THE GROWTH OF THE RANK OF ABELIAN VARIETIES UPON EXTENSIONS

PETER BRUIN AND FILIP NAJMAN

Abstract. We study the growth of the rank of elliptic curves and, more generally, Abelian varieties upon extensions of number fields.

First, we show that if L/K is a finite Galois extension of number fields such that $\mathrm{Gal}(L/K)$ does not have an index 2 subgroup and A/K is an Abelian variety, then $\operatorname{rk} A(L) - \operatorname{rk} A(K)$ can never be 1. We obtain more precise results when $\mathrm{Gal}(L/K)$ is of odd order, alternating, $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{PSL}_2(\mathbb{F}_p)$. This implies a restriction on $\operatorname{rk} E(K(E[p])) - \operatorname{rk} E(K(\zeta_p))$ when E/K is an elliptic curve whose mod p Galois representation is surjective. Similar results are obtained for the growth of the rank in certain non-Galois extensions.

Second, we show that for every $n \geq 2$ there exists an elliptic curve E over a number field K such that $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}} \mathrm{Res}_{K/\mathbb{Q}} E$ contains a number field of degree 2^n. We ask whether every elliptic curve E/K has infinite rank over $K\mathbb{Q}(2)$, where $\mathbb{Q}(2)$ is the compositum of all quadratic extensions of $\mathbb{Q}$. We show that if the answer is yes, then for any $n \geq 2$, there exists an elliptic curve E/K admitting infinitely many quadratic twists whose rank is a positive multiple of 2^n.

1. Introduction

Let A be an Abelian variety over a number field K. By the Mordell–Weil theorem, the Abelian group $A(K)$ of K-rational points of A is finitely generated, so it is of the form $T \oplus \mathbb{Z}^r$, where T is the torsion group and r is the rank of A. In this paper, we study the growth of the rank of Abelian varieties upon extensions of number fields.

In Section 2, we consider an Abelian variety A over a number field K and a finite Galois extension L/K. We show that the structure of the group $G = \mathrm{Gal}(L/K)$ can impose restrictions on the growth of the rank of A under base extension from K to L. Suppose throughout this paragraph that $\operatorname{rk} A(L)$ is strictly greater than $\operatorname{rk} A(K)$. We prove that if G has odd order, then $\operatorname{rk} A(L) - \operatorname{rk} A(K) \geq p - 1$, where p is the smallest prime factor of $\#G$. If G is the alternating group A_n with $n \geq 5$, we obtain $\operatorname{rk} A(L) - \operatorname{rk} A(K) \geq n - 1$. If G is A_3 or A_4, then $\operatorname{rk} A(L) - \operatorname{rk} A(K) \geq 2$. If G is $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{PSL}_2(\mathbb{F}_p)$ for a prime $p > 2$, then $\operatorname{rk} A(L) - \operatorname{rk} A(K) \geq \frac{p-1}{2}$. As a corollary, if E/K is an elliptic curve and $p > 2$ is a prime such that the mod p Galois representation of E is surjective, then $\operatorname{rk} E(K(E[p])) - \operatorname{rk} E(K(\zeta_p))$ is either zero or at least $\frac{p-1}{2}$. We prove that $\operatorname{rk} A(L) - \operatorname{rk} A(K) \geq 2$ whenever G does not have an index 2 subgroup.

Furthermore, for certain non-Galois extensions L/K with Galois closure M, we exhibit non-trivial relations between $\operatorname{rk} A(M) - \operatorname{rk} A(K)$ and $\operatorname{rk} A(L) - \operatorname{rk} A(K)$.

In Section 3, we build on the ideas of [1], where it was proved that $\mathbb{Q}$-curves of certain type have additional structure, which forces them to have even rank over their field of definition. The additional structure of these curves can be seen in

P.B. was supported by Swiss National Science Foundation grants 124737 and 137928, and by the Max-Planck-Institut für Mathematik, Bonn.

F.N. was supported by the Ministry of Science, Education, and Sports, Republic of Croatia, grant 037-0372781-2821.

the endomorphisms of their restrictions of scalars. In a similar way we construct, for arbitrarily large n, an elliptic curve E_n defined over a number field K_n such that the endomorphism algebra of the restriction of scalars $\operatorname{Res}_{K_n/\mathbb{Q}} E_n$ contains a cyclotomic field of degree 2^n.

Let $\mathbb{Q}(2)$ be the compositum of all quadratic extensions of $\mathbb{Q}$. We ask the following question: does every elliptic curve E over a number field K have infinite rank over $K\mathbb{Q}(2)$? We show that if the answer is yes, then an elliptic curve E_n/K_n as above has infinitely many quadratic twists whose rank is a positive multiple of 2^n.

2. Growth of the rank in extensions

In this section we study how the rank of an Abelian variety can grow upon finite extensions.

2.1. Galois extensions.

Let A be an Abelian variety over K, and let L be a finite Galois extension of K. We compare the ranks of $A(K)$ and $A(L)$ by looking at the action of $G = \operatorname{Gal}(L/K)$ on $\mathbb{Q} \otimes A(L)$. In particular, we are interested in the possible $\mathbb{Q}$-dimensions of $\mathbb{Q} \otimes (A(L)/A(K))$. This is controlled by the dimensions of the non-trivial irreducible $\mathbb{Q}$-linear representations of G. For example, the smallest non-trivial increase of the rank of A when going from K to L equals the smallest dimension of an irreducible non-trivial $\mathbb{Q}$-linear representation of $\operatorname{Gal}(L/K)$. We will study such constraints on the rank of $A(L)$ for various groups G.

Theorem 1. *Let $p > 2$ be a prime, let A be an Abelian variety defined over a number field K, and let L be a Galois extension of K such that* $\operatorname{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$. *Then*

$$\operatorname{rk} A(L) \equiv \operatorname{rk} A(K) \pmod{p-1}.$$

Proof. First note that the fixed subspace of $\mathbb{Q} \otimes A(L)$ under $\operatorname{Gal}(L/K)$ corresponds to $\mathbb{Q} \otimes A(K)$, the dimension of which is $\operatorname{rk} A(K)$.

Over $\mathbb{C}$, the irreducible representations of the group $\mathbb{Z}/p\mathbb{Z}$ are the trivial representation and the $p-1$ representations corresponding to the non-trivial characters of $\mathbb{Z}/p\mathbb{Z}$. However, the smallest field over which the non-trivial characters are defined is $\mathbb{Q}(\zeta_p)$. In fact, there are two irreducible $\mathbb{Q}$-linear representations: the trivial representation and a representation of dimension $p-1$. This implies that $\operatorname{rk} A(L) - \operatorname{rk} A(K) = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes (A(L)/A(K)))$ is a multiple of $p-1$. ☐

Corollary 2. *Let A be an Abelian variety defined over a number field K, and let L/K be a Galois extension of odd degree n. Then*

$$\operatorname{rk} A(L) = \operatorname{rk} A(K) \text{ or } \operatorname{rk} A(L) \geq \operatorname{rk} A(K) + p - 1,$$

where p is the smallest prime dividing n.

Proof. By the Feit–Thompson theorem [4], $\operatorname{Gal}(L/K)$ is solvable, so there is a sequence of intermediate fields $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that each extension K_i/K_{i-1} is cyclic of some prime degree $p_i \mid n$. Theorem 1 implies that $\operatorname{rk} A(L) - \operatorname{rk} A(K)$ is a linear combination of the $p_i - 1$, and the claim follows. ☐

We now turn our attention to the case where G is an alternating group.

Theorem 3. *Let A be an Abelian variety defined over a number field K. Let $n \geq 3$ and let L/K be a Galois extension with group A_n. Then*

$$\operatorname{rk} A(L) = \operatorname{rk} A(K) \text{ or } \operatorname{rk} A(L) \geq \operatorname{rk} A(K) + \begin{cases} 2 & \text{if } n = 4, \\ n-1 & \text{if } n = 3 \text{ or } n \geq 5. \end{cases}$$

Proof. As $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$, the case $n = 3$ is already proved in Theorem 1.

The group A_4 has two non-trivial complex representations of dimension 1, but their images involve third roots of unity and are therefore are not defined over $\mathbb{Q}$. Hence all non-zero, non-trivial representations of A_4 over $\mathbb{Q}$ have dimension ≥ 2.

The group A_5 has two irreducible complex representations of dimension 3, but these involve fifth roots of unity. The minimal dimension of a non-trivial $\mathbb{Q}$-linear irreducible representation equals 4.

It is well known [6, Exercise 5.5] that the dimension of the smallest irreducible $\mathbb{C}$-linear (and hence also $\mathbb{Q}$-linear) representation of A_n is of dimension $n - 1$ for $n > 5$, completing the proof. □

Remark. In the setting of Theorem 3 for $n = 4$, as A_4 has one 2-dimensional and one 3-dimensional $\mathbb{Q}$-linear irreducible representation. As every positive integer apart from 1 can be written as the sum of multiples of 2 and 3, it follows that $\operatorname{rk} A(L) - \operatorname{rk} A(K)$ can a priori be any non-negative integer apart from 1.

Here is a similar result about extensions with Galois group $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{PSL}_2(\mathbb{F}_p)$.

Theorem 4. *Let A be an Abelian variety over a number field K, and let L be a finite Galois extension with group $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{PSL}_2(\mathbb{F}_p)$ for some prime $p > 2$. Then*

$$\operatorname{rk} A(L) = \operatorname{rk} A(K) \text{ or } \operatorname{rk} A(L) \geq \operatorname{rk} A(K)) + \frac{p-1}{2}.$$

Proof. The minimal dimension of an irreducible non-trivial $\mathbb{Q}$-linear representation of $\mathrm{SL}_2(\mathbb{F}_p)$ is $(p-1)/2$ [6, Chapter 5.2, pages 71–73]. Similarly, the smallest dimension of a non-trivial irreducible $\mathbb{Q}$-linear representation of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $(p-1)/2$ [6, Exercise 5.10, page 71]. □

Corollary 5. *Let E be an elliptic curve over a number field K, and let $p > 2$ be a prime such that the Galois representation*

$$\rho_p \colon \operatorname{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_p).$$

coming from the action of $\operatorname{Gal}(\overline{K}/K)$ on $E[p]$ is surjective. Let L be a subfield of $K(E[p])$ with $[K(E[p]) : L] \leq 2$. Then

$$\operatorname{rk} E(L) = \operatorname{rk} E(K(\zeta_p)) \text{ or } \operatorname{rk} E(L) \geq \operatorname{rk} E(K(\zeta_p)) + \frac{p-1}{2}$$

Proof. We note that ρ_p factors through $\operatorname{Gal}(K(E[p])/K)$. By the properties of the Weil pairing, $K(E[p])$ contains $K(\zeta_p)$, and ρ_p identifies $\operatorname{Gal}(K(E[p])/K(\zeta_p))$ with $\mathrm{SL}_2(\mathbb{F}_p)$. If $[K(E[p]) : L] = 2$, then L is the fixed field of $-I$, the unique element of order 2 in $\mathrm{SL}_2(\mathbb{F}_p)$, and ρ identifies $\operatorname{Gal}(L/K(\zeta_p))$ with $\mathrm{PSL}_2(\mathbb{F}_p)$. Hence $\operatorname{Gal}(K(E[p])/K(\zeta_p))$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$ if $L = K(E[p])$, and to $\mathrm{PSL}_2(\mathbb{F}_p)$ if $[K(E[p]) : L] = 2$. The claim now follows from Theorem 4. □

Remark. By Serre's open image theorem [13], if E does not have complex multiplication, then the map ρ_p is surjective for all but finitely many primes p.

In view of the results proved in this section, it is natural to wonder what characterizes the groups G such that for Galois extensions L/K with group G, one can give a non-trivial lower bound on $\operatorname{rk} A(L) - \operatorname{rk} A(K)$, whenever $\operatorname{rk} A(L) - \operatorname{rk} A(K) > 0$. The following theorem answers this question.

Theorem 6. *Let L/K be a finite Galois extension of number fields such that $G = \operatorname{Gal}(L/K)$ does not contain a subgroup of index 2. Then for any Abelian variety A over K, either $\operatorname{rk} A(L) = \operatorname{rk} A(K)$ or $\operatorname{rk} A(L) \geq \operatorname{rk} A(K) + 2$.*

Proof. As G has no subgroup of index 2, there is no non-trivial homomorphism $G \to \mathbb{Q}^\times_{\mathrm{tors}} = \{1, -1\}$. Therefore G has no non-trivial irreducible representation of dimension 1 over $\mathbb{Q}$. $\square$

Note that none of the groups G considered above has an index 2 subgroup. If L/K is a finite Galois extension for which $\mathrm{Gal}(L/K)$ does have an index 2 subgroup, then L contains $K(\sqrt{d})$ for some $d \in K^\times \setminus (K^\times)^2$. If A is an Abelian variety over K, we cannot exclude that $\mathrm{rk}\, A(L) = \mathrm{rk}\, A(K(\sqrt{d})) > \mathrm{rk}\, A(K)$. Now $\mathrm{rk}\, A(K(\sqrt{d})) = \mathrm{rk}\, A(K) + \mathrm{rk}\, A^d(K)$, where A^d is the quadratic twist of A by d; in general, we cannot prove any restrictions on $\mathrm{rk}\, A^d(K)$. So index 2 subgroups form an obstruction for results of the type of Theorems 1, 3 and 4; in this sense, Theorem 6 is best possible.

Remark. The above results rely on the decomposition of $A(L)$ into irreducible representations of $G = \mathrm{Gal}(L/K)$. More conceptually, they can be interpreted via a decomposition of the Weil restriction $B = \mathrm{Res}_{L/K} A_L$ in the category of Abelian varieties over K up to isogeny, namely

$$B \sim \bigoplus_\rho B_\rho,$$

where ρ ranges over the irreducible $\mathbb{Q}$-linear representations of G and the group algebra $\mathbb{Q}[G]$ acts on B_ρ through a simple quotient algebra R_ρ; see [3, § 3.4] and [8, Theorem 4.5]. Our results can then be explained by the fact that in the situations we consider, R_ρ is strictly larger than $\mathbb{Q}$ for all non-trivial ρ.

2.2. **Non-Galois extensions.** We start by recalling a bit of representation theory. Let G be a finite group, and let $H \subseteq G$ a subgroup. For finite-dimensional $\mathbb{Q}$-linear representations V of G, we are interested in non-trivial relations between the dimensions of the $\mathbb{Q}$-vector spaces $V^G \subseteq V^H \subseteq V$.

Let C_G denote the set of conjugacy classes of G, and let χ_V denote the character of the representation V, viewed as a function on C_G. It is well known, as a special case of Schur's orthogonality relations, that the dimension of V^G equals

$$\begin{aligned} d_G(\chi_V) &= \frac{1}{\#G} \sum_{g \in G} \chi_V(\text{conjugacy class of } g) \\ &= \frac{1}{\#G} \sum_{c \in C_G} \#c \cdot \chi_V(c). \end{aligned}$$

We can write $\chi_V = \sum_{\chi \in X(G)} n_\chi \chi$, where $X(G)$ is the set of characters of irreducible $\mathbb{Q}$-linear representations of G and the n_χ are non-negative integers. Then we have

$$\begin{aligned} \dim V^G &= n_{\mathbf{1}}, \\ \dim V^H &= \sum_{\chi \in X(G)} n_\chi d_H(\chi), \\ \dim V &= \sum_{\chi \in X(G)} n_\chi d_{\{\mathrm{id}\}}(\chi). \end{aligned}$$

In the above notation, $d_{\{\mathrm{id}\}}(\chi) = \chi(\{\mathrm{id}\})$ is the dimension of the irreducible representation of G with character χ. The results obtained above for Galois extensions L/K with group G are explained by the fact that in all the cases we considered, $d_{\{\mathrm{id}\}}(\chi) > 1$ for all non-trivial irreducible representations χ of G over $\mathbb{Q}$.

The explanation of the following theorem is that the pairs (G, H) we consider have the property that $d_{\{\mathrm{id}\}}(\chi)$ is strictly greater than $d_H(\chi)$ for all non-trivial χ.

Namely, we note that

$$\begin{aligned}\dim V^H - \dim V^G &= \sum_{\chi\neq\mathbf{1}} n_\chi d_H(\chi),\\ \dim V - \dim V^H &= \sum_{\chi\in X(G)} n_\chi(d_{\{\mathrm{id}\}}(\chi) - d_H(\chi)).\end{aligned}$$

If $\dim V^H > \dim V^G$, then n_χ is non-zero for some $\chi \neq \mathbf{1}$, and the contribution of this χ in the formula for $\dim V - \dim V^H$ shows that $\dim V > \dim V^H$.

We apply the above observations to the Galois group of a normal closure of a non-Galois extension L/K of number fields. For simplicity, we assume $[L : K] \leq 4$.

Theorem 7. *Let L/K be an extension of number fields, let $n = [L : K]$, let M/K be a normal closure of L/K, and let $G = \mathrm{Gal}(M/K)$. Let A be an Abelian variety over K.*

1. *If $n = 3$ and $G \simeq S_3$, then $\mathrm{rk}\, A(M) - \mathrm{rk}\, A(K) \geq 2(\mathrm{rk}\, A(L) - \mathrm{rk}\, A(K))$.*
2. *If $n = 4$ and $G \simeq A_4$, then $\mathrm{rk}\, A(M) - \mathrm{rk}\, A(K) \geq 3(\mathrm{rk}\, A(L) - \mathrm{rk}\, A(K))$, and $\mathrm{rk}\, A(L)$ and $\mathrm{rk}\, A(M)$ have the same parity.*
3. *If $n = 4$ and $G \simeq S_4$, then $\mathrm{rk}\, A(M) - \mathrm{rk}\, A(K) \geq 3(\mathrm{rk}\, A(L) - \mathrm{rk}\, A(K))$.*

Proof. Let $H = \mathrm{Gal}(M/L) \subseteq G$, so that $[G : H] = n$. We identify G with a transitive subgroup of S_n acting on $\{1, 2, \ldots, n\}$, in such a way that H is the stabilizer of 1. We put $V = A(M)$, so that $A(L) = V^H$ and $A(K) = V^G$.

First let L/K be a non-cyclic extension of degree 3, so that $G = S_3$ and $H = \{\mathrm{id}, (23)\} \subset G$. The group S_3 has three irreducible representations over $\mathbb{Q}$ (the situation is the same as over $\mathbb{C}$): the trivial representation $\mathbf{1}$, the sign representation ϵ, and a unique two-dimensional representation ρ, namely the obvious permutation representation of S_3 on $\{(x_1, x_2, x_3) \in \mathbb{Q}^3 \mid x_1 + x_2 + x_3 = 0\}$. One can check easily that the H-invariant subspaces of $\mathbf{1}$, ϵ, ρ are of dimension 1, 0, 1, respectively. This implies that if

$$V \simeq n_{\mathbf{1}} \cdot \mathbf{1} \oplus n_\epsilon \cdot \epsilon \oplus n_\rho \cdot \rho,$$

then

$$\begin{aligned}\dim V^G &= n_{\mathbf{1}},\\ \dim V^H &= n_{\mathbf{1}} + n_\rho,\\ \dim V &= n_{\mathbf{1}} + n_\epsilon + 2n_\rho.\end{aligned}$$

This is equivalent to (1).

Let V_4 denote the unique normal subgroup of order 4 of S_4; more concretely,

$$V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \subset A_4 \subset S_4.$$

Let us now consider $G = A_4$. Then we have $H = \langle(234)\rangle$ and $G = V_4 \rtimes H$. The group A_4 has three irreducible representations over $\mathbb{Q}$: the trivial representation $\mathbf{1}$, the direct sum of the two non-trivial one-dimensional representations ϵ and $\bar{\epsilon}$ of A_4/V_4 (each of which is defined over $\mathbb{Q}(\zeta_3)$), and the standard 3-dimensional representation ρ_3. One checks that the H-invariant subspaces of $\mathbf{1}$, $\epsilon + \bar{\epsilon}$, ρ_3 are of dimension 1, 0, 1, respectively. This proves (2).

Finally, we consider $G = S_4$. Then we have $H \simeq S_3$ and $G = V_4 \rtimes H$. The group S_4 has five irreducible representations, both over $\mathbb{C}$ and over $\mathbb{Q}$: the trivial representation $\mathbf{1}$, the sign representation ϵ, a two-dimensional representation ρ_2 arising via the surjection $S_4 \to S_3$ from the two-dimensional representation ρ of S_3, the standard 3-dimensional representation ρ_3, and the 3-dimensional representation $\epsilon \otimes \rho_3$. One checks that the H-invariant subspaces of $\mathbf{1}$, ϵ, ρ_2, ρ_3, $\epsilon \otimes \rho_3$ are of dimension 1, 0, 0, 1, 0, respectively. This proves (3). ∎

Finally, we note a curious property of certain quadratic twists of Abelian varieties over quadratic extensions of number fields.

Proposition 8. *Let L/K be a quadratic extension of number fields, and let A be an Abelian variety of dimension g over L. Let $B = \operatorname{Res}_{L/K} A$, and assume that $\mathbb{Q} \otimes \operatorname{End}_K B$ contains a number field of some degree n. Let $\delta \in K^\times$, and let M be the Galois closure of $L(\sqrt{\delta})$ over K.*

1. *The rank of $A(L)$ is divisible by n.*
2. *If $\operatorname{Gal}(M/K) \simeq V_4$, then $\operatorname{rk} A^\delta(L)$ is divisible by n.*
3. *If $\operatorname{Gal}(M/K) \simeq D_4$, then $2 \operatorname{rk} A^\delta(L)$ is divisible by n.*

Proof. Our assumption on $\operatorname{End}_K B$ implies that $\operatorname{rk} A(L) = \operatorname{rk} B(K)$ is divisible by n, so (1) is clear.

If $\operatorname{Gal}(M/K) \simeq V_4$, the field M is equal to $L(\sqrt{\delta})$, and M is also of the form $L(\sqrt{e})$ with $e \in K$. Hence

$$\begin{aligned} \operatorname{rk} A^\delta(L) &= \operatorname{rk} A(M) - \operatorname{rk} A(L) \\ &= \operatorname{rk} B(K(\sqrt{e})) - \operatorname{rk} B(K). \end{aligned}$$

By assumption, both terms on the right-hand side are divisible by n, implying (2).

If $\operatorname{Gal}(M/K) \simeq D_4$, the field M is a quadratic extension of $L(\sqrt{\delta})$. Let M_0 be the unique V_4-extension of K contained in M. By looking at the irreducible representations of D_4, one can show that there are non-negative integers a, b, c, d, e such that

$$\begin{aligned} \operatorname{rk} A(M) &= a + b + c + d + 2e, \\ \operatorname{rk} A(M_0) &= a + b + c + d, \\ \operatorname{rk} A(L(\sqrt{\delta})) &= a + c + e, \\ \operatorname{rk} A(L) &= a + c. \end{aligned}$$

We note that L, M_0, M (but not $L(\sqrt{\delta})$) are all of the form $L \otimes_K N$ for some number field N. This implies that the ranks of $A(L)$, $A(M)$, and $A(M)$ are all divisible by n. Therefore $2e$ is divisible by n. Furthermore,

$$\begin{aligned} \operatorname{rk} A^\delta(L) &= \operatorname{rk} A(L(\delta)) - \operatorname{rk} A(L) \\ &= e, \end{aligned}$$

which proves (3). ∎

3. $\mathbb{Q}$-curves and ranks of twists

The question whether the rank of an elliptic curve over $\mathbb{Q}$ can be arbitrarily large is one of the most important open problems concerning elliptic curves. Somewhat similar questions are: how large can the rank of a twist of a fixed elliptic curve $E/\mathbb{Q}$ be, and what is the largest n such that E has infinitely many twists with rank at least n? The best known result about the latter question for an arbitrary $E/\mathbb{Q}$ is that there exist infinitely many twists of E with rank at least 2 [9]. There exist elliptic curves with infinitely many twists of rank at least 4 [10, 11]. If one assumes the parity conjecture, then there are also elliptic curves over $\mathbb{Q}$ with infinitely many quadratic twists of rank 5 [11].

In this section, for arbitrarily large n, we construct elliptic curves E_n over number fields K_n such that the endomorphism ring of the Weil restriction of scalars $\operatorname{Res}_{K_n/\mathbb{Q}} E_n$ contains an order in a number field of degree 2^n. We also study the problem of constructing, for arbitrarily large n, elliptic curves over number fields admitting infinitely many quadratic twists whose rank is a positive multiple of 2^n. We ask the question whether every elliptic curve E/K has infinite rank over $K\mathbb{Q}(2)$, where $\mathbb{Q}(2)$ is the compositum of all quadratic extensions of $\mathbb{Q}$. A positive answer would imply that the elliptic curves E_n/K_n just mentioned have infinitely many quadratic twists whose rank is a positive multiple of 2^n.

The ideas are inspired by [1], where it was proved that every elliptic curve E with a point of order 13 or 18 over a quadratic field K has even rank. The reason for this is that the endomorphism ring of $\operatorname{Res}_{K/\mathbb{Q}} E$ contains $\mathbb{Z}[\sqrt{d}]$, where d is not a square. This forces $(\operatorname{Res}_{K/\mathbb{Q}} E)(\mathbb{Q}) \simeq E(K)$ to be a $\mathbb{Z}[\sqrt{d}]$-module. Hence, $E(K)$ is of even rank. The result mentioned in the previous paragraph shows that one can similarly construct elliptic curves over number fields whose rank is divisible by integers larger than 2.

A $\mathbb{Q}$-*curve* is an elliptic curve E over $\overline{\mathbb{Q}}$ that is $\overline{\mathbb{Q}}$-isogenous to ${}^{\sigma}E$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. An interesting property of $\mathbb{Q}$-curves is the fact that the rich structure of these curves has consequences for their rank. For example, the proof that all elliptic curves over quadratic fields with a point of order 13 or 18 have even rank [1] uses the fact that all such curves are in fact $\mathbb{Q}$-curves. A good and thorough account of the properties of the endomorphism algebras of the restrictions of scalars of $\mathbb{Q}$-curves can be found in [12].

Proposition 9. *For every integer $n \geq 2$, there exists an elliptic curve E over a number field K such that $\mathbb{Q}\otimes\operatorname{End}_{\mathbb{Q}}(\operatorname{Res}_{K/\mathbb{Q}} E)$ contains a number field of degree 2^n.*

Proof. Most of the work needed for this proposition has already been done in [12, pages 309–312]. Let

$$E_a\colon y^2 = x^3 - 3\sqrt{a}(4+5\sqrt{a})x + 2\sqrt{a}(2+14\sqrt{a}+11a), \tag{1}$$

where a is a non-square rational number, be a member of the family of $\mathbb{Q}$-curves parametrized by $X^*(3)$ (the quotient of $X_0(3)$ by the Atkin–Lehner involution w_3); see [12, page 309]. Let p be a prime such that $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod{2^n}$; there exists infinitely many such primes by the Chinese remainder theorem and Dirichlet's theorem on primes in arithmetic progressions. Note also that this prime satisfies $p \equiv 5 \pmod{12}$.

Let us write $\nu = \operatorname{ord}_2(p-1)$. Let ϵ be a Dirichlet character of order 2^ν and conductor $4p$. Such a character exists, since $(\mathbb{Z}/4p\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/(p-1)\mathbb{Z}$ and an element $(1,t)$, where t is of order 2^ν, written in additive notation, has the desired properties. We write $K = K_\epsilon(\sqrt{-p})$, where K_ϵ is the splitting field of ϵ.

As explained in [12, page 312 (d)], under these assumptions, there exists an element $\gamma \in K^\times$ such that E_{-p}^{γ} satisfies

$$\mathbb{Q}\otimes\operatorname{End}_{\mathbb{Q}}\operatorname{Res}_{K/\mathbb{Q}} E_{-p}^{\gamma} \simeq \mathbb{Q}(\zeta_{2^{\nu+1}}, \sqrt{3}).$$

Note that $\nu \geq n$, so $[\mathbb{Q}(\zeta_{2^{\nu+1}}, \sqrt{3}) : \mathbb{Q}] \geq 2\phi(2^{n+1}) = 2^{n+1}$. The claim follows. □

Remark. Let $\mathbb{Q}(2)$ be the compositum of all quadratic extensions of $\mathbb{Q}$. Note that the elliptic curve E_a from (1) is defined over a quadratic field. By [7, Theorem 5], $E_a(\mathbb{Q}(2))$ has infinite rank. (The statement of loc. cit. is that $E_a(\mathbb{Q}^{\mathrm{ab}})$ has infinite rank, but the proof shows in fact that already $E_a(\mathbb{Q}(2))$ has infinite rank.) This implies that there exist infinitely many quadratic twists E_a^d with d a rational integer, pairwise non-isomorphic over $\mathbb{Q}(\sqrt{a})$, such that $E_a^d(\mathbb{Q}(\sqrt{a}))$ has positive rank. Let S be the set of such integers d. Since for any finite extension $F/\mathbb{Q}(\sqrt{a})$ the set of $d \in \mathbb{Q}$ with $\sqrt{d} \in F$ is finite, it follows that also over F there are infinitely many $d \in F^\times/(F^\times)^2$ such that $E_a^d(F)$ has positive rank.

If E is a $\mathbb{Q}$-curve and $K \subset \overline{\mathbb{Q}}$ is a number field, we say that E is *completely defined over* K if E and all isogenies $E \to {}^{\sigma}E$, for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, are defined over K.

Proposition 10. *Let E be a $\mathbb{Q}$-curve completely defined over a number field K such that $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(\mathrm{Res}_{K/\mathbb{Q}} E)$ contains a number field B. For every number field N which can be written as $K \otimes_{\mathbb{Q}} N'$ for some number field N', $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(\mathrm{Res}_{N/\mathbb{Q}} E)$ is a B-vector space.*

Proof. Let N' be a number field such that $N = K \otimes_{\mathbb{Q}} N'$ is also a field. Then

$$E(N) = E(K \otimes_{\mathbb{Q}} N') \simeq \mathrm{Res}_{K/\mathbb{Q}} E(N').$$

As $\mathbb{Q} \otimes \mathrm{End}_{N'}(\mathrm{Res}_{K/\mathbb{Q}} E)$ contains B, it follows that $\mathbb{Q} \otimes E(N) \simeq \mathbb{Q} \otimes \mathrm{Res}_{K/\mathbb{Q}} E(N')$ has a natural B-vector space structure. □

Let $\mathbb{Q}(2)$ be the compositum of all quadratic extensions of $\mathbb{Q}$. The following question is a variant of [7, Question 2].

Question 11. Does every elliptic curve over a number field K have infinite rank over $K\mathbb{Q}(2)$?

Remark. Suppose that every Abelian variety over $\mathbb{Q}$ has infinite rank over $\mathbb{Q}(2)$; this is a variant of [5, page 127, Problem]. Then by taking the Weil restriction, we obtain a positive answer to Question 11.

Theorem 12. *Suppose that Question 11 has a positive answer. Let n be a positive integer. There exist a number field K and an elliptic curve E over K possessing infinitely many twists E^d over K such that $\mathrm{rk}\, E^d(K)$ is a positive multiple of 2^n.*

Proof. As shown in Proposition 9, there exists an elliptic curve E over a number field K such that $\mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(\mathrm{Res}_{K/\mathbb{Q}} E)$ contains a number field B of degree 2^n. It follows that the rank of $E(K) = (\mathrm{Res}_{K/\mathbb{Q}} E)(\mathbb{Q})$ is divisible by 2^n.

By assumption, E has infinitely many (pairwise non-isomorphic) quadratic twists E^d, with d a square-free integer, such that $\mathrm{rk}\, E^d(K) > 0$. Let E^d be such a twist, with $\sqrt{d} \notin K$. As $K \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) \simeq K(\sqrt{d})$ is a field (see for example [2, Theorem 2.2]), it follows from Proposition 10 that the rank of $E(K(\sqrt{d})) = (\mathrm{Res}_{K/\mathbb{Q}} E)(\mathbb{Q}(\sqrt{d}))$ is divisible by 2^n. But

$$\mathrm{rk}\, E(K(\sqrt{d})) = \mathrm{rk}\, E(K) + \mathrm{rk}\, E^d(K),$$

from which it follows that $\mathrm{rk}\, E^d(K)$ is divisible by 2^n. □

Acknowledgments. We are greatly indebted to Jordi Quer for help with the proof of Proposition 9. We are grateful to Andrej Dujella, Ivica Gusić, and Matija Kazalicki for many helpful comments and motivating discussions.

References

[1] J. Bosman, P. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, preprint.

[2] P. M. Cohn, *On the decomposition of a field as a tensor product of fields*, Glasgow Math. J. **20** (1979), 141–145.

[3] C. Diem and N. Naumann, *On the structure of Weil restrictions of abelian varieties*, J. Ramanujan Math. Soc. **18** (2003), no. 2, 153–174.

[4] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.

[5] G. Frey and M. Jarden, *Approximation theory and the rank od Abelian varieties over large algebraic fields*, Proc. London. Math. Soc. **28** (1974), 112–128.

[6] W. Fulton and J. Harris, Representation theory: A first course, Springer-Verlag, New York, 1993.

[7] B.-H. Im and M. Larsen, *Infinite rank of elliptic curves over* $\mathbb{Q}^{\mathrm{ab}}$, http://arxiv.org/abs/1202.1187.

[8] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), 419–438.

[9] J.-F. Mestre. *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **314** (1992), 919–922.

[10] J.-F. Mestre, *Rang de certaines familles de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **327** (1998), 763–764.

[11] K. Rubin and A. Silverberg, *Twists of elliptic curves of rank at least four*, in: Ranks of elliptic curves and random matrix theory, J. B. Conrey et al., eds., London Math. Soc. Lect. Notes **341**, Cambridge University Press (2007), 177–188.

[12] J. Quer, $\mathbb{Q}$-*curves and abelian varieties of* GL_2-*type*, Proc. London Math. Soc. **81** (2000), 285–317.

[13] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–311.

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, 8057 Zürich, Switzerland

E-mail address: `peter.bruin@math.uzh.ch`

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address: `fnajman@math.hr`