Math. Res. Lett. **19** (2012), *no.* 06, 1171–1184

PULLING BACK TORSION LINE BUNDLES TO IDEAL CLASSES

Jean Gillibert and Aaron Levin

Abstract. We prove results concerning the specialization of torsion line bundles on a variety V defined over $\mathbb{Q}$ to ideal classes of number fields. This gives a new general technique for constructing and counting number fields with large class group.

1. Introduction

The purpose of this paper is to study the specialization of torsion line bundles, on a variety V defined over $\mathbb{Q}$, to ideal classes of number fields, and to make this operation optimal, that is, to make the kernel of specialization as small as possible.

The main motivation for introducing this technique is the construction of number fields whose class group has large torsion from varieties (over $\mathbb{Q}$) whose Picard group has large torsion. For instance, we show how the problem of constructing quadratic number fields with large class group can be reduced to the problem of finding a hyperelliptic curve with a rational Weierstrass point and a large rational torsion subgroup in its Jacobian (see Corollary 3.2). This technique is an abstraction and generalization of the method used in [13], which used certain superelliptic curves to obtain new constructions of number fields with a large ideal class group. Further results on the construction of large ideal class groups will appear in a separate paper by the second author. We mention also the closely related geometric techniques used by Mestre in [15–18] to construct number fields with a large ideal class group.

On the other hand, the question of pulling back line bundles on arithmetic varieties to nontrivial ideal classes of number fields has been raised by Agboola and Pappas in [1]. Our results positively answer their question in the case of torsion line bundles on a hyperelliptic curve (see Corollary 3.8 for the precise statement).

A consequence of our main result is the following:

Theorem 1.1. *Let V be a smooth projective variety over $\mathbb{Q}$, and let $m > 1$ be an integer. Let S be the set of places of bad reduction of V, and let $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$ be a smooth projective model of V. Then there exists an infinity of number fields K with a point $P \in V(K)$ such that the specialization map*

$$P^* : \operatorname{Pic}(V)[m] = \operatorname{Pic}(\mathcal{V})[m] \longrightarrow \operatorname{Cl}(\mathcal{O}_{K,S})[m]$$

satisfies

$$\operatorname{rk}_m \operatorname{Im}(P^*) \geq \operatorname{rk}_m \operatorname{Pic}(V)[m] + \#S - \operatorname{rk} \mathcal{O}_{K,S}^\times.$$

Received by the editors September 19, 2011.

More precisely, given a generically finite rational map $V \to \mathbb{A}^l$ of degree d, it is possible to find an infinity of such K of degree d.

Two short comments: (1) in our terminology, a variety over $\mathbb{Q}$ is a geometrically integral separated scheme of finite type over $\mathbb{Q}$. (2) If A is a finitely generated abelian group and $m \geq 2$ an integer, $\operatorname{rk}_m A$ denotes the largest integer r such that A has a subgroup isomorphic to $(\mathbb{Z}/m)^r$. See Section 2.1 for further notation.

Of course, results analogous to those given here can also be established when the variety V is defined over any number field instead of $\mathbb{Q}$. Another generalization would be to replace line bundles, i.e., $\mathbf{G}_{\mathrm{m}}$-torsors, by torsors under other group schemes, like tori.

Let us briefly describe the proof of Theorem 1.1. We first choose r linearly independent elements of order m in the group $\operatorname{Pic}(V) = \operatorname{Pic}(\mathcal{V})$ (see Lemma 2.7). By Kummer theory over $\mathcal{V}$, it is possible to lift these r elements to r elements in the flat (fppf) cohomology group $H^1(\mathcal{V}, \mu_m)$. These classes in $H^1(\mathcal{V}, \mu_m)$ are represented by μ_m-torsors $\mathcal{X}_i \to \mathcal{V}$. Let $X_i \to V$ be the restriction of $\mathcal{X}_i$ to V, and let $X \to V$ be the fiber product over V of the X_i. We choose a generically finite rational map $V \to \mathbb{A}^l$ of degree d and apply Hilbert's irreducibility theorem to the composite cover $X \to V \to \mathbb{A}^l$. Thus, we get an infinity of points in $\mathbb{A}^l$ whose inverse image in V is a point $P \in V(K)$, with $[K : \mathbb{Q}] = d$. Moreover, the images of the $\mathcal{X}_i$ by the map

$$P^* : H^1(\mathcal{V}, \mu_m) \longrightarrow H^1(\mathcal{O}_{K,S}, \mu_m)$$

are r linearly independent elements of order m. Now, we look at the image of these elements by the natural map $c : H^1(\mathcal{O}_{K,S}, \mu_m) \to \operatorname{Cl}(\mathcal{O}_{K,S})$. By Kummer theory (see Section 2.1), the kernel of this map is $\mathcal{O}_{K,S}^\times/m$, but we can improve the situation by asking that the subgroup generated by the $P^*\mathcal{X}_i$ has trivial intersection with the subgroup $\mathbb{Z}_S^\times/m$. It is also possible to ensure that K is linearly disjoint from the cyclotomic field $\mathbb{Q}(\zeta_{2m})$. Under these conditions, the kernel of the map $c \circ P^*$ is isomorphic to a subgroup of $(\mathbb{Z}/m)^{\operatorname{rk} \mathcal{O}_{K,S}^\times - \#S}$, which proves the result after invoking Lemma 2.6.

The plan of this paper is as follows. In Section 2, after recalling effective versions of Hilbert's irreducibility theorem, we prove our main result, Theorem 2.4, involving a variety V that satisfies some special properties with respect to some set S of prime numbers. Then, using the theory of integral models, we give consequences of our result in the case when V is smooth and S is the set of primes of bad reduction of V. In Section 3, using superelliptic and hyperelliptic curves, we give applications of our technique to the construction of number fields with large class group. Finally, we explain how these results can be applied, in the case of torsion line bundles on hyperelliptic curves, to the question of Agboola and Pappas.

2. Specialization of μ_m-torsors

2.1. Notation and definitions. By a variety over a field k, we will mean a geometrically integral separated scheme of finite type over k.

If A is an abelian group, and if $m > 1$ is an integer, we will denote by $A[m]$ the kernel of multiplication by m in A (that is, the m-torsion of A), and by A/m the cokernel of multiplication by m in A. Also, if A is a finitely generated abelian group, the m-rank of A, which we denote by $\mathrm{rk}_m A$, is the largest integer r such that A has a subgroup isomorphic to $(\mathbb{Z}/m)^r$.

In the following, S will denote a finite set of prime numbers. If K is a number field, we will denote by $\mathcal{O}_{K,S}$ the ring of S_K-integers of K, where S_K is the set of primes of K lying above primes in S. In the particular case when $K = \mathbb{Q}$, we denote this ring by $\mathbb{Z}_S$ instead of $\mathcal{O}_{\mathbb{Q},S}$. Let us note that $\mathbb{Z}_S$ is nothing else than the ring of fractions $\mathbb{Z}[S^{-1}]$.

We recall that, by Kummer theory, we have a canonical isomorphism

$$H^1(K, \mu_m) \simeq K^\times/m.$$

Under this isomorphism, one identifies the first cohomology group $H^1(\mathcal{O}_{K,S}, \mu_m)$, computed using the fppf topology, as the following subgroup of $H^1(K, \mu_m)$:

$$H^1(\mathcal{O}_{K,S}, \mu_m) = \{z \in K^\times/m \mid \forall\, \mathfrak{p} \notin S_K, v_{\mathfrak{p}}(z) \equiv 0 \pmod{m}\},$$

where $\mathfrak{p}$ runs through nonzero prime ideals of K. According to fppf Kummer theory over $\mathrm{Spec}(\mathcal{O}_{K,S})$, this group fits into the exact sequence

$$0 \longrightarrow \mathcal{O}_{K,S}^\times/m \longrightarrow H^1(\mathcal{O}_{K,S}, \mu_m) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[m] \longrightarrow 0. \tag{2.1}$$

Let us note that all the groups involved here are m-torsion.

Unless specified, all our cohomology groups are computed with respect to the fppf topology.

2.2. Hilbert's irreducibility theorem. An essential tool in our proofs is Hilbert's Irreducibility Theorem, which we now recall in a suitably general, quantitative form due to Cohen [6] (see also [21, Ch. 9]).

For a point $t = (t_1, \dots, t_n) \in \mathbb{A}^n(\mathbb{Z})$, define the height $H(t) = \max_j |t_j|$.

Theorem 2.1 (**Hilbert Irreducibility Theorem**). *Let V be a variety over $\mathbb{Q}$ of dimension l. Let $\phi : V \to \mathbb{A}^l$ be a generically finite rational map. For $t \in \phi(V)(\mathbb{Q})$, let $P_t = \phi^{-1}(t)$. Let k be a number field. Then for all but $O(N^{l-\frac{1}{2}} \log N)$ points $t \in \mathbb{A}^l(\mathbb{Z})$ with $H(t) \le N$, we have $t \in \phi(V)$ and $P_t = \mathrm{Spec}(\mathbb{Q}(P_t))$, where $[k(P_t) : k] = \deg \phi$. If $l = 1$, $O(\sqrt{N} \log N)$ can be replaced by $O(\sqrt{N})$ in the above.*

A very natural problem that arises in connection with Hilbert's Irreducibility Theorem is to determine the number of distinct number fields $\mathbb{Q}(P_t)$ with $H(t) \le N$ in Theorem 2.1. For $l = 1$, this problem has been studied by Dvornicich and Zannier [8,9]. Let C be a curve over $\mathbb{Q}$ and let $\phi : C \to \mathbb{P}^1$ be a morphism. For each integer $t \in \mathbb{A}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Q})$, let $P_t = \phi^{-1}(t)$. Dvornicich and Zannier studied the degree of the field extension $\mathbb{Q}(P_1, \dots, P_N)$. Their results imply in particular a useful result on the number of isomorphism classes of number fields in the set $\{\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N)\}$.

Theorem 2.2 (**Dvornicich and Zannier**). *Let C be a curve over $\mathbb{Q}$. Let $\phi : C \to \mathbb{P}^1$ be a morphism with $\deg \phi > 1$. For each integer t, let $P_t = \phi^{-1}(t)$. Let $g(N)$ denote the number of isomorphism classes of number fields in the set $\{\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N)\}$. Then $g(N) \gg \frac{N}{\log N}$.*

Remark 2.3. The implied constants in Theorems 2.1 and 2.2 are effective and can be explicitly computed.

2.3. The main result. Let V be a variety over $\mathbb{Q}$. By Kummer theory, we have an exact sequence

$$0 \longrightarrow \mathbf{G}_{\mathrm{m}}(V)/m \longrightarrow H^1(V,\mu_m) \longrightarrow \operatorname{Pic}(V)[m] \longrightarrow 0.$$

Given $L \in \operatorname{Pic}(V)[m]$, we say that a μ_m-torsor on V is a lift of L if its image by the right-hand side map is equal to L.

Theorem 2.4. *Let V be a variety of dimension l over $\mathbb{Q}$, and let $m>1$ be an integer. Assume that there exists a finite set S of prime numbers such that, for any $L \in \operatorname{Pic}(V)[m]$, there exists a μ_m-torsor $T \to V$ lifting L such that, for any number field K and for any point $P \in V(K)$, the pull-back P^*T belongs to $H^1(\mathcal{O}_{K,S},\mu_m)$.*

Let $\phi : V \to \mathbb{A}^l$ be a generically finite rational map. For $t \in \phi(V)(\mathbb{Q})$, let $P_t := \phi^{-1}(t)$. Then for all but $O(N^{l-\frac{1}{2}}\log N)$ ($O(\sqrt{N})$ if $l=1$) points $t \in \mathbb{A}^l(\mathbb{Z})$ with $H(t) \leq N$, we have $t \in \phi(V)$, $P_t = \operatorname{Spec}(\mathbb{Q}(P_t))$ where $\mathbb{Q}(P_t)$ is a number field of degree deg(ϕ), and

$$\operatorname{rk}_m \operatorname{Cl}(\mathcal{O}_{\mathbb{Q}(P_t),S}) \geq \operatorname{rk}_m \operatorname{Pic}(V)_{\mathrm{tors}} + \#S - \operatorname{rk}\mathcal{O}^{\times}_{\mathbb{Q}(P_t),S}. \tag{2.2}$$

Proof. Let $r = \operatorname{rk}_m \operatorname{Pic}(V)_{\mathrm{tors}}$. Using the hypotheses of the theorem, we obtain r torsors $X_i \to V$ that generate a subgroup isomorphic to $(\mathbb{Z}/m)^r$ in $H^1(V,\mu_m)$, and that satisfy the key property: for any number field K and for any point $P \in V(K)$, the pull-back P^*X_i belongs to $H^1(\mathcal{O}_{K,S},\mu_m)$.

Let X be the product of the X_i over V. Then $f : X \to V$ is irreducible of degree m^r, because the $X_i \to V$ are irreducible and linearly independent in $H^1(V,\mu_m)$. Let $k = \mathbb{Q}[\sqrt[m]{u} \mid u \in \mathbb{Z}_S^{\times}]$. One can apply Hilbert's irreducibility theorem to the composition $X \to V \to \mathbb{A}^l$: for all but $O(N^{l-\frac{1}{2}}\log N)$ ($O(\sqrt{N})$ if $l=1$) points $t \in \phi(V) \cap \mathbb{A}^l(\mathbb{Z})$ with $H(t) \leq N$, we have $(\phi \circ f)^{-1}(t) = \operatorname{Spec}(F)$ where F is a field and $[F:\mathbb{Q}] = [kF:k] = (\deg\phi)(\deg f)$. Now, if t is such a point, then $\phi^{-1}(t) = P \in V(K)$ with $K \subseteq F$ and $[K:\mathbb{Q}] = \deg(\phi)$. Then, pulling back the torsors $X_i \to V$ along P, we get r-independent elements in $H^1(K,\mu_m)$ that, by the key property, belong to the subgroup $H^1(\mathcal{O}_{K,S},\mu_m)$. In other words,

$$\operatorname{rk}_m H^1(\mathcal{O}_{K,S},\mu_m) \geq r.$$

In fact, since F is linearly disjoint from k, we have

$$\operatorname{rk}_m H^1(\mathcal{O}_{K,S},\mu_m)/(\mathbb{Z}_S^{\times}/m) \geq r,$$

where we identify $\mathbb{Z}_S^{\times}/m$ with its image under the composite map

$$\mathbb{Z}_S^{\times}/m \to \mathcal{O}_{K,S}^{\times}/m \to H^1(\mathcal{O}_{K,S},\mu_m).$$

Note that K is also linearly disjoint from k, and in particular is linearly disjoint from the cyclotomic field $\mathbb{Q}(\zeta_{2m})$, which is contained in k. So the map $\mathbb{Z}_S^{\times}/m \to \mathcal{O}_{K,S}^{\times}/m$ is injective and

$$(\mathcal{O}_{K,S}^{\times}/m)/(\mathbb{Z}_S^{\times}/m) \simeq (\mathbb{Z}/m)^{\operatorname{rk}\mathcal{O}_{K,S}^{\times} - \#S}.$$

On the other hand, starting from the Kummer exact sequence (2.1), we deduce an exact sequence

$$0 \longrightarrow (\mathcal{O}_{K,S}^{\times}/m)/(\mathbb{Z}_S^{\times}/m) \longrightarrow H^1(\mathcal{O}_{K,S}, \mu_m)/(\mathbb{Z}_S^{\times}/m) \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[m] \longrightarrow 0.$$

This implies, by the second statement of Lemma 2.6, that

$$\begin{aligned}\mathrm{rk}_m \mathrm{Cl}(\mathcal{O}_{K,S})[m] &= \mathrm{rk}_m H^1(\mathcal{O}_{K,S}, \mu_m)/(\mathbb{Z}_S^{\times}/m) - (\mathrm{rk}\, \mathcal{O}_{K,S}^{\times} - \#S) \\ &\geq r + \#S - \mathrm{rk}\, \mathcal{O}_{K,S}^{\times},\end{aligned}$$

hence the result. □

Remark 2.5. (i) In the theorem, the set S *a priori* depends on V and on m. In the applications we give, V is smooth and in this case one may take S to be the set of places of bad reduction of V. Moreover, in the case of curves (cf. Corollary 2.11), it is possible to find a smaller S by taking m into account.

(ii) The inequality (2.2) also holds for the group $\mathrm{Cl}(\mathbb{Q}(P_t))$, because $\mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(P_t),S})$ is a quotient of that group.

Lemma 2.6. *Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{2.3}$$

be an exact sequence of finite m-torsion abelian groups. Then

$$\mathrm{rk}_m B \geq \mathrm{rk}_m A + \mathrm{rk}_m C.$$

Moreover, if A or C is isomorphic to $(\mathbb{Z}/m)^n$ for some n, then

$$\mathrm{rk}_m B = \mathrm{rk}_m A + \mathrm{rk}_m C.$$

Proof. Let us first note that m-torsion abelian groups are modules over the ring $\mathbb{Z}/m$. It follows from the definition that, if M is a finite m-torsion abelian group, and if N is a subgroup or a quotient of M, then $\mathrm{rk}_m N \leq \mathrm{rk}_m M$.

We prove the last statement first. Let us assume that C is isomorphic to $(\mathbb{Z}/m)^n$ for some n. This means that C is a free $(\mathbb{Z}/m)$-module of finite rank, thus is a projective object in the category of $(\mathbb{Z}/m)$-modules. Therefore, by basic homological algebra, the exact sequence (2.3) splits, that is,

$$B \simeq (\mathbb{Z}/m)^n \oplus A.$$

Without loss of generality, we may assume that $m = p^e$ where p is prime and $e \geq 1$. Using the structure theorem for finite abelian groups, we find that

$$\mathrm{rk}_m M = \dim_{\mathbb{F}_p} p^{e-1} M$$

for any $(\mathbb{Z}/m)$-module M. It follows that we have, for any two $(\mathbb{Z}/m)$-modules M and N,

$$\mathrm{rk}_m(M \oplus N) = \mathrm{rk}_m(M) + \mathrm{rk}_m(N).$$

Finally, we get that $\mathrm{rk}_m B = n + \mathrm{rk}_m A$, as desired.

The case when A is isomorphic to $(\mathbb{Z}/m)^n$ for some n is similar to the previous one; indeed, it follows from the structure theorem for finite abelian groups that $(\mathbb{Z}/m)^n$ is an injective object in the category of $(\mathbb{Z}/m)$-modules, and so once again the exact sequence (2.3) splits.

In the general case, let $n = \operatorname{rk}_m C$ and let us choose a subgroup of C isomorphic to $(\mathbb{Z}/m)^n$ (we note that such a subgroup is not unique in general). Then, pulling back the sequence (2.3) by the inclusion $(\mathbb{Z}/m)^n \to C$, we get an exact sequence

$$0 \longrightarrow A \longrightarrow B_1 \longrightarrow (\mathbb{Z}/m)^n \longrightarrow 0$$

where B_1 is some subgroup of B. In particular, $\operatorname{rk}_m B \geq \operatorname{rk}_m B_1$. Now, by the second statement of the Lemma, we have $\operatorname{rk}_m B_1 = \operatorname{rk}_m A + n = \operatorname{rk}_m A + \operatorname{rk}_m C$, from which the result follows. □

2.4. Corollaries. Let V be a smooth projective variety over $\mathbb{Q}$. We say that V has good reduction at a prime p if there exists a smooth projective model of V over $\operatorname{Spec}(\mathbb{Z}_{(p)})$. Otherwise, we say that V has bad reduction at p.

It is well known that the set S of primes of bad reduction of V is finite. Moreover, it is possible to construct a smooth projective model $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$.

Lemma 2.7. *Let V be a smooth projective variety over $\mathbb{Q}$. Let S be the set of primes of bad reduction of V. Then there exists a smooth projective model $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$ of V. Moreover, any such model satisfies*

$$\mathcal{V}(\mathcal{O}_{K,S}) = V(K)$$

for any number field K, and

$$\operatorname{Pic}(\mathcal{V}) = \operatorname{Pic}(V).$$

Proof. The existence of a smooth projective model $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$ was noted above. The projectivity of $\mathcal{V}$ ensures us that any morphism $P : \operatorname{Spec}(K) \to V$ extends to a morphism $\operatorname{Spec}(\mathcal{O}_{K,S}) \to \mathcal{V}$ (valuative criterion of properness).

Because $\mathcal{V}$ is regular, any divisor on V can be extended (by scheme-theoretic closure) to a divisor on $\mathcal{V}$. Thus, the restriction map

$$\operatorname{Pic}(\mathcal{V}) \to \operatorname{Pic}(V)$$

is surjective. The kernel of this map is the subgroup of $\operatorname{Pic}(\mathcal{V})$ generated by fibral (or "vertical") divisors. By assumption V is geometrically connected, so by Zariski's connectedness theorem $\mathcal{V}$ has connected fibers. Therefore, $\mathcal{V}$ has integral fibers (because smooth and connected implies integral), so any fibral divisor is a sum of fibers. In other words, any fibral divisor is the inverse image of a divisor on $\operatorname{Spec}(\mathbb{Z}_S)$. Such a divisor is principal, because $\mathbb{Z}_S$ is principal. So the subgroup generated by fibral divisors is trivial, and the restriction map is bijective. □

Corollary 2.8. *Let V be a smooth projective variety over $\mathbb{Q}$. Then, for any $m > 1$, the hypotheses of Theorem 2.4 hold for V and m when taking S to be the set of primes of bad reduction of V.*

Proof. Let $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$ be the model of V as in Lemma 2.7. By Kummer theory, we have a diagram with exact lines

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{G}_{\mathrm{m}}(\mathcal{V})/m \arrow[r] \arrow[d] & H^1(\mathcal{V}, \mu_m) \arrow[r] \arrow[d] & \operatorname{Pic}(\mathcal{V})[m] \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbf{G}_{\mathrm{m}}(V)/m \arrow[r] & H^1(V, \mu_m) \arrow[r] & \operatorname{Pic}(V)[m] \arrow[r] & 0
\end{tikzcd}$$

where the vertical lines are obtained by restriction to the generic fiber. So, starting from $L \in \operatorname{Pic}(V)[m]$, we get a μ_m-torsor $\mathcal{T} \to \mathcal{V}$ whose generic fiber $T \to V$ is a lift of L.

Now, if $P : \operatorname{Spec}(K) \to V$ is a point, we have a commutative diagram

$$\begin{tikzcd}
H^1(\mathcal{V}, \mu_m) \arrow[r, "P^*"] \arrow[d] & H^1(\mathcal{O}_{K,S}, \mu_m) \arrow[d] \\
H^1(V, \mu_m) \arrow[r, "P^*"] & H^1(K, \mu_m)
\end{tikzcd}$$

where the horizontal lines are pull-backs along P. This proves that P^*T belongs to the subgroup $H^1(\mathcal{O}_{K,S}, \mu_m)$. □

Remark 2.9. If A is an abelian variety over $\mathbb{Q}$, then $A(\mathbb{Q}) = \operatorname{Pic}^0(A^t)$ where A^t is the dual abelian variety of A. It seems interesting to apply Corollary 2.8 to this situation (i.e., taking $V = A^t$). However, then one has to bound the degree of a generically finite rational map $A^t \to \mathbb{A}^l$, where $l = \dim(A)$.

Let us recall that, if C is a curve defined over $\mathbb{Q}$, the index $\operatorname{ind}(C)$ of C is, by definition, the quantity

$$\operatorname{ind}(C) = \gcd\{[K : \mathbb{Q}] \mid C(K) \neq \emptyset\}.$$

Of course, if $C(\mathbb{Q}) \neq \emptyset$, then $\operatorname{ind}(C) = 1$. The converse is false.

We now assume that C is a smooth projective curve of genus $g \geq 1$. Then C has a minimal regular model $\mathcal{C} \to \operatorname{Spec}(\mathbb{Z})$.

Let p be any prime number, and let $\Gamma_1, \ldots, \Gamma_r$ be the irreducible components of the fiber of $\mathcal{C}$ at p. For each i, let δ_i be the geometric multiplicity of Γ_i in the fiber of $\mathcal{C}$ at p (see [3, Section 9.1, Def. 3]). We let

$$I_p(C) := \gcd(\delta_1, \ldots, \delta_r).$$

It is well-known that $I_p(C)$ divides $\operatorname{ind}(C)$ for all p, cf. [2, Cor. 1.5].

Let $\operatorname{Jac}(C)$ be the Jacobian variety of the curve C. This is an abelian variety of dimension g. For each prime number p, we let Φ_p be the group of connected components of the fiber at p of the Néron model of $\operatorname{Jac}(C)$, and we denote by

$$t_p(\operatorname{Jac}(C)) := \#\Phi_p(\mathbb{F}_p)$$

the order of the group of $\mathbb{F}_p$-valued points of Φ_p. Usually, $t_p(\operatorname{Jac}(C))$ is called the Tamagawa number of $\operatorname{Jac}(C)$ at p.

Proposition-Definition 2.10. *Let C be a smooth projective curve of genus $g \geq 1$ over $\mathbb{Q}$, and let $m > 1$. We let $U(C, m) \subseteq \operatorname{Spec}(\mathbb{Z})$ be the set of primes p such that $I_p(C) = 1$ and $t_p(\operatorname{Jac}(C))$ is coprime to m. Then the following holds:*

(*i*) *If $g \geq 2$, the set $U(C, m)$ contains the set of primes of good reduction of $\operatorname{Jac}(C)$.*

(*ii*) *If $\operatorname{ind}(C) = 1$ then $I_p(C) = 1$ for all p. Hence, $U(C, m)$ is the set of primes p such that $t_p(\operatorname{Jac}(C))$ is coprime to m.*

Proof. If $g \geq 2$ and $\operatorname{Jac}(C)$ has good reduction at p, then it follows from [7, Thm. 2.4] that the curve $\mathcal{C}$ is semi-stable at p, hence $I_p(C) = 1$. This proves (*i*). According to [2, Cor. 1.5], $I_p(C)$ divides $\operatorname{ind}(C)$ for all p, hence (*ii*). □

Corollary 2.11. *Let C be a smooth projective curve of genus $g \geq 1$ over $\mathbb{Q}$, and let $m > 1$. Let S be the complement of $U(C, m)$ in $\operatorname{Spec}(\mathbb{Z})$. Let $\phi : C \to \mathbb{A}^1$ be a rational map. Then (with the notation of Theorem 2.4), for all but $O(\sqrt{N})$ values $t = 1, \dots, N$, we have $[\mathbb{Q}(P_t) : \mathbb{Q}] = \deg \phi$ and*

$$\operatorname{rk}_m \operatorname{Cl}(\mathbb{Q}(P_t)) \geq \operatorname{rk}_m \operatorname{Pic}(C)_{\text{tors}} + \#S - \operatorname{rk} \mathcal{O}^{\times}_{\mathbb{Q}(P_t),S}.$$

Proof. Let $Z = U(C, m)$, and let $\pi : \mathcal{C} \to Z$ be the minimal regular model of C over Z. The curve C being geometrically integral, we know (see [14, Section 8.3, Cor. 3.6 (c)]) that $\pi_* \mathcal{O}_{\mathcal{C}} = \mathcal{O}_Z$ holds.

Let $\operatorname{Pic}_{\mathcal{C}/Z}$ be the relative Picard functor of $\mathcal{C}$ over Z, and let $\operatorname{Pic}^0_{\mathcal{C}/Z}$ be its identity component. Let $\mathcal{J} \to Z$ be the Néron model of $\operatorname{Jac}(C)$ over Z, and let $\mathcal{J}^0$ be the identity component of $\mathcal{J}$. By definition of Z, we know that $I_p(C) = 1$ for all $p \in Z$. Hence, according to [3, Section 9.5, Thm. 4 (b)], the functor $\operatorname{Pic}^0_{\mathcal{C}/Z}$ is representable by $\mathcal{J}^0$.

It is clear that $\operatorname{Pic}(Z) = 0$. Therefore, according to [3, Section 8.1, Prop. 4], we have an exact sequence

$$0 \longrightarrow \operatorname{Pic}(\mathcal{C}) \longrightarrow \operatorname{Pic}_{\mathcal{C}/Z}(Z) \longrightarrow H^2(Z, \mathbf{G}_{\mathrm{m}}).$$

Let $\operatorname{Pic}^0(\mathcal{C}/Z)$ be the subgroup of $\operatorname{Pic}(\mathcal{C})$ consisting of elements whose image belongs to $\operatorname{Pic}^0_{\mathcal{C}/Z}(Z)$. By looking at m-torsion, we get an exact sequence

$$0 \longrightarrow \operatorname{Pic}^0(\mathcal{C}/Z)[m] \longrightarrow \operatorname{Pic}^0_{\mathcal{C}/Z}(Z)[m] \longrightarrow H^2(Z, \mathbf{G}_{\mathrm{m}}).$$

Of course, it is possible to consider a similar exact sequence where $\mathcal{C}$ is replaced by C. Putting the two sequences together, we get a diagram with exact lines

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Pic}^0(\mathcal{C}/Z)[m] \arrow[r] \arrow[d, "\rho_1"] & \operatorname{Pic}^0_{\mathcal{C}/Z}(Z)[m] \arrow[r] \arrow[d, "\rho_2"] & H^2(Z, \mathbf{G}_{\mathrm{m}}) \arrow[d, "\rho_3"] \\ 0 \arrow[r] & \operatorname{Pic}^0(C)[m] \arrow[r] & \operatorname{Jac}(C)(\mathbb{Q})[m] \arrow[r] & H^2(\operatorname{Spec}(\mathbb{Q}), \mathbf{G}_{\mathrm{m}}) \end{tikzcd} \tag{2.4}$$

where the vertical maps ρ_i are obtained by restriction to the generic fiber. We claim that ρ_2 is an isomorphism. Indeed, $\operatorname{Pic}^0_{\mathcal{C}/Z}$ being isomorphic to $\mathcal{J}^0$, this map can be identified with

$$\mathcal{J}^0(Z)[m] \subseteq \mathcal{J}(Z)[m] \simeq \operatorname{Jac}(C)(\mathbb{Q})[m],$$

and the inclusion is in fact an equality because $t_p(\mathrm{Jac}(C))$ is coprime to m for all $p \in Z$. Moreover, the map ρ_3 is injective according to [11, Prop. 2.1]. It follows from the snake lemma applied to the diagram (2.4) that ρ_1 is an isomorphism.

By the same arguments as in the proof of Corollary 2.8, it follows that C, m and S satisfy the hypotheses of Theorem 2.4. □

Remark 2.12. If C has genus $g \geq 2$, then, according to Proposition–Definition 2.10, the set S of Corollary 2.11 is contained in the set of primes of bad reduction of $\mathrm{Jac}(C)$. This set is in general strictly smaller than the set of primes of bad reduction of C, even in the case when C has a rational point. This is the main interest of Corollary 2.11 compared to Corollary 2.8.

Remark 2.13. If C has genus one, then $\mathrm{Jac}(C)$ is an elliptic curve, that we denote by E. Moreover, we have

$$\mathrm{Pic}^0(C) \subseteq E(\mathbb{Q}) \simeq \mathrm{Pic}^0(E),$$

where the isomorphism follows from auto-duality of elliptic curves. Hence, if we are interested in building number fields with a large class group, we may apply Corollary 2.11 to E instead of C, which permits a possibly smaller S (see also Corollary 3.1).

Remark 2.14. By definition of $\mathrm{ind}(C)$, it is possible to find number fields $K_1, \dots, K_n$ together with points $P_i \in C(K_i)$ such that the gcd of the degrees $[K_i : \mathbb{Q}]$ is $\mathrm{ind}(C)$. Hence, according to [3, Section 9.1, Prop. 11], the cokernel of the map $\mathrm{Pic}^0(C) \to \mathrm{Jac}(C)(\mathbb{Q})$ is killed by $\mathrm{ind}(C)$. Therefore, if we let

$$m' = \frac{m}{\gcd(m, \mathrm{ind}(C))},$$

then we have

$$\mathrm{rk}_{m'} \mathrm{Pic}^0(C)_{\mathrm{tors}} \geq \mathrm{rk}_m \mathrm{Jac}(C)(\mathbb{Q})_{\mathrm{tors}}$$

and equality holds when $\gcd(m, \mathrm{ind}(C)) = 1$.

3. Applications

3.1. Curves. In this section, we consider some applications and further refinements of Corollary 2.11. Note that if we fix the degree of ϕ, the quantity $\mathrm{rk}\,\mathcal{O}^\times_{\mathbb{Q}(P_t),S} - \#S$ that appears in Corollary 2.11 is minimized if every prime in S is totally ramified in $\mathbb{Q}(P_t)$ and $\mathbb{Q}(P_t)$ has the maximum possible number of complex places for a number field of degree ϕ. In this case, we have the equalities

$$\mathrm{rk}\,\mathcal{O}^\times_{\mathbb{Q}(P_t),S} - \#S = \mathrm{rk}\,\mathcal{O}^\times_{\mathbb{Q}(P_t)} = \left[\frac{\deg\phi - 1}{2}\right].$$

By choosing appropriate maps ϕ in Corollary 2.11, we show that this advantageous situation can be achieved for hyperelliptic or, more generally, superelliptic curves.

Corollary 3.1. *Let C be (a smooth projective model of) the plane curve defined by*

$$y^n = f(x), \quad f(x) \in \mathbb{Q}[x], \quad n > 1,$$

with $(\deg f, n) = 1$. *Let* $m > 1$ *be an integer. Then there exist* $\gg X^{\frac{1}{(n-1)\deg f}}/\log X$ *number fields* k *of degree* $[k:\mathbb{Q}] = n$ *with discriminant* d_k, $|d_k| < X$, *and*

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - \left[\frac{n-1}{2}\right].$$

Proof. Let $r = \deg f$ and let $f(x) = \sum_{i=0}^{r} a_i x^i$. By rescaling x and y we can assume that $a_i \in \mathbb{Z}$ for all i and, using $(r,n) = 1$, that $a_r = -1$. Let S be the set of primes from Corollary 2.11. Let $M = \prod_{p\in S} p$. Let ϕ be the rational function on C defined by $\phi = x - \frac{1}{M}$. For $t \in \mathbb{Z}$, let $P_t = \phi^{-1}(t)$. Then $\mathbb{Q}(P_t) \cong \mathbb{Q}(\sqrt[n]{f(\frac{tM+1}{M})})$. Let $p \in S$. Since $a_r = -1$, we have that $v_p(f(\frac{tM+1}{M})) = -r$. Since $(r,n) = 1$, this implies that p totally ramifies in $\mathbb{Q}(P_t)$. Note also that $[\mathbb{Q}(P_t):\mathbb{Q}] = n$. So every prime in S is totally ramified in $\mathbb{Q}(P_t)$. The condition $(r,n) = 1$ also implies that $y^n = f(x)$ has a rational point at infinity. Then Corollary 2.11 applied to ϕ and C implies that for all but $O(\sqrt{N})$ values $t = 1,\ldots,N$, we have $[\mathbb{Q}(P_t):\mathbb{Q}] = n$ and

$$\operatorname{rk}_m \operatorname{Cl}(\mathbb{Q}(P_t)) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - \operatorname{rk} \mathcal{O}^*_{\mathbb{Q}(P_t)}.$$

Since $a_r = -1$, for $t \gg 0$, $f\left(\frac{tM+1}{M}\right)$ is negative. It follows that for $t \gg 0$, $\mathbb{Q}(P_t)$ has exactly one real place if n is odd and no real places if n is even. So by Dirichlet's theorem, $\operatorname{rk} \mathcal{O}^*_{\mathbb{Q}(P_t)} = [\frac{n-1}{2}]$ for $t \gg 0$. It follows from Theorem 2.2 that there are $\gg N/\log N$ distinct number fields in the set $\{\mathbb{Q}(P_1),\ldots,\mathbb{Q}(P_N)\}$. An easy calculation shows that $|d_{\mathbb{Q}(P_t)}| = O(t^{(n-1)t})$. Combining the above statements then gives the corollary. □

Of particular interest is the case where C is a hyperelliptic curve.

Corollary 3.2. *Let* C *be a smooth projective hyperelliptic curve over* $\mathbb{Q}$ *with a rational Weierstrass point. Let* g *denote the genus of* C. *Let* $m > 1$ *be an integer. Then there exist* $\gg X^{\frac{1}{2g+1}}/\log X$ *imaginary quadratic number fields* k *with*

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}}, \quad |d_k| < X,$$

and $\gg X^{\frac{1}{2g+1}}/\log X$ *real quadratic number fields* k *with*

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - 1, \quad d_k < X.$$

Proof. Since C has a rational Weierstrass point, C is birational to a plane curve defined by $y^2 = f(x)$, for some $f(x) \in \mathbb{Q}[x]$ with $\deg f = 2g+1$. The statement on imaginary quadratic fields now follows from the proof of Corollary 3.1. The statement for real quadratic fields follows similarly from the proof of Corollary 3.1 using points P_t, $t < 0$, with the extra -1 term coming from the rank one unit group of a real quadratic field. □

A classical result of Nagell [19, 20] states that for any positive integer m there exist infinitely many imaginary quadratic number fields with an element of order m in the ideal class group. Weinberger [22] and Yamamoto [23], independently, extended Nagell's result to real quadratic fields and Yamamoto [23] improved Nagell's result for imaginary quadratic fields to class groups of m-rank two. As a sample application of Corollary 3.2, we show that it easily implies (largely known) quantitative versions of the results of Weinberger [22] and Yamamoto [23].

Lemma 3.3. *Let $b, c \in \mathbb{Q}$, with $c \neq 0$, $b^2 \neq 4c^2$, and let $m > 1$ be an integer. Let C be the (smooth projective model of the) hyperelliptic curve $y^2 = x^{2m} + bx^m + c^2$. Then $\operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}} \geq 2$.*

Proof. The curve C has two $\mathbb{Q}$-rational points at infinity that we will denote by ∞ and $\overline{\infty}$. Let $P, \bar{P} \in C$ be the two points with coordinates $P = (0, c)$ and $\overline{P} = (0, -c)$. Then, after possibly switching ∞ and $\overline{\infty}$, we have

$$\begin{aligned}\operatorname{div}(y - x^m - c) &= m(P - \infty),\\ \operatorname{div}(y - x^m + c) &= m(\overline{P} - \infty).\end{aligned}$$

Let $i, j \in \{0, \ldots, m-1\}$ with $i \geq j$, $i > 0$. Then, since $P + \overline{P} \sim \infty + \overline{\infty}$,

$$\begin{aligned} i(P - \infty) + j(\overline{P} - \infty) &\sim (i - j)P + j(P + \overline{P}) - (i + j)\infty \\ &\sim (i - j)P + j\overline{\infty} - i\infty. \end{aligned}$$

Since the genus of C is $m - 1$ and ∞ is not a Weierstrass point of C, we have $l(i\infty) = 1$ as $i \leq m - 1$. Then $i(P - \infty) + j(\overline{P} - \infty)$ is not a principal divisor and it follows that the divisors classes of $P - \infty$ and $\overline{P} - \infty$ generate a subgroup $(\mathbb{Z}/m)^2$ in $\operatorname{Jac}(C)(\mathbb{Q})$. □

Note that there are hyperelliptic curves as in Lemma 3.3 with a rational Weierstrass point (e.g., curves with $b = -1 - c^2$). Then from Corollary 3.2 we immediately obtain the following result.

Corollary 3.4. *Let $m > 1$ be an integer. There exist $\gg X^{\frac{1}{2m-1}} / \log X$ imaginary quadratic number fields k with $|d_k| < X$ and $\operatorname{rk}_m \operatorname{Cl}(k) \geq 2$ and $\gg X^{\frac{1}{2m-1}} / \log X$ real quadratic number fields k with $d_k < X$ and $\operatorname{rk}_m \operatorname{Cl}(k) \geq 1$.*

If m is odd, then Byeon [4] and Yu [24] have proved, for imaginary and real quadratic fields, respectively, the better lower bound of $\gg X^{1/m - \epsilon}$. If m is even, in the real quadratic case a lower bound of $\gg X^{1/m}$ was proved by Chakraborty *et al.* [5]. The imaginary quadratic case of Corollary 3.4 with m even appears to be new.

Using the results presented here, it is in fact possible to derive quantitative versions of many of the known results on constructing number fields with class groups of large rank. This aspect of the results will be pursued in a future paper.

Corollary 3.2 raises the following natural question.

Question 3.5. *Let p be an odd prime. Do there exist hyperelliptic curves C over $\mathbb{Q}$ with $\operatorname{rk}_p \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}}$ arbitrarily large?*

More generally, one can ask whether there exist curves C over $\mathbb{Q}$ of gonality n with $\operatorname{rk}_p \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}}$ arbitrarily large, where p is a prime not dividing n (in the case $p|n$, a positive answer is easily obtained from curves of the form $y^n = f(x)$, where $f(x)$ splits over $\mathbb{Q}$). This question does not appear to have been extensively investigated. Previous papers studying the problem of constructing Jacobians of curves with large rational torsion subgroups have primarily focused on either curves of low genus (e.g., [12]), or on producing a rational torsion point of large order in the Jacobian of a curve of genus g, for every genus g (e.g., [10]).

3.2. Torsion line bundles on arithmetic varieties. We consider here the question formulated in [1], namely:

Question 3.6. *Let $\mathcal{L}$ be a nontrivial line bundle over an arithmetic variety $\mathcal{X}$. Is it possible to find a section P of $\mathcal{X}$ over some number field such that the pull-back of $\mathcal{L}$ by this section is also nontrivial?*

Here "arithmetic variety" means a normal scheme whose structural morphism to $\mathrm{Spec}(\mathbb{Z})$ is proper and flat. Let us note that, under these assumptions, the generic fiber of $\mathcal{X}$ need not be geometrically integral.

Corollary 3.7. *Let $\mathcal{X}$ be an arithmetic variety whose generic fiber X is smooth and geometrically integral. Let S be the set of places of bad reduction of $\mathcal{X}$, and let $\mathcal{X}_S := \mathcal{X} \times_{\mathbb{Z}} \mathrm{Spec}(\mathbb{Z}_S)$. Then, given an integer $m > 1$, there exists an infinity of number fields K with a point $P \in X(K)$ such that the image of the restriction map*

$$P^* : \mathrm{Pic}(\mathcal{X}_S)[m] \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[m]$$

satisfies

$$\mathrm{rk}_m \mathrm{Im}(P^*) \geq \mathrm{rk}_m \mathrm{Pic}(\mathcal{X}_S)[m] + \#S - \mathrm{rk}\, \mathcal{O}_{K,S}^{\times}.$$

If X is the normalization of a plane curve defined by

$$y^n = f(x)$$

with $(\deg(f), n) = 1$, then the same holds with

$$\mathrm{rk}_m \mathrm{Im}(P^*) \geq \mathrm{rk}_m \mathrm{Pic}(\mathcal{X}_S)[m] - \left[\frac{n-1}{2}\right].$$

Proof. Let us note here that our S is *a priori* larger than the set of places of bad reduction of X, but the arguments in the proof of Lemma 2.7 still hold, and give us the equality $\mathrm{Pic}(\mathcal{X}_S) = \mathrm{Pic}(X)$. Then Corollary 2.8 can be applied with the same set S, and the first statement can be extracted from the proof of Theorem 2.4. The second statement follows from the proof of Corollary 3.1. □

Corollary 3.8. *Let $\mathcal{X}$ be an arithmetic variety whose generic fiber is a smooth hyperelliptic curve with a rational Weierstrass point. Let $\mathcal{L}$ be a torsion line bundle over $\mathcal{X}$ whose generic fiber is nontrivial. Then there exists an infinity of imaginary quadratic fields K with a section P of $\mathcal{X}$ over $\mathcal{O}_K$ such that the pull-back $P^*\mathcal{L}$ is nontrivial.*

Proof. Obviously, it suffices to prove the result when $\mathcal{L}$ has prime order p. In this case, the equality $\mathrm{rk}_p \mathrm{Im}(P^*) = \mathrm{rk}_p \mathrm{Pic}(\mathcal{X}_S)[p]$ implies that $\ker(P^*) = 0$. Therefore, the second statement in Corollary 3.7 implies that, for an infinity of imaginary quadratic fields K, the map

$$P^* : \mathrm{Pic}(\mathcal{X}_S)[p] \longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S})[p]$$

is injective. On the other hand, we know that $\mathcal{L}$ has a nontrivial generic fiber, so the restriction of $\mathcal{L}$ to $\mathcal{X}_S$ is also nontrivial. This proves the result. □

Acknowledgments

We thank Qing Liu for inspiring conversations, and Cédric Pépin for technical advice about line bundles on integral models.

References

[1] A. Agboola and G. Pappas, *Line bundles, rational points and ideal classes*, Math. Res. Lett. **7**(5–6) (2000), 709–717.

[2] S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math. **98**(3) (1999), 275–293.

[3] S. Bosch, W. Lütkebohmert and M. Raynaud, Néron models, Vol. 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, Springer-Verlag, Berlin (1990).

[4] D. Byeon, *Imaginary quadratic fields with noncyclic ideal class groups*, Ramanujan J. **11**(2) (2006), 159–163.

[5] K. Chakraborty, F. Luca and A. Mukhopadhyay, *Exponents of class groups of real quadratic fields*, Int. J. Number Theory **4**(4) (2008), 597–611.

[6] S.D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3) **43**(2) (1981), 227–250.

[7] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[8] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Superior. Pisa Cl. Sci. (4) **21**(3) (1994), 421–443.

[9] ———, *Fields containing values of algebraic functions. II. (On a conjecture of Schinzel)*, Acta Arith. **72**(3) (1995), 201–210.

[10] E.V. Flynn, *Sequences of rational torsions on abelian varieties*, Invent. Math. **106**(2) (1991), 433–442.

[11] A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, in Dix Exposés sur la Cohomologie des Schémas, 88–188, North-Holland, Amsterdam (1968).

[12] E.W. Howe, F. Leprévost and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12**(3) (2000), 315–364.

[13] A. Levin, *Ideal class groups, Hilbert's irreducibility theorem, and integral points of bounded degree on curves*, J. Théor. Nombres Bordeaux **19**(2) (2007), 485–499.

[14] Q. Liu, Algebraic geometry and arithmetic curves, Vol. 6 of *Oxford Graduate Texts in Mathematics*, Oxford University Press, Oxford (2002). Translated from the French by Reinie Erné, Oxford Science Publications.

[15] J.-F. Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, in Seminar on number theory, 1979–1980 (French), Exp. No. 15, 18, University of Bordeaux I, Talence (1980).

[16] ———, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35.

[17] ———, *Groupes de classes d'ideaux non cycliques de corps de nombres*, in Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Vol. 38 of *Progr. Math.*, 189–200, Birkhäuser Boston, Boston, MA (1983).

[18] ———, *Corps quadratiques dont le* 5*-rang du groupe des classes est* ≥ 3, C. R. Acad. Sci. Paris Sér. I Math. **315**(4) (1992), 371–374.

[19] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.

[20] ———, Collected papers of Trygve Nagell. Vol. 1, Vol. 121 of *Queen's Papers in Pure and Applied Mathematics*, Queen's University, Kingston, ON (2002).

[21] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 3rd edn. (1997).

[22] P.J. Weinberger, *Real quadratic fields with class numbers divisible by* n, J. Number Theory **5**(3) (1973), 237–241.

[23] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

[24] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory **97**(1) (2002), 35–44.

Institut de Mathématiques de Bordeaux, CNRS UMR 5251, Université Bordeaux 1, 351, cours de la Libération, F-33400 Talence, France
E-mail address: jean.gillibert@math.u-bordeaux1.fr

Department of Mathematics, Michigan State University, 619 Red Cedar Road, East Lansing, MI 48824, USA
E-mail address: adlevin@math.msu.edu