Chevalley-Weil Theorem and Subgroups of Class Groups

Yuri Bilu Jean Gillibert

September 2017

Abstract

We prove, under some mild hypothesis, that an étale cover of curves defined over a number field has infinitely many specializations into an everywhere unramified extension of number fields. This constitutes an "absolute" version of the Chevalley-Weil theorem. Using this result, we are able to generalise the techniques of Mestre, Levin and the second author for constructing and counting number fields with large class group.

Contents

1 Introduction

In this article, "curve" always stands for a "smooth geometrically irreducible projective curve".

Let H be a finite abelian group, K a number field and $d > 1$ an integer. The following conjecture is widely believed to be true.

Conjecture 1.1. *The field K has infinitely many extensions L of degree $[L : K] = d$ such that H is a subgroup of the class group* $\mathrm{Cl}(L)$.

This conjecture is known to be true in many special cases, for instance, when $K = \mathbb{Q}$ and H is a cyclic group or a product of two cyclic groups, see [1]. However, the general case remains widely open. We refer to [6, 14, 17] for the history of the problem and further references.

It is clear that one may restrict to the case when $H = (\mathbb{Z}/n)^r$, the product of r cyclic groups of order n, where n and r are positive integers. Denote by $\mathrm{rk}_n M$ the n-rank of a finite abelian group M; that is, the maximal integer r such that $(\mathbb{Z}/n)^r \leq M$. Then Conjecture 1.1 is equivalent to the following.

Conjecture 1.2. *Let $n > 1$ be an integer. Then* $\mathrm{rk}_n \mathrm{Cl}(L)$ *is unbounded when L runs through the extensions of K of degree $[L : K] = d$.*

When $n = d$, and more generally when n divides d, this conjecture follows easily from Class Field Theory. On the other hand, when n and d are coprime, there is not a single case where Conjecture 1.2 is known to hold. For example, given $n > 1$, there exists infinitely many imaginary quadratic fields such that $\mathrm{rk}_n \mathrm{Cl}(L)$ is at least 2. For $n \geq 7$ this is currently the best known result on n-ranks of quadratic fields.

All partial results towards this conjecture were obtained by the same strategy: one considers a suitable curve $\mathcal{C}$ over K admitting a finite K-morphism $\mathcal{C} \to \mathbb{P}^1$ of degree d. Hilbert's Irreducibility Theorem implies abundance of $P \in \mathcal{C}(\bar{K})$ such that $[K(P) : K] = d$. When $\mathcal{C}$ has many independent étale Galois covers with cyclic group of order n, "most" of the fields $K(P)$ have a class group with large n-rank.

In particular, systematizing and generalizing the previous work, most notably the results of [17], the following theorem was proved in [14] in the case when $K = \mathbb{Q}$ and $\mathcal{C}$ is a superelliptic curve defined by a "nice equation" (see Corollary 3.1 of [14]).

Theorem 1.3. *Let $\mathcal{C}$ be a curve over a number field K, let $J(\mathcal{C})$ be the Jacobian of $\mathcal{C}$, and let $n > 1$ be an integer. Assume that $\mathcal{C}$ admits a finite K-morphism $\mathcal{C} \to \mathbb{P}^1$ of degree d, totally ramified over some point belonging to $\mathbb{P}^1(K)$. Then there exist infinitely many (isomorphism classes of) number fields L with $[L : K] = d$ such that*

$$\mathrm{rk}_n \mathrm{Cl}(L) \geq \mathrm{rk}_n J(\mathcal{C})(K)_{\mathrm{tors}} - \mathrm{rk}_{\mathbb{Z}} \mathcal{O}_L^{\times} + \mathrm{rk}_{\mathbb{Z}} \mathcal{O}_K^{\times} + \mathrm{rk}_n \mathrm{Cl}(K). \tag{1}$$

The proof of this theorem is based on Kummer theory and can be found in Subsection 4.3. The last sentence can be made quantitative; see Theorem 1.5 below.

While Theorem 1.3 is quite general, its applicability in concrete cases is impaired by the presence of the negative term $-\mathrm{rk}_{\mathbb{Z}} \mathcal{O}_L^{\times}$ on the right: the rank of the unit group of the field L is quite large, especially if $K \neq \mathbb{Q}$.

The principal result of the present article is the following theorem, where this deficiency is avoided. Denote by $\mathrm{rk}_{\mu_n} J(\mathcal{C})$ the maximal integer r such that $J(\mathcal{C})$ has a $\mathrm{Gal}(\bar{K}/K)$-submodule isomorphic to μ_n^r. In particular, if $\mu_n \subset K$ then $\mathrm{rk}_{\mu_n} J(\mathcal{C}) = \mathrm{rk}_n J(\mathcal{C})$.

Theorem 1.4. *In the set-up of Theorem 1.3, there exist infinitely many number fields L with $[L : K] = d$ such that*

$$\mathrm{rk}_n \mathrm{Cl}(L) \geq \mathrm{rk}_{\mu_n} J(\mathcal{C}) + \mathrm{rk}_n \mathrm{Cl}(K). \tag{2}$$

The proof is based on Class Field Theory (see Subsection 4.3). It can be seen as a generalization of the construction of Mestre [18]. In Section 5, we revisit Mestre's result in the light of Theorem 1.4.

In both Theorems 1.3 and 1.4 the "infinitely many" can be made quantitative. Given a number field extension L/K, we define

$$\mathcal{D}(L/K) = \left|\mathcal{N}_{K/\mathbb{Q}} \Delta(L/K)\right|^{1/[K:\mathbb{Q}]},$$

where $\Delta(L/K)$ is the discriminant of L over K.

Theorem 1.5. *Let $t \in K(\mathcal{C})$ be the rational function defining the K-morphism $\mathcal{C} \to \mathbb{P}^1$ appearing in both Theorems 1.3 and 1.4. Assume that there exists a rational function $x \in K(\mathcal{C})$ of degree m such that $K(\mathcal{C}) = K(t, x)$. Then, for sufficiently large positive X, in both these theorems the number of (isomorphism classes of) the fields L satisfying (1) or (2), respectively, and such that $\mathcal{D}(L/K) \leq X$ is at least $cX^{\ell/(2m(d-1))}/\log X$. Here $\ell = [K : \mathbb{Q}]$ and $c > 0$ depends on $\mathcal{C}$, t, x and K.*

Remark 1.6. Assuming that $\mathcal{C}$ has a K-rational point (which is the case in both Theorems 1.3 and 1.4), the Theorem of Riemann-Roch implies that there is a function $x \in K(\mathcal{C})$ of degree $m \leq 2\mathbf{g}(\mathcal{C}) + 1$ and such that $K(\mathcal{C}) = K(t, x)$. In concrete examples a suitable x of much smaller degree m can often be found.

We believe that Theorem 1.4 has more potential, but we have few examples up to now. Here is one application.

Theorem 1.7. *Let $p \geq 3$ be a prime, and let d be an integer such that $2 \leq d \leq p-1$. Let K be a number field containing the p-th roots of unity. Then there exist infinitely many (non-isomorphic) extensions L/K with $[L : K] = d$ such that*

$$\mathrm{rk}_p \mathrm{Cl}(L) \geq 3 + \mathrm{rk}_p \mathrm{Cl}(K).$$

More precisely, for sufficiently large positive X the number of such L with $\mathcal{D}(L/K) \leq X$ is at least $cX^{(p-1)/2p(d-1)}/\log X$, where $c = c(K, p) > 0$.

For instance, the cyclotomic field $\mathbb{Q}(\zeta_p)$ has infinitely many quadratic extensions $L/\mathbb{Q}(\zeta_p)$ such that $\mathrm{rk}_p \mathrm{Cl}(L) \geq 3$.

Moreover, we know that there exist infinitely many irregular primes, for which $\mathrm{rk}_p \mathrm{Cl}(\mathbb{Q}(\zeta_p)) \geq 1$. If we take $p = 37$ for example, our result says that there exist infinitely many quadratic extensions $L/\mathbb{Q}(\zeta_{37})$ such that $\mathrm{rk}_{37} \mathrm{Cl}(L) \geq 4$.

Our main tool in proving Theorem 1.4 is the Chevalley-Weil theorem. Recall that the (one-dimensional) Chevalley-Weil theorem asserts the following.

Theorem 1.8. *Let $\psi : \widetilde{\mathcal{C}} \to \mathcal{C}$ be an étale morphism of curves over a number field K. Then there exists a finite set S of places of K with the following property: for every $P \in \mathcal{C}(\bar{K})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{K})$ such that $\psi(\widetilde{P}) = P$, the number field extension $K(\widetilde{P})/K(P)$ is unramified at all finite places except perhaps those above S.*

See [19, Section 4.2] for a quick proof and [7] for several quantitative versions.

Following an idea of Mestre [18] (see "Remarque" on p. 372), we are going to show that, under certain assumptions, for "many" such P and $\widetilde{P}$ the extension $K(\widetilde{P})/K(P)$ is unramified everywhere, that is, at all places including the archimedean ones.

If X is a finite set of points on a K-variety, we denote by $K(X)$ the smallest field over which all points of X are rational. In particular, if we start from some point $P \in \mathcal{C}(K)$, then $K(\psi^{-1}(P))$ is the compositum of fields $K(\widetilde{P})$ where $\widetilde{P}$ runs through all points in $\widetilde{\mathcal{C}}(\bar{K})$ such that $\psi(\widetilde{P}) = P$.

We prove the following.

Theorem 1.9 (Absolute Chevalley-Weil Theorem)**.** *In the set-up of Theorem 1.8, assume that there exists a point $A \in \mathcal{C}(K)$ such that $K(\psi^{-1}(A)) = K$. Then there exist infinitely many points $P \in \mathcal{C}(\bar{K})$ such that the extension $K(\psi^{-1}(P))/K(P)$ is unramified everywhere, that is, at all places including the archimedean ones.*

More precisely, let $t \in K(\mathcal{C})$ be a rational function having A as its single zero[1]*, and let S be the set of places from Theorem 1.8. Then there exists $\varepsilon > 0$ such that, for every $P \in \mathcal{C}(\bar{K})$ satisfying $t(P) \in K$ and $|t(P)|_v < \varepsilon$ for all $v \in S \cup M_K^\infty$, the extension $K(\psi^{-1}(P))/K(P)$ is unramified everywhere.*

[1] Existence of such t easily follows from the Riemann-Roch Theorem.

In the statement above, M_K^∞ denotes the set of archimedean places of K. We refer to Section 3 for further notation.

Remark 1.10. 1. In fact, we prove a stronger statement, namely that primes above S are totally split in the extension $K(\psi^{-1}(P))/K(P)$.

2. The points P whose existence is ensured by Theorem 1.9 belong to the inverse image of $\mathbb{P}^1(K)$ by t, in particular they satisfy $[K(P) : K] \leq \deg(t)$.

3. It is certainly possible to prove a similar theorem in the case when the curves $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ are replaced by smooth projective varieties of arbitrary dimension.

Plan of the article In Section 2 we prove the Absolute Chevalley-Weil Theorem.

In Section 3 we establish a counting result for number fields in fibers of a morphism $\mathcal{C} \to \mathbb{P}^1$, following, mainly, Dvornicich and Zannier. This will be our main tool in obtaining the quantitative results like Theorem 1.5.

In Section 4 we study specializations of torsors over algebraic curves, and prove Theorems 1.3, 1.4 and 1.5.

In the final Section 5 we obtain some applications of our general results; in particular, we prove Theorem 1.7.

Acknowledgments A substantial part of this article was written when Yuri Bilu was visiting the Max-Planck-Institut für Mathematik in Bonn. He thanks this institute for the financial support and stimulating working conditions.

We thank Qing Liu for many stimulating discussions. We thank Lev Birbrair and Martin Widmer for helpful suggestions. We also thank Ted Chinburg for sharing his valuable comments. Finally, we thank the anonymous referee for the encouraging report and detecting many inaccuracies, some quite deeply hidden.

2 The Absolute Chevalley-Weil Theorem

In this section we prove Theorem 1.9. The idea of the proof is as follows: we take S to be the set whose existence is ensured by Theorem 1.8. Then, using a variant of Hensel's Lemma, we prove that, if P is v-adically close enough to A with respect to some place $v \in S$, then $K(\psi^{-1}(P))/K(P)$ is unramified at v.

In Subsection 2.1 we collect the local results we need. Theorem 1.9 is proved in Subsection 2.2.

2.1 Local Lemmas

In this subsection K is a complete field $(K, |\cdot|)$ (it might be archimedean). The absolute value has a unique extension to the algebraic closure $\bar{K}$, that we denote also $|\cdot|$ by abuse of notation.

Lemma 2.1 ("Separable Hensel's lemma")**.** *Let $f(X) \in K[X]$ be a monic polynomial of degree n having exactly n distinct roots in $\bar{K}$. Then there exists $\varepsilon > 0$ such that the following*

holds : for every monic polynomial $f^*(X) \in K[X]$ of degree n in the ε-neighbourhood of f, one has an isomorphism

$$K[X]/f^*(X) \simeq K[X]/f(X).$$

In other words, one may write $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ and $f^*(X) = \prod(X - \alpha_i^*)$ such that $K(\alpha_i) = K(\alpha_i^*)$ for all i.

(The ε-neighbourhood is considered with respect to the ℓ_∞-norm.)

Proof. In the non-archimedean case the proof can be found in [8, Theorem 1]. In the archimedean case this follows from the well-known fact (see, for instance, [2, 1.5.9]) that on the space of monic separable real polynomials of degree n the function "number of real roots" is locally constant. □

Now let $\mathcal{C}$ be a smooth projective K-curve and let $t \in K(\mathcal{C})$ be a rational function on $\mathcal{C}$ having $A \in \mathcal{C}(K)$ as its single zero. We denote by N the order of this zero, which is none other than the degree of $t : \mathcal{C} \to \mathbb{P}^1$.

Lemma 2.2 ("Puiseux expansion")**.** *Let $x \in \bar{K}(\mathcal{C})$ be a $\bar{K}$-rational function on $\mathcal{C}$ not having a pole at A. Then there exists $\varepsilon > 0$ such that for every $P \in \mathcal{C}(\bar{K})$ with $|t(P)| < \varepsilon$ we have*

$$x(P) = x(A) + O(|t(P)|^{1/N}),$$

where the implicit constant may depend on $\mathcal{C}$, A, t and x, but not on P.

Proof. The lemma is an easy consequence of the following formally weaker statement.

Claim Under the same hypothesis, there exists $\varepsilon > 0$ such that the function $P \mapsto |x(P)|$ is bounded on the set $P \in \mathcal{C}(\bar{K})$ satisfying $|t(P)| < \varepsilon$.

The claim is trivial in the case $x \in \bar{K}(t)$. Indeed, if $x = a(t)/b(t)$ with $a(T), b(T) \in \bar{K}[T]$ coprime polynomials, then $b(0) \neq 0$ because x has no pole at A. Hence there exits $\varepsilon > 0$ such that the set $\{|b(\alpha)| : \alpha \in \bar{K}, |\alpha| < \varepsilon\}$ is separated away from 0, which immediately implies the claim.

To prove the claim in general, recall the following well-known fact: given a monic polynomial $f(X) \in \bar{K}[X]$ whose coefficients in absolute value are bounded by some $C > 0$, the roots of f are bounded in absolute value by $2C$ (or even by C in the non-archimedean case); see, for instance, [5, Proposition 3.2]. In fact, we do not need such a precise statement: it suffices to know that when f runs over a set of monic polynomials with bounded coefficients, its roots stay bounded as well.

Now let $X^m + u_{m-1}X^{m-1} + \cdots + u_0 \in \bar{K}(t)[X]$ be the minimal polynomial of x over the field $\bar{K}(t)$. Since x has no pole at A, none of the coefficients $u_0, \ldots, u_{m-1}$ does. Since they belong to $\bar{K}(t)$, the claim holds true for them. Since $x(P)$ is a root of the polynomial $X^m + u_{m-1}(P)X^{m-1} + \cdots + u_0(P)$, the validity of the claim for x follows from that for $u_0, \ldots, u_{m-1}$ due to the property of polynomials quoted in the previous paragraph. This proves our claim.

The lemma follows immediately by applying the claim to the function $(x - x(A))^N/t$. □

Lemma 2.3 ("Main Lemma"). *Let $\mathcal{C}$, A, t be as above, and let $\psi : \widetilde{\mathcal{C}} \to \mathcal{C}$ be a finite morphism of curves over K unramified above A. Then there exists $\varepsilon > 0$ such that*

$$\psi^{-1}(P) \simeq \psi^{-1}(A) \otimes_K K(P)$$

for every $P \in \mathcal{C}(\bar{K})$ satisfying $|t(P)| < \varepsilon$.

Proof. Let $U_0 = \mathrm{Spec}(R_0)$ be an affine open subset of $\mathcal{C}$ containing A. We note that R_0 is a Dedekind ring with fraction field $K(\mathcal{C})$. Moreover, $V_0 := \psi^{-1}(U_0) = \mathrm{Spec}(\widetilde{R_0})$, where $\widetilde{R_0}$ is the normalization of R_0 in $K(\widetilde{\mathcal{C}})$.

If Q is a closed point of V_0, we denote by $\mathfrak{M}_Q$ the corresponding maximal ideal of $\widetilde{R_0}$. In particular, the residue field $\widetilde{R_0}/\mathfrak{M}_Q$ is the field $K(Q)$.

The map ψ being unramified above A, we have:

$$\sum_{Q \in \psi^{-1}(A)} [K(Q) : K] = \deg(\psi)$$

where the sum runs through closed points of $\psi^{-1}(A)$.

Let us choose in each $K(Q)$ an element $\beta_Q \in K(Q)$ such that the l.c.m. of their minimal polynomials over K has degree $\deg(\psi)$. This can be acheived according to the equality above.

According to the Chinese remainder theorem, the map

$$\widetilde{R_0} \to \prod_{Q \in \psi^{-1}(A)} K(Q)$$

is surjective. Therefore, there exists a function $y \in \widetilde{R_0}$ such that $y \equiv \beta_Q \pmod{\mathfrak{M}_Q}$ for all Q. This means that y takes the value β_Q at Q.

We claim that $K(\widetilde{\mathcal{C}}) = K(\mathcal{C})(y)$. Let us observe first that y belongs to $\widetilde{R_0}$ which is a finite R_0-algebra, hence y is integral over R_0. We let $f \in R_0[Y]$ be the (monic) minimal polynomial of y over R_0.

For any closed point $P \in U_0$, we let f_P be the image of f by the reduction map $R_0[Y] \to K(P)[Y]$. In classical language, f_P is the polynomial obtained by specializing the coefficients of f at the point P.

By definition, $f(y) = 0$ holds true in the ring $\widetilde{R_0}$, therefore it holds true after reduction modulo any ideal of $\widetilde{R_0}$. By construction of y, we know that $y \equiv \beta_Q \pmod{\mathfrak{M}_Q}$ for all $Q \in \psi^{-1}(A)$. Therefore, $f_A(\beta_Q) = 0$ holds true for all $Q \in \psi^{-1}(A)$. In other words, the values of y at points from $\psi^{-1}(A)$ are roots of f_A.

It follows that the l.c.m. of the minimal polynomials of the β_Q divides f_A, hence f_A (and therefore f) has degree at least equal to $\deg(\psi)$. But we already know that the degree of f is at most $[K(\widetilde{\mathcal{C}}) : K(\mathcal{C})]$, because $K(\mathcal{C})(y)$ is a subfield of $K(\widetilde{\mathcal{C}})$. Hence the equality holds, and y generates $K(\widetilde{\mathcal{C}})$ over $K(\mathcal{C})$.

We can resume the situation by the following commutative diagram

$$\begin{array}{ccc} V_0 = \psi^{-1}(U_0) & \xrightarrow{\psi} & U_0 \\ \downarrow & & \| \\ \mathrm{Spec}(R_0[Y]/f) & \longrightarrow & \mathrm{Spec}(R_0) \end{array}$$

in which the vertical map on the left is generically an isomorphism. In fact, the affine curve V_0 being normal, it is equal to the normalization of $\mathrm{Spec}(R_0[Y]/f)$.

Let $\mathrm{Disc}(f)$ be the discriminant of the polynomial f, and let $R := R_0[\mathrm{Disc}(f)^{-1}]$. Thus, $U := \mathrm{Spec}(R)$ is the largest open subset of U_0 over which $\mathrm{Disc}(f)$ is invertible. We note that U contains A, because f_A has no double root by construction. By standard algebra, $R[Y]/f$ is an étale R-algebra. The ring R being regular, it follows that $R[Y]/f$ is regular, hence normal. So, the map $\psi^{-1}(U) \to \mathrm{Spec}(R[Y]/f)$ is an isomorphism.

Therefore, given any $P \in U(\bar{K})$, we have

$$\psi^{-1}(P) = \mathrm{Spec}(K(P)[Y]/f_P).$$

According to Lemma 2.2, when $|t(P)|$ is sufficiently small, the coefficients of f_P are sufficiently close to the coefficients of f_A. Hence, according to Lemma 2.1, if $|t(P)|$ is sufficiently small, then

$$K(P)[Y]/f_P \simeq K(P)[Y]/f_A \simeq (K[Y]/f_A) \otimes_K K(P)$$

i.e.

$$\psi^{-1}(P) \simeq \psi^{-1}(A) \otimes_K K(P)$$

hence the result. □

Remark 2.4. The following more general version of the "Main Lemma" can be proved similarly. Let $\psi : \widetilde{\mathcal{C}} \to \mathcal{C}$ be a finite morphism of curves over K. Assume that there exists a non-constant function $t \in K(\mathcal{C})$ such that:

i) the zeroes of t are K-rational points $A_1, \dots A_r$;

ii) the morphism ψ is unramified above the A_i;

iii) for any i, j, we have an isomorphism $\psi^{-1}(A_i) \simeq \psi^{-1}(A_j)$.

Then a similar conclusion to that of Lemma 2.3 holds.

2.2 Proof of Theorem 1.9

According to Theorem 1.8, there exists a finite set S of places of K such that for every $P \in \mathcal{C}(\bar{K})$ and $\widetilde{P} \in \psi^{-1}(P)$ the number field extension $K(\widetilde{P})/K(P)$ is unramified outside places above S. This is equivalent to saying that the extension $K(\psi^{-1}(P))/K(P)$ is unramified outside places above S.

Now fix a place $v \in S \cup M_K^\infty$. Applying Lemma 2.3 over K_v, we find that there exists $\varepsilon_v > 0$ such that, for every $P \in \mathcal{C}(\bar{K}_v)$ with $t(P) \in K$ and $|t(P)|_v < \varepsilon_v$, we have, for any place w of $K(P)$ lying above v,

$$\psi^{-1}(P) \otimes_{K(P)} K(P)_w \simeq \psi^{-1}(A) \otimes_K K(P)_w.$$

In particular, these finite varieties have the same function fields. But by assumption we have $K(\psi^{-1}(A)) = K$, hence this yields $K(P)_w(\psi^{-1}(P)) = K(P)_w$, in other words $\psi^{-1}(P)$ has all its points defined over $K(P)_w$. This means that w is totally split in $K(\psi^{-1}(P))$. In particular, the extension $K(\psi^{-1}(P))/K(P)$ is unramified at w.

We complete the proof setting $\varepsilon = \min\{\varepsilon_v : v \in S \cup M_K^\infty\}$.

Remark 2.5. Replacing Lemma 2.3 by Remark 2.4, one can prove a more general statement. In the set-up of Theorem 1.8 assume that there exists $t \in K(\mathcal{C})$ with the following property: for any point $A \in \mathcal{C}(\bar{K})$ with $t(A) = 0$ we have $K(A) = K(\psi^{-1}(A)) = K$. Then the conclusion of Theorem 1.9 holds.

3 Counting Number Fields in Fibers: the Theorem of Dvornicich & Zannier

Unless the contrary is stated explicitly, everywhere in this section

- K is a number field of degree ℓ over $\mathbb{Q}$,
- $\mathcal{C}$ is a (smooth geometrically irreducible projective) curve over K,
- $t : \mathcal{C} \to \mathbb{P}^1$ is a finite K-morphism of degree d.

According to the Hilbert Irreducibility Theorem (see Subsection 3.1), for "most" $\alpha \in K$ the fiber $t^{-1}(\alpha)$ is K-irreducible. For our purposes we need a more precise statement: first, we have to consider not the entire field K, but a proper subset, and second, we need to know that among the fields generated by the fibers there are "many" distinct.

We normalize the absolute values on number fields to extend the standard absolute values on $\mathbb{Q}$: if $v \mid \infty$ then $|2016|_v = 2016$, and if $v \mid p < \infty$ then $|p|_v = p^{-1}$. We denote by M_L the set of all absolute values on the number field L normalized as above, and by M_L^∞ and M_L^0 the sets of infinite and of finite absolute values, respectively.

We denote by $\mathrm{H}(\alpha)$ the multiplicative absolute height of an algebraic number α: if L is a number field containing α then

$$\mathrm{H}(\alpha) = \prod_{v \in M_L} \max\{1, |\alpha|_v\}^{[L_v:\mathbb{Q}_v]/[L:\mathbb{Q}]}.$$

We will use the standard properties of heights like

$$\mathrm{H}(\alpha + \beta) \le 2\mathrm{H}(\alpha)\mathrm{H}(\beta), \quad \mathrm{H}(\alpha\beta) \le \mathrm{H}(\alpha)\mathrm{H}(\beta), \quad \mathrm{H}(\alpha^n) = \mathrm{H}(\alpha)^{|n|}, \tag{3}$$

etc.

Theorem 3.1. *Let S be a finite set of places of K and ε a positive real number. Further, let $\mathcal{U}$ be a thin subset of K (see Subsection 3.1). Then there exist positive numbers $c = c(K, \mathcal{C}, t, S, \varepsilon)$ and $B_0 = B_0(K, \mathcal{C}, t, S, \varepsilon, \mathcal{U})$ such that, for every $B \ge B_0$ the following holds. Consider the points $P \in \mathcal{C}(\bar{K})$ satisfying*

$$t(P) \in K \setminus \mathcal{U}, \tag{4}$$

$$|t(P)|_v < \varepsilon \qquad (v \in S), \tag{5}$$

$$\mathrm{H}(t(P)) \le B.$$

Then among the number fields $K(P)$, where P satisfies the conditions above, there are at least $cB^\ell/\log B$ distinct fields of degree d over K.

This theorem is, essentially, due to Dvornicich and Zannier [12]. In particular, the case $K = \mathbb{Q}$ (and arbitrary S, ε) can be easily deduced from [12, Theorem 2(a)]. For the general case we need a suitable generalization of the result of Dvornicich and Zannier, which can be found in [4], see Subsection 3.3.

Remark 3.2. The estimate $cB^\ell/\log B$ is sufficient for us, but it is, probably, far from best possible. For instance, a result of Corvaja and Zannier [10, Corollary 1] implies, for sufficiently large B, a lower bound of the form $B^\ell(\log B)^k$ with arbitrary $k > 0$ provided t has at least 3 zeros in $\mathcal{C}(\bar{K})$. Using methods of article [20][2], one can show that for sufficiently large B there are at least $c'B^{2\ell}$ numbers $\alpha \in K$ satisfying $|\alpha|_v < \varepsilon$ for every $v \in S$, and $\mathrm{H}(\alpha) \le B$; here $c' > 0$ depends on K, S and ε. Moreover, one can probably even prove the asymptotics $\gamma B^{2\ell}$ (as $B \to \infty$) for the counting function of such numbers; here $\gamma > 0$ depends on K, S and ε. This suggests that a lower bound of the form $cB^{2\ell}/(\log B)^A$ must hold true with some $A > 0$.

In Subsection 3.4 we estimate the discriminants of the fields emerging in Theorem 3.1. Recall that, given a number field extension L/K, we define

$$\mathcal{D}(L/K) = \left|\mathcal{N}_{K/\mathbb{Q}}\Delta(L/K)\right|^{1/[K:\mathbb{Q}]},$$

where $\Delta(L/K)$ is the discriminant of L over K. In Subsection 3.4 we estimate $\mathcal{D}(K(P)/K)$, where P is as in Theorem 3.1; see Proposition 3.14.

Combining Theorem 3.1 and Proposition 3.14, we obtain the following consequence.

Corollary 3.3. *In the set-up of Theorem 3.1, assume in addition that there exists a non-constant rational function $x \in K(\mathcal{C})$ of degree m such that*

$$K(\mathcal{C}) = K(t, x).$$

Then there exist positive numbers

$$c = c(K, \mathcal{C}, t, S, \varepsilon) \quad \text{and} \quad X_0 = X_0(K, \mathcal{C}, t, S, \varepsilon)$$

such that, for every $X \ge X_0$ there exist at least $cX^{\ell/(2m(d-1))}/\log X$ distinct fields L with

$$[L : K] = d, \qquad \mathcal{D}(L/K) \le X,$$

and of the form $L = K(P)$, where P satisfies (4), (5).

3.1 Thin Subsets and Hilbert's Irreducibility Theorem

In this subsection we recall basic definitions and facts about thin sets, and state Hilbert's Irreducibility Theorem.

Let K be a field of characteristic 0. We call $\mathcal{U} \subset K$ a *basic thin subset* of K if there exists a (smooth geometrically irreducible) curve $\mathcal{C}$ defined over K and a non-constant rational function $u \in K(\mathcal{C})$ of degree at least 2 such that $\mathcal{U} \subset u(\mathcal{C}(K))$. A *thin subset* of K is a union of finitely many basic thin subsets. Thin subsets form an ideal in the algebra of subsets of K. Serre in [19, Section 9.1] gives a differently looking, but equivalent definition of thin sets.

Any finite set is thin, and if K is algebraically closed then any subset of K is thin.

[2] Attention: in [20] the height is normalized with respect to K, and not with respect to $\mathbb{Q}$, as in the present article.

Remark 3.4. If L is an extension of K then any thin subset of K is also thin as a subset of L. The converse is true when L is finitely generated over K [6, Proposition 2.1] but not in general; for instance, any number field K is a thin subset of its algebraic closure $\bar{K}$ but is not a thin subset of itself by the Hilbert Irreducibility Theorem quoted below.

Using elementary Galois theory one easily proves the following (see [19, Section 9.2])

Proposition 3.5. *Let $\mathcal{C}$ be a curve over K and $t \in K(\mathcal{C})$ a non-constant rational function. Then the set of $\alpha \in K$ such that the fiber $t^{-1}(\alpha)$ is reducible over K is thin.*

Hilbert's Irreducibility Theorem asserts that when K is a number field then its ring of integers $\mathcal{O}_K$ is not a thin subset of K. In fact, one has the following counting result (see [19], Theorem on page 134).

Theorem 3.6. *Let K be a number field of degree ℓ over $\mathbb{Q}$ and $\mathcal{U}$ a thin subset of K. Then for $B \geq 1$ the set $\mathcal{U} \cap \mathcal{O}_K$ has at most $O(B^{\ell/2})$ elements α satisfying $|\alpha|_v \leq B$ for every $v \in M_K^\infty$; the implicit constant depends on K and on $\mathcal{U}$.*

3.2 Counting Algebraic Integers

To prove Theorem 3.1 we need to count algebraic integers in the number field K whose conjugates are bounded by given quantities. We denote by s_1 and s_2 the number of real and of complex infinite places of K, so that $\ell = s_1 + 2s_2$ and $|M_K^\infty| = s_1 + s_2$. We also denote by D_K the discriminant of K over $\mathbb{Q}$.

Proposition 3.7. *For every $v \in M_K^\infty$ pick $B_v \geq 1$. Then the total number of $\alpha \in \mathcal{O}_K$ satisfying $|\alpha|_v \leq B_v$ for $v \in M_K^\infty$ is*

$$\frac{2^{s_1+s_2}\pi^{s_2}\prod_v B_v^{e_v}}{|D_K|^{1/2}}\left(1 + O\left(\frac{1}{\min\{B_v : v \in M_K^\infty\}}\right)\right),$$

where $e_v = 1$ if v is real, $e_v = 2$ if v is complex, and the implicit constant depends only on K.

This is, of course, well-known and classical, but we did not find exactly this statement in the literature. Therefore we add some details for the reader's convenience.

Let us recall some standard facts from the Geometry of Numbers. If Γ is a lattice in $\mathbb{R}^\ell$ and $\mathcal{U} \subset \mathbb{R}^\ell$ a bounded symmetric convex set, then $|\mathcal{U} \cap \Gamma|$ must be approximated by $\frac{\mathrm{Vol}\,\mathcal{U}}{\det \Gamma}$, where Vol denotes the standard Euclidean volume on $\mathbb{R}^\ell$ and $\det \Gamma$ is the fundamental volume of Γ. To make this precise, we define the *inner radius* of $\mathcal{U}$ as the minimal (Euclidean) distance from the boundary of $\mathcal{U}$ to the origin:

$$\mathrm{innr}\,\mathcal{U} = \min\{\|x\|_2 : x \in \partial U\}.$$

Proposition 3.8. *Let Γ be a lattice in $\mathbb{R}^d$. Then for any bounded symmetric convex set $\mathcal{U}$ we have*

$$|\mathcal{U} \cap \Gamma| = \mathrm{Vol}\,\mathcal{U}\left(\frac{1}{\det \Gamma} + O\left(\frac{1}{\mathrm{innr}\,\mathcal{U}}\right)\right),$$

where the implied constant may depend on Γ, but not on $\mathcal{U}$.

Proposition 3.7 readily follows from this, by viewing $\mathcal{O}_K$ as a lattice in $\mathbb{R}^{s_1} \times \mathbb{C}^{s_2}$, of fundamental volume $2^{-s_2}|D_K|^{1/2}$.

Proving Proposition 3.8 requires some preparation. The standard inner product on the Euclidean space $\mathbb{R}^\ell$ induces an inner product on every subspace $\mathcal{L}$, and we denote by $\mathrm{Vol}_\mathcal{L}$ the volume on $\mathcal{L}$ induced by this inner product.

Lemma 3.9. *Let $\mathcal{L}$ be a subspace of $\mathbb{R}^\ell$ and denote by $\pi_\mathcal{L} : \mathbb{R}^\ell \to \mathcal{L}^\perp$ the orthogonal projection along $\mathcal{L}$. Then for any bounded symmetric convex set $\mathcal{U} \subset \mathbb{R}^d$ we have*

$$\mathrm{Vol}_\mathcal{L}(\mathcal{U} \cap \mathcal{L}) \, \mathrm{Vol}_{\mathcal{L}^\perp}(\pi_\mathcal{L}(\mathcal{U})) \le \binom{\ell}{m} \mathrm{Vol}\,\mathcal{U},$$

where $m = \dim \mathcal{L}$.

Proof. See [3, Lemma 6.6]. □

The intersection $\mathcal{U} \cap \mathcal{L}$ contains the (open) ℓ-dimensional ball of radius $\mathrm{innr}\,\mathcal{U}$. Hence Lemma 3.9 has the following consequence.

Corollary 3.10. *In the set-up of Lemma 3.9 we have*

$$\mathrm{Vol}_{\mathcal{L}^\perp}(\pi_\mathcal{L}(\mathcal{U})) \le \frac{c}{(\mathrm{innr}\,\mathcal{U})^m} \mathrm{Vol}\,\mathcal{U},$$

where c depends only on the dimension d.

Proof of Proposition 3.8. We may assume that $\Gamma = \mathbb{Z}^\ell$. Indeed, pick some basis of Γ and consider the new inner product, making this basis orthonormal. The quantities $|\mathcal{U} \cap \Gamma|$ and $\frac{\mathrm{Vol}\,\mathcal{U}}{\det \Gamma}$ will be not altered, and the inner radius R will be replaced by $R' \ge cR$, where c depends only on the basis we picked.

For a subset $S \subseteq \{1, 2, \dots, \ell\}$ let $\mathcal{L}_S$ be the subspace of $\mathbb{R}^\ell$ defined by $x_i = 0$ for $i \in S$. By the classical result of Davenport [11],

$$\big||\mathcal{U} \cap \mathbb{Z}^\ell| - \mathrm{Vol}\,\mathcal{U}\big| \le \sum_{S \ne \varnothing} \mathrm{Vol}_{\mathcal{L}_S^\perp}(\pi_{\mathcal{L}_S}(\mathcal{U})),$$

the sum being over the non-empty subsets $S \subseteq \{1, 2, \dots, \ell\}$. By Corollary 3.10, each summand on the right is bounded by $c(\ell)\frac{\mathrm{Vol}\,\mathcal{U}}{\mathrm{innr}\,\mathcal{U}}$. This proves Proposition 3.8. □

Here is an immediate consequence.

Corollary 3.11. *For positive real numbers B and E satisfying $B \ge E \ge 2$, at most $O(EB^{\ell-1})$ numbers $\alpha \in \mathcal{O}_K$ satisfy*

$$\max_{v \in M_K^\infty} |\alpha|_v \le B, \qquad \min_{v \in M_K^\infty} |\alpha|_v \le E.$$

The implicit constant depends only on K.

3.3 Proof of Theorem 3.1

The following result is Corollary 8.2 from [4].

Theorem 3.12. *There exist positive numbers $c = c(K, \mathcal{C}, t)$ and $B_0 = B_0(K, \mathcal{C}, t)$ such that, for every $B \geq B_0$, the following holds. Consider the points $P \in \mathcal{C}(\bar{K})$ satisfying*

$$t(P) \in \mathcal{O}_K, \tag{6}$$
$$|t(P)|_v \leq B \qquad (v \in M_K^\infty). \tag{7}$$

Then among the number fields $K(P)$, where P satisfies the conditions above, there are at least $cB^\ell/\log B$ distinct fields.

Combining this with Theorem 3.6 and Corollary 3.11, we obtain the following statement.

Corollary 3.13. *Let $E \geq 2$ be a real number and let $\mathcal{U}$ be a thin subset of K. Then there exist positive numbers $c = c(K, \mathcal{C}, t)$ and $B_0 = B_0(K, \mathcal{C}, t, E, \mathcal{U})$ such that, for every $B \geq B_0$, the following holds. Consider the points $P \in \mathcal{C}(\bar{K})$ satisfying*

$$t(P) \in \mathcal{O}_K \setminus \mathcal{U}, \tag{8}$$
$$|t(P)|_v \geq E \qquad (v \in M_K^\infty), \tag{9}$$
$$\mathrm{H}(t(P)) \leq B. \tag{10}$$

Then among the number fields $K(P)$, where P satisfies the conditions above, there are at least $cB^\ell/\log B$ distinct fields of degree d over K.

Proof. Corollary 3.11 implies that there exists at most $O(EB^{\ell-1})$ points P for which (6) and (7) hold, but (9) does not hold. Denote by c' and B_0' the numbers c and B_0 from Theorem 3.12. Then for $B \geq B_0'$ we find $c'B^\ell/\log B - O(EB^{\ell-1})$ points P satisfying (7), (8) and (9), for which the fields $K(P)$ are pairwise distinct. Since $\mathrm{H}(\alpha) \leq \max_{v \in M_K^\infty} |\alpha|_v$ for $\alpha \in \mathcal{O}_K$, all these points satisfy (10).

By Proposition 3.5 and Theorem 3.6, only $O(B^{\ell/2})$ of these points P satisfy $t(P) \in \mathcal{U}$ or $[K(P) : K] < d$. It remains to observe that for sufficiently large B we have

$$c'B^\ell/\log B - O(EB^{\ell-1}) - O(B^{\ell/2}) \geq (c'/2)B^\ell/\log B.$$

This proves Corollary 3.13 with $c = c'/2$. □

Now we are ready to complete the proof of Theorem 3.1. Applying a suitable coordinate change, we reduce it to Corollary 3.13.

Let S and ε be as in Theorem 3.1. Pick a non-zero $a \in \mathcal{O}_K$ and a real $E \geq 2$ satisfying

$$|a|_v < \min\{\varepsilon, 1\} \qquad (v \in S^0),$$
$$E > \varepsilon^{-1} + |a|_v^{-1} \qquad (v \in S^\infty),$$

where S^0 and S^∞ denote the sets of finite and of infinite places from S. Set $t^* = 1/t + 1/a$, so that $t = 1/(t^* - a^{-1})$, and $\mathcal{U}^* = \{1/\tau + 1/a : \tau \in \mathcal{U}\}$.

Applying Corollary 3.13 to the data K, $\mathcal{C}$, t^*, E and $\mathcal{O}^*$, for every $B \geq B_0$ we find $cB^\ell/\log B$ points P satisfying

$$t^*(P) \in \mathcal{O}_K \smallsetminus \mathcal{O}^*, \tag{11}$$

$$|t^*(P)|_v \geq E \qquad (v \in M_K^\infty), \tag{12}$$

$$\mathrm{H}(t^*(P)) \leq B.$$

and such that the fields $K(P)$ are pairwise distinct and of degree d over K.

Due to our choice of a and E, inequality (5) follows from (11) for $v \in S^0$ and from (12) for $v \in S^\infty$. Also, $t(P) \in \mathcal{O}$ if and only if $t^*(P) \in \mathcal{O}^*$. Finally, using (3) we obtain

$$\mathrm{H}(t(P)) \leq 2\mathrm{H}(a)\mathrm{H}(t^*(P)) \leq 2\mathrm{H}(a)B.$$

This proves Theorem 3.1 with suitably adjusted c and B_0. □

3.4 Estimating the discriminants

In this subsection we estimate the discriminants of number fields generated by irreducible fibers. Recall that, given a number field extension L/K, we define

$$\mathcal{D}(L/K) = \left|\mathcal{N}_{K/\mathbb{Q}}\Delta(L/K)\right|^{1/\ell},$$

where $\Delta(L/K)$ is the discriminant of L over K and $\ell = [K : \mathbb{Q}]$.

For a point $P \in \mathcal{C}(\bar{K})$ such that $t(P) \in K$, we will write $\mathcal{D}(P)$ for $\mathcal{D}(K(P)/K)$.

Proposition 3.14. *Assume that there exists a non-constant rational function $x \in K(\mathcal{C})$ of degree m such that $K(\mathcal{C}) = K(t, x)$. Then for every point $P \in \mathcal{C}(\bar{K})$ such that*

$$t(P) \in K, \qquad [K(P) : K] = d \tag{13}$$

we have

$$\mathcal{D}(P) \leq c\mathrm{H}(t(P))^{2m(d-1)}, \tag{14}$$

where c depends on $\mathcal{C}$ and t (but not on K).

For the proof we need some lemmas. Recall the notion of projective height: if $\underline{\alpha} = (\alpha_0, \ldots, \alpha_N) \in \mathbb{P}^N(\bar{\mathbb{Q}})$ then

$$\mathrm{H}_\mathrm{p}(\underline{\alpha}) := \prod_{v \in M_L} \max\{|\alpha_0|_v, \ldots, |\alpha_N|_v\}^{[L_v:\mathbb{Q}_v]/[L:\mathbb{Q}]},$$

where L is a number field containing $\alpha_0, \ldots, \alpha_N$. Note that $\mathrm{H}(\alpha) = \mathrm{H}_\mathrm{p}(1, \alpha)$ for $\alpha \in \bar{\mathbb{Q}}$.

The projective height of a polynomial with algebraic coefficients is the projective height of the vector of its non-zero coefficients.

Lemma 3.15. *Let $f(X) \in K[X]$ be a K-irreducible polynomial of degree d. Then for any of its roots $\beta \in \bar{K}$ we have*

$$\mathcal{D}(K(\beta)/K) \leq d^{3d}\mathrm{H}_\mathrm{p}(f)^{2(d-1)}.$$

Proof. Let $\beta_1, \dots, \beta_d$ be the roots of f. According to Corollary 3.17 from [7],

$$\prod_{i=1}^{d} \mathcal{D}(K(\beta_i)/K)^{1/[K(\beta_i):K]} \le d^{3d} \mathrm{H_p}(f)^{2(d-1)}.$$

However, since f is K-irreducible, all the $\mathcal{D}(K(\beta_i)/K)$ are equal, and all the $[K(\beta_i):K]$ are equal to d. Whence the result. □

Lemma 3.16. *Let $F(T,X) \in \bar{\mathbb{Q}}[T,X]$ be a polynomial of T-degree m, and let $\alpha \in \bar{\mathbb{Q}}$. Then the polynomial $f(X) = F(\alpha, X)$ satisfies*

$$\mathrm{H_p}(f) \le (m+1)\mathrm{H_p}(F)\mathrm{H}(\alpha)^m.$$

Proof. Let L be a number field containing α and the coefficients of F. For $v \in M_L$ denote by $|F|_v$ and $|f|_v$ the maximal v-value of the coefficients of F, respectively f. We estimate trivially

$$|f|_v \le \begin{cases} |F|_v \max\{1, |\alpha|_v\}^m, & v \in M_L^0, \\ (m+1)|F|_v \max\{1, |\alpha|_v\}^m, & v \in M_L^\infty. \end{cases}$$

Multiplying over $v \in M_L$, the result follows. □

Proof of Proposition 3.14. For all but finitely many points $P \in \mathcal{C}(\bar{K})$ we have

$$K(P) = K(t(P), x(P)).$$

In particular, $K(P) = K(x(P))$ for all but finitely many points P satisfying $t(P) \in K$.

There exists a polynomial $F(T,X) \in K[T,X]$ such that

$$F(t,x) = 0, \qquad \deg_T F = m, \quad \deg_X F = d.$$

Now assume that P satisfies (13), that $K(P) = K(x(P))$, and that P is not a pole of t and not a pole of x. Then the polynomial $f_P(X) = F(t(P), X)$ is K-irreducible, of degree d, and has $x(P)$ as one of its roots. Using Lemmas 3.15 and 3.16, we obtain

$$\mathcal{D}(P) \le d^{3d} \mathrm{H_p}(f_P)^{2(d-1)} \le d^{3d} \big((m+1)\mathrm{H_p}(F)\big)^{2(d-1)} \mathrm{H}(t(P))^{2m(d-1)}.$$

This proves (14) for all but finitely many P satisfying (13). By adjusting c we obtain it for all such P. □

4 Specialization of torsors

In this section we consider a finite flat (not necessarily commutative) $\mathcal{O}_K$-group scheme $\mathcal{G}$. We denote by $H^1_{\mathrm{et}}(\mathcal{O}_K, \mathcal{G})$ (resp. $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G})$) the cohomology set which classifies étale (resp. flat) $\mathcal{G}$-torsors over $\mathcal{O}_K$. We denote by $\mathcal{G}_K$ the generic fibre of $\mathcal{G}$, and by $H^1(K, \mathcal{G}_K)$ the (possibly non-abelian) Galois cohomology set $H^1(\mathrm{Gal}(\bar{K}/K), \mathcal{G}_K(\bar{K}))$.

Let us recall that the "restriction to the generic fiber" map $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \to H^1(K, \mathcal{G}_K)$ is injective. Indeed, if ξ is a flat $\mathcal{G}$-torsor over $\mathcal{O}_K$, then, by descent theory, ξ is representable by a finite flat $\mathcal{O}_K$-scheme. Therefore, if the generic fiber of ξ has a section, then the valuative criterion of properness implies that ξ itself has a section. By consequence, we have a chain of inclusions

$$H^1_{\mathrm{et}}(\mathcal{O}_K, \mathcal{G}) \subset H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \subset H^1(K, \mathcal{G}_K).$$

4.1 Local splitting of torsors

We now define a set of cohomology classes which are locally trivial at all places in S.

Definition 4.1. If S is a finite set of places of K, we let

$$H^1_{S\text{-split}}(\mathcal{O}_K, \mathcal{G}) := \ker\left(H^1_{\mathrm{fl}}(\mathcal{O}_{K,S}, \mathcal{G}) \to \prod_{v\in S} H^1_{\mathrm{fl}}(K_v, \mathcal{G}_{K_v}) \right).$$

Lemma 4.2. *The set $H^1_{S\text{-split}}(\mathcal{O}_K, \mathcal{G})$ is a subset of $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G})$. Moreover, if $\mathcal{G}$ is étale over $\mathcal{O}_{K,S}$, then it is a subset of $H^1_{\mathrm{et}}(\mathcal{O}_K, \mathcal{G})$.*

Proof. It follows from [9, Corollary 4.2] that, if S is a finite set of places of K, the square

$$\begin{array}{ccc} H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) & \longrightarrow & H^1_{\mathrm{fl}}(\mathcal{O}_{K,S}, \mathcal{G}) \\ \downarrow & & \downarrow \\ \prod_{v\in S} H^1_{\mathrm{fl}}(\mathcal{O}_{K_v}, \mathcal{G}) & \longrightarrow & \prod_{v\in S} H^1(K_v, \mathcal{G}_{K_v}) \end{array}$$

is cartesian, with injective horizontal maps. Hence the result. □

Theorem 4.3. *Let K be a number field, and let $\mathcal{G}$ be a finite flat (non necessarily commutative) $\mathcal{O}_K$-group scheme. Consider the following setting:*

- *$\mathcal{C}$ is a (smooth geometrically irreducible projective) curve over K;*
- *$\psi : \widetilde{\mathcal{C}} \to \mathcal{C}$ is a $\mathcal{G}_K$-torsor (where $\widetilde{\mathcal{C}}$ is geometrically irreducible);*
- *A is a K-rational point of $\mathcal{C}$ such that $\psi^{-1}(A)$ is the trivial $\mathcal{G}_K$-torsor;*
- *$t : \mathcal{C} \to \mathbb{P}^1$ is a finite K-morphism, having A as its single zero.*

Let S be any finite set of places of K which contains the set from Theorem 1.8. Let also F be a finite extension of K. Then:

1) *there exists $\varepsilon > 0$ such that, for every point $P \in \mathcal{C}(\bar{K})$ satisfying $t(P) \in K$ and $|t(P)|_v < \varepsilon$ for all $v \in S$, the torsor $\psi^{-1}(P)$ belongs to the subset*

$$H^1_{S\text{-split}}(\mathcal{O}_{K(P)}, \mathcal{G}) \subset H^1(K(P), \mathcal{G}_K),$$

   in particular, $\psi^{-1}(P)$ extends into a flat $\mathcal{G}$-torsor over $\mathcal{O}_{K(P)}$ (or even an étale torsor, up to enlarging the set S).

2) *there exist infinitely many P as in 1) such that $[K(P) : K] = \deg(t)$ and $\psi^{-1}(P)$ is the spectrum of a field which is linearly disjoint from F.*

More precisely, there exist positive numbers c and B_0 such that, for every $B \geq B_0$, the following holds: among the number fields $K(P)$, where P is as in 2) and $H(t(P)) \leq B$, there are at least $cB^\ell / \log B$ distinct fields.

Remark 4.4. In general, given a finite K-group scheme G, it may not be possible to extend G into a finite flat group scheme over $\mathcal{O}_K$, and, in case such a group scheme exists, it may not be unique. Nevertheless, if the set S contains all places dividing the order of G, there exists at most one way to extend G into a finite flat (automatically étale) group scheme over $\mathcal{O}_{K,S}$. In the statement above, what really matters is the fact that the group scheme $\mathcal{G}_K$ can be extended into a finite flat group scheme $\mathcal{G}$ over $\mathcal{O}_K$, not the choice of $\mathcal{G}$.

Proof. Let $\psi : \widetilde{\mathcal{C}} \to \mathcal{C}$ be a $\mathcal{G}_K$-torsor. Then there exists a finite set S of finite places of K such that ψ extends into a $\mathcal{G}$-torsor $\tilde{C} \to C$ between $\mathcal{O}_{K,S}$-schemes, where C is a smooth projective model of $\mathcal{C}$ over $\mathcal{O}_{K,S}$. We note that such an S contains places of bad reduction of the curve $\mathcal{C}$, and also additional places that we may consider as being places where ψ has bad reduction. Up to enlarging S, we may assume that $\mathcal{G}$ is étale over $\mathcal{O}_{K,S}$.

By projectivity of C over $\mathcal{O}_{K,S}$, any point $P \in \mathcal{C}(\bar{K})$ can be extended into a section $\mathrm{Spec}(\mathcal{O}_{K(P),S'}) \to C$, where S' is the set of places of $K(P)$ that lie above places in S. It follows that, for any $P \in \mathcal{C}(\bar{K})$, $\psi^{-1}(P)$ belongs to the subset

$$H^1_{\mathrm{et}}(\mathcal{O}_{K(P),S'}, \mathcal{G}) \subset H^1(K(P), \mathcal{G}_K).$$

Let us fix a place v of K. Applying Lemma 2.3 over the completion K_v, we find that there exists $\varepsilon_v > 0$ such that, for every $P \in \mathcal{C}(\bar{K}_v)$ satisfying $|t(P)|_v < \varepsilon_v$, we have

$$\psi^{-1}(P) \otimes_{K(P)} K_v(P) \simeq \psi^{-1}(A) \otimes_K K_v(P)$$

where $K_v(P)$ is the smallest extension of K_v over which P is defined. This means that $\psi^{-1}(P)$ is the trivial torsor over $K_v(P)$, because by hypothesis $\psi^{-1}(A)$ is the trivial torsor.

Now, if we consider a point $P \in \mathcal{C}(\bar{K})$ and a place w of $K(P)$ lying above v, then $K(P)_w$ contains $K_v(P)$ as a subfield, hence if $|t(P)| < \varepsilon_v$ then $\psi^{-1}(P)$ becomes trivial over $K(P)_w$.

If we set $\varepsilon = \min\{\varepsilon_v : v \in S\}$, then $\psi^{-1}(P)$ belongs to $H^1_{S\text{-split}}(\mathcal{O}_{K(P)}, \mathcal{G})$ for every $P \in \mathcal{C}(\bar{K})$ satisfying $t(P) \in K$ and $|t(P)|_v < \varepsilon$ for all $v \in S$. This completes the proof of the first (qualitative) statement. Let us finally note that, according to Lemma 4.2, for such P the torsor $\psi^{-1}(P)$ extends into an étale $\mathcal{G}$-torsor over $\mathcal{O}_{K(P)}$.

To prove the second (quantitative) statement, we apply Theorem 3.1. Set $\tilde{t} = t \circ \psi$ and define the set $\mathcal{U} \subset K$ as follows: $\mathcal{U} = \mathcal{U}_1 \cup \mathcal{U}_2$, where

$$\mathcal{U}_1 = \{\tilde{t}(Q) : Q \in \widetilde{\mathcal{C}}(\bar{K}),\ \tilde{t}(Q) \in K,\ [K(Q) : K] < \deg \tilde{t}\},$$
$$\mathcal{U}_2 = \{\tilde{t}(Q) : Q \in \widetilde{\mathcal{C}}(\bar{K}),\ \tilde{t}(Q) \in K,\ K(Q) \text{ is not linearly disjoint from } F\}.$$

Proposition 3.5 implies that $\mathcal{U}_1$ is a thin set in K. The set $\mathcal{U}_2$ is thin in K as well. Indeed, since $\widetilde{\mathcal{C}}$ is geometrically irreducible, the degree of $\tilde{t}$ does not change if we extend the base field from K to F. But, if $K(Q)$ is not linearly disjoint from F, then

$$[F(Q) : F] < [K(Q) : K] \leq \deg \tilde{t},$$

which implies that $\mathcal{U}_2$ is thin in F. Remark 3.4 implies that $\mathcal{U}_2$ is thin in K as well. Thus, the set $\mathcal{U}$ is thin.

Theorem 3.1 implies that there exists a positive number c such that, for sufficiently large B, among the number fields $K(P)$ where $P \in \mathcal{C}(\bar{K})$ satisfies

$$\begin{aligned} t(P) &\in K \smallsetminus \mathcal{U}, \\ |t(P)|_v &< \varepsilon \qquad (v \in S), \\ \mathrm{H}(t(P)) &\leq B, \end{aligned}$$

there are at least $cB^\ell/\log B$ distinct fields of degree d over K. Moreover, if P is one of these points, then, by definition of our set $\mathfrak{V}$, for any $Q \in \psi^{-1}(P)$ we have $[K(Q) : K(P)] = \deg(\psi)$ and $[K(P) : K] = \deg(t)$, which means that P satisfies 2). The theorem is proved. □

4.2 From finite subgroups of Jacobians to finite covers

In this section we consider a commutative finite flat $\mathcal{O}_K$-group scheme $\mathcal{G}$, whose generic fiber $\mathcal{G}_K$ becomes constant cyclic of order n over $\bar{K}$. Typical examples are $\mathbb{Z}/n\mathbb{Z}$ (the constant group scheme) and μ_n (the group scheme of n-th roots of unity). We denote by $\mathcal{G}^D$ the Cartier dual of $\mathcal{G}$.

Let $\mathcal{C}$ be a curve over K, with a given K-rational point A, and let $J(\mathcal{C})$ be the Jacobian of $\mathcal{C}$. The point A gives rise to an embedding $i_A : \mathcal{C} \to J(\mathcal{C})$ such that $i_A(A) = 0$.

Lemma 4.5. *Assume that $J(\mathcal{C})$ contains a subgroup scheme isomorphic to $(\mathcal{G}_K^D)^r$ for some integer $r \geq 1$. Then there exists $\mathcal{G}_K$-torsors*

$$\psi_1 : X_1 \to \mathcal{C}, \ldots, \psi_r : X_r \to \mathcal{C}$$

such that:

1. *$\psi_i^{-1}(A)$ is the trivial torsor for all i;*
2. *the ψ_i generate a subgroup of $H^1(\mathcal{C}, \mathcal{G}_K)$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$;*
3. *the fiber product $X_1 \times_{\mathcal{C}} \cdots \times_{\mathcal{C}} X_r$ is a geometrically irreducible curve.*

Proof. Let us fix an embedding $\mathcal{G}_K^D \to J(\mathcal{C})$. Let B be the quotient abelian variety $J(\mathcal{C})/\mathcal{G}_K^D$, and let $\theta : J(\mathcal{C}) \to B$ be the isogeny with kernel $\mathcal{G}_K^D$. This isogeny gives rise to a dual isogeny $\theta^t : B^t \to J(\mathcal{C})^t$ where B^t is the dual abelian variety of B. By duality of abelian varieties, the kernel of θ^t is the Cartier dual of the kernel of θ, hence is isomorphic to $\mathcal{G}_K$. By auto-duality of the Jacobian, we have $J(\mathcal{C})^t \simeq J(\mathcal{C})$. Let $\psi : X \to \mathcal{C}$ be the morphism defined by the following cartesian square (or pull-back)

$$\begin{array}{ccc} X & \longrightarrow & B^t \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\theta^t} \\ \mathcal{C} & \xrightarrow{i_A} & J(\mathcal{C}) \end{array}$$

then ψ is a $\mathcal{G}_K$-torsor, because θ^t is, and $\psi^{-1}(A)$ is the trivial torsor, because $(\theta^t)^{-1}(0)$ is.

Because $\mathcal{C}(K) \neq \emptyset$, the Leray spectral sequence (see [16, exposé V, §3]) associated to $\mathcal{C} \to \mathrm{Spec}(K)$ and $\mathcal{G}_K$ gives us a short exact sequence

$$0 \longrightarrow H^1(K, \mathcal{G}_K) \longrightarrow H^1(\mathcal{C}, \mathcal{G}_K) \longrightarrow \mathrm{Hom}(\mathcal{G}_K^D, J(\mathcal{C})) \longrightarrow 0 \tag{15}$$

More precisely, the right hand side map above induces a bijection

$$\ker\left(A^* : H^1(\mathcal{C}, \mathcal{G}_K) \to H^1(K, \mathcal{G}_K)\right) \longrightarrow \mathrm{Hom}(\mathcal{G}_K^D, J(\mathcal{C}))$$

Indeed, according to the ker-coker Lemma, the section $A : \mathrm{Spec}(K) \to \mathcal{C}$ gives rise to an isomorphism between the cokernel of the map $H^1(K, \mathcal{G}_K) \to H^1(\mathcal{C}, \mathcal{G}_K)$ and the kernel of the map $A^* : H^1(\mathcal{C}, \mathcal{G}_K) \to H^1(K, \mathcal{G}_K)$.

If we start from an injective morphism $\mathcal{G}_K^D \to J(\mathcal{C})$, we get from the construction above a geometrically irreducible $\mathcal{G}_K$-torsor $X \to \mathcal{C}$ which belongs to $\ker(A^*)$. By hypothesis, we have r independent injections $\mathcal{G}_K^D \to J(\mathcal{C})$, which generate a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$ in $\mathrm{Hom}(\mathcal{G}_K^D, J(\mathcal{C}))$. Therefore, we obtain r torsors $\psi_1, \dots \psi_r$ which generate a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$ in $\ker\big(A^* : H^1(\mathcal{C}, \mathcal{G}_K) \to H^1(K, \mathcal{G}_K)\big)$. Their fiber product $X_1 \times_{\mathcal{C}} \cdots \times_{\mathcal{C}} X_r$ is a geometrically irreducible $(\mathcal{G}_K)^r$-torsor. □

Theorem 4.6. *Let $\mathcal{C}$ be a curve over K, and let $J(\mathcal{C})$ be the Jacobian of $\mathcal{C}$. Let $t : \mathcal{C} \to \mathbb{P}^1$ be a finite K-morphism which is totally ramified at some K-rational point of $\mathcal{C}$.*

Let $\mathcal{G}$ be a finite flat $\mathcal{O}_K$-group scheme, whose generic fiber $\mathcal{G}_K$ is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$ over $\bar{K}$, and let $r \geq 1$ be an integer such that $J(\mathcal{C})$ contains a subgroup scheme isomorphic to $(\mathcal{G}_K^D)^r$.

Then there exist an infinity of number fields L/K with $[L : K] = \deg(t)$ such that the natural map

$$H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \longrightarrow H^1_{\mathrm{fl}}(\mathcal{O}_L, \mathcal{G}) \tag{16}$$

is injective, and satisfies

$$\mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_L, \mathcal{G})/H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \geq r. \tag{17}$$

The "infinity" in this theorem can be made quantitative as follows.

Theorem 4.7. *Let $t \in K(\mathcal{C})$ be the rational function defining the K-morphism $\mathcal{C} \to \mathbb{P}^1$ appearing in Theorem 4.6. Assume that there exists a rational function $x \in K(\mathcal{C})$ of degree m such that $K(\mathcal{C}) = K(t, x)$. Then, for sufficiently large positive X, there are at least $cX^{\ell/2m(d-1)}/\log X$ number fields L/K with $[L : K] = d$, $\mathcal{D}(L/K) \leq X$ and such that the map (16) is injective and satisfies (17). Here $\ell = [K : \mathbb{Q}]$ and $c > 0$ depends on $\mathcal{C}$, t, x and K.*

Proof of Theorem 4.6. The strategy of the proof is that of Theorem 2.4. of [14]. According to Lemma 4.5, we are able to choose r torsors

$$\psi_1 : X_1 \to \mathcal{C}, \dots, \psi_r : X_r \to \mathcal{C}$$

such that $\psi_i^{-1}(A)$ is trivial for all i, and the fiber product $X_1 \times_{\mathcal{C}} \cdots \times_{\mathcal{C}} X_r$ is geometrically irreducible.

We apply Theorem 4.3 to $\Psi : X_1 \times_{\mathcal{C}} \cdots \times_{\mathcal{C}} X_r \to \mathcal{C}$, which is a geometrically irreducible $\mathcal{G}_K^r$-torsor such that $\Psi^{-1}(A)$ is the trivial torsor. This proves the existence of infinitely many $P \in \mathcal{C}(\bar{K})$ with $[K(P) : K] = \deg(t)$ such that $\Psi^{-1}(P)$ is the spectrum of a field and extends into a flat $\mathcal{G}^r$-torsor over $\mathcal{O}_{K(P)}$. Then, for such points P, the torsors $\psi_1^{-1}(P), \dots, \psi_r^{-1}(P)$ can be extended into flat $\mathcal{G}$-torsors over $\mathcal{O}_{K(P)}$, and these torsors generate a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$ in $H^1(K(P), \mathcal{G}_K)$, hence:

$$\mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_{K(P)}, \mathcal{G}) \geq r.$$

Furthermore, according to Theorem 4.3, there are infinitely many isomorphism classes among the fields $K(P)$, and we may impose the additional requirement that $\Psi^{-1}(P)$ is the spectrum of a field which is linearly disjoint from a given finite extension F/K. Let us now choose F/K to be the compositum of all the fields $K(\xi)$, where ξ runs through $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G})$; this is a finite extension, because the group $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G})$ is finite, according to Hermite-Minkowski's Theorem. We note that all points of $\mathcal{G}_K$ are defined over F. The

map $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \to H^1_{\mathrm{fl}}(\mathcal{O}_{K(P)}, \mathcal{G})$ is injective because, $K(P)$ being linearly disjoint from F, a nontrivial $\mathcal{G}$-torsor over $\mathcal{O}_K$ cannot acquire a point over $K(P)$. Moreover, the image of $H^1_{\mathrm{fl}}(\mathcal{O}_K, \mathcal{G}) \to H^1_{\mathrm{fl}}(\mathcal{O}_{K(P)}, \mathcal{G})$ has trivial intersection with the subgroup generated by the $\psi_i^{-1}(P)$, because the compositum of the corresponding fields are linearly disjoint. Hence the result. □

Remark 4.8. In the statement of Theorem 4.3, it is possible to enlarge the set S as one likes. Therefore, Theorem 4.6 still holds when replacing the flat cohomology groups by the étale ones, and more generally by the groups $H^1_{S\text{-split}}$ of S-split classes. In particular, one may impose the additional requirement that the torsors are unramified at infinite places.

Proof of Theorem 4.7. Our fields L occur as $K(P)$, where the points P are produced by a suitable special case of Theorem 4.3. The "quantitative statement" of the latter theorem implies that, for large positive B, there are at least $cB^\ell/\log B$ distinct fields among such $K(P)$ with $\mathrm{H}(P) \leq B$. Proposition 3.14 implies now that for every such $L = K(P)$ we have $\mathcal{D}(L/K) \leq c'B^{2m(d-1)}$. Setting here $B = X^{1/2m(d-1)}$, we obtain the result. □

4.3 Proof of Theorems 1.3, 1.4 and 1.5

If A is a finite abelian group, we denote by $A^\vee := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ its Pontryagin dual. The group $A^\vee$ being (non canonically) isomorphic to A, we have, for any integer n,

$$\mathrm{rk}_n\, A^\vee[n] = \mathrm{rk}_n\, A^\vee = \mathrm{rk}_n\, A.$$

Let us recall the following result [14, Lemma 2.6], that we shall extensively use below: if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence of n-torsion abelian groups, then we have

$$\mathrm{rk}_n\, B \geq \mathrm{rk}_n\, A + \mathrm{rk}_n\, C. \tag{18}$$

Moreover, if the exact sequence splits then the equality holds.

Proof of Theorem 1.4. Let $\mathcal{G} = \mathbb{Z}/n\mathbb{Z}$, then, according to class field theory, we have for any number field L a canonical isomorphism

$$H^1_{M_L^\infty\text{-split}}(\mathcal{O}_L, \mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Hom}(\mathrm{Cl}(L), \mathbb{Z}/n\mathbb{Z}) = \mathrm{Cl}(L)^\vee[n].$$

Indeed, for an archimedean place, splitting and being unramified are the same. In fact, one could replace M_L^∞ by the set of real archimedean places of L, since complex places never ramify.

Let $r = \mathrm{rk}_{\mu_n}\, J(\mathcal{C})$ be the maximal integer such that $J(\mathcal{C})$ has a subgroup scheme isomorphic to μ_n^r. Then Theorem 4.6, in the light of Remark 4.8, implies that there exist infinitely many fields L with $[L : K] = \deg(t) = d$ such that the map $\mathrm{Cl}(K)^\vee[n] \to \mathrm{Cl}(L)^\vee[n]$ is injective, and:

$$\mathrm{rk}_n\, \mathrm{Cl}(L)^\vee[n]/\, \mathrm{Cl}(K)^\vee[n] \geq r.$$

According to (18), this implies that

$$\mathrm{rk}_n\, \mathrm{Cl}(L)^\vee[n] \geq r + \mathrm{rk}_n\, \mathrm{Cl}(K)^\vee[n],$$

hence the result. □

Before we start the next proof, let us recall that Kummer theory (in flat topology) yields, for any number field L, an exact sequence

$$0 \longrightarrow \mathcal{O}_L^\times/n \longrightarrow H^1_{\mathrm{fl}}(\mathcal{O}_L, \mu_n) \longrightarrow \mathrm{Cl}(L)[n] \longrightarrow 0.$$

According to [13, Prop. 1.1], this exact sequence always splits. As pointed above, it follows that the inequality (18) is an equality:

$$\mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_L, \mu_n) = \mathrm{rk}_n(\mathcal{O}_L^\times/n) + \mathrm{rk}_n\, \mathrm{Cl}(L)[n]. \tag{19}$$

Proof of Theorem 1.3. Let $\mathcal{G} = \mu_n$, then we recover the situation considered in [14]. We note that $\mu_n^D = \mathbb{Z}/n\mathbb{Z}$, hence if we let $r = \mathrm{rk}_n\, J(\mathcal{C})(K)_{\mathrm{tors}}$ then $J(\mathcal{C})$ contains a subgroup isomorphic to $(\mu_n^D)^r$.

In this setting, Theorem 4.6 reads as follows: there exist infinitely many fields L with $[L : K] = \deg(t)$ such that $H^1(\mathcal{O}_K, \mu_n) \to H^1_{\mathrm{fl}}(\mathcal{O}_L, \mu_n)$ is injective and:

$$\mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_L, \mu_n)/H^1_{\mathrm{fl}}(\mathcal{O}_K, \mu_n) \geq \mathrm{rk}_n\, J(\mathcal{C})(K)_{\mathrm{tors}}.$$

According to (18), this implies that

$$\mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_L, \mu_n) - \mathrm{rk}_n\, H^1_{\mathrm{fl}}(\mathcal{O}_K, \mu_n) \geq \mathrm{rk}_n\, J(\mathcal{C})(K)_{\mathrm{tors}}.$$

According to (19), the left-hand side is equal to the following quantity:

$$\mathrm{rk}_n(\mathcal{O}_L^\times/n) - \mathrm{rk}_n(\mathcal{O}_K^\times/n) + \mathrm{rk}_n\, \mathrm{Cl}(L) - \mathrm{rk}_n\, \mathrm{Cl}(K).$$

Finally, let us point out that, by construction, the field L is linearly disjoint from the field $K(\zeta_n)$. In other terms, $\mu_n(K) = \mu_n(L)$, which implies that

$$\mathrm{rk}_n(\mathcal{O}_L^\times/n) - \mathrm{rk}_n(\mathcal{O}_K^\times/n) = \mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_L^\times - \mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_K^\times.$$

Putting all the pieces together we obtain:

$$\mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_L^\times - \mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_K^\times + \mathrm{rk}_n\, \mathrm{Cl}(L) - \mathrm{rk}_n\, \mathrm{Cl}(K) \geq \mathrm{rk}_n\, J(\mathcal{C})(K)_{\mathrm{tors}}.$$

which yields the required lower bound on $\mathrm{rk}_n\, \mathrm{Cl}(L)$. □

Proof of Theorem 1.5. It is an immediate consequence of Theorem 4.7. □

5 Applications and examples

In all our examples, $\mathcal{C}$ is a superelliptic curve, defined (over K) by an affine equation of the form

$$y^m = f(x),$$

where f is a separable polynomial with coefficients in K. If the degree of f is coprime to m, then the curve C has a unique point A_∞ at infinity, which is K-rational. Moreover, there are two natural functions $C \to \mathbb{P}^1$ whose unique zero is A_∞, namely:

(i) the map $(x, y) \mapsto 1/x$, which has degree m;

(ii) the map $(x, y) \mapsto 1/y$, which has degree $\deg f$.

Each of those is a natural candidate to play the role of the function t.

5.1 Mestre's example revisited

We briefly review the construction by Mestre [18] from which the present paper is inspired. For the reader's convenience, we stick to Mestre's notation.

In his paper, Mestre constructs:

1. a genus 5 hyperelliptic curve $\mathcal{C}$ defined over $\mathbb{Q}$, which admits three rational Weierstrass points;
2. three elliptic curves E_1, E_2 and E_3 defined over $\mathbb{Q}$, each of them endowed with an isogeny $\varphi_i : E_i \to F_i$ with kernel $\mathbb{Z}/5\mathbb{Z}$;
3. three independent Galois covers $\tau_i : \mathcal{C} \to F_i$ with group $(\mathbb{Z}/2\mathbb{Z})^2$.

The existence of the maps τ_i implies that the Jacobian of $\mathcal{C}$ splits, and that each of the F_i is an isogenus factor of $J(\mathcal{C})$ via an isogeny of degree 4. More precisely, there exists an abelian surface B and an isogeny

$$F_1 \times F_2 \times F_3 \times B \longrightarrow J(\mathcal{C})$$

whose degree is a power of 2.

On the other hand, the dual isogeny $\hat{\varphi}_i : F_i \to E_i$ has kernel μ_5 (the Cartier dual of the constant group scheme $\mathbb{Z}/5\mathbb{Z}$). Hence $J(\mathcal{C})$ contains μ_5^3 as a subgroup.

Let us apply Theorem 1.4 to this situation.

Theorem 5.1. *Let K be a number field. There exist infinitely many quadratic extensions L/K such that*

$$\mathrm{rk}_5\, \mathrm{Cl}(L) \geq 3 + \mathrm{rk}_5\, \mathrm{Cl}(K).$$

More precisely, for every large positive X there exist at least $cX^{\ell/22}$ such fields L with $\mathcal{D}(L/K) \leq X$. Here $\ell = [K : \mathbb{Q}]$ and c is an absolute positive constant.

When $K = \mathbb{Q}$, we recover Mestre's result.

5.2 Extensions of cyclotomic fields: proof of Theorem 1.7

Let us recall the following result of Greenberg [15, Theorem 1], obtained in his work on Jacobians of quotients of Fermat curves.

Theorem 5.2. *Let $p \geq 3$ be a prime, and let s be an integer such that $1 \leq s \leq p-2$. Let $\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field, and let $C_{p,s}$ be the curve defined by the affine equation*

$$y^p = x^s(1-x).$$

Then $J(C_{p,s})(\mathbb{Q}(\zeta_p))$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.

Theorem 1.7 is a simple consequence of this result and Theorem 1.4.

Proof of Theorem 1.7. Let us put $s := d-1$ and let $C_{p,s}$ be the curve defined in Theorem 5.2. Then the rational map $t : C_{p,s} \to \mathbb{P}^1$ defined by $t := 1/y$ has degree d. Because d is coprime to p, its unique zero is the point at infinity.

On the other hand, if $\zeta_p \in K$ then $\mu_p \simeq \mathbb{Z}/p\mathbb{Z}$ over K, hence over that field we have

$$\mathrm{rk}_{\mu_p} J(C_{p,s}) = \mathrm{rk}_p J(C_{p,s})(K).$$

According to Theorem 5.2, the right-hand side is at least 3. Therefore, the result follows from Theorem 1.4. □

In case $d \geq 5$, one can improve on Theorem 1.7 as follows.

Theorem 5.3. *Let p be a prime number, K a number field containing ζ_p, and let d be coprime to p. Then there exist infinitely many fields L/K with $[L : K] = d$ such that*

$$\mathrm{rk}_p \mathrm{Cl}(L) \geq d - 1 + \mathrm{rk}_p \mathrm{Cl}(K).$$

Proof. Let us consider the curve $\mathcal{C}$ defined by an equation of the form

$$y^p = (x - a_1) \dots (x - a_d)$$

where the a_i are pairwise distinct rational numbers. Then $J(\mathcal{C})(\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{d-1}$, which becomes isomorphic to $(\mu_p)^{d-1}$ over K. The result now follows from Theorem 1.4. □

We omit the "quantitative" version, which can be done in the same way as previously.

Remark 5.4. By considering the same curve over $\mathbb{Q}$, and applying Theorem 1.3 (instead of Theorem 1.4), one recovers the following result, due to Azuhata and Ichimura [1]: there exist infinitely many $L/\mathbb{Q}$ with $[L : \mathbb{Q}] = d$ such that $\mathrm{rk}_p \mathrm{Cl}(L) \geq \lfloor d/2 \rfloor$. In this result, the base field is $\mathbb{Q}$ instead of $\mathbb{Q}(\zeta_p)$, but the p-rank is half the degree, whereas in Theorem 5.3 the p-rank has the size of the degree.

References

[1] T. Azuhata, H. Ichimura, On the divisibility problem of the class numbers of algebraic number fields, *J. Fac. Sci. Univ. Tokyo* **30** (1984), 579–585.

[2] R. Benedetti, J.-J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, Paris, 1990.

[3] Yu. Bilu, Structure of sets with small sumsets, *Astérisque* **258** (1999), 77–108.

[4] Yu. Bilu, Counting number fields in fibers (with an appendix by J. Gillibert), *Math. Z.* (2017), doi:10.1007/s00209-017-1900-5.

[5] Yu. Bilu, A. Borichev, Remarks on Eisenstein, *J. Austral. Math. Soc* **94** (2013), 158–180.

[6] Yu. F. Bilu, F. Luca, Divisibility of class numbers: enumerative approach, *J. reine angew. Math.* **578** (2005), 79–91.

[7] Yu. Bilu, M. Strambi, A. Surroca, Quantitative Chevalley-Weil theorem for curves, *Monatsh. Math.* **171** (2013), 1–32.

[8] D. Brink, New light on Hensel's lemma, *Expo. Math.* **24** (2006), 291–306.

[9] K. Česnavičius, Selmer groups as flat cohomology groups, *Journal of the Ramanujan Mathematical Society*, to appear.

[10] P. Corvaja, U. Zannier, On the number of integral points on algebraic curves, *J. reine angew. Math.* **565** (2003), 27–42.

[11] H. Davenport, On a principle of Lipschitz, *J. London Math. Soc.* **26** (1951), 179-183; corrigendum: **39** (1964), 580.

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

[13] J. Gillibert, P. Gillibert, On the splitting of the Kummer exact sequence, submitted (2017), `arXiv:1705.08195[math.AG]`.

[14] J. Gillibert, A. Levin, Pulling back torsion line bundles to ideal classes, *Math. Research Letters* **19** (2012), no 6, 1171–1184.

[15] R. Greenberg, On the Jacobian variety of some algebraic curves, *Compositio Math.* **42** (1981), 345–359.

[16] A. Grothendieck, M. Artin and J. L. Verdier, Théorie des topos et cohomologie étale des schémas, Tome II, *Lecture Notes in Math.* **270** (Springer, 1972).

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

[18] J.-F. Mestre, Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3, *C. R. Acad. Sci. Paris (Série 1)* **315** (1992), 371–374.

[19] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Vieweg & Sohn, Braunschweig, 1997.

[20] S. H. Schanuel, Heights in number fields, *Bull. Soc. Math. France* **107** (1979), 433–449.

Yuri Bilu

Institut de Mathématiques de Bordeaux
351, cours de la Libération
33405 Talence Cedex, France

`yuri.bilu@math.u-bordeaux.fr`

Jean Gillibert

Institut de Mathématiques de Toulouse
118, route de Narbonne
31062 Toulouse Cedex 9, France

`jean.gillibert@math.univ-toulouse.fr`