divide n . Let L be a quadratic extension of \mathbb{Q}_l in which l is inert. Let O_L be the ring of integers of L . Let h be a Hermitian form which represents 0. If $H \subseteq \mathrm{SU}_n(O_L, h)$ is topologically closed and $r_1(H) = \mathrm{SU}_n(\mathbb{F}_{l^2})$ then $H = \mathrm{SU}_n(O_L, h)$.*

Proof. Again, the proof is by induction. We show that if

$$r_{m-1}(H) = \mathrm{SU}_n(O_L/l^{m-1}O_L, h)$$

then $r_m(H) = \mathrm{SU}_n(O_L/l^mO_L, h)$.

We again assume that $s \equiv 1 \pmod{l^mO_L}$. We then find an element $x \in H$ such that $r_m(x) = r_m(s)$.

For $m \geq 3$, we write $s = I + l^{m-1}u$. Then there is an element $y \in H$ such that $y \equiv I + l^{m-2}u \pmod{l^{m-1}O_L}$. We take $y^l \equiv (I + l^{m-2}u)^l \equiv I + l^{m-1}u$

(mod $l^m O_L$) as in equation (3) in the proof of Lemma 5. Thus the difficult step is when $m = 2$, that is, the first step of the induction.

We first consider the case that $n = 2$. Recall that the groups $\text{PSU}_n(\mathbb{F}_{l^2}, h)$ are isomorphic for all Hermitian forms h so that we may consider a single realization of this group.

To see that u can be written as the sum of matrices u_j with $u_j^2 \equiv 0$ (mod lO_L), consider the case $L = \mathbb{Q}[i]$ with $i^2 = -1$ and $h = z_1 \bar{z}_2 - \bar{z}_1 z_2$. We then take u of the form $\begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$. The space of such matrices with trace zero is spanned by $\begin{pmatrix} i & i \\ -i & -i \end{pmatrix}$, $\begin{pmatrix} i & 1 \\ 1 & -i \end{pmatrix}$ and $\begin{pmatrix} -i & 1 \\ 1 & i \end{pmatrix}$, all of which have square zero. We write $s \equiv \prod (I + lu_j) \equiv I + l \sum u_j$ (mod $l^2 O_L$) where the u_j have square zero. It suffices to show that for each term in this product there is an $x_j \in H$ such that $r_2(x_j) = r_2(1 + u_j)$. Hence, we assume that $s = 1 + lu$ where $u^2 = 0$. We take $y \in H$ such that $y \equiv 1 + u$ (mod lO_L). Such a y exists as $r_1(H) = \text{SU}_n(\mathbb{F}_{l^2})$ by the induction hypothesis. We see that $y^l \equiv I + lu + \binom{l}{2} u^2 + \dots + u^l \equiv 1 + lu$ (mod $l^2 O_L$) as u^2 divides all other terms.

In the case that $n \geq 3$, consider the space of u such that $1 + lu$ is unitary with determinant 1. This has dimension $n^2 - 1$ over O_L . Choose an isotropic basis $\{v_j\}$ for O_L^n , that is, a basis such that h represents 0 on the space spanned by any two elements v_j and v_k of the basis.

For a pair (v_j, v_k) in this basis, the space of $s \in \text{SU}_n(O_L, h)$ such that s is trivial outside of the hyperplane spanned by v_j and v_k is isomorphic to $\text{SU}_2(O_L, h_2)$, where h_2 , the restriction of h to this space, is a Hermitian form that represents 0. Restricting to $s \equiv 1$ (mod lO_L), we write each

of these s as $1 + lu$. This defines a three dimensional vector space of the elements u . This space is spanned by three elements u_i such that $u_i^2 = 0$ as $\{u : 1 + lu \in \text{SU}_2(O_L, h_2)\}$ has such a basis. The set of the u_i as $\{v_j, v_k\}$ run over all pairs in the basis span the space $\{1 + lu \in \text{SU}_n(O_L, h)\}$. Hence s may be written as $s \equiv \prod(1 + lu_j) \pmod{l^2 O_L}$ where each $u_j^2 = 0$. We therefore assume that $s = 1 + lu$ where $u^2 \equiv 0 \pmod{l O_L}$.

As $r_1(H) = \text{SU}_n(\mathbb{F}_{l^2})$, there is an $x \in H$ such that $r_1(x) = r_1(1 + u)$. Then $r_2((1 + u)^l) = r_2(1 + lu)$ as in the previous lemma. We have produced $y = x^l \in H$ such that $r_2(y) = r_2(s)$ as desired.

□

Definition 3. Let G be a profinite group with the Krull topology. Then a finite simple group S is said to *occur* in G if there are closed subgroups G_1 and G_2 of G with G_2 normal in G_1 such that $S \cong G_1/G_2$. We write $\text{Occ}(G)$ for the set of S which occur in G ([16]).

If H is normal in G , then $\text{Occ}(G) = \text{Occ}(G/H) \cup \text{Occ}(H)$ ([16]).

If $G = \varprojlim_a G_a$ for some family G_a and G surjects onto each G_a , then $\text{Occ}(G) = \cup_a \text{Occ}(G_a)$ ([16]).

Lemma 7. *Let l be a prime not dividing n . If $n = 2$ we further require that $l \neq 2, 3$.*

- *Let G be open in $GL_n(\mathbb{Z}_l)$, Suppose that $SL_n(\mathbb{F}_l) \subseteq r_1(G)$. Then G contains $SL_n(\mathbb{Z}_l)$.*

- Let h be a Hermitian form on \mathbb{Z}_l^n which represents 0. Let G be open in $\mathrm{GU}_n(\mathcal{O}_L, h)$. Suppose that $\mathrm{SU}_n(\mathbb{F}_{l^2}) \subseteq r_1(G)$. Then G contains $\mathrm{SU}_n(\mathcal{O}_L)$.

Proof. We need the condition that $l \neq 2, 3$ if $n = 2$ as we use the simplicity of $\mathrm{PSL}_n(\mathbb{F}_l)$ and $\mathrm{PSU}_n(\mathbb{F}_{l^2})$.

We give the proof for $G \subseteq \mathrm{GL}_n(\mathbb{Z}_l)$. The proof for $G \subseteq \mathrm{GU}_n(\mathcal{O}_L, h)$ is identical.

As $r_1(G)$ contains $\mathrm{SL}_n(\mathbb{F}_l)$, it is clear that $\mathrm{PSL}_n(\mathbb{F}_l)$ occurs in G . Let $H = G \cap \mathrm{SL}_n(\mathbb{Z}_l)$. Then $\mathrm{PSL}_n(\mathbb{F}_l)$ does not occur in G/H .

Let $\tilde{H} = r_1(H) \subseteq \mathrm{SL}_n(\mathbb{F}_l)$. The kernel of this reduction is a pro- l group. Thus $\mathrm{Occ}(H)$ is equal to $\mathrm{Occ}(\tilde{H})$ as pro- l groups are solvable.

Since $\mathrm{PSL}_n(\mathbb{F}_l) \in \mathrm{Occ}(G) = \mathrm{Occ}(G/H) \cup \mathrm{Occ}(H)$ but $\mathrm{PSL}_n(\mathbb{F}_l)$ does not occur in G/H , we have $\mathrm{PSL}_n(\mathbb{F}_l) \in \mathrm{Occ}(H) = \mathrm{Occ}(\tilde{H})$. Thus \tilde{H} maps onto $\mathrm{PSL}_n(\mathbb{F}_l)$ and hence onto $\mathrm{SL}_n(\mathbb{F}_l)$ by Lemma 3. This implies that $H = \mathrm{SL}_n(\mathbb{Z}_l)$ by Lemma 5 as required.

□

We have shown that it suffices to show that $r_1(G \cap \mathrm{SL}_n(\mathbb{Z}_l))$ has image $\mathrm{PSL}_n(\mathbb{F}_l)$ in order to demonstrate that $\mathrm{SL}_n(\mathbb{Z}_l) \subseteq G$. Similarly, when h is a Hermitian form that represents 0 (for example, any Hermitian form if n is odd) and $G \subseteq \mathrm{GU}_n(\mathcal{O}_L) = \mathrm{GU}_n(\mathcal{O}_L, h)$, it is sufficient to show that $r_1(G \cap \mathrm{SU}_n(\mathcal{O}_L))$ reduces to $\mathrm{PSU}_n(\mathbb{F}_{l^2})$ in order to deduce that $\mathrm{SU}_n(\mathcal{O}_L) \subseteq G$. This is exactly what was needed for Proposition 1.

2 Picard curves

2.1 Definitions and preliminaries

A Picard curve over a field F is a nonsingular algebraic curve C which is isomorphic to a plane projective curve given by

$$WY^3 = G_0X^4 + G_1WX^3 + G_2W^2X^2 + G_3W^3X + G_4W^4$$

with $G_0 \neq 0$ and $G_j \in F$ for $j = 0, 1, 2, 3, 4$.

In affine coordinates $x = X/W$ and $y = Y/W$, this equation is

$$y^3 = G_0x^4 + G_1x^3 + G_2x^2 + G_3x + G_4$$

which reduces to the normal form

$$y^3 = x^4 + g_2x^2 + g_3x + g_4 \tag{4}$$

(with $g_j \in F$ for $j = 2, 3, 4$) if the characteristic of F is not 3.

This curve has good reduction at primes not dividing its discriminant $\Delta = 16g_2^4g_4 - 128g_2^2g_4^2 - 4g_2^3g_3^2 + 144g_2g_3^2g_4 - 27g_3^4 + 256g_4^3$ ([9]).

This is a homogeneous polynomial of degree 4, so by means of the genus formula for nonsingular curves, we have that the genus of a Picard curve is 3.

2.2 Jacobian

Recall that K is a number field containing $\mathbb{Q}(\zeta_3)$. Let C be a Picard curve over K . Then the map $(x, y) \mapsto (x, \zeta_3 y)$, where ζ_3 is a primitive cube root of unity, is in $\text{Aut}(C)$. Note that $\mathbb{Q}_l \otimes \mathbb{Q}(\zeta_3)$ is either a quadratic extension of \mathbb{Q}_l , or, if l splits in $\mathbb{Q}(\zeta_3)$, isomorphic to $\mathbb{Q}_l \oplus \mathbb{Q}_l$.

Let \bar{K} be an algebraic closure of K . Write $G_K = \text{Gal}(\bar{K}/K)$. For each l , let

$$\tilde{\rho}_{l,6} : G_K \rightarrow \text{Aut}(J[l^\infty]) \cong \text{GL}_6(\mathbb{Z}_l) \quad (5)$$

be the l -adic Galois representation given by the action of the Galois group on the l -primary torsion $J[l^\infty]$ of the Jacobian J of C .

There is a nondegenerate symplectic pairing, the Weil pairing, on the Jacobian of C . This implies that in general $\tilde{\rho}_{l,6}(G_K)$ is conjugate to a subgroup of $\text{GSp}(6, \mathbb{Z}_l)$.

Let $l \geq 5$ be a rational prime, $l \equiv 1 \pmod{3}$, $l \nmid \Delta$. Then l splits in $\mathbb{Q}(\zeta_3)$ so that $\mathbb{Q}_l \otimes \mathbb{Q}(\zeta_3) \cong \mathbb{Q}_l \oplus \mathbb{Q}_l$. We fix a prime λ of $\mathbb{Q}(\zeta_3)$ above l . The space $J[l^\infty]$ splits into two spaces, each of dimension three as $\text{End}(J)$ contains $\mathbb{Z}[\zeta_3]$. We write $J[l^\infty]_I$ for the space associated to the prime λ and $J[l^\infty]_c$ for the space associated to the conjugate of λ .

The representation $\tilde{\rho}_{l,6}$ has image in a subgroup of $\text{GL}_6(\mathbb{Q}_l)$ isomorphic to $\text{GL}_3(\mathbb{Q}_l) \times \text{GL}_3(\mathbb{Q}_l)$ and therefore

$$\tilde{\rho}_{l,6} : G_K \rightarrow \text{Aut}_{\bar{K}}(J[l^\infty]_I) \times \text{Aut}_{\bar{K}}(J[l^\infty]_c) \cong \text{GL}_3(\mathbb{Z}_l) \times \text{GL}_3(\mathbb{Z}_l).$$

When l is split and $J[l^\infty] \cong J[l^\infty]_I \times J[l^\infty]_c$, the Weil pairing pairs $J[l^\infty]_I$ with $J[l^\infty]_c$. Hence, the images of $\tilde{\rho}_{l,6}$ in the two copies of $\mathrm{GL}_3(\mathbb{Q}_l)$ are dual, up to a twist by a cyclotomic character. This splitting is canonical as the full ring of integers $\mathbb{Z}[\zeta_3]$ of $\mathbb{Q}(\zeta_3)$ acts on $J[l^\infty]$. When l splits in $\mathbb{Q}(\zeta_3)$, we consider the map

$$\tilde{\rho}_l : G_K \rightarrow \mathrm{GL}_3(\mathbb{Z}_l)$$

given by the action of G_K on $J[l^\infty]_I$. Similarly, let $\tilde{\rho}_{l,c}$ be given by the action of G_K on $J[l^\infty]_c$.

Recall that the Weil pairing is symplectic and thus, when l does not split in $\mathbb{Q}(\zeta_3)$, we may consider the Weil pairing as a Hermitian form over \mathbb{F}_{l^2} . The image of $\tilde{\rho}_{l,6}$ can be viewed as a subgroup of the group $\mathrm{GU}_3(O_L)$ of unitary similitudes over the group of integers O_L of the quadratic extension $L = \mathbb{Q}(\zeta_3) \otimes \mathbb{Q}_l$ of \mathbb{Q}_l . In this case, let

$$\tilde{\rho}_l : G_K \rightarrow \mathrm{GU}_3(O_L).$$

3 Determination of the image of $\tilde{\rho}_l$

Henceforth we make the key assumption that C is a Picard curve with $\mathrm{End}(J) \cong \mathbb{Z}[\zeta_3]$.

Let ρ_l be the reduction mod l of the representation $\tilde{\rho}_l$ defined above and, for $l \equiv 1 \pmod{3}$, let $\rho_{l,c}$ be the reduction of $\tilde{\rho}_{l,c}$. Let $\bar{\rho}_l$ be the corresponding map with image in $\mathrm{PSL}_3(\mathbb{F}_l)$ or $\mathrm{PSU}_3(\mathbb{F}_{l^2})$.

We wish to show that $\tilde{\rho}_l = \mathrm{GL}_3(\mathbb{Z}_l)$ for almost all $l \equiv 1 \pmod{3}$ and $\tilde{\rho}_l = \mathrm{GU}_3(O_L)$ for almost all $l \equiv 2 \pmod{3}$.

By Proposition 1 from section 1.4, we may reduce this question to one on $\rho_l(G_K)$ and $\det \circ \tilde{\rho}_l(G_K)$, the image of $\tilde{\rho}_l$ composed with the determinant map. That is, we need to show that $\rho_l(G_K) \cap \mathrm{SL}_3(\mathbb{F}_l)$ projects onto $\mathrm{PSL}_3(\mathbb{F}_l)$ for almost all $l \equiv 1 \pmod{3}$ and that $\rho_l(G_K) \cap \mathrm{SU}_3(\mathbb{F}_{l^2})$ projects onto $\mathrm{PSU}_3(\mathbb{F}_{l^2})$ for almost all $l \equiv 2 \pmod{3}$. We also need that $\det \circ \tilde{\rho}_l(G_K) = \mathbb{Z}_l^*$.

3.1 Inertia and fundamental characters

Let F be a number field. Fix a rational prime l and a prime λ of F above l . Let I_l be the inertia subgroup of $G_F = \mathrm{Gal}(\overline{F}/F)$ at λ and let I_w be the l -power subgroup, that is, the subgroup of wild inertia. Then $I_t = I_l/I_w$ is the subgroup of tame inertia.

Let F_{nr} be the maximal unramified extension of F . Let π be a uniformizer of F_λ , the completion of F at λ . One then defines characters

$$\theta_d : I_t \rightarrow \mu_d \cong \mathrm{Gal}(F_{nr}(\pi^{1/d})/F_{nr})$$

by setting $s(\pi^{1/d}) = \theta_d(s)\pi^{1/d}$ for $s \in \mathrm{Gal}(F_{nr}(\pi^{1/d})/F_{nr})$. The fundamental characters of level n are the characters

$$\theta_{l^{n-1}} : I_t \rightarrow \mathbb{F}_{l^n}$$

composed with an embedding of \mathbb{F}_{l^n} into its separable closure ([17]). If ϕ is one fundamental character of level n , then the other fundamental characters of level n are given by ϕ^{p^h} with $1 \leq h < n$. The norm of a fundamental character of level n is the fundamental character of level 1 ([14]). Any character $I_t \rightarrow \mathbb{F}_{l^n}$ is uniquely given by $\phi_1^{a_1} \phi_2^{a_2} \cdots \phi_n^{a_n}$ where the ϕ_j are the fundamental characters of level n and $0 \leq a_j < l$ ([14]).

For an unramified l , the fundamental character $\phi : I_t \rightarrow \mathbb{F}_l^* \cong \text{Aut}(\mu_l)$ of level 1 is equal to χ_l , the l -th cyclotomic character.

If A is an abelian variety over the number field F and \bar{A}_λ is the reduction of A at λ , then $\bar{A}_\lambda[l]$ is the direct sum of Jordan-Hölder factors. That is, $\bar{A}_\lambda[l] = \bigoplus V_j$ where V_j are \mathbb{F}_l vector spaces which are irreducible under the Galois action.

The theorem below was proven by Raynaud in a much more general form.

Theorem 2 (Raynaud [14]). *Let A be an abelian variety of dimension d over a local field F with good reduction at l . Let V be a Jordan-Hölder quotient of $A[l](\bar{F})$ of dimension n where $1 \leq n \leq d$. Then the wild inertia I_w acts trivially on V . We may give V a one dimensional \mathbb{F}_{l^n} vector space structure such that the action of I_t is given by a single character $\phi = \phi_1^{a_1} \cdots \phi_n^{a_n}$. The exponents $a_j = 0$ or 1 and the ϕ_j are the fundamental characters of level n .*

We also recall the following well known result ([14]).

Lemma 8. *The determinant of the action of the Galois group on $A[l]$ is given by χ_l^d , where χ_l is the cyclotomic character.*

3.2 Action on the Picard curve

Recall that C is a Picard curve with $\text{End}(J(C)) = \mathbb{Z}[\zeta_3]$. Let $l \geq 5$ be a rational prime at which C has good reduction. Fix a prime λ of K above l . As the Jacobian $J = J(C)$ has a canonical integral structure, we may take the reduction of J modulo λ .

There is an exact sequence on the l torsion of J

$$0 \rightarrow J[l]^0 \rightarrow J[l] \rightarrow J[l]^{et} \cong (J/\mathbb{F}_l)[l] \rightarrow 0$$

where $(J/\mathbb{F}_l)[l]$ is the l -torsion of the reduction modulo λ of J viewed as a Galois module with respect to G_K . The inertia group acts trivially on $J[l]^{et}$. Taking the inverse limit of similar sequences on the l^h ($h \geq 1$) torsion, there is another exact sequence ([20])

$$0 \rightarrow J[l^\infty]^0 \rightarrow J[l^\infty] \rightarrow J[l^\infty]^{et} \rightarrow 0.$$

If $l \equiv 1 \pmod{3}$ (so that l splits in K), $J[l] = J[l]_I \oplus J[l]_c$ where each component has dimension 3. Thus $J[l]^{et}$ can be written as $J[l]_I^{et} \oplus J[l]_c^{et}$.

The sequences

$$0 \rightarrow J[l^\infty]_I^0 \rightarrow J[l^\infty]_I \rightarrow J[l^\infty]_I^{et} \rightarrow 0$$

and

$$0 \rightarrow J[l]_I^0 \rightarrow J[l]_I \rightarrow J[l]_I^{et} \rightarrow 0$$

remain exact as do the corresponding sequences for $J[l]_c$ and $J[l^\infty]_c$.

Since $\dim_{\mathbb{Z}_l} J[l^\infty]_I = 3$, it is clear that $0 \leq \dim_{\mathbb{Z}_l} J[l^\infty]_I^{et} \leq 3$. We consider $J[l^\infty] \cong H_{et}^1(J, \mathbb{Z}_l) \cong H_B^1(J, \mathbb{Z}_l)$, where $H_B^1(J, \mathbb{Z}_l)$ is the familiar Betti cohomology and $H_{et}^1(J, \mathbb{Z}_l)$ is the l -adic cohomology from section 1.1.2. Suppose $\dim_{\mathbb{F}_l} J[l^\infty]_I^{et} = 3$. Then, as ζ_3 acts as the identity on $J[l^\infty]_I$, we would have that ζ_3 acts as the identity on $H_B^1(J, \mathbb{Z}_l)$. However a basis of these differentials is given by $\{\frac{dx}{y}, \frac{dx}{y^2}, \frac{xdx}{y^2}\}$ ([9]) and ζ_3 acting as $(x, y) \mapsto (x, \zeta_3 y)$ on C thus acts via the identity map on $H_B^1(J, \mathbb{Z}_l)$ with multiplicity 2. Hence, $\dim_{\mathbb{Z}_l} J[l^\infty]_I^0 = 2$ and $\dim_{\mathbb{Z}_l} J[l^\infty]_c^0 = 1$.

When $l \equiv 2 \pmod{3}$, the action of inertia can be considered as \mathbb{F}_{l^2} linear. We note that $\dim_{\mathbb{F}_{l^2}} J[l]^0 \neq 2$ so that $\dim_{\mathbb{F}_l} J[l]^0 = 4$ or 6 .

We therefore have:

Lemma 9. *If $l \equiv 1 \pmod{3}$, then $\dim_{\mathbb{F}_l} J[l]_I^0 = 2$ and $\dim_{\mathbb{F}_l} J[l]_c^0 = 1$. If $l \equiv 2 \pmod{3}$, then $\dim_{\mathbb{F}_{l^2}} J[l]^0 = 2$ or 3 .*

3.3 A brief comment on the methods of the following sections

The method of the following sections is to consider the possible Jordan-Hölder decompositions of $J[l]^0$. The action of I_t on each of these quotients is given by a character ϕ as described in Theorem 2. As the determinant of $\tilde{\rho}_{l,6}$ on I_t is χ_l^3 , there must be three fundamental characters involved in the action of I_t on $J[l]^0$.

These conditions enable us to list a finite number of possible forms for the image of I_t . We then remark on the order of a cyclic subgroup of $\rho_l(I_t)$. As the homotheties are in $\rho_l(G_K)$, we use the results to discuss $\bar{\rho}_l(G_K)$ in later sections.

3.4 Supersingular reduction

We say that the reduction of J at l is supersingular when $J[l]^0 = J[l]$. While “supersingular” is sometimes used to refer only to a variety which is a product of supersingular elliptic curves, the more general sense of a variety where $J[l]^0 = J[l]$ is also used. This case only occurs for us when $l \equiv 2 \pmod{3}$.

In the supersingular case, the dimension of $J[l]^0$ over \mathbb{F}_l is 6. We consider $J[l]^0$ as an \mathbb{F}_{l^2} vector space of dimension 3. The Jordan-Hölder decomposition of $J[l]^0$ may contain quotients of dimension 1, 2 or 3 over \mathbb{F}_{l^2} . We discuss these separately.

3.4.1 Jordan-Hölder quotient of dimension 3

Suppose that $J[l]^0$ has only a single Jordan-Hölder quotient of dimension 3 over \mathbb{F}_{l^2} . By theorem 2, I_t acts on $J[l]^0$ as a character ϕ which is a non-trivial product of fundamental characters of level 6 and I_w acts trivially. The determinant of the action of I_t is χ_l^3 and hence we see that ϕ is the product of 3 fundamental characters of level 6 (since each character has norm χ_l). Thus $\phi = \phi_6^{1+l^{h_1}+l^{h_2}}$ for $1 < h_1 < h_2 < 6$ and for ϕ_6 some fundamental character of level 6.

The image of I_t under ρ_l is isomorphic to $(\mathbb{F}_{l^6}^*)^{1+l^{h_1}+l^{h_2}}$. We may assume that $1+l^{h_1}+l^{h_2}$ is one of $1+l+l^2$, $1+l+l^3$, $1+l+l^4$ or $1+l^2+l^4$. (If it is not, we may change which of the fundamental characters of level 6 we name ϕ_6 . The case $1+l^2+l^4$, where $\phi_6^{1+l^2+l^4}$ is a fundamental character of level 2, will be discussed in section 3.4.3.) The group $\phi_6(I_t) = (\mathbb{F}_{l^6}^*)^{1+l^{h_1}+l^{h_2}}$ is a cyclic group of order $\frac{l^6-1}{\gcd(l^6-1, 1+l^{h_1}+l^{h_2})}$, which is at least l^2-1 . By extending our field to \mathbb{F}_{l^6} , we may diagonalize this action. These diagonal matrices are given by $\phi_6^{1+l^{h_1}+l^{h_2}}$ and its conjugates $\phi_6^{l^2+l^{h_1}+2+l^{h_2}+2}$ and $\phi_6^{l^4+l^{h_1}+4+l^{h_2}+4}$. Thus the action of I_t is conjugate, after our extension to \mathbb{F}_{l^6} , to a group of the form

$$\left\{ \left(\begin{array}{ccc} \phi_6^{1+l^{h_1}+2+l^{h_2}+2}(g) & 0 & 0 \\ 0 & \phi_6^{l^2+l^{h_1}+2+l^{h_2}+2}(g) & 0 \\ 0 & 0 & \phi_6^{l^4+l^{h_1}+4+l^{h_2}+4}(g) \end{array} \right) : g \in I_t \right\}.$$

This group is cyclic of order at least l^2-1 .

The corresponding subgroup in $\mathrm{SU}_3(\mathbb{F}_{l^2})$ is given by

$$\left\{ \left(\begin{array}{ccc} \chi_l(g)^{-1} \phi_6^{1+l^{h_1}+2+l^{h_2}+2}(g) & 0 & 0 \\ 0 & \chi_l(g)^{-1} \phi_6^{l^2+l^{h_1}+2+l^{h_2}+2}(g) & 0 \\ 0 & 0 & \chi_l(g)^{-1} \phi_6^{l^4+l^{h_1}+4+l^{h_2}+4}(g) \end{array} \right) : g \in I_t \right\}.$$

which is obtained by multiplying by a homothety. This group projects to a subgroup of the same size in $\mathrm{PSU}_3(\mathbb{F}_{l^2})$.

3.4.2 Jordan-Hölder quotient of dimension 2

If $J[l]^0$ has a Jordan-Hölder quotient of dimension 2 over \mathbb{F}_{l^2} , I_t acts on this quotient as the product of fundamental characters of level 4. Recall that the

determinant of the action of the inertia group is given by χ_l^3 , the cube of the fundamental character of level 1. The determinant of the action on a Jordan-Hölder quotient of dimension 1 over \mathbb{F}_{l^2} can be at most χ_l^2 , therefore the inertia group does not act trivially on a quotient of dimension 2 over \mathbb{F}_{l^2} . Hence, I_t acts either as $\phi_4, \phi_4^{1+l}, \phi_4^{1+l+l^2}$ where ϕ_4 is some fundamental character of level 4. The image of ρ_l in this quotient is isomorphic to $\mathbb{F}_{l^4}^*$, $(\mathbb{F}_{l^4}^*)^{1+l}$ or $(\mathbb{F}_{l^4}^*)^{1+l+l^2}$. We note that these groups are non-central and cyclic of order at least $l-1$ so that $\bar{\rho}_l(G_K)$ will contain an element of order at least $l-1$.

3.4.3 Jordan-Hölder quotients of dimension 1

On a Jordan-Hölder quotient of dimension 1 over \mathbb{F}_{l^2} , the action of I_t is given by the product of zero, one or two of the two fundamental characters of level 2. Hence, I_t acts either as 1, ϕ_2 or ϕ_2^{1+l} where ϕ_2 is a fundamental character of level 2.

Suppose that the action of I_t is given by three fundamental characters of level 2. Each fundamental character of level 2 is the action of I_t on a supersingular elliptic curve. Therefore, write $J[l] = J[l]^0 = E_1 \oplus E_2 \oplus E_3$ where the E_j are supersingular elliptic curves over \mathbb{F}_l . The action of $\zeta_3 \in \text{End}(J)$ gives an action on $\text{Hom}_{\mathbb{F}_{l^2}}(J[l], J[l]) \cong \text{Hom}_{\mathbb{F}_l}(E_1 \oplus E_2 \oplus E_3, E_1 \oplus E_2 \oplus E_3)$. Recall from section 3.2 that the action of ζ_3 on $J[l^\infty]$ is given by $(1, 1, c)$, where c is complex conjugation. Hence, ζ_3 does not act identically on E_1, E_2 and E_3 and the three characters of level 2 are not all identical.

There are only two fundamental characters of level 2 so two of the three characters must be identical. Write the three characters as ϕ_2 , ϕ_2 and ϕ_2^l where ϕ_2 is the repeated fundamental character of level 2.

If $[J]^0$ has three quotients of dimension 1 over \mathbb{F}_{l^2} and I_t acts trivially on one quotient, then one of the characters must be the product of the two fundamental characters of level 2 as the determinant of the action is χ_l^3 . In this case, I_t acts as the characters ϕ_2^{1+l} , ϕ_2 and 1 where ϕ_2 is one of the fundamental characters of level 2.

Note that ϕ_2 is onto $\mathbb{F}_{l^2}^*$ and ϕ_2^{1+l} is onto \mathbb{F}_l^* . Thus each situation considered above gives rise to a non-central element of order $l - 1$.

3.4.4 Summary of the supersingular case

In summary, the action of I_t in the case that J is supersingular at l is conjugate over \mathbb{F}_{l^6} to one of the following groups.

$$\begin{aligned}
& \bullet \left\{ \left(\begin{array}{ccc} \phi_6^{1+l^{h_1+2+l^{h_2+2}}}(g) & 0 & 0 \\ 0 & \phi_6^{l^2+l^{h_1+2+l^{h_2+2}}}(g) & 0 \\ 0 & 0 & \phi_6^{l^4+l^{h_1+4+l^{h_2+4}}}(g) \end{array} \right) : g \in I_t \right\} \\
& \bullet \left\{ \left(\begin{array}{ccc} \phi_4(g)^{1+l} & 0 & * \\ 0 & \phi_4(g)^{l^2+l^3} & * \\ 0 & 0 & \phi_2(g) \end{array} \right) : g \in I_t \right\} \\
& \bullet \left\{ \left(\begin{array}{ccc} \phi_4(g) & 0 & * \\ 0 & \phi_4(g)^{l^2} & * \\ 0 & 0 & \phi_2(g)^{1+l} \end{array} \right) : g \in I_t \right\} \\
& \bullet \left\{ \left(\begin{array}{ccc} \phi_4^{1+l+l^2}(g) & 0 & * \\ 0 & \phi_4^{1+l^2+l^3}(g) & * \\ 0 & 0 & 1 \end{array} \right) : g \in I_t \right\} \\
& \bullet \left\{ \left(\begin{array}{ccc} \phi_2^{1+l}(g) & * & * \\ 0 & \phi_2(g) & * \\ 0 & 0 & 1 \end{array} \right) : g \in I_t \right\}
\end{aligned}$$

$$\bullet \left\{ \begin{pmatrix} \phi_2(g) & * & * \\ 0 & \phi_2(g) & * \\ 0 & 0 & \phi_2(g)^l \end{pmatrix} : g \in I_t \right\}$$

Two of these groups are also possible in the case of mixed reduction.

In each case above $\bar{\rho}_l(G_K)$ has an element of order at least $l - 1$.

3.5 Ordinary and mixed reduction

We now consider the cases where $\dim_{\mathbb{F}_l} J[l]^0 < 6$.

3.5.1 The case $l \equiv 1 \pmod{3}$

Suppose that $l \equiv 1 \pmod{3}$. Recall that I_w acts trivially on each Jordan-Hölder quotient of $J[l]^0$.

Recall that $J[l]_c^0$ has dimension 1 over \mathbb{F}_l . From Theorem 2, we conclude that I_t acts as 1 or as χ_l . However, the action of I_t on $J[l]_I^0$ has determinant at most χ_l^2 so that the action of I_t on $J[l]_c^0$ has determinant χ_l . Therefore, this action is given by χ_l . The image of this character is all of \mathbb{F}_l^* . Thus I_t acts on $J[l]_c^0$ by a cyclic group of order $l - 1$.

Recall that the dimension of $J[l]_I^0$ over \mathbb{F}_l is 2.

Suppose that $J[l]_I^0$ has a single Jordan-Hölder quotient of dimension 2 over \mathbb{F}_l . Then I_t acts on $J[l]_I^0$ as a non-trivial product of fundamental characters of level 2. Since the determinant of the action is χ_l^3 and the action on $J[l]_c^0$ is given by the single fundamental character of level 1, the action is the product of the two fundamental characters of level 2. Thus the action on $J[l]_I^0$ is by ϕ_2^{l+1} where ϕ_2 and ϕ_2^l are the two fundamental characters of level 2. However,

$\phi_2^{l+1} = \chi_l$. The image of I_t is conjugate to a group of the form

$$\left\{ \begin{pmatrix} \phi_2(g)^{l+1} = \chi_l(g) & 0 & * \\ 0 & \phi_2(g)^{l+1} = \chi_l(g) & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}.$$

Thus the image of G_K contains a subgroup which is cyclic of order $l - 1$.

If $J[l]_I^0$ has two Jordan-Hölder quotients of dimension 1, then I_t acts on each as the unique fundamental character of level 1. As the determinant of the action of I_t on $J[l]^0$ is χ_l^3 and the determinant of the action on $J[l]_c^0$ is at most χ_l , the action of I_t must be nontrivial on both quotients. The image of I_t is conjugate to a group of the form $\left\{ \begin{pmatrix} \chi_l(g) & * & * \\ 0 & \chi_l(g) & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}$. Thus the image of I_t is a non-central cyclic subgroup of order $l - 1$.

3.5.2 Mixed reduction at a prime $l \equiv 2 \pmod{3}$

We return to the case that $l \equiv 2 \pmod{3}$ and consider the case where $J[l]^0$ has dimension 2 over \mathbb{F}_{l^2} and thus dimension 4 over \mathbb{F}_l .

If $J[l]^0$ has a single Jordan-Hölder quotient of dimension 2 over \mathbb{F}_{l^2} , I_t acts as a non-trivial product of three fundamental characters of level 4. Hence, it acts as $\phi_4^{1+l+l^2}$ where ϕ_4 is a fundamental character of level 4. Thus the action of I_t is cyclic of order $\frac{l^4-1}{\gcd(l^4-1, 1+l+l^2)}$ which is at least $l - 1$.

If $J[l]^0$ has two Jordan-Hölder quotients of dimension 1 over \mathbb{F}_{l^2} , I_t acts on each quotient as a product of fundamental characters of level 2. This is similar to the situation discussed in the previous section. We conclude that I_t acts as the characters ϕ_2^{1+l} and ϕ_2 , where ϕ_2 is a fundamental character of

level 2. Hence the image of I_t is conjugate to a group of the form

$$\left\{ \begin{pmatrix} \phi_2(g)^{1+l} = \chi_l(g) & * & * \\ 0 & \phi_2(g) & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}.$$

For example this occurs in the case that $J(C) \cong E_{o,1} \times E_{o,2} \times E_{ss}$ where $E_{o,1}$ and $E_{o,2}$ are ordinary elliptic curves and E_{ss} is a supersingular elliptic curve.

Thus $\rho_l(G_K)$ and $\rho_{l,c}(G_K)$ always contain an element of order at least $l - 1$ which is not central.

3.6 Determinant

Recall from Lemma 8 that the map $\det \circ \tilde{\rho}_{l,6}$ is equal to χ_l^3 , where χ_l is the fundamental character of level 1, that is, the cyclotomic character. In the case that $l \equiv 2 \pmod{3}$, this implies that $\det \circ \tilde{\rho}_{l,6}$ is surjective.

When $l \equiv 1 \pmod{3}$, $\tilde{\rho}_{l,6}$ is given by the direct sum of $\tilde{\rho}_l$ and a twist of $\tilde{\rho}_l$ by χ_l . The determinant of $\tilde{\rho}_l$ cannot be directly determined from this relation. However, the action of I_t on $J[l]_I^0$ and $J[l]_c^0$ results in $\det \circ \rho_{l,c}(I_t) = \chi(I_t) = \mathbb{F}_l^*$.

4 Possibilities for the image

Recall that $\bar{\rho}_l$ is the projection of $\rho_l(G_K)$ to $\mathrm{PSL}_3(\mathbb{F}_l)$ for $l \equiv 1 \pmod{3}$ and to $\mathrm{PSU}_3(\mathbb{F}_{l^2})$ for $l \equiv 2 \pmod{3}$.

Suppose that for an infinite number of primes l , the map $\bar{\rho}_l$ is not surjec-

tive. That is, suppose that for an infinite number of primes $l \equiv 1 \pmod{3}$ we have $\bar{\rho}_l(G_K) \neq \mathrm{PSL}_3(\mathbb{F}_l)$ or for an infinite number of primes $l \equiv 2 \pmod{3}$ we have $\bar{\rho}_l(G_K) \neq \mathrm{PSU}_3(\mathbb{F}_{l^2})$. As the curve C has good reduction at all but finitely many places of K , this holds if and only if it holds for infinitely many primes l where C has good reduction.

At a place $l > 360$ where C has good reduction, the existence of an element of $\bar{\rho}_l(G_K)$ of order at least $l - 1$ shows that $\bar{\rho}_l(G_K)$ cannot be one of the subgroups enumerated as item 5 in Lemma 1 or item 4 in Lemma 2. This is a simple consideration of the size of the listed groups. We can improve the bound $l > 360$ by considering the maximal order of the elements of A_6 , $\mathrm{PSL}_2(\mathbb{F}_7)$ and the Hessian group.

Hence $\bar{\rho}_l(G_K)$ and $\bar{\rho}_{l,c}(G_K)$ must be one of the following types of subgroups for infinitely many primes.

1. A non-degenerate orthogonal group.
2. A subgroup of a Borel or Cartan subgroup.
3. A subgroup of the normalizer of a Cartan subgroup.
4. A subgroup of a proper parabolic group.

Since this list is finite, one item on the list must occur infinitely often if $\bar{\rho}_l(G_K)$ is not full almost everywhere.

We now show

Theorem 3. *The image of G_K under $\bar{\rho}_l$ is never contained in an orthogonal group. Furthermore, it is contained in a Borel or Cartan subgroup, in a normalizer of a Cartan subgroup or in a non-Borel proper parabolic subgroup for only finitely many l . Hence, $\bar{\rho}_l(G_K) = PSL_3(\mathbb{F}_l)$ for all but finitely many $l \equiv 1 \pmod{3}$ and $\bar{\rho}_l(G_K) = PSU(\mathbb{F}_{l^2})$ for all but finitely many $l \equiv 2 \pmod{3}$.*

4.1 The orthogonal group

Here we show that $\bar{\rho}_l(G_K)$ is never contained in an orthogonal group. We do this by showing that $\rho_l(G_K)$ and $\rho_{l,c}(G_K)$ are not contained in a group of orthogonal similitudes. That is, by showing that they do not preserve a quadratic form up to a character.

Suppose that a conjugate of $\tau(G_K) \subseteq GO_3(\mathbb{F}_q)$ contains matrices of the form $\left\{ \begin{pmatrix} \psi_1(g) & * & * \\ 0 & \psi_2(g) & * \\ 0 & 0 & \psi_3(g) \end{pmatrix} : g \in G_K \right\}$ where ψ_1, ψ_2 and ψ_3 are characters of G_K . Each of these matrices is independently diagonalizable so we consider the matrices $\begin{pmatrix} \psi_1(g) & 0 & 0 \\ 0 & \psi_2(g) & 0 \\ 0 & 0 & \psi_3(g) \end{pmatrix}$. These each preserve some quadratic form $\sum_{i,j=1}^3 a_{ij}x_i x_j$ with $a_{ij} \in \mathbb{F}_l$ and $\det(a_{ij}) \neq 0$ up to a character σ of G_K . Then $\psi_i(g)\psi_j(g)a_{ij}x_i x_j = \sigma(g)a_{ij}x_i x_j$. Hence, if $a_{ij} \neq 0$, $\psi_i(g)\psi_j(g) = \sigma(g)$. If this quadratic form is non-degenerate so that $\det(a_{ij}) \neq 0$, there are, for each g , three distinct pairs (i, j) where $a_{ij} \neq 0$, in which each of 1, 2 and 3 appear at least once but none of 1, 2 and 3 appear in every pair. Therefore the products $\psi_i(g)\psi_j(g)$ agree on these pairs.

We now show why this is not the case for any subgroup enumerated in

sections 3.4 and 3.5. We do this by considering the characters corresponding to the ψ_1 , ψ_2 and ψ_3 above and their pairwise products.

We first consider the case $l \equiv 1 \pmod{3}$.

Consider $J[l]_c^0$ which is of dimension 1 over \mathbb{F}_l . We know that I_l acts as a subgroup which is given by $\left\{ \begin{pmatrix} \chi_l(g) & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}$ where χ_l is the fundamental character of level 1. The possible products $\psi_i(g)\psi_j(g)$ are $\chi_l^2(g)$ for $(i, j) = (1, 1)$, $\chi_l(g)$ for $(i, j) = (1, 2), (1, 3), (2, 1)$ and $(3, 1)$ and 1 for $(i, j) = (2, 3), (3, 2), (2, 2)$ and $(3, 3)$. Since χ_l is onto \mathbb{F}_l^* there are g such that $\chi_l(g) \neq 1$. Hence no set of three pairs (i, j) exists as required and $\rho_{l,c}(I_t)$ is not contained in the general orthogonal group.

The space $J[l]_l^0$ has dimension 2 over \mathbb{F}_l . Recall that I_t acts as $\left\{ \begin{pmatrix} \chi_l(g) & * & * \\ 0 & \chi_l(g) & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}$ where χ_l is the fundamental character of level 1 on $J[l]_l^0$. The pairwise products of characters here are $\chi_l(g)^2$ for $(i, j) = (1, 2), (2, 1), (1, 1)$ and $(2, 2)$, $\chi_l(g)$ for $(i, j) = (1, 3), (3, 1), (2, 3)$ and $(3, 2)$ and 1 for $(i, j) = (3, 3)$. As χ_l is the cyclotomic character, it is clear that there are g such that all of $\chi_l(g)^2$, $\chi_l(g)$ and 1 are distinct. This shows that $\rho_l(G_K) \not\subseteq \text{GO}_3(\mathbb{F}_l)$

In the case where $l \equiv 2 \pmod{3}$, there are more possibilities.

We first consider the case of one Jordan-Hölder quotient of dimension 3 over \mathbb{F}_{l^2} . Here I_t acts as $\phi_6^{1+l^{h_1}+l^{h_2}}$, where ϕ_6 is a fundamental character of level 6. The tame inertia I_t acts as a group which is conjugate over \mathbb{F}_{l^6} to a diagonal group described by characters $\phi_6^{1+l^{h_1}+l^{h_2}}$, $\phi_6^{l^2+l^{h_1}+2+l^{h_2}+2}$ and $\phi_6^{l^4+l^{h_1}+4+l^{h_2}+4}$. These characters are distinct since, as discussed in section 3.4, the action of I_t is not given by three identical fundamental characters of

level 2. An examination of the possibilities for h_1, h_2 and (i, j) shows that the pairwise products of these characters are distinct powers of ϕ_6 for $l \geq 3$ (except that $\psi_i\psi_j = \psi_j\psi_i$) and hence are distinct characters. Thus no set of pairs (i, j) exists as required.

For example, when $1 + l^{h_1} + l^{h_2} = 1 + l + l^2$, the pairwise products are the $2 + 2l + 2l^2, 1 + l + 2l^2 + l^3 + l^4, 2l^2 + 2l^3 + 2l^4, 2 + l + l^2 + l^4 + l^5, 1 + l^2 + l^3 + 2l^4 + l^5$ and $2 + 2l^4 + 2l^5$ powers of ϕ_6 . (Recall that $\phi_6^{l^6} = \phi_6$ so that these exponents are considered modulo the relation $l^6 \equiv 1$.) Since ϕ_6 is onto $\mathbb{F}_{l^6}^*$, these characters are distinct and there are g such that all of these pairwise products are distinct. Thus $\rho_l(I_t)$ is not contained in the group of orthogonal similitudes.

Similarly, in the case of Jordan-Hölder quotients of dimension 2 and 1 over \mathbb{F}_{l^2} the image of I_t is conjugate over \mathbb{F}_{l^6} to one of

1. $\left\{ \begin{pmatrix} \phi_4(g)^{1+l+i^2} & 0 & * \\ 0 & \phi_4(g)^{l^2+i^3+1} & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}$
2. $\left\{ \begin{pmatrix} \phi_2(g)^{1+l} & * & * \\ 0 & \phi_2(g) & * \\ 0 & 0 & 1 \end{pmatrix} : g \in I_t \right\}$
3. $\left\{ \begin{pmatrix} \phi_4(g)^{1+l} & 0 & * \\ 0 & \phi_4(g)^{l^2+i^3} & * \\ 0 & 0 & \phi_2(g) \end{pmatrix} : g \in I_t \right\}$
4. $\left\{ \begin{pmatrix} \phi_4(g) & 0 & * \\ 0 & \phi_4(g)^{l^2} & * \\ 0 & 0 & \phi_2(g)^{1+l} \end{pmatrix} : g \in I_t \right\}$
5. $\left\{ \begin{pmatrix} \phi_2(g) & * & * \\ 0 & \phi_2(g) & * \\ 0 & 0 & \phi_2(g)^l \end{pmatrix} : g \in I_t \right\}$

where ϕ_4 is a fundamental character of level 4 and ϕ_2 is a fundamental character of level 2. In none of these cases are there three equal pairwise products

of the type required. For example, in case 3, the pairwise products are ϕ_4^{2+2l} , $\phi_4^{1+l+l^2+l^3}$, $\phi_4^{2l^2+2l^3}$, $\phi_4^{1+l}\phi_2$, $\phi_4^{l^2+l^3}\phi_2$ and ϕ_2^2 . Note that $\phi_4^{1+l^2}$ is a fundamental character of level 2, that is, $\phi_4^{1+l^2}$ is either ϕ_2 or ϕ_2^l . We see that these characters are distinct powers of ϕ_4 . Hence, there are $g \in G_K$ where they are all distinct.

Thus, in none of the types of good reduction can the image of ρ_l be contained in the general orthogonal group.

4.2 The Borel and Cartan groups

Here we show that the image of ρ_l is contained in a Borel or Cartan subgroup only finitely often. This directly implies that the same condition holds for $\bar{\rho}_l$.

We first remark on the case that $\rho_l(G_K)$ is contained in the normalizer N_l of a Cartan subgroup C_l but not in the Cartan subgroup itself. Let F be the finite extension of K associated to the representation

$$\phi_l : \text{Gal}(\bar{K}/K) \rightarrow \rho_l(\text{Gal}(\bar{K}/K)) \rightarrow N_l/C_l.$$

Then $\rho_l(\text{Gal}(\bar{F}/F))$ is contained in C_l . Let E be the intermediate extension of K in F such that $[F : E] \mid 2$ and $[E : K] \mid 3$. The size of N_l/C_l is known to be either 3 or 6, thus this extension exists.

As ρ_l is ramified only at l and primes of bad reduction, F/K is also unramified outside Δl . To see the the extension E/K is unramified at l , we

consider the possible images of I_l . The order of N_l is prime to l ; hence, the order of $\rho_l(I_l)$ is not divisible by l . An examination of the possible images reveals that each possibility with order prime to l is contained in a Cartan group C' . That is, $\rho_l(I_l) \subseteq C'$ for some Cartan group C' contained in N_l .

We consider the case that $F = E$, i.e. the case that the image of ϕ_l in N_l/C_l has order 3. Then C' is of index 3 in a subgroup $N' = \rho_l(\text{Gal}(\overline{K}/K))$ of N_l . Each element in $N' - C_l$ has order three. The Cartan group C' is generated by elements of order either $l - 1$ or $l^2 - 1$ in SL_3 . Therefore all the generators of C' are contained in C_l so that $C' = C_l$. This reasoning applies to the image of $\rho_l(\text{Gal}(\overline{E}/E))$ in the case that $[F : E] = 2$. Hence E/K is unramified at l in both cases.

There are only finitely many extensions of K of bounded degree which are unramified outside Δ . Therefore, we may take E to be a fixed extension independent of l .

If $F = E$, then $\rho_l(\text{Gal}(\overline{E}/E))$ is contained in a Cartan subgroup. If $[F : E] = 2$, then $\rho_l(\text{Gal}(\overline{E}/E))$ is reducible. In the proofs below it will be evident that the choice of local ground field does not affect the result. Thus the case of a subgroup of the normalizer of a Cartan subgroup may be considered as either the case of a Cartan subgroup or of a proper parabolic subgroup over this finite extension E of K . The latter case is addressed in section 4.3.

Let $G_F = \text{Gal}(\overline{F}/F)$ where $F = K$ or a finite extension of K as above. Let $q = l$ if $l \equiv 1 \pmod{3}$ and l^2 if $l \equiv 2 \pmod{3}$. Let k_l be the algebraic

closure of \mathbb{F}_q . Let Γ be the set of embeddings of F into $\overline{\mathbb{Q}}$.

Suppose that there is an infinite set Σ of primes l with $\rho_l(G_F)$ contained in a Borel or Cartan subgroup of $\mathrm{GL}_3(\mathbb{F}_q)$. We may of course assume that C has good reduction at all $l \in \Sigma$, since there are only finitely many places where C has bad reduction.

For each such l , let $\rho_l^{ss} : G_F \rightarrow \mathrm{GL}_3(\mathbb{F}_q)$ be the semi-simplification of ρ_l . The representation ρ_l^{ss} is abelian. There are characters

$$\theta_l^{(i)} : \mathrm{Gal}(F^{ab}/F) \rightarrow k_l^*$$

for $i = 1, 2, 3$ such that $\rho_l^{ss} \cong \theta_l^{(1)} \oplus \theta_l^{(2)} \oplus \theta_l^{(3)}$ over some extension of F .

Let \mathfrak{m} be a modulus of support (see section 1.2) for the set S of places where the curve C has bad reduction. Then ρ_l is unramified outside $S_l = S \cup \{v|l\}$, where $\{v|l\}$ is the set of places in F above l . As the $\theta_l^{(i)}$ are unramified at $v \in \Gamma - S_l$, we can, by class field theory ([17]), write

$$\theta_l^{(i)}(a) = \theta_l^{(i)}(\tau) = \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{n(\sigma, l, i)} \pmod{l}$$

as in equation (2) in section 1.2. Here the σ_l are the maps defined in section 1.2 for $a \in U_{\mathfrak{m}}$, τ is the Artin symbol of a and $i = 1, 2, 3$ ([16]).

To apply Theorem 1, we must show that the absolute values of the $n(\sigma, l, i)$ are bounded.

Since we know the action of the inertia group, we see that the $\theta_l^{(i)}$ re-

stricted to I_t are products of no more than 3 fundamental characters of level no more than 6. The modular characters defined by $\sigma_l(a_l^{-1})$ are known by class field theory to be the fundamental characters of level $[F_v : \mathbb{Q}_l]$, where F_v is the completion of F at a place v over l ([17]).

For a fundamental character of level h , we consider the embeddings $\tau^1 \dots \tau^h$ of \mathbb{F}_{l^h} into k_l . Then a fundamental character ϕ_h of level h is given by $\phi_h = \prod_{\sigma \in \Gamma} \sigma_l(a_l^{-1})^{m_{\phi_h}(\sigma, l, i)}$ where $m_{\phi_h}(\sigma, l, i) = 1$ if σ_l extends τ^i and 0 otherwise ([17]). When the action of I_t is given by the product of fundamental characters $\phi_{h,j}$ of level h , $n(\sigma, l, i)$ is the sum of the h values $m_{\phi_{h,j}}(\sigma, l, i)$.

We therefore see that the absolute values of the $n(\sigma, l, i)$ are bounded.

Recall that $\tilde{\rho}_l$ is the map $\tilde{\rho}_l : G_K \rightarrow \mathrm{GL}_3(\mathbb{Z}_l)$ for $l \equiv 1 \pmod{3}$ and $\tilde{\rho}_l : G_K \rightarrow \mathrm{GU}_3(O_L)$ for $l \equiv 2 \pmod{3}$.

Theorem 1, applied to the system $(\tilde{\rho}_l^{ss})$, shows that $\tilde{\rho}_l^{ss}$ is abelian at all places. Hence $\tilde{\rho}_l$ is contained in a Borel subgroup at all places l . As $\mathrm{End}(J)$ is the commutant of $\tilde{\rho}_l(G_K)$ ([7]) and the commutant of a Borel group is larger than $\mathbb{Z}[\zeta_3]$, this implies that the curve has $\mathrm{End}(J)$ larger than $\mathbb{Z}[\zeta_3]$. Thus for those curves with $\mathrm{End}(J) = \mathbb{Z}[\zeta_3]$, only finitely many l can have $\rho_l(G_K)$ contained in a Borel or Cartan subgroup.

4.3 The parabolic case

We now show that the image of ρ_l is contained in a proper parabolic subgroup for at most finitely many $l \equiv 1 \pmod{3}$. Consequently, $\bar{\rho}_l(G_K)$ is contained in a proper parabolic subgroup of $\mathrm{PSL}_3(\mathbb{F}_l)$ only finitely often. We need not

consider the case $l \equiv 2 \pmod{3}$ as there is no proper parabolic subgroup of $\mathrm{PSU}_3(\mathbb{F}_{l^2})$ which is not a Borel subgroup.

This section follows the methods of Dieulefait ([5]). Of course, it may also be regarded as an alternative proof that $\rho_l(G_K)$ is not contained in a Borel subgroup for infinitely many $l \equiv 1 \pmod{3}$.

Suppose that $\rho_l(G_K)$ is contained in a proper parabolic subgroup of GL_3 for some $l \equiv 1 \pmod{3}$, that is, the $\rho_l(G_K)$ fix a two dimensional subspace or quotient.

The semi-simplification ρ_l^{ss} of ρ_l is of the form

$$\rho_l^{ss} \cong \rho_{l,2} \oplus \mu_l$$

where μ is a character and $\rho_{l,2}$ is a two dimensional representation. Recall that ρ_l is a representation into $\mathrm{GL}_3(\mathbb{F}_l)$ so that this decomposition is defined over \mathbb{F}_l . By our knowledge of the action of I_l , we may write $\mu_l = \epsilon_l \chi_l^i$, where $i = 0$ or 1 and ϵ_l is unramified at l .

The system (ρ_l) is strictly compatible in the sense of Serre and so has a conductor \mathfrak{c} such that ρ_l is trivial on the Artin symbols of $U_{v,\mathfrak{c}}$ away from l . The $U_{v,\mathfrak{c}}$ are defined in section 1.2. The conductor \mathfrak{m} of ϵ_l has support contained in the support of \mathfrak{c} and $\mathfrak{m}_v \leq \mathfrak{c}_v$ for all v in the support of \mathfrak{c} .

Let p be a rational prime such that $p \equiv 1 \pmod{\mathfrak{c}}$. Then $\epsilon(\mathrm{Fr}_p) = 1$. Hence $\chi^i(\mathrm{Fr}_p)$ is a root of the characteristic polynomial $P_p(x)$ of the Frobenius at p . As the roots of $P_p(x)$ are pairs with product p , we may assume that 1

is a root of $P_p(x)$. We write

$$P_p(x) = x^6 + a_{5,p}x^5 + a_{4,p}x^4 + a_{3,p}x^3 + pa_{4,p}x^2 + p^2a_{5,p}x + p^3,$$

as it is known that $P_p(x)$ is of this form. We substitute in $\mu(\text{Fr}_p)$ to get

$$1 + (p^2 + 1)a_{5,p} + (p + 1)a_{4,p} + a_{3,p} + p^3 \equiv 0 \pmod{l}.$$

The complex roots of $P_p(x)$ are known to be of size \sqrt{p} which allows us to bound $a_{5,p}$ by $6\sqrt{p}$, $a_{4,p}$ by $15p$ and so forth.

For sufficiently large p , $1 + (p^2 + 1)a_{5,p} + (p + 1)a_{4,p} + a_{3,p} + p^3 \neq 0$ and hence is congruent to zero for only finitely many l .

This implies that the image of ρ_l^{ss} can be written as $\rho_{l,2} \oplus \mu$ for only finitely many l . Thus $\rho_l(G)$ cannot be contained in a proper parabolic subgroup for more than finitely many l .

5 Conclusion

For $l \equiv 1 \pmod{3}$, we have shown that $\bar{\rho}_l(G_K)$ has image in a proper subgroup of $\text{PSL}_3(\mathbb{F}_l)$ only finitely often. Therefore $\bar{\rho}_l(G_K)$ is all of $\text{PSL}_3(\mathbb{F}_l)$ for all but finitely many l . By Proposition 1 we therefore conclude that $\text{SL}_3(\mathbb{Z}_l) \subseteq \tilde{\rho}_l(G_K)$ for those l where $\bar{\rho}_l(G_K) = \text{PSL}_3(\mathbb{F}_l)$. The discussion of the determinant in section 3.6, then implies that $\det \circ \tilde{\rho}_l(G_K)$ is onto \mathbb{Z}_l^* for those l .

For $l \equiv 2 \pmod{3}$, we have shown that $\bar{\rho}_l(G_K)$ has image in a proper subgroup of $\mathrm{PSU}_3(\mathbb{F}_{l^2})$ only finitely often. Proposition 1 then implies that $\mathrm{SU}_3(O_L) \subseteq \tilde{\rho}_l(G_K)$ for those l where $\bar{\rho}_l(G_K) = \mathrm{PSU}_3(\mathbb{F}_{l^2})$. From section 3.6 we recall that $\det \circ \tilde{\rho}_l(G_K)$ is onto.

Theorem 4. *Let C be a Picard curve with $\mathrm{End}(J(C)) = \mathbb{Z}[\zeta_3]$. Let $\tilde{\rho}_l$ be the representation defined by the action of the Galois group on the Jacobian of C as in section 2.2. Then, for almost all $l \equiv 1 \pmod{3}$,*

$$\tilde{\rho}_l(\mathrm{Gal}(\bar{K}/K)) \cong \mathrm{GL}_3(\mathbb{Z}_l)$$

and for almost all $l \equiv 2 \pmod{3}$,

$$\tilde{\rho}_l(\mathrm{Gal}(\bar{K}/K)) \cong \mathrm{GU}_3(O_L),$$

where O_L is the ring of integers of the unramified quadratic extension L of \mathbb{Q}_l .

6 Examples

6.1 Examples at primes which split in K

To show that $\rho_l(G_K) = \mathrm{GL}_3(\mathbb{F}_l)$ in the $l \equiv 1 \pmod{3}$ case, it is enough to show that the image is irreducible and not contained in any of the subgroups listed in Lemma 1 as item 5. The former can be done by showing that there

are primes p_1 , p_2 and p_3 such that the characteristic polynomial $P_{p_1}(x)$ of $\tilde{\rho}_l(\text{Fr}_{p_1})$ splits linearly over \mathbb{F}_l , $P_{p_2}(x)$ is an irreducible cubic over \mathbb{F}_l and $P_{p_3}(x)$ splits into an irreducible quadratic and a linear factor over \mathbb{F}_l . To do this, we calculate the characteristic polynomials of the images of Frobenius elements.

For the calculations, it was necessary to calculate the number of points on the curve above the fields of p , p^2 and p^3 elements. Letting $-n_k = \#C(\mathbb{F}_{p^k}) - p^k - 1$, we have the L function

$$P_p(p^{-s}) = L_p(s) = 1 - n_1 p^{-s} + \frac{1}{2}(n_1^2 - n_2)p^{-2s} - \frac{1}{6}(n_1^3 - 3n_2 n_1 + 2n_3)p^{-3s} \\ + \frac{p}{2}(n_1^2 - n_2)p^{-4s} - p^2 n_1 p^{-5s} + p^3 p^{-6s}$$

and the zeta function $Z_p(x) = \frac{L_p(x)}{(1-x)(1-px)}$. By choosing only primes $l \equiv 1 \pmod{3}$ which split in K , we restrict to polynomials which factor into two cubic polynomials of the same splitting type. As only the factoring type is relevant, it is unnecessary to consider which terms make up $\rho_l(\text{Fr}_p)$ and which make up $\rho_{l,c}(\text{Fr}_p)$.

6.1.1 A first example

Let C be the curve

$$y^3 = x^4 + 3x^2 + 2x + 1$$

over $\mathbb{Q}(\zeta_3)$. We show that $\rho_7(G_K) \cong \text{GL}_3(\mathbb{F}_7)$ and hence $\tilde{\rho}_7(G_K) \cong \text{GL}_3(\mathbb{Z}_7)$.

Note that $l^3 - 1 = 342$ is divisible by 19 so that there is potentially a

Frobenius element of order divisible by 19 which cannot be contained in the groups of order 36, 72, 168, 216 or 360 listed in Lemma 1 as item 5.

The points on this curve can be counted by computer without too much difficulty. Maple was used to calculate the values of y^3 and of $x^4 + 3x^2 + 2x + 1$ in several finite fields to count the number of points on this curve. There are more efficient algorithms for this calculation such as those discussed by Bauer, Teske and Weng ([1]), but for curves with small coefficients and at small primes they are not necessary.

Table 1: Point counting for the curve $y^3 = x^4 + 3x^2 + 2x + 1$

	$p = 13$	$p = 19$	$p = 37$
$\#C(\mathbb{F}_p)$	14	31	31
$\#C(\mathbb{F}_{p^2})$	170	397	7308
$\#C(\mathbb{F}_{p^3})$	1999	6880	51303

For example, over \mathbb{F}_{13} there are exactly 13 finite points plus the point at infinity. Similarly, there are 13^2 finite points over \mathbb{F}_{13^2} . Over \mathbb{F}_{13^3} there are $1998 = 13^3 - 210$. Thus, $P_{13}(x) = x^6 + 70x^3 + 2197$ which splits linearly in \mathbb{F}_7 .

Over $p = 19$, $P_{19}(x) = x^6 + 11x^5 + 78x^4 + 421x^3 + 1482x^2 + 3971x + 6859$ factors as $(x^3 + 3x^2 + 6x + 2)(x^3 + x^2 + 6x + 3)$ giving the irreducible cubic component.

Note that x generates the multiplicative group of $\mathbb{F}_7[x]/(x^3 + x^2 + 6x + 3)$, and thus Fr_{19} is of order $7^3 - 1 = 19 * 3^2 * 2$. This eliminates the small groups from Lemma 1 item 5.

Over $p = 37$, $P_{37}(x) = x^6 - 7x^5 - 6x^4 + 373x^3 - 222x^2 - 9583x + 50653 =$

$$(x + 5)(x + 6)(x^2 + 5x + 2)^2.$$

Thus ρ_7 is onto $\mathrm{GL}_3(\mathbb{F}_7)$.

6.1.2 A second example

Let C be the curve

$$y^3 = x^4 + x + 1$$

over $\mathbb{Q}(\zeta_3)$. Then we show that $\rho_{67}(G_K) \cong \mathrm{GL}_3(\mathbb{F}_{67})$ and hence $\tilde{\rho}_{67}(G_K) \cong \mathrm{GL}_3(\mathbb{Z}_{67})$.

Table 2: Point counting for the curve $y^3 = x^4 + x + 1$

	$p = 13$	$p = 19$	$p = 31$
$\#C(\mathbb{F}_p)$	13	20	34
$\#C(\mathbb{F}_{p^2})$	157	386	982
$\#C(\mathbb{F}_{p^3})$	2380	7196	30666

Over 13, the polynomial is $P_{13}(x) = x^6 - x^5 - 6x^4 + 67x^3 - 78x^2 - 169x + 2197 = (x + 47)(x + 63)(x^2 + 49x + 9)(x^2 + 41x + 56) \pmod{67}$, giving a Frobenius element whose characteristic polynomial is an irreducible quadratic times a linear factor.

Over 19, we have $P_{19}(x) = x^6 + 12x^4 + 112x^3 + 228x^2 + 6859 = (x^3 + 59x^2 + 66x + 6)(x^3 + 8x^2 + 10x + 60) \pmod{67}$ which is the product of irreducible cubics. The order of Fr_{19} divides $67^3 - 1 = 2 * 3^2 * 7^2 * 11 * 31$ so it is necessary to check that the order of this element does not divide 18. In fact, the order is $42966 = 2 * 3^2 * 7 * 11 * 31$.

Over 31, the characteristic polynomial of Fr_{31} splits completely with

$$P_{31}(x) = x^6 + 2x^5 + 12x^4 + 313x^3 + 372x^2 + 1922x + 29791 = (x + 21)(x + 27)(x + 24)(x + 1)(x + 32)(x + 31) \pmod{67}.$$

Thus ρ_{67} is onto $\mathrm{GL}_3(\mathbb{F}_{67})$

6.2 An inert prime

When $l \equiv 2 \pmod{3}$, the characteristic polynomial of $\tilde{\rho}_{l,6}(\mathrm{Fr}_p)$ in $\mathrm{GL}_6(\mathbb{Q}_l)$ remains as in the $l \equiv 1 \pmod{3}$ case, however $n_1 = 0$ and $n_3 = 0$ as l is inert in $\mathbb{Q}(\zeta_3)$. We therefore consider the polynomial

$$\tilde{P}_p(x) = x^3 + \frac{1}{2}n_2x^2 + \frac{p}{2}n_2x + p^3$$

where $x = \mathrm{Norm}_{L/\mathbb{Q}(\zeta_3)}(z)$ and $\tilde{P}_p(z)$ is the characteristic polynomial of $\tilde{\rho}_l(\mathrm{Fr}_p)$ in $\mathrm{GU}(O_L)$.

As $\mathrm{PSU}_3(\mathbb{F}_{l^2})$ has no proper non-Borel parabolic subgroup, it now suffices to find primes p_1 and p_2 such that $\tilde{P}_{p_1}(x)$ splits completely and $\tilde{P}_{p_2}(x)$ does not.

We now consider the curve

$$y^3 = x^4 + x + 1$$

over $\mathbb{Q}(\zeta_3)$ and show that $\rho_5(G_K) = \mathrm{GU}_3(\mathbb{F}_{25})$ and hence $\tilde{\rho}_5(G_K) = \mathrm{GU}(O_L)$.

There are 134 points on the curve over \mathbb{F}_{11^2} so $\tilde{P}_{11}(x) = x^3 + 6x^2 + 66x + 1331 \equiv (x + 1)(x + 1)(x + 3) \pmod{5}$.

We have $\#C(\mathbb{F}_{17^2}) = 368$ so $\tilde{P}_{17}(x) = x^3 + 39x^2 + 663x + 4913 \equiv (x^2 + 2x + 4)(x + 2) \pmod{5}$.

Hence we have that $\tilde{\rho}_5(G_K) = \text{GU}(O_L)$.

More examples may be obtained by the same method.

References

- [1] Mark Bauer, Edlyn Teske, and Annegret Weng. Point counting on Picard curves in large characteristic. *Math. Comp.*, 74(252):1983–2005 (electronic), 2005.
- [2] Fedor Aleksevich Bogomolov. Sur l’algébricité des représentations l -adiques. *C. R. Acad. Sci. Paris Sér. A-B*, 290(15):A701–A703, 1980.
- [3] Wên Chên Chi. On the l -adic representations attached to simple abelian varieties of type IV. *Bull. Austral. Math. Soc.*, 44(1):71–78, 1991.
- [4] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. B.G. Teubner, Leipzig, 1901. Available online at Cornell library.
- [5] Luis V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\text{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

- [6] Jorge Estrada-Sarlabous, Ernesto Reinaldo-Barreiro, Jean-Pierre Cherdieu, and Rolf-Peter Holzapfel. The emergence of Picard Jacobians in cryptography. In *Fourth Italian-Latin American Conference on Applied and Industrial Mathematics (Havana, 2001)*, pages 266–275. Inst. Cybern. Math. Phys., Havana, 2001.
- [7] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.
- [8] Larry C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.
- [9] Rolf-Peter Holzapfel. *The ball and some Hilbert problems*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1995. Appendix I by J. Estrada Sarlabous.
- [10] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.
- [11] Serge Lang. *Algebra*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.
- [12] Howard H. Mitchell. Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.*, 12(2):207–242, 1911.
- [13] Emile Picard. Sur des fonctions de deux variables indépendantes analogues aux fonctions modulaires. *Acta Math.*, 2(1):114–135, 1883.

- [14] Michel Raynaud. Schémas en groupes de type (p, \dots, p) . *Bull. Soc. Math. France*, 102:241–280, 1974.
- [15] Jean-Pierre Serre. Lettre à Marie-France Vignéras du 10/2/1986.
- [16] Jean-Pierre Serre. *Abelian l -adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.
- [17] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [18] Jean-Pierre Serre. Représentations l -adiques. In *Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976)*, pages 177–193. Japan Soc. Promotion Sci., Tokyo, 1977.
- [19] Yutaka Taniyama. L -functions of number fields and zeta functions of abelian varieties. *J. Math. Soc. Japan*, 9:330–366, 1957.
- [20] J. T. Tate. p -divisible groups.
- [21] Oswald Veblen and John Wesley Young. *Projective geometry. Vol. 1*. The Atheneum Press Ginn and Co. Boston, 1910.