ONE FORMAL RESULT FOR TORSION AND ARBOREAL REPRESENTATIONS OF COMMUTATIVE ALGEBRAIC GROUPS

ANTIGONA PAJAZITI AND ANTONELLA PERUCCA

Abstract. Consider a connected commutative algebraic group defined over a number field. For every positive integer n we have a torsion representation ρ_n describing the Galois action on the torsion points of order dividing n. The image of ρ_n is usually seen as a subgroup of some finite group G_n (that depends on which type of algebraic group we are considering). We assume some basic properties for G_n and ρ_n, for example that the index $[G_n : \mathrm{Im}(\rho_n)]$ is bounded by varying n, and we prove that there exists some positive integer N such that the index for n is the same as the index for $\gcd(n, N)$. The same holds for the arboreal representations describing the Galois action on the division points over a rational point of $\mathcal{A}$ having infinite order.

1. Introduction

Let E be an elliptic curve defined over a number field K and without CM over $\bar{K}$. For every positive integer n we consider its mod n torsion representation ρ_n, describing the Galois action on the group of torsion points $E[n]$. To determine the image of ρ_n for every $n \geqslant 1$ it suffices to determine it for finitely many values of n:

Theorem 1. *There exists an integer $N \geqslant 1$ such that for every $n \geqslant 1$ we have*

$$[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Im}(\rho_n)] = [\mathrm{GL}_2(\mathbb{Z}/\gcd(n,N)\mathbb{Z}) : \mathrm{Im}(\rho_{\gcd(n,N)})]\,.$$

Consequently, the image of ρ_n is the preimage in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ of the image of $\rho_{\gcd(n,N)}$ under the reduction modulo $\gcd(n, N)$.

A similar result holds for the arboreal representations attached to a rational point $P \in E(K)$ of infinite order. Indeed, consider the Galois representation ρ'_n describing the Galois action on the group of division points $n^{-1}P$. Up to choosing a division point, the image of ρ'_n can be identified to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$. Then the following holds:

Theorem 2. *There exists an integer $N \geqslant 1$ such that for every $n \geqslant 1$ we have*

$$[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2 : \mathrm{Im}(\rho'_n)] = [\mathrm{GL}_2(\mathbb{Z}/\gcd(n,N)\mathbb{Z}) \ltimes (\mathbb{Z}/\gcd(n,N)\mathbb{Z})^2 : \mathrm{Im}(\rho'_{\gcd(n,N)})]\,.$$

Consequently, the image of ρ'_n is the preimage in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$ of the image of $\rho'_{\gcd(n,N)}$ under the reduction modulo $\gcd(n, N)$.

The proof of the two above results is substantially the same. To easily allow for generalizations, we provide a formal proof (see Theorem 6), where the assumptions are properties that hold in particular for torsion and arboreal representations of elliptic curves without CM. One property is that the indices are bounded by varying n (for the torsion representations of elliptic curves without CM, this is Serre's open image theorem).

Our results reduce the computation of the infinite family of groups $\mathrm{Im}(\rho_n)$ (respectively, $\mathrm{Im}(\rho'_n)$) to the computation of finitely many of them. For applications, it is important that an integer N as in the above statements is known, and it is to be expected that effective results will be proven. It is also an interesting question to determine under which conditions the arboreal representations are surjective, building on the investigation by Jones and Rouse [5] and by Lombardo and Perucca [7].

2. Formal setting

Definition 3. For every positive integer n let G_n be a finite group and let H_n be a subgroup of G_n. Suppose that the following properties hold:

(i) For all positive integers n, N such that $n \mid N$ there is a group homomorphism $\pi_{N,n} : G_N \to G_n$. For all positive integers n_1,n_2,n_3 such that $n_3 \mid n_2$ and $n_2 \mid n_1$ we have
$$\pi_{n_1,n_3} = \pi_{n_2,n_3} \circ \pi_{n_1,n_2}\,.$$

(ii) For all coprime positive integers n, m the product map
$$\pi_{nm,n} \times \pi_{nm,m} : G_{nm} \to G_n \times G_m$$
is a group isomorphism. Consequently, G_1 is trivial and for all coprime positive integers N, M such that $n \mid N$ and $m \mid M$ we have (with the identification provided by the above isomorphisms)
$$\pi_{NM,nm} = \pi_{N,n} \times \pi_{M,m}\,.$$

(iii) For all prime numbers ℓ there exists a smallest non-negative integer g_ℓ such that for all integers $E \geqslant e \geqslant g_\ell$ the group homomorphism $\pi_{\ell^E,\ell^e} : G_{\ell^E} \to G_{\ell^e}$ is surjective. For all but finitely many prime numbers ℓ we have $g_\ell = 0$.

(iv) For every positive integer n the restriction of $\pi_{N,n}$ to H_N is surjective onto H_n.

(v) The positive integer $[G_n : H_n]$ is bounded from above by varying $n \geqslant 1$.

We call N_0 the smallest positive integer that is divisible by all integers ℓ^{g_ℓ}. Moreover, if n, m are coprime, we identify H_{nm} with a subgroup of $G_n \times G_m$.

Remark 4. Let n be a positive integer, and consider its prime decomposition $n = \prod_{\ell \mid n} \ell^e$. Properties (i) and (ii) of Definition 3 imply, by iteration, that the product map
$$\prod_{\ell \mid n} \pi_{n,\ell^e} : G_n \to \prod_{\ell \mid n} G_{\ell^e}$$
is a group isomorphism. Consequently, for all positive multiples N of n, considering their prime decomposition $N = \prod_{\ell \mid N} \ell^E$, we have
$$\pi_{N,n} = \prod_{\ell \mid n} \pi_{\ell^E,\ell^e}\,.$$

Lemma 5. *Let n and N be positive integers such that $n \mid N$ and for every prime number ℓ we have $v_\ell(N_0) \leqslant v_\ell(n)$ or $v_\ell(n) = v_\ell(N)$. If the groups G_n and H_n are as in Definition 3, then $\pi_{N,n}$ is surjective and $[G_N : H_N]$ is a multiple of $[G_n : H_n]$.*

Proof. By Remark 4 it is sufficient to prove the first assertion for the prime powers $\ell^{v_\ell(n)} \mid \ell^{v_\ell(N)}$, and we may clearly suppose that $v_\ell(n) \neq v_\ell(N)$. So we have $g_\ell \leqslant v_\ell(n)$ and we may apply Property (iii). The second assertion follows from the first and Property (iv) because we have
$$\#H_N/\#H_n = \#\ker(\pi_{N,n}\mid_{H_N}) \mid \#\ker(\pi_{N,n}) = \#G_N/\#G_n\,.$$
□

Theorem 6. *We work in the setting of Definition 3. There exists a positive integer N such that*
$$[G_n : H_n] = [G_{gcd(n,N)} : H_{gcd(n,N)}] \tag{1}$$
holds for every positive integer n.

Proof. Fix a positive integer N such that $N_0 \mid N$ and such that $[G_N : H_N]$ is maximal among the multiples of N_0. We prove that (1) holds for any positive integer n.

Let S be the set of prime numbers such that $v_\ell(n) > v_\ell(N)$. We then write $a = \prod_{\ell \in S} \ell^{v_\ell(N)}$ and $A = \prod_{\ell \in S} \ell^{v_\ell(n)}$ and $n = An'$ and $N = aN'$. Notice that $n' \mid N'$ and $v_\ell(n') = v_\ell(N') = 0$ holds for every $\ell \in S$. We consider the following commutative diagram:

$$\begin{tikzcd}
H_{AN'} = H_{\mathrm{lcm}(n,N)} \arrow[r] \arrow[d] & H_{aN'} = H_N \arrow[d] \\
H_{An'} = H_n \arrow[r] & H_{an'} = H_{\mathrm{gcd}(n,N)}
\end{tikzcd}$$

The maps in the diagram are surjective by Property (iv). We claim that $\pi_{AN',aN'}$ and $\pi_{An',an'}$ are surjective and that $\#\ker(\pi_{An',an'}) = \#\ker(\pi_{AN',aN'})$.

By maximality of $[G_N : H_N]$ among the multiples of N_0 there are $\#\ker(\pi_{AN',aN'})$ preimages for any element under the upper horizontal map. Indeed, we have

$$[G_{AN'} : H_{AN'}] = [G_N : H_N]$$

and hence

$$\#H_{AN'}/\#H_{aN'} = \#G_{AN'}/\#G_{aN'}\,.$$

To prove (1) it suffices to show that the number of preimages of any element under the lower horizontal map is $\#\ker(\pi_{An',an'})$. Clearly, this number of preimages cannot exceed $\#\ker(\pi_{An',an'})$. Consider an element $(M_a, M_{n'}) \in H_{an'}$ and a lift $(M_a, M_{N'}) \in H_{aN'}$. As shown above, this element has $\#\ker(\pi_{An',an'})$ preimages $(M_A, M_{N'}) \in H_{AN'}$, and their first component are all distinct. The elements $(M_A, M_{n'}) \in H_{An'}$ all have image $(M_a, M_{n'})$ under the lower horizontal map.

As for the claim: the former assertion is true by Lemma 5, while the latter is because $\pi_{An',an'}$ and $\pi_{AN',aN'}$ are the product of $\pi_{A,a}$ and the identity by Property (ii). □

Theorem 7. *We work in the setting of Definition 3, replacing Properties (ii) and (iii) by the following two assumptions for all positive integers m, M, n_1, n_2 such that $m \mid M$ and n_1, n_2 are coprime to M: the map $\pi_{M,m}$ is surjective (consequently, $[G_m : H_m]$ divides $[G_M : H_M]$); the kernels of the maps π_{Mn_1,mn_1} and π_{Mn_2,mn_2} have the same size. There exists a positive integer N such that*

$$[G_n : H_n] = [G_{gcd(n,N)} : H_{gcd(n,N)}] \tag{2}$$

holds for every positive integer n. Moreover, this property is equivalent to $[G_N : H_N]$ being maximal.

Proof. Notice that our assumptions imply $N_0 = 1$. The fact that (2) implies the maximality of $[G_N : H_N]$ is because we have

$$[G_n : H_n] = [G_{gcd(n,N)} : H_{gcd(n,N)}] \mid [G_N : H_N] \qquad \forall n \geqslant 1\,.$$

For the remaining assertions we can make use of the proof of Theorem 6 (where $N_0 = 1$), the only difference being that the claim now holds because of our two new assumptions. □

Remark 8. We work under the assumptions of Theorem 6 (respectively, Theorem 7), and recall that $N_0 = 1$ in the latter case. The results imply that, to compute $[G_n : H_n]$ for every positive integer n, it suffices to compute this index for the finitely many divisors of N. Consider an integer N such that $N_0 \mid N$ and satisfying (1) (equivalently, (2)) for all positive integers n. Then the map $\pi_{n,\mathrm{gcd}(N,n)}$ is surjective (see Lemma 5 for Theorem 6) hence the group H_n is the preimage in G_n of $H_{n,\mathrm{gcd}(n,N)}$ under the map $\pi_{n,\mathrm{gcd}(N,n)}$.

3. Relevant matrix groups

We write $\mathbb{G}_m$ for the multiplicative group and $\mathbb{G}_a$ for the additive group, which are in particular commutative group schemes defined over $\operatorname{Spec}\mathbb{Z}$. For any positive integer d we write $\mathrm{Mat}(d)$ for $\mathbb{G}_a^{d^2}$, choosing an identification of its points with the $d \times d$ matrices. Moreover, we denote by $\mathrm{GL}(d)$ the general linear group of degree d, which is a group scheme defined over $\mathbb{Z}$. We can identify $\mathbb{G}_a^d$ with the $d \times 1$ matrices and hence we may consider the action of $\mathrm{GL}(d)$ on $\mathbb{G}_a^d$ that is given by matrix multiplication. With this action we define the semi-direct product $\mathrm{GL}(d) \ltimes \mathbb{G}_a^d$. If G is a group scheme defined over $\mathbb{Z}$ that is a subgroup scheme of $\mathrm{GL}(d)$, then $G \ltimes \mathbb{G}_a^d$ is a group scheme defined over $\mathbb{Z}$ that is a subgroup scheme of $\mathrm{GL}(d) \ltimes \mathbb{G}_a^d$.

Remark 9. We can identify $\mathrm{GL}(d) \ltimes \mathbb{G}_a^d$ with a subgroup scheme of $\mathrm{GL}(d+1)$. This can be seen by identifying its points with the invertible $d \times d$ matrices with the following properties: the upper $d \times d$ block on the main diagonal is a point of $\mathrm{GL}(d)$; the last row consists of zeroes, with the exception of the last entry that is 1; the first d entries on the last column give a point of $\mathbb{G}_a^d$. Similarly, if G is a subgroup scheme of $\mathrm{GL}(d)$ that is defined over $\mathbb{Z}$, then $G \ltimes \mathbb{G}_a^d$ is a subgroup scheme of $\mathrm{GL}(d+1)$ that is defined over $\mathbb{Z}$ (the $d \times d$ block being now in G).

If G is a subgroup scheme of $\mathrm{GL}(d)$ defined over $\mathbb{Z}$, then for any positive integer n we denote by $G(\mathrm{mod} n)$ the group of points of G over $\mathbb{Z}/n\mathbb{Z}$, which consists of invertible $d \times d$ matrices with entries in $\mathbb{Z}/n\mathbb{Z}$, setting $G(\mathrm{mod} 1)$ to be the trivial group. If ℓ is a prime number, we define $\mathrm{GL}(d, \mathbb{Z}_\ell)$ to be the group of $\mathbb{Z}_\ell$-points of $\mathrm{GL}(d)$, and we similarly define $\mathrm{GL}(d, \hat{\mathbb{Z}})$.

Remark 10. If n, N are positive integers such that $n \mid N$ then the reduction modulo n provides a group homomorphism $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and hence (by considering the reduction entrywise) it induces a group homomorphism $\pi_{N,n} : \mathrm{GL}(d, \mathrm{mod} N) \to \mathrm{GL}(d, \mathrm{mod} n)$. For all positive integers n_1, n_2, n_3 such that $n_3 \mid n_2$ and $n_2 \mid n_1$ we have $\pi_{n_1,n_3} = \pi_{n_2,n_3} \circ \pi_{n_1,n_2}$ because this property holds for the reductions of the integers. Moreover, the reduction maps $\pi_{N,n}$ are surjective (because for any $E \geqslant e \geqslant 0$ the lift of a matrix that is invertible modulo ℓ^e is invertible modulo ℓ^E). The same properties hold replacing $\mathrm{GL}(d)$ by $\mathrm{GL}(d) \ltimes \mathbb{G}_a^d$ (in view of Remark 9), where the map $\pi_{N,n}$ is the reduction modulo n.

Lemma 11. *Let G be a subgroup scheme of $\mathrm{GL}(d)$ that is defined over $\mathbb{Z}$. For all coprime positive integers n, m, we have a group isomorphism*

$$\pi_{nm,n} \times \pi_{nm,m} : G(\mathrm{mod} nm) \to G(\mathrm{mod} n) \times G(\mathrm{mod} m)\,.$$

The analogous result holds for the semi-direct product $G \ltimes \mathbb{G}_a^d$.

Proof. By Chinese remainder theorem the product of the reductions modulo n and modulo m gives an isomorphism

$$\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\,.$$

This isomorphism extends to the invertible $d \times d$ matrices with entries in those rings (because an integer is invertible modulo nm if and only if it is invertible modulo n and modulo m). For the first assertion, we may conclude because G is defined by polynomial equations with integer coefficients (and an equality of integers holds modulo nm if and only if it holds modulo n and modulo m). The second assertion follows by Remark 9. □

Remark 12. Let ℓ be a prime number, and consider a Cartan subgroup C of $\mathrm{GL}(2, \mathbb{Z}_\ell)$. Let $c, d \in \mathbb{Z}$ be parameters for C (see [6, Theorem 8 and Remark 9]). As shown in [6, Section 2.4 and Lemma 13], for any non-negative integer n the group of points of C over $\mathbb{Z}/\ell^n\mathbb{Z}$ consists of the invertible matrices of the form

$$\begin{pmatrix} x & (d \bmod \ell^n)y \\ y & x + y(c \bmod \ell^n) \end{pmatrix}$$

where $x, y \in \mathbb{Z}/\ell^n\mathbb{Z}$. Then the reduction map $C(\mathrm{mod}\ell^E) \to C(\mathrm{mod}\ell^e)$ is surjective for all non-negative integers $E \geqslant e$.

Remark 13. Fix some positive integer g and consider the algebraic group $\mathrm{GSp}(2g)$ of symplectic similitudes, which is a subgroup scheme of $\mathrm{GL}(2g)$ that is defined over $\mathbb{Z}$. Denoting by I the $g \times g$ identity matrix and considering the matrix $J = \begin{pmatrix} & I \\ -I & \end{pmatrix}$, we have

$$\mathrm{GSp}(2g) := \{M \in \mathrm{GL}(2g) \mid \exists \lambda \in \mathbb{G}_m, M^T J M = \lambda J\}\,.$$

For every prime number ℓ and for all integers $E \geqslant e \geqslant 0$ the reduction map

$$\pi_{\ell^E,\ell^e} : \mathrm{GSp}(2g, \mathrm{mod}\ell^E) \to \mathrm{GSp}(2g, \mathrm{mod}\ell^e)$$

is surjective. This holds by the infinitesimal lifting criterion [13, Lemma 37.11.7] because $\mathrm{GSp}(2g)$ is an algebraic subgroup of $\mathrm{GL}(2g)$ that is defined over $\mathbb{Z}$ and it is reductive hence smooth (see [9, Section 1.2.1]).

4. Torsion and arboreal representations of commutative algebraic groups

Let $\mathcal{A}$ be a connected commutative algebraic group of positive dimension defined over a number field K. We fix some algebraic closure $\bar{K}$ of K and let $\mathcal{G}_K := \mathrm{Gal}(\bar{K}/K)$ be the absolute Galois group of K. We will consider the Kummer representations associated to a point $P \in \mathcal{A}(K)$ of infinite order (supposing that such a point exists).

4.1. **Torsion points and torsion representations.** For every positive integer n we denote by $\mathcal{A}[n]$ the subgroup of $\mathcal{A}(\bar{K})$ consisting of the torsion points of order dividing n. Choosing a basis for $\mathcal{A}[n]$ we identify this group with $(\mathbb{Z}/n\mathbb{Z})^b$, where b is the first Betti number of $\mathcal{A}$. If $\mathcal{A}$ is a torus (respectively, an abelian variety) then b is the dimension (respectively, twice the dimension) of $\mathcal{A}$.

If n,m are positive integers, then the multiplication by m is a surjective group homomorphism $\mathcal{A}[nm] \to \mathcal{A}[n]$ whose corresponding map $(\mathbb{Z}/nm\mathbb{Z})^b \to (\mathbb{Z}/n\mathbb{Z})^b$ is the reduction modulo n. We say that basis choices in $\mathcal{A}[nm]$ and $\mathcal{A}[n]$ are coherent if the latter basis is the image of the former under multiplication by m.

The field $K(\mathcal{A}[n])$ obtained by adjoining the coordinates of the points in $\mathcal{A}[n]$ is a finite Galois extension of K. Any Galois automorphism acts $\mathbb{Z}/n\mathbb{Z}$-linearly on $\mathcal{A}[n]$, and this action defines the *torsion representation* of $\mathcal{A}$, namely the group homomorphism

$$\rho_n : \mathcal{G}_K \to \mathrm{Aut}(\mathcal{A}[n])\,.$$

Notice that ρ_n factors through the Galois group of $K(\mathcal{A}[n])/K$ because its kernel is the Galois group of $\bar{K}/K(\mathcal{A}[n])$.

Choosing (coherently) a $\mathbb{Z}/n\mathbb{Z}$ basis of $\mathcal{A}[n]$, we identify $\mathrm{Im}(\rho_n)$ with a subgroup of $\mathrm{GL}_b(\mathbb{Z}/n\mathbb{Z})$. For all positive integers n, N such that $n \mid N$ the Galois action on $\mathcal{A}[N]$ determines, by restriction, the action on $\mathcal{A}[n]$ and ρ_n is the composition of ρ_N with the reduction modulo n. So we have:

Remark 14. Property (iv) from Definition 3 holds for $H_n := \mathrm{Im}(\rho_n)$, considering the restriction of the reduction map on $\mathrm{GL}(d, \bmod N)$.

Remark 15. Consider subgroups $G_n < \mathrm{GL}(b, \bmod n)$ such that $G_n = G(\bmod n)$ holds for some subgroup scheme G of $\mathrm{GL}(b)$ that is defined over $\mathbb{Z}$. Setting $\pi_{N,n}$ to be the reduction modulo n, Properties (i) and (ii) from Definition 3 hold. Indeed, the former property is because $\pi_{N,n}$ is the restriction of the reduction map on $\mathrm{GL}(b, \bmod N)$, while the latter property holds by Lemma 11.

If $\mathcal{A}$ is an abelian variety, as a candidate for the group G we may consider the Zariski closure of the Mumford-Tate group $\mathrm{MT}(\mathcal{A})$.

4.2. **Division points and arboreal representations.** Consider a point $P \in \mathcal{A}(K)$ of infinite order. For every positive integer n we let $n^{-1}P$ be the set of points in $\mathcal{A}(\bar{K})$ that are mapped to P under multiplication by n. We may consider $P_n \in n^{-1}P$ such that for all positive integers n, m we have $[m]P_{nm} = P_n$. Remark that $n^{-1}P$ consists of the points $P_n + T_n$ for $T_n \in \mathcal{A}[n]$, so we have $K(\mathcal{A}[n], n^{-1}P) = K(\mathcal{A}[n], P_n)$. We also define $n^{-1}\mathbb{Z}P$ as the group generated by $n^{-1}P$ (it consists of the points whose image under multiplication by n is a multiple of P).

Since the multiplication by n on $\mathcal{A}$ is defined over K and it has a finite kernel, for any $n \geqslant 1$ the extensions $K(\mathcal{A}[n])/K$ and $K(\mathcal{A}[n], P_n)/K$ are finite and Galois. Moreover, the extension $K(\mathcal{A}[n], P_n)/K(\mathcal{A}[n])$ is abelian because its Galois group can be identified to a subgroup of $\mathcal{A}[n]$ thanks to the *Kummer map*, which is the group homomorphism

$$\begin{aligned} \kappa_n : \mathrm{Gal}(\bar{K}/K(\mathcal{A}[n])) &\to \mathcal{A}[n] \\ \sigma &\mapsto \sigma(P_n) - P_n\,. \end{aligned}$$

Notice that this map does not depend on the choice of $P_n \in n^{-1}P$ because by definition σ is the identity on $\mathcal{A}[n]$. Moreover, this map factors through the Galois group of $K(\mathcal{A}[n], P_n)/K(\mathcal{A}[n])$

and the quotient map is injective. By considering (coherently) bases for $\mathcal{A}[n]$ we identify this group with $(\mathbb{Z}/n\mathbb{Z})^b$ and $\operatorname{Im}(\kappa_n)$ to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^b$. Notice that for all positive integers n, m the group $[m]\operatorname{Im}(\kappa_{nm})$ is a subgroup of $\operatorname{Im}(\kappa_n)$.

The *arboreal representation* describes the Galois action on $n^{-1}\mathbb{Z}P$. Knowing the Galois action on $n^{-1}\mathbb{Z}P$ is equivalent to knowing the action on $\mathcal{A}[n]$ and P_n. This is why we define the arboreal representation as the group homomorphism

$$\rho'_n : \mathcal{G}_K \to \mathrm{GL}_b(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^b \qquad \sigma \mapsto (\rho_n(\sigma), \sigma(P_n) - P_n)\,.$$

This map factors through the Galois group of $K(\mathcal{A}[n], P_n)/K$ and the quotient map is injective.

Remark 16. For all positive integers n, N such that $n \mid N$, the Galois action on $N^{-1}\mathbb{Z}P$ determines by restriction the action on $n^{-1}\mathbb{Z}P$. Then ρ'_n is the composition of ρ'_N with the reduction modulo n. So we have a surjective group homomorphism $\operatorname{Im}(\rho'_N) \to \operatorname{Im}(\rho'_n)$.

5. Eventual maximal growth of the Kummer extensions

We keep the notation introduced in the previous sections, and consider a point $P \in \mathcal{A}(K)$ of infinite order. We call $\mathcal{A}_P$ the smallest (not necessarily connected) algebraic subgroup of $\mathcal{A}$ defined over K that contains P. The connected component $\mathcal{A}_P^0$ of $\mathcal{A}_P$ that contains zero is a connected commutative algebraic group defined over K (the dimension of $\mathcal{A}_P^0$ is positive because P has infinite order). We write c_P for the number of connected components of $\mathcal{A}_P$, which is finite.

For example, if $\mathcal{A} = A \times T$ is the product of an abelian variety A and a torus T, then we have $\mathcal{A}_P^0 = A' \times T'$ for some abelian subvariety A' of A and a torus T' which is an algebraic subgroup of T (because there is no non-zero homomorphism from A to $\mathbb{G}_m$ or conversely).

We now consider the Kummer map:

Lemma 17. *We have* $[c_P]\operatorname{Im}(\kappa_n) < \mathcal{A}_P^0[\frac{n}{\gcd(c_P,n)}]$. *Consequently,* $\operatorname{Im}(\kappa_n)$ *is contained in the group* $\langle \mathcal{A}_P^0[n], \mathcal{A}[\gcd(c_P, n)]\rangle$.

Proof. We know that $\operatorname{Im}(\kappa_n)$ is a subgroup of $\mathcal{A}[n]$, so we are left to prove that $[c_P]\operatorname{Im}(\kappa_n)$ consists of torsion points in $\mathcal{A}_P^0$. If $\sigma \in \mathcal{G}_K$, then $c_P(\sigma(P_n) - P_n) = \sigma(c_P P_n) - c_P P_n$. The point $c_P P_n$ is in $n^{-1}(c_P P)$, so we are left to prove that the image of the Kummer map κ'_n for the point $c_P P$ consists of points in $\mathcal{A}_P^0$. We conclude because the image of the Kummer map does not depend on the choice of the division point so we have $\kappa'_n(\sigma) = \sigma(P'_n) - P'_n$ where $P'_n \in n^{-1}(c_P P) \cap \mathcal{A}_P^0(\bar{K})$. □

Remark that, in the following property, the ratio is an integer by Lemma 17 because the denominator is the size of $\operatorname{Im}(\kappa_n)$:

Definition 18 (Eventual maximal growth of the Kummer extensions)**.** The positive integer

$$\frac{\#\mathcal{A}_P^0[n] \cdot c_P^b}{[K(\mathcal{A}[n], n^{-1}P) : K(\mathcal{A}[n])]}$$

is bounded independently of n.

Lemma 19. *If the eventual maximal growth of the Kummer extensions holds under the assumption that* $c_P = 1$, *then it holds in general.*

Proof. The property holds for the point $c_P P$, which generates the connected algebraic group $\mathcal{A}_P^0$. We deduce that the property holds for P because the degree of $K(\mathcal{A}[n], n^{-1}P)/K(\mathcal{A}[n])$ is a multiple of the degree of $K(\mathcal{A}[n], n^{-1}(c_P P))/K(\mathcal{A}[n])$. □

Remark 20. Suppose that $\mathcal{A}$ is the product of an abelian variety and a torus. Betrand's theorem [1, Theorem 1] states that the eventual growth of the Kummer extensions holds for $c_P = 1$. If $\mathcal{A}$ is an abelian variety, a proof of Bertrand's result [1, Theorem 1] is provided by Hindry in [3, Lemme 14] and by Bertrand in [1, Theorème 5.2]. If $\mathcal{A}$ is a torus, Bertrand's result has a proof that relies on Schinzel's theorem on abelian radical extensions, see [10, Corollary 2] by Perucca and Sgobba.

Remark 21. Notice that $\mathcal{A}^0_P[n]$ is mapped to itself by any Galois automorphism hence $\operatorname{Im}(\rho_n)$ acts on it. If $c_P = 1$, then $\operatorname{Im}(\rho'_n)$ is a subgroup of $\operatorname{Im}(\rho_n) \ltimes \mathcal{A}^0_P[n]$. This is because we may choose $P_n \in \mathcal{A}^0_P(\bar{K})$ hence for any $\sigma \in \mathcal{G}_K$ we have $\sigma(P_n) - P_n \in \mathcal{A}^0_P[n]$. Moreover, the index of $\operatorname{Im}(\rho'_n)$ in $\operatorname{Im}(\rho_n) \ltimes \mathcal{A}^0_P[n]$ is bounded by varying n if $\mathcal{A}$ and P are as in Definition 18 because the ratio $\# \operatorname{Im}(\rho'_n)/\# \operatorname{Im}(\rho_n)$ is the denominator in (18).

6. Applications of the formal setting

In this section we present various situations where we can apply our formal framework from Section 2 to investigate the torsion and arboreal representations of a connected commutative algebraic group $\mathcal{A}$ defined over a number field K. We keep the notation introduced in the previous sections. With a choice for the basis of $\mathcal{A}[n]$ (coherent by varying n) we identify $H_n := \operatorname{Im}(\rho_n)$ with a subgroup of $\operatorname{GL}(b, \operatorname{mod} n)$.

6.1. **Powers of commutative algebraic groups.** Suppose that there are subgroups G_n of $\operatorname{GL}(b, \operatorname{mod} n)$ such that H_n and G_n satisfy the properties in Definition 3 (where the map $\pi_{N,n}$ is the reduction modulo n). Now consider the algebraic group $\mathcal{A}^m$ for some positive integer m. We then work in $\operatorname{GL}(bm, \operatorname{mod} n)$, choosing as basis for $\mathcal{A}^m[n]$ the torsion points whose m entries belong to the given basis of $\mathcal{A}[n]$. The image of the modulo n torsion representation for $\mathcal{A}^m$, which we denote by $\hat{H}_n$, is a subgroup of $\operatorname{GL}(bm, \operatorname{mod} n)$. We have $\#\hat{H}_n = \#H_n$. More precisely, the elements of $\hat{H}_n$ are the $bm \times bm$ matrices whose non-zero entries are in the m blocks on the main diagonal of size $b \times b$; all such blocks are equal and they are in H_n. With this same construction for G_n we obtain subgroups $\hat{G}_n$ of $\operatorname{GL}(bm, \operatorname{mod} n)$ such that $\#\hat{G}_n = \#G_n$. Moreover, $\hat{H}_n$ and $\hat{G}_n$ satisfy the properties in Definition 3 (considering the reduction maps). Now consider algebraic groups $\mathcal{A}_1, \dots, \mathcal{A}_r$ defined over K and positive integers $e_1, \dots, e_r$. A straightforward adaptation of the above reasoning allows us to describe the modulo n torsion representation for $\prod_i \mathcal{A}_i^{e_i}$ starting from the modulo n torsion representation for $\prod_i \mathcal{A}_i$.

6.2. **Elliptic curves.** Consider first an elliptic curve $\mathcal{A}$ that is without CM over $\bar{K}$.

Proof of Theorem 1. For every $n \geqslant 1$ we set $G_n := \operatorname{GL}(\operatorname{mod} n)$. By Theorem 6 it suffices to show that G_n and H_n satisfy the properties of Definition 3, letting $\pi_{N,n}$ be the reduction modulo n. We may apply Remarks 14, 10, and 15 while Property (v) is Serre's open image theorem [12, Theorem 3']. □

We refer to [8, Theorem 1.1] for an explicit description of the Cartan group C and the matrix M (with a suitable coherent choice for the basis of $\mathcal{A}[n]$) mentioned in the following result.

Theorem 22. *Let $\mathcal{A}$ be an elliptic curve with CM over $\bar{K}$. If the complex multiplication is defined over K, then there exists a Cartan subgroup C of* $\operatorname{GL}(2)$ *defined over* $\mathbb{Z}$ *such that Theorems 6 and 7 apply to $H_n := \operatorname{Im}(\rho_n)$ and $G_n := C(\operatorname{mod} n)$, the maps $\pi_{N,n}$ being the reduction modulo n. If the complex multiplication is not defined over K, then Theorem 7 applies, taking instead $G_n := \langle (M \bmod n), C(\operatorname{mod} n)\rangle$, where C is a Cartan subgroup C of* $\operatorname{GL}(2)$ *defined over* $\mathbb{Z}$ *and $(M \bmod n)$ is the reduction modulo n of a matrix $M \in \operatorname{GL}(2, \mathbb{Z})$ such that M^2 is the identity, and such that $(M \bmod n) \notin C(\operatorname{mod} n)$.*

Proof. Remark 14 gives Property (iv) of Definition 3. We assume to make coherent base choices for $\mathcal{A}[n]$ as in [8]. The fact that H_n is a subgroup of G_n and that the index $[G_n : H_n]$ is bounded follows from [8, Theorem 1.1]. If the complex multiplication is defined over K, Remarks 15 and 12 (see also Lemma 5) imply Properties (i), (ii), and (iii) of Definition 3 with $N_0 = 1$, and also the two additional assumptions of Theorem 7. If the complex multiplication is not defined over K, Property (i) and the two additional assumptions in Theorem 7 hold by Remark 10 and the explicit description of G_n given in [8, Theorem 1.1]. □

6.3. **Abelian varieties of type GSp.** Let $\mathcal{A}$ be an abelian variety of positive dimension $g \notin \mathcal{S}$ (for example, if $g = 2$ or g is odd), where

$$\mathcal{S} = \Big\{ g \geqslant 1 \mid \exists k \geqslant 3, \text{ odd }, \exists a \geqslant 1, g = 2^{k-1}a^k \} \cup \{ g \geqslant 1 \mid \exists k \geqslant 3, \text{ odd}, \ g = \frac{1}{2}\binom{2k}{k} \Big\} .$$

We fix a polarization of $\mathcal{A}$ and an embedding of K into $\mathbb{C}$. We say that $\mathcal{A}$ is of type GSp if the Mumford Tate group of $\mathcal{A}$ is $\mathrm{GSp}(2g)$ (see Remark 13), which holds if $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$ and $g \notin S$. Because of the Weil pairing, with an appropriate choice of basis of $\mathcal{A}[n]$ (coherent by varying n) we identify $\mathrm{Im}(\rho_n)$ with a subgroup of $\mathrm{GSp}(\mathrm{mod} n)$.

Theorem 23. *Let $\mathcal{A}$ be an abelian variety such that $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$ and $g \notin S$. Then Theorem 6 applies to $H_n := \mathrm{Im}(\rho_n)$ and $G_n := \mathrm{GSp}(2g, \mathrm{mod} n)$ (the map $\pi_{N,n}$ being the reduction modulo n).*

Proof. It suffices to show that G_n and H_n satisfy the properties of Definition 3. We may apply Remarks 15 and 14. Property (iii) holds by Remark 13. Property (v) holds because the adelic Mumford Tate conjecture amounts to the ℓ-adic Mumford Tate conjecture [2, Theorem 5.3] and the latter holds by [4, Theorem 1.1]. □

6.4. **Abelian varieties with real multiplication.** Let $\mathcal{A}$ be an abelian variety of dimension g defined over a number field K that has real multiplication. This means that its endomorphism algebra is a totally real number field, which we call F. We suppose that $F/\mathbb{Q}$ has degree g. Let $\mathcal{O}$ be the ring of integers of F, and choose an identification of $\mathcal{O}$ with $\mathbb{Z}^g$. This induces (coherently by varying n) an identification of $(\mathbb{Z}/n\mathbb{Z})$-modules between $\mathcal{O}/n\mathcal{O}$ and $(\mathbb{Z}/n\mathbb{Z})^g$. Then we identify $\mathrm{GL}(2, \mathcal{O}/n\mathcal{O})$ with a subgroup of $\mathrm{GL}(2g, n)$.

Theorem 24. *Let $\mathcal{A}$ be an abelian variety that has real multiplication such that the degree over $\mathbb{Q}$ of its endomorphism algebra is g. Suppose that the open image theorem holds for the torsion representations (some sufficient conditions can be found in [11]). Then Theorem 6 applies to $H_n := \mathrm{Im}(\rho_n)$ and $G_n := \mathrm{GL}(2, \mathcal{O}/n\mathcal{O})$ (the maps $\pi_{N,n}$ being the reduction modulo n).*

Proof. It suffices to verify that the properties in Definition 3 hold. Property (v) holds by assumption, and the other properties are immediate by the definition of G_n and $\pi_{N,n}$, see also Remarks 15 and 14. □

6.5. **Tori.** We denote by ζ_n a root of unity in $\bar{K}$ of order n and let Ω be a positive integer such that the largest cyclotomic subextension of K is contained in $\mathbb{Q}(\zeta_\Omega)$.

For the multiplicative group $\mathcal{A} = \mathbb{G}_m$ we have $\mathcal{A}[n] = \langle \zeta_n \rangle$. A Galois automorphism maps $\zeta_n \mapsto \zeta_n^a$ where a is some integer coprime to n. Thus the image of ρ_n can be identified to a subgroup of $\mathrm{GL}(1, \mathrm{mod} n)$. The index of $\mathrm{Im}(\rho_n)$ in $\mathrm{GL}(1, \mathrm{mod} n)$ is finite because the former group contains all matrices $(a \bmod n)$ where a is an integer coprime to n such that $a \equiv 1 \bmod \Omega$. By the discussion in Section 6.1 we deduce that for $\mathcal{A} = \mathbb{G}_m^b$ the image of ρ_n can be identified to a subgroup of $\mathrm{GL}(b, \mathrm{mod} n)$ that has finite index in the scalar matrices.

Now let $\mathcal{A}$ be a non-split one-dimensional torus defined by an equation of the form $x^2 - dy^2 = 1$, where $d \in K^\times \backslash K^{\times 2}$. The splitting field is $K(\sqrt{d})$. For every $n \geqslant 1$ the group $\mathcal{A}[n]$ is cyclic, and the points of order n are those of the form

$$T_n = \Big(\frac{\zeta_n + \zeta_n^{-1}}{2}, \frac{\zeta_n - \zeta_n^{-1}}{2\sqrt{d}} \Big) .$$

For any $\sigma \in \mathcal{G}_K$ we have $\sigma(T_n) = mT_n$ for some integer m coprime to n. So $\mathrm{Im}(\rho_n)$ is a subgroup of $\mathrm{GL}(1, \mathrm{mod} n)$. Notice that $\sigma(T_n)$ is determined by $\sigma(\zeta_n) = \zeta_n^a$ and $\sigma(\sqrt{d}) = (-1)^\epsilon \sqrt{d}$. We have

$$\sigma(T_n) = \Big(\zeta_n^{(-1)^\epsilon a} + \zeta_n^{-(-1)^\epsilon a}, \frac{\zeta_n^{(-1)^\epsilon a} - \zeta_n^{-(-1)^\epsilon a}}{2\sqrt{d}} \Big)$$

hence m and $(-1)^\epsilon a$ are congruent modulo n.

More generally, let $\mathcal{A}$ be a torus of dimension $b \geqslant 1$ defined over K. Let L/K be a finite Galois extension such that there is an isomorphism $\xi : \mathcal{A} \to \mathbb{G}_m^b$ of algebraic groups that is defined over

L. For any n we can choose (in a coherent way) a basis $\{\zeta_n\}$ for $\mathbb{G}_m[n]$, and then we have a basis for $\mathbb{G}_m^b[n]$ whose elements have all coordinates 1 except for one coordinate that is equal to ζ_n. By taking the preimage under ξ of this basis we have chosen (in a coherent way) a basis for $\mathcal{A}[n]$. The image of ρ_n is then identified to a subgroup of $\mathrm{GL}(b, \bmod n)$. By restricting to the Galois automorphisms that are the identity on L we deduce from the split case that $\mathrm{Im}(\rho_n)$ contains a subgroup of the scalar matrices whose index is bounded by varying n.

We have a group homomorphism

$$\psi : \mathcal{G}_K \to \mathrm{GL}(b, \mathbb{Z}) \qquad \sigma \mapsto \xi^{-1}(\sigma^{-1}\xi\sigma)$$

that factors through $\mathrm{Gal}(L/K)$, and we call ψ_n the composition of ψ with the reduction map from $\mathrm{GL}(b, \mathbb{Z})$ to $\mathrm{GL}(b, \bmod n)$. We remark that $\mathcal{A}$ is determined up to a K-isomorphism by the conjugacy class of ψ (meaning, up to conjugating with a fixed matrix in $\mathrm{GL}(b, \mathbb{Z})$). With the above choice of the basis for $\mathcal{A}[n]$, we have

$$\rho_n(\sigma) = \chi_n(\sigma)\psi_n(\sigma)\,,$$

where $\chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ is the image of σ under the modulo n torsion representation of $\mathbb{G}_m$, composed with the natural identification of a 1×1 matrix with its only entry.

Theorem 25. *If $\mathcal{A}$ is a torus, then Theorem 6 applies to $H_n := \mathrm{Im}(\rho_n) < \mathrm{GL}(b, \bmod n)$ and the subgroup G_n of $\mathrm{GL}(b, \bmod n)$ that is generated by the scalar matrices and $\mathrm{Im}(\psi_n)$ (the maps $\pi_{N,n}$ being the reduction modulo n). In particular, for a one-dimensional torus, we have $G_n = \mathrm{GL}(1, \bmod n)$.*

Proof. We verify the properties of Definition 3. Properties (i), (ii), and (iv) hold by Remarks 15 and 14. By the above discussion, $\mathrm{Im}(\psi)$ is finite and $H_n < G_n$. By considering the split torus over L, we deduce that Property (v) holds. Finally, Property (iii) holds because the reduction modulo n of a scalar matrix in $\mathrm{GL}(b, \bmod N)$ is a scalar matrix, while ψ_n is the composition of ψ_N and the reduction modulo n. □

6.6. **Application of the formal setting to arboreal representations.** We now investigate the arboreal representations ρ'_n associated to a point $P \in \mathcal{A}(K)$ of infinite order. We set $H_n := \mathrm{Im}(\rho_n) < \mathrm{GL}(b, \bmod n)$, after having (coherently) chosen a basis $T_{n,1}, \ldots, T_{n,b}$ for $\mathcal{A}[n]$.

With the construction from Remark 9 we then identify $H'_n := \mathrm{Im}(\rho'_n)$ with a subgroup of $\mathrm{GL}(b+1, \bmod n)$. In particular, for any element of H'_n the following holds: all entries in the last row are 0, with the exception of the last entry that is 1; the upper $b \times b$ block on the main diagonal is in H_n; if $c_P = 1$, the first b entries $m_1, \ldots, m_b$ in the last column are such that the point $\sum_i m_i T_{n,i}$ belongs to $\mathcal{A}_P^0[n]$, see Remark 21 (by choosing a basis for $\mathcal{A}[n]$ such that the first elements are a basis for $\mathcal{A}_P^0[n]$ the last condition means $m_{b_P+1} = \cdots = m_b = 0$, where b_P is the Betti number of $\mathcal{A}_P^0$).

Theorem 26. *Let $c_P = 1$ and suppose that $\mathcal{A}$ and P are as in Definition 18. Suppose that $H_n := \mathrm{Im}(\rho_n)$ and groups $G_n < \mathrm{GL}(b, \bmod n)$ satisfy all assumptions in Theorem 6 (respectively, Theorem 7) with the reduction maps. Then the same holds for H'_n and for the subgroups G'_n of $\mathrm{GL}(b+1, \bmod n)$ defined by the following conditions: all entries in the last row are 0, with the exception of the last entry that is 1; the upper $b \times b$ block on the main diagonal is in G_n; the first b entries $m_1, \ldots, m_b$ in the last column are such that the point $\sum_i m_i T_{n,i}$ belongs to $\mathcal{A}_P^0[n]$. The map $G_N \to G_n$ is the reduction modulo n.*

Proof. We consider the properties of Definition 3 and the two additional assumptions of Theorem 7. Property (i) is clear because we are considering the reduction maps. For the former case, Property (ii) holds by Remark 15. Property (iii) (respectively, the assumptions of Theorem 7) hold because they hold for the groups G_n and $\mathbb{Z}/n\mathbb{Z}$. Property (iv) is due to the fact that the Galois action on $N^{-1}P$ determines the Galois action on $n^{-1}P$. Finally, Property (v) holds because by assumption it holds for the index $[G_n : H_n]$ and because we may apply Remark 21. □

Proof of Theorem 2. Since $\mathcal{A}$ has dimension 1, we have $\mathcal{A}_P = \mathcal{A}$ and in particular $c_P = 1$. Then the result follows from Theorem 1, in view of Theorem 26 and Remark 20. □

To study arboreal representations we may reduce to the case $c_P = 1$:

Remark 27. Denote by $\tilde{\rho}'_n$ the arboreal representation for the point $c_P P \in \mathcal{A}(K)$. To study $\tilde{\rho}'_n$ it is clearly sufficient to study the product map $(\rho'_n, \rho_{c_P n})$. We now explain how to identify the representations (ρ'_n, ρ_{cn}) and $\tilde{\rho}'_{c_P n}$. We can write $P_n = Q_{c_P n} + T_{c_P n}$ for some $Q_{c_P n} \in \mathcal{A}^0_P(\bar{K})$ such that $[c_P n]Q_{c_P n} = c_P P$ and $T_{c_P n} \in \mathcal{A}[c_P n]$. Consider $\sigma \in \mathcal{G}_K$. The image of σ under (ρ'_n, ρ_{cn}) amounts to $\rho_{c_P n}(\sigma)$ (which determines $\rho_n(\sigma)$) and $\sigma(P_n) - P_n$. The image of σ under $\tilde{\rho}'_{c_P n}$ amounts to $\rho_{c_P n}(\sigma)$ and $\sigma(Q_{c_P n}) - Q_{c_P n}$. The image of σ under one map determines the image under the other map because we have

$$(\sigma(P_n) - P_n) - (\sigma(Q_{c_P n}) - Q_{c_P n}) = \sigma(T_n) - T_n = (\rho_{c_P n}(\sigma))T_n - T_n\,.$$

Acknowledgements

The first-named author is supported by the Luxembourg National Research Fund AFR-PhD 16981197. A CC BY or equivalent licence is applied to the AAM/VoR arising from this submission, in accordance with the grant's open access conditions. The authors thank Jan Vonk for helpful discussions.

References

[1] D. Bertrand, *Galois representations and transcendental numbers*, in: A. Baker (Ed.), New Advances in Transcendence Theory (Durham 1986), Cambridge University Press, 1988, 37–55. 6

[2] A. Cadoret and B. Moonen, *Integral and adelic aspects of the Mumford-Tate conjecture*, J. Inst. Math. Jussieu **19**, No. 3 (2020), 869–890. 8

[3] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603. 6

[4] M. Hindry and N. Ratazzi, *Points de torsion sur les variétés abéliennes de type GSp*, J. Inst. Math. Jussieu **11**, No. 1 (2012), 27–65. 8

[5] R. Jones and J. Rouse, *Galois theory of iterated endomorphisms*, Proc. Lond. Math. Soc. **100**, No. 3 (2010), 763–794. 1

[6] D. Lombardo and A. Perucca, *The 1-eigenspace for matrices in* $\mathrm{GL}_2(\mathbb{Z}_\ell)$, New York J. Math. **23** (2017), 897–925. 4

[7] D. Lombardo and A. Perucca, *Reductions of points on algebraic groups*, Inst. Math. Jussieu **20**, No. 5 (2021), 1637–1669. 1

[8] A. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, Algebra Number Theory **16**, No. 4 (2022), 777–837. 7

[9] S. Morel, *Shimura varieties*, (2023), https://arxiv.org/abs/2310.16184. 5

[10] A. Perucca and P. Sgobba, *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory **15**, No. 8 (2019), 1617–1633. 6

[11] K. Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98**, No. 3 (1976), 751–804. 8

[12] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 123–201. 7

[13] The Stacks Project Authors, *Stacks Project*, (2018), https://stacks.math.columbia.edu/tag/02H6. 5