JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jędrzej GARNEK

On class numbers of division fields of abelian varieties

Tome 31, nº 1 (2019), p. 227-242.

<http://jtnb.cedram.org/item?id=JTNB_2019__31_1_227_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 227–242

On class numbers of division fields of abelian varieties

par Jędrzej GARNEK

Résumé. Soit A une variété abélienne définie sur un corps de nombres K. On fixe un nombre premier p et pour tout nombre naturel n, on note K_n le corps engendré sur K par les coordonnées des points de p^n-torsion de A. Nous donnons une minoration de l'ordre de la p-partie du groupe de classes de K_n pour $n \gg 0$, en construisant une extension non ramifiée suffisamment grande de K_n. Cette minoration dépend du rang du groupe de Mordell–Weil de A et de la réduction des points de p-torsion en nombres premiers au-dessus de p.

Abstract. Let A be an abelian variety defined over a number field K. Fix a prime p and a natural number n and consider the field K_n, obtained by adjoining to K all the coordinates of the p^n-torsion points of A. We give a lower bound on the p-part of the class group of K_n for large n, by finding a large unramified extension of K_n. This lower bound depends on the Mordell–Weil rank of A and the reduction of p-torsion points modulo primes above p.

1. Introduction

Let us fix a prime p. Denote by K a number field with ring of integers $\mathcal{O}_K$. Let A be an abelian variety of dimension d defined over K and let $\mathcal{R} := \mathrm{End}_K(A)$. Let us consider the p^nth division field of A:

$$K_n := K(A[p^n]).$$

Let $\mathrm{Cl}(K_n)$ be the ideal class group of K_n, defined as the quotient of the group of fractional ideals of the ring of integers of K_n by the subgroup of principal ideals. We define the number k_n by the equality:

$$\#\,\mathrm{Cl}(K_n)[p^\infty] = p^{k_n}.$$

In this paper we prove lower bounds on k_n. Let $\mathfrak{p}$ be a prime of K lying above p with residue field $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. In case when A has a good reduction at $\mathfrak{p}$, we denote the special fiber of the Néron model of A by $A_\mathfrak{p}$ and the reduction homomorphism by:

$$\mathrm{red}_\mathfrak{p} : A(\overline{K}) \to A_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p}).$$

Manuscrit reçu le 28 mai 2018, révisé le 24 septembre 2018, accepté le 16 novembre 2018.
2010 *Mathematics Subject Classification.* 11R29, 11G10.
Mots-clefs. division fields, class number, abelian varieties.
The author was supported by NCN research grant UMO-2017/27/N/ST1/00497 and by the doctoral scholarship of Adam Mickiewicz University.

We define also:

$$h_{\mathfrak{p}} := \begin{cases} \dim_{\mathbb{F}_p} \ker\left(A[p] \to A_{\mathfrak{p}}[p]\right), & \text{if } A \text{ has good reduction at } \mathfrak{p}, \\ 2d, & \text{otherwise.} \end{cases} \tag{1.1}$$

Note that for a given prime $\mathfrak{p}$ of good reduction we can compute $h_{\mathfrak{p}}$ by evaluating $\#A_{\mathfrak{p}}(\mathbb{F}_{p^n})$ for sufficiently large $n \in \mathbb{N}$. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. We show the following bound for k_n:

Theorem 1.1. *Let A/K be an abelian variety of dimension d. Denote by r the maximal possible number of $\mathcal{R}$-independent points of $A(K)$. Then:*

$$k_n \geq \left(2rd - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \cdot \min\left\{[K_{\mathfrak{p}} : \mathbb{Q}_p] \cdot d, r\right\}\right) \cdot n - C,$$

where the constant C depends on K, A and p.

The constant C in Theorem 1.1 may be computed explicitly in terms of d, r, some local invariants of A and the order of the cokernel of the Kummer map, see (3.4) for the precise value of C.

Note that always:

$$d \leq h_{\mathfrak{p}} \leq 2d,$$

thus the best bound in Theorem 1.1 is obtained when all primes lying above p have good ordinary reduction (in this case $h_{\mathfrak{p}} = d$). Recall that an unproven conjecture of Serre asserts that for any abelian variety A over a number field K there exist infinitely many primes $\mathfrak{p}$ such that A has good ordinary reduction at $\mathfrak{p}$. This is known to be true for elliptic curves (cf. [23]) and for abelian surfaces (cf. [18]). These observations lead to the following corollary:

Corollary 1.2. *Let $A/\mathbb{Q}$ be an abelian variety of dimension d. If either of the following condition holds:*

- *$r \geq 1$ and A has good reduction at p with positive p-rank, i.e. $A_p(\overline{\mathbb{F}}_p)[p] \neq 0$,*
- *$r > d$,*

then: $\lim_{n\to\infty} \#\operatorname{Cl}(K_n) = \infty$.

Proof. By Theorem 1.1:

$$k_n \geq (2rd - h_p \min\{d, r\}) \cdot n.$$

If any of the above conditions holds then the right-hand side tends to infinity. □

The basic idea of our proof of Theorem 1.1 is to find a large unramified abelian extension of K_n inside the Kummer extension L_n (cf. Section 2 for

the relevant definitions). The Bashmakov–Ribet theory of Kummer extensions provides us a monomorphism with bounded cokernel:

$$\Gamma^{(\infty)} : \mathrm{Gal}(L_\infty/K_\infty) \to T_p(A)^{\oplus r},$$

where $K_\infty = \bigcup_n K_n$, $L_\infty = \bigcup_n L_n$. This allows to estimate the degree $[L_n : K_n]$. The rest of the proof of Theorem 1.1 focuses on estimating inertia groups in Kummer extensions. The basic tools to this end are the classification theorem for compact p-adic Lie groups and the theory of Néron models. In order to illustrate our estimates of class numbers we offer a numerical example.

Example 1.3. *Consider the genus two curve over $\mathbb{Q}$ with label 25913.a.25913 in* [29]. *Its affine part is given by the equation:*

$$X : y^2 + (x^3 + x + 1)y = x^3 - x^2 - 2x.$$

Let $A = \mathrm{Jac}(X)$ be the Jacobian of X. Its endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ equals $\mathbb{Z}$. By using Magma we compute that $A(\mathbb{Q}) \cong \mathbb{Z}^3$. By Theorem 1.1 for each prime we have the following estimate (since $h_p \leq 4$):

$$k_n \geq 2 \cdot (2 \cdot 3 - 4) \cdot n - C = 4n - C,$$

where $C = C(p)$ is an explicit constant, which we compute in Example 3.4.

In many cases it is possible to compute the constant C from Theorem 1.1. To this end we need the following strengthening of Kummer theory:

Theorem 1.4. *Suppose that the image of the p-adic representation*

$$\rho_p : G_K \to \mathrm{GSp}_{2d}(\mathbb{Z}_p)$$

associated to the abelian variety A contains $\mathrm{Sp}_{2d}(\mathbb{Z}_p)$. Then the map $\Gamma^{(\infty)}$ is an isomorphism.

Note that $\rho_p(G_K)$ contains $\mathrm{Sp}_{2d}(\mathbb{Z}_p)$ for almost all p, if one of the following conditions is satisfied:

- d equals 2, 6 or is odd and A is a principally polarized abelian variety of dimension d with $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ (cf. [25, Theorem 3]),
- $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$ and K has a discrete valuation at which A has semistable reduction of toric dimension one (this follows from [11] or [19, Main Theorem] and [14, Theorem 1.1]).

In particular, for the abelian varieties of the type mentioned above, $\Gamma^{(\infty)}$ is an isomorphism for almost all primes p. We expect that a similar result should be true for an arbitrary abelian variety, but despite our attempts, we were unable to find it in the literature or to prove it.

Previous estimates on class numbers of division fields were given in two cases: for abelian varieties with complex multiplication and for elliptic

curves. Suppose that A/K is an abelian variety with complex multiplication and that the prime p splits completely in the CM-field $\mathrm{End}_K^0(A)$. Let $\mathfrak{p}$ be a prime ideal above p. Then the tower of division fields $K_n := K(\mathbb{Q}(A[\mathfrak{p}^n]))$ forms a $\mathbb{Z}_p$-extension of K. Therefore by Iwasawa theory, $\#\,\mathrm{Cl}(K_n) \geq p^{\mu p^n + \lambda n + O(1)}$ for some $\mu, \lambda \in \mathbb{N}$. Estimates on λ, depending on the dimension and the Mordell–Weil rank of A, were given in [9] and in [7]. Lower bounds on class numbers of division fields in the case of an elliptic curve E over $\mathbb{Q}$ were recently given in papers [21], [22] and [13]. The best obtained in loc. cit. bound was of the form:

$$\#\,\mathrm{Cl}(\mathbb{Q}(E[p^n])) \geq p^{2n(r-1)-O(1)}$$

(where r is the Mordell–Weil rank of $E/\mathbb{Q}$) under some additional assumptions on p, including surjectivity of the Galois representation mod p associated to E and vanishing of p-torsion in $\mathbb{Q}_p$ (cf. [13, Theorem 1.1]).

Outline of the paper. In Section 2 we give a brief overview of the Kummer theory of abelian varieties and prove the Theorem 1.4. We prove Theorem 1.1 in Section 3, assuming some bounds on inertia groups. These bounds are proven separately for primes lying above $\ell \neq p$ (in Section 4) and above p (in Section 5).

Acknowledgment. The author wishes to thank Wojciech Gajda for suggesting this problem and for helpful conversations. The author also thanks Bartosz Naskręcki and Bernadeta Tomasz for valuable comments and technical help. Finally, the author would like to express his gratitude to the anonymous referee for his thorough review.

2. Kummer theory for abelian varieties

For any point $P \in A(\overline{K})$ and $N \in \mathbb{N}$, we will denote by $\frac{1}{N}P$ an arbitrary point T, such that $NT = P$. Note that there are N^2 such points. Fix some $\mathcal{R}$-independent points $P_1, \ldots, P_r \in A(K)$. We define:

$$L_n := K_n\left(\frac{1}{p^n}P_1, \ldots, \frac{1}{p^n}P_r\right).$$

Note that the field L_n doesn't depend on the choice of the points

$$\frac{1}{p^n}P_1, \ldots, \frac{1}{p^n}P_r.$$

The extension L_n/K_n is abelian, which can be seen by considering the monomorphism $\Gamma^{(n)} : \mathrm{Gal}(L_n/K_n) \to A[p^n]^{\oplus r}$, $\Gamma^{(n)}(\sigma) = \bigoplus_{i=1}^r \kappa_n(P_i, \sigma)$, where:

$$\kappa_n : A(\overline{K}) \times \mathrm{Gal}(L_n/K_n) \to A[p^n], \quad \kappa_n(P, \sigma) = \left(\frac{1}{p^n}P\right)^\sigma - \left(\frac{1}{p^n}P\right)$$

is the Kummer pairing. It turns out that for n large enough, $\Gamma^{(n)}$ is "almost an isomorphism". More precisely, consider the fields:

$$K_\infty = \bigcup_n K_n, \quad L_\infty = \bigcup_n L_n.$$

By taking an inverse limit of homomorphisms $\Gamma^{(n)} : \mathrm{Gal}(L_n/K_n) \to A[p^n]^{\oplus r}$ we obtain a monomorphism:

$$\Gamma^{(\infty)} : \mathrm{Gal}(L_\infty/K_\infty) \to T_p(A)^{\oplus r},$$

where $T_p(A) := \varprojlim A[p^n]$ is the p-adic Tate module for A. Note that $\Gamma^{(\infty)}$ is continuous, if we endow $\mathrm{Gal}(L_\infty/K_\infty)$ and $T_p(A)^{\oplus r}$ with the usual profinite topologies. The following theorem is based on results of Bashmakov [2] and Ribet [20].

Theorem 2.1 ([1, Lemma 2.13])**.** $\Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty))$ *is an open subgroup of finite index in* $T_p(A)^{\oplus r}$.

Define the integer m_p by the equality:

$$p^{m_p} := [T_p(A)^{\oplus r} : \Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty))]$$

(observe that this index must be a power of p, since $T_p(A)^{\oplus r}$ is a pro-p group).

Corollary 2.2.

$$p^{2drn-m_p} \leq [L_n : K_n] \leq p^{2drn}.$$

Proof. Note that $[L_n : K_n] \leq p^{2drn}$, since $\Gamma^{(n)}$ is injective. Let us denote $K'_n := L_n \cap K_\infty$. Note that $K_n \subset K'_n$ and thus

$$\mathrm{Gal}(L_n/K'_n) \subset \mathrm{Gal}(L_n/K_n).$$

The commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xhookrightarrow{\quad\Gamma^{(\infty)}\quad} & T_p(A)^{\oplus r} \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_n/K'_n) & \xhookrightarrow{\quad\Gamma^{(n)}|_{\mathrm{Gal}(L_n/K'_n)}\quad} & A[p^n]^{\oplus r} \end{array}$$

implies that

$$T_p(A)^{\oplus r}/\Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty)) \twoheadrightarrow A[p^n]^{\oplus r}/\Gamma^{(n)}(\mathrm{Gal}(L_n/K_n)).$$

It follows that:

$$[L_n : K_n] \geq [L_n : K'_n] \geq \#A[p^n]^{\oplus r}/p^{m_p} = p^{2drn-m_p}. \qquad \square$$

The above results are however insufficient to obtain any effective bound on m_p. Recall that Theorem 1.4 gives a criterion for m_p to vanish. Its proof will occupy the remainder of this section. First, we need few preliminary lemmas concerning the symplectic groups. Recall that for any commutative unital ring R:

$$\mathrm{GSp}_{2d}(R) := \{M \in M_{2d}(R) : M\Omega M^T = \lambda(M) \cdot \Omega \quad \text{for some } \lambda(M) \in R^\times\},$$

where $\Omega = \left(\begin{smallmatrix} 0 & I_d \\ -I_d & 0 \end{smallmatrix}\right)$. Note that $\lambda(M)$ may be considered as a surjective homomorphism $\mathrm{GSp}_{2d}(R) \to R^\times$. Its kernel is denoted by $\mathrm{Sp}_{2d}(R)$. For any local ring R with the maximal ideal $\mathfrak{m}$ we introduce the following notation:

$$\begin{aligned}\mathrm{GSp}_{2d}(R)_n &:= \{M \in \mathrm{GSp}_{2d}(R) : M \equiv I_{2d} \pmod{\mathfrak{m}^n}\} \\ &= \ker\left(\mathrm{GSp}_{2d}(R) \to \mathrm{GSp}_{2d}(R/\mathfrak{m}^n)\right).\end{aligned}$$

We define $\mathrm{Sp}_{2d}(R)_n$ in a similar manner.

Lemma 2.3. *If R is a local ring then for any positive integers m, n:*

$$[\mathrm{GSp}_{2d}(R)_n, \mathrm{GSp}_{2d}(R)_m] = [\mathrm{Sp}_{2d}(R)_n, \mathrm{Sp}_{2d}(R)_m] = \mathrm{Sp}_{2d}(R)_{n+m}.$$

Proof. The first equality is immediate. The second equality follows from [27, Theorem, p. 843] by taking $\mathfrak{b}_r := \mathfrak{m}^r$, $f(i,j,k) = k$ and by noting that a maximal ideal in a local ring must be quasi-regular. □

Lemma 2.4. *The representation of $\mathrm{Sp}_{2d}(\mathbb{F}_p)$ on the $\mathbb{F}_p$-vector space:*

$$\mathfrak{sp}_{2d}(\mathbb{F}_p) = \{M \in M_{2d}(\mathbb{F}_p) : M\Omega + \Omega M^T = 0\}$$

(given by conjugation) is irreducible.

Proof. Let $S(2)$ be the space of symmetric matrices in $M_{2d}(\mathbb{F}_p)$ with an action of $\mathrm{Sp}_{2d}(\mathbb{F}_p)$ given by:

$$(A, M) \mapsto AMA^T$$

(one may also identify $S(2)$ with the space of quadratic forms over $\mathbb{F}_p$ in $2d$ variables). The maps:

$$\begin{aligned}\eta &: S(2) \to \mathfrak{sp}_{2d}(\mathbb{F}_p), \quad M \mapsto M\Omega \\ \delta &: \mathfrak{sp}_{2d}(\mathbb{F}_p) \to S(2), \quad N \mapsto -N\Omega\end{aligned}$$

provide isomorphisms of $\mathbb{F}_p[\mathrm{Sp}_{2d}(\mathbb{F}_p)]$-modules. It suffices now to note that $S(2)$ is a simple $\mathbb{F}_p[\mathrm{Sp}_{2d}(\mathbb{F}_p)]$-module by [28, Proposition 2.2]. □

The following proposition is a generalization of [21, Lemma 2.2] to the case of abelian varieties.

Proposition 2.5. *If the image of $\rho_p : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GSp}_{2d}(\mathbb{Z}_p)$ contains $\mathrm{Sp}_{2d}(\mathbb{Z}_p)$ then $L_1 \cap K_\infty = K_1$.*

Proof. Let $N := L_1 \cap K_\infty$. Let $K_1^{(p)}$ be the maximal abelian extension of exponent p of K_1 inside of K_∞. Then obviously $N \subset K_1^{(p)}$. Moreover, both $\mathrm{Gal}(K_1^{(p)}/K_1)$ and $\mathrm{Gal}(N/K_1)$ are $\mathbb{F}_p[\mathrm{Gal}(K_1/K)]$-modules. We'll compare their structure as $\mathbb{F}_p[\mathrm{Sp}_{2d}(\mathbb{F}_p)]$-modules. Note that by assumption

$$\mathrm{Sp}_{2d}(\mathbb{Z}_p)_1 \subset \mathrm{Gal}(K_\infty/K_1) \subset \mathrm{GSp}_{2d}(\mathbb{Z}_p)_1.$$

By Lemma 2.3 we see that

$$\begin{aligned}[\mathrm{Gal}(K_\infty/K_1), \mathrm{Gal}(K_\infty/K_1)] &= [\mathrm{Sp}_{2d}(\mathbb{Z}_p)_1, \mathrm{Sp}_{2d}(\mathbb{Z}_p)_1] \\ &= [\mathrm{GSp}_{2d}(\mathbb{Z}_p)_1, \mathrm{GSp}_{2d}(\mathbb{Z}_p)_1] \\ &= \mathrm{Sp}_{2d}(\mathbb{Z}_p)_2.\end{aligned}$$

Therefore we have:

$$\mathrm{Sp}_{2d}(\mathbb{Z}_p)_1^{ab} \leq \mathrm{Gal}(K_\infty/K_1)^{ab} \leq \mathrm{GSp}_{2d}(\mathbb{Z}_p)_1^{ab}$$

and

$$\begin{aligned}\mathrm{GSp}_{2d}(\mathbb{Z}_p)_1^{ab} &\cong \mathrm{GSp}_{2d}(\mathbb{Z}_p)_1 / \mathrm{Sp}_{2d}(\mathbb{Z}_p)_2 \\ &\cong \mathrm{Sp}_{2d}(\mathbb{Z}/p^2)_1 \times (1 + p\mathbb{Z}_p) \\ &\cong \mathfrak{sp}_{2d}(\mathbb{F}_p) \times \mathbb{Z}_p,\end{aligned}$$

where:

- the isomorphism $\mathrm{GSp}_{2d}(\mathbb{Z}_p)_1 / \mathrm{Sp}_{2d}(\mathbb{Z}_p)_2 \cong \mathrm{Sp}_{2d}(\mathbb{Z}/p^2)_1 \times (1 + p\mathbb{Z}_p)$ is given by $A \mapsto (\lambda(A)^{-1} \cdot A, \lambda(A))$,
- the isomorphism $\mathrm{Sp}_{2d}(\mathbb{Z}/p^2)_1 \cong \mathfrak{sp}_{2d}(\mathbb{F}_p)$ is given by $I + pM \mapsto M$.

Analogously, we have: $\mathrm{Sp}_{2d}(\mathbb{Z}_p)_1^{ab} \cong \mathfrak{sp}_{2d}(\mathbb{F}_p)$. This implies easily that

$$\mathrm{Gal}(K_1^{(p)}/K_1) \cong \mathfrak{sp}_{2d}(\mathbb{F}_p) \times (\mathbb{Z}/p)^i \qquad \text{for } i \in \{0, 1\}$$

as $\mathbb{F}_p[\mathrm{Sp}_{2d}(\mathbb{F}_p)]$-modules (with trivial action on $\mathbb{Z}/p$ and action on $\mathfrak{sp}_{2d}(\mathbb{F}_p)$ given by conjugation). The assumption implies that $A[p]$ is an irreducible $\mathrm{Sp}_{2d}(\mathbb{F}_p)$-module. Thus $\mathrm{Gal}(L_1/K_1) \cong A[p]^{\oplus r'}$ for some $r' \leq r$. Moreover, since

$$\mathrm{Gal}(L_1/K_1) \cong A[p]^{\oplus r'} \twoheadrightarrow \mathrm{Gal}(N/K_1)$$

we obtain $\mathrm{Gal}(N/K) \cong A[p]^{\oplus s}$ for some $s \leq r'$. On the other hand:

$$\mathrm{Gal}(K_1^{(p)}/K_1) \cong \mathfrak{sp}_{2d}(\mathbb{F}_p) \times (\mathbb{Z}/p)^i \twoheadrightarrow \mathrm{Gal}(N/K_1),$$

and since $\mathfrak{sp}_{2d}(\mathbb{F}_p)$ and $\mathbb{Z}/p$ are simple $\mathbb{F}_p[\mathrm{Sp}_{2d}(\mathbb{F}_p)]$-modules, which are non-isomorphic to $A[p]$, we obtain $s = 0$ and $N = K_1$. □

Proof of Theorem 1.4. It suffices to check that $\Gamma^{(\infty)}$ is surjective. One easily checks that $\mathrm{Sp}_{2d}(\mathbb{Z}_p) \subset \rho_p(G_K)$ implies that the axioms B_1, B_2 and B_3

from [20] are satisfied. Thus $\Gamma^{(1)}$ is an isomorphism. By Proposition 2.5 we obtain $L_1 \cap K_\infty = K_1$. Consider the commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xhookrightarrow{\quad\Gamma^{(\infty)}\quad} & T_p(A)^{\oplus r} \\ \big\downarrow & & \big\downarrow \\ \mathrm{Gal}(L_1/L_1\cap K_\infty) = \mathrm{Gal}(L_1/K_1) & \xrightarrow[\cong]{\quad\Gamma^{(1)}\quad} & A[p]^{\oplus r} \end{array}$$

Note that the $\mathbb{Z}_p$-modules

$$M := \Gamma^{(\infty)}(\mathrm{Gal}(L_\infty/K_\infty)) \quad \text{and} \quad N := T_p(A)^{\oplus r}$$

satisfy $M \subset N$ and

$$M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p\mathbb{Z}_p = \Gamma^{(1)}(\mathrm{Gal}(L_1/K_1)) \cong A[p]^{\oplus r} = N \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p\mathbb{Z}_p.$$

Therefore $M = N$ by Nakayama's lemma, which ends the proof. □

3. Proof of Theorem 1.1

The main idea behind the proof of Theorem 1.1 is to control the ramification in L_n/K_n. A standard argument used in the proof of the weak Mordell–Weil theorem shows that the only possible ramified primes of L_n/K_n, are primes lying over primes of bad reduction for A or primes over p. We need to bound the inertia group for those primes. Let $I(\mathcal{P})$ denote the inertia group of the extension L_n/K_n at a prime $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_{L_n})$. For an arbitrary prime $\mathfrak{p}$ of K we define the following subgroup of $\mathrm{Gal}(L_n/K_n)$, generated by inertia subgroups over $\mathfrak{p}$:

$$I_{\mathfrak{p}}^{(n)} := \left\langle \bigcup_{\mathcal{P}} I(\mathcal{P}) \right\rangle,$$

where the union is over all primes $\mathcal{P}$ of L_n above $\mathfrak{p}$. We define also:

$$I^{(n)} := \left\langle \bigcup_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)} I_{\mathfrak{p}}^{(n)} \right\rangle.$$

We will estimate the order of interia groups $I_{\mathfrak{p}}$ separately for $\mathfrak{p} \nmid p$ and for $\mathfrak{p}|p$. In order to do this, we will work in the local setting. Let us fix $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ and introduce the following notation:

- ℓ, the unique rational prime such that $\mathfrak{p}|\ell$,
- $K_{\mathfrak{p}}$, completion of K at $\mathfrak{p}$ with ring of integers $\mathcal{O}_{K_{\mathfrak{p}}}$,
- $\mathcal{A}_{\mathfrak{p}}$, the Néron model of A over $K_{\mathfrak{p}}$ with special fiber $A_{\mathfrak{p}}$ and the connected component of the identity $A_{\mathfrak{p}}^0$,

- we denote the group scheme of geometric components of $\mathcal{A}$ over $\mathfrak{p}$ by:
$$\Phi_{\mathfrak{p}} := A_{\mathfrak{p}}/A^0_{\mathfrak{p}},$$
- $p^{\alpha_{\mathfrak{p}}}$, the exponent of the group $\Phi_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}})[p^\infty]$,
- $p^{\beta_{\mathfrak{p}}}$, the exponent of the group $A(K_{\mathfrak{p}})[p^\infty]$.

Note that the group $\Phi_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}})$ is finite (its order is called the Tamagawa number of A at $\mathfrak{p}$) and thus $\alpha_{\mathfrak{p}}$ is well-defined. Moreover, $\alpha_{\mathfrak{p}} = 0$ whenever A has good reduction at $\mathfrak{p}$. Also, $\beta_{\mathfrak{p}}$ is finite, since $A(K_{\mathfrak{p}})$ contains a subgroup of finite index isomorphic to $\mathcal{O}^d_{K_{\mathfrak{p}}}$, cf. [16]. However, it is unknown whether $\beta_{\mathfrak{p}} = 0$ holds for almost all p, even in the case of elliptic curves over $\mathbb{Q}$, cf. [5] and [8].

With this notation we have the following proposition:

Proposition 3.1. *If $\mathfrak{p} \nmid p$, then:*
$$\#I^{(n)}_{\mathfrak{p}} \leq p^{2dr\min\{\alpha_{\mathfrak{p}},\beta_{\mathfrak{p}}\}}.$$

Note that in particular this bound is independent of n and that it equals 1 for primes $\mathfrak{p}$ of good reduction for $\mathcal{A}$. Proposition 3.1 will be proven in Section 4. In Section 5 we will estimate the order of $I^{(n)}_{\mathfrak{p}}$ for $\mathfrak{p}|p$ and will prove the following result.

Proposition 3.2. *If $\mathfrak{p}|p$, then:*
$$\#I^{(n)}_{\mathfrak{p}} \leq p^{h_{\mathfrak{p}}\cdot\min\{d\cdot[K_{\mathfrak{p}}:\mathbb{Q}_p],r\}\cdot n + rh_{\mathfrak{p}}\beta_{\mathfrak{p}}}.$$

Before the proof of Theorem 1.1 we need one more lemma:

Lemma 3.3. *K_n has no real embeddings for $(p,n) \neq (2,1)$.*

Proof. Suppose to the contrary that $\sigma : K_n \hookrightarrow \mathbb{R}$ is a real place of K_n. Then may view A as an abelian variety over the field $\mathbb{R}$, satisfying $A(\mathbb{R})[p^n] = (\mathbb{Z}/p^n)^{2d}$. On the other hand, we have:
$$A(\mathbb{R}) \cong (\mathbb{S}^1)^d \times (\mathbb{Z}/2)^t$$
for some integer $0 \leq t \leq d$ (cf. [10, Proposition 1.1 (c)]). Thus:
$$A(\mathbb{R})[p^n] \cong (\mathbb{Z}/p^n)^d \times (\mathbb{Z}/2)^t[p^n],$$
which leads to a contradiction for $(p,n) \neq (2,1)$. □

Proof of Theorem 1.1. Let $\widetilde{L_n}$ be the maximal unramified extension of K_n inside L_n. Then it must be a subfield of the Hilbert class field of K_n. The degree of the Hilbert class field of K_n is $\#\operatorname{Cl}(K_n)$ and thus:
$$[\widetilde{L_n} : K_n] \text{ divides } \#\operatorname{Cl}(K_n). \tag{3.1}$$

Note that by Propositions 3.1 and 3.2:

$$\begin{aligned}\#I^{(n)} &\le \prod_{\mathfrak{p}} \#I_{\mathfrak{p}}^{(n)} = \prod_{\mathfrak{p}|p} \#I_{\mathfrak{p}}^{(n)} \cdot \prod_{\mathfrak{p}\nmid p} \#I_{\mathfrak{p}}^{(n)} \\ &\le p^{\sum_{\mathfrak{p}|p}(h_{\mathfrak{p}} \min\{d\cdot[K_{\mathfrak{p}}:\mathbb{Q}_p],r\}\cdot n + r h_{\mathfrak{p}}\beta_{\mathfrak{p}}) + 2dr\cdot\sum_{\mathfrak{p}\nmid p}\min\{\alpha_{\mathfrak{p}},\beta_{\mathfrak{p}}\}}. \qquad (3.2)\end{aligned}$$

By Lemma 3.3 K_n has no real places and thus any extension of K_n is unramified at infinite places. Therefore $\widetilde{L_n} = (L_n)^{I^{(n)}}$, which yields (using Corollary 2.2):

$$\begin{aligned}[\widetilde{L_n} : K_n] = [L_n : K_n]/\#I^{(n)} &\ge p^{2dnr - m_p}/\#I^{(n)} \\ &\overset{(3.2)}{\ge} p^{\left(2dr - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}} \min\{d\cdot[K_{\mathfrak{p}}:\mathbb{Q}_p],r\}\right)\cdot n - C}, \qquad (3.3)\end{aligned}$$

where for $(p,n) \neq (2,1)$ one can take:

$$C := 2dr \sum_{\mathfrak{p}\nmid p} \min\{\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}\} + r \sum_{\mathfrak{p}|p} h_{\mathfrak{p}}\beta_{\mathfrak{p}} + m_p. \qquad (3.4)$$

The proof follows by combining (3.1), (3.3) and noting that $[\widetilde{L}_n : K_n]$ must be a power of p, since $[L_n : K_n]$ is a power of p. □

Example 3.4. *Consider the abelian variety $A = \mathrm{Jac}(X)$ from Example 1.3. We compute now the constant C for almost all primes p. Recall that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \cong \mathbb{Z}$. The conductor of A is* 25913*, which is a prime number. Let p be a prime outside of the set $S := \{2, 3, 5, 7, 25913\}$.*

- *Using algorithm described in* [6]*, we check that the Galois representation $\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Z}_\ell)$ is surjective for primes outside S (note that the primality of the conductor simplifies the calculations, cf.* [6, Remark 5.14]*). Thus by Theorem 1.4 we have $m_p = 0$.*
- *Using Magma we check that for every prime p the Tamagawa number of A at p is trivial and thus $\alpha_p = 0$.*
- *By* [24, IV.II.9, Theorem 4] *the formal group $\widehat{\mathcal{A}_p}(p\mathbb{Z}_p)$ (which may be identified with the kernel of $\mathrm{red}_p : A(\mathbb{Q}_p) \to A_p(\mathbb{F}_p)$) is torsion-free and thus p^{β_p} divides the exponent of $A_p(\mathbb{F}_p)$. Therefore by Weil's estimate we obtain $\beta_p \le 2$.*

Finally, using (3.4) *it follows that we may take $C = 24$ in this case, i.e.*

$$k_n \ge 4n - 24.$$

4. Inertia groups over $\ell \neq p$

In this section we estimate the order of the inertia group $I_{\mathfrak{p}}^{(n)}$ for a prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, $\mathfrak{p} \nmid p$. We use the notation introduced in Section 2.

Proposition 4.1. *If $p \nmid \mathfrak{p}$, then*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{2dr\beta_{\mathfrak{p}}}.$$

Proof. Let us fix a point $P \in A(K_{\mathfrak{p}})$. Recall that ℓ is the rational prime below $\mathfrak{p}$. By the classification theorem of compact ℓ-adic Lie groups (cf. [4, Theorem 21]):

$$A(K_{\mathfrak{p}}) \cong \mathcal{O}_{K_{\mathfrak{p}}}^{d} \times A(K_{\mathfrak{p}})_{tors} \cong \mathbb{Z}_{\ell}^{d\cdot[K_{\mathfrak{p}}:\mathbb{Q}_{\ell}]} \times A(K_{\mathfrak{p}})_{tors}$$

as topological groups. Note that multiplication by p is an isomorphism on $\mathbb{Z}_{\ell}$. Therefore and by definition of $\beta_{\mathfrak{p}}$:

$$p^{\beta_{\mathfrak{p}}} A(K_{\mathfrak{p}}) \cong \mathbb{Z}_{\ell}^{d\cdot[K_{\mathfrak{p}}:\mathbb{Q}_{\ell}]} \times T,$$

where T is a finite group satisfying $p \nmid \#T$. This implies that multiplication by p on $p^{\beta_{\mathfrak{p}}} A(K_{\mathfrak{p}})$ is an isomorphism and

$$p^{\beta_{\mathfrak{p}}} P = p^{n} R$$

for some $R \in A(K_{\mathfrak{p}})$. Thus for the Kummer map κ_n:

$$\begin{aligned} p^{\beta_{\mathfrak{p}}} \kappa_n(P,\sigma) &= \kappa_n(p^{\beta_{\mathfrak{p}}} P, \sigma) = \kappa_n(p^n R, \sigma) \\ &= R^{\sigma} - R = 0 \end{aligned}$$

for any $\sigma \in I_{\mathfrak{p}}$. In particular, taking $P = P_i$ for $i = 1, \ldots, r$ we obtain:

$$\Gamma^{(n)}(I_{\mathfrak{p}}^{(n)}) \subset A[p^{\beta_{\mathfrak{p}}}]^{\oplus r}.$$

This ends the proof. □

We now move on to prove the second estimate on the order of $I_{\mathfrak{p}}^{(n)}$. We start with the following lemma that will be used later.

Lemma 4.2. *Let G be a connected commutative algebraic group over an algebraically closed field k. Then for any m relatively prime to* $\operatorname{char} k$ *the morphism*

$$[m] : G(k) \to G(k)$$

of multiplication by m is surjective.

Proof. The proof follows by noting that the image of $[m]$ is a closed subgroup of G (cf. [15, Proposition 1.5]) and its dimension is $\dim G$ (since multiplication by m on the Lie algebra of G is invertible). □

Let $K_{\mathfrak{p}}^{ur}$ be the maximal unramified extension of $K_{\mathfrak{p}}$ inside $\overline{\mathbb{Q}}_{\ell}$. We denote its ring of integers by $\mathcal{O}^{ur}$ and the maximal ideal of $\mathcal{O}^{ur}$ by $\mathfrak{m}^{ur}$. Note that formation of the Néron model commutes with étale base change (cf. [3, Proposition 1.2.2]) and thus we can consider $\mathcal{A}_{\mathfrak{p}}$ as the Néron model over $K_{\mathfrak{p}}^{ur}$. Therefore the reduction morphism extends to $K_{\mathfrak{p}}^{ur}$:

$$\operatorname{red}_{\mathfrak{p}} : A(K_{\mathfrak{p}}^{ur}) \cong \mathcal{A}_{\mathfrak{p}}(\mathcal{O}^{ur}) \to A_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}}).$$

The kernel of the reduction is isomorphic to $\widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur})$, which is by definition the $K_{\mathfrak{p}}^{ur}$-analytic Lie group obtained by using the formal group law $\widehat{\mathcal{A}_p}$ as a group operation on $(\mathfrak{m}^{ur})^d$. Recall that $[p] : \widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur}) \to \widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur})$ is an isomorphism, since p is invertible in $\mathcal{O}^{ur}$ (cf. [24, Chapter IV, §9, Theorem 3]).

Proposition 4.3. *If $\mathfrak{p} \nmid p$ then*

$$\#I_{\mathfrak{p}}^{(n)} \leq p^{2dr\alpha_{\mathfrak{p}}}.$$

Proof. Consider $\mathcal{A}_{\mathfrak{p}}$ as the Néron model for A over $\mathcal{O}^{ur}$. Let $\alpha := \alpha_{\mathfrak{p}}$ and

$$c := \#\Phi_{\mathfrak{p}}(\overline{\mathbb{F}}_{\mathfrak{p}}).$$

Fix $P \in A_{\mathfrak{p}}(K_{\mathfrak{p}})$. We have $c \cdot \mathrm{red}_{\mathfrak{p}}(P) \in A_{\mathfrak{p}}^0(\overline{\mathbb{F}}_{\mathfrak{p}})$. But $A_{\mathfrak{p}}^0$ is a connected commutative group scheme over an algebraically closed field $\overline{k}$ of characteristic $\ell \neq p$ and thus by Lemma 4.2:

$$c \cdot \mathrm{red}_{\mathfrak{p}}(P) = p^n R'$$

for some $R' \in A_{\mathfrak{p}}^0(\overline{\mathbb{F}}_{\mathfrak{p}})$. But $K_{\mathfrak{p}}^{ur}$ is henselian and thus by Hensel's lemma (cf. [3, 2.3, Proposition 5]) $R' = \mathrm{red}_{\mathfrak{p}}(R)$ for some $R \in \mathcal{A}_{\mathfrak{p}}(R')$, i.e.

$$cP - p^n R \in \widehat{\mathcal{A}_{\mathfrak{p}}}(\mathcal{O}^{ur}).$$

The multiplication by p is an automorphism of the formal group $\widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur})$ and thus $\widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur})$ is p-divisible. Therefore (modifying R by some element of $\widehat{\mathcal{A}_{\mathfrak{p}}}(\mathfrak{m}^{ur})$ if necessary) we can assume without loss of generality that $cP = p^n R$. Note that $c = p^\alpha \cdot c'$, where $p \nmid c'$. Thus we can modify R by a multiple of P to obtain:

$$p^\alpha P = p^n R,$$

where $R \in A(K_{\mathfrak{p}}^{ur})$. This implies for the Kummer map κ_n:

$$\begin{aligned} p^\alpha \kappa_n(P, \sigma) &= \kappa_n(p^\alpha P, \sigma) = \kappa_n(p^n R, \sigma) \\ &= R^\sigma - R = 0 \end{aligned}$$

for any $\sigma \in I_{\mathfrak{p}}^{(n)}$. Therefore $\Gamma^{(n)}(I_{\mathfrak{p}}^{(n)}) \subset A[p^\alpha]^{\oplus r}$ and we are done. □

Proof of Proposition 3.1. It follows by combining together Propositions 4.1 and 4.3. □

Remark 4.4. The form of the bound in Proposition 3.1 raises a natural question: are both inequalities $\alpha_{\mathfrak{p}} < \beta_{\mathfrak{p}}$ and $\alpha_{\mathfrak{p}} > \beta_{\mathfrak{p}}$ possible? The answer is *yes*. It turns out that in the case of elliptic curves with split multiplicative reduction both cases are possible:

- Let $\mathrm{ord}_p(x)$ denote the p-adic valuation of x. We choose primes ℓ, p such that $\mathrm{ord}_p(\ell-1) = k \geq 2$. Consider the Tate curve $E_q/\mathbb{Q}_\ell$, where $q = \ell$. Then by [26, Corollary IV.9.2.(d)] $\Phi_\ell(\overline{\mathbb{F}}_\ell)$ is trivial. On the other hand, one easily checks that

$$E_q(\mathbb{Q}_\ell)[p] \cong (\mathbb{Q}_\ell/q^{\mathbb{Z}})[p] = \langle \zeta_{p^k} \rangle \cong \mathbb{Z}/p^k,$$

  thus $\alpha_\ell = 0 < \beta_\ell = k$.
- Let ℓ, p be primes such that $\mathrm{ord}_p(\ell-1) = 1$. Note that not every element of $\mathbb{Q}_\ell^\times$ is a pth power, since
  $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^p \neq 1$.
  Let $a \in \mathbb{Q}_\ell^\times \setminus (\mathbb{Q}_\ell^\times)^p$ and $q := \ell^{p^k} \cdot a$ for some $k \geq 2$. Consider the Tate curve $E_q/\mathbb{Q}_\ell$. Using again [26, Corollary IV.9.2.(d)] we obtain:

$$\Phi_\ell(\overline{\mathbb{F}}_\ell) \cong \mathbb{Z}/(\mathrm{ord}_\ell(q)) \cong \mathbb{Z}/p^k.$$

  On the other hand, one easily checks that

$$E_q(\mathbb{Q}_\ell)[p] \cong (\mathbb{Q}_\ell/q^{\mathbb{Z}})[p] = \langle \zeta_p \rangle \cong \mathbb{Z}/p,$$

  thus $\beta_\ell = 1 < \alpha_\ell = k$.

However, it turns out that it is possible to compare the exponents of $\Phi_\ell(\overline{\mathbb{F}}_\ell)[p^\infty]$ and $A(K_\mathfrak{p}^{ur})[p^\infty]$.

Proposition 4.5. *Let p^{γ_p} be the exponent of $A(K_\mathfrak{p}^{ur})[p^\infty]$. Then*

$$\alpha_p \leq \gamma_p.$$

Proof. Let $\mathbb{F}/\mathbb{F}_\mathfrak{p}$ be a finite extension such that $\Phi_\mathfrak{p}(\mathbb{F}) = \Phi_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p})$ and let $K'_\mathfrak{p}$ be the finite unramified extension of $K_\mathfrak{p}$ with $\mathbb{F}$ as the residue field. By a similar argument as in proof of Proposition 4.1 the group $p^{\gamma_\mathfrak{p}} A(K'_\mathfrak{p})$ is p-divisible. Therefore $p^{\gamma_\mathfrak{p}} \Phi_\mathfrak{p}(\mathbb{F})$ must also be p-divisible and thus (since it is a finite group) it contains no p-torsion. This means that $\alpha_p \leq \gamma_p$. □

5. Inertia groups over p

In this section we estimate the order of $I_\mathfrak{p}^{(n)}$ in the remaining case when $\mathfrak{p}|p$. We use the notation from Sections 2 and 3. Assume for a while that A has good reduction at p. In this case the Néron model of A over $\mathcal{O}_{K_\mathfrak{p}}$ is an abelian scheme. Thus, by applying the valuative criterion of properness (cf. [12, Theorem II.4.7]) to the valuation ring $\mathcal{O}_{\overline{K_\mathfrak{p}}}$ and by using the universal property of the fiber product, we can extend the reduction homorphism to the algebraic closure of $K_\mathfrak{p}$:

$$\mathrm{red}_\mathfrak{p} : A(\overline{K_\mathfrak{p}}) \cong \mathcal{A}_\mathfrak{p}(\mathcal{O}_{\overline{K_\mathfrak{p}}}) \to \mathcal{A}_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p}) \cong A_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p}).$$

Let:

$$H_n := \begin{cases} \ker\left(A(\overline{K_\mathfrak{p}})[p^n] \to A_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p})\right), & \text{if } A \text{ has good reduction at } \mathfrak{p}, \\ A[p^n], & \text{otherwise.} \end{cases}$$

Note that $h_\mathfrak{p}$ defined in (1.1) satisfies

$$|H_n| = p^{nh_\mathfrak{p}},$$

since by definition $|H_1| = p^{h_\mathfrak{p}}$ and by [17, Chapter III.15, p. 146–147] for any prime $\mathfrak{p}$ of good reduction we have:

$$|A_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p})[p^n]| = |A_\mathfrak{p}(\overline{\mathbb{F}}_\mathfrak{p})[p]|^n.$$

Proof of Proposition 3.2. Observe that $\Gamma^{(n)}(I_\mathfrak{p}^{(n)}) \subset H_n^{\oplus r}$. If A has bad reduction at $\mathfrak{p}$, then this obviously holds true. If A has good reduction at $\mathfrak{p}$, then for all $\sigma \in I_\mathfrak{p}^{(n)}$:

$$\mathrm{red}_\mathfrak{p}(\kappa_n(P_i, \sigma)) = \mathrm{red}_\mathfrak{p}(P_i)^\sigma - \mathrm{red}_\mathfrak{p}(P_i) = 0.$$

This yields the bound:

$$\#I_\mathfrak{p}^{(n)} \leq \#H_n^{\oplus r} = p^{h_\mathfrak{p} rn}.$$

We put $b := d \cdot [K_\mathfrak{p} : \mathbb{Q}_p]$. Using the classification theorem of compact p-adic Lie groups (cf. [4, Thm. 21]) we obtain:

$$A(K_\mathfrak{p}) \cong \mathcal{O}_{K_\mathfrak{p}}^d \times A(K_\mathfrak{p})_{tors} \cong \mathbb{Z}_p^b \times A(K_\mathfrak{p})_{tors}.$$

Let G be the group generated by the images of $p^{\beta_\mathfrak{p}} P_1, \ldots, p^{\beta_\mathfrak{p}} P_r$ inside the group

$$p^{\beta_\mathfrak{p}} A(K_\mathfrak{p}) / p^{n+\beta_\mathfrak{p}} A(K_\mathfrak{p}) \cong (\mathbb{Z}/p^n)^b.$$

The group G is generated by images of at most b elements $Q_1, \ldots, Q_b \in A(K_\mathfrak{p})$. Suppose

$$p^{\beta_\mathfrak{p}} P_i \equiv \sum_j a_{ij} Q_j \pmod{p^n A(K_\mathfrak{p})} \qquad \text{for some } a_i \in \mathbb{Z}.$$

Then for $\sigma \in I_\mathfrak{p}^{(n)}$ we have:

$$p^{\beta_\mathfrak{p}} \kappa_n(P_i, \sigma) = \sum_j a_{ij} \kappa_n(Q_j, \sigma). \tag{5.1}$$

Consider the homomorphism

$$\Psi^{(n)} : I_\mathfrak{p}^{(n)} \to H_n^{\oplus b},$$

$$\Psi^{(n)}(\sigma) = \bigoplus_{i=1}^{b} \kappa_n(Q_i, \sigma).$$

Note that the equality (5.1) implies that $\Gamma^{(n)}(\ker \Psi^{(n)}) \subset H_{\beta_\mathfrak{p}}^{\oplus r}$ and thus, since $\Gamma^{(n)}$ is injective, $\#(\ker \Psi^{(n)}) \leq p^{h_\mathfrak{p} r \beta_\mathfrak{p}}$. Finally we obtain:

$$\begin{aligned}\#I_\mathfrak{p}^{(n)} &= \#\Psi^{(n)}(I_\mathfrak{p}^{(n)}) \cdot \#(\ker \Psi^{(n)}) \\ &\leq p^{h_\mathfrak{p} bn} \cdot p^{h_\mathfrak{p} r \beta_\mathfrak{p}} = p^{h_\mathfrak{p} bn + h_\mathfrak{p} r \beta_\mathfrak{p}}.\end{aligned}$$

□

References

[1] G. Banaszak, W. Gajda & P. Krasoń, "Detecting linear dependence by reduction maps", *J. Number Theory* **115** (2005), no. 2, p. 322-342.

[2] M. I. Bashmakov, "The cohomology of abelian varieties over a number field", *Russ. Math. Surv.* **27** (1972), no. 6, p. 25-70.

[3] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 21, Springer, 1990.

[4] P. L. Clark & A. Lacy, "There are genus one curves of every index over every infinite, finitely generated field", *J. Reine Angew. Math.* **794** (2019), p. 65-86.

[5] C. David & T. Weston, "Local torsion on elliptic curves and the deformation theory of Galois representations", *Math. Res. Lett.* **15** (2008), no. 2-3, p. 599-611.

[6] L. V. Dieulefait, "Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$", *Exp. Math.* **11** (2003), no. 4, p. 503-512.

[7] T. Fukuda, K. Komatsu & S. Yamagata, "Iwasawa λ-invariants and Mordell–Weil ranks of abelian varieties with complex multiplication", *Acta Arith.* **127** (2007), no. 4, p. 305-307.

[8] J. Garnek, "On p-degree of elliptic curves", *Int. J. Number Theory* **14** (2018), no. 3, p. 693-704.

[9] R. Greenberg, "Iwasawa theory—past and present", in *Class field theory—its centenary and prospect (Tokyo, 1998)*, Advanced Studies in Pure Mathematics, vol. 30, Mathematical Society of Japan, 2001, p. 335-385.

[10] B. H. Gross & J. Harris, "Real algebraic curves", *Ann. Sci. Éc. Norm. Supér.* **14** (1981), no. 2, p. 157-182.

[11] C. Hall, "An open-image theorem for a general class of abelian varieties", *Bull. Lond. Math. Soc.* **43** (2011), no. 4, p. 703-711.

[12] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer, 1977.

[13] T. Hiranouchi, "Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$", `https://arxiv.org/abs/1703.08275`, 2017.

[14] M. Larsen, "Maximality of Galois actions for compatible systems", *Duke Math. J.* **80** (1995), no. 3, p. 601-630.

[15] G. Malle & D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, vol. 133, Cambridge University Press, 2011.

[16] A. Mattuck, "Abelian varieties over p-adic ground fields", *Ann. Math.* **62** (1955), p. 92-119.

[17] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research, 2008, corrected reprint of the second (1974) edition.

[18] A. Ogus, "Hodge Cycles and Crystalline Cohomology", in *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer, 1981, p. 357-414.

[19] S. Arias-de Reyna, W. Gajda & S. Petersen, "Big monodromy theorem for abelian varieties over finitely generated fields", *J. Pure Appl. Algebra* **217** (2013), no. 2, p. 218-229.

[20] K. A. Ribet, "Kummer theory on extensions of abelian varieties by tori", *Duke Math. J.* **46** (1979), no. 4, p. 745-761.

[21] F. Sairaiji & T. Yamauchi, "On the class numbers of the fields of the p^n-torsion points of certain elliptic curves over $\mathbb{Q}$", *J. Number Theory* **156** (2015), p. 277-289.

[22] ———, "On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$", `https://arxiv.org/abs/1603.01296`, 2016.

[23] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, 1989.

[24] ———, *Lie algebras and Lie groups. 1964 lecture,s given at Harvard University*, Lecture Notes in Mathematics, vol. 1500, Springer, 1992.
[25] ———, *Oeuvres/Collected papers. IV. 1985–1998*, Springer Collected Works in Mathematics, Springer, 2013.
[26] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
[27] Y. V. SOSNOVSKIJ, "Commutator structure of symplectic groups", *Mat. Zametki* **24** (1978), no. 5, p. 641-648.
[28] I. D. SUPRUNENKO & A. E. ZALESSKI, "Reduced symmetric powers of natural realizations of the groups $sl_m(p)$ and $sp_m(p)$ and their restrictions to subgroups", *Sib. Math. J.* **31** (1990), no. 4, p. 33-46.
[29] THE LMFDB COLLABORATION, "The L-functions and modular forms database", 2017, `http://www.lmfdb.org`.

Jędrzej GARNEK
Graduate School, Adam Mickiewicz University
Faculty of Mathematics and Computer Science
Umultowska 87, 61-614 Poznan, Poland
E-mail: `jgarnek@amu.edu.pl`
URL: `http://jgarnek.faculty.wmi.amu.edu.pl/`