GALOIS REPRESENTATIONS ATTACHED TO ABELIAN VARIETIES OF CM TYPE

Davide Lombardo

Diffusion

Tarifs

Secrétariat : Nathalie Christiaën

GALOIS REPRESENTATIONS ATTACHED
TO ABELIAN VARIETIES OF CM TYPE

by Davide Lombardo

Abstract. — Let K be a number field, A/K be an absolutely simple abelian variety of CM type, and ℓ be a prime number. We give explicit bounds on the degree over K of the division fields $K(A[\ell^n])$, and when A is an elliptic curve we also describe the full Galois group of $K(A_{\text{tors}})/K$. This makes explicit previous results of Serre [17] and Ribet [14], and strengthens a theorem of Banaszak, Gajda and Krasoń [2]. Our bounds are especially sharp when the CM type of A is nondegenerate.

Résumé (*Représentations galoisiennes associées aux variétés abéliennes de type CM*). — Soient K un corps de nombres, A/K une variété abélienne géométriquement simple de type CM et ℓ un nombre premier. Nous donnons des bornes explicites sur le degré sur K des extensions $K(A[\ell^n])$ engendrées par les points de ℓ^n-torsion de A, et quand A est une courbe elliptique nous décrivons le groupe de Galois de $K(A_{\text{tors}})/K$ tout entier. Cela fournit une version explicite de résultats antérieurs de Serre [17] et Ribet [14], et renforce un théorème de Banaszak, Gajda and Krasoń [2]. Nos bornes sont particulièrement fines quand le type CM de A est non-dégénéré.

1. Introduction and statement of the result

The aim of this work is to study division fields of simple abelian varieties of CM type. Recall that an abelian variety A, of dimension g and defined over a number field K, is said to admit (potential) complex multiplication, or CM for short, if there is an embedding $E \hookrightarrow \mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$, where E is an étale $\mathbb{Q}$-algebra of degree $2g$. We shall very often restrict to the situation of A admitting complex multiplication by E over K, by which we mean that $\mathrm{End}_K(A)$ is equal to $\mathrm{End}_{\overline{K}}(A)$, and of A being absolutely simple, or equivalently, of E being a number field (of degree $2g$ over $\mathbb{Q}$). The problem we discuss is that of estimating the degree $[K(A[\ell^n]) : K]$, where ℓ is a prime number and $K(A[\ell^n])$ is the field generated over K by the coordinates of the ℓ^n-torsion points of A in $\overline{K}$. As we shall see shortly, this is really a problem in the theory of Galois representations, and the seminal contributions of Shimura–Taniyama [21] and Serre–Tate [19] provide us with powerful tools for handling these representations in the CM case. Employing such tools, Silverberg studied in [22] the extension of K generated by a single torsion point of A, while Ribet gave in [14] asymptotic (non-effective) bounds on $[K(A[\ell^n]) : K]$ as $n \to \infty$. Our first result can be seen as an explicit version of the main theorem of [14]:

THEOREM 1.1. — *Let K be a number field and A/K be an abelian variety of dimension g admitting complex multiplication over K by an order in the CM field E. Denote by μ be the number of roots of unity contained in E and by $h(K)$ the class number of K. Let r be the rank of the Mumford-Tate group of A (cf. Definition 2.10) and $\ell > \sqrt{2 \cdot g!}$ be a prime unramified in $E \cdot K$. The following inequality holds:*

$$\frac{1}{4\mu\sqrt{g!}} \cdot \ell^{nr} \le [K(A[\ell^n]) : K] \le \frac{5}{2}\mu \cdot h(K) \cdot \ell^{nr}.$$

Even though Theorem 1.1 gives a good idea of the actual order of magnitude of the degree $[K(A[\ell^n]) : K]$, we can in fact prove much more precise results that apply to all primes ℓ and which are most easily described in the language of Galois representations. Recall that for every ℓ and every n there is a natural continuous action of $\mathrm{Gal}\left(\overline{K}/K\right)$ on $A[\ell^n]$, giving rise to a representation

$$\rho_{\ell^n} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(A[\ell^n]);$$

the extension $[K(A[\ell^n]) : K]$ is Galois, and its Galois group can be identified with the image G_{ℓ^n} of ρ_{ℓ^n}. Taking the inverse limit of this system of representations gives rise to the ℓ-adic representation on the Tate module $T_\ell A$,

$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell A).$$

We denote by G_{ℓ^∞} the image of ρ_{ℓ^∞} and remark that, for every n, the group G_{ℓ^n} is clearly isomorphic to the image of G_{ℓ^∞} through the canonical projection

$$\operatorname{Aut}(T_\ell A) \to \operatorname{Aut}\left(\frac{T_\ell A}{\ell^n T_\ell A}\right) \cong \operatorname{Aut}(A[\ell^n]);$$

for simplicity of exposition, we fix once and for all a $\mathbb{Z}_\ell$-basis of $T_\ell A$ and consider G_{ℓ^∞} (resp. G_{ℓ^n}) as a subgroup of $\operatorname{GL}_{2g}(\mathbb{Z}_\ell)$ (resp. of $\operatorname{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$).

We have thus reduced the problem of giving bounds on $[K(A[\ell^n]) : K]$ to that of describing G_{ℓ^n}: in trying to do so, it is natural to compare G_{ℓ^∞} with $\operatorname{MT}(A)$, the Mumford-Tate group of A (cf. Definition 2.10). By construction, $\operatorname{MT}(A)$ is an algebraic subtorus of GL_{2g} which is only defined over $\mathbb{Q}$, so there is no obvious good definition for the group of its $\mathbb{Z}_\ell$-valued points. However, Ono [12] has shown that there is in fact a good notion of $\operatorname{MT}(A)(\mathbb{Z}_\ell)$ (cf. Definition 2.3), and the Mumford-Tate conjecture [8, §4]—which is a theorem for CM abelian varieties ([13] and [21])—can be expressed by saying that, possibly after replacing K by a finite extension, G_{ℓ^∞} is a finite-index subgroup of $\operatorname{MT}(A)(\mathbb{Z}_\ell)$. For the sake of simplicity, assume for now that no extension of the base field K is necessary to attain the condition $G_{\ell^\infty} \subseteq \operatorname{MT}(A)(\mathbb{Z}_\ell)$ (our results do not depend on this assumption). The problem of estimating the degree $[K(A[\ell^n]) : K]$ is then reduced to the study of two separate quantities: the order of the finite group $\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ and the index $[\operatorname{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty}]$.

We treat the first problem in two important situations: when ℓ is unramified in E (a rather simple case, covered by Lemma 2.5), and when the CM type of A is nondegenerate (Theorem 6.1). Our result can be stated as follows:

THEOREM 1.2. — *Let A/K be an absolutely simple abelian variety of dimension g, admitting (potential) complex multiplication by the CM field E. Denote by $\operatorname{MT}(A)$ the Mumford-Tate group of A and let r be its rank.*

  1. *If ℓ is unramified in E the following inequalities hold:*

$$(1 - 1/\ell)^r \ell^{nr} \leq |\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq (1 + 1/\ell)^r \ell^{nr}.$$

  2. *Suppose $r = g + 1$. For all primes $\ell \neq 2$ and all $n \geq 1$ we have*

$$(1 - 1/\ell)^{g+1} \cdot \ell^{(g+1)n} \leq |\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq 2^g (1 + 1/\ell)^{g-1} \ell^{(g+1)n},$$

  while for $\ell = 2$ and all $n \geq 1$ we have

$$\frac{1}{2^{2g+3}} \cdot 2^{(g+1)n} \leq |\operatorname{MT}(A)(\mathbb{Z}/2^n\mathbb{Z})| \leq 2^{2g-1} \cdot 2^{(g+1)n}.$$

As for the index $[\operatorname{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty}]$, our main result is as follows (cf. Definition 2.9 for the notion of reflex norm):

THEOREM 1.3. — *(Theorem 5.5) Let A/K be an absolutely simple abelian variety of dimension g admitting complex multiplication over K by the CM type (E, S), and let ℓ be a prime number. If A has bad reduction at a place of K dividing ℓ let $\mu^* = |\mu(E)|$, the number of roots of unity in E; if on the contrary*

A has good reduction at all places of K of characteristic ℓ set $\mu^* = 1$. Denote by r the rank of $\mathrm{MT}(A)$ and by F the group of connected components of the kernel of the reflex norm $T_{E^*} \to T_E$, where E^* is the reflex field of E. Then:

(1) *The index $[G_{\ell^\infty} : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ does not exceed $|\mu(E)| \cdot h(K)$, where $h(K)$ is the class number of K.*

(2) *We have $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)] \leq \mu^* \cdot [K : E^*] \cdot |F|^{2r}$.*

(3) *If ℓ is unramified in E and does not divide $|F|$, then the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ divides $\mu^* \cdot [K : E^*] \cdot |F|$. If ℓ is also unramified in K, the bound can be improved to $\mu^* \cdot |F|$.*

Finally we have $r \leq g + 1$ and $|F| \leq f(r) \leq f(g + 1)$, where

$$f(x) = \left\lfloor 2 \left(\frac{x+1}{4} \right)^{(x+1)/2} \right\rfloor.$$

REMARK 1.4. — A few comments are in order:

- Theorem 1.1 follows immediately upon combining Theorems 1.2 and 1.3.
- The assumption that the action of E is defined over K implies that the reflex field E^* is contained in K, see [6, Chap. 3, Theorem 1.1]. In particular, the degree $[K : E^*]$ makes sense.
- The condition $\ell \nmid |F|$ is certainly satisfied if $\ell > |F|$: in particular, it is true for all primes $\ell > f(r)$.
- Since $|F|$ is bounded by $f(g+1)$, the degree $[K : E^*]$ does not exceed $[K : \mathbb{Q}]$, and μ^* can be controlled in terms of g alone (a trivial bound is for example $\mu^* \leq 16g^2$), we see that part (2) of Theorem 1.3 gives a universal bound on $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ that only depends on g and $[K : \mathbb{Q}]$.
- For small values of g the function $f(g+1)$ takes reasonably small values: we have $f(3) = 2$, $f(4) = 3$, $f(5) = 6$, $f(6) = 14$ and $f(7) = 32$.

In the special case of elliptic curves the Mumford-Tate group admits a particularly simple description, which leads to a very precise characterization of the corresponding Galois representation. Such a description can already be found (in a non-effective form) in [17, Corollaire on p.302], and the following result makes it completely explicit:

THEOREM 1.5. — *(Theorem 6.6) Let A/K be an elliptic curve such that $\mathrm{End}_{\overline{K}}(A)$ is an order in an imaginary quadratic field E. Denote by $\rho_\infty : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_\ell \mathrm{Aut}\, T_\ell A$ the natural adelic representation attached to A, and let G_∞ be its image. For every prime ℓ denote by C_ℓ the group $(\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times$, considered as a subgroup of $\mathrm{Aut}_{\mathbb{Z}_\ell}(\mathcal{O}_E \otimes \mathbb{Z}_\ell) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}\, T_\ell A$, and let $N(C_\ell)$ be the normalizer of C_ℓ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

1. *Suppose that $E \subseteq K$: then G_∞ is contained in $\prod_\ell C_\ell$, and the index $[\prod_\ell C_\ell : G_\infty]$ does not exceed $3[K : \mathbb{Q}]$. The equality $G_{\ell^\infty} = C_\ell$ holds for*

every prime ℓ unramified in K and such that A has good reduction at all places of K of characteristic ℓ.

2. *Suppose that $E \not\subseteq K$: then G_∞ is contained in $\prod_\ell N(C_\ell)$ but not in $\prod_\ell C_\ell$, and the index $[\prod_\ell N(C_\ell) : G_\infty]$ is not finite. The intersection $H_\infty = G_\infty \cap \prod_\ell C_\ell$ has index 2 in G_∞, and the index $[\prod_\ell C_\ell : H_\infty]$ does not exceed $6[K : \mathbb{Q}]$. The equality $G_{\ell^\infty} = N(C_\ell)$ holds for every prime ℓ unramified in $K \cdot E$ and such that A has good reduction at all places of K of characteristic ℓ.*

Finally, the constants 3 and 6 appearing in parts (1) and (2) respectively can be replaced by 1 and 2 if we further assume that the j-invariant of A is neither 0 nor 1728.

As a by-product of the proof of Theorem 1.3 we also obtain the following proposition, which slightly strengthens a result first proved by Banaszak, Gajda and Krasoń ([2, Theorem A]) by removing both the assumption that the CM type of A is nondegenerate and the hypothesis that ℓ is completely split in K.

PROPOSITION 1.6. — *(Proposition 5.6) Let A/K be an absolutely simple abelian variety admitting complex multiplication (over K) by the CM field E, and let ℓ be a prime unramified in E. Let E^* be the reflex field of E and suppose that A has good reduction at all places of K of characteristic ℓ.*

- *The index $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)]$ divides $[K : E^*] \cdot |F|$.*
- *If ℓ is also unramified in K, then $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)]$ divides $|F|$.*

Let us conclude this introduction by giving a brief overview of the material in the paper.

In Section 2 we recall some fundamental notions about algebraic tori over $\mathbb{Q}$ and their $\mathbb{Z}_\ell$-points; this part also includes a brief account of the theory of abelian varieties of CM type and of their Mumford-Tate groups. In Section 3 we apply cohomological machinery to study the map induced on $\mathbb{Z}_\ell$-points by algebraic maps between $\mathbb{Q}$-tori with good reduction at ℓ. With more effort, the method could also give results in the bad reduction setting, but the argument would become quite cumbersome and the result would not be very satisfactory for our purposes. To remedy this situation, in Section 4 we treat the case of arbitrary reduction through a purely geometric argument inspired by [23]; it should be pointed out, however, that—in the good reduction setting— the cohomological approach gives much sharper bounds. In Section 5 we recall a form of the Fundamental Theorem of Complex Multiplication, which gives a complete description of the Galois representations attached to A, and apply it to deduce Theorem 1.3. In Section 6 we give bounds on the order of $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ under the assumption that A is of nondegenerate type, i.e., that $\mathrm{rank}\,\mathrm{MT}(A) = \dim A + 1$. Finally, in the short Section 7 we give a simple

example that shows that the optimal bound on $\ell^{n \operatorname{rank} \operatorname{MT}(A)} \big/ [K(A[\ell^n]) : K]$ grows at least exponentially fast in g, so that our bounds are not too far from the truth.

Acknowledgments. — I thank Nicolas Ratazzi for his unending support and invaluable advice. I am also grateful to Jacob Tsimerman for his help with understanding parts of his paper [23], and to the anonymous referee for their thorough reading of the manuscript.

2. Preliminaries on algebraic tori

Recall that over a perfect field k there is an equivalence of categories between algebraic tori and finitely generated, torsion-free, continuous $\operatorname{Gal}\left(\overline{k}/k\right)$-modules: if T is a k-torus, the corresponding $\operatorname{Gal}\left(\overline{k}/k\right)$-module is the group of characters $\hat{T} = \operatorname{Hom}\left(T_{\overline{k}}, \mathbb{G}_{m,\overline{k}}\right)$. Also recall that this construction extends to an equivalence between finitely generated, continuous $\operatorname{Gal}\left(\overline{k}/k\right)$-modules and k-group schemes of multiplicative type; we will make use of this fact to study the kernel of the reflex norm. We now introduce a family of $\mathbb{Q}$-algebraic tori that will be especially relevant for us:

DEFINITION 2.1. — *If E is any number field we set $T_E = \operatorname{Res}_{E/\mathbb{Q}}(\mathbb{G}_{m,\mathbb{Q}})$.*

The torus T_E is of rank $[E : \mathbb{Q}]$, and it admits a very simple description in terms of characters: it is the $\mathbb{Q}$-torus that corresponds to the free module over the set $\operatorname{Hom}(E, \overline{\mathbb{Q}})$, endowed with its natural (right) $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-action.

PROPOSITION 2.2. — *Let E be a number field. The torus T_E has good reduction at all the primes not dividing $\operatorname{disk}(E)$.*

Proof. — By the Galois criterion ([9, Proposition 1.1]), T_E has good reduction at ℓ if and only if the inertia group at (a place of $\overline{\mathbb{Q}}$ over) ℓ acts trivially on $\widehat{T_E}$. In the present case $\widehat{T_E}$ is the free module over $\operatorname{Hom}(E, \overline{\mathbb{Q}})$, so if we let L be the Galois closure of E in $\overline{\mathbb{Q}}$ the action of $\operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on $\widehat{T_E}$ factors through its finite quotient $\operatorname{Gal}(L/\mathbb{Q})$. Now if a prime ℓ is unramified in E it is also unramified in L, hence the inertia at ℓ has trivial image in $\operatorname{Gal}(L/\mathbb{Q})$ and T_E has good reduction at ℓ, as claimed. $\square$

2.1. Points of tori with values in $\mathbb{Z}_\ell$ and $\mathbb{Z}/\ell^n\mathbb{Z}$. — We briefly discuss the various possible definitions for the group of $\mathbb{Z}_\ell$-valued points of a $\mathbb{Q}_\ell$-torus; our main reference for this section is [14, §2]. Let T be a $\mathbb{Q}_\ell$-torus, not necessarily having good reduction over $\mathbb{F}_\ell$. We fix a finite Galois extension L of $\mathbb{Q}_\ell$ that splits T, and we regard $\hat{T}$ as a Γ-module, where $\Gamma := \operatorname{Gal}(L/\mathbb{Q}_\ell)$. Also notice that a character $\chi \in \hat{T}$ can in particular be considered as a homomorphism $\chi : T(L) \to L^\times$.

DEFINITION 2.3. — *Following Ono (cf. [12, §2]), we define $T(\mathbb{Z}_\ell)$ to be* $\mathrm{Hom}_\Gamma\left(\hat{T}, \mathcal{O}_L^\times\right)$, *the group of Γ-equivariant morphisms (of abelian groups) of $\hat{T}$ in $\mathcal{O}_L^\times$. Equivalently, $T(\mathbb{Z}_\ell)$ is the maximal compact subgroup of $T(\mathbb{Q}_\ell)$.*

If furthermore we suppose that T has good reduction, then it is known ([24, Theorem 2 on p.109]) that there exists a $\mathbb{Z}_\ell$-model $\mathcal{T}$ of T (that is, a commutative smooth group scheme over $\mathrm{Spec}(\mathbb{Z}_\ell)$ whose generic fiber is T). As pointed out in [14, Remark 2.2], in this case the $\mathbb{Z}_\ell$-points of T in the sense of Ono agree with the $\mathbb{Z}_\ell$-valued points of $\mathcal{T}$, so that we are free to use whichever definition we find more convenient. When a smooth model $\mathcal{T}$ exists we can also give the following definition:

DEFINITION 2.4. — *If T has good reduction, the $\mathbb{Z}/\ell^n\mathbb{Z}$-points of T are the $\mathbb{Z}/\ell^n\mathbb{Z}$-valued points of its smooth $\mathbb{Z}_\ell$-model $\mathcal{T}$.*

We still need to discuss the meaning of $T(\mathbb{Z}/\ell^n\mathbb{Z})$ when T does *not* have good reduction. The construction in this case is again due to Ono. For $n \geq 0$, we define subgroups of $T(\mathbb{Q}_\ell)$ by the rule

$$T(1 + \ell^n\mathbb{Z}_\ell) = \left\{x \in T(\mathbb{Q}_\ell) \mid v_\ell(\chi(x) - 1) \geq n \quad \forall \chi \in \hat{T}\right\}.$$

We simply write $T(\mathbb{Z}_\ell)$ for the group corresponding to $n = 0$: it can be easily checked that this definition agrees with our previous ones. We can now set $T(\mathbb{Z}/\ell^n\mathbb{Z}) = \frac{T(\mathbb{Z}_\ell)}{T(1+\ell^n\mathbb{Z}_\ell)}$; once again, when T has a smooth $\mathbb{Z}_\ell$-model $\mathcal{T}$, the group $T(\mathbb{Z}/\ell^n\mathbb{Z})$ agrees with $\mathcal{T}(\mathbb{Z}/\ell^n\mathbb{Z})$. Finally, when T is a $\mathbb{Q}$-torus we define $T(\mathbb{Z}/\ell^n\mathbb{Z})$ to be the group of $\mathbb{Z}/\ell^n\mathbb{Z}$-points of $T \otimes \mathbb{Q}_\ell$. We conclude this discussion with the following well-known lemma:

LEMMA 2.5. — *Let $T/\mathbb{Q}_\ell$ have good reduction. For every positive integer n we have*

$$(1 - 1/\ell)^{\dim T} \ell^{n \dim T} \leq |T(\mathbb{Z}/\ell^n\mathbb{Z})| \leq (1 + 1/\ell)^{\dim T} \ell^{n \dim T}.$$

Proof. —   A combination of Hensel's lemma and [24, Theorem 2 on p.104]; for further details, we refer the reader to [4, Lemme 2.1 and Proposition 2.2].   □

2.2. CM types and reflex norm. —   We briefly recall the notions of CM type, of reflex type, and of reflex norm; we refer the reader to [14, §3] for further details. Let E be a CM field of degree $2g$ and $\tilde{E}$ be its Galois closure in $\overline{\mathbb{Q}}$, and write G, H for the Galois groups $\mathrm{Gal}(\tilde{E}/\mathbb{Q})$ and $\mathrm{Gal}(\tilde{E}/E)$ respectively. We denote by τ the complex conjugation of $\mathbb{C}$, or any of its restrictions, and we take the convention that the set $\mathrm{Hom}(E, \overline{\mathbb{Q}})$ be identified with the coset space $H\backslash G$.

LEMMA 2.6. — *The degree $[\tilde{E} : \mathbb{Q}]$ divides $2^g g!$.*

Proof. — Let E_0 be the maximal totally real subfield of E and $a \in E_0$ be such that $E = E_0(\sqrt{a})$. Let $\tilde{E}_0$ be the Galois closure of E_0 and $a_1 = a, \ldots, a_k \in \tilde{E}_0$ be the conjugates of a over $\mathbb{Q}$, where $k \leq [E_0 : \mathbb{Q}] = g$. It is clear that $\tilde{E}$ is generated over $\tilde{E}_0$ by $\sqrt{a_1}, \ldots, \sqrt{a_k}$, so $[\tilde{E} : \mathbb{Q}]$ divides $[\tilde{E}_0 : \mathbb{Q}] \cdot 2^k$. As $[\tilde{E}_0 : \mathbb{Q}] \mid g!$ and $k \leq g$ the lemma follows. $\square$

DEFINITION 2.7. — *A CM-type for the CM field E is a subset S of $H \backslash G$ such that $S \cap \tau(S) = \emptyset$ and $H \backslash G = S \cup \tau(S)$.*

Let S be a CM type for E and $\tilde{S}$ be the inverse image of S in G, i.e., $\tilde{S} = \{g \in G \mid Hg \in S\}$. We set $H' = \{g \in G \mid \tilde{S}g = \tilde{S}\}$ and let E^* be the fixed field of H'; we then set $\tilde{R} = \{s^{-1} \mid s \in \tilde{S}\}$ and let R be the image of $\tilde{R}$ in $H' \backslash G \cong \mathrm{Hom}\left(E^*, \overline{\mathbb{Q}}\right)$. It is not hard to check that R is a CM type for E^*.

DEFINITION 2.8. — *The pair (E^*, R) is called the **reflex type** of (E, S).*

Finally, a CM type (E, S) is called simple if the equality

$$H = \left\{g \in G \mid g\tilde{S} = \tilde{S}\right\}$$

holds. We are now ready to define the reflex norm:

DEFINITION 2.9. — *Let (E, S) be a CM type, $\tilde{E}$ the Galois closure of $E/\mathbb{Q}$ and (E^*, R) the reflex type of (E, S). The **reflex norm** associated with (E, S) is the $\mathbb{Q}$-morphism*

$$\Phi_{(E,S)} : T_{E^*} \to T_E$$

of algebraic tori given on characters by

$$\Phi^*_{(E,S)} : \widehat{T_E} \to \widehat{T^*_E}$$
$$[g] \mapsto \sum_{r \in R}[rg],$$

where $[g]$ (resp. $[rg]$) is the embedding of E (resp. E^*) in $\overline{\mathbb{Q}}$ induced by the automorphism $g \in \mathrm{Gal}(\tilde{E}/\mathbb{Q})$ (resp. $rg \in \mathrm{Gal}(\tilde{E}/\mathbb{Q})$).

2.3. The Mumford-Tate group. — Our interest in the reflex norm stems from the fact that it allows us to define the Mumford-Tate group of a CM abelian variety rather directly. Before doing so, however, we need to recall how one associates a CM type with a CM abelian variety.

Let A/K be an absolutely simple abelian variety, admitting complex multiplication (over $\overline{K}$) by the field E. The tangent space at the identity of $A_{\overline{K}}$ is a $\overline{K}$-module and an E-module, and the two actions are compatible: it follows that this tangent space is a $(E \otimes \overline{K})$-bimodule, so it decomposes as $T_{\mathrm{id}} A_{\overline{K}} \cong \prod_{\varphi \in S} \overline{K}_\varphi$, where $\overline{K}_\varphi$ is a 1-dimensional $\overline{K}$-vector space on which E acts through the embedding $\varphi : E \hookrightarrow \overline{K}$. The set S of embeddings that appear in this decomposition can be shown to be a CM type for E, and in this case

we say that A admits complex multiplication by the CM type (E, S). When furthermore we have $\operatorname{End}_K(A) = \operatorname{End}_{\overline{K}}(A)$ we say that A admits complex multiplication by (E, S) over K.

DEFINITION 2.10. — *Let A/K be an absolutely simple abelian variety admitting complex multiplication (over $\overline{K}$) by the CM type (E, S), and let (E^*, R) be the reflex type. We define the Mumford-Tate torus $\operatorname{MT}(A)$ to be the image of the reflex norm $\Phi_{(E,S)} : T_{E^*} \to T_E$.*

REMARK 2.11. — The Mumford-Tate group of A is in fact a purely geometric object—it can described in terms of the Hodge structure associated with the complex abelian variety $A_{\mathbb{C}}$. In particular, it is insensitive to extensions of the base field K.

REMARK 2.12. — It is known that the rank of $\operatorname{MT}(A)$ is at most $g + 1$. When equality holds, the CM type is said to be nondegenerate, and the Mumford-Tate group has a very simple description in terms of E: if τ denotes complex conjugation on E, for any $\mathbb{Q}$-algebra B the B-points of $\operatorname{MT}(A)$ are given by

$$\operatorname{MT}(A)(B) = \left\{ x \in (E \otimes_{\mathbb{Q}} B)^{\times} \mid x\tau(x) \in B^{\times} \right\}.$$

For all these facts see for example [14], Proposition 3.3 and the remarks following it.

2.4. The group of connected components of $\ker \Phi_{(E,S)}$. — An object which will be crucial to our study is the kernel of the reflex norm $\Phi_{(E,S)}$: in this short subsection we establish a bound on the order of its group of components. The bound is ultimately a consequence of Hadamard's inequality, which is the main tool used to establish the following lemma:

LEMMA 2.13. — *Let A be a $n \times n$ integral matrix all of whose entries are in $\{0, 1\}$. The following inequality holds:*

$$|\det A| \le \lfloor 2^{-n}(n + 1)^{(n+1)/2} \rfloor.$$

Proof. — Consider the matrix

$$B(A) = \begin{pmatrix} 1 & 1 \cdots 1 \\ \hline 0 & \\ \vdots & 2A \\ 0 & \end{pmatrix}.$$

It is clear by definition that $\det B(A) = 2^n \det(A)$. Consider the matrix $H(A)$ obtained from $B(A)$ by subtracting the first row to each of the others. Clearly $H(A)$ and $B(A)$ have the same determinant, and furthermore all the

entries of $H(A)$ are in $\{\pm 1\}$. In particular, the L^2-norm of every row of $H(A)$ is $\sqrt{n+1}$, so Hadamard's inequality implies

$$|\det A| = 2^{-n}|\det B(A)| = 2^{-n}|\det H(A)| \leq 2^{-n}(n+1)^{(n+1)/2}.$$

The claim then follows from the fact that $\det(A)$ is an integer. $\qquad\square$

LEMMA 2.14. — *Let $T : \mathbb{Z}^n \to \mathbb{Z}^m$ be a linear map, represented in the standard bases by a matrix A all of whose entries are in $\{0,1\}$. Let Y be the image of T, denote by k the rank of Y, and let Z be given by*

$$Z = \left\{ z \in \mathbb{Z}^m \mid \exists q \in \mathbb{Z} \text{ such that } qz \text{ belongs to } Y \right\}.$$

The quotient Z/Y, which is isomorphic to the torsion part of $\mathbb{Z}^m/Y$, has order at most $\lfloor 2^{-k}(k+1)^{(k+1)/2} \rfloor$.

Proof. — The order of Z/Y is given by

$$\gcd\left\{ \det(A_k) \mid A_k \text{ is a minor of } A \text{ of size } k \right\}.$$

Lemma 2.13 ensures that the determinant of every minor of size k does not exceed $\lfloor 2^{-k}(k+1)^{(k+1)/2} \rfloor$, and the lemma follows. $\qquad\square$

PROPOSITION 2.15. — *Let C be the group of multiplicative type defined by the exact sequence*

$$1 \to C \to T_{E^*} \xrightarrow{\Phi_{(E,S)}} \mathrm{MT}(A) \to 1$$

and let $\hat{C}$ be its character group. Suppose $\mathrm{MT}(A)$ has rank r. The torsion subgroup of $\hat{C}$ has order at most $\lfloor 2^{-r}(r+1)^{(r+1)/2} \rfloor$.

Proof. — Let Y be the image of $\Phi^*_{(E,S)} : \hat{T}_E \to \hat{T}_{E^*}$ and

$$Z = \left\{ \chi \in \hat{T}_{E^*} \mid \exists n \in \mathbb{Z} \text{ such that } n\chi \in Y \right\}.$$

The torsion subgroup of $\hat{C}$ is isomorphic to Z/Y. Moreover, it is apparent from Definition 2.9 that the matrix representing $\Phi^*_{(E,S)}$ in the natural bases of $\widehat{T_{E^*}}, \widehat{T_E}$ has entries in $\{0,1\}$, so the proposition follows from Lemma 2.14. $\quad\square$

3. Cohomology and integral points of tori

The purpose of this section is to study the map induced on $\mathbb{Z}_\ell$-points by a surjection of tori over $\mathbb{Q}_\ell$. More precisely, we let $T \xrightarrow{\beta} T'' \to 1$ be a surjection of $\mathbb{Q}_\ell$-algebraic tori, and we assume that T has good reduction. We let T' be the kernel of β, which is in general just a group of multiplicative type (and not necessarily a torus), and write F for the torsion subgroup of its character group $\hat{T}'$. We also denote by a the rank of T', so that we have an isomorphism of abelian groups $\hat{T}'/F \cong \mathbb{Z}^a$. Finally, we fix a finite *unramified* Galois extension

L of $\mathbb{Q}_\ell$ that splits T, and we let Γ denote the Galois group of L over $\mathbb{Q}_\ell$. It is also useful to introduce the following notation:

Notation. If n is any integer and ℓ is a prime we write $|n|_\ell$ for $\ell^{-v_\ell(n)}$. When M is a finite group we also write $|M|_\ell$ for $\ell^{-v_\ell(|M|)}$.

With this notation we shall show:

PROPOSITION 3.1. — *The cokernel of* $T(\mathbb{Z}_\ell) \xrightarrow{\ \beta\ } T''(\mathbb{Z}_\ell)$ *has order dividing* $|F| \cdot |F|_\ell^{-[L:\mathbb{Q}_\ell]}$.

The proof is given below in §3.2, and relies mainly on the basic tools of Galois cohomology, together with the following classical theorem of Nakayama (cf. for example [20, §2, Theorem 32]):

THEOREM 3.2. — *Let A and B be modules over the finite group G. Assume that A is cohomologically trivial. In order for $\mathrm{Hom}(B, A)$ to be cohomologically trivial it is necessary and sufficient that $\mathrm{Ext}^1(B, A)$ be cohomologically trivial. In particular, if B is $\mathbb{Z}$-free, then $\mathrm{Hom}(B, A)$ is cohomologically trivial.*

3.1. Preliminaries on p-adic fields. — The following two lemmas are certainly well-known, but for lack of an easily accessible reference we prefer to include a short proof.

LEMMA 3.3. — *Let L be a finite extension of $\mathbb{Q}_\ell$ with ring of integers $\mathcal{O}_L$, and let n be a positive integer. The quotient $\mathcal{O}_L/\mathcal{O}_L^{\times n}$ has order dividing $n \cdot |n|_\ell^{-[L:\mathbb{Q}_\ell]}$.*

Proof. — We regard all the involved groups as $\mathbb{Z}/n\mathbb{Z}$-modules with trivial action, and denote by h_n the associated Herbrand quotient, that is to say for every finite $\mathbb{Z}/n\mathbb{Z}$-module M we set

$$h_n(M) := \frac{|\hat{H}^0(\mathbb{Z}/n\mathbb{Z}, M)|}{|H^1(\mathbb{Z}/n\mathbb{Z}, M)|}.$$

As $\mathcal{O}_L^1$, the subgroup of principal units of $\mathcal{O}_L$, has finite index in $\mathcal{O}_L^\times$ (and the Herbrand quotient is invariant by passage to finite-index subgroups), we have $h_n(\mathcal{O}_L^\times) = h_n(\mathcal{O}_L^1)$.

On the other hand, $\mathcal{O}_L^1$ contains a subgroup of finite index that is isomorphic to $\mathcal{O}_L$ ([16, Chapitre XIV, prop. 10]), so $h_n(\mathcal{O}_L^\times) = h_n(\mathcal{O}_L^1) = h_n(\mathcal{O}_L)$. Furthermore, $H^1(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_L^\times) = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_L^\times) = \mathcal{O}_L^\times[n]$ has order dividing n, while $H^1(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_L) = \mathcal{O}_L[n] = 0$. The lemma then follows easily because the quantity $\left|\frac{\mathcal{O}_L^\times}{\mathcal{O}_L^{\times n}}\right| = h^1(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_L^\times) \cdot h_n(\mathcal{O}_L^\times)$ divides

$$n \cdot h_n(\mathcal{O}_L) = n \frac{|\mathcal{O}_L/n\mathcal{O}_L|}{h^1(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_L)} = n \cdot |n|_\ell^{-[L:\mathbb{Q}_\ell]}. \qquad \square$$

LEMMA 3.4. — *Let F be a finite abelian group and L be a finite extension of $\mathbb{Q}_\ell$. Then $|\mathrm{Ext}^1(F, \mathcal{O}_L^\times)|$ divides $|F| \cdot |F|_\ell^{-[L:\mathbb{Q}_\ell]}$.*

Proof. —   Writing F as $\bigoplus_i \frac{\mathbb{Z}}{d_i\mathbb{Z}}$ we have

$$\text{Ext}^1\left(F, \mathcal{O}_L^\times\right) \cong \prod_i \text{Ext}^1\left(\frac{\mathbb{Z}}{d_i\mathbb{Z}}, \mathcal{O}_L^\times\right) \cong \prod_i \frac{\mathcal{O}_L^\times}{\mathcal{O}_L^{\times d_i}}.$$

The result follows from the previous lemma.   □

3.2. Proof of Proposition 3.1. —   Note that—since $L/\mathbb{Q}_\ell$ is unramified—the group $\mathcal{O}_L^\times$ is a cohomologically trivial Γ-module (cf. for example [11, Prop. 7.1.2 (i)]). As $\hat{T}$ and $\hat{T}''$ are free abelian groups, Nakayama's theorem implies in particular that $\text{Hom}\left(\hat{T}, \mathcal{O}_L^\times\right)$ and $\text{Hom}\left(\hat{T}'', \mathcal{O}_L^\times\right)$ are cohomologically trivial Γ-modules. We will make extensive use of this fact. The character groups of T, T', T'' fit into an exact sequence

$$0 \to \hat{T}'' \to \hat{T} \to \hat{T}' \to 0;$$

applying the functor $\text{Hom}\left(-, \mathcal{O}_L^\times\right)$ gives another exact sequence

$$0 \to \text{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right) \to \text{Hom}\left(\hat{T}, \mathcal{O}_L^\times\right)$$
$$\to \text{Hom}\left(\hat{T}'', \mathcal{O}_L^\times\right) \to \text{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right) \to 0,$$

where the following Ext term vanishes since $\hat{T}$ is free. If we let

$$I := \text{Image}\left(\text{Hom}\left(\hat{T}, \mathcal{O}_L^\times\right) \to \text{Hom}\left(\hat{T}'', \mathcal{O}_L^\times\right)\right),$$

the previous sequence gives rise to the two exact sequences

(1) $$0 \to \text{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right) \to \text{Hom}\left(\hat{T}, \mathcal{O}_L^\times\right) \to I \to 0$$

and

(2) $$0 \to I \to \text{Hom}\left(\hat{T}'', \mathcal{O}_L^\times\right) \to \text{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right) \to 0.$$

The long exact sequences in Galois cohomology associated with (1) and (2) give

(3)
$$0 \to \text{Hom}_\Gamma\left(\hat{T}', \mathcal{O}_L^\times\right) \to T(\mathbb{Z}_\ell) \to H^0(\Gamma, I) \to H^1\left(\Gamma, \text{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \to 0,$$

(4) $$0 \to H^1(\Gamma, I) \to H^2\left(\Gamma, \text{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \to 0,$$

and

(5) $$0 \to H^0(\Gamma, I) \to T''(\mathbb{Z}_\ell) \to H^0\left(\Gamma, \text{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \to H^1(\Gamma, I) \to 0,$$

where we have used the fact that $\text{Hom}\left(\hat{T}, \mathcal{O}_L^\times\right)$ and $\text{Hom}\left(\hat{T}'', \mathcal{O}_L^\times\right)$ are cohomologically trivial. Also notice that we have an exact sequence of Γ-modules

(6) $$0 \to F \to \hat{T}' \to \hat{T}'/F \to 0$$

where $\hat{T}'/F \cong \mathbb{Z}^a$ is free. We can then apply $\mathrm{Hom}\left(-, \mathcal{O}_L^\times\right)$ to (6) to get

$$0 \to \mathrm{Hom}\left(\hat{T}'/F, \mathcal{O}_L^\times\right) \to \mathrm{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right) \to \mathrm{Hom}\left(F, \mathcal{O}_L^\times\right) \to 0,$$

and since $\mathrm{Hom}\left(\hat{T}'/F, \mathcal{O}_L^\times\right)$ is again cohomologically trivial by Theorem 3.2 we deduce that for every $n \geq 1$ we have canonical isomorphisms

(7)
$$H^n\left(\Gamma, \mathrm{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \xrightarrow{\sim} H^n\left(\Gamma, \mathrm{Hom}\left(F, \mathcal{O}_L^\times\right)\right).$$

Straightforward manipulations of sequences (3) and (5) show that

$$|\mathrm{coker}\left(T(\mathbb{Z}_\ell) \to T''(\mathbb{Z}_\ell)\right)| = \frac{h^0\left(\Gamma, \mathrm{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \cdot h^1\left(\Gamma, \mathrm{Hom}\left(\hat{T}', \mathcal{O}_L^\times\right)\right)}{h^1(\Gamma, I)}.$$

For the sake of notational simplicity set $M = \mathrm{Hom}\left(F, \mathcal{O}_L^\times\right)$. Using (4) and (7) we arrive at

(8)
$$|\mathrm{coker}\left(T(\mathbb{Z}_\ell) \to T''(\mathbb{Z}_\ell)\right)| = \frac{h^0\left(\Gamma, \mathrm{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right) \cdot h^1\left(\Gamma, M\right)}{h^2(\Gamma, M)}.$$

Observe now that the group Γ is cyclic (since it is the Galois group of an unramified extension) and the module M is finite: as it is well-known, the Tate cohomology $\hat{H}^n$ of a cyclic group with values in a finite module is 2-periodic in n. Moreover, the Herbrand quotient $\frac{|\hat{H}^0(\Gamma, M)|}{|\hat{H}^1(\Gamma, M)|}$ equals 1 since M is finite, and therefore $h^2(\Gamma, M) = \left|\hat{H}^0(\Gamma, M)\right| = h^1(\Gamma, M)$ (for all these facts cf. for example [11, §I.7]). Using this equality in (8) we finally find $|\mathrm{coker}\left(T(\mathbb{Z}_\ell) \to T''(\mathbb{Z}_\ell)\right)| = h^0\left(\Gamma, \mathrm{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right)$. Proposition 3.1 then follows from the fact that $h^0\left(\Gamma, \mathrm{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right)$ divides

$$\left|\mathrm{Ext}^1\left(\hat{T}', \mathcal{O}_L^\times\right)\right| = \left|\mathrm{Ext}^1\left(\mathbb{Z}^a \oplus F, \mathcal{O}_L^\times\right)\right| = \left|\mathrm{Ext}^1\left(F, \mathcal{O}_L^\times\right)\right|$$

and from Lemma 3.4.

4. The cokernel of an isogeny, without the good reduction assumption

Let T, T' be $\mathbb{Q}_\ell$-tori and $\lambda : T \to T'$ be a $\mathbb{Q}_\ell$-isogeny. We do not assume that T or T' has good reduction, and for the purposes of this section we define the $\mathbb{Z}_\ell$-points of a $\mathbb{Q}_\ell$-torus to be the maximal compact subgroup of $T(\mathbb{Q}_\ell)$ (cf. Definition 2.3). Our aim is again to bound the order of $\mathrm{coker}\left(T(\mathbb{Z}_\ell) \xrightarrow{\lambda} T'(\mathbb{Z}_\ell)\right)$, in terms of the degree m of λ and of $\dim T = \dim T' =: d$. Cohomological tools could again be used to investigate the problem, but we find that an entirely different approach (through p-adic differential geometry) yields simpler and more

effective proofs; the method is inspired by [23], see especially Lemma 4.4 in *op. cit.*

PROPOSITION 4.1. — *Let T, T' be $\mathbb{Q}_\ell$-tori of dimension d and $\lambda : T \to T'$ be an isogeny of degree m. The order of* coker $\left(T(\mathbb{Z}_\ell) \xrightarrow{\lambda} T'(\mathbb{Z}_\ell) \right)$ *is at most $m^d \cdot |m|_\ell^{-d}$.*

Proof. — Notice first that λ fits into a commutative diagram

$$T'(\mathbb{Z}_\ell) - - - - \overset{\lambda^\vee}{- - - - -} \to T(\mathbb{Z}_\ell)$$

$$[m] \searrow \qquad \swarrow \lambda$$

$$T'(\mathbb{Z}_\ell)$$

and therefore it is enough to bound the cokernel of $[m] : T'(\mathbb{Z}_\ell) \to T'(\mathbb{Z}_\ell)$. Fix now a Haar measure μ on $T'(\mathbb{Q}_\ell)$, normalized in such a way that $\mu(T'(\mathbb{Z}_\ell)) = 1$.

Consider the kernel K of $[m]$ (as a subgroup of $T'(\mathbb{Z}_\ell)$, not as a group scheme) and the quotient $S = T'(\mathbb{Z}_\ell)/K$, and note that $\pi : T'(\mathbb{Z}_\ell) \to S$ is a covering map. We denote by μ_S the measure on S given by $\mu_S(A) = \frac{1}{|K|}\mu\left(\pi^{-1}(A)\right)$: it can also be interpreted as the measure induced on S by the (Haar) volume form of $T'(\mathbb{Z}_\ell)$, which passes to the quotient since it is translation-invariant. The volume of S (for the measure μ_S) is $\frac{\text{vol}(T'(\mathbb{Z}_\ell))}{|K|} = \frac{1}{|K|}$, and we have an ℓ-adic analytic map $q : S \to T'(\mathbb{Z}_\ell)$ such that the following diagram commutes:

$$T'(\mathbb{Z}_\ell) \xrightarrow{\quad [m] \quad} T'(\mathbb{Z}_\ell)$$

$$\pi \searrow \qquad \nearrow q$$

$$S.$$

Clearly q is an ℓ-adic analytic embedding and we have Image q = Image$[m] =: I$. We have the following immediate equality:

$$(9) \qquad \text{vol}(I) = \frac{1}{|T'(\mathbb{Z}_\ell)/I|} \text{vol}\left(T'(\mathbb{Z}_\ell)\right) = \frac{1}{|T'(\mathbb{Z}_\ell)/I|}.$$

On the other hand, a simple computation in coordinates shows $q^*\mu = |m|_\ell^d \, \mu_S$: we can parametrize a neighborhood of $g \in T'(\mathbb{Z}_\ell)$ by $x \mapsto g \exp(x)$ (for x varying in some small neighborhood of 0 in the Lie algebra of $T'(\mathbb{Q}_\ell)$), and composing with π this also induces a parametrization of a neighborhood of $\pi(g) \in S$. In these coordinates the map q is simply multiplication by m, so its Jacobian determinant is $|m|_\ell^d$ and the change of variables formula for ℓ-adic integration gives the required result. This yields

$$\text{vol}(I) = \int_I d\mu = \int_{q(S)} d\mu = \int_S d(q^*\mu) = \int_S |m|_\ell^d \, d\mu_S = |m|_\ell^d \frac{1}{|K|},$$

and comparing this equality with Equation (9) gives

$$\left| \operatorname{coker} \left(T'(\mathbb{Z}_\ell) \xrightarrow{[m]} T'(\mathbb{Z}_\ell) \right) \right| = |T'(\mathbb{Z}_\ell)/I| = \frac{1}{\operatorname{vol}(I)} = \frac{|K|}{|m|_\ell^d}.$$

Finally, it is clear that $|K| \le \left| T'(\overline{\mathbb{Q}_\ell})[m] \right| = m^d$, and this finishes the proof. □

5. Description of the Galois representation

Let A/K be an absolutely simple g-dimensional CM abelian variety admitting complex multiplication (over K) by the CM type (E, S). Let $\tilde{E}$ be the Galois closure of E, denote by (E^*, R) the reflex type of (E, S), and let ℓ be a prime number. It is known that—since the action of E is defined over K—the reflex field E^* is contained in K ([6, Chap. 3, Theorem 1.1]), and by [19, Corollary 2 to Theorem 5], the ℓ-adic Galois representation attached to A can be viewed as a map

$$\rho_{\ell^\infty} : \operatorname{Gal}\left(\overline{K}/K \right) \to \left(\operatorname{End}_K(A) \otimes \mathbb{Z}_\ell \right)^\times \hookrightarrow \left(\mathcal{O}_E \otimes \mathbb{Z}_\ell \right)^\times.$$

We denote by G_{ℓ^∞} the image of ρ_{ℓ^∞}. We now recall the description of ρ_{ℓ^∞} coming from the fundamental theorem of complex multiplication, and refer the reader to [14, §4] and [19] for further details. Let I_K be the group of idèles of K. As $(\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times$ is commutative, there is a factorization

$$
\begin{array}{ccc}
I_K \longrightarrow & \operatorname{Gal}\left(\overline{K}/K \right)^{ab} & \dashrightarrow \left(\mathcal{O}_E \otimes \mathbb{Z}_\ell \right)^\times \\
& \uparrow \quad \nearrow_{\rho_{\ell^\infty}} & \\
& \operatorname{Gal}\left(\overline{K}/K \right), &
\end{array}
$$

which (by class field theory) allows us to regard ρ_{ℓ^∞} as a map from I_K to $(\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times$. Let us introduce some notation: we write $\mu(E)$ for the group of roots of unity in E, and if v is a place of K we write $\mathcal{O}_{K,v}$ for the completion at v of the ring of integers of K. If v is furthermore finite we denote by p_v its residual characteristic; we also let Ω_K be the set of all finite places of K. If F is a number field we denote by F_ℓ the algebra $F \otimes \mathbb{Q}_\ell$, and for an idèle $a \in I_K$ we write a_ℓ for the component of a in $K_\ell \cong \prod_{p_v = \ell} K_v^\times$. With this notation, the map ρ_{ℓ^∞} is described very precisely by the following theorem:

THEOREM 5.1. — ([19, Theorems 6, 10 and 11]) *There exists a unique continuous homomorphism* $\varepsilon : I_K \to E^\times$ *such that, for all finite places v of K, the group* $\varepsilon\left(\mathcal{O}_{K,v}^\times \right)$ *is contained in $\mu(E)$, and*

$$\rho_{\ell^\infty}(a) = \varepsilon(a) \Phi_{(E,S)} \left(N_{K_\ell/E_\ell^*}(a_\ell) \right)^{-1}$$

for all $a \in I_K$. If furthermore $v \in \Omega_K$ is a place of good reduction for A, then $\varepsilon \left(\mathcal{O}_{K,v}^\times \right)$ is trivial.

We now consider the restriction of ρ_{ℓ^∞} to $K^\times \cdot \prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$: as it is well-known (cf. for example [10, Proposition 2.3]), this is the group of idèles of H, the Hilbert class field of K. In terms of Galois groups, this has the effect of restricting ρ_{ℓ^∞} to $\mathrm{Gal}\left(\overline{H}/H\right) \subseteq \mathrm{Gal}\left(\overline{K}/K\right)$, so it is clear that $\rho_{\ell^\infty}\left(\mathrm{Gal}\left(\overline{H}/H\right)\right)$ is a subgroup of $\rho_{\ell^\infty}\left(\mathrm{Gal}\left(\overline{K}/K\right)\right)$ of index dividing $h(K)$, the class number of K. Now as ρ_{ℓ^∞} factors through $\mathrm{Gal}\left(\overline{K}/K\right)$ we see that $\rho_{\ell^\infty}(K^\times)$ is trivial, so we can just consider the restriction of ρ_{ℓ^∞} to $\prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$. We now remark that for an idèle $(a_v) \in \prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$ Theorem 5.1 implies

$$\varepsilon(a) = \prod_{v \in \Omega_K} \varepsilon\left(a_v\right) = \prod_{\substack{v : A \text{ has bad} \\ \text{reduction at v}}} \varepsilon(a_v) \in \mu(E),$$

whence $J := \ker \varepsilon \cap \prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$ has index dividing $|\mu(E)|$ in $\prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$, and likewise the index of $J_\ell := \ker \varepsilon \cap \prod_{v | \ell} \mathcal{O}_{K,v}^\times$ in $\prod_{v | \ell} \mathcal{O}_{K,v}^\times$ divides $|\mu(E)|$. Furthermore, since the function $a \mapsto \Phi_{(E,S)}\left(N_{K_\ell/E_\ell^*}(a_\ell)\right)^{-1}$ kills $\mathcal{O}_{K,v}^\times$ when $p_v \neq \ell$, we have $\rho_{\ell^\infty}(J) = \rho_{\ell^\infty}(J_\ell)$. Also notice that, upon restriction to J_ℓ, the representation ρ_{ℓ^∞} coincides with the map

$$\begin{aligned} \varphi_{\ell^\infty} : \prod_{v|\ell} \mathcal{O}_{K,v}^\times &\to \quad \left(\mathcal{O}_E \otimes \mathbb{Z}_\ell\right)^\times \\ a &\mapsto \Phi_{(E,S)}\left(N_{K_\ell/E_\ell^*}(a)\right)^{-1}, \end{aligned}$$

and that if A has good reduction at v, then ρ_{ℓ^∞} and φ_{ℓ^∞} coincide on all of $\prod_{v|\ell} \mathcal{O}_{K,v}^\times$. For the sake of notational simplicity let us then set

$$\mu^* = \begin{cases} |\mu(E)| & \text{if } A \text{ has bad reduction at some place } v \text{ of characteristic } \ell, \\ 1 & \text{otherwise.} \end{cases}$$

We have proved:

PROPOSITION 5.2. — *For all primes ℓ the group G_{ℓ^∞} contains $\rho_{\ell^\infty}\left(J_\ell\right)$ as a subgroup of index dividing $|\mu(E)| \cdot h(K)$. We have $\rho_{\ell^\infty}\left(J_\ell\right) = \varphi_{\ell^\infty}\left(J_\ell\right)$, and if A has good reduction at all places v of characteristic ℓ we have $J_\ell = \prod_{v|\ell} \mathcal{O}_{K,v}^\times$. Finally,*

$$(10) \qquad \left[\varphi_{\ell^\infty}\left(\prod_{v|\ell} \mathcal{O}_{K,v}^\times\right) : \rho_{\ell^\infty}\left(J_\ell\right)\right] \mid \mu^*.$$

We can now interpret φ_{ℓ^∞} as a map between algebraic tori: indeed, the norm N_{K/E^*} can be seen as a morphism $T_K \to T_{E^*}$, and $\prod_{v|\ell} \mathcal{O}_{K,v}^\times$ is nothing

but $T_K(\mathbb{Z}_\ell)$, so the map φ_{ℓ^∞} is simply the map induced on $\mathbb{Z}_\ell$-points by

$$\left(\Phi_{(E,S)}\right)^{-1} \circ N_{K/E^*} : T_K \to \mathrm{MT}(A);$$

together with the previous proposition, this implies in particular that $\rho_{\ell^\infty}(J_\ell) = \varphi_{\ell^\infty}(J_\ell)$ is contained in $\mathrm{MT}(A)(\mathbb{Z}_\ell)$, and that $\varphi_{\ell^\infty}(J_\ell)$ has index at most μ^* in $\varphi_{\ell^\infty}(T_K(\mathbb{Z}_\ell))$. We thus want to understand the composition

$$T_K(\mathbb{Z}_\ell) \xrightarrow{N_{K/E^*}} T_{E^*}(\mathbb{Z}_\ell) \xrightarrow{\psi_\ell} \mathrm{MT}(A)(\mathbb{Z}_\ell),$$

where for simplicity of notation we write ψ_ℓ for the base-change to $\mathbb{Q}_\ell$ of the map $\left(\Phi_{(E,S)}(\cdot)\right)^{-1}$. Even though the extension K/E^* is in general non-abelian, the cokernel of N_{K/E^*} can be understood through class field theory:

THEOREM 5.3. — ([1, Theorem 7 on p. 161]) *Let L/M be an extension of local fields, and let L_{ab} be the largest abelian subextension of L/M. Then we have $N_{L/M}L^\times = N_{L_{ab}/M}\left(L_{ab}^\times\right)$, and the cokernel $\frac{M^\times}{N_{L/M}L^\times}$ has order dividing $[L : M]$.*

Note that the image of ψ_ℓ is open and $\mathrm{MT}(A)(\mathbb{Z}_\ell)$ is compact, so the cokernel of $\psi_\ell : T_{E^*}(\mathbb{Z}_\ell) \xrightarrow{\psi_\ell} \mathrm{MT}(A)(\mathbb{Z}_\ell)$ is finite; since furthermore by Theorem 5.3 $\left|\frac{T_{E^*}(\mathbb{Z}_\ell)}{N_{K/E^*}(T_K(\mathbb{Z}_\ell))}\right|$ divides $[K : E^*]$ we find that

$$(11) \qquad [\mathrm{MT}(A)(\mathbb{Z}_\ell) : \varphi_{\ell^\infty}(T_K(\mathbb{Z}_\ell))] \text{ divides } [K : E^*] \cdot \left|\frac{\mathrm{MT}(A)(\mathbb{Z}_\ell)}{\psi_\ell(T_{E^*}(\mathbb{Z}_\ell))}\right|.$$

REMARK 5.4. — When ℓ is unramified in K the local norm $T_K(\mathbb{Z}_\ell) \to T_{E^*}(\mathbb{Z}_\ell)$ is surjective and the factor $[K : E^*]$ can be omitted, cf. [16, Corollary to Proposition 3 of Chapter V].

It is clear that $\psi_\ell = \Phi_{(E,S)}^{-1}$ and $\Phi_{(E,S)}$ have the same cokernel, so ultimately we just need to compute the cokernel of the reflex norm. Denote by T' the kernel of $\Phi_{(E,S)}$ and write F for the torsion of its character group $\widehat{T'}$. By Proposition 2.15 we have $|F| \leq \lfloor 2^{-r}(r+1)^{(r+1)/2}\rfloor$, where $r = \dim \mathrm{Im}\,\Phi_{(E,S)}^* = \mathrm{rk}\,\mathrm{MT}(A)$ does not exceed $g+1$. Set now $T = T_{E^*} \otimes \mathbb{Q}_\ell$ and $T'' = \mathrm{MT}(A) \otimes \mathbb{Q}_\ell$, and let L be one of the fields appearing in the decomposition of $\tilde{E} \otimes \mathbb{Q}_\ell$ as a direct sum of fields: $L/\mathbb{Q}_\ell$ is then a finite Galois extension that splits T (recall that $\tilde{E}$ is Galois and contains E^*). If ℓ is unramified in E (hence in $\tilde{E}$) the extension $L/\mathbb{Q}_\ell$ is itself unramified, so T has good reduction over $\mathbb{Q}_\ell$; furthermore, $[L : \mathbb{Q}_\ell] \mid [\tilde{E} : \mathbb{Q}] \mid 2^g \cdot g!$ (cf. Lemma 2.6).

Applying Proposition 3.1 to the surjection of algebraic tori $T \xrightarrow{\Phi_{(E,S)}} T''$ we find that

$$(12) \qquad \left|\mathrm{coker}\left(T_{E^*}(\mathbb{Z}_\ell) \xrightarrow{\Phi_{(E,S)}} \mathrm{MT}(A)(\mathbb{Z}_\ell)\right)\right| \text{ divides } |F| \cdot |F|_\ell^{-[L:\mathbb{Q}_\ell]},$$

and the right hand side in turn divides $|F| \cdot |F|_\ell^{-2^g g!}$; we have thus almost completely established the following result:

THEOREM 5.5. — *(Theorem 1.3) Let A/K be an absolutely simple abelian variety of dimension g admitting complex multiplication over K by the CM type (E, S), and let ℓ be a prime number. If A has bad reduction at a place of K dividing ℓ let $\mu^* = |\mu(E)|$, the number of roots of unity in E; if on the contrary A has good reduction at all places of K of characteristic ℓ set $\mu^* = 1$. Denote by r the rank of $\mathrm{MT}(A)$ and by F the group of connected components of the kernel of the reflex norm $T_{E^*} \to T_E$, where E^* is the reflex field of E. Then:*

(1) *The index $[G_{\ell^\infty} : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ does not exceed $|\mu(E)| \cdot h(K)$, where $h(K)$ is the class number of K.*
(2) *We have $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)] \leq \mu^* \cdot [K : E^*] \cdot |F|^{2r}$.*
(3) *If ℓ is unramified in E and does not divide $|F|$, then the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ divides $\mu^* \cdot [K : E^*] \cdot |F|$. If ℓ is also unramified in K, the bound can be improved to $\mu^* \cdot |F|$.*

Finally we have $r \leq g + 1$ and $|F| \leq f(r) \leq f(g + 1)$, where

$$f(x) = \left\lfloor 2 \left(\frac{x+1}{4} \right)^{(x+1)/2} \right\rfloor .$$

Proof. — We have already proved (1): the intersection $G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)$ contains $\varphi_{\ell^\infty}(J_\ell) = \rho_{\ell^\infty}(J_\ell)$, and by Proposition 5.2 the group $\varphi_{\ell^\infty}(J_\ell)$ has index at most $|\mu(E)| \cdot h(K)$ in G_{ℓ^∞}. As for part (2), the exact sequence

$$1 \to T' \to T_{E^*} \otimes \mathbb{Q}_\ell \to \mathrm{MT}(A) \otimes \mathbb{Q}_\ell \to 1$$

induces, by quotienting out by $(T')^0$ (the connected component of the identity of T'), the exact sequence

$$1 \to \mathcal{F} \to \frac{T_{E^*} \otimes \mathbb{Q}_\ell}{(T')^0} \xrightarrow{\tau_\ell} \mathrm{MT}(A) \otimes \mathbb{Q}_\ell \to 1,$$

where $\mathcal{F}$ is a finite group scheme of order $|F|$. Proposition 4.1 implies

$$\left| \frac{\mathrm{MT}(A)(\mathbb{Z}_\ell)}{\psi_\ell (T_{E^*}(\mathbb{Z}_\ell))} \right| = \left| \mathrm{coker} \left(\tau_\ell : \frac{T_{E^*} \otimes \mathbb{Q}_\ell}{(T')^0}(\mathbb{Z}_\ell) \to \mathrm{MT}(A)(\mathbb{Z}_\ell) \right) \right|$$
$$\leq |\deg(\tau_\ell)|^{\dim \mathrm{MT}(A)} |\deg(\tau_\ell)|_\ell^{-\dim \mathrm{MT}(A)}$$
$$= |F|^{\dim \mathrm{MT}(A)} |F|_\ell^{-\dim \mathrm{MT}(A)},$$

which, together with Equations (10) and (11), gives the desired result. Finally, consider part (3). As $\rho_{\ell^\infty}(J_\ell)$ is a subgroup of $\mathrm{MT}(A)(\mathbb{Z}_\ell)$ the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ divides $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : \rho_{\ell^\infty}(J_\ell)]$, and we can

write

$$\left| \frac{\mathrm{MT}(A)(\mathbb{Z}_\ell)}{\rho_{\ell^\infty}(J_\ell)} \right| \Big| \ \mu^* \cdot [\mathrm{MT}(A)(\mathbb{Z}_\ell) : \varphi_{\ell^\infty}(T_K(\mathbb{Z}_\ell))] \qquad\qquad (\text{by } (10))$$

$$\Big| \ \mu^* \cdot [K : E^*] \cdot |\mathrm{coker}\,(\psi_\ell : T_{E^*}(\mathbb{Z}_\ell) \to \mathrm{MT}(A)(\mathbb{Z}_\ell))| \quad (\text{by } (11))$$

$$\Big| \ \mu^* \cdot [K : E^*] \cdot |F| \cdot |F|_\ell^{-2^g g!}. \qquad\qquad\qquad\qquad (\text{by } (12))$$

Since by assumption ℓ does not divide $|F|$ we conclude that the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)]$ divides $\mu^* \cdot [K : E^*] \cdot |F|$. Finally, when ℓ is unramified in K the factor $[K : E^*]$ can be omitted, cf. Remark 5.4. $\qquad\square$

Starting from Equations (11) and (12) it is also easy to prove the following result, which might have some independent interest:

PROPOSITION 5.6. — *(Proposition 1.6) Let A/K be an absolutely simple abelian variety admitting complex multiplication (over K) by the CM field E, and let ℓ be a prime unramified in E. Let E^* be the reflex field of E and suppose that A has good reduction at all places of K of characteristic ℓ.*

- *The index $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)]$ divides $[K : E^*] \cdot |F|$.*
- *If ℓ is also unramified in K, then $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)]$ divides $|F|$.*

Proof. — By Proposition 2.2 the hypothesis implies that T_{E^*} has good reduction at ℓ, hence the same is true for its quotient $\mathrm{MT}(A)$, which therefore defines a torus over $\mathbb{F}_\ell$: in particular, the group $\mathrm{MT}(A)(\mathbb{F}_\ell)$ makes sense and its order is not divisible by ℓ. On the other hand, the index of $G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)$ in $\mathrm{MT}(A)(\mathbb{F}_\ell)$ divides $[K : E^*] \cdot |F| \cdot |F|_\ell^{-2^g g!}$ by Proposition 5.2 and Equations (11) and (12), and since $|\mathrm{MT}(A)(\mathbb{F}_\ell)|$ is prime to ℓ we deduce that $[\mathrm{MT}(A)(\mathbb{F}_\ell) : G_\ell \cap \mathrm{MT}(A)(\mathbb{F}_\ell)]$ divides $[K : E^*] \cdot |F|$ as claimed. The second part follows by the same argument using Remark 5.4. $\qquad\square$

6. The Mumford-Tate group in the nondegenerate case

In this section we consider CM abelian varieties A with nondegenerate CM type, that is to say we assume that $\mathrm{rank}(\mathrm{MT}(A)) = \dim A + 1$: this is the "generic" case, and it is also known that all simple CM varieties of prime dimension have nondegenerate CM type (a result due to Ribet, cf. [15]). In this situation we have the following bounds on the order of $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$:

THEOREM 6.1. — *Suppose A is simple of nondegenerate CM type. For all primes $\ell \neq 2$ and all $n \geq 1$ we have*

$$(1 - 1/\ell)^{g+1} \cdot \ell^{(g+1)n} \leq |\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq 2^g (1 + 1/\ell)^{g-1} \ell^{(g+1)n},$$

while for $\ell = 2$ and all $n \geq 1$ we have

$$\frac{1}{2^{2g+3}} \cdot 2^{(g+1)n} \leq |\operatorname{MT}(A)(\mathbb{Z}/2^n\mathbb{Z})| \leq 2^{2g-1} \cdot 2^{(g+1)n}.$$

The proof of this result will occupy Sections 6.1 and 6.2, while in Sections 6.3 and 6.4 we discuss the special cases of elliptic curves and abelian surfaces.

6.1. The natural filtration on the norm-1 torus. — Let $\ell \neq 2$ be a rational prime, L be a finite extension of $\mathbb{Q}_\ell$ and τ be an involution of L. Denote L^τ the fixed field of τ, so that L/L^τ is a quadratic (Galois) extension. Fix a squarefree $d \in \mathcal{O}_{L^\tau}$ such that $L = L^\tau\left(\sqrt{d}\right)$ and consider the (multiplicative) group

$$C = \left\{ x \in \mathcal{O}_L^\times \mid x \cdot \tau(x) = 1 \right\}.$$

We write λ for a uniformizer of L^τ, set $e = e\left(L^\tau/\mathbb{Q}_\ell\right)$, and consider v_ℓ and v_λ as valuations on $\overline{\mathbb{Q}_\ell}$, normalized so as to have $v_\lambda(\lambda) = 1$ and $v_\ell(\ell) = 1$; in particular, $v_\lambda = e \cdot v_\ell$. We want to investigate the structure of the filtration of C given by $C(n) := \left\{ x \in C \mid v_\lambda(x-1) \geq n \right\}$. It is easy to see that every $x \in C(1)$ can be represented as

$$x = 1 + 2du \cdot \lambda^{2+2v} + 2u_2 \cdot \lambda^{1+v}\sqrt{d}$$

with $u, u_2 \in \mathcal{O}_{L^\tau}^\times$ and $v \in \mathbb{N}$ subject to the condition

(13) $$u(1 + du \cdot \lambda^{2+2v}) = u_2^2.$$

Furthermore, for $n \geq 1$ we have an exact sequence of abelian groups

$$0 \to C(n+1) \to C(n) \xrightarrow{\alpha} \mathcal{O}_L/(\lambda)\mathcal{O}_L,$$
$$x \quad \mapsto \quad \left[\frac{x-1}{2\lambda^n}\right]$$

where $[\cdot]$ denotes the class of an element of $\mathcal{O}_L$ in the quotient $\mathcal{O}_L/(\lambda)\mathcal{O}_L$. Let us describe the image of α for $n \geq 1$. Clearly $x \in C(n)$ implies $v \geq n-1$, and for $v \geq n$ we have $\alpha(x) = 0$; when $v = n-1$ we have $\alpha(x) = [u_2\sqrt{d}]$. Notice now that we have an injection (of additive groups) $\frac{\mathcal{O}_{L^\tau}}{(\lambda)\mathcal{O}_{L^\tau}} \hookrightarrow \frac{\mathcal{O}_L}{(\lambda)\mathcal{O}_L}$ induced by $x \mapsto x\sqrt{d}$, and we claim that all points in the image of this embedding can be realized as $\alpha(x)$ for some $x \in C(n)$. This is clear for the zero element, so let us consider an element of the form $[u_2\sqrt{d}]$ with $u_2 \in \mathcal{O}_{L^\tau}^\times$. Consider the equation

(14) $$t\left(1 + \lambda^{2n}dt\right) = u_2^2$$

in the variable t. By Hensel's lemma, the discriminant $\Delta := 1 + 4u_2^2\lambda^{2n}d$ is a square in $\mathcal{O}_{L^\tau}$ (recall that $n > 0$). Let $1 + z$ be the square root of Δ that is congruent to 1 modulo λ: then z satisfies $(1 + z)^2 = 1 + 4u_2^2\lambda^{2n}d$, from which we easily find $v_\lambda(z) = 2n + v_\lambda(d)$. It follows that $u := \frac{-1+\sqrt{\Delta}}{2d\lambda^{2n}} = \frac{z}{2d\lambda^{2n}}$ is a solution to Equation (14) which is also a λ-adic unit. We can then set $x = 1 + 2du \cdot \lambda^{2n} + 2u_2 \cdot \lambda^n\sqrt{d}$: by construction x is an element of $C(n)$, and

it satisfies $\alpha(x) = [u_2\sqrt{d}]$. This shows that the image of α is in bijection with $\frac{\mathcal{O}_{L^\tau}}{(\lambda)\mathcal{O}_{L^\tau}}$. Finally, a very similar argument can be repeated when $\ell = 2$, except that Hensel's lemma is now only applicable for $n > v_\lambda(2)$. We thus deduce the following lemma:

LEMMA 6.2. — *Suppose $\ell \neq 2$. For every $n \geq 1$, the quotient $C(n)/C(n+1)$ has order $\left|\frac{\mathcal{O}_{L^\tau}}{(\lambda)\mathcal{O}_{L^\tau}}\right|$. For $\ell = 2$ the same conclusion holds for every $n > v_\lambda(2)$.*

The quotients $C(n)/C(n+1)$ for small values of n are described by the following lemma:

LEMMA 6.3. — *Let f be the inertia degree of L^τ over $\mathbb{Q}_\ell$. Suppose first $\ell \neq 2$: then the quotient $\frac{C(0)}{C(1)}$ has order either $2\ell^f$ or $\ell^f + 1$, with the first (resp. second) case happening exactly when L/L^τ is ramified (resp. unramified). Suppose on the other hand that $\ell = 2$ and $n \leq v_\lambda(2)$: then the quotient $\frac{C(n)}{C(n+1)}$ has order at most 4^f.*

Before giving a proof, recall the following

DEFINITION 6.4. — *Let L be a finite extension of $\mathbb{Q}_\ell$ with ring of integers $\mathcal{O}_L$ and residue field $\mathbb{F}$. Let $\pi : \mathcal{O}_L \to \mathbb{F}$ be the canonical projection. The **Teichmüller lift** is the unique group homomorphism $\omega : \mathbb{F}^\times \to \mathcal{O}_L^\times$ such that, for all $y \in \mathbb{F}^\times$, the element $\omega(y) \in \mathcal{O}_L^\times$ is the unique solution to the equation $x^{|\mathbb{F}|-1} = 1$ satisfying $\pi(x) = y$.*

Proof. — Consider first the case of L/L^τ being unramified (and $\ell \neq 2$). Let $\pi : \mathcal{O}_L \to \mathbb{F} := \frac{\mathcal{O}_L}{(\lambda)\mathcal{O}_L}$ be the canonical projection, and observe that $\mathbb{F}$ has order ℓ^{2f}. It is clear that π restricts to a map $C(0) \to \mathbb{F}^\times$, and on the other hand $x \in C(0)$ maps to 1 if and only if $v_\lambda(x - 1) > 0$, i.e., if and only if $x \in C(1)$: this implies that $C(0)/C(1)$ injects into $\mathbb{F}^\times$. The involution τ induces on $\mathbb{F}$ an automorphism $\tau_\mathbb{F}$, which is necessarily the unique nontrivial involution $x \mapsto x^{\ell^f}$. Let now $x \in C(0)$. By definition we have $x \cdot \tau(x) = 1$, hence

$$1 = \pi(x) \cdot \pi(\tau(x)) = \pi(x) \cdot \tau_\mathbb{F}(\pi(x)) = \pi(x)^{\ell^f + 1},$$

so $C(0)/C(1)$ injects into the subgroup H of $\mathbb{F}^\times$ consisting of the roots of unity of order dividing $\ell^f + 1$. The group H is of order $\ell^f + 1$, and it is not hard to see that $C(0)/C(1)$ surjects onto it: indeed for every $h \in H$ we have $\omega(h) \in C(0)$, and by definition $\pi(\omega(h)) = h$. Suppose on the other hand that L/L^τ is ramified, so that $L = L^\tau(\sqrt{d})$ with $v_\lambda(d) = 1$. Again we see that $C(0)/C(1)$ injects into $\mathbb{F}^\times := \left(\frac{\mathcal{O}_L}{(\lambda)\mathcal{O}_L}\right)^\times$ (which however is not a field anymore), and the involution τ acts on an element $[a + b\sqrt{d}] \in \left(\frac{\mathcal{O}_L}{(\lambda)\mathcal{O}_L}\right)^\times$, with $a, b \in \mathcal{O}_{L^\tau}$, by sending it to $[a - b\sqrt{d}]$. Writing $\pi(x) = [a + b\sqrt{d}]$, the equation $x\tau(x) = 1$

implies $[a^2 - db^2] = 1$, which in turn, since $v_\lambda(d) = 1$, means $[a^2] = 1$ and $[a] = \pm 1$. This shows that $C(0)/C(1)$ injects into $\{\pm 1\} \times \frac{\mathcal{O}_{L^\tau}}{(\lambda)\mathcal{O}_{L^\tau}}$, a set of order $2 \cdot \ell^f$. On the other hand, for any value of $[\pm 1 + b\sqrt{d}] \in \mathbb{F}^\times$, the equation $a^2 = 1 + db^2$ (with fixed b, in the variable a) admits solutions in $\mathcal{O}_{L^\tau}$ by Hensel's lemma; the elements $\pm a + b\sqrt{d} \in C(0)$ then satisfy

$$(\pm a + b\sqrt{d}) \cdot \tau(\pm a + b\sqrt{d}) = a^2 - db^2 = 1,$$

and on the other hand $\pi(\pm a + b\sqrt{d}) = [\pm 1 + b\sqrt{d}]$, so $C(0)/C(1)$ actually projects surjectively on $\{\pm 1\} \times \frac{\mathcal{O}_{L^\tau}}{(\lambda)\mathcal{O}_{L^\tau}}$; this shows that $|C(0)/C(1)| = 2\ell^f$ as claimed. The upper bound for $\ell = 2$ likewise follows from the fact that for any $n \geq 0$ the quotient $C(n)/C(n+1)$ injects into $\frac{\mathcal{O}_L}{(\lambda)\mathcal{O}_L}$. $\qquad\square$

6.2. The order of $\mathbf{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$. — Let E be a CM field of degree $2g$ over $\mathbb{Q}$ and T_E be the associated algebraic torus, and let τ denote complex conjugation on E. If A/K is an abelian variety with complex multiplication by the nondegenerate CM type (E, S), it is known that we have

$$\mathrm{MT}(A)(B) = \left\{ x \in (E \otimes_\mathbb{Q} B)^\times \mid x\tau(x) \in B^\times \right\} \quad \forall \, \mathbb{Q}\text{-algebra } B.$$

We can also consider the 'norm 1' (or Hodge) subtorus of $\mathrm{MT}(A)$ given as a functor by

$$\mathrm{Hg}(A)(B) = \left\{ x \in (E \otimes_\mathbb{Q} B)^\times \mid x\tau(x) = 1 \right\} \quad \forall \, \mathbb{Q}\text{-algebra } B.$$

We aim to give bounds on the number of $\frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$-points of $\mathrm{MT}(A)$, but it is easier to first consider $\mathrm{Hg}(A)$. If we write $E \otimes \mathbb{Q}_\ell \cong \prod_{i=1}^s F_i$ (a product of fields), we have

$$\mathrm{Hg}(A)(\mathbb{Q}_\ell) = \left\{ x = (x_1, \ldots, x_s) \in \prod_{i=1}^s F_i^\times \mid x\tau(x) = 1 \right\}.$$

We can renumber the F_i's in such a way that τ acts by exchanging F_{2i-1} and F_{2i} for $i = 1, \ldots, r$ and it acts as an involution on F_i for $i = 2r+1, \ldots, s$. With this convention, a point $(x_1, \ldots, x_{2r}, x_{2r+1}, \ldots, x_s) \in \prod_{i=1}^s F_i^\times$ is in $\mathrm{Hg}(A)(\mathbb{Q}_\ell)$ if and only if $x_{2i-1}x_{2i} = 1$ for $i = 1, \ldots, r$ and $x_i\tau(x_i) = 1$ for $i = 2r+1, \ldots, s$, that is,

$$(15) \quad \mathrm{Hg}(A)(\mathbb{Q}_\ell) \cong \prod_{i=1}^r \left\{ x_{2i-1} \in F_{2i-1}^\times \right\} \times \prod_{i=2r+1}^s \left\{ x_i \in F_i^\times \mid x_i\tau(x_i) = 1 \right\}.$$

The character groups of $\mathrm{MT}(A)_{\mathbb{Q}_\ell}$ and of $\mathrm{Hg}(A)_{\mathbb{Q}_\ell}$ are quotients of $\widehat{T_{E,\mathbb{Q}_\ell}}$, which in turn is generated by elements of the form $(\chi_1, \ldots, \chi_s)$, where χ_i ranges over the embeddings of F_i in $\overline{\mathbb{Q}_\ell}$. It follows that a point $x \in \mathrm{Hg}(A)(\mathbb{Q}_\ell)$ is in $\mathrm{Hg}(A)(\mathbb{Z}_\ell)$ if and only if for any choice of embeddings $\chi_i : F_i \hookrightarrow \overline{\mathbb{Q}_\ell}$ we have $\chi_i(x_i) \in \mathcal{O}_{\chi_i(F_i)}$; as the property of being ℓ-integral is Galois-invariant we deduce that a necessary and sufficient condition is $x_i \in \mathcal{O}_{F_i}^\times$. Hence we find

$\mathrm{Hg}(A)(\mathbb{Z}_\ell) \cong \prod_{i=1}^{r} \mathcal{O}_{F_{2i-1}}^{\times} \times \prod_{i=2r+1}^{s} \{x_i \in \mathcal{O}_{F_i}^{\times} \mid x_i \tau(x_i) = 1\}$, and a perfectly analogous argument shows that

$$\mathrm{Hg}(A)(1 + \ell^n \mathbb{Z}_\ell) \cong \prod_{i=1}^{r} \left\{ x_{2i-1} \in \mathcal{O}_{F_{2i-1}}^{\times} \mid v_\ell(x_{2i-1} - 1) \geq n \right\}$$

$$\times \prod_{i=2r+1}^{s} \left\{ x_i \in \mathcal{O}_{F_i}^{\times} \mid v_\ell(x_i - 1) \geq n, \ x_i \tau(x_i) = 1 \right\}.$$

Write e_i and f_i for the ramification index and inertia degree of F_i^τ over $\mathbb{Q}_\ell$, and λ_i for a uniformizer of F_i^τ $(i = 2r+1, \ldots, s)$. The order of $\left| \frac{\mathrm{Hg}(A)(\mathbb{Z}_\ell)}{\mathrm{Hg}(A)(1+\ell^n\mathbb{Z}_\ell)} \right|$ is then given by

$$(16) \qquad |\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| = \prod_{i=1}^{r} \left| \frac{\mathcal{O}_{F_{2i-1}}^{\times}}{1 + \ell^n \mathcal{O}_{F_{2i-1}}} \right| \times \prod_{i=2r+1}^{s} \left| \frac{C^{(i)}(0)}{C^{(i)}(ne_i)} \right|,$$

where

$$C^{(i)}(k) = \left\{ x_i \in \mathcal{O}_{F_i}^{\times} \mid v_{\lambda_i}(x_i - 1) \geq k, \ x_i \cdot \tau(x_i) = 1 \right\}$$

is the filtration we studied in the previous section for the field F_i and the involution $\tau|_{F_i}$. For $i = 1, \ldots, r$ let furthermore π_i (resp. e_i, f_i) be a uniformizer (resp. the ramification index over $\mathbb{Q}_\ell$, the inertia degree over $\mathbb{Q}_\ell$) of F_{2i-1}. We now compute the order of $\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$. Basic properties of local fields show that for $i = 1, \ldots, r$ the quotient $\left| \frac{\mathcal{O}_{F_{2i-1}}^{\times}}{1+\ell^n\mathcal{O}_{F_{2i-1}}} \right|$ has order

$$\left| \frac{\mathcal{O}_{F_{2i-1}}^{\times}}{1 + \pi_i \mathcal{O}_{F_{2i-1}}} \right| \cdot \prod_{j=1}^{ne_i-1} \left| \frac{1 + (\pi_i)^j \mathcal{O}_{F_{2i-1}}}{1 + (\pi_i)^{j+1} \mathcal{O}_{F_{2i-1}}} \right| = \left(\ell^{f_i} - 1 \right) \cdot \ell^{f_i(ne_i-1)},$$

while (for $\ell \neq 2$) Lemma 6.2 gives

$$\left| \frac{C^{(i)}(0)}{C^{(i)}(ne_i)} \right| = \left| \frac{C^{(i)}(0)}{C^{(i)}(1)} \right| \cdot \left| \frac{C^{(i)}(1)}{C^{(i)}(ne_i)} \right| = \left| \frac{C^{(i)}(0)}{C^{(i)}(1)} \right| \cdot \ell^{f_i(ne_i-1)}.$$

Now notice that $s - 2r$ does not exceed g: indeed $[F_i : F_i^\tau] = 2$ for every $i = 2r+1, \ldots, r$, hence $2g = [E \otimes \mathbb{Q}_\ell : \mathbb{Q}_\ell] \geq \sum_{i=2r+1}^{s} [F_i : \mathbb{Q}_\ell] \geq 2(s - 2r)$ as claimed. Applying Lemma 6.3 we then deduce that the order of $\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ is at most

$$\prod_{i=1}^{r} \ell^{nf_ie_i} \cdot \prod_{i=2r+1}^{s} 2 \left(1 + \ell^{f_i} \right) \left(\ell^{f_i} \right)^{ne_i-1}$$

$$= 2^{s-2r} \prod_{i=1}^{2r} \ell^{\frac{1}{2}n[F_i:\mathbb{Q}_\ell]} \prod_{i=2r+1}^{s} \left(1 + \ell^{-f_i} \right) \left(\ell^{f_i} \right)^{ne_i}$$

$$\leq 2^{s-2r} \left(1+1/\ell\right)^{s-2r} \prod_{i=1}^{s} \ell^{\frac{1}{2}n[F_i:\mathbb{Q}_\ell]}$$

$$\leq 2^g \left(1+1/\ell\right)^g \ell^{gn},$$

and at least

$$\prod_{i=1}^{r} \left(\ell^{f_i}-1\right) \ell^{(ne_i-1)f_i} \prod_{i=2r+1}^{s} \left(\ell^{f_i}+1\right) \left(\ell^{f_i}\right)^{ne_i-1}$$

$$\geq (1-1/\ell)^r \cdot \prod_{i=1}^{r} \ell^{nf_ie_i} \prod_{i=2r+1}^{s} \ell^{nf_ie_i}$$

$$= (1-1/\ell)^r \cdot \prod_{i=1}^{2r} \ell^{\frac{1}{2}n[F_i:\mathbb{Q}_\ell]} \times \prod_{i=2r+1}^{s} \ell^{\frac{1}{2}n[F_i:\mathbb{Q}_\ell]}$$

$$\geq (1-1/\ell)^g \cdot \ell^{gn};$$

moreover, if for at least one index $i \in \{2r+1, \ldots, s\}$ the extension F_i/F_i^τ is ramified, then we see from Lemma 6.3 that the lower bound can be improved to

$$(17) \qquad\qquad |\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \geq 2(1-1/\ell)^g \cdot \ell^{gn}.$$

To finish the proof of Theorem 6.1 we shall use the following result:

LEMMA 6.5. — *Consider the map*

$$\Psi : \mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})^\times \to \mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$$
$$(h, m) \qquad\qquad \mapsto \qquad m^{-1}h.$$

If $\ell \neq 2$, the group $\mathrm{Im}\,\Psi$ has order equal to $\frac{1}{2}\,|\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \times (1-1/\ell)\ell^n$ and has index at most 2 in $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$. Moreover, Ψ is surjective if and only if for all $x \in \mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ the number $x\tau(x)$ is a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$. On the other hand, for $\ell = 2$ we have

- *for $n = 1$, the group $\mathrm{Im}\,\Psi$ has order equal to that of $|\mathrm{Hg}(A)(\mathbb{Z}/2\mathbb{Z})|$ and Ψ is surjective;*
- *for $n = 2$, the group $\mathrm{Im}\,\Psi$ has order equal to that of $|\mathrm{Hg}(A)(\mathbb{Z}/4\mathbb{Z})|$ and $\mathrm{Im}\,\Psi$ has index either 1 or 2 in $\mathrm{MT}(A)(\mathbb{Z}/4\mathbb{Z})$;*
- *for $n \geq 3$, the group $\mathrm{Im}\,\Psi$ has order equal to $2^{n-3} \cdot |\mathrm{Hg}(A)(\mathbb{Z}/2^n\mathbb{Z})|$ and $\mathrm{Im}\,\Psi$ has index 1, 2 or 4 in $\mathrm{MT}(A)(\mathbb{Z}/2^n\mathbb{Z})$;*

Proof. — Let us start with the case $\ell \neq 2$. The kernel of ψ is given by the intersection of $\mathrm{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ and $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ inside $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$, namely

$$\left\{h \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \mid h\tau(h) = 1\right\} = \left\{h \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \mid h^2 = 1\right\} = \{\pm 1\},$$

so Im Ψ has order

$$\frac{1}{|\ker \Psi|} \cdot |\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \cdot \left|(\mathbb{Z}/\ell^n\mathbb{Z})^\times\right| = \frac{(\ell-1)\ell^{n-1}}{2} \cdot |\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})|$$

as claimed.

As for the index of Im Ψ, notice first that for every $x = m^{-1}h \in \operatorname{Im} \Psi$ we have that $x \cdot \tau(x) = m^{-2}$ is a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, so if Ψ is surjective we necessarily have $x \cdot \tau(x) \in (\mathbb{Z}/\ell^n\mathbb{Z})^{\times 2}$ for every $x \in \operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$. Conversely, suppose that for every x in $\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ the number $x\tau(x)$ is a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, say $x\tau(x) = \mu(x)^2$ with $\mu(x) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$. Then every x can be written as $x = \mu(x) \cdot \frac{x}{\mu(x)}$, and since $\frac{x}{\mu(x)}$ is in $\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ this shows that x belongs to Im Ψ, which is therefore surjective.

Finally, if there is a $y \in \operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $y\tau(y)$ is not a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, then using the fact that $(\mathbb{Z}/\ell^n\mathbb{Z})^{\times 2}$ is of index 2 in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ we easily see that for every $x \in \operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ either x or xy belongs to Im Ψ, thus proving the remaining claim. The conclusion for $\ell = 2$ follows by the same argument upon noticing that $\frac{(\mathbb{Z}/2^n\mathbb{Z})^\times}{(\mathbb{Z}/2^n\mathbb{Z})^{\times 2}}$ has order $1, 2$, or 4, according to whether n is 1, 2, or at least 3. $\qquad\square$

Combining this last lemma with our previous estimates gives the desired upper bound

$$|\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq 2 |\operatorname{Im} \Psi| = |\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \times \left|(\mathbb{Z}/\ell^n\mathbb{Z})^\times\right|$$
$$\leq 2^g (1 + 1/\ell)^{g-1} \ell^{(g+1)n}.$$

As for the lower bound, suppose first that for at least one index i in the set $\{2r+1, \ldots, s\}$ the extension L_i/L_i^τ is ramified: then using the lower bound of Equation (17) (which is conditional on this hypothesis) we find

$$|\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \geq \frac{1}{2} |\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \times \left|(\mathbb{Z}/\ell^n\mathbb{Z})^\times\right| \geq (1 - 1/\ell)^{g+1} \ell^{(g+1)n}.$$

Suppose on the other hand that L_i/L_i^τ is unramified for every $i = 2r+1, \ldots, s$: then we claim that map Ψ from Lemma 6.5 is not surjective. Assuming this is the case, we have

$$|\operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \geq 2 \times \frac{1}{2} \times |\operatorname{Hg}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \times \left|(\mathbb{Z}/\ell^n\mathbb{Z})^\times\right| \geq (1 - 1/\ell)^{g+1} \ell^{(g+1)n},$$

which is what we want to show. We are thus reduced to proving that Ψ is not surjective, or equivalently (by Lemma 6.5), to showing that there is an $x \in \operatorname{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ such that $x\tau(x)$ is not a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$. By the same argument that leads to Equations (15) and (16), we can represent elements

of $\mathrm{MT}(A)(\mathbb{Z}_\ell)$ as tuples

$$(x_1, \ldots, x_{2r}, x_{2r+1}, \ldots, x_s, m) \in \prod_{i=1}^{2r} \mathcal{O}_{F_i}^\times \times \prod_{j=2r+1}^{s} \mathcal{O}_{F_j}^\times \times \mathbb{Z}_\ell^\times,$$

satisfying $x_{2i-1}x_{2i} = m$ for $i = 1, \ldots, r$ and $x_j \tau(x_j) = m$ for $j = 2r+1, \ldots, s$. Now if $2r = s$ it is clear that $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ contains elements x such that $x\tau(x)$ is not a square (it suffices to choose $m \in \mathbb{Z}_\ell^\times$ which is not a square in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ and set $x_{2i-1} = 1, x_{2i} = m$ for $i = 1, \ldots, r$), so we can assume $s > 2r$. For $j = 2r+1, \ldots, s$ write $F_j = F_j^\tau(\sqrt{d_j})$ for some squarefree $d_j \in \mathcal{O}_{F_j}^\times$ (recall that we assume F_j/F_j^τ to be unramified), and likewise write $x_j = a_j + b_j\sqrt{d_j}$ for some $a_j, b_j \in \mathcal{O}_{F_j^\tau}$. We claim that since F_j/F_j^τ is unramified every element $m \in \mathbb{Z}_\ell^\times$ can be represented as $a_j^2 - d_j b_j^2$ for some choice of $a_j, b_j \in \mathcal{O}_{F_j^\tau}$. To see this, notice that for fixed m and d_j the conic section $\mathcal{C} : \{a^2 - d_j b^2 = mc^2\}$ admits a point (a_0, b_0, c_0) over the residue field of F_j^τ; as d_j is not a square in F_j^τ we cannot have $c_0 = 0$, and since $\mathcal{C}$ is smooth the point (a_0, b_0, c_0) lifts to a point $(a, b, c) \in \mathcal{C}\left(\mathcal{O}_{F_j^\tau}\right)$, with c a unit (since it does not reduce to 0 in the residue field). Dividing through by c^2 then yields $(a/c)^2 - d_j(b/c)^2 = m$ as desired. Pick now a fixed non-square $m \in \mathbb{Z}_\ell^\times$ and for each $j = 2r+1, \ldots, s$ fix a representation $m = a_j^2 - d_j b_j^2$. Take furthermore $x_{2i-1} = 1, x_{2i} = m$ for $i = 1, \ldots, r$.

The corresponding point $x = ((x_i)_{i=1,\ldots,2r}, (x_j)_{j=2r+1,\ldots,s}, m)$ of $\mathrm{MT}(A)(\mathbb{Z}_\ell)$ has the property that $x\tau(x) = m$ is not a square in $\mathbb{Z}_\ell^\times$, and therefore the image of x in $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ has again the property that $x\tau(x) = [m] \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ is not a square. Combined with Lemma 6.5, this shows that Ψ is not surjective in this case and concludes the proof of Theorem 6.1 for $\ell \neq 2$.

Notice now that for $\ell = 2$ the lower bound of Theorem 6.1 is trivial for $n \leq 2$, so we can assume $n \geq 3$. We then remark that (by Equation (16)) $\mathrm{Hg}(A)(\mathbb{Z}/2^n\mathbb{Z})$ has order at least

$$\prod_{i=1}^{r} 2^{(n-1)[F_{2i-1}:\mathbb{Q}_\ell]} \times \prod_{i=2r+1}^{s} \left| \frac{C^{(i)}(e_i+1)}{C^{(i)}(ne_i)} \right|,$$

which (by the same argument as above, using the second part of Lemma 6.2) in turn is at least

$$\prod_{i=1}^{r} 2^{(n-1)[F_{2i-1}:\mathbb{Q}_\ell]} \times \prod_{i=2r+1}^{s} \left(2^{f_i}\right)^{(n-1)e_i - 1} \geq 2^{g(n-2)}.$$

Furthermore, taking into account the factor coming from the homotheties—namely $(\mathbb{Z}/2^n\mathbb{Z})^\times$—we find $|\mathrm{MT}(A)(\mathbb{Z}/2^n\mathbb{Z})| \geq 2^{(g+1)(n-2)-1}$. Finally, the upper bound for $\ell = 2$ follows trivially from the previous computations and from the second halves of Lemmas 6.3 and 6.5.

6.3. Elliptic curves. — When the CM abelian variety under consideration is an elliptic curve we can give a complete description of the full adelic Galois representation:

THEOREM 6.6. — *Let A/K be an elliptic curve such that $\mathrm{End}_{\overline{K}}(A)$ is an order in an imaginary quadratic field E. Denote by $\rho_\infty : \mathrm{Gal}\left(\overline{K}/K\right) \to \prod_\ell \mathrm{Aut}\, T_\ell A$ the natural adelic representation attached to A, and let G_∞ be its image. For every prime ℓ denote by C_ℓ the group $(\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times$, considered as a subgroup of $\mathrm{Aut}_{\mathbb{Z}_\ell} (\mathcal{O}_E \otimes \mathbb{Z}_\ell) \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \cong \mathrm{Aut}\, T_\ell A$, and let $N(C_\ell)$ be the normalizer of C_ℓ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

1. *Suppose that $E \subseteq K$: then G_∞ is contained in $\prod_\ell C_\ell$, and the index $[\prod_\ell C_\ell : G_\infty]$ does not exceed $3[K : \mathbb{Q}]$. The equality $G_{\ell^\infty} = C_\ell$ holds for every prime ℓ unramified in K and such that A has good reduction at all places of K of characteristic ℓ.*
2. *Suppose that $E \not\subseteq K$: then G_∞ is contained in $\prod_\ell N(C_\ell)$ but not in $\prod_\ell C_\ell$, and the index $[\prod_\ell N(C_\ell) : G_\infty]$ is not finite. The intersection $H_\infty = G_\infty \cap \prod_\ell C_\ell$ has index 2 in G_∞, and the index $[\prod_\ell C_\ell : H_\infty]$ does not exceed $6[K : \mathbb{Q}]$. The equality $G_{\ell^\infty} = N(C_\ell)$ holds for every prime ℓ unramified in $K \cdot E$ and such that A has good reduction at all places of K of characteristic ℓ.*

Finally, the constants 3 and 6 appearing in parts (1) and (2) respectively can be replaced by 1 and 2 if we further assume that the j-invariant of A is neither 0 nor 1728.

We start by recording the following consequence of Theorem 5.5:

COROLLARY 6.7. — *Let A/K be an elliptic curve admitting complex multiplication (over K) by the imaginary quadratic field E. The group G_{ℓ^∞} is contained in $\mathrm{MT}(A)(\mathbb{Z}_\ell) = C_\ell$, and if A has good reduction at all places of K of characteristic ℓ the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty}]$ is at most $\frac{1}{2}[K : \mathbb{Q}]$. If in addition ℓ is also unramified in K we have $G_{\ell^\infty} = (\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times$.*

Proof. — Since E is quadratic, E and E^* coincide and the reflex norm is simply the identity $T_E \to T_E$, hence $\mathrm{MT}(A) = T_E$ and (in the notation of Theorem 5.5) F is the trivial group. In particular $T_E(\mathbb{Z}_\ell) = (\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times = C_\ell$ contains G_{ℓ^∞} by [19, Corollary 2 to Theorem 5] (cf. also [17, Corollaire on p. 302]): the claim on the index then follows from Theorem 5.5 upon noticing that $[K : E^*] = [K : E] = \frac{1}{2}[K : \mathbb{Q}]$. Furthermore, if ℓ is unramified in K, then it is also unramified in E, and the remaining assertion $G_{\ell^\infty} = C_\ell = \mathrm{MT}(A)(\mathbb{Z}_\ell)$ follows from part (3) of Theorem 5.5. □

We shall also need some results concerning elliptic curves A/K that admit complex multiplication over $\overline{K}$ but not over K. Results similar to Lemmas 6.8, 6.9 and 6.10 already appear for example in [18, Appendix A.5], but we include

short proofs that do not depend on the splitting and/or ramification properties of the prime ℓ in the ring $\mathcal{O}_E$.

LEMMA 6.8. — C_ℓ is of index 2 in $N(C_\ell)$. In particular, $N(C_\ell)$ is generated by C_ℓ and any element in $N(C_\ell) \setminus C_\ell$. Furthermore, if H_ℓ is an open subgroup of C_ℓ, then the normalizer of H_ℓ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is contained in $N(C_\ell)$.

Proof. — Fix $\omega \in \mathcal{O}_E$ such that $(1, \omega)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_E$. There exist $c, d \in \mathbb{Z}$ such that ω satisfies the quadratic relation $\omega^2 = c\omega + d$. In the $\mathbb{Z}_\ell$-basis $(1, \omega)$ of $\mathcal{O}_E \otimes \mathbb{Z}_\ell$, the group C_ℓ is the subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ given by the invertible matrices that can be written as $\begin{pmatrix} a & bd \\ b & a+bc \end{pmatrix}$ for some $a, b \in \mathbb{Z}_\ell$. We thus see that C_ℓ is given by the intersection of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with a 2-dimensional plane Π (that defined by the equations $x_{11} + cx_{21} = x_{22}, x_{12} = dx_{21}$, where x_{ij} is the coefficient on the i-th row and j-th column). In particular, for an element $g \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ the condition of normalizing C_ℓ is equivalent to that of stabilizing Π. The latter is a Zariski-closed condition, and since any subgroup H_ℓ of C_ℓ open in the ℓ-adic topology is Zariski-dense in Π we see that if g normalizes H_ℓ, then it stabilizes Π and hence it normalizes C_ℓ. Finally, with the explicit description at hand it is immediate to see that $[N(C_\ell) : C_\ell] = 2$, and that a nontrivial element of $N(C_\ell) \setminus C_\ell$ is given by $\begin{pmatrix} 1 & c \\ 0 & -1 \end{pmatrix}$. $\qquad\square$

LEMMA 6.9. — *Suppose A/K is an elliptic curve such that $\mathrm{End}_K(A) = \mathbb{Z}$ but $\mathrm{End}_{\overline{K}}(A)$ is an order in an imaginary quadratic field E: then for every prime ℓ the group G_{ℓ^∞} is contained in $N(C_\ell)$.*

Proof. — The field $K^1 = K \cdot E$ is a quadratic extension of K over which all the endomorphisms of A are defined, and the group $G^1_{\ell^\infty} = \rho_{\ell^\infty}\left(\mathrm{Gal}\left(\overline{K^1}/K^1\right)\right)$ is a closed subgroup of G_{ℓ^∞} of index at most 2 (hence in particular it is normal and open in G_{ℓ^∞}). Let $R = \mathrm{End}_{\overline{K}}(A)$. Since A admits complex multiplication by R over K^1, we know by [17, §4.5, Corollaire] that $G^1_{\ell^\infty}$ is of finite index in $(R \otimes \mathbb{Z}_\ell)^\times$, which in turn is of finite index in C_ℓ. Thus the normalizer of $G^1_{\ell^\infty}$ is included in $N(C_\ell)$ by Lemma 6.8, and since $G^1_{\ell^\infty}$ is normal in G_{ℓ^∞} we have $G_{\ell^\infty} \subseteq N(G^1_{\ell^\infty}) \subseteq N(C_\ell)$ as claimed. $\qquad\square$

LEMMA 6.10. — *In the situation of the previous lemma, for all primes ℓ the group G_{ℓ^∞} has nontrivial intersection with $N(C_\ell) \setminus C_\ell$.*

Proof. — For all primes ℓ we have $G_{\ell^\infty} \subseteq N(C_\ell)$. On the other hand, we know by Faltings' theorem that the centralizer of G_{ℓ^∞} in $\mathrm{End}\left(T_\ell A\right) \otimes \mathbb{Q}_\ell$ equals $\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell$. It follows that G_{ℓ^∞} cannot be abelian, for otherwise its centralizer would contain all of G_{ℓ^∞} (which is not contained in the homotheties $\mathbb{Q}_\ell$): in particular, G_{ℓ^∞} must have nontrivial intersection with $N(C_\ell) \setminus C_\ell$. $\quad\square$

We can now prove Theorem 6.6:

Proof. — (of Theorem 6.6) The proof is quite similar to that of Theorem 5.5, the main differences being that we need to treat all places at the same time and that the action of E needs not be defined over K. Consider first case (1). The inclusion $G_{\ell^\infty} \subseteq C_\ell$ is part of Corollary 6.7, and implies $G_\infty \subseteq \prod_\ell G_{\ell^\infty} \subseteq \prod_\ell C_\ell$. In particular, G_∞ is abelian, so class field theory allows us to interpret ρ_∞ as a map

$$I_K \xrightarrow{\rho_\infty} \prod_\ell C_\ell$$

that is trivial on K^*. As in the proof of Theorem 5.5, since we are looking for a *lower* bound on G_∞ no harm is done in replacing I_K by the group of idèles of the Hilbert class field of K; concretely, this means considering the restriction of ρ_∞ to $\prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$, where Ω_K is the set of finite places of K. Recall from Theorem 5.1 that the action of ρ_∞ on a finite idèle $a = (a_v)_{v \in \Omega_K}$ is given by

$$\rho_\infty(a) = \varepsilon(a) \left(N_{K_\ell/E_\ell}(a_\ell^{-1}) \right)_{\ell \text{ prime}}.$$

As in the proof of Theorem 5.5, if we let $\mu(E)$ be the group of roots of unity in E we know that $\ker \varepsilon$ is a subgroup of $\prod_{v \in \Omega_K} \mathcal{O}_{K,v}^\times$ of index at most $|\mu(E)|$, and since E is a quadratic imaginary field we have $|\mu(E)| \leq 6$. Therefore the image of ρ_∞ has index at most $|\ker \varepsilon| \leq 6$ in the image of the map

$$\varphi_\infty : \prod_{v \in \Omega_K} \mathcal{O}_v^\times \to \prod_\ell (\mathcal{O}_E \otimes \mathbb{Z}_\ell)^\times = \prod_\ell C_\ell$$
$$(a)_v \mapsto \left(N_{K_\ell/E_\ell}(a_\ell) \right)_\ell$$

given by taking local norms from K_ℓ to E_ℓ. Hence in particular we have $[\prod_\ell C_\ell : G_\infty] \leq 6 [\prod_\ell C_\ell : \operatorname{Im} \varphi_\infty]$, and it suffices to show that

$$\left[\prod_\ell C_\ell : \operatorname{Im} \varphi_\infty \right] \leq [K : E] = \frac{1}{2}[K : \mathbb{Q}],$$

which follows from [1, Theorem 7 on p. 161] (the global field counterpart of Theorem 5.3). The remaining assertion of part (1) is exactly the content of Corollary 6.7.

As for part (2), we have seen in Lemmas 6.9 and 6.10 that in this case G_{ℓ^∞} is contained in $N(C_\ell)$, but not in C_ℓ. If we let $K^1 = K \cdot E$, then A admits complex multiplication by E over K^1, so $\rho_\infty \left(\operatorname{Gal}\left(\overline{K^1}/K^1 \right) \right)$ is contained in $\prod_\ell C_\ell$ by part (1). Since $\operatorname{Gal}\left(\overline{K^1}/K^1 \right)$ has index 2 in $\operatorname{Gal}\left(\overline{K}/K \right)$ we must have $H_\infty = \rho_\infty \left(\operatorname{Gal}\left(\overline{K^1}/K^1 \right) \right)$, so that the index $[G_\infty : H_\infty]$ is indeed 2 and applying part (1) we find $[\prod_\ell C_\ell : H_\infty] \leq 3[K^1 : \mathbb{Q}] = 6[K : \mathbb{Q}]$; moreover, the index $[\prod_\ell N(C_\ell) : G_\infty]$ is not finite since the same is clearly true for the index $[\prod_\ell N(C_\ell) : \prod_\ell C_\ell]$. Finally, if ℓ is unramified in K^1 we see from Corollary 6.7 (applied to A/K^1) that G_{ℓ^∞} contains all of C_ℓ, and by Lemma 6.10 we know

that G_{ℓ^∞} also contains an element of $N(C_\ell) \setminus C_\ell$. The equality $G_{\ell^\infty} = N(C_\ell)$ then follows from Lemma 6.8.

As for the last assertion, notice that if we exclude elliptic curves with j-invariant equal to 0 or 1728 the field of complex multiplication E is neither $\mathbb{Q}(i)$ nor $\mathbb{Q}(\zeta_3)$, so the only roots of unity in E are ± 1. This implies that $\ker \varepsilon$ has index at most 2 in $\prod_{v \in \Omega_K} \mathcal{O}_v^\times$, and the same argument as above shows that the constants 3 and 6 can indeed be replaced by 1 and 2. $\square$

REMARK 6.11. — The following simple example shows that the constants 3 and 6 cannot be improved in general. We consider the elliptic curve A over the field $K = \mathbb{Q}(\zeta_3)$ given by the Weierstrass equation $y^2 = x^3 + 1$. As it is clear, A has complex multiplication (over K) by the full ring of integers of $E = K$. Moreover, all the 2-torsion points of A are defined over K, so G_2 has trivial reduction modulo 2. Hence G_2 is a subgroup of $\ker(\mathbb{Z}_2[\zeta_3]^\times \to \mathbb{F}_2[\zeta_3]^\times)$, and its index in $(\mathcal{O}_E \otimes \mathbb{Z}_2)^\times \cong \mathbb{Z}_2[\zeta_3]^\times$ is divisible by $|\mathbb{F}_2[\zeta_3]^\times| = 3$. Likewise, the fact that the 3-torsion point with coordinates $(0, 1)$ is defined over K shows that the index of G_3 in $(\mathcal{O}_E \otimes \mathbb{Z}_3)^\times$ is divisible by 2. Thus we conclude that the index of G_∞ in $\prod_\ell C_\ell$ is at least $6 = 3[K : \mathbb{Q}]$, so that the constant 3 is indeed sharp. Finally, considering the $\mathbb{Q}$-elliptic curve given by the same Weierstrass equation shows the optimality of part (2): in this case H_∞ is exactly the image of the Galois representation attached to A/K, so we have $[\prod_\ell C_\ell : H_\infty] = 6$ by what we just showed.

6.4. Abelian surfaces. — An easy direct computation shows that when $\dim A = 2$ the kernel of the reflex norm is always connected, and therefore the group F of Theorem 5.5 is trivial. Since furthermore simple CM types are automatically non-degenerate in dimension 2, combining Theorems 5.5 and 6.1 we deduce:

COROLLARY 6.12. — *Let A/K be an absolutely simple abelian variety of dimension 2. Suppose that A has CM over K by the field E and let ℓ be a prime number such that A has good reduction at all places of K of characteristic ℓ. The group $G_{\ell^\infty} \cap \mathrm{MT}(A)(\mathbb{Z}_\ell)$ has index at most $[K : E^*]$ in $\mathrm{MT}(A)(\mathbb{Z}_\ell)$, hence we have $[K(A[\ell^n]) : K] \geq \frac{1}{[K:E^*]}(1 - 1/\ell)^3 \ell^{3n}$ for $\ell \neq 2$, while for $\ell = 2$ we have $[K(A[2^n]) : K] \geq \frac{1}{2^7 [K:E^*]} 2^{3n}$. Finally, if ℓ is unramified in $K \cdot E$ we even have $[K(A[\ell^n]) : K] \geq (1 - 1/\ell)^3 \ell^{3n}$.*

7. A family of varieties with small 2-torsion fields

Let $p \geq 3$ be a prime number and K_p be the cyclotomic field $\mathbb{Q}(\zeta_p)$. We let C_p be the unique smooth K_p-curve birational to $y^p = x(1 - x)$ and $J(p)$ be its Jacobian, again over K_p. It is clear that C_p admits an action of μ_p, so $J(p)$ is a

CM abelian variety, admitting complex multiplication over K_p by the full ring of integers of K_p. Notice furthermore that C_p is birational to the curve

$$z^2 = w^p + 1/4$$

(just set $x = z + 1/2$, $y = -w$), so it is hyperelliptic of genus $\frac{p-1}{2}$. Direct inspection of the model $y^p = x(1-x)$ reveals that C_p is smooth away from p, so $J(p)$ has everywhere good reduction over K_p except perhaps at the unique place dividing p. The reflex field is $K_p^* = K_p$. Let us compute the CM type S of $J(p)$: in the basis $\omega_j := w^j \frac{dw}{z}$ ($j = 0, \ldots, \frac{p-3}{2}$) of the space of differentials on C_p, the action of ζ_p is given by $[\zeta_p]^* \omega_j = \zeta_p^{j+1} \omega_j$, hence the CM type, considered as a subset of $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$, is $\left\{1, \ldots, \frac{p-1}{2}\right\}$. Equivalently,

$$S = \left\{ g \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \mid 2\langle g \rangle < p \right\},$$

where $\langle g \rangle$ is the unique integer lying in the interval $[0, p-1]$ that is congruent to g modulo p. This description shows that our CM type agrees with the type S_1 described in [7], which by [7, Lemma 1] is nondegenerate (cf. also [5]): thus we have rank $\mathrm{MT}(A) = \dim A + 1 = \frac{p+1}{2}$.

Let now $\beta_1, \ldots, \beta_p$ be the roots of $w^p + 1/4 = 0$ in $\overline{\mathbb{Q}}$, and let $P_i = (\beta_i, 0)$ be the corresponding points of C_p (in the coordinates (w, z)). Finally, for $i = 1, \ldots, p$ let d_i denote the divisor $(P_i) - (\infty)$. It is known (see for example [3, §5.1]) that the 2-torsion of $J(p)$ is an $\mathbb{F}_2$-vector space of dimension $p-1$ spanned by the d_i's, which are only subject to the linear relation $\sum_{i=1}^p d_i = [0]$. It follows that the 2-torsion field $K_p(J(p)[2]) = K_p(\{\beta_i\}) = K_p\left(\sqrt[p]{1/4}\right)$ has degree p over K_p, so for $\ell = 2$ and $n = 1$ the ratio $\ell^{n\,\mathrm{rank}\,\mathrm{MT}(A)} \big/ [K(A[\ell^n]) : K]$ is given by

$$\frac{2^{\mathrm{rank}\,\mathrm{MT}(A)}}{[K(J(p)[2]) : K]} = \frac{2^{(p+1)/2}}{p} = \frac{2^{\dim J(p)+1}}{2\dim J(p) + 1},$$

which shows in particular that, as claimed in the introduction, the optimal bound on the quantity $\ell^{n\,\mathrm{rank}\,\mathrm{MT}(A)} \big/ [K(A[\ell^n]) : K]$ grows at least exponentially in the dimension of A.

BIBLIOGRAPHY

[1] E. ARTIN & J. TATE – *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009, Reprinted with corrections from the 1967 original.

[2] G. BANASZAK, W. GAJDA & P. KRASOŃ – "On Galois representations for abelian varieties with complex and real multiplications", *J. Number Theory* **100** (2003), p. 117–132.

[3] M. Bhargava & B. H. Gross – "The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point", in *Automorphic representations and L-functions*, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, p. 23–91.

[4] M. Hindry & N. Ratazzi – "Points de torsion sur les variétés abéliennes de type GSp", *J. Inst. Math. Jussieu* **11** (2012), p. 27–65.

[5] T. Kubota – "On the field extension by complex multiplication", *Trans. Amer. Math. Soc.* **118** (1965), p. 113–122.

[6] S. Lang – *Complex multiplication*, Grundl. math. Wiss., vol. 255, Springer, New York, 1983.

[7] L. Mai – "Lower bounds for the ranks of CM types", *Journal of Number Theory* **32** (1989), p. 192 – 202.

[8] D. Mumford – "Families of abelian varieties", in *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, Amer. Math. Soc., Providence, R.I., 1966, p. 347–351.

[9] E. Nart & X. Xarles – "Additive reduction of algebraic tori", *Arch. Math. (Basel)* **57** (1991), p. 460–466.

[10] J. Neukirch – *Class field theory*, Grundl. math. Wiss., vol. 280, Springer, Berlin, 1986.

[11] J. Neukirch, A. Schmidt & K. Wingberg – *Cohomology of number fields*, Grundl. math. Wiss., Springer, 2013.

[12] T. Ono – "Arithmetic of algebraic tori", *Ann. of Math.* **74** (1961), p. 101–139.

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

[14] K. A. Ribet – "Division fields of abelian varieties with complex multiplication", *Mém. Soc. Math. France (N.S.)* **2** (1980/81), p. 75–94, Abelian functions and transcendental numbers (Colloq., École Polytech., Palaiseau, 1979).

[15] ———, "Generalization of a theorem of Tankeev", in *Seminar on Number Theory, 1981/1982*, Univ. Bordeaux I, Talence, 1982, p. Exp. No. 17, 4.

[16] J.-P. Serre – *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[17] ———, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. math.* **15** (1972), p. 259–331.

[18] ———, *Lectures on the Mordell-Weil theorem*, third éd., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[19] J.-P. Serre & J. Tate – "Good reduction of abelian varieties", *Ann. of Math.* **88** (1968), p. 492–517.

[20] S. S. Shatz – *Profinite groups, arithmetic, and geometry*, Princeton Univ. Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972, Annals of Mathematics Studies, No. 67.

[21] G. SHIMURA & Y. TANIYAMA – *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[22] A. SILVERBERG – "Torsion points on abelian varieties of CM-type", *Compos. math.* **68** (1988), p. 241–249.

[23] J. TSIMERMAN – "Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points", *J. Amer. Math. Soc.* **25** (2012), p. 1091–1117.

[24] V. E. VOSKRESENSKIĬ – *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, Amer. Math. Soc., Providence, RI, 1998.