FINITE WEIL RESTRICTION OF CURVES

E.V. FLYNN AND D. TESTA

Abstract. Given number fields $L \supset K$, smooth projective curves C defined over L and B defined over K, and a non-constant L-morphism $h\colon C \to B_L$, we denote by C_h the curve defined over K whose K-rational points parametrize the L-rational points on C whose images under h are defined over K. We compute the geometric genus of the curve C_h and give a criterion for the applicability of the Chabauty method to find the points of the curve C_h. We provide a framework which includes as a special case that used in Elliptic Curve Chabauty techniques and their higher genus versions. The set $C_h(K)$ can be infinite only when C has genus at most 1; we analyze completely the case when C has genus 1.

Introduction

Let L be a number field of degree d over $\mathbb{Q}$, let $f \in L[x]$ be a polynomial with coefficients in L, and define

$$A_f := \big\{x \in L \;\mid\; f(x) \in \mathbb{Q}\big\}.$$

Choosing a basis of L over $\mathbb{Q}$ and writing explicitly the conditions for an element of L to lie in A_f, it is easy to see that the set A_f is the set of rational solutions of $d-1$ polynomials in d variables. Thus we expect the set A_f to be the set of rational points of a (possibly reducible) curve C_f; indeed, this is always true when f is non-constant. A basic question that we would like to answer is to find conditions on L and f that guarantee that the set A_f is finite, and ideally to decide when standard techniques can be applied to explicitly determine this set.

We formalize and generalize the previous problem as follows. Let $L \supset K$ be a finite separable field extension, let $B \to \mathrm{Spec}(K)$ be a smooth projective curve defined over K and let C be a smooth projective curve defined over L. Denote by B_L the base-change to L of the curve B, and suppose that $h\colon C \to B_L$ is a non-constant morphism defined over L. Then there is a (possibly singular and reducible) curve C_h defined over K whose K-rational points parametrize the L-rational points $p \in C(L)$ such that $h(p) \in B(K) \subset B_L(L)$ (see Lemma 4). In this context, Theorem 11 identifies an abelian subvariety F of the Jacobian of the curve C_h and provides a formula to compute the rank of the Mordell-Weil group of F: these are the ingredients needed to apply the Chabauty method to determine the rational points of the curve C_h. To see the relationship of this general problem with the initial motivating question, we let $C := \mathbb{P}^1_L$ and $B := \mathbb{P}^1_{\mathbb{Q}}$. The polynomial f determines a morphism $h\colon \mathbb{P}^1_L \to (\mathbb{P}^1_{\mathbb{Q}})_L$ and the L-points of $\mathbb{P}^1_L$ (different from ∞) with image in $\mathbb{P}^1(\mathbb{Q})$ correspond to the set A_f.

Over an algebraic closure of the field L, the curve C_h is isomorphic to the fibered product of morphisms $h_i\colon C_i \to B_L$ obtained from the initial morphism h by taking Galois conjugates (Lemma 5). Thus we generalize further our setup: we concentrate our attention on the fibered product of finitely many morphisms $h_1\colon C_1 \to B$, …, $h_n\colon C_n \to B$, where $C_1, \ldots, C_n$ and B are smooth curves and the morphisms $h_1, \ldots, h_n$ are finite and separable. We determine the geometric

Date: 2 November, 2014.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Higher Genus Curves, Jacobians, Weil Restriction.

Both authors have been partially supported by EPSRC grant EP/F060661/1. The second author was also partially supported by EPSRC grant EP/K019279/1.

genus of the normalization of C_h (Theorem 7), as well as a natural abelian subvariety J_h of the Jacobian of C_h. Due to the nature of the problem and of the arguments, it is immediate to convert results over the algebraic closure to statements over the initial field of definition.

Suppose now that K is a number field. If the abelian variety J_h satisfies the condition that the rank of $J_h(K)$ is less than the genus of C_h, then we may use the Chabauty method to find the rational points on C_h; by Chabauty's Theorem (see [5–7]) this guarantees that $C_h(K)$ is finite. Chabauty's Theorem has been developed into a practical technique, which has been applied to a range of Diophantine problems, for example in [8, 9, 11, 16]. Further, if the set $C_h(K)$ is infinite, then, by Faltings' Theorem [10], the curve C_h contains a component of geometric genus at most one; thus the computation of the arithmetic genus of the normalization of C_h is a first step towards answering the question of whether $C_h(K)$ is finite or not. Moreover, since all the irreducible components of C_h dominate the curve C, it follows that the set $C_h(K)$ can be infinite only in the case in which the curve C has geometric genus at most one. In the case in which C has genus zero, results equivalent to special cases of this question have already been studied ([1, 2, 17, 19, 22]). We shall analyze completely the case in which the genus of C is one and the curve C_h has infinitely many rational points. This covers as a special case the method called Elliptic Curve Chabauty which is commonly applied to an elliptic curve E defined over a number field $L \supset K$, satisfying that the rank of $E(L)$ is less than $[L : K]$ and we wish to find all $(x, y) \in E(L)$ subject to an arithmetic condition such as $x \in K$; see, for example, [3, 4, 12, 13, 21] and a hyperelliptic version in [20].

Example 1. Let K be a number field and let $E\colon y^2 = (a_2x^2 + a_1x + a_0)(x + b_1 + b_2\sqrt{d})$, with $a_0, a_1, a_2, b_1, b_2, d \in K$, be an elliptic curve defined over $L = K(\sqrt{d})$; suppose also that $b_2 \neq 0$ and that d is not a square in K, so that E is not defined over K. We are interested in $(x, y) \in E(L)$ with $x \in K$. Let $y = r + s\sqrt{d}$, with $r, s \in K$. Equating coefficients of $1, \sqrt{d}$ gives

$$r^2 + ds^2 = (a_2x^2 + a_1x + a_0)(x + b_1), \quad 2rs = (a_2x^2 + a_1x + a_0)b_2.$$

Let $t = s^2/(a_2x^2 + a_1x + a_0)$. Eliminate r to obtain $\frac{(b_2)^2}{4t} + dt = x + b_1$, so that

$$x = x(t) = \frac{(b_2)^2}{4t} + dt - b_1.$$

Hence s, t satisfy the curve $C : (st)^2 = t^3(a_2x(t)^2 + a_1x(t) + a_0)$, for which the right hand side is a quintic in t. One can check directly that this quintic has discriminant whose factors are powers of a_0, b_2, d, the discriminant of E and its conjugate. All of these are guaranteed to be nonzero, from our assumptions, so that C has genus 2. By Faltings' Theorem, $C(K)$ is finite, so there are finitely many such $s, t \in K$, and hence finitely many $x = x(t)$, and so finitely many $(x, y) \in E(L)$ with $x \in K$. Furthermore, one can check directly from the induced map from C to E that, if J is the Jacobian of C then $\operatorname{rank}\big(J(K)\big) = \operatorname{rank}\big(E(L)\big)$; hence if $\operatorname{rank}\big(E(L)\big) < [L : K] = 2$ (the condition for Elliptic Curve Chabauty) then C satisfies the conditions for Chabauty's Theorem over K. So, for this special case, there is a perfect match between both conditions.

Example 2. Let $f \in \mathbb{Q}(\sqrt{2})[x]$ be the polynomial $f(x) = x^2(x - \sqrt{2})$ and suppose that we are interested in finding the set A_f of values of $x \in \mathbb{Q}(\sqrt{2})$ such that $f(x) \in \mathbb{Q}$. Writing $x = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ and substituting in f we find that $f(a + b\sqrt{2})$ is a rational number if and only if the equality $a^2 + 2b^2 = 3a^2b + 2b^3$ holds. Apart from the solution $(a, b) = (0, 0)$, all the remaining solutions of the resulting equation can be determined by the substitution $a = tb$ and the set A_f is the set

$$\left\{ \frac{t^2 + 2}{(3t^2 + 2)}(t + \sqrt{2}) \;\middle|\; t \in \mathbb{Q} \right\} \cup \{0\}.$$

Example 3. Let $f \in \mathbb{Q}(\sqrt{2})[x]$ be the polynomial $f(x) = \frac{x(x-\sqrt{2})}{x-1}$. Arguing similarly to the previous example, we find that the set values of $x \in \mathbb{Q}(\sqrt{2})$ such that $f(x) \in \mathbb{Q}$ consists of the solutions to the equation $a^2b - a^2 - 2ab + a - 2b^3 + 2b^2 = 0$. The projective closure of the previous equation defines an elliptic curve E with Weierstrass form $y^2 = x^3 - x$; by a 2-descent it is easy to show that $E(\mathbb{Q}) = E(\mathbb{Q})[2]$ and we conclude that the set we are seeking is the set $\{0, \sqrt{2}\}$.

The last two of these examples exhibit the two qualitative behaviours that we analyze in what follows.

Before beginning the technical details, we first identify what will be the main results in the upcoming sections. Theorem 7 in Section 2 is the main geometric result for potentially deciding if Faltings' Theorem applies; given smooth curves $S, C_1, \ldots, C_n$ and finite separable morphisms $f_i \colon C_i \to S$ whose ramification indices are coprime to the characteristic of k, it describes the arithmetic genus of the normalisation of $C_1 \times_S \cdots \times_S C_n$. We note that there has already been a significant application of this result; in [14], the authors prove that elliptic curves over real quadratic fields are modular, and in one of their steps they use our Theorem 7 (citing a preprint version of this article) in order to describe points on certain modular curves (see Section 16.1 of [14] for details). Theorem 11, summarised above, in Section 3 is the main result for applications of the Chabauty method (using the geometric input from Theorem 10). Corollary 15 is the main result for handling the case of curves of genus one.

1. Relative Weil Restriction

We begin this section by recalling the definition of the Weil restriction functor. The setup is quite general, though we will only use it in a very specialized context. We prefer to adopt this formal point of view at the beginning, since it simplifies the arguments; for the cases mentioned in the introduction, it is straightforward to translate all our arguments into explicit computations that are also easy to verify.

Let $s \colon S' \to S$ be a morphism of schemes and let X' be an S'-scheme; the contravariant functor

$$\begin{aligned} \mathfrak{R}_{S'/S}(X') \colon (\mathrm{Sch}/S)^o &\longrightarrow \mathrm{Sets} \\ T &\longmapsto \mathrm{Hom}_{S'}(T \times_S S', X') \end{aligned}$$

is the *Weil restriction functor*. If the functor $\mathfrak{R}_{S'/S}(X')$ is representable, then we denote by $\mathfrak{R}_{S'/S}(X')$ also the scheme representing $\mathfrak{R}_{S'/S}(X')$; sometimes, to simplify the notation, we omit the reference to S and S' and write that $\mathfrak{R}(X')$ is the Weil restriction of X'. The scheme $\mathfrak{R}(X')$ is determined by the isomorphism

$$\mathrm{Hom}_S(-, \mathfrak{R}(X')) \xrightarrow{\sim} \mathrm{Hom}_{S'}(- \times_S S', X')$$

of functors $(\mathrm{Sch}/S)^o \to \mathrm{Sets}$. Informally this means that the S-valued points of $\mathfrak{R}(X')$ are the same as the S'-valued points of X'.

Suppose now that $Y \to S$ is another morphism of schemes, denote by Y' the fibered product $Y \times_S S'$ with natural morphism $b \colon Y' \to Y$, and let $h \colon X \to Y'$ be any scheme. We have the diagram

(1)
$$\begin{array}{ccc} X & & \\ {\scriptstyle h}\downarrow & & \\ Y' & \xrightarrow{b} & Y \\ \downarrow & & \downarrow \\ S' & \xrightarrow{s} & S \end{array}$$

and X is therefore both a Y'-scheme and an S' scheme. Thus there are two possible Weil restrictions we can construct:

- the Weil restriction $\mathfrak{R}_{S'/S}(X)$, using the S'-scheme structure of X,
- the Weil restriction $\mathfrak{R}_{Y'/Y}(X)$, using the Y'-scheme structure of X.

Below we shall use the notation $\mathrm{Res}_h(X)$ for the Weil restriction $\mathfrak{R}_{Y'/Y}(X)$ and call it the *relative Weil restriction*.

In order to relate the Weil restriction $\mathfrak{R}_{Y'/Y}(X)$ to the discussion in the introduction, we give an alternative definition of this functor and then proceed to prove the equivalence of the two. For concreteness, suppose that in diagram (1) the morphism $S' \to S$ is induced by a (finite, separable) field extension $L \supset K$; then there is a subset of the L-points of X whose image under h is not simply an L-point of Y', but it is actually a K-point of Y. We would like to say that this set of L-points of X with K-rational image under h are the K-rational points of a scheme defined over K, and that this scheme *is* the relative Weil restriction of X. This is what we discussed in the introduction and we now formalize it.

Hence, let T be any S-scheme and denote by T' the S'-scheme $T \times_S S'$. Pull-back by the morphism s defines a function $\mathrm{Hom}_S(T, Y) \to \mathrm{Hom}_{S'}(T', Y')$; there is also a function $\mathrm{Hom}_{S'}(T', X) \to \mathrm{Hom}_{S'}(T', Y')$ determined by composition with h. Summing up, for any S-scheme T, we obtain a diagram

$$\begin{array}{ccc} \mathrm{Hom}(T, X/Y) & \dashrightarrow & \mathrm{Hom}_{S'}(T', X) \\ \downarrow & & \downarrow{\scriptstyle h\circ -} \\ \mathrm{Hom}_S(T, Y) & \xrightarrow{s^*} & \mathrm{Hom}_{S'}(T', Y'). \end{array} \tag{2}$$

We denote by $\mathrm{Hom}(T, X/Y)$ the pull-back of diagram (2), and we define the *relative Weil restriction functor* to be the functor

$$\begin{array}{rcl} \mathrm{Res}_h \colon (\mathrm{Sch}/S)^o & \longrightarrow & \mathrm{Sets} \\ T & \longmapsto & \mathrm{Hom}(T, X/Y). \end{array}$$

If the functor Res_h is representable, we denote a scheme representing it by $\mathrm{Res}_h(X)$.

Lemma 4. *Let $s \colon S' \to S$ be a morphism of schemes. Let X be an S'-scheme and let Y be an S-scheme; denote by $Y_{S'}$ the S'-scheme $Y \times_S S'$. Let $h \colon X \to Y_{S'}$ be an S'-morphism and assume that both Weil restriction functors $\mathfrak{R}(X)$ and $\mathfrak{R}(Y_{S'})$ are representable (notation as in (1)). Then the relative Weil restriction functor $\mathrm{Res}_h \colon (\mathrm{Sch}/S)^o \to \mathrm{Sets}$ is representable and the schemes $\mathrm{Res}_h(X)$ and $\mathfrak{R}_{Y'/Y}(X)$ coincide. Moreover, there is a commutative diagram of S-schemes*

$$\begin{array}{ccc} \mathrm{Res}_h(X) & \longrightarrow & \mathfrak{R}(X) \\ \downarrow & & \downarrow{\scriptstyle h'} \\ Y & \xrightarrow{\iota} & \mathfrak{R}(Y_{S'}) \end{array} \tag{3}$$

exhibiting $\mathrm{Res}_h(X)$ as a fibered product of $\mathfrak{R}(X)$ and Y over $\mathfrak{R}(Y_{S'})$.

Proof. We begin by constructing an S-morphism $h' \colon \mathfrak{R}(X) \to \mathfrak{R}(Y_{S'})$. By representability of $\mathfrak{R}(Y_{S'})$ and of $\mathfrak{R}(X)$ there are natural bijections

$$\begin{array}{rcll} \mathrm{Hom}_S(\mathfrak{R}(X), \mathfrak{R}(Y_{S'})) & \xrightarrow{\sim} & \mathrm{Hom}_{S'}(\mathfrak{R}(X)_{S'}, Y_{S'}) & \text{and} \\ \mathrm{Hom}_S(\mathfrak{R}(X), \mathfrak{R}(X)) & \xrightarrow{\sim} & \mathrm{Hom}_{S'}(\mathfrak{R}(X)_{S'}, X). & \end{array}$$

Let $\gamma \in \mathrm{Hom}_{S'}(\mathfrak{R}(X)_{S'}, X)$ be the S'-morphism corresponding to the identity in $\mathrm{Hom}_S(\mathfrak{R}(X), \mathfrak{R}(X))$ and let $h' \colon \mathfrak{R}(X) \to \mathfrak{R}(Y_{S'})$ be the S-morphism corresponding to $h \circ \gamma \in \mathrm{Hom}_{S'}(\mathfrak{R}(X)_{S'}, Y_{S'})$. Note

also that there is an S-morphism $\iota\colon Y \to \mathfrak{R}(Y_{S'})$ corresponding to the identity in $\mathrm{Hom}_{S'}(Y_{S'}, Y_{S'})$. Define $\mathrm{Res}_h(X) := Y \times_{\mathfrak{R}(Y_{S'})} \mathfrak{R}(X)$ so that there is a commutative diagram as in (3). To check that $\mathrm{Res}_h(X)$ represents Res_h, let T be any S-scheme; we have

$$\begin{aligned}\mathrm{Hom}_S(T, \mathrm{Res}_h(X)) &= \mathrm{Hom}_S(T, Y) \times_{\mathrm{Hom}_S(T, \mathfrak{R}(Y_{S'}))} \mathrm{Hom}_S(T, \mathfrak{R}(X)) \\ &= \mathrm{Hom}_S(T, Y) \times_{\mathrm{Hom}_S(T, \mathfrak{R}(Y_{S'}))} \mathrm{Hom}_{S'}(T_{S'}, X) = \mathrm{Hom}(T, X/Y),\end{aligned}$$

as required. Thus, the scheme $\mathrm{Res}_h(X)$ defined above represents the functor Res_h and is obtained by the fibered product (3).

Finally, we check that the schemes $\mathrm{Res}_h(X)$ and $\mathfrak{R}_{Y'/Y}(X)$ coincide. Let T be any Y-scheme; we have $T \times_Y Y' = T \times_Y (Y \times_S S') = (T \times_Y Y) \times_S S' = T \times_S S'$ and

$$\begin{aligned}\mathrm{Hom}_Y(T, \mathfrak{R}(X)) &= \mathrm{Hom}_{Y'}(T \times_Y Y', X) = \mathrm{Hom}_{Y'}(T \times_S S', X) \\ &= \left\{ f \in \mathrm{Hom}_{S'}(T \times_S S', X) \;\middle|\; h \circ f = s^*(T_Y \to Y) \right\} \\ &= \mathrm{Hom}(T, X/Y) = \mathrm{Hom}_Y(T, \mathrm{Res}_h(X)).\end{aligned}$$

We conclude using Yoneda's Lemma that $\mathrm{Res}_h(X)$ and $\mathfrak{R}_{Y'/Y}(X)$ coincide, and hence the lemma follows. □

Informally, we may describe the scheme $\mathrm{Res}_h(X)$ as the scheme whose S-valued points correspond to the points in $X(S')$ lying above the points in $Y(S)$.

Observe that, by the construction of $\mathrm{Res}_h(X)$ and diagram (3), there is an S'-morphism $\mathrm{Res}_h(X)_{S'} \to X$. The morphism $\mathrm{Res}_h(X)_{S'} \to X$ will prove useful later.

We now introduce some notation that is used in the following lemma. Let $L \supset K$ be a finite, separable field extension of degree n, and let K^{s} be a separable closure of K. Set $S' := \mathrm{Spec}(L)$, $S := \mathrm{Spec}(K)$, and $S^{\mathrm{s}} := \mathrm{Spec}(K^{\mathrm{s}})$, denote by $s\colon S' \to S$ the morphism of schemes corresponding to the extension $L \supset K$ and suppose that $\varphi_1, \ldots, \varphi_n\colon S^{\mathrm{s}} \to S'$ are the morphisms corresponding to all the distinct embeddings of L into K^{s} fixing K. Given an S'-scheme X, we denote by $X_1, \ldots, X_n$ the S^{s}-schemes obtained by pulling back $X \to S'$ under the morphisms $\varphi_1, \ldots, \varphi_n$.

Lemma 5. *Let X be an S'-scheme and let Y be an S-scheme. Let $h\colon X \to Y_{S'}$ be an S'-morphism and assume that both Weil restriction functors $\mathfrak{R}(X)$ and $\mathfrak{R}(Y_{S'})$ are representable. Then the isomorphism*

$$\mathrm{Res}_h(X)_{S^{\mathrm{s}}} \simeq X_1 \times_{Y_{S^{\mathrm{s}}}} X_2 \times_{Y_{S^{\mathrm{s}}}} \cdots \times_{Y_{S^{\mathrm{s}}}} X_n \tag{4}$$

holds. More precisely, the isomorphism (4) *holds replacing K^{s} by any normal field extension of K containing L.*

Proof. To prove the result, it suffices to consider the case in which both X and Y are affine; thus suppose that $Y = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$, and that $\underline{x}$ denotes a set of generators of B as an A-algebra.

Let $\alpha_1, \ldots, \alpha_n$ denote a basis of K over L and let $\underline{x}_1, \ldots, \underline{x}_n$ denote disjoint sets of variables each in bijection with $\underline{x}$; whenever we denote a variable in $\underline{x}$ by a symbol such as x, we denote by the symbols $x_1, \ldots x_n$ the variables corresponding to x in $\underline{x}_1, \ldots, \underline{x}_n$. For every $x \in \underline{x}$ define linear forms $\tilde{x}_1 := \sum_i x_i \varphi_1(\alpha_i), \ldots, \tilde{x}_n := \sum_i x_i \varphi_n(\alpha_i)$ in $A[\underline{x}_1, \ldots, \underline{x}_n]$. First we show that the forms $\tilde{x}_1, \ldots, \tilde{x}_n$ are linearly independent. Indeed, let Δ be the matrix whose (i, j) entry is $\varphi_j(\alpha_i)$; the (i, j) entry of $\Delta\Delta^t$ is $\sum_k \varphi_k(\alpha_i \alpha_j) = \mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$. Thus the determinant of $\Delta\Delta^t$ is equal to the discriminant of L over K, and it is therefore non-zero. We deduce that the matrix Δ is invertible and that the forms $\tilde{x}_1, \ldots, \tilde{x}_n$ are independent. Thus, defining $\underline{\tilde{x}}_j := \{\tilde{x}_j \mid x \in \underline{x}\}$ for $j \in \{1, \ldots, n\}$, we proved that there is an isomorphism $K^{\mathrm{s}} \otimes_K A[\underline{x}_1, \ldots, \underline{x}_n] \simeq K^{\mathrm{s}} \otimes_K A[\underline{\tilde{x}}_1, \ldots, \underline{\tilde{x}}_n]$.

The relative Weil restriction of X may be defined as follows. Let $g(\underline{x})$ be an element of the polynomial ring $A[\underline{x}]$ contained in the ideal defining X; evaluate $g(\underline{x})$ substituting for each variable $x \in \underline{x}$ the sum $\sum x_i\alpha_i$ and write the resulting polynomial in $L \otimes_K A[\underline{x}_1, \dots, \underline{x}_n]$ as $\sum g_i\alpha_i$, where $g_1, \dots, g_n$ are elements of $A[\underline{x}_1, \dots, \underline{x}_n]$; denote the sequence $(g_1, \dots, g_n)$ by $\tilde{g}$. Then the scheme $\mathrm{Res}(X)$ is the scheme in $\mathrm{Spec}(A[\underline{x}_1, \dots, \underline{x}_n])$ whose ideal is the ideal generated by the elements of $\tilde{g}$, as g varies among all the elements of the ideal defining X. It is therefore clear that the ideal I defining $\mathrm{Res}(X)$ in $K^{\mathrm{s}} \otimes_K A[\underline{x}_1, \dots, \underline{x}_n]$ contains, for every embedding $\varphi\colon L \to K^{\mathrm{s}}$ fixing K, the elements $\sum_i g_i\varphi(\alpha_i) = \varphi\bigl(\sum g_i\alpha_i\bigr) = \varphi(g)$, and conversely that the ideal containing all such elements contains $g_1, \dots, g_n$ and hence it contains I. Let $\mathscr{F} \in A[\underline{x}]$ be a set of generators of the ideal of X; since, for $i \in \{1, \dots, n\}$, the scheme X_i is defined by $\{\varphi_i(f) \mid f \in \mathscr{F}\}$ in $A[\underline{\tilde{x}}_i]$ the result follows. □

2. The case of curves over an algebraically closed field

In this section we compute the geometric genus of the relative Weil restriction $\mathscr{C}$ of a curve and we also determine a natural abelian variety isogenous to a subvariety of the Jacobian of $\mathscr{C}$.

Let C be a reduced and possibly reducible curve. The geometric genus $p_g(C)$ of C is the arithmetic genus of the normalization of the curve itself. For instance, if C is a reduced curve and $C_1, \dots, C_r$ are the geometric irreducible components of C with geometric genera $g_1, \dots, g_r$, then the geometric genus of C is $g_1 + \cdots + g_r - (r-1)$. In particular, let $f\colon C \to B$ be a finite separable morphism from a reduced curve C to a smooth curve B and let $f^\nu\colon C^\nu \to B$ denote the composition of the morphism f with the normalization map $C^\nu \to C$. Applying the Hurwitz formula in [15, Corollary 2.4] to each irreducible component of C we find that the Hurwitz formula holds for C as well:

$$2p_g(C) - 2 = \deg(f^\nu)(2p_g(B) - 2) + \deg R,$$

where $\deg(f^\nu)$ is the sum of the degrees of the morphism f^ν restricted to the irreducible components of C^ν and R is the ramification divisor of the morphism f^ν. Note that the geometric genus of a curve can therefore be negative, but this then implies that the curve itself is reducible (and has at least two irreducible components of geometric genus zero).

To calculate the geometric genus in Theorem 7 we may clearly assume that the ground field is algebraically closed; the proof reduces the computation to the étale local case, settled in Lemma 6.

Lemma 6. *Let n be a positive integer. Suppose that k is an algebraically closed field and that $r_1, \dots, r_n$ are positive integers relatively prime with the characteristic of k. Let R be the least common multiple of $r_1, \dots, r_n$ and let $C \subset \mathbb{A}^{n+1}_{x,y_1,\dots,y_n}$ be the affine scheme defined by*

$$C\colon \begin{cases} y_1^{r_1} &= x, \\ &\vdots \\ y_n^{r_n} &= x. \end{cases}$$

The scheme C has $\frac{r_1 \cdots r_n}{R}$ irreducible components and the morphism induced by the projection onto the x-axis from the normalization of each component ramifies at the origin to order R.

Proof. Observe that the curve C carries the action ρ of $\mathbb{G}_m$ defined by

$$t \cdot (x, y_1, \dots, y_n) = (t^R x, t^{R/r_1} y_1, \dots, t^{R/r_n} y_n).$$

First we show that the action ρ has trivial stabilizer at all points of C different from the origin. Indeed, let $q = (x, y_1, \dots, y_n)$ be a point of C different from the origin; it follows that all the coordinates of q are non-zero and the equality $(x, y_1, \dots, y_n) = (t^R x, t^{R/r_1} y_1, \dots, t^{R/r_n} y_n)$ implies that t is a root of unity of order dividing $\gcd(R/r_1, \dots, R/r_n) = 1$. Thus the complement of the origin in C is a principal homogeneous space for $\mathbb{G}_m$. There are $r_1 \cdots r_n$ points on C such that $x = 1$

and these are stabilized precisely by the action of the R-th roots of unity; we deduce that C consists of $\frac{r_1\cdots r_n}{R}$ irreducible components, each isomorphic to closure of the orbit of a point $(1,\eta_1,\ldots,\eta_n)$, where η_i is an r_i-th root of unity, for $i\in\{1,\ldots,n\}$. Therefore the normalization of C consists of $\frac{r_1\cdots r_n}{R}$ components each mapping to the x-axis by $(t^R,\eta_1 t^{R/r_1},\ldots,\eta_n t^{R/r_n})\mapsto t^R$, as required. □

Theorem 7. *Let k be an algebraically closed field and let n be a positive integer. Suppose that $S,C_1,\ldots,C_n$ are smooth curves; for $i\in\{1,\ldots,n\}$ let $f_i\colon C_i\to S$ be a finite separable morphism whose ramification indices are coprime to the characteristic of k. Let f denote the morphism of the curve $C:=C_1\times_S\cdots\times_S C_n$ to S, and let C' be the normalization of C; denote by g_S and $g_{C'}$ the arithmetic genera of S and C' respectively. For any point $p\in C$ and any $i\in\{1,\ldots,n\}$ denote by $r_i=r_i(p)$ the ramification index of f_i at the point corresponding to p and let $R=R(p):=\operatorname{lcm}\{r_1(p),\ldots,r_n(p)\}$. Then the curve C is a local complete intersection and the curve C' has arithmetic genus*

$$\begin{aligned} g_{C'} &= 1+(g_S-1)\prod_{i=1}^n\deg(f_i)+\frac{1}{2}\sum_{p\in C}r_1(p)\cdots r_n(p)\left(1-\frac{1}{R(p)}\right)\\ &= 1+\frac{1}{2}(r-2g_S-2)\prod_{i=1}^n\deg(f_i)-\frac{1}{2}\sum_{p\in f^{-1}(R_f)}\frac{r_1(p)\cdots r_n(p)}{R(p)}\end{aligned}$$

where $R_f\subset S$ is the union of the sets of branch points of the morphisms $f_1,\ldots,f_n$ and r is the cardinality of R_f.

Proof. Let $\pi\colon C'\to S$ be the morphism induced by the structure morphism $f\colon C\to S$. Let $p'\in C'$ be a closed point, let p be the corresponding point of C and let $p_1,\ldots,p_n$ be the points of $C_1,\ldots,C_n$ respectively corresponding to p. We prove the result by finding a local model of C near p which is a local complete intersection, and then applying the Hurwitz formula to the morphism induced by f on the normalization of such a model. Choosing a local coordinate x on S near $\pi(p')$ we reduce to the case in which S is $\mathbb{A}^1$ and $\pi(p')=0$. Similarly choose local coordinates $z_1,\ldots,z_n$ on $C_1,\ldots,C_n$ near $p_1,\ldots,p_n$ respectively. Thus, near p, the curve C is defined by

$$C\colon\begin{cases} z_1^{r_1}\varphi_1(z_1) &= x,\\ &\vdots\\ z_n^{r_n}\varphi_n(z_n) &= x,\end{cases}$$

where $(\varphi_1,\ldots,\varphi_n)$ is a rational function on C defined and non-zero at p, and $r_1,\ldots,r_n$ are the local ramification indices. In particular, the curve C is a local complete intersection near p. Denote by $\mathcal{O}_p$ the local ring of C near p; the base-change defined by the inclusion

$$\mathcal{O}_p\longrightarrow\mathcal{O}_p[t_1,\ldots,t_n]/\big(t_1^{r_1}-\varphi_1(z_1),\ldots,t_n^{r_n}-\varphi_n(z_n)\big)$$

is finite étale (of degree $r_1\cdots r_n$) by the assumption that the ramification indices are relatively prime to the characteristic of the field k. Hence, each component of the resulting curve is locally isomorphic to the curve $C_p\subset\mathbb{A}^{n+1}_{x,y_1,\ldots,y_n}$ defined by

$$C_p\colon\begin{cases} y_1^{r_1} &= x,\\ &\vdots\\ y_n^{r_n} &= x,\end{cases}$$

where $y_1=z_1t_1,\ldots,y_n=z_nt_n$. The morphism induced by π on C_p is the morphism induced by the coordinate x. Using Lemma 6, we conclude that the contribution of the point p to the Hurwitz

formula is $\frac{r_1\cdots r_n}{R}(R-1) = r_1\cdots r_n(1-\frac{1}{R})$, and hence we obtain

$$2g_C - 2 = (2g_S - 2)\prod \deg(f_i) + \sum_{p\in C} r_1(p)\cdots r_n(p)\left(1 - \frac{1}{R(p)}\right)$$

and the first formula follows. To prove the second one note that the quantity $r_1(p)\cdots r_n(p)(1-\frac{1}{R(p)})$ vanishes for $p \notin R_f$, since in this case all the local ramification indices equal 1, and that for all points s of S we have

$$\sum_{p\in f^{-1}(s)} r_1(p)\cdots r_n(p) = \prod_{i=1}^{n}\sum_{p\in f_i^{-1}(s)} r_i(p) = \prod \deg(f_i)$$

and we conclude. □

In the next results, for a projective scheme Y, we denote by $\mathrm{Jac}(Y)$ the *Jacobian variety of* Y, that is the connected component of the identity of the group $\mathrm{Pic}(Y)$.

Lemma 8. *Suppose that $X_1,\dots,X_n$ are smooth projective varieties defined over an algebraically closed field k and let $X = X_1\times\cdots\times X_n$. For $i\in\{1,\dots,n\}$ let $\rho_i\colon X\to X_i$ denote the canonical projection. The morphism*

$$\rho_\bullet^* = (\rho_1^*,\dots,\rho_n^*)\colon \mathrm{Jac}(X_1)\times\cdots\times\mathrm{Jac}(X_n)\to\mathrm{Jac}(X)$$

is an isomorphism.

Proof. Choosing a point in each variety $X_1,\dots,X_n$ allows us to define, for $i\in\{1,\dots,n\}$, an inclusion $X_i\hookrightarrow X$. These inclusions in turn determine a section $\mathrm{Jac}(X)\to\mathrm{Jac}(X_1)\times\cdots\times\mathrm{Jac}(X_n)$ of the morphism $\rho_\bullet^*$. We deduce that $\rho_\bullet^*$ is indeed an isomorphism of Jacobian varieties $\mathrm{Jac}(X_1)\times\cdots\times\mathrm{Jac}(X_n)\simeq\mathrm{Jac}(X)$. □

Remark 9. Maintaining the notation of the previous lemma, the morphisms $\rho_1,\dots,\rho_n$ also induce a homomorphism $\psi^*\colon\mathrm{Pic}(X_1)\times\cdots\times\mathrm{Pic}(X_n)\to\mathrm{Pic}(X)$. The morphism ψ though need not be an isomorphism. Since ψ induces an isomorphism on the connected component of the identity, it factors through the Néron-Severi group and in particular its cokernel is a finitely generated abelian group. For instance, if E is an elliptic curve and $X_1 = X_2 = E$, then the three classes $\{0\}\times E$, $E\times\{0\}$ and the diagonal are independent in $\mathrm{NS}(E\times E)$ so that $\mathrm{NS}(E\times E)\supset\mathbb{Z}^3$. On the other hand, the group $\mathrm{NS}(E)\times\mathrm{NS}(E)$ is isomorphic to $\mathbb{Z}^2$.

For the next theorem we need to introduce some notation. Suppose that $B, X_1,\dots,X_n$ are smooth projective varieties defined over an algebraically closed field k. For each $i\in\{1,\dots,n\}$ let $f_i\colon X_i\to B$ be a finite morphism. Denote by X the product $X_1\times\cdots\times X_n$, by X_B the fibered product $X_1\times_B\cdots\times_B X_n$ and by $\iota\colon X_B\to X$ the natural inclusion. For each $i\in\{1,\dots,n\}$

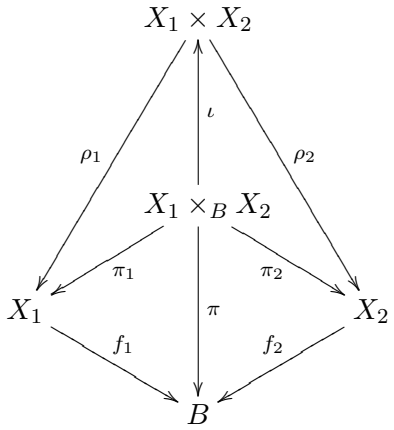
- let d_i denote the degree of f_i,
- let $\rho_i\colon X\to X_i$ and $\pi_i = \rho_i\circ\iota\colon X_B\to X_i$ be the canonical projections,
- let $\pi\colon X\to B$ be the composition $f_1\circ\pi_1 = \cdots = f_n\circ\pi_n$,
- let $d = d_1\cdots d_n$ denote the degree of π.

We summarize the notation in the case $n = 2$ in (5).

(5)

$$X := X_1 \times X_2$$

$$X_B := X_1 \times_B X_2$$



Warning. Even though the diagram may suggest it, the identities $f_1 \circ \rho_1 = \cdots = f_n \circ \rho_n$ *do not* hold necessarily. On the other hand, the identities $f_1 \circ \pi_1 = \cdots = f_n \circ \pi_n = \pi$ hold.

Let $\phi\colon \mathrm{Jac}(X) \to \mathrm{Jac}(X)$ be the isogeny defined by

$$\begin{array}{rccc} \phi\colon & \mathrm{Jac}(X) & \longrightarrow & \mathrm{Jac}(X) \\ & \rho_1^* D_1 + \cdots + \rho_n^* D_n & \longmapsto & \frac{d}{d_1} D_1 + \cdots + \frac{d}{d_n} D_n, \end{array}$$

where we used the identification of $\mathrm{Jac}(X)$ with $\mathrm{Jac}(X_1) \times \cdots \times \mathrm{Jac}(X_n)$ of Lemma 8.

Let M' denote the kernel of the multiplication map $\mathrm{Jac}(B)^n \to \mathrm{Jac}(B)$, so that $M' \simeq \mathrm{Jac}(B)^{n-1}$; define the group M as the image of M' under the morphism

$$\begin{array}{rcl} \mathrm{Jac}(B)^n & \longrightarrow & \mathrm{Jac}(X) \\ (D_1, \ldots, D_{n-1}) & \longmapsto & \rho_1^* f_1^* D_1 + \cdots + \rho_n^* f_n^* D_n. \end{array}$$

By construction, the group M is connected and contained in the kernel of ι^*. Moreover, it follows from Lemma 8 and the fact that the morphisms $f_1, \ldots, f_n$ are finite that the morphism $M' \to M$ is finite and hence that the dimension of the group M is $(n-1)\dim(\mathrm{Jac}(B))$.

Theorem 10. *Maintaining the notation introduced above, the group M has finite index in $\ker(\iota^*)$. More precisely, for each element D of $\ker(\iota^*)$ there are elements $D_1, \ldots, D_n$ of $\mathrm{Jac}(B)$ such that the identities*

$$\begin{array}{rcl} \phi(D) & = & \sum_i \rho_i^* f_i^* D_i \qquad \textit{and} \\ d \sum_i D_i & = & 0 \end{array}$$

hold. In particular, the dimension of the kernel of ι^* is $(n-1)\dim(\mathrm{Jac}(B))$.

Proof. By Lemma 8, the morphism

$$\begin{array}{rcl} \mathrm{Jac}(X_1) \times \cdots \times \mathrm{Jac}(X_n) & \longrightarrow & \mathrm{Jac}(X) \\ (D_1, \ldots, D_n) & \longmapsto & \rho_1^* D_1 + \cdots + \rho_n^* D_n \end{array}$$

is an isomorphism. Thus we identify the divisor classes in $\mathrm{Jac}(X)$ with n-tuples of divisor classes, one in each Jacobian variety $\mathrm{Jac}(X_1), \ldots, \mathrm{Jac}(X_n)$. Let i, j be distinct indices in $\{1, \ldots, n\}$ and let P be a divisor on X_i; it is easy to check that the identities

$$\begin{array}{rcl} \pi_{i*}\pi_i^*(P) & = & \dfrac{d}{d_i} P\,, \\ \pi_{i*}\pi_j^*(P) & = & \dfrac{d}{d_i d_j} f_i^* f_{j*}(P) \end{array}$$

hold, and hence the class of the divisor $\pi_{i*}\pi_j^*(P)$ is contained in $f_i^*\mathrm{Pic}(B)$. Suppose that $D = \rho_1^*D_1 + \cdots + \rho_n^*D_n$ is a divisor on X representing an element of $\mathrm{Jac}(X)$. Let i be an index in $\{1, \ldots, n\}$; we have

$$\pi_{i*}\iota^*(D) = \pi_{i*}(\pi_1^*D_1 + \cdots + \pi_n^*D_n) \in \frac{d}{d_i}D_i + f_i^*\mathrm{Jac}(B)$$

and summing over all indices i, we find the equivalence

$$\begin{aligned}\sum_i \pi_{i*}\iota^*(D) &\equiv \sum_i \frac{d}{d_i}D_i \\ &\equiv \phi(D) \pmod{f_1^*\mathrm{Jac}(B) \times \cdots \times f_n^*\mathrm{Jac}(B)}.\end{aligned}$$

In particular, if D is contained in the kernel of ι^*, then $\phi(D)$ is contained in $f_1^*\mathrm{Jac}(B) \times \cdots \times f_n^*\mathrm{Jac}(B)$, establishing the first of the two identities. Finally, let $D_1, \ldots, D_n \in \mathrm{Jac}(B)$ be divisor classes such that the element $\rho_1^*f_1^*D_1 + \cdots + \rho_n^*f_n^*D_n$ of $\mathrm{Jac}(X)$ lies in $\ker(\iota^*)$. Then, the element $D_1 + \cdots + D_n$ of $\mathrm{Jac}(B)$ lies in the kernel of π^*, so that $d(D_1 + \cdots + D_n) = \pi_*\pi^*(D_1 + \cdots + D_n) = 0$, proving the second identity.

It follows from what we just proved that the equalities

$$\dim(\ker(\iota^*)) = \dim M = (n-1)\dim(\mathrm{Jac}(B))$$

hold, proving the final assertion of the theorem. □

3. Mordell-Weil groups and relative Weil restriction

From now on, we shall be in the following set up (specializing the assumptions of Lemma 4):

- L is a number field and $S' := \mathrm{Spec}(L)$,
- $K \subset L$ is a subfield and $S := \mathrm{Spec}(K)$,
- C is a smooth projective curve over L,
- B is a smooth projective curve over K, and
- $h\colon C \to B_{S'} = B_L$ is a finite morphism.

To simplify the notation, for any variety Z defined over a number field k denote by $mw_k(Z)$ the rank of the Mordell-Weil group of the Jacobian of Z; we are only going to apply this notation with $k \in \{K, L\}$ to varieties Z that are either reduced curves or products of smooth integral curves.

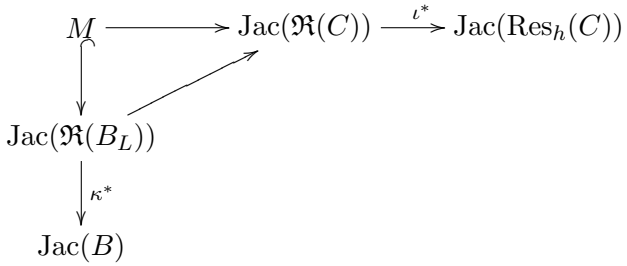
Theorem 11. *Suppose that C is a smooth projective curve defined over a number field L. Suppose that B is a smooth projective curve defined over a subfield K of L, and let $h\colon C \to B_L := B \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L)$ be a finite morphism. Denote by n the dimension of L as a vector space over K and by $g(C)$ and $g(B)$ the genera of C and B respectively. The Jacobian of $\mathrm{Res}_h(C)$ contains an abelian subvariety F of dimension $ng(C) - (n-1)g(B)$ defined over K and with Mordell-Weil group over K of rank $mw_L(C) - \big(mw_L(B_L) - mw_K(B)\big)$.*

Proof. The L-morphism $h\colon C \to B_L$ induces a K-morphism $\mathfrak{R}(C) \to \mathfrak{R}(B_L)$ which in turn induces a pull-back K-morphism $\mathrm{Jac}(\mathfrak{R}(B_L)) \to \mathrm{Jac}(\mathfrak{R}(C))$. Furthermore, from the inclusion $\iota\colon \mathrm{Res}_h(C) \subset \mathfrak{R}(C)$ we obtain a sequence of K-morphisms

$$\mathrm{Jac}(\mathfrak{R}(B_L)) \longrightarrow \mathrm{Jac}(\mathfrak{R}(C)) \xrightarrow{\iota^*} \mathrm{Jac}(\mathrm{Res}_h(C)).$$

From the representability of $\mathfrak{R}(B_L)$, there is a K-morphism $\kappa\colon B \to \mathfrak{R}(B_L)$ associated to the identity $B_L \to B_L$ using the bijection $\mathrm{Hom}_K(B, \mathfrak{R}(B_L)) = \mathrm{Hom}_L(B_L, B_L)$. The morphism κ induces a pull-back K-morphism $\kappa^*\colon \mathrm{Jac}(\mathfrak{R}(B_L)) \to \mathrm{Jac}(B)$; we denote by M the kernel of the morphism of κ^*. Geometrically, the Jacobian of $\mathfrak{R}(B_L)$ is isomorphic to the product of n copies of the Jacobian of B and the morphism κ^* corresponds to the addition of the line bundles in the various components using the isomorphisms between them (defined over an algebraic closure of

K). We obtain that the group M is the specialization to our setting of the group denoted also by M in Theorem 10. Therefore M is geometrically isomorphic to $\mathrm{Jac}(B)^{n-1}$, and it is connected of dimension $(n-1)g(B)$. Thus we obtain the diagram



of K-morphisms and it follows from Theorem 10 that the group M has finite index in $\ker(\iota^*)$. We let F be the connected component of the identity of the image of ι^* and we show that it has the required properties. First of all, F is an abelian variety over K, isogenous over K to $\mathrm{Jac}(\mathfrak{R}(C))/M$, and hence the dimension of F is

$$\dim(F) = \dim\left(\frac{\mathrm{Jac}(\mathfrak{R}(C))}{M}\right) = ng(C) - (n-1)g(B)$$

as needed. Next, we prove the statement about the Mordell-Weil rank of F. For a curve D defined over L we have

$$\begin{aligned} mw_K\big(\mathfrak{R}(D)\big) &= \mathrm{rk}\Big(\mathrm{Jac}\big(\mathfrak{R}(D)\big)(K)\Big) \\ &= \mathrm{rk}\Big(\mathrm{Hom}_K\Big(\mathrm{Spec}(K), \mathrm{Jac}\big(\mathfrak{R}(D)\big)\Big)\Big) \\ &= \mathrm{rk}\Big(\mathrm{Hom}_K\Big(\mathrm{Spec}(K), \mathfrak{R}\big(\mathrm{Jac}(D)\big)\Big)\Big) \\ &= \mathrm{rk}\Big(\mathrm{Hom}_L\big(\mathrm{Spec}(L), \mathrm{Jac}(D)\big)\Big) \\ &= mw_L(D). \end{aligned}$$

Since the abelian varieties F and $\mathrm{Jac}(\mathfrak{R}(C))/M$ are K-isogenous, the ranks of their Mordell-Weil groups are the same. By the previous computation we conclude that

$$\begin{aligned} \mathrm{rk}\big(F(K)\big) &= \mathrm{rk}\left(\frac{\mathrm{Jac}\big(\mathfrak{R}(C)\big)}{M}(K)\right) \\ &= mw_K\big(\mathfrak{R}(C)\big) - \Big(mw_K\big(\mathfrak{R}(B_L)\big) - mw_K(B)\Big) \\ &= mw_L(C) - \big(mw_L(B_L) - mw_K(B)\big), \end{aligned}$$

as required, and the result follows. □

The theorem just proved opens the way to applications of the Chabauty method to find the L-rational points of the curve C with K-rational image in B.

We show how this method works on an example.

Example 12. Let $d \neq 1$ be a squarefree integer; we let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$. Denote by $g(x) \in \mathbb{Q}[x]$ the polynomial

$$g(x) = x^3 + ax + b$$

and by $f(x) \in \mathbb{Q}(\sqrt{d})[x]$ the polynomial

$$f(x) = g(x^2 + \sqrt{d}).$$

Let E be the elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = g(x)$ and let C be the smooth projective model over $\mathbb{Q}(\sqrt{d})$ of the genus two hyperelliptic curve with affine equation $y^2 = f(x)$. By construction, there is a morphism $\phi\colon C \to E$ given by

$$\begin{aligned} \phi\colon C &\longrightarrow E \\ (x,y) &\longmapsto (x^2+\sqrt{d}, y). \end{aligned}$$

Suppose we wish to find all points P in $C\big(\mathbb{Q}(\sqrt{d})\big)$ such that $\phi(P)$ is in $E(\mathbb{Q})$. Such points are the rational points of the curve $D = \mathrm{Res}_\phi(C)$ over $\mathbb{Q}$, for which we now determine an explicit model. Let $x = x_1 + x_2\sqrt{d}$ and $y = y_1 + y_2\sqrt{d}$, where x_1, x_2, y_1, y_2 are $\mathbb{Q}$-rational variables. Substituting $x = x_1 + x_2\sqrt{d}$ and $y = y_1 + y_2\sqrt{d}$ in the polynomial defining C we find the polynomial

$$r(x_1,x_2,y_1,y_2) = (y_1 + y_2\sqrt{d})^2 - f(x_1 + x_2\sqrt{d})$$

in $\mathbb{Q}(\sqrt{d})$, whose vanishing represents the condition that the point $P = (x_1 + x_2\sqrt{d}, y_1 + y_2\sqrt{d})$ lies on C. Define polynomials with rational coefficients

$$r_1 := \frac{r + \overline{r}}{2} \quad \text{and} \quad r_2 := \frac{r - \overline{r}}{2\sqrt{d}}$$

where $\overline{r}$ denotes the polynomial obtained from r by applying the nontrivial element of the Galois group of $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$; we have the identity $r = r_1 + \sqrt{d}r_2$. Thus, the two equations $r_1 = r_2 = 0$ in x_1, y_1, x_2, y_2 correspond to P lying on C; these are also the equations defining (an affine model of) the Weil restriction of C from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}$. To determine $D = \mathrm{Res}_\phi(C)$, we also wish $\phi(P)$ to be in $E(\mathbb{Q})$. Note that the coordinates of $\phi(P)$ are

$$\phi(P) = \big(x_1^2 + dx_2^2 + \sqrt{d}(2x_1x_2+1), y_1 + \sqrt{d}y_2\big)$$

and the condition that the point $\phi(P)$ lies in $\mathbb{Q}$ translates to the equations $2x_1x_2 + 1 = y_2 = 0$. We have therefore obtained the four equations

$$(6) \qquad \begin{cases} y_1^2 &= (x_1^6 + d^3x_2^6) + 3(x_1^2 + dx_2^2)\big(5dx_1^2x_2^2 + 4dx_1x_2 + d + \frac{a}{3}\big) + b \\ 0 &= (2x_1x_2+1)(3x_1^4 + 10x_1^2x_2^2d + 4x_1x_2d + 3x_2^4d^2 + a + d) \\ 0 &= 2x_1x_2 + 1 \\ y_2 &= 0 \end{cases}$$

in the variables x_1, y_1, x_2, y_2. But of course the second equation is divisible by the third equation, and we may ignore it (this is not a coincidence, but it is a consequence of the fact that the curve E is defined over $\mathbb{Q}$). Multiplying the first equation in (6) by $2^{12}x_1^6$, we can use the relation $2x_1x_2 = -1$ to eliminate the variable x_2, obtaining the single equation $(2^6x_1^3y_1)^2 = \overline{\rho}(x_1)$ in x_1, y_1 for D. After the birational substitution $x = 2x_1$ and $y = 2^6x_1^3y_1$, we obtain that the curve D is birational to the genus 5 curve with equation

$$D\colon y^2 = x^{12} + 4(3d+4a)x^8 + 64bx^6 + 16d(3d+4a)x^4 + 64d^3.$$

The curve D admits the non-constant map $(x,y) \mapsto (x^2, y)$ to the genus 2 curve F with equation

$$F\colon y^2 = x^6 + 4(3d+4a)x^4 + 64bx^3 + 16d(3d+4a)x^2 + 64d^3.$$

Summarizing, the curve D is a genus 5 curve defined over $\mathbb{Q}$ and it admits two morphisms defined over $\mathbb{Q}(\sqrt{d})$ to the curves

$$C\colon y^2 = f(x) = g(x^2+\sqrt{d}) \quad \text{and} \quad \overline{C}\colon y^2 = \overline{f}(x) = g(x^2-\sqrt{d}).$$

Each of the two curves C and $\overline{C}$ admits a $\mathbb{Q}(\sqrt{d})$-morphism to the elliptic curve E, and the corresponding two compositions $D \to E$ coincide, and are defined over $\mathbb{Q}$. We deduce that the Jacobians of C and of $\overline{C}$ are contained, up to isogeny, in the Jacobian of D, and they have an

isogenous copy of E in common. This implies that the five-dimensional Jacobian of D contains a further two-dimensional abelian variety: up to isogeny this is the Jacobian of the curve F.

It is now easy to provide examples where the inequality of the Chabauty method is not satisfied for the curve C, nor for the curve E, but it satisfied for the curve F, so that we can still apply the Chabauty method to find the points on D. For example, setting $a = 1$, $b = 3$, and $d = 13$, we find $\mathrm{rk}\big(E(\mathbb{Q})\big) = 1$ and $\mathrm{rk}\big(\mathrm{Jac}(F)(\mathbb{Q})\big) = 1$, and moreover

$$\mathrm{rk}\left(\mathrm{Jac}(C)\big(\mathbb{Q}(\sqrt{d})\big)\right) \geq \mathrm{rk}\left(E\big(\mathbb{Q}(\sqrt{d})\big)\right) \geq 2.$$

Thus, in this example the Chabauty method is not applicable to C or E, but it is only applicable to $F(\mathbb{Q})$.

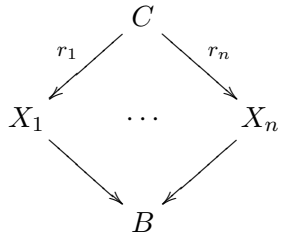
4. Cases where Faltings' Theorem does not apply

In this section we analyze the cases where the relative Weil restriction of a morphism of curves contains a component of geometric genus at most one. In such cases, Faltings' Theorem cannot be applied to deduce the finiteness of rational points of the relative Weil restriction and we find explicit non-tautological examples in which these sets of rational points are infinite. The following remark is an immediate consequence of Faltings' Theorem and guides the choice of cases we handle in this section.

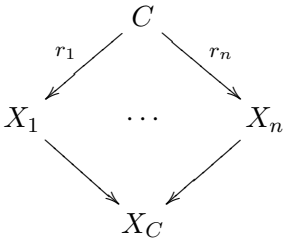
Remark 13. Let L/K be an extension of number fields, and suppose that C is an irreducible curve defined over L, B is a curve defined over K and $h\colon C \to B$ is a non-constant morphism. If the curve $\mathrm{Res}_h(C)$ has infinitely many K-rational points, then the genus of C is at most one.

In the case of the relative Weil restriction of a morphism from a curve of genus one, we completely characterize the cases where the set of rational points is not finite.

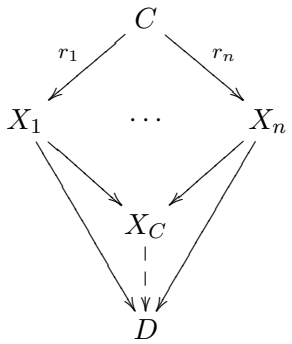
Proposition 14. *Let $C, X_1, \ldots, X_n, B$ be smooth projective curves (not necessarily connected), and let*



be a commutative diagram, where all morphisms are finite and flat. There is a smooth projective curve X_C and a commutative diagram



such that for every projective curve D fitting in the commutative diagram of solid arrows



the dashed arrow $X_C \dashrightarrow D$ exists uniquely.

Proof. Let X be the disjoint union $X := X_1 \sqcup \cdots \sqcup X_n$. The morphisms $r_1, \ldots, r_n$ determine an equivalence relation $\sim_C$ on X, where $x \sim_C y$ if there is a sequence $(i_1, \ldots, i_t)$ of elements of $\{1, \ldots, n\}$, and points $x_1 = x \in X_{i_1}$, $x_2 \in X_{i_2}$, $\ldots$, $x_{t-1} \in X_{i_{t-1}}$, $x_t = y \in X_{i_t}$ and a sequence $c_1, \ldots, c_{t-1}$ of points of C such that for all $j \in \{1, \ldots, t-1\}$ we have $r_{i_j}(c_i) = r_{i_{j+1}}(c_i)$. Thus, a pair $(x, y) \in X \times X$ is in the relation determined by the morphisms $r_1, \ldots, r_n$ if and only if there is a sequence $I := (i_1, \ldots, i_t)$ of elements of $\{1, \ldots, n\}$ such that the pair (x, y) is in the image of the composition

$$C \times_{X_{i_2}} \times \cdots \times_{X_{i_{t-1}}} C \xrightarrow{\pi} C \times C \xrightarrow{(r_{i_1}, r_{i_t})} X_{i_1} \times X_{i_t} \subset X \times X$$

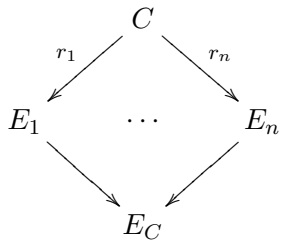
where π is the projection to the first and last factor; denote by $C_I \subset X \times X$ the image of this morphism. Observe that, for every finite sequence I of elements of $\{1, \ldots, n\}$, the scheme C_I is a closed subscheme of $X \times X$ that is finite and flat over each factor X and hence also over B; in particular, each scheme C_I has non-zero degree over B. Moreover, if the pair (x, y) is in the relation $\sim_C$, then x and y have the same image in B. From this it follows that pairs (x, y) in the relation $\sim_C$ are covered by at most $\left(\sum_i \deg(f_i)\right)^2$ of the schemes C_I defined above since they are contained in $X \times_B X$. It follows that the whole graph $R_C \subset X \times X$ of the relation $\sim_C$ is a subscheme of finite type of $X \times X$ that is flat and proper over each factor. The hypotheses of [18, Théorème V.7.1] are therefore satisfied and the result follows. □

Corollary 15. *With the notation of the previous proposition, assume further that the curves $C, X_1, \ldots, X_n$ all have genus one. Then the curve X_C is a torsor under $\mathrm{Jac}(C)/K$, where K is the subgroup of $\mathrm{Jac}(C)$ generated by the kernels of the morphisms $\mathrm{Jac}(C) \to \mathrm{Jac}(X_1)$, $\ldots$, $\mathrm{Jac}(C) \to \mathrm{Jac}(X_n)$.*

Proof. We can clearly assume that the ground field is algebraically closed, and further reduce to the case in which the morphisms $r_1, \ldots, r_n$ are all homomorphisms of elliptic curves. Thus $K \subset C$ is identified with the subgroup generated by the kernels of all the morphisms $r_1, \ldots, r_n$ and let $C' := C/K$ denote the quotient of C by the subgroup K. Clearly, the curves $X_1, \ldots, X_n$ all admit a morphism to C' making the diagram of Proposition 14 commute. It follows from the previous proposition that X_C admits a morphism to C' that is necessarily non-constant, and we conclude that X_C has genus one. Moreover, it is also clear that the curve X_C is isomorphic to the curve C': if D is any curve making the diagram of Proposition 14 commute, then the fiber in C of the morphism $C \to D$ over the image of the origin in C contains all the kernels of the morphisms $r_1, \ldots, r_n$, and hence it contains the subgroup K, since the morphism factors through the elliptic curve X_C. □

Thus we see that if the curves $X_1, \ldots, X_n$ have genus one and if the fibered product $X_1 \times_B \cdots \times_B X_n$ contains a geometrically integral curve of geometric genus one defined over the ground field, then the morphism $X_1 \to B$ factors through a morphism $E \to B$ defined over the ground field, where E is a smooth geometrically integral curve of geometric genus one and the morphism $X_1 \to E$ is an isogeny defined over the extension field.

4.1. **Genus one.** We specialize what we just proved to the case of the relative Weil restriction from an elliptic curve. Let L/K be an extension of number fields; let E be an elliptic curve defined L and let B be a smooth projective integral curve defined over K. Suppose that $h\colon E \to B_L$ is a non-constant morphism. The relative Weil restriction $\mathrm{Res}_h(E)$ is a curve defined over K. Fix an algebraic closure $\overline{K}$ of K, denote by $\sigma_1, \ldots, \sigma_n$ the distinct embeddings of L/K in $\overline{K}$, and let $E_1, \ldots, E_n$ be the corresponding Galois conjugates of E. Over the field $\overline{K}$, the curve $\mathrm{Res}_h(E)$ is isomorphic to $E_1 \times_B \cdots \times_B E_n$ (Lemma 5). Suppose that the curve $\mathrm{Res}_h(E)$ contains infinitely many K-rational points. It follows from Faltings' Theorem that there is a component C of $\mathrm{Res}_h(E)$ of geometric genus at most one, defined over K; if C is not normal, we replace it by its normalization. Since the morphism $\mathrm{Res}_h(E) \to B$ is flat, all its fibers are finite and therefore the curve C is also finite over B. In particular, the L-morphisms $C \to E_1, \ldots, C \to E_n$ are all finite, since all the curves are smooth. Let E_C denote the universal curve fitting in the diagram



of Proposition 14. Since the curves $C, E_1, \ldots, E_n$ all have genus one, we may therefore apply Corollary 15 to deduce that the curve E_C is also a torsor under an elliptic curve, and therefore also E_C has genus one. In the case in which L is a number field, we obtain the following corollary.

Corollary 16. *Let L/K be an extension of number fields and suppose that E is an elliptic curve over L, B is a curve over K, and $h\colon E \to B_L$ is a non-constant morphism. If the set of K-rational points of $\mathrm{Res}_h(E)$ is infinite, then the curve E is L-isogenous to an elliptic curve defined over K having positive rank over K.*

Proof. By Faltings' Theorem we deduce that $\mathrm{Res}_h(E)$ contains a geometrically integral component E' of genus at most one defined over K and having infinitely many K-rational points. Since E' admits a non-constant L-morphism to E, it follows that E' has genus one and that it is L-isogenous to E, as required. □

Remark 17. In the case in which E and B have genus one, then all the geometric components of $\mathrm{Res}_h(E)$ have genus one. Hence, finding the K-rational points of $\mathrm{Res}_h(E)$ is equivalent to finding the K-rational points of finitely many elliptic curves that are K-isogenous to B.

This completes our analysis in the case in which the curve C of Remark 13 has genus one. We next discuss the case in which C has genus zero. We are not able to give a treatment of this case that is as detailed as the case of genus one.

4.2. **Genus zero.** We specialize to the case in which the curve C is isomorphic to $\mathbb{P}^1_L$ and hence B is isomorphic to $\mathbb{P}^1_K$. The morphism $h\colon \mathbb{P}^1_L \to \mathbb{P}^1_L = (\mathbb{P}^1_K)_L$ is therefore determined by a rational function $F \in L(x)$. The set of K-rational points of $\mathrm{Res}_h(\mathbb{P}^1_L)$ is essentially the set $A_F \subset L$ of values of $x \in L$ such that $F(x)$ lies in K, mentioned in the introduction.

Fiber type of the pair $F, \overline{F}$	Fiber type of $\mathrm{Res}_F(F)$	Hurwitz contribution to $[F, \overline{F}]$ and $[\mathrm{Res}_F(F)]$	Symmetrized contribution
$\big((1,1,1),(1,1,1)\big)$	$(1,1,1,1,1,1,1,1,1)$	[0,0] , [0]	[0,0] , [0]
$\big((2,1),(1,1,1)\big)$	$(2,2,2,1,1,1)$	[1,0] , [3]	[1,1] , [6]
$\big((3),(1,1,1)\big)$	$(3,3,3)$	[2,0] , [6]	[2,2] , [12]
$\big((2,1),(2,1)\big)$	$(2,2,2,2,1)$	[1,1] , [4]	[1,1] , [4]
$\big((2,1),(3)\big)$	$(6,3)$	[1,2] , [7]	[3,3] , [14]
$\big((3),(3)\big)$	$(3,3,3)$	[2,2] , [6]	[2,2] , [6]

TABLE 1. Fiber types and contributions to the Hurwitz formula for fiber products of morphisms of degree three

Definition 18. Let $G\colon C \to D$ be a finite morphism between smooth curves, let $p \in D$ be a geometric point. The *type* of p is the partition λ_p of $\deg(G)$ determined by the fiber $G^{-1}(p)$. We extend this definition to the case in which the curve C is reduced, but not necessarily smooth, by replacing G with the morphism $G^\nu\colon C^\nu \to D$, where C^ν is the normalization of C and G^ν is the morphism induced by G.

In this section we restrict our attention to a field extension $L \supset K$ of degree two.

Degree three. Suppose that $F\colon \mathbb{P}^1_L \to \mathbb{P}^1_L$ is a morphism of degree three, and suppose that the characteristic of K is neither two nor three. As usual, we are interested in the values $\ell \in L$ such that $f(\ell) \in K$. Denote by $\overline{F}$ the morphism conjugate to F under the Galois involution of L/K. We construct examples of morphisms F such that $\mathrm{Res}_F(\mathbb{P}^1_L)$ is a geometrically integral curve of geometric genus zero. Note that the curve $\mathrm{Res}_F(\mathbb{P}^1_L)$ has a line bundle of degree nine given by pull-back of $\mathcal{O}_{\mathbb{P}^1_K}(1)$; since this curve is geometrically rational and it has a line bundle of odd degree, it follows that it is rational over K.

Denote by $\mathrm{Res}_F(F)^\nu$ the composition of the normalization map of $\mathrm{Res}_F(\mathbb{P}^1_L)$ and $\mathrm{Res}_F(F)$. Applying the Hurwitz formula to the morphisms F, $\overline{F}$ and $\mathrm{Res}_F(F)^\nu$, we find that the respective total degrees of the ramification divisors are 4, 4 and 16.

We begin by analyzing the ramification patterns. For a geometric point $p \in \mathbb{P}^1$, Table 4.2 shows the possibilities of the types of the fibers of the three morphisms F, $\overline{F}$ and $\mathrm{Res}_F(F)^\nu$ and the contributions of each to the Hurwitz formula. In our setup, the Galois involution of L/K induces a bijection between fiber types of F and of $\overline{F}$: this is recorded in the last column of Table 4.2.
It is now easy to check that the only possibilities for the fiber types of the morphisms $F, \overline{F}$ are

$$\big((3),(3)\big) + \big((2,1),(1,1,1)\big) + \big((1,1,1),(2,1)\big) + \big((2,1),(2,1)\big) \tag{7}$$

and

$$\big((2,1),(2,1)\big) + \big((2,1),(2,1)\big) + \big((2,1),(2,1)\big) + \big((2,1),(2,1)\big). \tag{8}$$

We only analyze the case (7).

Fiber types (7). The fiber type $((3),(3))$ in (7) implies that the coordinate on $\mathbb{P}^1$ can be chosen so that the morphism F is a polynomial and the fiber type $((2,1),(2,1))$ shows that one of the ramification points in defined over K. This case is realized by morphisms $F\colon \mathbb{P}^1_L \to \mathbb{P}^1_L$ of the form $p(x) = x^2(x-\alpha)$, for $\alpha \in L$. Since the derivative of p vanishes at 0 and at $\frac{2\alpha}{3}$, it follows that the ramification types of $F, \overline{F}$ are of the form (7) when $\alpha \notin K$.

Let $L \supset K$ be a field extension of degree two, let $F\colon \mathbb{P}^1_L \to \mathbb{P}^1_L$ be a morphism of degree three. We are interested in the values $\ell \in L$ such that $f(\ell) \in K$. Assume that $L = K(\sqrt{d})$ where $d \in K \setminus K^2$; write $\alpha = a + b\sqrt{d}$, for $a, b \in K$. Parameterizing the rational curve $\mathrm{Res}_F(F)$ we find that, for every element t in K, the evaluation

$$p\left(\frac{dbt^2 + 2at + b}{t(dt^2+3)}(\sqrt{d}t + 1)\right)$$

is also in K.

References

[1] R.M. Avanzi and U.M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation*, Acta Arith. **99** (2001), no. 3, 227–256. ↑2

[2] Y.F. Bilu and R.F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), no. 3, 261–288. ↑2

[3] N.R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, vol. 133, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. Dissertation, University of Leiden, Leiden, 1999. ↑2

[4] ———, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. ↑2

[5] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. ↑2

[6] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885. ↑2

[7] ———, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris **212** (1941), 1022–1024. ↑2

[8] R.F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. ↑2

[9] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. ↑2

[10] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. ↑2

[11] E.V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), no. 1, 79–94. ↑2

[12] E.V. Flynn and J.L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533. ↑2

[13] ———, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205. ↑2

[14] N. Freitas, B. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, http://arxiv.org/abs/1310.7088. ↑3

[15] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. ↑6

[16] D. Lorenzini and T.J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77. ↑2

[17] F. Pakovich, *On the equation $P(f) = Q(g)$, where P, Q are polynomials and f, g are entire functions*, Amer. J. Math. **132** (2010), no. 6, 1591–1607. ↑2

[18] J.-P. Serre, A. Grothendieck, M. Artin, J.E. Bertin, M. Demazure, P. Gabriel, and M. Raynaud, *Schémas en groupes. Fasc. 2a: Exposés 5 et 6*, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, vol. 1963/64, Institut des Hautes Études Scientifiques, Paris, 1963/1965. ↑14

[19] A. Schinzel, *Selected topics on polynomials*, University of Michigan Press, Ann Arbor, Mich., 1982. ↑2

[20] S. Siksek, *Explicit chabauty over number fields*, arXiv:1010.2603v2. ↑2

[21] J.L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley. ↑2

[22] U. Zannier, *Ritt's second theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), 175–203. ↑2

Mathematical Institute, University of Oxford, Andrew Wiles Building, Woodstock Road, Oxford OX2 6GG, United Kingdom

E-mail address: flynn@maths.ox.ac.uk

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, United Kingdom

E-mail address: D.Testa@warwick.ac.uk