Abelian varieties — Galois representations and properties of ordinary reduction

Rutger Noot

Introduction

In this paper we will look at abelian varieties over number fields. We will be interested in particular in the number of places where such an abelian variety has ordinary reduction. Recall that if k is a field of characteristic p and if X/k is an abelian variety, then X is said to be ordinary if $X[p](\bar{k}) \cong (\mathbf{Z}/p)^g$, where $g = \dim X$.

If X is an abelian variety over any field k, then, for each prime number $\ell \neq p = \mathrm{char}(k)$, the Galois group $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ acts on the Tate module $T_\ell X$. For our purposes, the case where the field k is finite will be of particular importance. It is well known that in this case the characteristic polynomial of the Frobenius element $\mathrm{Fr} \in \mathrm{Gal}(\bar{k}/k)$ acting on $T_\ell X$ has coefficients in $\mathbf{Z}$ and is independent of ℓ. This means that for each $\ell \neq p$, the eigenvalues of Fr on $T_\ell X$ are the same algebraic integers. The variety X is ordinary if and only if for some, or equivalently for any, valuation on $\bar{\mathbf{Q}}$ extending the p-adic valuation on $\mathbf{Q}$, precisely half these eigenvalues have valuation 0.

Suppose that F is a number field and that X/F is an abelian variety. At every finite place v of F, the residue field F_v is a finite field. For all but finitely many of these places, the reduction X_v/F_v of X is an abelian variety. One can ask for how many valuations v this reduction is ordinary. From what we have seen above, it follows that the question whether X_v is ordinary can be answered by looking at the eigenvalues of a Frobenius element $\mathrm{Fr}_v \in \mathrm{Gal}(\bar{F}/F)$ at v acting on $T_\ell X \cong T_\ell X_v$, for any ℓ with $v(\ell) = 0$. Note that the fact that X has good reduction at v implies that the image in $\mathrm{End}(T_\ell X)$ of such a Frobenius element is determined up to conjugation, and hence that the eigenvalues of this image are well defined.

The only thing which seems to be known about this question in the general case can be found in [Og, 2.7]. The result is that, after replacing F by a finite extension, there is a set P of places, of Dirichlet density 1, such that for each $v \in P$, at least two eigenvalues of Fr_v on $T_\ell X$ are v-adic units. It follows that if the dimension of X is 1 or 2, then there is a finite extension of the base field F such that the set of places where X has ordinary reduction has density 1. The existence of such an extension is also known for all abelian varieties of CM-type.

In the second section of this paper we will prove a similar result for abelian varieties X with the property that the image of the ℓ-adic Galois representation associated to X is of a very particular form. To be precise, we will assume that the Lie algebra of the image of $\mathrm{Gal}(\bar{F}/F)$ in $\mathrm{End}(T_\ell X)$ is geometrically isomorphic to $\mathfrak{sp}(2)^{2k+1} \times \mathbf{G}_a$. The exact statement is given in Theorem 2.2. The proof of this theorem uses one of the main results of [Se1], namely the fact that, after replacing F by a finite extension, the image of Fr_v in $\mathrm{End}(T_\ell X)$ generates a maximal torus of the image of the Galois representation, for all v in a set of places with Dirichlet density 1. It will be shown that the fact that the Frobenius element at v generates a maximal torus of this image is, in sufficiently many cases, sufficient to ensure that X_v is ordinary. This proof occupies almost all of Section 2.

In the first section it will be shown that there actually exist abelian varieties satisfying our assumption. The proof of this fact rests on the observation, recorded in Theorem 1.7, that every group that occurs as a Mumford–Tate group of an abelian variety over $\mathbf{C}$ also occurs as the image of the Galois representation associated to an abelian variety over a number field. This fact, which is also of independent interest, is alluded to by Serre in [Se1].

Acknowledgements. I should like to express my gratitude to Prof. F. Oort for his support during the time I have been working on my thesis under his direction. The present article is based on a part of this thesis. I thank Bas Edixhoven for remarking that Theorem 2.2, which I had originally only proved in a particular case, is true in the generality in which it is stated here. Finally, I should like to thank the referee for pointing out an inaccuracy in an earlier version of this paper.

1 The image of the Galois representation

1.1 The aim of this section is to prove Theorem 1.7, which states that every group that occurs as the Mumford–Tate group of an abelian variety also occurs as the image of the Galois representation associated to an abelian variety. To do so, we have to treat some results about specialization in a family of Galois representations which are needed in this proof. We will show in Proposition 1.3 that if we have a family of abelian varieties over a number field, then we can specialize in such a way that the image of the Galois representation at the special point is equal to that at the generic point. This result will be applied to a family of abelian varieties for which the image of the Galois representation at the generic point is the group we want. This family will be the universal family over a Shimura variety, the fundamental group of which is easy to compute.

1.2 Let F be a field of finite type over $\mathbf{Q}$ and let S be a normal, absolutely irreducible variety over F. We write $K = F(S)$ for the function field of S and $\eta : \mathrm{Spec}(K) \to S$ for the inclusion of the generic point. For every point σ of S we will write $F(\sigma)$ for the residue field at σ. We write $\bar{S}$ for the normalization of S in $\mathrm{Spec}(\bar{K})$, and we choose closed points $\sigma \in S$ and $\bar{\sigma} \in \bar{S}$ such that $\bar{\sigma}$ maps down to σ. If we let $\bar{F}$ be the algebraic closure of F in $\bar{K}$, we have an identification $F(\bar{\sigma}) = \bar{F}$.

Let X/S be an abelian scheme. We intend to show that we can find a closed point σ of S such that the image of the Galois representation associated to $X_\sigma/F(\sigma)$ is the same as the image of the Galois representation of X_η/K. Because F has characteristic 0, the

n-torsion scheme $X[n]$ is a finite étale S-scheme for each integer n. Because $X[n]$ is a finite cover of S, every point of $X_\eta[n](\bar{K})$ extends uniquely to a point of $X[n](\bar{S})$. This gives rise to a bijection $X_\eta[n](\bar{K}) \to X[n](\bar{S})$. The choice of the point $\bar{\sigma}$ gives a map $X[n](\bar{S}) \to X_\sigma[n](\bar{F})$ and since $X[n]$ is étale over S this map is a bijection. Composing these two maps we get an isomorphism of groups

$$s_n : X_\eta[n](\bar{K}) \xrightarrow{\cong} X_\sigma[n](\bar{F}).$$

Clearly, the maps s_n are compatible for varying n.

We denote the decomposition group of $\bar{\sigma}$ by $D_{\bar{\sigma}} \subset \mathrm{Gal}(\bar{K}/K)$. We have maps

$$\mathrm{Gal}(\bar{K}/K) \supset D_{\bar{\sigma}} \twoheadrightarrow \mathrm{Gal}(\bar{F}/F(\sigma)).$$

For each n, the map s_n is compatible with the action of $D_{\bar{\sigma}}$ induced by the above maps.

If ℓ is a prime number and if we take the projective limit of the maps s_{ℓ^n}, we get a $D_{\bar{\sigma}}$-equivariant isomorphism $s : T_\ell X_\eta \longrightarrow T_\ell X_\sigma$. We have a commutative diagram

$$\begin{array}{ccccc}
\mathrm{Gal}(\bar{K}/K) & \supset & D_{\bar{\sigma}} & \twoheadrightarrow & \mathrm{Gal}(\bar{F}/F(\sigma)) \\
\downarrow{\scriptstyle \rho_\eta} & & & & \downarrow{\scriptstyle \rho_\sigma} \\
\mathrm{End}(T_\ell X_\eta) & & \cong & & \mathrm{End}(T_\ell X_\sigma),
\end{array}$$

in which ρ_η and ρ_σ denote the Galois representations associated to X_η and X_σ respectively. Note that it depends only on σ whether or not $\mathrm{im}(\rho_\eta) = \mathrm{im}(\rho_\sigma)$, not on the choice of a point $\bar{\sigma}$ lying over it.

1.3 Proposition (Serre). *Suppose F is a field, of finite type over $\mathbf{Q}$, that S is a normal and absolutely irreducible F-variety, and that X is an abelian scheme over S. Let $\eta : \mathrm{Spec}(K) \to S$ be the inclusion of the generic point. Then there is a closed point σ of S such that*

$$\rho_\eta(\mathrm{Gal}(\bar{K}/K)) = \rho_\sigma(\mathrm{Gal}(\bar{F}/F(\sigma)))$$

if $T_\ell X_\eta$ and $T_\ell X_\sigma$ are identified in the way described above.

1.4 Proof. This proposition can be found in [Se1]. After replacing S by a non-empty open subset, as we may do without loss of generality, we can assume that S is smooth and affine. Let $\mathcal{F}_\eta$ be the extension field of K that corresponds to $\ker(\rho_\eta) \subset \mathrm{Gal}(\bar{K}/K)$ and let $\mathrm{Spec}(\mathcal{F})$ be the normalization of S in $\mathcal{F}_\eta$. Because $X[\ell^n]$ is étale over S for every n, $\mathrm{Spec}(\mathcal{F})$ is an unramified cover of S. By construction, $\mathrm{Gal}(\mathcal{F}_\eta/K)$ is a compact ℓ-adic Lie group.

Because S is smooth over F, there is a non-empty affine open subset $U \subset S$ that admits an étale map to the affine space $\mathbf{A}^d = \mathbf{A}^d_F$, where d is the dimension of S. We replace S by U and $\mathcal{F}$ by its pullback to U. Let $\zeta : \mathrm{Spec}(F(t_1, \ldots, t_d)) \to \mathbf{A}^d$ be the generic point of $\mathbf{A}^d$ and let $\mathcal{F}'$ be the Galois closure of $\mathcal{F}/F[t_1, \ldots, t_d]$. The Galois group $\mathrm{Gal}(\mathcal{F}'_\eta/F(t_1, \ldots, t_d))$

is a compact ℓ-adic Lie group because $\mathrm{Gal}(\mathcal{F}_\eta/K)$ is one. Here $\mathcal{F}'_\eta$ denotes the fraction field of $\mathcal{F}'$. For every point $\tau \in \mathbf{A}^d(F)$ we can form the following diagram, in which all squares are cartesian

$$\begin{array}{ccccc}
\mathrm{Spec}(\mathcal{F}'_\eta) & \longrightarrow & \mathrm{Spec}(\mathcal{F}') & \longleftarrow & \mathrm{Spec}(\mathcal{F}'_\tau) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Spec}(\mathcal{F}_\eta) & \longrightarrow & \mathrm{Spec}(\mathcal{F}) & \longleftarrow & \mathrm{Spec}(\mathcal{F}_\tau) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Spec}(K) & \xrightarrow{\eta} & S & \longleftarrow & S_\tau \\
\downarrow & & \downarrow{\scriptstyle\pi} & & \downarrow \\
\mathrm{Spec}(F(t_1,\ldots,t_d)) & \xrightarrow{\zeta} & \mathbf{A}^d & \xleftarrow{\tau} & \mathrm{Spec}(F).
\end{array}$$

If σ' is a point of $\mathrm{Spec}(\mathcal{F}')$, the decomposition group of σ' in $\mathrm{Gal}(\mathcal{F}'_\eta/F(t_1,\ldots,t_d))$ will be denoted by $D_{\sigma'}$. It follows from [Se2, 10.6], and in particular from Example 1 and the theorem on page 149, that there is a thin subset $\Omega \subset \mathbf{A}^d(F)$ such that, for all $\tau \in \mathbf{A}^d(F)$ outside Ω we have that $\mathcal{F}'_\tau$ is a field and that

$$\mathrm{Gal}(\mathcal{F}'_\eta/F(t_1,\ldots,t_d)) = D_{\sigma'} = \mathrm{Gal}(\mathcal{F}'_\tau/F),$$

where $\sigma' \in \mathrm{Spec}(\mathcal{F}')$ is the unique closed point lying over τ. The reader is referred to [Se2, 9.1] for an explanation of the concept of thin sets. In all points τ outside Ω we automatically have that $\mathcal{F}_\tau$ is a field. The equality we claim holds for all σ lying over these τ.

Since F is hilbertian by [Se2, 9.6], the complement of a thin set is infinite, so we can in fact choose a τ with these properties. Proposition 1.3 follows. □

1.5 Corollary. *Suppose that we are in the situation of the proposition, and that $\sigma \in S$ is a closed point fulfilling the statement of the proposition. Then we have*

$$\mathrm{End}_{\bar{K}}(X_\eta) = \mathrm{End}_{\overline{F(\sigma)}}(X_\sigma).$$

1.6 Proof. By assumption, we have a finite extension L of F and a point $\sigma \in S(L)$ such that the images of the maps

$$\rho_\eta : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{End}(T_\ell X_\eta)$$

and

$$\rho_\sigma : \mathrm{Gal}(\bar{L}/L) \longrightarrow \mathrm{End}(T_\ell X_\sigma)$$

are equal. We write $R = \mathrm{End}_{\bar{K}}(X_\eta)$. Let us see why $\mathrm{End}_{\bar{L}}(X_\sigma) = R$ as well.

There is a finite extension K' of K such that $\mathrm{End}_{K''}(X_\eta) = R$ for every finite extension K'' of K'. By [FW, VI,3] we have

$$\mathrm{End}_{\mathrm{Gal}(\bar{K}/K'')}(T_\ell X_\eta) = \mathrm{End}_{K''}(X_\eta) \otimes \mathbf{Z}_\ell = R \otimes \mathbf{Z}_\ell$$

for every such K''. The group $\rho_\sigma^{-1}\rho_\eta(\mathrm{Gal}(\bar{K}/K'))$ is a closed normal subgroup of $\mathrm{Gal}(\bar{L}/L)$ of finite index. Let L' be the extension of L corresponding to this subgroup. For all finite extensions L'' of L' we have that $\rho_\sigma(\mathrm{Gal}(\bar{L}/L'')) \subset \rho_\eta(\mathrm{Gal}(\bar{K}/K'))$ is of finite index and hence $\mathrm{End}_{\mathrm{Gal}(\bar{L}/L'')}(T_\ell X_\sigma) = R \otimes \mathbf{Z}_\ell$ for all such L''. It follows that $\mathrm{End}_{\bar{L}}(X_\sigma) \otimes \mathbf{Z}_\ell = R \otimes \mathbf{Z}_\ell$. Because $\mathrm{End}_{\bar{K}}(X_\eta) \subset \mathrm{End}_{\bar{L}}(X_\sigma)$ and because the quotient is torsion free, it follows that $\mathrm{End}_{\bar{L}}(X_\sigma) = R$. □

1.7 Theorem. *Let G be the Mumford–Tate group of an abelian variety $X/\mathbf{C}$. Fix a prime number ℓ. There exist a number field F and an abelian variety Y/F with Mumford–Tate group G, such that the image of the ℓ-adic Galois representation*

$$\rho_\ell : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{End}(T_\ell Y)$$

is an open and Zariski dense subgroup of $G(\mathbf{Q}_\ell)$.

1.8 Proof. Once we have found Y/F such that $\mathrm{im}(\rho_\ell)$ is Zariski dense in $G(\mathbf{Q}_\ell)$, the fact that it is open for the ℓ-adic topology follows from [Bo].

Let $G' = [G, G]$ be the derived group and $C = Z_G^0$ be the connected centre of G. Since X is polarizable, G is reductive by [De2, 3.6], so $G = G' \cdot C$ and $G' \cap C$ is finite. As usual, S denotes the Weil restriction $R_{\mathbf{C}/\mathbf{R}}\mathbf{G}_m$. The Hodge structure on $V = H_1(X(\mathbf{C}), \mathbf{Q})$ determines and is determined by a group homomorphism $h : S \to G_{\mathbf{R}} \subset \mathrm{GL}(V_{\mathbf{R}})$. Let $K_\infty \subset G(\mathbf{R})$ be the centralizer of h and let $G(\mathbf{R})^0$ and K_∞^0 be the connected components of the unit element in $G(\mathbf{R})$ and K_∞ respectively. For any sufficiently small arithmetic subgroup $\Gamma \subset G'(\mathbf{Q})$, we can form the connected Shimura variety

$$M_{\mathbf{C}}(\mathbf{C}) = \Gamma \backslash G(\mathbf{R})^0 / K_\infty^0.$$

It is well known that $M_{\mathbf{C}}(\mathbf{C})$ is the set of $\mathbf{C}$-valued points of a quasi-projective $\mathbf{C}$-scheme $M_{\mathbf{C}}$ and that it is a component of a moduli space for abelian varieties over $\mathbf{C}$ with certain properties, see for example [De1, 1.7]. By choosing Γ sufficiently small, we can make sure that it is torsion free, that $M_{\mathbf{C}}$ is smooth, and that there exists a universal polarized abelian scheme $\mathcal{X}_{\mathbf{C}} \to M_{\mathbf{C}}$. The variety X is isomorphic to a fibre of this family and the Mumford–Tate group of the generic fibre is equal to G.

By [De1, 5.9], $M_{\mathbf{C}}$ admits a quasi-canonical model M over a number field F. We can assume that F is so large that the abelian scheme $\mathcal{X}_{\mathbf{C}}$ descends to an abelian scheme $\mathcal{X}/M$. We will denote the function field of M by K and the inclusion of the generic point by η. There is a Galois representation

$$\rho_\ell : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{End}(T_\ell \mathcal{X}_\eta \otimes \mathbf{Q}_\ell).$$

We claim that the Zariski closure of the image of this representation contains G. This claim will be proved afterwards, let us first show that it implies the theorem.

Proposition 1.3 allows us to find a closed point y of M such that the image of the Galois representation $\rho_{\ell,Y}$ associated to $Y = \mathcal{X}_y/F(y)$ is equal to the image of ρ_ℓ. By construction, the Mumford–Tate group of Y is contained in G, and the claim implies that G is contained in the Zariski closure of $\mathrm{im}(\rho_{\ell,Y})$. It follows from [De2, 2.9b, 2.11] that, after replacing $F(y)$ by a finite extension, the image of $\rho_{\ell,Y}$ is Zariski dense in the Mumford–Tate group of Y. The Mumford–Tate group of Y is therefore in fact equal to G. After replacing $F(y)$ by this finite extension, $\mathrm{im}(\rho_{\ell,Y})$ is a Zariski dense subgroup of $G(\mathbf{Q}_\ell)$. This concludes the proof that the claim implies the theorem, so we now only need to prove the claim.

We will first show that the Zariski closure of $\mathrm{im}(\rho_\ell)$ contains G'. To this end, it suffices to show that the Zariski closure of the image of the representation

$$\rho_\eta : \pi_1(M_{\mathbf{C}}, \overline{\eta_{\mathbf{C}}}) \longrightarrow \mathrm{End}(T_\ell\,(\mathcal{X}_{\mathbf{C}})_{\eta_{\mathbf{C}}} \otimes \mathbf{Q}_\ell)$$

of the algebraic fundamental group at a geometric generic point of $M_{\mathbf{C}}$ is equal to G'. This image is independent of the choice of the base point, so it suffices to prove the assertion for the representation

$$\rho_p : \pi_1(M_{\mathbf{C}}, p) \longrightarrow \mathrm{End}(T_\ell\,(\mathcal{X}_{\mathbf{C}})_p \otimes \mathbf{Q}_\ell)$$

for any point $p \in M_{\mathbf{C}}(\mathbf{C})$. By [AGV, XI, 4.3(iii)], the category of finite topological covers of $M_{\mathbf{C}}(\mathbf{C})$ is equivalent to the category of finite étale covers of $M_{\mathbf{C}}$. It therefore suffices to show that the image of the topological fundamental group $\pi_1(M_{\mathbf{C}}(\mathbf{C}), p)$ acting on V is Zariski dense in G'. But $G(\mathbf{R})^0/K_\infty^0$ is homeomorphic to $\mathbf{R}^n$ for some n and Γ acts freely on this space, so $\pi_1(M_{\mathbf{C}}(\mathbf{C}), p) = \Gamma$. If H is an almost simple factor of G over $\mathbf{Q}$, the group $H(\mathbf{R})^0$ is not compact. It therefore follows from [Ma, I, 3.2.11] that the Zariski closure of Γ is equal to G'.

To conclude the proof of the claim, we will show that the Zariski closure of $\mathrm{im}(\rho_\ell)$ contains a group which maps onto G/G'. Let y be a closed point of M corresponding to an abelian variety Y of CM-type. To show that such a point exists, it suffices to show that there is a special point of M which is defined over $\bar{\mathbf{Q}}$. This follows because the existence of a special point in $M(\mathbf{C})$ is guaranteed by [De1, 5.1] and the fact fact that M is a quasi-canonical model of $M_{\mathbf{C}}$ implies that all special points are defined over $\bar{\mathbf{Q}}$. The Mumford–Tate group of $Y_{\mathbf{C}}$ is a torus $T \subset G$. The Hodge structure on $H_1(Y(\mathbf{C}), \mathbf{Q}) \cong V$ is determined by a map $h' : S \to T_{\mathbf{R}}$ which is conjugate to $h : S \to G_{\mathbf{R}}$ by an element of $G(\mathbf{R})$. Hence, the composite

$$S \xrightarrow{h'} T_{\mathbf{R}} \subset G_{\mathbf{R}} \longrightarrow (G/G')_{\mathbf{R}}$$

is equal to the composite

$$S \xrightarrow{h} G_{\mathbf{R}} \longrightarrow (G/G')_{\mathbf{R}}.$$

Since T and G are the smallest subgroups of $\mathrm{GL}(V)$ defined over $\mathbf{Q}$ containing the images of h' and h respectively, it follows that T maps onto G/G'. It follows from [Po, Theorem 4] that, after replacing $F(y)$ by a finite extension, the image of the ℓ-adic Galois representation associated to Y is Zariski dense in $T(\mathbf{Q}_\ell)$, so by 1.2 the Zariski closure of $\mathrm{im}(\rho_\ell)$ contains the group T, which maps onto G/G'. This completes the proof of the claim and hence that of the theorem. $\square$

2 Properties of ordinary reduction

2.1 It is known (see [Tan, 5.5] or [Ad, 6.2]) that, for every natural number k, there are abelian varieties such that the Lie algebra of the Mumford–Tate group G is isomorphic over $\bar{\mathbf{Q}}$ to $\mathfrak{sp}(2)^{2k+1} \times \mathbf{G}_a$. By Theorem 1.7, this implies that there exist abelian varieties such that the image of the associated ℓ-adic Galois representation is open in the group $G(\mathbf{Q}_\ell)$ of $\mathbf{Q}_\ell$-valued points of such a group G.

In this section we will study the properties of ordinary reduction of an abelian variety X over a number field F for which the Lie-algebra of the image of the Galois representation

$$\rho_\ell : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{End}(T_\ell X)$$

is a $\mathbf{Q}_\ell$-form of $\mathfrak{sp}(2)^{2k+1} \times \mathbf{G}_a$.

2.2 Theorem. *Suppose that X is an abelian variety of dimension 2^{2k} over a number field F. Assume that for some prime number ℓ, the Zariski closure G_ℓ of the image of the ℓ-adic Galois representation satisfies*

$$\mathrm{Lie}(G_\ell)_{\bar{\mathbf{Q}}_\ell} \cong (\mathfrak{sp}(2)^{2k+1} \times \mathbf{G}_a)_{\bar{\mathbf{Q}}_\ell},$$

where $\mathfrak{sp}(2)^{2k+1}$ acts on $T_\ell X \otimes \bar{\mathbf{Q}}_\ell$ via the $(2k+1)$-th tensor power of the standard representation. Then there are a finite extension F' of F and a set P of places of F', of Dirichlet density 1, such that X has good and ordinary reduction at every place $v \in P$.

2.3 Proof. Without loss of generality, we can assume that G_ℓ is connected. Let us consider the weights of the representation of $(G_\ell)_{\bar{\mathbf{Q}}_\ell}$. The weights of the representation of $\mathrm{Sp}(2)^{2k+1}$ are the vertices $\{\pm e_1 \pm \ldots \pm e_{2k+1}\}$ of a hypercube in $\mathbf{R}^{2k+1}$. The weights of the representation of $(G_\ell)_{\bar{\mathbf{Q}}_\ell}$ are the translates of these weights over the vector $e_{2k+2} \in \mathbf{R}^{2k+2}$, the last coordinate corresponding to the connected centre $\mathbf{G}_m$.

Suppose that m is an integer such that $\ell^m > 8k+4$ and let F' be a finite extension of F containing the ℓ^m-th roots of unity and enjoying the property that all elements of $\rho_\ell(\mathrm{Gal}(\bar{\mathbf{Q}}/F'))$ are congruent to id modulo ℓ^m. Let P' be the set of places v of F' with the properties that

- v does not divide ℓ,
- X has good reduction X_v at v, and
- $\rho_\ell(\mathrm{Fr}_v)$ generates a maximal torus of G_ℓ, i.e. the Zariski closure of the subgroup of $G_\ell(\mathbf{Q}_\ell)$ generated by $\rho_\ell(\mathrm{Fr}_v)$ is a maximal torus of G_ℓ.

It follows from [Ch, 3.8] that P' has Dirichlet density 1. Let P be the largest subset of P' such that

- F' is unramified at the places contained in P, and
- all $v \in P$ have degree 1.

The set P also has Dirichlet density 1. We will show that X_v is ordinary for each $v \in P$.

Let $v \in P$ and suppose that v has residue characteristic p. Because v has degree 1, X_v is defined over the prime field $\mathbf{F}_p$. The condition that $\rho_\ell(\mathrm{Fr}_v)$ should generate a maximal torus of G_ℓ is equivalent to the condition that its eigenvalues $\lambda_1, \ldots, \lambda_{2g}$ should not have any more multiplicative relations with integer coefficients than the weights of the representation of $(G_\ell)_{\bar{\mathbf{Q}}_\ell}$ on $T_\ell X \otimes \bar{\mathbf{Q}}_\ell$ have additive relations. This means that we can map the subgroup of $\bar{\mathbf{Q}}^*$ generated by $\lambda_1, \ldots, \lambda_{2g}$ injectively to $\mathbf{R}^{2k+2}$ by mapping each λ_i to the corresponding weight. From now on, we will identify this subgroup of $\bar{\mathbf{Q}}^*$ with its image Λ in $\mathbf{R}^{2k+2}$ and the λ_i with the vertices of the hypercube described above. The algebraic number corresponding to $Q \in \Lambda$ will be denoted by α_Q. Conversely, we write Q_α for the element of Λ corresponding to $\alpha \in \langle \lambda_1, \ldots, \lambda_{2g} \rangle \subset \bar{\mathbf{Q}}^*$. Note that $\alpha_{Q+R} = \alpha_Q \alpha_R$ and $Q_{\alpha\beta} = Q_\alpha + Q_\beta$.

By [Tat], the λ_i are the zeros of a polynomial with coefficients in $\mathbf{Z}$, so $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on the set $\{\lambda_1, \ldots, \lambda_{2g}\}$. The λ_i satisfy the same relations as the vertices of the hypercube, so this action factors through the automorphism group of this hypercube. Because $\lambda_i \bar{\lambda}_i = p$ for every complex conjugation $\alpha \mapsto \bar{\alpha}$ on $\bar{\mathbf{Q}}$, there is a well defined complex conjugation on the subgroup of $\bar{\mathbf{Q}}^*$ generated by the λ_i. Because the λ_i correspond to the vertices of the hypercube, this complex conjugation acts on these vertices and since $\lambda_i \bar{\lambda}_i = p$, this action is given by inversion of the hypercube in its centre e_{2k+2}. In other words, the action of complex conjugation on Λ is induced by the map on $\mathbf{R}^{2k+2}$ given by

$$(x_1, \ldots, x_{2k+1}, x_{2k+2}) \mapsto (-x_1, \ldots, -x_{2k+1}, x_{2k+2}).$$

We also see that p corresponds to the vector $2e_{2k+2}$.

Let w be a valuation of $\bar{\mathbf{Q}}$ lying over p, normalized by $w(p) = 1$. It gives a map from $\bar{\mathbf{Q}}^*$ to $\mathbf{Q}$ and hence a map $\Lambda \to \mathbf{Q}$. On the set $\{\lambda_1, \ldots, \lambda_{2g}\}$, w takes values in the interval $[0, 1]$ and to prove that X_v is ordinary, we have to show that the only values it assumes are 0 and 1. To do so, we suppose that it does take another value and proceed to derive a contradiction.

For each $1 \leq j \leq 2k+1$ we put $Q_j^+ = 2e_j + 2e_{2k+2} \in \Lambda$ and $Q_j^- = -2e_j + 2e_{2k+2}$. The algebraic numbers $\alpha_j^+ = \alpha_{Q_j^+}$ and $\alpha_j^- = \alpha_{Q_j^-}$ have absolute value p for every archimedian absolute value on $\bar{\mathbf{Q}}$, because each of these numbers is the product of two eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$. We claim that our assumption that $w(\lambda_i) \notin \{0, 1\}$ for some i implies that $w(\alpha_j^+) > 0$ and $w(\alpha_j^-) > 0$ for all j. To show this, note that, for any j, the set of eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ is the union of the set of the eigenvalues corresponding to a vertex for which the j-th coordinate is positive and the set of the eigenvalues for which this coordinate is negative. Our assumption on $w(\lambda_i)$ implies that both these sets contain an eigenvalue of $\rho_\ell(\mathrm{Fr}_v)$ with positive valuation, namely λ_i for the one and $\bar{\lambda}_i$ for the other subset. Let us assume that λ_i lies in the former of these sets. Then $\alpha_j^+ = \lambda_i\lambda_{i'}$ for some i' and hence $w(\alpha_j^+) > 0$. Similarly we see that $w(\alpha_j^-) > 0$.

Because the group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts on the set $\{\lambda_1, \ldots, \lambda_{2g}\}$ through the automorphism group of the hypercube, it acts on the set $\{\alpha_j^+, \alpha_j^-\}_{1\le j\le 2k+1}$. We will be interested in the algebraic integer

$$\beta = \sum_{j=1}^{2k+1} (\alpha_j^+ + \alpha_j^-).$$

It is invariant under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and therefore $\beta \in \mathbf{Z}$. We also know that $w(\beta) > 0$, whence $p \mid \beta$, and that $|\beta| \le (4k+2)p$.

Because of the assumptions on F', we know that the numbers $\alpha_j^\pm$ are congruent to 1 modulo ℓ^m, so $\beta \equiv 4k+2 \pmod{\ell^m}$. Because v has degree 1 in F' and since F' contains the ℓ^m-th roots of unity, we have $p \equiv 1 \pmod{\ell^m}$. It follows that $\beta \equiv (4k+2)p \pmod{p\ell^m}$. Because $\ell^m > 8k+4$, the facts that

$$|\beta| \le (4k+2)p$$

and

$$\beta \equiv (4k+2)p \pmod{p\ell^m}$$

imply that $\beta = (4k+2)p$ and it follows that all $\alpha_j^\pm$ are equal to p, contradicting the fact that the eigenvalues of $\rho_\ell(\mathrm{Fr}_v)$ do not satisfy more relations then the weights of ρ_ℓ. This means that our assumption that $w(\{\lambda_i\}_{i=1}^{2g}) \ne \{0,1\}$ was incorrect and hence that X has ordinary reduction at v. $\square$

References

[Ad] S. L. Addington, *Equivariant holomorphic maps of symmetric domains.* Duke Math. J. 55 (1987), 65–88.

[AGV] M. Artin, A. Grothendieck, J. L. Verdier, *Théorie des topos et cohomologie étale des schémas (SGA 4).* Lecture Notes in Math. 269, 270, 305; Springer-Verlag, 1973.

[Bo] F. A. Bogomolov, *Sur l'algébricité des représentations ℓ-adiques.* C. R. Acad. Sc. Paris, Série A, t. 290 (1980), 701–703.

[Ch] W. Chi, *ℓ-Adic and λ-adic representations associated to abelian varieties defined over number fields.* Amer. J. Math. 114 (1992), 315-353.

[De1] P. Deligne, *Travaux de Shimura.* Séminaire Bourbaki, Exposé 389, Février 1971. Lecture Notes in Math. 244, pp. 123–165; Springer-Verlag, 1971.

[De2] P. Deligne, *Hodge cycles on abelian varieties*. Hodge Cycles, Motives, and Shimura Varieties (P. Deligne, J. S. Milne, A. Ogus and K.-y. Shih), Chapter I. Lecture Notes in Math. 900, pp. 9–100; Springer-Verlag, 1982.

[FW] G. Faltings, G. Wüstholz et al., *Rational points*. Vieweg 1984.

[Ma] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*. Springer-Verlag 1991.

[Og] A. Ogus, *Hodge cycles and crystalline cohomology*. Hodge Cycles, Motives, and Shimura Varieties (P. Deligne, J. S. Milne, A. Ogus and K.-y. Shih), Chapter VI. Lecture Notes in Math. 900, pp. 357–414; Springer-Verlag, 1982.

[Po] H. Pohlmann, *Algebraic cycles on abelian varieties of complex multiplication type*. Ann. of Math. 88 (1968), 161–180.

[Se1] J-P. Serre, Letter to Ribet, 1–1–1981.

[Se2] J-P. Serre, *Lectures on the Mordell–Weil theorem*. Vieweg, 1989.

[Tan] S. G. Tankeev, *On algebraic cycles on surfaces and abelian varieties*. Math. USSR-Izv., Vol. 18, No. 2 (1982), 349–380.

[Tat] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*. Séminaire Bourbaki, Exposé 352, Novembre 1968. Lecture Notes in Math. 179, pp. 95–110; Springer-Verlag, 1971.

Rutger Noot[1]
Mathematisches Institut
Einsteinstrasse 62
48149 Münster
Germany

[1]Current address: Institut Mathématique, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes cedex, France.