Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

GALOIS REPRESENTATIONS ATTACHED TO ABELIAN VARIETIES OF CM TYPE

Davide Lombardo

Tome 145
Fascicule 3

2017

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 469-501

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 3, tome 145, septembre 2017

Diffusion

Maison de la SMF - Case 916 - Luminy - 13288 Marseille Cedex 9 - France
`christian.smf@cirm-math.fr`

Hindustan Book Agency
O-131, The Shopping Mall
Arjun Marg, DLF Phase 1
Gurgaon 122002, Haryana
Inde

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 135 € ($ 202),
avec supplément papier : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
`bullsmf@ihp.fr` • `smf.emath.fr`

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Stéphane SEURET

Bull. Soc. Math. France
145 (3), 2017, p. 469-501

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 $K(A_{\mathrm{tors}})/K$. 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 $K(A_{\mathrm{tors}})/K$ 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.

Texte reçu le 5 septembre 2015, modifié le 21 septembre 2016, accepté le 29 novembre 2016.

DAVIDE LOMBARDO, Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa (Italia), `http://people.dm.unipi.it/lombardo/` • *E-mail :* `davide.lombardo@unipi.it`

Mathematical subject classification (2010). — 14K22, 11F80, 11G10.

Key words and phrases. — Complex multiplication, Galois representations, elliptic curves, Mumford-Tate group.

 0037-9484/2017/469/$ 5.00
 doi:10.24033/bsmf.2745

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 $E \hookrightarrow \operatorname{End}_{\overline{K}}(A) \otimes \mathbb{Q}$, 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 $\operatorname{End}_K(A)$ is equal to $\operatorname{End}_{\overline{K}}(A)$, 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:*

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

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 $\operatorname{Gal}\left(\overline{K}/K\right)$ on $A[\ell^n]$, giving rise to a representation

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

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 $T_\ell A$,

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

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 $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ (resp. of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z})$).

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 $\mathrm{MT}(A)$, the Mumford-Tate group of A (cf. Definition 2.10). By construction, $\mathrm{MT}(A)$ 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 $\mathrm{MT}(A)(\mathbb{Z}_\ell)$ (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 $\mathrm{MT}(A)(\mathbb{Z}_\ell)$. For the sake of simplicity, assume for now that no extension of the base field K is necessary to attain the condition $G_{\ell^\infty} \subseteq \mathrm{MT}(A)(\mathbb{Z}_\ell)$ (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 $\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})$ and the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty}]$.

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 $\mathrm{MT}(A)$ the Mumford-Tate group of A and let r be its rank.*

1. *If ℓ is unramified in E the following inequalities hold:*
$$(1-1/\ell)^r \ell^{nr} \leq |\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq (1+1/\ell)^r \ell^{nr}.$$
2. *Suppose $r = g+1$. For all primes $\ell \neq 2$ and all $n \geq 1$ we have*
$$(1-1/\ell)^{g+1} \cdot \ell^{(g+1)n} \leq |\,\mathrm{MT}(A)(\mathbb{Z}/\ell^n\mathbb{Z})| \leq 2^g\,(1+1/\ell)^{g-1}\,\ell^{(g+1)n},$$
while for $\ell = 2$ and all $n \geq 1$ we have
$$\frac{1}{2^{2g+3}} \cdot 2^{(g+1)n} \leq |\,\mathrm{MT}(A)(\mathbb{Z}/2^n\mathbb{Z})| \leq 2^{2g-1} \cdot 2^{(g+1)n}.$$

As for the index $[\mathrm{MT}(A)(\mathbb{Z}_\ell) : G_{\ell^\infty}]$, 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*