Computability of Rational Points on Curves over Function Fields in Characteristic p

by

Campbell L. Hewett

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

Massachusetts Institute of Technology

May 2020

Signature of Author: _____

Department of Mathematics
April 30, 2020

Certified by: _____

Bjorn Poonen
Claude Shannon Professor of Mathematics
Thesis Supervisor

Accepted by: _____

Wei Zhang
Chairman, Department Committee on Graduate Theses

Computability of Rational Points on Curves over Function Fields in Characteristic p

by

Campbell L. Hewett

Submitted to the Department of Mathematics
on April 30, 2020, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy of Mathematics

Abstract

The motivating problem of this thesis is that of explicitly computing the K-rational points of a regular nonsmooth curve X over a finitely generated field K of characteristic p. We start with an in-depth study of such curves in general and the tools exclusive to characteristic p geometry needed to compute their K-points. We describe a combined going-down and going-up approach to compute $X(K)$ that generalizes and makes effective the proof of finiteness of $X(K)$ given by Voloch ([39]). We break the problem up into three separate cases according to the absolute genus of X. In the absolute genus 0 case, we give an algorithm to compute $X(K)$ that is an effective version of a method given by Jeong ([16]). We also implement a special case of this algorithm in Sage and apply it to example curves. In the absolute genus 1 case, we give an algorithm to compute $X(K)$ that works when we make extra assumptions about X, and we make some remarks in the case where those assumptions are removed. In the absolute genus at least 2 case, we give an unconditional algorithm to compute $X(K)$.

Some tools and algorithms we provide along the way do not directly involve regular nonsmooth curves and are interesting in their own right. We describe ways to effectively descend curves with respect to transcendental or purely inseparable field extensions. We explore the methods of p-descent on elliptic curves in characteristic p and provide explicit equations defining $\mathbb{Z}/p\mathbb{Z}$- and μ_p-torsors over them. We prove an effective de Franchis-Severi theorem for characteristic p that generalizes the one given by Baker, et al. over number fields ([3]). Lastly, we use a height bound proved by Szpiro ([34]) to give an algorithm to compute $Y(K)$ for any smooth nonisotrivial curve Y over K followed by an algorithm to compute $Y(K^{1/p^\infty})$, which was proved to be finite by Kim ([17]).

Thesis Supervisor: Bjorn Poonen
Title: Claude Shannon Professor of Mathematics

Acknowledgements

I would like to thank my advisor, Bjorn Poonen, for his mentoring and commitment to my success at MIT. Our weekly meetings forced me to frequently collect my thoughts in a precise way, which was crucial for me to make consistent progress on my research. Whenever I was stuck, he would offer a new direction to take. There were times I would come to Bjorn after feeling like I had tried everything, and he would make some comment or suggestion that would instantly make everything fall into place for me.

I would like to thank my family for their love and support. It was nice to be able to go to both college and graduate school nearby. I thank my mom for constantly encouraging me and always being there for me. I thank my dad for being the best teacher I ever had; I would not be where I am today if he had not shared his love of math with me at an early age. I thank my sister, Emma, for being a great friend I can always relate to, and also for being hilarious. I also thank our close friend, Andre, for always encouraging my love of math.

This research was supported in part by Simons Foundation grant #402472 and by Simons Foundation grant #550033.

Contents

1 Introduction

Let k be a perfect field and K be a function field over k; that is, $K = k(V)$ for some integral variety V over k. Let X be a geometrically integral regular projective curve over K with arithmetic genus $g := g(X) = \dim_K H^1(X, \mathcal{O}_X)$. There are two important cases when $X(K)$ is known to be finite, namely

(i) X is smooth, $g \geq 2$, and X is not isotrivial [27], and

(ii) X is not smooth.

Case (i) can be thought of as a function field analogue of the Mordell conjecture. It was first proved by Grauert in characteristic 0 ([13]) and by Samuel in characteristic p ([27]). Case (ii) occurs only in characteristic p and is equivalent to $g > g(\widetilde{X_{\overline{K}}})$, where $X_{\overline{K}}$ is the base extension of X to an algebraic closure $\overline{K}$ of K and $\widetilde{X_{\overline{K}}}$ is its normalization. The number $\widetilde{g} := g(\widetilde{X_{\overline{K}}})$ is known as the *absolute genus* of X. The fact that $X(K)$ is finite for such curves was proved by Samuel in the case where $\widetilde{g} \geq 2$ ([27, Théorème 6]) and by Voloch and Jeong in the cases where $\widetilde{g} = 0$ or $\widetilde{g} = 1$ ([39],[16]).

This thesis is concerned with the question of computing the set $X(K)$. For case (i), an effective Mordell conjecture is known in the case where k is a finite field; this follows from explicit bounds for the heights of K-points on X. The first such height bound was given by Szpiro in [34]. We show in Section 6 that his bound can also be used to give an algorithm to compute $X(K)$ for infinite fields k of characteristic p. The motivating problem for this thesis is to answer the question for case (ii).

Conjecture 1.0.1. *Let K be a field of characteristic p finitely generated over a perfect field k. Let X be a geometrically integral regular projective curve over K that is not smooth. Then the finite set $X(K)$ is computable.*

The progress we present on this conjecture is given in the following theorem.

Theorem 1.0.2. *Conjecture 1.0.1 is true in the following cases:*

(i) X has absolute genus 0,

(ii) X has absolute genus 1 and the j-invariant of $\widetilde{X_{\overline{K}}}$ is in K,

(iii) X has absolute genus 1, k is a finite field, and $K = k(t)$, and

(iv) X has absolute genus at least 2.

Case (ii) includes the case where X has absolute genus 1 and is isotrivial (see Remark 5.3.1).

The remainder of this thesis is organized as follows. In Section 2, we elaborate on what it means for $X(K)$ to be computable, and we list several known computational procedures relating to rings and varieties that will be needed in our algorithms. In Section 3, we give some background concerning curves in characteristic p and prove facts for regular nonsmooth curves that hold in any absolute genus. In particular, for the purposes of proving Theorem 1.0.2, we reduce to the case where K is a function field in one variable over k and there exists an inseparable degree p morphism $\pi\colon X \to Y$, where Y is a *smooth* curve over K of genus $\widetilde{g}$. The latter reduction was a crucial step in [39] and is important for Proposition 3.4.6, which lays out the main procedure for computing points. In Section 4, we handle the case where $\widetilde{g} = 0$. The approach here is an effective version of the proof of finiteness of $X(K)$ given in [16]. In Sections 5 and 6, we handle the cases where $\widetilde{g} = 1$ and $\widetilde{g} \geq 2$ respectively. In both sections, we give separate proofs in the cases where Y is isotrivial and Y is not isotrivial. Lastly, in Appendix A, we provide Sage code implementing a special case of the algorithm given in Section 4.3.

2 Computability

2.1 Conventions and notation

As in Section 1, let k be a perfect field of characteristic p, K be a field finitely generated over k, and X be a geometrically integral regular nonsmooth projective curve over K. To make sense of the statement of Theorem 1.0.2, each element of K needs to be described by a finite amount of information. Therefore, we assume that k has finite transcendence degree over $\mathbb{F}_p$. If k is not algebraically closed, then the strategy is to replace k by $\overline{k}$ and K by $\overline{k}K$. By the following theorem, $X_{\overline{k}K}$ is regular but not smooth, so $X(\overline{k}K)$ is a finite set. Thus, $X(K)$ can be computed by first computing $X(\overline{k}K)$ and checking which points are K-points.

Theorem 2.1.1. *Let L/F be a separable field extension and X be a curve over F.*

(i) If X is regular, then X_L is regular.

(ii) If $\widetilde{X_L}$ is smooth, then $\widetilde{X}$ is smooth.

Proof. For (i), see [2, XV.5, Theorem 22]. For (ii), we have $\widetilde{X_L} = (\widetilde{X})_L$ by (i). Therefore, $\widetilde{X}$ is smooth, as smooth is equivalent to geometrically regular. □

For this reason, we will typically assume that k is algebraically closed. The curve X will be definable over some field $K_0 \subset K$ that is finitely generated over $\mathbb{F}_p$. Its field of constants $k_0 := k \cap K_0$ is then finitely generated over $\mathbb{F}_p$ as well. Because $X(K)$ is finite, there will then exist a finite field extension k_1 of k_0 such that $X(K) = X(k_1K_0)$.

To explicitly specify a finitely generated field F, we give a transcendence basis $t_1, \ldots, t_m$ for F over $\mathbb{F}_p$ as well as a list of elements $u_1, \ldots, u_n$ algebraic over $\mathbb{F}_p(t_1, \ldots, t_m)$, together with their minimal polynomials, such that $F = \mathbb{F}_p(t_1, \ldots, t_m, u_1, \ldots, u_n)$. To specify a projective variety V over a field F, we give generators of its homogeneous ideal for an embedding of V in some projective space over F.

Given all of the above, the meaning of Theorem 1.0.2 is that there exists an algorithm that takes the following as input.

Input 2.1.2.

(i) *a prime number p,*

(ii) *a field k_0 finitely generated over $\mathbb{F}_p$,*

(iii) *a nonnegative number $m \in \mathbb{Z}_{\geq 0}$,*

(iv) *a finite extension K_0 of $k_0(t_1, \ldots, t_m)$, and*

(v) *a geometrically integral nonsmooth projective curve X over K_0 such that $X_{\overline{k_0}K_0}$ is regular.*

These data will be written (p, k_0, m, K_0, X) for short. For such data, we will also assume the notation $k := \overline{k_0}$ and $K := kK_0$.

The algorithm will then give as output a finite extension k_1/k_0 with $K_1 := k_1K_0$, such that $X(K) = X(K_1)$ for any K_0-embedding of K_1 in K, as well as the set $X(K_1)$. Note that our goal is to compute $X(K)$, but the focus has mostly switched from k and K to k_0 and K_0.

There are two types of theorems in this thesis. The first type contain statements of the form "There exists an algorithm that takes input [blah] and returns [blah]". The proof of such a statement will not be given as pseudocode followed by proof of validity. Instead, I have chosen to format the proofs by a sequence of command sentences "Compute [blah]" with proof of validity and other general reasoning interspersed. The fields involved in these theorems will always be finitely generated. We do not analyze the runtime of any algorithm, but we try to give efficient algorithms when possible.

The second type make no reference to computation. These typically do not require fields to be finitely generated. For this reason, theorems of this type use the notation k, K rather than k_0, K_0. Furthermore, in order to prove statements in the greatest generality possible, the hypotheses on k, K, and any relevant varieties will not be consistent across all theorems. For this reason, the hypotheses will be made clear in the statement of every theorem, unless

the hypotheses are clear from context as part of running notation in the section that contains the theorem.

2.2 Algorithms

There are several computations we will need throughout this thesis for which there are known algorithms. Let F be a field finitely generated over $\mathbb{F}_p$, R be a finitely generated F-algebra, and I and J be ideals of R. The following are procedures that can be done using Gröbner bases:

(i) compute the radical of I ([22]),

(ii) compute a primary decomposition of I ([11], [15]),

(iii) compute the ideal quotient $(I : J)$ and saturation $(I : J^\infty)$ ([6, Chapter 4, §4]),

(iv) compute the normalization of R ([33]),

(v) compute the Hilbert polynomial of R in the case where R is graded ([4]).

We can apply these procedures on F-algebras to perform the following ones on varieties. Let $V \subset \mathbb{P}^n_F$ be a projective variety over F with homogeneous ideal $I \subset S := F[x_0, \ldots, x_n]$, and set $R := S/I$.

(i) Compute the dimension of V and the arithmetic genus of V.

If $P_V(z) \in \mathbb{Q}[z]$ is the Hilbert polynomial of S/I, then the dimension of V is $\dim V = \deg P_V(z)$ and the arithmetic genus is $(-1)^{\dim V}(P_V(0) - 1)$. In the case where V is a geometrically integral curve, the latter is equal to $\dim_F H^1(V, \mathcal{O}_V)$ ([14, Exercises III.5.2-3]).

(ii) Compute the nonsmooth locus of V.

If $I = (f_1, \ldots, f_r)$ and d is the dimension of V, then the nonsmooth locus of V, as a reduced subvariety of $\mathbb{P}^n_F$, is the radical of the ideal generated by I and the determinants of the $(n-d)$-by-$(n-d)$ minors of the Jacobian matrix $(\partial f_i/\partial x_j)$.

(iii) Compute a finite inseparable extension F'/F such that the reduced variety of $V_{F'}$ is geometrically reduced.

For $i \geq 0$, let V_i denote the reduced variety of $V_{F^{1/p^i}}$, and let $W_i \subset V_i$ be its nonsmooth locus. If $W_i \neq V_i$, then V_i is geometrically reduced. Thus, compute V_i and W_i for $i = 0, 1, 2, \ldots$ to determine the smallest i such that $W_i \neq V_i$. Then take $F' = F^{1/p^i}$.

(iv) Compute the irreducible components of V.

The irreducible components, as *reduced* subvarieties of $\mathbb{P}^n_F$, correspond to the minimal primes in the primary decomposition of I. The only cases where we will need to compute irreducible components are when V is already reduced or when $\dim V = 0$.

(v) Compute the Zariski closure of $V \setminus W$, where W is a closed subvariety of V.

If $J \subset S$ is the homogeneous ideal defining W, then the Zariski closure of $V \setminus W$ is $(I : J^\infty)$.

(vi) Compute a finite field extension F'/F such that the irreducible components of $V_{F'}$ are geometrically irreducible.

Using (iii), we can first find a finite field extension F''/F such that the reduced variety W of $V_{F''}$ is geometrically reduced. We proceed by induction on the number of irreducible components of $W_{\overline{F}}$. Choose any F''-point P in the smooth locus of W, and let F' be its residue field. Then P will split into a number of points in $W_{F'}$, at least one of them being purely inseparable. The irreducible component W' of $W_{F'}$ containing such a purely inseparable point will be geometrically irreducible. The Zariski closure of $W_{F'} \setminus W'$ in $\mathbb{P}^n_{F'}$ will have fewer irreducible components over $\overline{F'}$ than $W_{F'}$, so we finish by induction.

(vii) Compute the global sections of a coherent sheaf $\mathcal{F}$ on V.

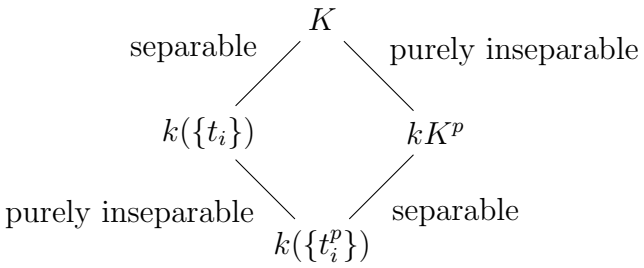
A finitely generated graded R-module M gives rise to a coherent sheaf $\widetilde{M}$ on V, and the F-vector space $H^0(V, \widetilde{M})$ can be computed ([10]). We will mostly need to compute $H^0(V, \mathcal{O}_V(D))$ as an F-vector subspace of $F(V)$, where D is a divisor on V, and typically in the case where V is a curve.

3 Curves in characteristic p

3.1 Inseparable field extensions and derivations

Lemma 3.1.1. *Let k be a field of characteristic p, and let K be a field with separating transcendence basis $\{t_i\}_{i\in I} \in K$ over k. Then, as a kK^p-algebra, K is generated by $\{t_i\}_{i\in I}$. If I is a finite set of size n, then $[K : kK^p] = p^n$.*

Proof. Every element of K^p is separable over $\big(k(\{t_i\})\big)^p \subset k(\{t_i^p\})$, and kK^p is the field extension of $k(\{t_i^p\})$ gotten by adjoining every element of K^p. Thus, kK^p is separable over $k(\{t_i^p\})$. Moreover, we have the following field extensions:



(3.1)

From this, we see that K is the compositum of its subfields $k(\{t_i\})$ and kK^p. Therefore, K is the field extension of kK^p gotten by adjoining the algebraic elements $\{t_i\}$.

If $I = \{1, 2, \ldots, n\}$, then by taking inseparable degrees in the above diagram,

$$[K : kK^p] = [k(t_1, \ldots, t_n) : k(t_1^p, \ldots, t_n^p)] = p^n. \qquad \square$$

We will use Lemma 3.1.1 frequently in the following two cases.

(i) Let K be a field of characteristic p that is finitely generated over a perfect field k. If $t_1, \ldots, t_m$ is a transcendence basis of K over k, then K is a degree p^m purely inseparable extension of K^p generated by $t_1, \ldots, t_m$.

(ii) Let K be a field of characteristic p, and let X be an integral curve over K. Assume further that X is geometrically reduced over K so that there exists $z \in K(X)$ such

that $K(X)$ is a finite separable extension of $K(z)$. Then $K(X)$ is a degree p purely inseparable extension of $K \cdot K(X)^p$ generated by z.

Proposition 3.1.2. *Let k be a field of characteristic p, and let K be a field separably generated over k with transcendence degree 1. Let $x \in K$, such that x is not algebraic over k. Then $[K : k(x)]_i = p^n$ for some $n \geq 0$, and $x \in kK^{p^n} \setminus kK^{p^{n+1}}$. In particular, K is an inseparable algebraic extension of $k(x)$ if and only if $x \in kK^p$.*

Proof. Let $y \in K$ be such that $K/k(y)$ is a separable algebraic extension. Let $F/k(x)$ be the maximal separable subextension of K. Because K is separable over $k(x, y)$, we have

$$[K : F] = [K : k(x)]_i = [k(x, y) : k(x)]_i,$$

which is finite. Let this number be p^n as in the statement of the proposition. Then $K^{p^n} \subset F$, so $kK^{p^n} \subset F$. By Lemma 3.1.1, we have $[K : kK^{p^n}] = p^n$, so $F = kK^{p^n}$ by comparing degrees. This proves $x \in kK^{p^n}$. It cannot be that $x \in kK^{p^{n+1}}$ because otherwise $[K : F]$ would be at least p^{n+1}.

If $K/k(x)$ is inseparable, then $n \geq 1$, so $x \in kK^{p^n} \subset kK^p$. If $K/k(x)$ is separable, then $n = 0$ and $x \in K \setminus kK^p$. □

The following can be thought of as an algorithmic version of Lemma 3.1.1.

Proposition 3.1.3. *There exists an algorithm that takes as input a finitely generated field k_0 of characteristic p, a field K_0 given as a separable extension of $k_0(t_1, \ldots, t_n)$, and an element $u \in K_0$ and returns for each $j \in \{0, 1, \ldots, p-1\}^{\{1,2,\ldots,n\}}$ an element $e_j(U^p) \in k_0(t_1^p, \ldots, t_n^p)(U^p)$, where U is an indeterminate, such that*

$$u = \sum_j e_j(u^p) t^j,$$

where we are using multi-index notation $t^j = t_1^{j_1} t_2^{j_2} \cdots t_n^{j_n}$.

Proof. Start by computing the minimal polynomial of u,

$$f(U) = a_0 + a_1U + \cdots + a_{d-1}U^{d-1} + U^d \in k_0(t_1, \ldots, t_n)[U],$$

and regroup terms so that

$$f(U) = b_0 + b_1U + \cdots + b_{p-1}U^{p-1},$$

where each $b_0, \ldots, b_{p-1} \in k_0(t_1, \ldots, t_n)[U^p]$. For each $0 \leq i \leq p-1$, we have

$$U^i f(U) = (b_{p-i}U^p) + (b_{p-i+1}U^p)U + \cdots + (b_{p-1}U^p)U^{i-1} + b_0U^i + b_1U^{i+1} + \cdots + b_{p-i-1}U^{p-1}.$$

Let $M(U)$ be the p-by-p matrix with entries in $k_0(t_1, \ldots, t_n)[U^p]$ whose ij-entry is the coefficient of U^j in $U^i f(U)$ as given above. Then $(1, u, u^2, \ldots, u^{p-1})^T$ is in the kernel of $M(u)$.

If $g(U) \in k(t_1, \ldots, t_n)[U]$ and $g(u) = 0$, then $g(U) = h(U)f(U)$ for some $h(U) \in k(t_1, \ldots, t_n)[U]$. Suppose

$$g(U) = b'_0 + b'_1U + \cdots + b'_{p-1}U^{p-1}$$

and

$$h(U) = c_0 + c_1U + \cdots + c_{p-1}U^{p-1},$$

with $b'_0, \ldots, b'_{p-1}, c_0, \ldots, c_{p-1} \in k_0(t_1, \ldots, t_n)[U^p]$. Then

$$g(U) = c_0f(U) + c_1Uf(U) + \cdots + c_{p-1}U^{p-1}f(U).$$

In other words, the row vector

$$\begin{pmatrix} b'_0 & b'_1 & \cdots & b'_{p-1} \end{pmatrix}$$

is some $k_0(t_1, \ldots, t_n)[U^p]$-linear combination of the rows of $M(U)$.

By Lemma 3.1.1, there exist some $c_1, c_2 \in k_0(t_1, \ldots, t_n)[U^p]$ such that $u = c_1/c_2$, or $-c_1 + c_2 u = 0$. By the previous paragraph applied to $g(U) := -c_1 + c_2 U$, the row vector

$$\begin{pmatrix} -c_1 & c_2 & 0 & \cdots & 0 \end{pmatrix}$$

is a $k_0(t_1, \ldots, t_n)[U^p]$-linear combination of the rows of $M(U)$. Use linear algebra over the field $k_0(t_1, \ldots, t_n)(U^p)$ to compute such a linear combination and therefore find such elements c_1, c_2.

Compute $c_1 c_2^{p-1}$ and group terms such that

$$c_1 c_2^{p-1} = \sum_j d_j t^j$$

for $j \in \{0, \ldots, p-1\}^{\{1,\ldots,n\}}$ and $d_j \in k_0(t_1^p, \ldots, t_n^p)[U^p]$. Because $u = (c_1 c_2^{p-1})/c_2^p$, return the elements $e_j(U) := d_j/c_2^p$. □

Remark 3.1.4. If we knew for some reason that $u \in K_0$ was a pth power of some element in $k_0^{1/p} K_0$, then we can compute its pth root. Apply Proposition 3.1.3 to compute $e_0(U^p), \ldots, e_{p-1}(U^p) \in k_0(t_1^p, \ldots, t_n^p)(U^p)$ such that $u = \sum_j e_j(u^p) t^j$. But, $e_j(u^p) = 0$ for all $j \neq (0, \ldots, 0)$ because $u \in k_0 K_0^p$. The element $e_0(U^p)$ is a fraction of polynomials in $t_1^p, \ldots, t_n^p, U^p$, so it is simple to take its pth root $e_0^{1/p}(U) \in k_0^{1/p}(t_1, \ldots, t_n)(U)$. Then $u = e_0^{1/p}(u)$.

Derivations are a key tool in the study of fields and varieties with respect to inseparable extensions. Here, a *derivation* of a ring S is a group homomorphism $\delta \colon S \to S$ such that, for all $r, s \in S$,

$$\delta(rs) = r\delta(s) + \delta(r)s.$$

If S is an R-algebra, then we say δ is an *R-derivation* if $\delta(r) = 0$ for all $r \in R$. Similarly, if $\mathcal{F}$ is a sheaf of rings (resp. R-algebras) on a topological space X, then a derivation (resp. R-derivation) of $\mathcal{F}$ is a morphism $\delta \colon \mathcal{F} \to \mathcal{F}$ of sheaves of rings (resp. R-algebras) such that

$\delta(U)$ is a derivation (resp. R-derivation) of $\mathcal{F}(U)$ for all open subsets $U \subset X$.

If δ is a derivation of S, then, for all $r, s \in S$,

$$\delta^n(rs) = \sum_{i=0}^{n} \binom{n}{i} \delta^i(r)\delta^{n-i}(s).$$

If $p = 0$ in S, then we see that δ^p is also a derivation of S. Similarly, if δ is an R-derivation, then δ^p is also an R-derivation, and the same statements are true for derivations of sheaves on X.

The following is a well known fact, whose proof we give here because we refer to it later. See [20, VIII, Section 5] for a more general version.

Lemma 3.1.5. *Let L/K be a finite separable field extension, and let δ be a derivation of K. Then δ extends uniquely to a derivation $\widetilde{\delta}$ of L.*

Proof. For $g \in K[x]$, let g' denote the derivative of g with respect to x, and let g^δ denote the polynomial gotten from g by applying δ to each of its coefficients. By the primitive element theorem, there exists some $\alpha \in L$ such that $L = K(\alpha)$. Let $f \in K[x]$ be the minimal polynomial of α. From $f(\alpha) = 0$, we see that for $\widetilde{\delta}$ to exist, it must satisfy

$$f'(\alpha)\widetilde{\delta}(\alpha) + f^\delta(\alpha) = 0.$$

One easily verifies that setting $\widetilde{\delta}(\alpha) = -f^\delta(\alpha)/f'(\alpha)$ (note that $f'(\alpha) \neq 0$ because α is separable) uniquely defines $\widetilde{\delta}$ on all of L and that this $\widetilde{\delta}$ is a well defined derivation. □

Remark 3.1.6. Let K be a field of characteristic p with finite separating transcendence basis $\{t_i\}_{i\in I}$ over a field k. For $i \in I$, let δ_i denote the k-derivation on $k(\{t_i\}_{i\in I})$ such that $\delta_i t_i = 1$ and $\delta_i t_j = 0$ for all $j \neq i$. By Lemma 3.1.5, each δ_i extends uniquely to a derivation on K, which we will also call δ_i.

Proposition 3.1.7. *Let K be a field of characteristic p that is finitely and separably generated over a field k, and let D be the set of k-derivations of K.*

(i) If $\alpha \in K$, then $\alpha \in kK^p$ if and only if $\delta\alpha = 0$ for all $\delta \in D$.

(ii) If V is a variety over kK^p, then each $\delta \in D$ can be extended to a k-derivation $\widetilde{\delta}$ of $\mathcal{O}_{V_K}$ such that

$$\bigcap_{\delta \in D} \ker \widetilde{\delta} = \mathcal{O}_V$$

(here, $V_K \to V$ is a homeomorphism, so we consider $\mathcal{O}_{V_K}$ and $\mathcal{O}_V$ to be sheaves on the same topological space).

Proof. (i) Let $\alpha \in K$. If $\alpha = \beta^p$ for some $\beta \in K$, then $\delta\alpha = p\beta^{p-1}\delta\beta = 0$. Conversely, suppose that $\delta\alpha = 0$ for all δ. Let $\{t_i\}_{i\in I}$ be a separating transcendence basis of K over k. By Lemma 3.1.1, $K = kK^p[\{t_i\}_{i\in I}]$. Write $\alpha = \sum_j c_j t^j$ in multi-index notation with $c_j \in kK^p$ for each $j \in \{0, 1, \ldots, p-1\}^I$. If δ_i are the derivations of K described in Remark 3.1.6, then $0 = \delta_i\alpha = \sum_j j_i c_j t^{j-1_i}$, where 1_i is the index with 1 in the ith entry and 0 in every other entry. Thus, $c_j = 0$ for all j such that $j_i \neq 0$ for some $i \neq 0$. In other words, $\alpha \in kK^p$.

(ii) Note that $\mathcal{O}_{V_K} = \mathcal{O}_V \otimes_{kK^p} K$. If $U \subset V$ is an open subset, define $\widetilde{\delta}$ on $\mathcal{O}_{V_K}(U)$ by $v \otimes u \mapsto v \otimes \delta u$ for $v \in \mathcal{O}_V(U)$ and $u \in K$. Thus,

$$\bigcap_{\delta \in D} \ker \widetilde{\delta} = \mathcal{O}_V \otimes_{kK^p} \bigcap_{\delta \in D} \ker \delta = \mathcal{O}_V \otimes_{kK^p} kK^p = \mathcal{O}_V. \qquad \square$$

Remark 3.1.8. If K is finitely generated over a perfect field k of characteristic p, then K is separably generated over k (e.g., [20, Corollary 4.4]). Furthermore, from the proof of Proposition 3.1.7, we see that to check $\delta\alpha = 0$ for all δ, it suffices to check $\delta_i\alpha = 0$ for all i. Similarly, $\widetilde{\delta}v = 0$ for all δ if and only if $\widetilde{\delta_i}v = 0$ for all i.

Part (ii) of Proposition 3.1.7 admits the following partial converse.

Proposition 3.1.9. *Let K be a field of characteristic p that is separably generated over a field k with* $\mathrm{tr.deg.}(K/k) = 1$. *Let δ be a nonzero k-derivation of K. Let Y be a geometrically*

integral curve over K, and let η be its generic point. Let $\mathrm{sp}(Y)$ *denote the topological space of* Y*.*

(i) Suppose that δ extends to a k-derivation $\widetilde{\delta}$ of $\mathcal{O}_Y$ whose kernel $\mathcal{O}'$ is such that $\mathcal{O}'_\eta$ is strictly larger than $kK(Y)^p$. Then the ringed space $Y' := (\mathrm{sp}(Y), \mathcal{O}')$ is a kK^p-variety such that $Y \cong Y'_K$.

(ii) If Y is smooth, projective, and of genus at least two, then there is at most one extension of δ to a k-derivation $\widetilde{\delta}$ of $\mathcal{O}_Y$. Furthermore, in the case that $\widetilde{\delta}$ exists, it is automatically true that $\mathcal{O}'_\eta$ is strictly larger than $kK(Y)^p$.

Proof. (i) Choose an element $t \in K \setminus kK^p$. By Proposition 3.1.2, K is a separable algebraic extension of $k(t)$, so we must have $\delta t \neq 0$. Furthermore, $\frac{1}{\delta t}\widetilde{\delta}$ is a k-derivation on $\mathcal{O}_Y$ that restricts to $\frac{1}{\delta t}\delta$ on K and has kernel $\mathcal{O}'$. Thus we may replace δ by $\frac{1}{\delta t}\delta$ to assume $\delta t = 1$. Define the homomorphism $\phi\colon \mathcal{O}' \otimes_{kK^p} K \to \mathcal{O}_Y$ of sheaves of K-algebras given by $r \otimes u \mapsto ur$ for $r \in \mathcal{O}'(U)$ and $u \in K$. We will show that ϕ is an isomorphism. Let $r \in (\mathcal{O}' \otimes_{kK^p} K)(U)$ be in the kernel of ϕ. We may write r as $r = \sum_{i=0}^{p-1} r_i \otimes t^i$, where $r_i \in \mathcal{O}'(U)$. Then $0 = \widetilde{\delta}(\phi(r)) = \sum_{i=0}^{p-1} i r_i t^{i-1}$, which forces $r = r_0 \otimes 1$. Then $r_0 = \phi(r) = 0$, so $r = 0$. This shows that ϕ is injective. Now choose any $s \in \mathcal{O}_Y(U)$. We have

$$K \cdot K(Y)^p = kK(Y)^p \otimes_{kK^p} K \subsetneq \mathcal{O}'_\eta \otimes_{kK^p} K \subset K(Y).$$

But $[K(Y) : K \cdot K(Y)^p] = p$, so $\mathcal{O}'_\eta \otimes_{kK^p} K = K(Y)$. Therefore we can write $s = \sum_{i=0}^{p-1} s_i t^i$ for $s_i \in \mathcal{O}'_\eta$. Suppose that $s_j \notin \mathcal{O}_Y(U)$ for some j, and assume that j is maximal. Then

$$\sum_{i=0}^{j} s_i t^i = s - \sum_{i=j+1}^{p-1} s_i t^i,$$

so

$$\sum_{i=0}^{j} s_i t^i \in \mathcal{O}_Y(U)$$

and

$$s_j = \frac{1}{j!}\widetilde{\delta}^j\left(\sum_{i=0}^{j} s_i t^i\right) \in \mathcal{O}_Y(U),$$

a contradiction. Thus, for all i, we have $s_i \in \mathcal{O}_Y(U)$. On the other hand, $s_i \in \mathcal{O}'_\eta$, so $\widetilde{\delta}(s_i) = 0$ and $s_i \in \mathcal{O}'(U)$. This proves that ϕ is surjective.

Let $U \subset Y$ be an affine open subset and $s \in \mathcal{O}_Y(U)$ be nonzero. If $r \in \mathcal{O}'(D(s))$, then there exists some $r' \in \mathcal{O}_Y(U)$ and an integer $i \geq 0$ such that $r = r'/s^{pi}$. Then $0 = \widetilde{\delta}(r) = \widetilde{\delta}(r')/s^{pi}$, so $\widetilde{\delta}(r') = 0$. This shows that $\mathcal{O}'(D(s)) = \mathcal{O}'(U)_{s^p}$, so we have an isomorphism of ringed spaces $(U, \mathcal{O}'|_U) \cong \operatorname{Spec} \mathcal{O}'(U)$. Therefore, the topological space of Y together with $\mathcal{O}'$ defines a kK^p-scheme Y'. The fact that ϕ is an isomorphism proves that $Y \cong Y'_K$.

(ii) Suppose that Y is smooth and has genus at least two. Suppose that $\widetilde{\delta}$ and $\widetilde{\delta}'$ are two extensions of δ to $\mathcal{O}_Y$. Then $\widetilde{\delta} - \widetilde{\delta}' \in \operatorname{Der}_K(\mathcal{O}_Y) = H^0(Y, \mathcal{T}_Y) = 0$. Thus, $\widetilde{\delta} = \widetilde{\delta}'$.

Now, $\delta^p(t) = 0$, so $\widetilde{\delta}^p$ is actually a K-derivation. Thus, as before, $\widetilde{\delta}^p = 0$. Localizing $\widetilde{\delta}$ at η gives a k-derivation $\widetilde{\delta}_\eta$ of $K(Y)$. Suppose for the sake of contradiction that $\ker \widetilde{\delta}_\eta = kK(Y)^p$. Then $\widetilde{\delta}_\eta$ has rank $p^2 - 1$ as a $kK(Y)^p$-linear map. This implies that $\widetilde{\delta}_\eta^p$ has rank at least $p^2 - p$, contradicting $\widetilde{\delta}_\eta^p = 0$. □

Corollary 3.1.10. *Let K be a field of characteristic p that is separably generated over a field k with* $\operatorname{tr.deg.}(K/k) = 1$. *Let δ be a nonzero k-derivation of K. Let Y be a geometrically integral smooth projective curve over K with $g(Y) \geq 2$. Then δ extends to a k-derivation of $\mathcal{O}_Y$ if and only if there exists a curve Y' over kK^p such that $Y \cong Y'_K$.*

Proof. This follows by combining Proposition 3.1.7(ii) and Proposition 3.1.9. □

Although it will not come up again, we note a phenomenon that occurs when Y is not projective. In this case, there may be many different curves Y' over kK^p such that $Y \cong Y'_K$. In the following proposition, we have a different Y' for every choice of étale morphism $r\colon Y \to \mathbb{A}^1_K$.

Proposition 3.1.11. *Assume the notation in the first three sentences of Proposition 3.1.9. Let $r\colon Y \to \mathbb{A}^1_K$ be an étale morphism of affine curves over K. Then there exists a unique morphism $r'\colon Y' \to \mathbb{A}^1_{kK^p}$ of affine curves over kK^p whose base extension to K is isomorphic to r.*

Proof. View r as an element of A. Because r is a separable morphism, $r \notin kK(Y)^p$. Therefore, by Proposition 3.1.9, we need to show that δ extends to a unique k-derivation $\widetilde{\delta}$ of A such that $\widetilde{\delta}r = 0$.

The proof that δ extends uniquely in this way generalizes the proof of Lemma 3.1.5. Certainly δ extends uniquely to a derivation of $K[r]$, and therefore to $K(r)$, that sends r to zero. By Lemma 3.1.5, δ then extends uniquely to a derivation $\widetilde{\delta}$ of $K(Y)$ that sends r to zero. All we need to do is show that $\widetilde{\delta}$ restricts to a derivation of A. If $y \in Y$ is a point, then there exists an open neighborhood $U \subset Y$ of y on which r is standard étale. That is, if $r(U) = \operatorname{Spec} R$, then U is R-isomorphic to $\operatorname{Spec}\big(R[s]/(g)\big)_h$, where $g, h \in R[s]$, the polynomial g is monic, and the derivative g' is a unit in $\big(R[s]/(g)\big)_h$. By the proof of Lemma 3.1.5, we have $\widetilde{\delta}s = -g^\delta/g' \in \big(R[s]/(g)\big)_h$. In other words, $\widetilde{\delta}$ restricts to a derivation of $\mathcal{O}_Y(U)$. Because A is covered by such open sets U, this means $\widetilde{\delta}$ restricts to a derivation of A. □

Now, suppose that Y is smooth and projective. In this case, any separable morphism $r\colon Y \to \mathbb{P}^1_K$ is étale outside of its ramification locus, so there is some dense open subset $U \subset Y$ and a curve U' over kK^p such that $U \cong U'_K$. Moreover, for every point $y \in Y$, there exists such an r unramified at y, so Y is covered by such open sets U. In general, the curves U' do not glue together to a smooth projective curve over kK^p. Furthermore, if Y' is the regular projective curve having U' as an open subvariety and Z is the smooth projective curve over kK^p with function field $kK(Y)^p$, then there exists a degree p inseparable morphism $Y' \to Z$ (the extensions $kK(Y)^p \subset kK^p(Y') \subset K(Y)$ are both inseparable of degree p). In general, Y' need not be smooth, and $Y' \to Z$ is the type of morphism described in (vi) of Proposition 3.4.1 below.

We will revisit the concept of descending curves from K to kK^p in Section 3.5, where we give effective ways to compute extensions of derivations as in Proposition 3.1.9.

3.2 The Cartier operator

Let k be a perfect field of characteristic p, let C be a geometrically integral smooth projective curve over k, and let $K := k(C)$. Let $t \in K \setminus K^p$. Any differential $\omega \in \Omega_{K/k}$ can be written uniquely as

$$\omega = \left(\omega_0^p + \omega_1^p t + \cdots + \omega_{p-1}^p t^{p-1}\right) dt \tag{3.2}$$

for some $\omega_0, \ldots, \omega_{p-1} \in K$.

Definition 3.2.1. Define the *Cartier operator* $\mathcal{C} \colon \Omega_{K/k} \to \Omega_{K/k}$ by $\mathcal{C}(\omega) = \omega_{p-1}\, dt$.

We recall the following basic facts about $\mathcal{C}$.

Proposition 3.2.2. *The Cartier operator does not depend on the choice of t, it is additive, and $\mathcal{C}(\alpha^p \omega) = \alpha \mathcal{C}(\omega)$ for all $\alpha \in K$ and $\omega \in \Omega_{K/k}$.*

Proof. For independence on t, see [19, Appendix 2, Sections 3 and 4]. The other two statements are easy to see from the definition of $\mathcal{C}$. □

Remark 3.2.3. If k is a perfect field algebraic over a finitely generated field k_0, C is defined over k_0, $K_0 := k_0(C)$, $t \in K_0 \setminus k_0 K_0^p$, and we are given a differential $\omega = \alpha\, dt \in \Omega_{K_0/k_0}$, then $\mathcal{C}(\omega) \in \Omega_{k_0^{1/p} K_0 / k_0^{1/p}}$ can be computed as follows. First use Proposition 3.1.3 to compute $e_0(U^p), \ldots, e_{p-1}(U^p) \in k_0(t^p)(U^p)$ such that

$$\alpha = \sum_{j=0}^{p-1} e_j(\alpha^p) t^j.$$

Then $\mathcal{C}(\omega)$ is simply $e_{p-1}^{1/p}(\alpha)\, dt$ (see Remark 3.1.4).

Proposition 3.2.4. *Let v be a place of K and $\omega \in \Omega_{K/k}$. If $\operatorname{ord}_v \omega \geq 0$, then $\operatorname{ord}_v \mathcal{C}(\omega) \geq 0$.*

If $\operatorname{ord}_v \omega < 0$*, then*

$$\operatorname{ord}_v \mathcal{C}(\omega) \geq \frac{\operatorname{ord}_v \omega + 1 - p}{p},$$

with equality if and only if $\operatorname{ord}_v \omega = -1 \pmod{p}$*. In particular, if* $\operatorname{ord}_v \omega = -1$*, then* $\operatorname{ord}_v \mathcal{C}(\omega) = -1$*.*

Proof. Let t be a uniformizer at v, and write

$$\omega = \left(\omega_0^p + \omega_1^p t + \cdots + \omega_{p-1}^p t^{p-1}\right) dt.$$

The valuations $\operatorname{ord}_v(\omega_i^p t^i)$ are all distinct modulo p. Therefore,

$$\operatorname{ord}_v \omega = \min_{0 \leq i \leq p-1} \operatorname{ord}_v(\omega_i^p t^i).$$

We first see that $\operatorname{ord}_v \omega \geq 0$ if and only if $\operatorname{ord}_v \omega_i \geq 0$ for all i. Therefore, $\operatorname{ord}_v \mathcal{C}(\omega) = \operatorname{ord}_v \omega_{p-1} \geq 0$. If $\operatorname{ord}_v \omega < 0$, then

$$\operatorname{ord}_v \omega = \min_{0 \leq i \leq p-1} \operatorname{ord}_v(\omega_i^p t^i) \leq \operatorname{ord}_v(\omega_{p-1}^p t^{p-1}) = p \operatorname{ord}_v \omega_{p-1} + p - 1 = p \operatorname{ord}_v \mathcal{C}(\omega) + p - 1,$$

with equality if and only if $\operatorname{ord}_v(\omega_i^p t^i)$ is minimal for $i = p - 1$. Rearranging this inequality gives the one stated in the proposition. □

Corollary 3.2.5. *Let* D *be a divisor on* C *and write* $D = E_1 - E_2$*, where* E_1 *and* E_2 *are effective divisors with disjoint supports. The Cartier operator restricts to a function* $H^0(C, \Omega_C(D)) \to H^0(C, \Omega_C(E_1))$*.*

Proof. Let d be the order of E_1 at a place v of C and $\omega \in H^0(C, \Omega_C(D))$. If $d = 0$, then $\operatorname{ord}_v \omega \geq 0$, so $\operatorname{ord}_v \mathcal{C}(\omega) \geq 0$. If $d > 0$, then regardless of the sign of $\operatorname{ord}_v \omega$,

$$\operatorname{ord}_v \mathcal{C}(\omega) \geq \frac{\operatorname{ord}_v \omega + 1 - p}{p} \geq \frac{-d + 1 - p}{p} \geq -d.$$

Thus, $\mathcal{C}(\omega) \in H^0(C, \Omega_C(E_1))$. □

Our main purpose for introducing the Cartier operator is the following.

Proposition 3.2.6. *If H is a subset of $\Omega_{K/k}$, we use the notation*

$$H^{\mathcal{C}=0} := \{\omega \in H \mid \mathcal{C}(\omega) = 0\} \qquad \text{and} \qquad H^{\mathcal{C}=1} := \{\omega \in H \mid \mathcal{C}(\omega) = \omega\}.$$

(i) The group homomorphisms $d\colon K \to \Omega_{K/k}$ and $d\log\colon K^\times \to \Omega_{K/k}$, where $d\log(\alpha) := d\alpha/\alpha$, induce isomorphisms $K/K^p \to \Omega_{K/k}^{\mathcal{C}=0}$ and $K^\times/K^{\times p} \to \Omega_{K/k}^{\mathcal{C}=1}$ respectively.

(ii) There exists an algorithm that takes as input a finitely generated field k_0, a geometrically integral smooth projective curve C over k_0 (set $K_0 := k_0(C)$), an element $t \in K_0 \backslash k_0 K_0^p$, and a differential $\omega := \beta\, dt \in \Omega_{\overline{k_0}K_0/\overline{k_0}}$ such that $\mathcal{C}(\omega) = 0$ (resp. $\mathcal{C}(\omega) = \omega$), and returns an element $\alpha \in \overline{k_0}K_0$ such that $d\alpha = \omega$ (resp. $d\log \alpha = \omega$).

Proof. Lang proves (i) in [19, Appendix 2, Theorem 4]. For (ii), let $K := \overline{k_0}(C)$. Let δ be the $\overline{k_0}$-derivation of K such that $\delta t = 1$ (see Section 3.1). Use Proposition 3.1.3 to write

$$\beta = \omega_0^p + \omega_1^p t + \cdots + \omega_{p-1}^p t^{p-1}$$

with $\omega_i \in K$ for each i. If $\mathcal{C}(\omega) = \omega_{p-1}\, dt = 0$, then we can compute α as an antiderivative of β:

$$\alpha = \omega_0^p t + \frac{1}{2}\omega_1^p t^2 + \cdots + \frac{1}{p-1}\omega_{p-2}^p t^{p-1}.$$

If $\mathcal{C}(\omega) = \omega$, then we use the identity $(\beta - \delta)^p = 0$ given by Lang in the proof of his Theorem 4 mentioned above (by $(\beta - \delta)^n$, we mean the map $\gamma \mapsto \beta\gamma - \delta\gamma$ on K composed with itself n times). Compute the sequence of elements

$$\beta, (\beta - \delta)\beta, (\beta - \delta)^2\beta, \ldots, (\beta - \delta)^{p-1}\beta \in K.$$

Take α to be the last nonzero element in this sequence, so that

$$d\log(\alpha) = \frac{d\alpha}{\alpha} = \frac{\delta\alpha}{\alpha}\,dt = \frac{\beta\alpha}{\alpha}\,dt = \omega. \qquad \square$$

Lemma 3.2.7.

(i) If k is a perfect field of characteristic p, V is a finite dimensional k-vector space, d is a nonzero integer, and $f\colon V \to V$ is an additive function such that $f(av) = a^{p^d} f(v)$ for all $a \in k$ and $v \in V$, then $\{v \in V \mid f(v) = v\}$ is a finite set.

(ii) There exists an algorithm that takes as input a finitely generated field k_0 of characteristic p, a nonzero integer d, a nonnegative integer n, and an n-by-n matrix M with entries in k_0 and returns the set $\{v \in \overline{k_0}^n \mid Mv^{p^d} = v\}$ (here v^{p^d} is the vector whose entries are the entries of v raised to the p^dth power).

Proof. (i) Note that $V^{f=1} := \{v \in V \mid f(v) = v\}$ is an $\mathbb{F}_{p^{|d|}}$-vector space. Suppose $v_1, \ldots, v_n \in V^{f=1}$ is a collection of elements such that

1. $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ are k-linearly independent in V for every i,
2. $v_1, \ldots, v_n$ are k-linearly dependent in V.

There exists some i and $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in k$ such that

$$a_1 v_1 + \cdots + a_{i-1} v_{i-1} + v_i + a_{i+1} v_{i+1} + \cdots + a_n v_n = 0.$$

By applying f and subtracting the result from the original equation, we get

$$(a_1 - a_1^{p^d}) v_1 + \cdots + (a_{i-1} - a_{i-1}^{p^d}) v_{i-1} + (a_{i+1} - a_{i+1}^{p^d}) v_{i+1} + \cdots + (a_n - a_n^{p^d}) v_n = 0.$$

It follows that, for all j, $a_j - a_j^{p^d} = 0$ and therefore $a_j \in \mathbb{F}_{p^{|d|}}$. Thus, $v_1, \ldots, v_n$ are $\mathbb{F}_{p^{|d|}}$-linearly dependent.

Now, if $\{v_1, \ldots, v_n\} \subset V^{f=1}$ is any set of elements that are k-linearly dependent in V, then some subset will satisfy 1 and 2 above, and so $v_1, \ldots, v_n$ are $\mathbb{F}_{p^{|d|}}$-linearly dependent by the first paragraph. Therefore,

$$\dim_{\mathbb{F}_{p^{|d|}}} V^{f=1} \leq \dim_k V,$$

so $V^{f=1}$ is finite.

(ii) The function $f\colon \overline{k_0}^n \to \overline{k_0}^n$ given by $f(v) = Mv^{p^d}$ is additive and satisfies $f(av) = a^{p^d} f(v)$ for all $a \in k$ and $v \in \overline{k_0}^n$. The set $\{v \in \overline{k_0}^n \mid Mv^{p^d} = v\}$ is the set of $\overline{k_0}$-points of a variety $W \subset \mathbb{A}^n_{k_0}$ that is 0-dimensional by part (i). Compute and return $W(\overline{k_0})$. □

Corollary 3.2.8. *There exists an algorithm that takes as input a finitely generated field k_0 (set $k := \overline{k_0}$), a geometrically integral smooth projective curve C over k_0, and a divisor D on C and returns $H^0(C_k, \Omega_{C_k}(D))^{\mathcal{C}=1}$.*

Proof. First write $D = E_1 - E_2$ for effective divisors E_1 and E_2 with disjoint supports. Compute a k-basis $\omega_1, \ldots, \omega_n$ of $H^0(C, \Omega_C(E_1))$. By Corollary 3.2.5, $\mathcal{C}$ restricts to a function $H^0(C, \Omega_C(E_1)) \to H^0(C, \Omega_C(E_1))$. For each i, compute elements $c_{i1}, \ldots, c_{in} \in k$ such that $\mathcal{C}(\omega_i) = \sum_{j=1}^n c_{ij}\omega_j$, and let $M := (c_{ij})$. Then $H^0(C_k, \Omega_{C_k}(E_1))^{\mathcal{C}=1}$ is in bijection with

$$\{v \in k^n \mid Mv^{1/p} = v\}.$$

Compute this set using Lemma 3.2.7(ii). Then compute $H^0(C_k, \Omega_{C_k}(D))^{\mathcal{C}=1}$, which is the intersection of the finite set $H^0(C_k, \Omega_{C_k}(E_1))^{\mathcal{C}=1}$ with the subspace $H^0(C_k, \Omega_{C_k}(D))$ inside $H^0(C_k, \Omega_{C_k}(E_1))$. □

3.3 Regular nonsmooth curves

For curves over a perfect field, smooth is equivalent to regular. This is not true if the field is imperfect. A standard example is the following.

Example 3.3.1. Let $p \geq 3$ be prime and $K := \mathbb{F}_p(t)$. Let X be the affine plane curve over K given by $y^2 = x^p - t$. By the Jacobian criterion, X has one nonsmooth closed point P, whose ideal is $\mathfrak{m}_P = (x^p - t, y) \subset K[x, y]$. However,

$$\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2 + (y^2 - x^p + t)} = \frac{(x^p - t, y)}{((x^p - t)^2, y^2, (x^p - t)y, y^2 - x^p + t)} = \frac{(x^p - t, y)}{(x^p - t, y^2)} \cong \frac{(y)}{((x^p - t)y, y^2)}.$$

This is a 1-dimensional vector space over $K[x]/(x^p - t)$, which is the residue field of P. So, X is regular at P.

Proposition 3.3.2. *Let K be a field of characteristic p, and let X be a geometrically integral regular projective curve over K. Let X_i be a regular projective curve over K with function field $K \cdot K(X)^{p^i}$. Let $g_i := g(X_i)$ and $\widetilde{g} := g(\widetilde{X_{\overline{K}}})$, where $\widetilde{X_{\overline{K}}}$ is the normalization of $X_{\overline{K}}$. Then*

$$g_0 \geq g_1 \geq g_2 \geq \cdots$$

and $g_i = \widetilde{g}$ for sufficiently large i. For such i, the curve X_i is smooth.

Proof. First, notice that for $i \geq 0$,

$$K^{p^{-i}}(\widetilde{X_{K^{p^{-i}}}}) = K^{p^{-i}} \cdot K(X) \cong K \cdot K(X)^{p^i} = K(X_i),$$

so $g_i = g(\widetilde{X_{K^{p^{-i}}}})$. Then

$$g_i = g(\widetilde{X_{K^{p^{-i}}}}) = g\left((\widetilde{X_{K^{p^{-i}}}})_{K^{p^{-i-1}}}\right) \geq g\left(\left((\widetilde{X_{K^{p^{-i}}}})_{K^{p^{-i-1}}}\right)^{\sim}\right) = g(\widetilde{X_{K^{p^{-i-1}}}}) = g_{i+1}$$

(for the inequality step, see, e.g., [14, Exercise IV.1.8]). Similarly, $g_i \geq \widetilde{g}$, with equality if and only if X_i is smooth.

Now, $\widetilde{X_{\overline{K}}}$ is smooth and definable over some finite extension L of K, so $\widetilde{X_L}$ is smooth. Let M be the maximal subextension of L that is separable over K. Then $L^{p^e} \subset M$ for some e, so $\widetilde{X_{M^{p^{-e}}}}$ is smooth. The field $M^{p^{-e}}$ is separable over $K^{p^{-e}}$, so $\widetilde{X_{K^{p^{-e}}}}$ is smooth by

Theorem 2.1.1. Thus, $g_i = \widetilde{g}$ for all $i \geq e$. $\square$

Lemma 3.3.3. *Let K be a field of characteristic p, let X be a geometrically integral regular curve over K. Let L and K' be finite extensions of K that are linearly disjoint over K. For a field M with $K \subset M \subset L$, we denote $M' := MK'$. Let $x_L \in X_L$ be a closed point, and let $x_{L'} \in (\widetilde{X_{K'}})_{L'}$ be in the preimage of x_L. If x_L is not a regular point of X_L, then $x_{L'}$ is also not a regular point of $(\widetilde{X_{K'}})_{L'}$. Therefore, if X_L is nonregular, then $(\widetilde{X_{K'}})_{L'}$ is nonregular.*

Proof. We first prove this in the case where L/K is a finite purely inseparable extension of degree p generated by an element t. In this case, the morphism $X_L \to X$ is a homeomorphism on the level of topological spaces. Let $x \in X$ be the image of x_L. Then

$$\mathcal{O}_{X_L,x_L} = \varinjlim_{\substack{U \subset X_L \\ x_L \in U}} \mathcal{O}_{X_L}(U) = \varinjlim_{\substack{V \subset X \\ x \in V}} \mathcal{O}_{X_L}(V_L) = \varinjlim_{\substack{V \subset X \\ x \in V}} (\mathcal{O}_X(V) \otimes_K L) = (\varinjlim_{\substack{V \subset X \\ x \in V}} \mathcal{O}_X(V)) \otimes_K L = \mathcal{O}_{X,x} \otimes_K L. \tag{3.3}$$

By assumption, $\mathcal{O}_{X_L,x_L}$ is not a regular local ring, so there exists some element $g \in \widetilde{\mathcal{O}_{X_L,x_L}}$ (the normalization of $\mathcal{O}_{X_L,x_L}$) that is not in $\mathcal{O}_{X_L,x_L}$. Write

$$g = g_0 + g_1 t + \cdots + g_{p-1} t^{p-1},$$

where $g_i \in K(X)$. Let $x_{K'} \in \widetilde{X_{K'}}$ be the image of $x_{L'}$. For any i, if $g_i \in \mathcal{O}_{\widetilde{X_{K'}},x_{K'}}$, then $g_i \in \mathcal{O}_{X,x}$ because $\mathcal{O}_{\widetilde{X_{K'}},x_{K'}}$ is integral over $\mathcal{O}_{X,x}$ and $\mathcal{O}_{X,x}$ is a regular local ring. But, because $g \notin \mathcal{O}_{X_L,x_L}$, there must be some i such that $g_i \notin \mathcal{O}_{X,x}$. Therefore, $g_i \notin \mathcal{O}_{\widetilde{X_{K'}},x_{K'}}$ as well. But, because L and K' are linearly disjoint over K, we also have $[L' : K'] = p$, $L' = K'(t)$, and $\mathcal{O}_{(\widetilde{X_{K'}})_{L'},x_{L'}} = \mathcal{O}_{\widetilde{X_{K'}},x_{K'}} \otimes_{K'} L'$. This proves that $g \notin \mathcal{O}_{(\widetilde{X_{K'}})_{L'},x_{L'}}$. But, g is integral over $\mathcal{O}_{(\widetilde{X_{K'}})_{L'},x_{L'}}$, so $\mathcal{O}_{(\widetilde{X_{K'}})_{L'},x_{L'}}$ is not a regular local ring, i.e., $x_{L'}$ is not a regular point.

Now consider the case of general L. Let M_0/K be the maximal separable subextension

of L. Consider a tower of fields

$$M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = L$$

such that $[M_i : M_{i-1}] = p$ for all $1 \leq i \leq n$. For each i, let x_{M_i} be the image of x_L in X_{M_i}. We know x_{M_0} is a regular point because M_0 is separable over K. Thus, there exists some $1 \leq j \leq n$ such that $x_{M_{j-1}}$ is a regular point and x_{M_j} is not a regular point. Let $y_{L'} \in (\widetilde{X_{M'_{j-1}}})_{L'}$ be a preimage of $x_{L'}$ and $x_{M'_j} \in (\widetilde{X_{M'_{j-1}}})_{M'_j}$ its image. By the previous paragraph, $x_{M'_j}$ is a nonregular point, making $y_{L'}$ a nonregular point as well. The morphism $(\widetilde{X_{M'_{j-1}}})_{L'} \to (\widetilde{X_{K'}})_{L'}$ is a birational morphism of curves. Therefore, $x_{L'}$ cannot be a regular point. □

Corollary 3.3.4. *Let K be a field of characteristic p, let X be a geometrically integral regular curve over K, and let x be a closed point of X. Let L/K be an algebraic extension linearly disjoint with the residue field of x. Then every point in the preimage of x in X_L is a regular point.*

Proof. Let $x_L \in X_L$ be in the preimage of x. Let K' be the residue field of x, and let $L' := LK'$. Let $x_{K'} \in \widetilde{X_{K'}}$ be a degree 1 point in the preimage of x, and let $x_{L'} \in (\widetilde{X_{K'}})_{L'}$ be in the preimages of both x_L and $x_{K'}$. Because $x_{K'}$ is a regular degree 1 point, it must be a smooth point (the proof is the same as the proof that regular implies smooth over an algebraically closed field, e.g., [14, Theorem I.5.1]). Therefore, $x_{L'}$ is a smooth point, so it is regular. If L/K is a finite extension and x_L were nonregular, then $x_{L'}$ would be nonregular by Lemma 3.3.3. Thus, x_L is regular.

Now suppose that L/K is infinite, and take any element $f \in L(X)$ that is integral over $\mathcal{O}_{X_L,x_L}$. There exists some finite subextension M/K such that $f \in M(X)$ and f is integral over $\mathcal{O}_{X_L,x_L} \cap M(X)$. Let $x_M \in X_M$ be the image of x_L, so that $\mathcal{O}_{X_M,x_M} = \mathcal{O}_{X_L,x_L} \cap M(X)$. By the previous paragraph, x_M is a regular point, so $f \in \mathcal{O}_{X_M,x_M} \subset \mathcal{O}_{X_L,x_L}$. This proves that x_L is regular. □

3.4 Algorithms and nonsmooth curves

It will be convenient to reduce the problem of computing $X(K)$, when X is a regular nonsmooth curve over K, to certain special cases. The following proposition describes the first such reduction.

Proposition 3.4.1. *Suppose there exists an algorithm that takes Input 2.1.2 data (p, k_0, m, K_0, X) as well as the extra input*

(vi) a geometrically integral smooth projective curve Y over K_0 together with a degree p inseparable morphism $\pi\colon X \to Y$ over K_0

and returns $X(K)$. Then there exists an algorithm that returns $X(K)$ without assuming (vi).

Proof. Let X_i be the normalization of $X^{(p^i)}$, the p^i-power Frobenius twist of X. Then $K_0(X_i) = K_0 \cdot K_0(X_i)^{p^i}$. Compute the curves X_i for $i = 1, 2, 3, \ldots, n$, where n is the smallest positive integer such that X_n is smooth, which exists by Proposition 3.3.2. The relative Frobenius morphisms lift to a sequence of morphisms

$$X = X_0 \to X_1 \to X_2 \to \cdots \to X_{n-1} \to X_n.$$

The curve X_{n-1} is nonsmooth and the morphism $X_{n-1} \to X_n$ satisfies the condition in (vi) (Lemma 3.1.1 says that $X_{n-1} \to X_n$ is degree p). Thus, use the presumed algorithm to compute the finite set $X_{n-1}(K)$. Then compute $X(K)$ by computing preimages in the above sequence of morphisms. □

The next proposition describes the second important reduction. The idea is to enlarge the fields k_0 and K_0 in a way that maintains all the hypotheses of Input 2.1.2 but makes K_0 the function field of a geometrically integral smooth curve over k_0.

Proposition 3.4.2. *There exists an algorithm that takes Input 2.1.2 data (p, k_0, m, K_0, X) and returns data (k_0', K_0', C), where k_0' is a finitely generated field extension of k_0 contained*

in $\overline{K_0}$, $K_0' = k_0' K_0$, *and* C *is a geometrically integral smooth projective curve over* k_0', *such that*

(i) $K_0' \cong k_0'(C)$ *and*

(ii) $(\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}$ *is regular but not smooth.*

Proof. Determine an integral variety T such that $K_0 = k_0(T)$. Compute an integer $n \geq 0$ such that the reduced variety of $T_{k_0^{p^{-n}}}$ is geometrically reduced. Replace k_0 by $k_0^{p^{-n}}$, K_0 by $k_0^{p^{-n}} K_0$, and T by the reduced variety of $T_{k_0^{p^{-n}}}$. Now, K_0 is separably generated over k_0. Take some nonempty affine open subset $T' \subset T$ given as the zero locus of polynomials $f_1(x_1, \ldots, x_M), \ldots, f_r(x_1, \ldots, x_M)$ in $\mathbb{A}^M_{k_0}$. The K_0-vector space Ω_{K_0/k_0} has dimension m and is spanned by $dx_1, \ldots, dx_M$. For each $1 \leq j \leq r$, there is a linear relation

$$\sum_{i=1}^{M} \frac{\partial f_j}{\partial x_i} dx_i = 0.$$

Use these to find $1 \leq i_1 < i_2 < \cdots < i_m \leq M$ such that $dx_{i_1}, \ldots, dx_{i_m}$ form a basis of Ω_{K_0/k_0}. It follows that $\{x_{i_1}, \ldots, x_{i_m}\}$ is a separating transcendence basis for K_0 over k_0 ([9, Theorem 16.14]). Rename $x_{i_1}, \ldots, x_{i_m}$ as $t_1, \ldots, t_m$ to match the notation in Input 2.1.2.

Next, find nonnegative integers $e_1, \ldots, e_m$ and $1 \leq j \leq m$ with $F := K_0(t_1^{p^{-e_1}}, \ldots, t_m^{p^{-e_m}})$ and $L := K_0(t_1^{p^{-e_1}}, \ldots, t_j^{p^{-e_j-1}}, \ldots, t_m^{p^{-e_m}})$ such that X_F is regular but X_L is not. This is possible because X is regular and $X_{K_0^{p^{-e}}}$ is nonregular for some e by Proposition 3.3.2. Rename $t_1, \ldots, t_m$ again so that $j = 1$.

Determine an integral curve U over $k_0(t_2^{p^{-e_2}}, \ldots, t_m^{p^{-e_m}})$ whose function field is $K_0(t_2^{p^{-e_2}}, \ldots, t_m^{p^{-e_m}})$. Compute a finite extension k_0' of $k_0(t_2^{p^{-e_2}}, \ldots, t_m^{p^{-e_m}})$ such that the reduced variety of $U_{k_0'}$ has geometrically integral irreducible components. Compute the normalization C of the projective closure of any irreducible component of the reduced variety of $U_{k_0'}$. Now, C is not necessarily smooth. To fix this, repeatedly replace k_0' by $(k_0')^{1/p}$ and replace C by its normalization in the enlarged field k_0' until C is smooth. This is possible because of Proposition 3.3.2.

Let $K_0' := k_0' K_0$. Now, $(\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}$ is not necessarily regular. We will find some integer $N \geq 0$ and replace k_0' by $(k_0')^{p^{-N}}$ and K_0' by $(k_0')^{p^{-N}} K_0'$ such that the following condition is true for every closed point x of $\widetilde{X_{K_0'}}$:

$$\text{every point in the preimage of } x \text{ in } (\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'} \text{ is regular.} \tag{3.4}$$

First, note that if x satisfies (3.4) and $n \geq 0$, then x still satisfies (3.4) after making the following replacements

$$k_0' \text{ by } (k_0')^{p^{-n}}, \qquad K_0' \text{ by } (k_0')^{p^{-n}} K_0', \qquad x \text{ by its preimage in } \widetilde{X_{(k_0')^{p^{-n}}K_0'}}. \tag{3.5}$$

Second, note that if x does not satisfy (3.4), then x is a nonsmooth point. Compute the finitely many nonsmooth points of $\widetilde{X_{K_0'}}$. Let x be such a nonsmooth point. In the following paragraph, we show that we can find some integer $n \geq 0$ and make the replacements in (3.5) such that x satisfies (3.4). Doing this for every nonsmooth point x then ensures that $(\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}$ is regular.

First, compute the residue field ℓ of x. Note that if $n \geq 0$ and we make the replacements in (3.5) and also replace

$$\ell \text{ by } (k_0')^{p^{-n}} \ell, \tag{3.6}$$

then ℓ is still the residue field of x. Determine an integral curve V over k_0' whose function field is ℓ. Compute an integer $n_1 \geq 0$ such that the reduced variety of $V_{(k_0')^{p^{-n_1}}}$ is geometrically reduced. Make the replacements in (3.5) and (3.6) with $n := n_1$ so that ℓ is separably generated over k_0'. Because K_0 is separable over $k_0(t_1, \ldots, t_m)$, the field K_0' is separable over $k_0'(t_1)$. Compute the integer n_2 such that $p^{n_2} = [\ell : K_0']_i = [\ell : k_0'(t_1)]_i$. By Proposition 3.1.2, $t_1 \in k_0' \ell^{p^{n_2}}$, so for some $\alpha_1, \ldots, \alpha_q \in k_0'$ and $u_1, \ldots, u_q \in \ell$,

$$t_1 = \alpha_1 u_1^{p^{n_2}} + \cdots + \alpha_q u_q^{p^{n_2}}.$$

Make the replacements in (3.5) and (3.6) again with $n := n_2$ to guarantee that $t_1^{p^{-n_2}} \in \ell$. We claim that x now satisfies (3.4). Let ℓ_s/K_0' be the maximal separable subextension of ℓ, and let ℓ_g be the Galois closure of ℓ_s. Then ℓ_g is separable over $k_0'(t_1)$, and therefore, $t_1^{1/p} \notin \ell_g$ and $\ell = \ell_s(t_1^{p^{-n_2}})$. The ℓ_g-algebra

$$\ell \otimes_{K_0'} \ell_g = \ell_s(t_1^{p^{-n_2}}) \otimes_{K_0'} \ell_g$$

is isomorphic to the direct product of $[\ell_s : K_0']$ copies of $\ell_g(t_1^{p^{-n_2}})$. We also know that $t_1^{1/p} \notin \overline{k_0'}\ell_g$ because $\overline{k_0'}\ell_g$ is separable over $\overline{k_0'}(t_1)$, so $\ell_g(t_1^{p^{-n_2}})$ and $\overline{k_0'}\ell_g$ are linearly disjoint over ℓ_g. Therefore, over ℓ_g, the field $\overline{k_0'}\ell_g$ is linearly disjoint with the residue field of every point in the preimage of x in $(\widetilde{X_{K_0'}})_{\ell_g}$. By Corollary 3.3.4, every point in the preimage of x in $\big((\widetilde{X_{K_0'}})_{\ell_g}\big)_{\overline{k_0'}\ell_g}$ is regular. But,

$$\big((\widetilde{X_{K_0'}})_{\ell_g}\big)_{\overline{k_0'}\ell_g} = \big((\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}\big)_{\overline{k_0'}\ell_g},$$

so every point in the preimage of x in $(\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}$ is regular.

Note that L and $k_0'F$ are linearly disjoint over F because $k_0'F$ does not contain a pth root of $t_1^{p^{-e_1}}$. Therefore, by the last sentence of Lemma 3.3.3 (the K, L, K', and L' in the statement of Lemma 3.3.3 are the F, L, $k_0'F$, and $k_0'L$ here, respectively), the curve $(\widetilde{X_{k_0'F}})_{k_0'L}$ is nonregular, so $\widetilde{X_{k_0'F}}$ is not smooth. But, $K_0' = k_0'K_0 \subset k_0'F$, so $\widetilde{X_{K_0'}}$ is not smooth and therefore $(\widetilde{X_{K_0'}})_{\overline{k_0'}K_0'}$ is not smooth. □

In light of Proposition 3.4.1 and Proposition 3.4.2, we define the following input to be used instead of Input 2.1.2.

Input 3.4.3.

(i) a prime number p,

(ii) a field k_0 finitely generated over $\mathbb{F}_p$,

(iii) *a geometrically integral smooth projective curve C over k_0 with function field $K_0 := k_0(C)$,*

(iv) *a geometrically integral nonsmooth projective curve X over K_0 such that $X_{\overline{k_0}K_0}$ is regular,*

(v) *a geometrically integral smooth projective curve Y over K_0, and*

(vi) *a degree p inseparable morphism $\pi\colon X \to Y$ over K_0.*

These data will be written $(p, k_0, C, K_0, X, Y, \pi)$ for short. As in Input 2.1.2, we will also assume the notation $k := \overline{k_0}$ and $K := kK_0$. Some lemmas and propositions that follow will only use the data (p, k_0, C, K_0), and some will use (p, k_0, C, K_0, Y).

Remark 3.4.4. Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data. Then $K_0(Y) = K_0 \cdot K_0(X)^p$, so by Proposition 3.3.2, the genus of Y is equal to the absolute genus $\widetilde{g}$ of X.

Lemma 3.4.5. *Let K be a field of characteristic p, and let $\pi\colon X \to Y$ be a surjective inseparable degree p morphism of integral curves over K, where X is regular. If z is any element of $K(X) \setminus \pi^*K(Y)$, then $z^p \in \pi^*K(Y)$. Let $r \in K(Y)$ be the rational function such that $z^p = r \circ \pi$. If $P \in \pi(X(K))$ and r is defined at P, then $r(P) \in K^p$.*

Proof. Because π is degree p and inseparable, we have $z^p \in K(X)^p \subset \pi^*K(Y)$. Let $Q \in X(K)$ be a point such that r is defined at $\pi(Q)$. Then, by the equality $z^p = r \circ \pi$, the function z^p is defined at Q. Therefore, $z^p \in \mathcal{O}_{X,Q}$, and, because X is regular, $z \in \mathcal{O}_{X,Q}$. Hence, $r(\pi(Q)) = z(Q)^p \in K^p$. □

The following is the main procedure that allows us to compute K-points on X.

Proposition 3.4.6. *There exists an algorithm that takes Input 3.4.3 data $(p, k_0, C, K_0, X, Y, \pi)$, a geometrically integral smooth projective curve Z over K_0, and an inseparable K_0-morphism $f : Z \to Y$ and returns the set*

$$f(Z(K)) \cap \pi(X(K)).$$

Proof. Choose $z \in K_0(X) \setminus \pi^* K_0(Y)$ and compute r such that $z^p = r \circ \pi$ as in Lemma 3.4.5. The composition $g := r \circ f$ is an inseparable morphism $Z \to \mathbb{P}^1_{K_0}$, so $K(Z)/K(g)$ is inseparable. By Proposition 3.1.2, $g \in K_0 \cdot K_0(Z)^p$, and $K_0 \cdot K_0(Z)^p$ is the image of the field embedding $F^* \colon K_0(Z^{(p)}) \to K_0(Z)$ induced by the relative Frobenius $F \colon Z \to Z^{(p)}$. Determine an element $s \in K_0(Z^{(p)})$ such that $r \circ f = g = s \circ F$.

Let V be the curve defined over $k_0 K_0^p$ given by the same polynomials as $Z^{(p)}$, so that $Z^{(p)} \cong V_{K_0}$. Choose any $t \in K_0 \setminus k_0 K_0^p$, and let δ be the derivation of K_0 such that $\delta t = 1$ (see Remark 3.1.6). Because Z is smooth, V is smooth and therefore geometrically reduced. So, extend δ to a derivation $\widetilde{\delta}$ of $\mathcal{O}_{Z^{(p)}}$ as in Proposition 3.1.7. Determine the maximal affine open subset $U \subset Z$ on which $r \circ f$ is defined. Compute the finitely many poles of r in $Y(\overline{K})$. For each pole Q, compute its preimages in X and Z and determine if $Q \in f(Z(K)) \cap \pi(X(K))$. According to Lemma 3.4.5, the remaining points in $f(Z(K)) \cap \pi(X(K))$ are points of the form $f(Q)$ with $Q \in U(K)$ such that $r(f(Q)) \in K^p$.

Claim 1. For $Q \in U(K)$, we have $r(f(Q)) \in K^p$ if and only if Q is a zero of $\widetilde{\delta}(s) \circ F$.

First, C is geometrically integral, so we may consider the extension of δ to a derivation of K by defining $\delta(c) = 0$ for all $c \in k$. In this way, for $\alpha \in K$, we have $\alpha \in K^p$ if and only if $\delta(\alpha) = 0$ by Remark 3.1.8. Consider an embedding $U \subset \mathbb{A}^n_{K_0}$ and write Q in coordinates as $Q = (\alpha_1, \ldots, \alpha_n) \in U(K)$. Then $U^{(p)}$ is embedded in $\mathbb{A}^n_{K_0}$ as well with defining polynomials the same as U but with coefficients raised to the pth power. The function s is defined on $U^{(p)}$ and can be thought of as a polynomial in the coordinates $x_1, \ldots, x_n$ on $\mathbb{A}^n_{K_0}$. Compute

$$\begin{aligned}
\delta(r(f(\alpha_1, \ldots, \alpha_n))) &= \delta(s(\alpha_1^p, \ldots, \alpha_n^p)) \\
&= \sum_{j=1}^{n} \frac{\partial s}{\partial x_j}(\alpha_1^p, \ldots, \alpha_n^p)\delta(\alpha_j^p) + \widetilde{\delta}(s)(\alpha_1^p, \ldots, \alpha_n^p) \\
&= (\widetilde{\delta}(s) \circ F)(\alpha_1, \ldots, \alpha_n).
\end{aligned}$$

Combining the previous two sentences, $r(f(Q)) \in K^p$ if and only if $(\widetilde{\delta}(s) \circ F)(Q) = 0$.

Claim 2. The rational function $\widetilde{\delta}(s) \circ F$ is not identically zero on Z.

Suppose for the sake of contradiction that $\widetilde{\delta}(s) \circ F = 0$. Then $\widetilde{\delta}(s) = 0$, so Remark 3.1.8 says $s \in (k_0 K_0^p)(V)$. The field homomorphism $F^*\colon K_0(Z^{(p)}) \to K_0(Z)$ maps $(k_0 K_0^p)(V)$ to $k_0 K_0(Z)^p$, so $s \circ F \in k_0 K_0(Z)^p$. Then $K(Z) \supset k_0^{1/p} K_0(Z)$ contains a pth root of $s \circ F = r \circ f$, so the field homomorphism $f_K^*\colon K(Y) \to K(Z)$ factors as

$$K(Y) \xrightarrow{\pi_K^*} K(X) \longrightarrow K(Z).$$

So, there exists a nonconstant morphism $Z_K \to X_K$. But, Z_K is smooth and X_K is not, a contradiction ([32, Tag 0CCW]). So, $\widetilde{\delta}(s) \neq 0$ and $\widetilde{\delta}(s) \circ F \neq 0$.

To finish the algorithm, compute the finitely many zeros of $\widetilde{\delta}(s) \circ F$. For each such zero Q, compute the preimage of $f(Q)$ in X and determine if $f(Q) \in \pi(X(K))$. □

Lemma 3.4.7. *There exists an algorithm that takes Input 3.4.3 data $(p, k_0, C, K_0, X, Y, \pi)$ and a finite separable extension L_0/K_0 and returns a finite extension ℓ_0'/k_0, the field $L_0' := \ell_0' L_0$, and a geometrically integral smooth curve C' over ℓ_0' such that $(p, \ell_0', C', L_0', X_{L_0'}, Y_{L_0'}, \pi_{L_0'})$ are valid data for Input 3.4.3.*

Proof. The base extension X_{L_0} is again regular and nonsmooth by Theorem 2.1.1. The extension kL_0/K is also separable, so X_{kL_0} is regular as well. Thus, we may apply Proposition 3.4.2 to the Input 2.1.2 data $(p, k_0, 1, L_0, X_{L_0})$ and get data (ℓ_0', L_0', C'). The properties of ℓ_0', L_0', and C' guaranteed by Proposition 3.4.2 prove the desired claim. □

Remark 3.4.8. Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data and $(p, \ell_0', C', L_0', X_{L_0'}, Y_{L_0'}, \pi_{L_0'})$ be as in Lemma 3.4.7. Set $L' := \overline{\ell_0'} L_0'$. To compute $X(K)$, it suffices to compute $X_{L_0'}(L')$ and then determine which L'-points are K-points. It will often be convenient to enlarge K_0 to assume certain properties of Y. In those cases, we will invoke this fact and replace $(p, k_0, C, K_0, X, Y, \pi)$ by $(p, \ell_0', C', L_0', X_{L_0'}, Y_{L_0'}, \pi_{L_0'})$.

3.5 Explicit descent and semistable models

In this section, we study explicit fpqc descent of curves with respect to transcendental or purely inseparable extensions of the base field. If k is a field of characteristic p, K is finitely generated over k, and Y is a curve over K, then we can ask whether there exists a curve Y' over k or over kK^{p^n} for some n such that $Y \cong (Y')_K$.

Definition 3.5.1. Let k be a field, K be a field finitely generated over k, and V be a variety over K.

(i) We say that V is *constant* if there exists a variety V_0 defined over k such that $V \cong (V_0)_K$.

(ii) We say that V is *isotrivial* if there exist algebraic extensions L/K and ℓ/k with $\ell \subset L$ and a variety V_0 over ℓ such that $V_L \cong (V_0)_L$.

The proof of Theorem 1.0.2 will handle the cases where Y is isotrivial and Y is non-isotrivial separately. For this reason, we will need a way to detect when a curve is isotrivial. In the case where V is a smooth isotrivial curve, it turns out that the L and ℓ in the above definition can be chosen to be separable extensions of K and k respectively. To prove this, we first need the following lemma.

Lemma 3.5.2. *There exists an algorithm that takes as input a finitely generated field K_0 and geometrically integral smooth projective curves C and D over K_0 with $g(C) = g(D) \geq 2$ and returns the set of isomorphisms $C_{\overline{K_0}} \to D_{\overline{K_0}}$ over $\overline{K_0}$.*

Proof. Embed C and D in $\mathbb{P}^N_{K_0}$ via the tricanonical embedding. An isomorphism $C \to D$ over $\overline{K_0}$ induces an isomorphism $H^0(D_{\overline{K_0}}, \Omega^{\otimes 3}_{D_{\overline{K_0}}}) \to H^0(C_{\overline{K_0}}, \Omega^{\otimes 3}_{C_{\overline{K_0}}})$. Thus, every isomorphism $C_{\overline{K_0}} \to D_{\overline{K_0}}$ is the restriction of an automorphism of $\mathbb{P}^N_{\overline{K_0}}$, i.e., an element of $\mathrm{PGL}_{N+1}(\overline{K_0})$. In the next paragraph, we will construct a closed subvariety $Z \subset (\mathrm{PGL}_{N+1})_{K_0}$ whose L-points, for any field extension L/K_0, parameterize the automorphisms of $\mathbb{P}^{N+1}_L$ that restrict to isomorphisms $C_L \to D_L$. So, by the discussion so far, we have K_0-morphisms $\Phi\colon \underline{\mathrm{Isom}}(C, D) \to Z$ and $\Psi\colon Z \to \underline{\mathrm{Isom}}(C, D)$ such that $\Psi \circ \Phi$ is the identity on $\underline{\mathrm{Isom}}(C, D)$.

Let $S = K_0[x_0, \ldots, x_N]$ be the homogeneous coordinate ring of $\mathbb{P}^N_{K_0}$. Let I and J be the homogeneous ideals in S for C and D respectively. Let $f_1, \ldots, f_m$ be generators for J. For each $1 \leq \ell \leq m$, let d_ℓ be the degree of f_ℓ and compute a K_0-basis $z_1, \ldots, z_{n_\ell}$ for $(S/I)_{d_\ell}$ (the degree d_ℓ graded piece of the homogeneous coordinate ring of C). The group PGL_{N+1} is an open subvariety of $\mathbb{P}^{(N+1)^2-1}$ with points thought of as $(N+1)$-by-$(N+1)$ matrices (a_{ij}). Let A denote the matrix (a_{ij}), where the a_{ij} are indeterminates, and let x denote the column vector (x_i). For each $1 \leq \ell \leq m$, compute the homogeneous elements $h_{\ell 1}, \ldots, h_{\ell n_\ell} \in K_0[\{a_{ij}\}]$ such that we have the following equation in $S/I \otimes_{K_0} K_0[\{a_{ij}\}]$:

$$f_\ell(Ax) = h_{\ell 1} z_1 + \cdots + h_{\ell n_\ell} z_{n_\ell}.$$

Let Z be the closed subvariety of $(\mathrm{PGL}_{N+1})_{K_0}$ that vanishes at each of $h_{\ell 1}, \ldots, h_{\ell n_\ell}$ for every ℓ.

If L/K_0 is a field extension and $\phi, \psi \in Z(L)$ such that $\phi|_{C_L} = \psi|_{C_L}$, then $\phi^{-1} \circ \psi$ fixes C_L. But C is not contained in a proper linear subspace of $\mathbb{P}^N_{K_0}$, so this implies $\phi = \psi$. This shows that $\Phi \circ \Psi$ is the identity on Z, and so $Z \cong \underline{\mathrm{Isom}}(C, D)$. But, $\underline{\mathrm{Isom}}(C, D)$ is 0-dimensional. Finish by computing $Z(\overline{K_0})$ and returning the corresponding isomorphisms. □

Remark 3.5.3. Assume the same notation as in Lemma 3.5.2. Then we claim that every isomorphism $C_{\overline{K_0}} \to D_{\overline{K_0}}$ is defined over the separable closure of K_0. First, the automorphism scheme $\underline{\mathrm{Aut}}(D)$ is étale over K_0 because $H^0(D, \mathcal{T}_D) = 0$ (see [32, Tags 0DSW and 0E6G]), and $\underline{\mathrm{Isom}}(C, D)$ is an $\underline{\mathrm{Aut}}(D)$-torsor over K_0 (see Section 5.2 for more discussion on torsors). Therefore, $\underline{\mathrm{Isom}}(C, D)$ is also étale over K_0, so its points are defined over separable extensions of K_0.

Proposition 3.5.4. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y) and determines whether Y is isotrivial. Furthermore, if Y is isotrivial, the algorithm returns finite separable extensions L_0/K_0 and ℓ_0/k_0 such that $\ell_0 \subset L_0$, a curve Y_0 over ℓ_0, and an isomorphism $\phi\colon Y_{L_0} \to (Y_0)_{L_0}$.*

Proof. Compute the genus $g := g(Y)$. If $g = 0$, then Y is isotrivial. In this case, choose any point $P \in Y(L_0)$, where L_0/K_0 is a finite separable extension. Then compute a basis $\{1, \phi\}$ for $H^0(Y_{L_0}, \mathcal{O}_{Y_{L_0}}(P))$. The nonconstant function ϕ can then be thought of as an isomorphism $Y_{L_0} \to \mathbb{P}^1_{L_0}$. We can set $\ell_0 := k_0$ and $Y_0 := \mathbb{P}^1_{k_0}$.

If $g = 1$, then first choose any $P \in Y(L_0')$, where L_0'/K_0 is a finite separable extension. Then put $Y_{L_0'}$ into Weierstrass form with respect to the base point P as in [31, Proposition 3.1], and compute its j-invariant $j := j(Y_{L_0'})$. Then Y_K is isotrivial if and only if j is algebraic over k_0, which is true if and only if $j \in k_0$ because $j \in K_0$. Suppose this is the case. Construct an elliptic curve Y_0 over $\ell_0 := k_0$ such that $j(Y_0) = j$ as in [31, Proposition III.1.4c]. Lastly, compute a finite extension L_0/L_0' and an isomorphism $\phi\colon Y_{L_0} \to (Y_0)_{L_0}$ as in [31, Proposition III.1.4b or Proposition A.1.2b]. Note that in this construction L_0 is separable over L_0'.

If $g \geq 2$, then suppose $Y \subset \mathbb{P}^n_{K_0}$. Compute the Jacobian matrix J for the defining equations for Y. Determine an open subset $U \subset C$ on which the entries of J are regular functions and such that J has rank $n - 1$. The equations for Y give rise to a smooth family $\pi\colon \mathcal{Y} \to U$ whose generic fiber is Y. Choose any point $P \in U(\ell_0)$ for some separable extension ℓ_0 of k_0. Let $Y_0 := \pi^{-1}(P)$ and $L_0' := \ell_0 K_0$. Use Lemma 3.5.2 to compute the isomorphisms $Y_{\overline{L_0'}} \to (Y_0)_{\overline{L_0'}}$. If no such isomorphism exists, then Y is nonisotrivial. Otherwise, choose any isomorphism ϕ and let L_0 be a separable extension of L_0' over which ϕ is defined (Remark 3.5.3). □

We now focus on the problem of determining whether there exists a curve Y' over kK^p such that $Y \cong (Y')_{kK^p}$. For this, suppose k is a field of characteristic p, C is a geometrically integral smooth projective curve over k, $K := k(C)$, and Y is a geometrically integral smooth projective curve over K with $g := g(Y) \geq 2$. The curve Y defines a K-point Q of $\overline{M_g}$, the coarse moduli space of stable curves of genus g over k. Let F be the residue field of Q. If Y is nonisotrivial, then K/F is a finite extension. Following Szpiro, we make the following definition.

Definition 3.5.5. Suppose that Y is nonisotrivial. The *modular inseparability exponent* of Y is the integer $e \geq 0$ such that $[K : F]_i = p^e$.

Let $B \subset C$ be a nonempty open subset such that Y spreads out to a smooth morphism $\phi\colon \mathcal{Y} \to B$. Consider the exact sequence of tangent sheaves on $\mathcal{Y}$:

$$0 \to \mathcal{T}_{\mathcal{Y}/B} \to \mathcal{T}_{\mathcal{Y}} \to \phi^*\mathcal{T}_B \to 0.$$

The natural homomorphism $\mathcal{T}_B \to \phi_*\phi^*\mathcal{T}_B$ is an isomorphism, so we have an exact sequence

$$0 \longrightarrow \phi_*\mathcal{T}_{\mathcal{Y}/B} \longrightarrow \phi_*\mathcal{T}_{\mathcal{Y}} \xrightarrow{\beta} \mathcal{T}_B \xrightarrow{\gamma} R^1\phi_*\mathcal{T}_{\mathcal{Y}/B}. \tag{3.7}$$

The map γ is known as the *Kodaira-Spencer map*. As mentioned by Szpiro, $e > 0$ if and only if γ is zero ([34, Section 0]).

Let $\varepsilon \in C$ be the generic point. We now explain how the stalk $(\phi_*\mathcal{T}_{\mathcal{Y}})_\varepsilon$ can be identified with the set of k-derivations of $\mathcal{O}_Y$. An element δ of $(\phi_*\mathcal{T}_{\mathcal{Y}})_\varepsilon$ is an element of $\mathcal{T}_{\mathcal{Y}}(\phi^{-1}(U))$ for some nonempty open $U \subset B$. Thus, δ can be identified with a k-derivation of $\mathcal{O}_{\mathcal{Y}}|_{\phi^{-1}(U)}$, which restricts to a k-derivation of $\mathcal{O}_Y$. Conversely, a k-derivation δ of $\mathcal{O}_Y$ can be spread out to a k-derivation of $\mathcal{O}_{\mathcal{Y}}|_{\phi^{-1}(U)}$ for some open $U \subset B$, which then defines an element of $(\phi_*\mathcal{T}_{\mathcal{Y}})_\varepsilon$.

Proposition 3.5.6. *Let k be a field of characteristic p, C be a smooth integral curve over k, and $K := k(C)$. Let Y be a geometrically integral smooth projective curve over K with genus $g(Y) \geq 2$ and modular inseparability exponent e. Then $e > 0$ if and only if there exists a curve Y' over kK^p such that $Y \cong Y'_K$. If this is the case, then the modular inseparability exponent of Y' is $e - 1$.*

Proof. Taking stalks of (3.7) at ε, we get

$$0 \longrightarrow H^0(Y, \mathcal{T}_Y) \longrightarrow (\phi_*\mathcal{T}_{\mathcal{Z}})_\varepsilon \xrightarrow{\beta_\varepsilon} \mathcal{T}_{B,\varepsilon} \xrightarrow{\gamma_\varepsilon} H^1(Y, \mathcal{T}_Y) = 0.$$

Here, $\mathcal{T}_{B,\varepsilon}$ is a one-dimensional K-vector space and can be identified with the set of k-derivations on K. Let δ be a nonzero k-derivation on K. Then the following are equivalent

(i) $e > 0$,

(ii) $\gamma_\varepsilon = 0$,

(iii) β_ε is an isomorphism,

(iv) δ extends to a derivation on $\mathcal{O}_{\mathcal{Z}}|_{\phi^{-1}(U)}$ for some open $U \subset B$,

(v) δ extends to a k-derivation on $\mathcal{O}_Y$, and

(vi) there exists a curve Y' over kK^p such that $Y \cong Y'_K$ (Proposition 3.1.10).

To prove the last sentence of the proposition, suppose the above conditions hold. With the notation in (3.1), the map $\operatorname{Spec} K \to \overline{M_g}$ factors as

$$\operatorname{Spec} K \to \operatorname{Spec} kK^p \to \operatorname{Spec} F \to \overline{M_g}.$$

Then, using Lemma 3.1.1, the modular inseparability exponent of Y' is

$$[kK^p : F]_i = \frac{[K : F]_i}{[K : kK^p]_i} = \frac{[K : F]_i}{p} = p^{e-1}. \qquad \square$$

Proposition 3.5.7. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y) with $g(Y) \geq 2$ and either returns a curve Y' over $k_0 K_0^p$ such that $Y \cong Y'_{K_0}$ or determines that no such Y' exists.*

Proof. First determine an affine open subset $B = \operatorname{Spec} A$ of C such that Y spreads out to a smooth projective k_0-morphism $\phi\colon \mathcal{Y} \to B$. Let ε denote the generic point of C. Let R be the homogeneous coordinate ring of $\mathcal{Y}$ as a projective B-scheme, and compute a graded R-module M such that $\mathcal{T}_{\mathcal{Y}} = \widetilde{M}$. Then compute $N := M \otimes_A K_0$, which is a module over

the homogeneous coordinate ring of Y. Also compute $H := H^0(Y, \widetilde{N})$. We have natural isomorphisms

$$H \cong H^0(Y, \mathcal{T}_{\mathcal{Y}}|_Y) \cong H^0(\mathcal{Y}, \mathcal{T}_{\mathcal{Y}}) \otimes_A K_0 \cong H^0(B, \phi_* \mathcal{T}_{\mathcal{Y}}) \otimes_A K_0 \cong (\phi_* \mathcal{T}_{\mathcal{Y}})_\varepsilon.$$

By the proof of Proposition 3.5.6, Y' exists if and only if $(\phi_* \mathcal{T}_{\mathcal{Y}})_\varepsilon \neq 0$. By the above line, this is true if and only if $H \neq 0$. So, if $H = 0$, then the algorithm stops here. Otherwise, choose any nonzero $\widetilde{\delta} \in H$ thought of as a k_0-derivation on $\mathcal{O}_Y$. Let δ be its image in $\mathcal{T}_{B,\varepsilon}$ under the map β_ε from the proof of Proposition 3.5.6. By Proposition 3.1.9(i), the kernel of $\widetilde{\delta}$ is the structure sheaf of the desired Y'. We now construct Y' by computing its function field.

Let $\eta \in Y$ be the generic point. From $\widetilde{\delta}$, determine the induced k-derivation $\widetilde{\delta}_\eta$ on $K_0(Y)$. Consider $\widetilde{\delta}_\eta$ as a $k_0 K_0(Y)^p$-linear operator on the $k_0 K_0(Y)^p$-vector space $K_0(Y)$ (which is p^2-dimensional by Lemma 3.1.1), and compute its kernel F. Determine an integral regular projective curve Y' over kK^p whose function field is F. The normalization of the projective closure of Z is isomorphic to Y' over $k_0 K_0^p$, so compute this to finish the proof. □

Corollary 3.5.8. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y), where Y is nonisotrivial and $g(Y) \geq 2$, and returns the modular inseparability exponent of Y.*

Proof. Apply Proposition 3.5.7 to compute a curve Y' over $k_0 K_0^p$ such that $Y \cong Y'_{K_0}$ if one exists. If no such Y' exists, then return 0. Otherwise, by recursion, compute the modular inseparability exponent e' of Y' and return $e' + 1$. □

In Sections 5 and 6, we will need to spread Y out to a surface $\mathcal{Y}$ fibered over all of C. We cannot guarantee that $\mathcal{Y} \to C$ will be smooth, but we do want it to have certain properties.

Definition 3.5.9. Let k be a field, C be a geometrically integral smooth projective curve over k, and Y be a geometrically integral smooth projective curve over $K := k(C)$. Then a *relatively minimal model* for Y is a projective morphism $\phi\colon \mathcal{Y} \to C$, where $\mathcal{Y}$ is a geometrically

integral smooth surface over k, whose geometric fibers contain no (-1)-curves and whose generic fiber is isomorphic to Y. If, in addition, the geometric fibers of ϕ are reduced with at worst normal crossing singularities, then we say ϕ is a *semistable model* for Y.

Theorem 3.5.10. *Let Y be a curve as in Definition 3.5.9. Then there exists a relatively minimal model for $Y_{\ell K}$ for some finite extension ℓ/k that is unique up to C_ℓ-isomorphism. Furthermore, there exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y) and returns a finite extension ℓ_0/k_0 together with a relatively minimal model for $Y_{\ell K_0}$.*

Proof. See [36, Sections 2.1 and 2.2]. □

Theorem 3.5.11. *Let k be a field of characteristic p, C be a smooth integral curve over k, and $K := k(C)$. Let Y be a geometrically integral smooth projective curve over K with genus $g(Y) \geq 1$. Let ℓ be a prime not equal to p with $\ell \geq 7$ if $g(Y) = 1$ and $\ell > 768g(Y)$ if $g(Y) \geq 2$. Assume that $Y(K) \neq \emptyset$ and $(\operatorname{Pic} Y)[\ell](\overline{K}) = (\operatorname{Pic} Y)[\ell](K)$. Then a relatively minimal model for Y is a semistable model.*

Proof. See [32, Tag 0CDN]. □

Corollary 3.5.12. *There exists an algorithm that takes Input 3.4.3 data $(p, k_0, C, K_0, X, Y, \pi)$, where $g(Y) \geq 1$, and returns finite extensions ℓ_0/k_0 and L_0/K_0 and a semistable model for Y_{L_0} such that $(p, \ell_0, C, L_0, X_{L_0}, Y_{L_0}, \pi_{L_0})$ are valid data for Input 3.4.3.*

Proof. Choose a prime ℓ not equal to p such that $\ell \geq 7$ if $g(Y) = 1$ and $\ell > 768g(Y)$ if $g(Y) \geq 2$. Compute $(\operatorname{Pic} Y)[\ell]$ using Proposition 4.2.1 below with $S = \emptyset$ (see also Corollary 4.1.2). Compute a separable field extension L_0/K_0 such that $(\operatorname{Pic} Y_{L_0})[\ell](\overline{K_0}) = (\operatorname{Pic} Y_{L_0})[\ell](L_0)$ (this is possible because $(\operatorname{Pic} Y)[\ell]$ is étale over K_0). Enlarge k_0 and K_0 by finite extensions to assume $(\operatorname{Pic} Y)[\ell](\overline{K_0}) = (\operatorname{Pic} Y)[\ell](K_0)$ (see Remark 3.4.8). Compute a finite extension ℓ_0/k_0 and relatively minimal model for $Y_{\ell_0 K_0}$ using Theorem 3.5.10. Replace k_0 by ℓ_0 so that we have a relatively minimal model $\phi\colon \mathcal{Y} \to C$ for Y. By Theorem 3.5.11, ϕ is a semistable model. □

4 Curves of absolute genus 0

4.1 The group $K(S, m)$

Let k be an algebraically closed field, C be a geometrically integral smooth projective curve over k, and $K := k(C)$. For S a set of places of K and an integer m, let $K(S, m)$ denote the subgroup of $K^\times/K^{\times m}$ of elements α with $\operatorname{ord}_v \alpha = 0 \pmod m$ for all places $v \notin S$.

Proposition 4.1.1. *If S is finite, then there is an exact sequence*

$$0 \longrightarrow (\operatorname{Pic} C)[m] \xrightarrow{f} K(S, m) \xrightarrow{g} (\mathbb{Z}/m\mathbb{Z})^S \xrightarrow{h} \mathbb{Z}/m\mathbb{Z} \tag{4.1}$$

where f, g, and h are defined as follows. If D is a divisor such that mD is the divisor of an element $\beta \in K^\times$, then $f(\text{class of } D)$ is the class of β. If $\alpha \in K^\times$, then $g(\alpha) = \big((\operatorname{ord}_v \alpha) \bmod m\big)_{v \in S}$. The map h sums the coordinates.

Proof. From the exact sequence

$$0 \longrightarrow \frac{K^\times}{k^\times} \longrightarrow \operatorname{Div} C \longrightarrow \operatorname{Pic} C \longrightarrow 0$$

we have

$$0 \longrightarrow (\operatorname{Pic} C)[m] \longrightarrow \frac{K^\times}{K^{\times m}} \longrightarrow \frac{\operatorname{Div} C}{m \operatorname{Div} C} \longrightarrow \frac{\operatorname{Pic} C}{m \operatorname{Pic} C} \longrightarrow 0. \tag{4.2}$$

From the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & \dfrac{K^\times}{K^{\times m}} & \longrightarrow & \dfrac{K^\times}{K^{\times m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^S & \longrightarrow & \dfrac{\operatorname{Div} C}{m \operatorname{Div} C} & \longrightarrow & \dfrac{\operatorname{Div}(C \setminus S)}{m \operatorname{Div}(C \setminus S)} & \longrightarrow & 0
\end{array}$$

and (4.2), the snake lemma gives

$$0 \longrightarrow (\operatorname{Pic} C)[m] \to K(S,m) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^S \longrightarrow \frac{\operatorname{Pic} C}{m \operatorname{Pic} C} \tag{4.3}$$

Because k is algebraically closed, the degree map $\operatorname{Pic} C/m \operatorname{Pic} C \to \mathbb{Z}/m\mathbb{Z}$ is an isomorphism such that $(\mathbb{Z}/m\mathbb{Z})^S \to \operatorname{Pic} C/m \operatorname{Pic} C \to \mathbb{Z}/m\mathbb{Z}$ is the sum of coordinates. □

Corollary 4.1.2. *The group $K(S,m)$ is finite. If $S = \emptyset$, then $K(S,m) \cong (\operatorname{Pic} C)[m]$. If $s := \#S \geq 1$ and $r := \dim_{\mathbb{Z}/p\mathbb{Z}}(\operatorname{Pic} C)[p]$ is the p-rank of C, then $K(S,m) \cong (\mathbb{Z}/m\mathbb{Z})^{2g(C)+s-1}$ for $p \nmid m$ and $K(S,p^n) \cong (\mathbb{Z}/p^n\mathbb{Z})^{r+s-1}$ for $n \geq 1$.*

Proof. This follows from the exact sequence (4.1). □

We are interested in computing the finite group $K(S,m)$, particularly in the case where $m = p$. Recall the group isomorphism $d\log\colon K^\times/K^{\times p} \to \Omega_{K/k}^{\mathcal{C}=1}$ in Section 3.2. There is a convenient description for the image of $K(S,p)$ in $\Omega_{K/k}$.

Lemma 4.1.3. *Let S be a finite set of places of K. Define the effective divisor $D := \sum_{s\in S} s$ of C. Then $d\log$ restricts to an isomorphism*

$$K(S,p) \to H^0(C, \Omega_C(D))^{\mathcal{C}=1}.$$

Proof. If $\alpha \in K^\times$, then $\operatorname{ord}_v(d\log\alpha) = -1$ if $\operatorname{ord}_v\alpha \neq 0 \pmod p$, and $\operatorname{ord}_v(d\log\alpha) \geq 0$ if $\operatorname{ord}_v\alpha = 0 \pmod p$. Therefore, for $\alpha \in K(S,p)$, we have $d\log\alpha \in H^0\big(C,\Omega_C(D)\big)^{\mathcal{C}=1}$. Conversely, if $\omega \in H^0\big(C,\Omega_C(D)\big)$ and $\mathcal{C}(\omega) = \omega$, then $\omega = d\log\alpha$ for some $\alpha \in K^\times$. For $v \notin S$, we have $\operatorname{ord}_v\omega \geq 0$, so by the first sentence again, $\alpha \in K(S,p)$. □

Proposition 4.1.4. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0) and a finite set of places S of K and returns a set of elements $T \subset K^\times$ mapping bijectively to $K(S,p)$ in $K^\times/K^{\times p}$.*

Proof. Let D be the divisor in Lemma 4.1.3. Use Corollary 3.2.8 to compute $H^0(C, \Omega_C(D))^{\mathcal{C}=1}$. Then use Proposition 3.2.6(ii) to compute a set of preimages T in $K^\times$. □

4.2 Computation on the Jacobian of C

Let k, C, K, and S be as in the previous section. The method to compute $K(S,p)$ above does not generalize to $K(S,m)$ for $m \neq p$. We now provide a way to compute $K(S,m)$ for a general m.

Relax the condition that k be algebraically closed, but assume $C(k) \neq 0$. The Jacobian J_C of C is a projective variety of dimension $g(C)$, and $J_C(\ell)$ can be identified with $\mathrm{Pic}^0 C_\ell$ for any field extension ℓ/k. Using Proposition 4.1.1, we can make the following observation.

Proposition 4.2.1. *There exists an algorithm that takes as input an integer m, a finitely generated field k_0, a geometrically integral smooth projective curve C over k_0, and a finite set of places S of K (where $K_0 := k_0(C)$, $k := \overline{k_0}$, and $K := kK_0$ as usual) and returns a set of elements $T \subset K^\times$ mapping bijectively to $K(S,m)$ in $K^\times/K^{\times m}$.*

Proof. Compute J_C as a closed subvariety of some projective space together with equations for the multiplication-by-m morphism $J_C \to J_C$ (see [1]). Fix a point $P_0 \in C(k)$. Take some $a \in (\mathbb{Z}/m\mathbb{Z})^S$, the sum of whose coordinates is 0. Choose integers a_v such that $a = (a_v)_{v \in S} \pmod m$, and set $d := \sum_{v \in S} a_v$. Consider the divisor $D := \sum_{v \in S} a_v v - dP_0$. A preimage of a in $K(S,m)$, according to Proposition 4.1.1, is the class of a function α on C such that $\operatorname{div} \alpha = D - mD'$ for some divisor D'. Furthermore, in this way, the preimages $\overline{\alpha}$ are in one-to-one correspondence with the linear equivalence classes of divisors D' such that $D - mD'$ is principal. Compute D as a point Q on J_C, compute the points $R_1, \ldots, R_N$ in the preimage of Q by the multiplication-by-m morphism, and compute corresponding divisors $D'_1, \ldots, D'_N$. These divisors are representatives of each unique linear equivalence class of divisors D' such that $D - mD'$ is principal. For each i, compute any nonzero element $\alpha_{a,i}$ in the Riemann-Roch space

$$H^0(C_k, \mathcal{O}_{C_k}(D - mD'_i)).$$

Do all of this for each a, and return the set

$$T := \bigcup_a \{\alpha_{a,1}, \ldots, \alpha_{a,N}\}. \qquad \square$$

The known methods for computing J_C as a projective variety are computationally infeasible for $g(C) \geq 3$. To avoid working with the Jacobian directly, we can use the g-fold symmetric product $C^{(g)}$, defined as the quotient of the g-fold product $C^g := C \underset{k}{\times} C \underset{k}{\times} \cdots \underset{k}{\times} C$ by the symmetric group S_g acting by permuting coordinates. For every field extension ℓ/k, think of $C^{(g)}(\ell)$ as parameterizing degree g effective divisors on C_ℓ. Fix a k-point P_0 of C. Then there is a birational k_0-morphism $\alpha\colon C^{(g)} \to J_C$ sending a degree g effective divisor D to the class of $D - gP_0$ (see [23, Sections 3-5]). If D is a degree 0 divisor of C and $[D]$ is its class in J_C, then $\alpha^{-1}([D])$ is the complete linear system of effective divisors linearly equivalent to $D + gP_0$.

Lemma 4.2.2. *There exist the following algorithms that take as input a finitely generated field F, a geometrically integral smooth projective curve C over F, and a divisor D of C of degree g:*

(i) one that returns an effective divisor E of C linearly equivalent to D, and

(ii) one that returns the closed subvariety W of $C^{(g)}$ parameterizing effective divisors linearly equivalent to D.

Proof. Compute the F-vector space $H := H^0(C, D)$, which has dimension at least 1 by the Riemann-Roch theorem. For (i), choose any nonzero $f \in H$. Compute and return the effective divisor E such that $\operatorname{div} f = E - D$. For (ii), consider the generic element of $\mathbb{P}H$. This defines a function $h \in F(\mathbb{P}H)(C)$ up to multiplication by an element of $F(\mathbb{P}H)^\times$. Compute the effective divisor $\widetilde{E}$ on $C_{F(\mathbb{P}H)}$ such that $\operatorname{div} h = \widetilde{E} - D$. Spread out $\widetilde{E}$ to an F-rational map from $\mathbb{P}H$ to $C^{(g)}$. Compute and return the Zariski closure W of the image of this map. $\square$

The multiplication-by-m morphism on J_C does not lift to a morphism $C^{(g)} \to C^{(g)}$ in general. However, as the following lemma shows, we can compute a partition of $C^{(g)}$ such that multiplication-by-m lifts to a morphism on each part.

Lemma 4.2.3. *There exists an algorithm that takes as input an integer m, a finitely generated field k_0, a geometrically integral smooth projective curve C over k_0, and a point $P_0 \in C(k_0)$ and returns disjoint locally closed subvarieties $V_1, \dots, V_n$ of $C^{(g)}$ and, for each i, a k_0-morphism $\phi_i \colon V_i \to C^{(g)}$ such that the V_i partition $C^{(g)}$ on the level of closed points and for every $D \in V_i(\overline{k_0})$, we have the following linear equivalence of divisors on $C_{\overline{k_0}}$:*

$$m(D - gP_0) \sim \phi_i(D) - gP_0.$$

Proof. We prove this by Noetherian induction. More precisely, we prove that for a given closed subvariety $Z \subset C^{(g)}$, we can compute $V_1, \dots, V_n \subset Z$ that partition Z as well as the ϕ_i with the property stated in the lemma. Then the lemma follows by taking $Z := C^{(g)}$.

If $Z = \emptyset$, then just take $n = 0$. Assume $\dim Z \geq 0$. By computing the irreducible components of Z and applying the algorithm to each component, we reduce to the case where Z is integral. Let E be the generic point of Z, thought of as a divisor of $C_{k_0(Z)}$. Use Lemma 4.2.2(i) to compute an effective divisor E' of $C_{k_0(Z)}$ such that $E' \sim \big(mE - g(m-1)P_0\big)$. Then E' defines a $k_0(Z)$-point of $C^{(g)}$. Spread this out to a k_0-morphism $\phi \colon V \to C^{(g)}$ for some dense open $V \subset Z$. The dimension of $Z \setminus V$ is less than the dimension of Z, so by induction, we are done. □

Lemma 4.2.4. *There exists an algorithm that takes as input an integer m, a finitely generated field k_0, a geometrically integral smooth projective curve C over k_0, a point $P_0 \in C(k_0)$, and a degree zero divisor D on C_{k_0} and computes a set of divisors $D'_1, \dots, D'_N$ on $C_{\overline{k_0}}$ such that if D' is a divisor on $C_{\overline{k_0}}$ with $mD' \sim D$, then $D' \sim D'_i$ for some i.*

Proof. Compute V_i and ϕ_i as in Lemma 4.2.3 with $Z := C^{(g)}$. Use Lemma 4.2.2(ii) to compute the closed subvariety W of $C^{(g)}$ whose points represent the complete system of

degree g effective divisors linearly equivalent to $gP_0 + D$. Compute the preimages $\phi_i^{-1}(W) \subset V_i$ for each i and their Zariski closures W_i' in $C^{(g)}$. Compute the reduced variety W' of the union of the W_i's. Thus, W' is the closed subvariety of $C^{(g)}$ whose points represent the set of all degree g effective divisors D'' such that $m(D'' - gP_0) \sim D$. There are finitely many linear equivalence classes of such divisors D'' because multiplication-by-m is a finite morphism on J_C. It follows that the irreducible components of $W'_{\overline{k_0}}$ are disjoint and represent the finitely many complete linear systems of such divisors D''. Choose a representative $\overline{k_0}$-point D_i'' from each of the irreducible components of $W'_{\overline{k_0}}$, a return the divisors $D_i' := D_i'' - gP_0$ on $C_{\overline{k_0}}$. □

Alternate proof of Proposition 4.2.1. The proof is essentially the same as the proof of Proposition 4.2.1 but with computation on $C^{(g)}$ instead of J_C. Fix a point $P_0 \in C(k)$. Take some $a := (a_v)_{v \in S} \in (\mathbb{Z}/m\mathbb{Z})^S$ such that $d_a := \sum_{v \in S} a_v = 0 \pmod m$. Compute divisors $D_1', \ldots, D_N'$ as in Lemma 4.2.4 with $D := \sum_{v \in S} a_v v - dP_0$. For each i, compute any nonzero element $\alpha_{a,i}$ in the Riemann-Roch space

$$H^0(C_k, \mathcal{O}_{C_k}(D - mD_i')).$$

Do all of this for each a, and return the set

$$T := \bigcup_a \{\alpha_{a,1}, \ldots, \alpha_{a,N}\}.$$ □

4.3 Proof of main theorem for $\widetilde{g} = 0$

Proof of Theorem 1.0.2(i). Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data with $g(Y) = \widetilde{g} = 0$. First, as in Proposition 3.5.4, determine a finite separable extension L_0 of K_0 such that $Y_{L_0} \cong \mathbb{P}^1_{L_0}$. Enlarge k_0 and K_0 using Remark 3.4.8 to assume $Y \cong \mathbb{P}^1_{K_0}$ and $K_0(Y) = K_0(x)$. As in Proposition 3.4.5, take any $z \in K_0(X) \setminus \pi^* K_0(Y)$ and compute $r \in K_0(Y)$ such that $z^p = r \circ \pi$.

Consider the divisor

$$\operatorname{div} r = \sum_{i=1}^{n} e_i P_i$$

over the separable closure K_0^{sep} of K_0, so that the P_i are all purely inseparable points of $\mathbb{P}^1_{K_0^{sep}}$. We claim that there exist distinct i and j such that $e_i \deg P_i \neq 0 \pmod{p}$ and $e_j \deg P_j \pmod{p}$. First, suppose for the sake of contradiction that $e_i \deg P_i = 0 \pmod{p}$ for all i. Then, over $\overline{K_0}$, there exists some divisor D such that $\operatorname{div} r = pD$. It follows that r is a pth power in $\overline{K_0}(Y)$. But, because $K_0(X)$ is gotten from $K_0(Y)$ by adjoining a pth root of r, this means that $K_0(X) \otimes_{K_0} \overline{K_0}$ has nilpotents and that X is not geometrically reduced, which is a contradiction. Thus, there exists some i such that $e_i \deg P_i \neq 0 \pmod{p}$. Now,

$$e_i \deg P_i + \sum_{j \neq i} e_j \deg P_j = 0,$$

so there must exist some $j \neq i$ with $e_j \deg P_j \neq 0 \pmod{p}$ as well.

By the previous paragraph, we may enlarge k_0 and K_0 using Remark 3.4.8 so that r is supported at two distinct degree 1 points of $\mathbb{P}^1_{K_0}$ with multiplicities not divisible by p. After a linear fractional transformation, we may assume those two points are 0 and ∞. Write $r = r_1/r_2$, where $r_1, r_2 \in K_0[x]$. Replace r by rr_2^p and z by $z \cdot (r_2 \circ \pi)$ to assume that r is a polynomial in x:

$$r = \alpha_{m_1} x^{m_1} + \alpha_{m_1+1} x^{m_1+1} + \cdots + \alpha_{m_2} x^{m_2}, \tag{4.4}$$

where $\alpha_{m_1}, \alpha_{m_2} \neq 0$ and $m_1, m_2 \neq 0 \pmod{p}$.

Compute the finite set S of places ξ of K such that there exists an i such that $\operatorname{ord}_\xi \alpha_i \neq 0$. If ξ is a place of K not in S and $w \in K$, then the only possible slopes in the Newton polygon for $r - w^p$ are 0, $-p(\operatorname{ord}_\xi w)/m_1$, or $-p(\operatorname{ord}_\xi w)/m_2$. This shows that for $\xi \notin S$, if $a \in K^\times$ and $r(a) \in K^p$, then $p | \operatorname{ord}_\xi a$. Using Proposition 4.1.4, compute a complete set of coset representatives $T \subset K^\times$ for $K(S, p)$. Replace k_0 by a finite extension such that $T \subset K_0^\times$. For each $\tau \in T$, define $g_\tau \colon \mathbb{P}^1_{K_0} \to \mathbb{P}^1_{K_0}$ by $x \mapsto \tau x^p$.

If $P \in \pi(X(K))$, then either $P = 0$, $P = \infty$, or $P \in K^\times$ and $r(P) \in K^p$ by Lemma 3.4.5. By the previous paragraph, $P \in g_\tau(\mathbb{P}^1_{K_0}(K))$ for some τ. Thus, compute $\pi(X(K))$ by using Proposition 3.4.6 to compute $g_\tau(\mathbb{P}^1_{K_0}(K)) \cap \pi(X(K))$ for every τ, and compute $X(K)$ by taking preimages. □

Example 4.3.1. Let $p > 2$, $k_0 := \mathbb{F}_p$, and $K_0 := k_0(\mathbb{P}^1) = \mathbb{F}_p(t)$. For $n \geq 1$ and $p \nmid n$, let X_n be the regular projective curve over K_0 with affine model

$$y^p = x^{p-1} - (t^n - 1)^{p-1}.$$

X_n is nonsmooth and is an inseparable degree p cover of $Y := \mathbb{P}^1_{K_0}$. When $p = 3$ and $n = 2$, the above algorithm computes

$$\begin{aligned} X_2(K_0) = \big\{&(t^2+2, 0), (t^2+t, 2t+2), (2t^2+2t, 2t+2), (t^2+2t, t+2), \\ &(t^3+2t, t^2+2), (2t^2+1, 0), (2t^3+t, t^2+2), (2t^2+t, t+2), \infty\big\}. \end{aligned}$$

The following table lists the number of K_0-points of X_n for $p = 3$ and $1 \leq n \leq 79$. This data was computed in Sage, the code for which is included in Appendix A.

n	$\#X_n(K_0)$	n	$\#X_n(K_0)$	n	$\#X_n(K_0)$
1	3	28	9	55	3
2	9	29	3	56	81
4	9	31	3	58	9
5	3	32	27	59	3
7	3	34	9	61	3
8	27	35	3	62	9
10	9	37	3	64	27
11	3	38	9	65	9
13	9	40	81	67	3
14	9	41	3	68	9
16	27	43	3	70	9
17	3	44	9	71	3
19	3	46	9	73	3
20	27	47	3	74	9
22	9	49	3	76	9
23	3	50	9	77	3
25	3	52	81	79	3
26	81	53	3		

The change of variables $X := 1/x$ and $Y := y/x$ gives the equation

$$Y^p = X - (t^n - 1)^{p-1} X^p,$$

which defines an algebraic subgroup of $\mathbb{G}_a \times \mathbb{G}_a$. The K_0-points of this curve therefore form an $\mathbb{F}_p$-vector space. This explains why the numbers in the table are all powers of 3.

5 Curves of absolute genus 1

5.1 The Mordell-Weil group

The original proof of finiteness of $X(K)$ in the case where $\widetilde{g} = 1$ was given by Voloch. It uses the fact that for an elliptic curve Y over K, the Mordell-Weil group $Y(K)/pY(K)$ is finite ([39]). The proof can be made effective in the cases where one knows how to compute $Y(K)/pY(K)$.

Proposition 5.1.1. *There exists an algorithm that takes Input 3.4.3 data $(p, k_0, C, K_0, X, Y, \pi)$, where Y is an elliptic curve, as well as a complete set of coset representatives $\{Q_1, \ldots, Q_n\} \subset Y(K)$ for $Y(K)/pY(K)$, and returns $X(K)$.*

Proof. Every element of $Y(K)$ is of the form $Q_i + pP$ for some $P \in Y(K)$. The morphism $Y \to Y$, $P \mapsto Q_i + pP$ is inseparable, so we can use Proposition 3.4.6 to compute $\pi(X(K)) \cap (Q_i + pY(K))$. Do this for every i to compute $\pi(X(K))$, and compute $X(K)$ by taking preimages. □

There is no known procedure for computing $Y(K)/pY(K)$ in general. One case in which we can compute $Y(K)/pY(K)$, however, is when Y is constant. We show this in two different ways. The first applies when k_0 is any finitely generated field, and the second applies when k_0 is a finite field. Both rely on the Tate conjecture for products of curves.

For a variety V, let $\mathrm{NS}\, V$ denote its *Néron-Severi group*, i.e., the group of divisors of V modulo algebraic equivalence. The Shioda-Tate theorem relates the Néron-Severi group of a relatively minimal model for a curve (see section 3.5) to the Mordell-Weil group of the Jacobian of the curve. To fix notation, let k be an algebraically closed field of characteristic p, C be a geometrically integral smooth projective curve over k, and Y be a geometrically integral smooth projective curve over $K := k(C)$ with $g(Y) \geq 1$. Let $\phi\colon \mathcal{Y} \to C$ be a relatively minimal model for Y. Consider the group homomorphism $\psi\colon \mathrm{Div}\, \mathcal{Y} \to \mathrm{Div}\, Y$ that maps an integral curve $D \subset \mathcal{Y}$ to its restriction $D \times_C Y$ to the generic fiber. Following the

notation in [36, Section 4.1], let $L^1 \operatorname{Div} \mathcal{Y} := \psi^{-1}(\operatorname{Div}^0 Y)$ and let $L^2 \operatorname{Div} \mathcal{Y} := \ker \psi$. Let $L^1 \operatorname{NS} \mathcal{Y}$ and $L^2 \operatorname{NS} \mathcal{Y}$ be the images of $L^1 \operatorname{Div} \mathcal{Y}$ and $L^2 \operatorname{Div} \mathcal{Y}$ in $\operatorname{NS} \mathcal{Y}$ respectively.

Let J_Y be the Jacobian of Y. Consider the category of pairs (A, σ), where A is an abelian variety over k and $\sigma\colon A_K \to J_Y$ is a homomorphism of abelian varieties over K. There exists a final object in this category called the K/k-trace of J_Y (see [5]).

Theorem 5.1.2 (Shioda-Tate)**.** *Assume the notation in the last two paragraphs, and assume $Y(K) \neq 0$. Let (B, τ) be the K/k-trace of J_Y. The homomorphism ψ induces an isomorphism*

$$\frac{L^1 \operatorname{NS} \mathcal{Y}}{L^2 \operatorname{NS} \mathcal{Y}} \to \frac{J_Y(K)}{\tau B(k)}.$$

Proof. See [36, Proposition 4.2.1]. □

Remark 5.1.3. The Shioda-Tate theorem specializes to the following three cases:

(i) If $g(Y) = 1$ and Y is nonconstant, then $B = 0$, so

$$\frac{L^1 \operatorname{NS} \mathcal{Y}}{L^2 \operatorname{NS} \mathcal{Y}} \cong Y(K).$$

(ii) If $g(Y) = 1$ and Y is constant, say $Y = (Y_0)_K$ for Y_0 defined over k, then $\mathcal{Y} = C \times Y_0$ and $B = Y_0$, so

$$\frac{L^1 \operatorname{NS}(C \times Y_0)}{L^2 \operatorname{NS}(C \times Y_0)} \cong \frac{Y_0(K)}{Y_0(k)}.$$

(iii) If more generally $Y = D_K$ for a curve D over k, let J_C and J_D be the Jacobians of C and D respectively. Then $\mathcal{Y} = C \times D$ and $B = J_D$, so

$$\frac{L^1 \operatorname{NS}(C \times D)}{L^2 \operatorname{NS}(C \times D)} \cong \frac{J_D(K)}{J_D(k)} \cong \operatorname{Hom}_k(J_C, J_D).$$

Proposition 5.1.4. *There exists an algorithm that takes as input a finitely generated field k_0 and geometrically integral smooth projective curves C and D over k_0 and returns a finite set of divisors on $(C \times D)_{\overline{k_0}}$ whose algebraic equivalence classes generate $\operatorname{NS}(C \times D)_{\overline{k_0}}$.*

Proof. The Tate conjecture is known for products of curves over a finitely generated field (the proof applies the Künneth formula [37, Lecture 2, Theorem 12.1] as well as Tate's isogeny theorem [24, Chapitre XII]). Therefore, we can use [26, Theorem 8.33 and Remark 8.35]. □

Corollary 5.1.5. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0) and an elliptic curve Y_0 over k_0 and returns a finite set of elements of $Y_0(K)$ whose classes generate $Y_0(K)/Y_0(k)$.*

Proof. Use Proposition 5.1.4 to compute a set of divisors $E_1, \dots, E_\rho$ on $(C \times Y_0)_k$ whose algebraic equivalence classes generate $\mathrm{NS}(C \times Y_0)_k$. The group $L^1 \mathrm{NS}(C \times Y_0)_k$ is the kernel of the composition of the (surjective) homomorphisms

$$\mathrm{NS}(C \times Y_0)_k \xrightarrow{\psi} \mathrm{Div}\, Y \xrightarrow{\deg} \mathbb{Z}.$$

Calculate linear combinations $D_1, \dots, D_{\rho-1}$ of the divisors $E_1, \dots, E_\rho$ that generate this kernel. The desired generators of $Y_0(K)/Y_0(k)$ are then the classes of $\psi(D_1), \dots, \psi(D_{\rho-1})$ in $\mathrm{Pic}^0 Y_0 = Y_0(K)$ by Remark 5.1.3(ii). □

Remark 5.1.6. If Y is nonconstant but the Tate conjecture is known for $\mathcal{Y}$, then generators for $\mathrm{NS}\,\mathcal{Y}$ and for $Y(K)$ can be computed using the same proofs above and Remark 5.1.3(i).

Remark 5.1.7. Suppose C and D are two geometrically integral smooth projective curves over k_0. After enlarging k_0, assume $C(k_0), D(k_0) \neq \emptyset$. Compute their respective Jacobians J_C and J_D as varieties embedded in projective space together with the addition morphisms $J_C \times J_C \to J_C$ and $J_D \times J_D \to J_D$ and embeddings $C \to J_C$ and $D \to J_D$ (see [1]). Then generators for the free abelian group $\mathrm{Hom}_k(J_C, J_D)$ can be computed using the same proofs above and Remark 5.1.3(iii).

In the case where Y_0 is an elliptic curve over $k_0 := \mathbb{F}_q$ is a *finite* field, there is a different algorithm for computing generators for $Y_0(K)$. First recall that the *zeta function* $Z(V, T)$

for a variety V over a finite field $\mathbb{F}_q$ is the power series in an indeterminate T given by

$$Z(V,T) := \exp\left(\sum_{n\geq 1} \#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right). \tag{5.1}$$

It is known by the Weil conjectures that $Z(V,T)$ is a rational function in $\mathbb{Q}(T)$ ([8]).

For the following, let C be a geometrically integral smooth projective curve over $k_0 := \mathbb{F}_q$, let $K_0 := \mathbb{F}_q(C)$, and let Y be an elliptic curve over K_0. As usual, $k := \overline{k_0}$ and $K := kK_0$. For a place v of K_0, let $\mathbb{F}_v$ be its residue field and $q_v := \#\mathbb{F}_v = q^{\deg v}$. For v at which Y has good reduction, let Y_v be the reduction. Define the integer a_v as

$$a_v := \begin{cases} q_v + 1 - \#Y_v(\mathbb{F}_v) & \text{if } Y \text{ has good reduction at } v \\ 1 & \text{if } Y \text{ has split multiplicative reduction at } v \\ -1 & \text{if } Y \text{ has nonsplit multiplicative reduction at } v \\ 0 & \text{if } Y \text{ has additive reduction at } v. \end{cases}$$

The *L-function* $L(Y,s)$ for Y in a complex variable s is given by

$$L(Y,s) := \prod_{\text{good } v} \left(1 - a_v q_v^{-s} + q_v^{1-2s}\right)^{-1} \prod_{\text{bad } v} (1 - a_v q_v^{-s})^{-1}.$$

Now, suppose that Y is constant, so there is an elliptic curve Y_0 over $\mathbb{F}_q$ such that $Y = (Y_0)_{K_0}$. The Birch and Swinnerton-Dyer conjecture is known to hold for Y (see [37, Lecture 3, Theorem 9.1]), meaning

$$\operatorname{rank} Y(K_0) = \operatorname{ord}_{s=1} L(Y,s). \tag{5.2}$$

The zeta functions for Y_0 and C have the forms

$$Z(Y_0,T) = \frac{\prod_{i=1}^{2}(1-\alpha_i T)}{(1-T)(1-qT)} \qquad \text{and} \qquad Z(C,T) = \frac{\prod_{j=1}^{2g(C)}(1-\beta_j T)}{(1-T)(1-qT)}, \tag{5.3}$$

and the L-function for Y is equal to the rational function

$$L(Y,s) = \frac{\prod_{i,j}(1-\alpha_i\beta_j q^{-s})}{\prod_{i=1}^{2}(1-\alpha_i q^{-s})\prod_{i=1}^{2}(1-\alpha_i q^{1-s})}$$

([37, Exercise 9.2]). Furthermore, for all i and j, $|\alpha_i| = |\beta_j| = q^{1/2}$, and the β_j can be indexed such that $\alpha_1 = \overline{\alpha_2}$ and $\beta_{2j-1} = \overline{\beta_{2j}}$. It follows from (5.2) that

$$\operatorname{rank} Y(K_0) = 2\#\{j \mid \beta_j = \alpha_1\}. \tag{5.4}$$

If k_0 is replaced by $\mathbb{F}_{q^n}$, then the numbers α_i and β_j are replaced with α_i^n and β_j^n, respectively. Thus,

$$\operatorname{rank} Y(K) = 2\#\{j \mid \beta_j^n = \alpha_1^n \text{ for some } n \in \mathbb{Z}\} = 2\#\{j \mid \beta_j/\alpha_1 \text{ is a root of unity}\}. \tag{5.5}$$

Proposition 5.1.8. *Let k be a finite field, C be a geometrically connected smooth projective curve over k, and $K := k(C)$. Let Y_0 be an elliptic curve over k. If* $\operatorname{rank} Y_0(K) = \operatorname{rank} Y_0(\overline{k}K)$*, then*

$$\frac{Y_0(K)}{Y_0(k)} \to \frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}$$

is an isomorphism.

Proof. Let $G := \operatorname{Gal}(\overline{k}/k)$. By taking Galois cohomology of the short exact sequence,

$$0 \to Y_0(\overline{k}) \to Y_0(\overline{k}K) \to \frac{Y_0(\overline{k}K)}{Y_0(\overline{k})} \to 0$$

we get

$$0 \to Y_0(k) \to Y_0(K) \to \left(\frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}\right)^G \to H^1(k, Y_0) = 0$$

(vanishing of the last term is due to Lang's theorem [18]). Now, $\operatorname{rank} Y_0(K) = \operatorname{rank} Y_0(\overline{k}K)$

and $Y_0(k)$ and $Y_0(\overline{k})$ are the torsion subgroups of $Y_0(K)$ and $Y_0(\overline{k}K)$, respectively, so

$$\frac{Y_0(K)}{Y_0(k)} \cong \left(\frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}\right)^G \qquad \text{and} \qquad \frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}$$

are free abelian groups of the same rank. If n is the index of $Y_0(K)/Y_0(k)$ in $Y_0(\overline{k}K)/Y_0(\overline{k})$ and $x \in Y_0(\overline{k}K)/Y_0(\overline{k})$, then nx is fixed by G. It follows that x is fixed by G, so

$$\frac{Y_0(K)}{Y_0(k)} \cong \left(\frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}\right)^G \cong \frac{Y_0(\overline{k}K)}{Y_0(\overline{k})}. \qquad \square$$

Now, assume that Y_0 is given in Weierstrass form as a curve in $\mathbb{P}^2_{\mathbb{F}_q}$. We recall the height function $h\colon Y(K_0) \to \mathbb{R}$ defined by

$$h(P) := \begin{cases} 0 & \text{if } P = O \\ \deg(x\colon C \to \mathbb{P}^1_{\mathbb{F}_q}) & \text{if } P = (x, y). \end{cases}$$

Because $Y = (Y_0)_{K_0}$, one can show that $h(mP) = m^2 h(P)$ for any integer m (see [30, III, Section 4 and Exercise 3.11]). The pairing

$$\langle P, Q \rangle := h(P + Q) - h(P) - h(Q) \tag{5.6}$$

is a positive definite bilinear form on $Y_0(K_0)/Y_0(\mathbb{F}_q)$.

Alternative proof of Proposition 5.1.5 in the case $k_0 = \mathbb{F}_q$. First, put Y_0 in Weierstrass form. Next, compute the zeta functions $Z(Y_0, T)$ and $Z(C, T)$ and the numbers α_i and β_j in (5.3). One possible method to do this is to compute $\#Y_0(\mathbb{F}_{q^n})$ and $\#C(\mathbb{F}_{q^n})$ for enough n to uniquely determine the numerators of the zeta functions according to (5.1) and (5.3).

Now, for each j, determine if β_j/α_1 is a root of unity. Note that β_j/α_1 has degree at most $4g(C)$ as an algebraic number, so one can do this by checking if $(\beta_j/\alpha_1)^n = 1$ for $n = 1, 2, \ldots, 4g(C)$. Let n_j be the smallest positive integer such that $(\beta_j/\alpha_1)^{n_j} = 1$ if one exists,

and $n_j := 1$ otherwise. Compute $r := 2\{j \mid n_j > 1\}$. Compute $n := \operatorname{lcm}(n_1, \ldots, n_{2g(C)})$, and let $k_1 := \mathbb{F}_{q^n}$. Thus, $\operatorname{rank} Y_0(K) = \operatorname{rank} Y_0(k_1 K_0) = r$ by (5.5), and $Y_0(K)/Y_0(k) = Y_0(k_1 K_0)/Y_0(k_1) \cong \mathbb{Z}^r$ by Proposition 5.1.8.

For simplicity, replace k_0 by k_1. Now, search for points in $\mathbb{P}^2_{k_0}(K_0)$ ordered by height that lie in $Y_0(K_0)$. Continue searching until points $Q_1, \ldots, Q_r \in Y_0(K_0)$ and an integer m have been found such that each of the linear combinations $c_1 Q_1 + \cdots + c_r Q_r$ for $0 \leq c_1, \ldots, c_r \leq m-1$ does not lie in $mY_0(K_0)$ unless $c_i = 0$ for all i. Thus, the points $Q_1, \ldots, Q_r$ generate $Y_0(K_0)/mY_0(K_0) \cong (\mathbb{Z}/m\mathbb{Z})^r$.

Now, compute the maximum height C of any linear combination $c_1 Q_1 + \cdots + c_r Q_r$ for $0 \leq c_1, \ldots, c_r \leq m-1$. By descent (see [31], for example), any missing generators of $Y_0(K_0)$ have height at most $\lfloor C/(m^2-1) \rfloor$. Check all points in $\mathbb{P}^2_{k_0}(K_0)$ up to this height to find all generators. □

Example 5.1.9. We will illustrate part of the above algorithm with the following data:

$$p = 5, \qquad k_0 = \mathbb{F}_5, \qquad C\colon v^2 = u^5 + u - 1, \qquad K_0 = \mathbb{F}_5(C), \qquad Y_0\colon y^2 = x^3 - 1.$$

We first count $\#Y_0(\mathbb{F}_5) = 6$, $\#C(\mathbb{F}_5) = 6$, and $\#C(\mathbb{F}_{5^2}) = 46$, from which we get

$$\alpha_1 = \beta_1 = \beta_2 = \sqrt{5}i$$
$$\alpha_2 = \beta_3 = \beta_4 = -\sqrt{5}i.$$

Thus, (5.4) says $\operatorname{rank}(Y_0(K_0)) = 4$, and (5.5) says $\operatorname{rank}(Y_0(K)) = \operatorname{rank}(Y_0(\mathbb{F}_{25} K_0)) = 8$. A search of points with small heights yields

$$P_1 := \left(\left(\frac{u-1}{u} \right)^2, \frac{2v}{u^3} \right), \; P_2 := \left(\left(\frac{u}{u-1} \right)^2, \frac{4v}{(u-1)^3} \right) \in Y_0(K_0).$$

Let $\omega \in \mathbb{F}_{25}$ be a primitive cube root of unity. To speed up computation, we apply the endomorphism $(x, y) \mapsto (\omega x, y)$ and the relative Frobenius F of $(Y_0)_K$ to find the following

additional points:

$$P_3 := \left(\omega\left(\frac{u-1}{u}\right)^2, \frac{2v}{u^3}\right), \qquad P_4 := \left(\omega\left(\frac{u}{u-1}\right)^2, \frac{4v}{(u-1)^3}\right)$$

$$P_5 := F(P_1) = \left(\left(\frac{u-1}{u}\right)^{10}, \frac{2v^5}{u^{15}}\right), \qquad P_6 := F(P_2) = \left(\left(\frac{u}{u-1}\right)^{10}, \frac{4v^5}{(u-1)^{15}}\right)$$

$$P_7 := F(P_3) = \left(\omega^2\left(\frac{u-1}{u}\right)^{10}, \frac{2v^5}{u^{15}}\right), \qquad P_8 := F(P_4) = \left(\omega^2\left(\frac{u}{u-1}\right)^{10}, \frac{4v^5}{(u-1)^{15}}\right).$$

We continue with this example in Example 5.2.6, where we prove that P_1, P_2, P_5, P_6 generate $Y_0(K_0)/5Y_0(K_0)$ and $P_1, \ldots, P_8$ generate $Y_0(K)/5Y_0(K)$.

5.2 Selmer groups and torsors

In the cases where we cannot compute $Y(K)/pY(K)$, we instead compute appropriate Selmer groups. Let k be a perfect field of characteristic p, C be a geometrically integral smooth projective curve over k, and $K := k(C)$. Let $\phi\colon Y \to Y'$ be an isogeny of elliptic curves over K. The short exact sequence of fppf group schemes over K

$$0 \longrightarrow \ker\phi \longrightarrow Y \xrightarrow{\phi} Y' \longrightarrow 0$$

induces an injective group homomorphism $Y'(K)/\phi(Y(K)) \to H^1(K, \ker\phi)$ (throughout this section, sheaves and cohomology will be on the fppf site). For each place v of K, let K_v denote the completion of K at v. We also have homomorphisms $Y'(K_v)/\phi(Y(K_v)) \to H^1(K_v, \ker\phi)$

for every v. Define the *Selmer group* $\mathrm{Sel}(K, \phi)$ to be the subgroup of elements of $H^1(K, \ker \phi)$ whose image in $H^1(K_v, \ker \phi)$ lies in the image of $Y'(K_v)/\phi(Y(K_v))$ for all v.

The isogenies we will be considering are the relative Frobenius $F\colon Y \to Y^{(p)}$ and its dual $V\colon Y^{(p)} \to Y$, also known as the Verschiebung isogeny. If ω is a nonzero invariant differential on Y, then $\mathcal{C}(\omega) = A^{1/p}\omega$ for some $A \in K$, where $\mathcal{C}$ is the Cartier operator. Following [38], we call A the *Hasse invariant* of Y with respect to ω. Note that if ω is replaced by $u^{-1}\omega$ for some $u \in K^\times$, then A is replaced by $u^{p-1}A$. Thus, the class of A in $K^\times/K^{\times(p-1)}$ is independent of the choice of ω.

From Section 4.1, we have an isomorphism

$$Y[p](\overline{K}) \to H^0(Y_{\overline{K}}, \Omega_{Y_{\overline{K}}})^{\mathcal{C}=1}.$$

If $\alpha \in \overline{K}$, then by properties of the Cartier operator, $\mathcal{C}(\alpha\omega) = \alpha\omega$ if and only if $\alpha = A^{1/p}\alpha^{1/p}$, i.e., $\alpha^p - A\alpha = 0$. We immediately see that $A = 0$ if and only if $Y[p](\overline{K}) = 0$, which is true if and only if Y is supersingular. If $A \neq 0$, then choose some $c \in \overline{K}$ such that $c^{p-1} = A$. Then

$$H^0(Y_{\overline{K}}, \Omega_{Y_{\overline{K}}})^{\mathcal{C}=1} = \{0, c\omega, 2c\omega, \ldots, (p-1)c\omega\}.$$

The procedure in the proof of Proposition 3.2.6 will give a function $f \in K(c)(Y)^\times$ such that $c\omega = df/f$ and therefore $ic\omega = df^i/f^i$ for any $i \in \mathbb{Z}$. If $P \in Y[p](\overline{K})$ and O is the identity element of Y, then we have an equality of divisors $p(P - O) = \mathrm{div}(f^i g^p)$ for some $i \in \mathbb{Z}$ and $g \in K(c)(Y)^\times$.

Suppose that Y is given in Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5.7}$$

and consider the invariant differential

$$\omega := \frac{dx}{2y + a_1x + a_3} = \frac{dy}{a_1y - 3x^2 - 2a_2x - a_4}. \tag{5.8}$$

Write

$$\left(4(x^3 + a_2x^2 + a_4x + a_6) + (a_1x + a_3)^2\right)^{(p-1)/2} = v(x)x^p + Ax^{p-1} + u(x), \tag{5.9}$$

where $u(x), v(x) \in K[x]$ and $u(x)$ and $v(x)$ both have degree at most $p-2$ (note that this is all valid even for $p = 2$). This gives us a convenient way to compute the Hasse invariant for ω, as we see by the following proposition.

Proposition 5.2.1. *Assume the notation in the preceding paragraph. The number A in (5.9) is equal to the Hasse invariant for ω.*

Proof. Compute

$$\begin{aligned}
\omega &= \frac{(2y + a_1x + a_3)^{p-1}dx}{(2y + a_1x + a_3)^p} \\
&= \frac{\left(4y^2 + 4a_1xy + 4a_3y + (a_1x + a_3)^2\right)^{(p-1)/2}}{(2y + a_1x + a_3)^p}dx \\
&= \frac{\left(4(x^3 + a_2x^2 + a_4x + a_6) + (a_1x + a_3)^2\right)^{(p-1)/2}}{(2y + a_1x + a_3)^p}dx \\
&= \frac{(u(x) + v(x)x^p) + Ax^{p-1}}{(2y + a_1x + a_3)^p}dx.
\end{aligned}$$

We have thus written ω in the form (3.2). From this, we have $\mathcal{C}(\omega) = A^{1/p}\omega$. □

Proposition 5.2.2. *Let Y be given by a Weierstrass equation, and assume the notation in the paragraph preceding Proposition 5.2.1. Suppose that Y is ordinary so that $V\colon Y^{(p)} \to Y$*

is separable. Define the function

$$s := \begin{cases} \dfrac{a_3 y + a_4 x + a_6}{x^2} & \text{if } p = 2 \\ \dfrac{u(x)(2y + a_1 x + a_3)}{x^p} & \text{if } p \geq 3 \end{cases}$$

on Y. The cover of Y given by $z^p - Az = s$ is isomorphic to $Y^{(p)}$ over K. Then $\ker V$ *is isomorphic over K to the kernel of the endomorphism of $\mathbb{G}_{a,K}$ given by $z \mapsto z^p - Az$. Furthermore,* $\ker F$ *is isomorphic to the Cartier dual of* $\ker V$*. In particular, the following are equivalent*

(i) $\ker V \cong \mathbb{Z}/p\mathbb{Z}$,

(ii) $\ker F \cong \mu_p$, *and*

(iii) $A \in K^{\times(p-1)}$.

Proof. For a proof that $Y^{(p)}$ is given as the cover $z^p - Az = s$, see [38, Section 1]. For the other statements, see [35, Proposition 2.1]. □

Proposition 5.2.3. *Let K be a field of characteristic p, and let Y be an ordinary elliptic curve over K. Let A be the Hasse invariant of Y with respect to an invariant differential ω, and let c be a $(p-1)$st root of A. The following are equivalent:*

(i) the j-invariant of Y is in K^p,

(ii) $Y \cong Y'_K$ for some elliptic curve Y' over K^p,

(iii) $Y[p](\overline{K}) \subset Y(K(c))$, and

(iv) there is an isomorphism $Y_{K(c)}[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$.

Proof. (i) implies (ii). There exists some elliptic curve Y'' defined over K^p such that Y is a twist of Y''_K. We claim that

$$H^1(K^p, \mathrm{Aut}(Y'')) \to H^1(K, \mathrm{Aut}(Y''_K)) \tag{5.10}$$

is surjective. If we can show this, then there is some twist Y' of Y'' such that $Y'_K \cong Y$. First suppose $p = 2$. Then $j(Y) \neq 0$ because Y is ordinary, so $\mathrm{Aut}(Y) \cong \mathrm{Aut}(Y'') \cong \mathbb{Z}/2\mathbb{Z}$ ([31, Appendix A, Proposition 1.2(c)]). Let $\wp$ denote the Artin-Schreier operator $x \mapsto x^2 - x$. The group homomorphism

$$K^2/\wp(K^2) \to K/\wp(K)$$

is surjective because for $x \in K$, we have $x + (x^2 - x) = x^2$. This proves that (5.10) is surjective. Suppose $p \geq 3$. Then for some $n \neq 0 \pmod p$, we have $\mathrm{Aut}(Y'') \cong \mu_n$ ([31, Appendix A, Proposition 1.2(c)] – for the case $p = 3$, note that again $j(Y) \neq 0$ because Y is ordinary). There are some $a, b \in \mathbb{Z}$ such that $1 = an + bp$. The group homomorphism

$$(K^p)^\times/(K^p)^{\times n} \to K^\times/K^{\times n}$$

is surjective because for $x \in K^\times$, we have $x \cdot (x^{-a})^n = (x^b)^p$. This proves that (5.10) is surjective.

(ii) implies (iii). We can assume $A \in K^p$. Then $K^p(c)$ is separable over K^p and therefore also separable over $K(c)^p$. But $K^p(c)$ is also purely inseparable over $K(c)^p$, so $K^p(c) = K(c)^p$. By the last sentence of Proposition 5.2.2, the kernel of $V\colon (Y')^{(p)} \to Y'$ is isomorphic over $K(c)^p$ to $\mathbb{Z}/p\mathbb{Z}$. Then

$$F(Y'[p](\overline{K})) \subset (\ker V)(\overline{K}) \subset Y^{(p)}(K(c)^p) = F(Y'(K(c))).$$

Therefore, $Y'[p](\overline{K}) \subset Y'(K(c))$ and $Y[p](\overline{K}) \subset Y(K(c))$.

(iii) implies (i). Take a nontrivial p-torsion element $P \in Y[p](K(c))$, and let Φ be the subgroup of $Y_{K(c)}$ generated by P. The morphism $\phi\colon Y_{K(c)} \to Y_{K(c)}/\Phi$ followed by its dual $\hat{\phi}\colon Y_{K(c)}/\Phi \to Y_{K(c)}$ is multiplication by p on $Y_{K(c)}$, which is inseparable. But, ϕ is separable, so $\hat{\phi}$ is inseparable of degree p. It follows that $j(Y_{K(c)}) = j(Y_{K(c)}/\Phi)^p$. Therefore, $j(Y) \in K \cap K(c)^p = K^p$.

Equivalence of (iii) and (iv). We have a short exact sequence

$$0 \to \ker F \to Y[p] \to \ker V \to 0.$$

Over $K(c)$, we have $\ker F \cong \mu_p$ and $\ker V \cong \mathbb{Z}/p\mathbb{Z}$ by Proposition 5.2.2. The sequence splits if and only if $Y(K(c))$ has a nontrivial p-torsion point. □

For the remainder of this section, we assume $A \in K^{\times(p-1)} \cup \{0\}$ so that either Y is supersingular or Y is ordinary and $(\ker V)(\overline{K}) \subset Y^{(p)}(K)$. First consider the case where Y is supersingular. Then

$$\ker F \cong \ker V \cong \alpha_p, \tag{5.11}$$

where α_p is the kernel of Frobenius on $\mathbb{G}_a$ ([35, Proposition 2.1]). Given Y in Weierstrass form, there is a simple way to compute an isomorphism $\ker F \to \alpha_p$. Make the change of variables $w = -1/y$ and $z = -x/y$ to get the affine neighborhood of the identity

$$f(w,z) := -w + z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = 0 \tag{5.12}$$

as in ([31, Chapter IV]). In this way,

$$\ker F = \operatorname{Spec} \frac{K[w,z]}{(f(w,z), w^p, z^p)} \cong \operatorname{Spec} \frac{K[z]}{(z^p)}$$

with coalgebra law $z \mapsto G(z_1, z_2) \pmod{z_1^p, z_2^p}$, where G is the formal group law on Y. We can then use linear algebra to find a nonzero polynomial $g(z)$ such that

$$g(G(z_1,z_2)) = g(z_1) + g(z_2) \pmod{z_1^p, z_2^p} \tag{5.13}$$

to establish an isomorphism $\alpha_p \to \ker F$.

Now consider the case where Y is ordinary. To compute an isomorphism $\mu_p \to \ker F$,

repeat the above steps, but compute a nonzero polynomial $g(z)$ such that

$$g(G(z_1, z_2)) = g(z_1) + g(z_2) + g(z_1)g(z_2) \pmod{z_1^p, z_2^p}.$$

There are $p - 1 = \#\operatorname{Aut}(\mu_p)$ possible choices for $g(z)$ here.

For the group schemes $\mathbb{Z}/p\mathbb{Z}$, μ_p, and α_p, we have the short exact sequences over K

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \longrightarrow 0$$

$$0 \longrightarrow \mu_p \longrightarrow \mathbb{G}_m \xrightarrow{F} \mathbb{G}_m \longrightarrow 0$$

$$0 \longrightarrow \alpha_p \longrightarrow \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \longrightarrow 0$$

where $\wp$ is the Artin-Schreier map $x \mapsto x^p - x$ and F is the relative Frobenius. Taking cohomology, we get isomorphisms

$$K/\wp(K) \cong H^1(K, \mathbb{Z}/p\mathbb{Z}), \qquad K^\times/K^{\times p} \cong H^1(K, \mu_p), \qquad K/K^p \cong H^1(K, \alpha_p).$$

Voloch explicitly describes the connecting homomorphisms, known as descent homomorphisms, $Y(K) \to K/\wp(K)$ and $Y^{(p)}(K) \to K^\times/K^{\times p}$ for Verschiebung and Frobenius respectively in the case where Y is ordinary ([38]). By a different approach, we now describe the composition of homomorphisms $Y^{(p)}(K) \to H^1(K, \ker F) \to \Omega_{K/k}$, where the latter homomorphism is $d\colon K/K^p \to \Omega_{K/k}$ if Y is supersingular and $d\log\colon K^\times/K^{\times p} \to \Omega_{K/k}$ if Y is ordinary (see Proposition 3.2.6). We will occasionally switch between x, y Weierstrass coordinates (5.7) and w, z coordinates (5.12). Which coordinates we are using for a point P will be given as a subscript, e.g., $P = (x_0, y_0)_{xy}$ or $P = (w_0, z_0)_{wz}$.

Lemma 5.2.4. *Let K be a field of characteristic p and Y be an elliptic curve over K given by a Weierstrass equation*

$$f(x,y) := (y^2 + a_1xy + a_3y) - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

For $(x_0, y_0)_{xy} \in Y(K)$ and $c \in K$, we have the following identity for the sum of $K[\varepsilon]/(\varepsilon^2)$-points of Y:

$$(x_0, y_0)_{xy} + (0, c\varepsilon)_{wz} = \left(x_0 + c\frac{\partial f}{\partial y}(x_0, y_0)\varepsilon, y_0 + c\frac{\partial f}{\partial x}(x_0, y_0)\varepsilon\right)_{xy}.$$

Proof. Reducing modulo ε, the left hand side is $(x_0, y_0)_{xy} + O = (x_0, y_0)_{xy}$. Therefore, we need to find the $\alpha, \beta \in K$ such that $(x_0, y_0)_{xy} + (0, c\varepsilon)_{wz} = (x_0 + a\varepsilon, y_0 + b\varepsilon)_{xy}$. Let $w_0 = -1/y_0$ and $z_0 = -x_0/y_0$. Compute $(x_0 + a\varepsilon, y_0 + b\varepsilon)_{xy}$ in w, z-coordinates

$$(x_0 + a\varepsilon, y_0 + b\varepsilon)_{xy} = \left(-\frac{1}{y_0 + b\varepsilon}, -\frac{x_0 + a\varepsilon}{y_0 + b\varepsilon}\right)_{wz} = \left(-w_0 + \frac{b}{y_0^2}\varepsilon, -z_0 - \frac{ay_0 + bx_0}{y_0^2}\varepsilon\right)_{wz}.$$

This point and the points $-(w_0, z_0)_{wz}$ and $-(0, c\varepsilon)_{wz}$ are collinear. Compute the inverses of $(w_0, z_0)_{wz}$ and $(0, c\varepsilon)_{wz}$

$$-(w_0, z_0)_{wz} = \left(\frac{w_0}{-1 + a_1z_0 + a_3w_0}, \frac{z_0}{-1 + a_1z_0 + a_3w_0}\right)_{wz}$$
$$-(0, c\varepsilon)_{wz} = (0, -c\varepsilon)_{wz}.$$

By this collinearity, we have an equation

$$\left(-z_0 - \frac{ay_0 + bx_0}{y_0^2} + c\varepsilon\right)\left(\frac{w_0}{-1 + a_1z_0 + a_3w_0} - 0\right) = \left(-w_0 + \frac{b}{y_0^2}\varepsilon - 0\right)\left(\frac{z_0}{-1 + a_1z_0 + a_3w_0} + c\varepsilon\right).$$

We also have the equation

$$\frac{\partial f}{\partial x}(x_0, y_0)a + \frac{\partial f}{\partial y}(x_0, y_0)b = 0$$

because $f(x_0 + a\varepsilon, y_0 + b\varepsilon) = 0$. From here, computing a and b is just a matter of solving these two simultaneous linear equations. □

Proposition 5.2.5. *Let k be a field of characteristic p, C be a geometrically integral smooth projective curve over k, and $K := k(C)$. Let Y be an elliptic curve over K given by a Weierstrass equation (5.7). Assume that the Hasse invariant is in $K^{\times(p-1)}$. Then, up to multiplication by an element of $K^{\times p}$, the connecting homomorphism $Y^{(p)}(K) \to \Omega_{K/k}$ for Frobenius is*

$$(x_0, y_0)_{xy} \mapsto \begin{cases} 0 & \text{if } (x_0, y_0)_{xy} = (0, 0)_{wz} = O \\ \dfrac{dx_0}{2y_0 + a_1^p x_0 + a_3^p} & \text{if } 2y_0 + a_1^p x_0 + a_3^p \neq 0 \\ \dfrac{dy_0}{a_1^p y_0 - 3x_0^2 - 2a_2^p x_0 - a_4^p} & \text{if } a_1^p y_0 - 3x_0^2 - 2a_2^p x_0 - a_4^p \neq 0. \end{cases}$$

Proof. Let $G = \alpha_p$ or μ_p, and fix an isomorphism $\ker F \cong G$ over K. We then have the following commutative diagram

$$\begin{array}{ccccc} Y^{(p)}(K) & \longrightarrow & H^1(K, \ker F) & \longrightarrow & \Omega_{K/k} \\ \downarrow & & \downarrow & & \downarrow \\ Y^{(p)}(\overline{k}K) & \longrightarrow & H^1(\overline{k}K, \ker F) & \longrightarrow & \Omega_{\overline{k}K/\overline{k}}. \end{array}$$

The vertical homomorphisms on the ends are injective. For this reason, it suffices to prove the proposition with k replaced by $\overline{k}$, C replaced by $C_{\overline{k}}$, K replaced by $\overline{k}K$, and Y replaced by $Y_{\overline{k}K}$. Therefore, we assume k is algebraically closed.

Fix some $t \in K \setminus K^p$ and let δ be the k-derivation on K such that $\delta t = 1$ (see Section 3.1). Identify $K^{1/p} \otimes_K K^{1/p}$ with $K^{1/p}[\varepsilon]/(\varepsilon^p)$ by the isomorphism of $K^{1/p}$-algebras defined

uniquely by $t^{1/p} \otimes 1 \mapsto t^{1/p}$ and $1 \otimes t^{1/p} \mapsto t^{1/p} + \varepsilon$. For an arbitrary element $\alpha^{1/p} \in K^{1/p}$ written as $\alpha^{1/p} = \sum_{i=0}^{p-1} c_i t^{i/p}$ with $c_i \in K$, we see that

$$\begin{aligned}
1 \otimes \alpha^{1/p} &= \sum_{i=0}^{p-1} c_i (1 \otimes t^{i/p}) \\
&= \sum_{i=0}^{p-1} c_i (t^{1/p} + \varepsilon)^i \\
&= \sum_{i=0}^{p-1} c_i \big(t^{i/p} + i\varepsilon t^{(i-1)/p} + O(\varepsilon^2)\big) \\
&= \sum_{i=0}^{p-1} c_i t^{i/p} + \left(\sum_{i=0}^{p-1} i c_i^p t^{i-1} \right)^{1/p} \varepsilon + O(\varepsilon^2) \\
&= \alpha^{1/p} + (\delta\alpha)^{1/p} \varepsilon + O(\varepsilon^2).
\end{aligned}$$

Now, $H^1(K, G) \cong K/K^p$ or $K^\times/K^{\times p}$ canonically. Then $H^1(K, G) \to H^1(K^{1/p}, G)$ is the zero homomorphism because the homomorphisms $K/K^p \to K^{1/p}/K$ and $K^\times/K^{\times p} \to (K^{1/p})^\times/K^\times$ are both zero. Therefore, an element of $H^1(K, G)$ can be given as a Čech 1-cocycle $\xi \in G(K^{1/p} \otimes_K K^{1/p}) \cong G(K^{1/p}[\varepsilon]/(\varepsilon^p))$; thus, think of ξ as an element of $K^{1/p}[\varepsilon]/(\varepsilon^p)$ such that $\xi^p = 0$ if $G = \alpha_p$ or $\xi^p = 1$ if $G = \mu_p$. First consider the case $G = \alpha_p$. Then $K/K^p \to H^1(K, G)$ is an isomorphism, so ξ is of the form

$$\xi = 1 \otimes \alpha^{1/p} - \alpha^{1/p} \otimes 1 = (\delta\alpha)^{1/p} \varepsilon + O(\varepsilon^2)$$

for some $\alpha \in K$. The image of ξ via the composition of homomorphisms $H^1(K, \alpha_p) \to K/K^p \to \Omega_{K/k}$ is therefore $d\alpha = \delta\alpha \cdot dt$. Now consider the case $G = \mu_p$. Then $K^\times/K^{\times p} \to H^1(K, G)$ is an isomorphism, so ξ is of the form

$$\xi = \frac{1 \otimes \alpha^{1/p}}{\alpha^{1/p} \otimes 1} = 1 + \left(\frac{\delta\alpha}{\alpha} \right)^{1/p} \varepsilon + O(\varepsilon^2)$$

for some $\alpha \in K$. The image of ξ via the composition of homomorphisms $H^1(K, \mu_p) \to$

$K^\times/K^{\times p} \to \Omega_{K/k}$ is therefore $d\log\alpha = (\delta\alpha/\alpha)\cdot dt$. Therefore, in either case, if $\xi \in G(K^{1/p}[\varepsilon]/(\varepsilon^p))$ is written as $\xi = \xi_0 + \xi_1\varepsilon + O(\varepsilon^2)$ where $\xi_0 = 0$ or 1 and $\xi_1 \in K^{1/p}$, then the image of ξ in $\Omega_{K/k}$ is $\xi_1^p\, dt$.

Now, suppose $(x_0, y_0)_{xy} \in Y^{(p)}(K)$. The image of this point in $H^1(K, \ker F)$ given as a Čech 1-cocycle is the element

$$(1\otimes x_0^{1/p}, 1\otimes y_0^{1/p})_{xy} - (x_0^{1/p}\otimes 1, y_0^{1/p}\otimes 1)_{xy} = \\ \left(x_0^{1/p} + (\delta x_0)^{1/p}\varepsilon + O(\varepsilon^2), y_0^{1/p} + (\delta y_0)^{1/p}\varepsilon + O(\varepsilon^2)\right)_{xy} - (x_0^{1/p}, y_0^{1/p})_{xy}$$

in $(\ker F)(K^{1/p}\otimes_K K^{1/p})$. According to Lemma 5.2.4, this difference is $(O(\varepsilon^2), c\varepsilon + O(\varepsilon^2))_{wz}$, where

$$(\delta x_0)^{1/p} = c\frac{\partial f}{\partial y}(x_0^{1/p}, y_0^{1/p}) = c(2y_0^{1/p} + a_1 x_0^{1/p} + a_3), \text{ and}$$
$$(\delta y_0)^{1/p} = c\frac{\partial f}{\partial x}(x_0^{1/p}, y_0^{1/p}) = c(a_1 y_0^{1/p} - 3x_0^{2/p} - 2a_2 x_0^{1/p} - a_4).$$

On $K^{1/p}[\varepsilon]/(\varepsilon^p)$-points, an isomorphism $\ker F \to \alpha_p$ or $\ker F \to \mu_p$ scales the ε term by some $\gamma \in K^\times$ (the polynomial g in (5.13) looks like $g(z) = \gamma z + O(z^2)$). Thus, the image of $(x_0, y_0)_{xy}$ in $\Omega_{K/k}$ is $\gamma^p c^p dt$. Solving for c in the above two equations gives the claimed formula up to the factor $\gamma^p \in K^{\times p}$. □

Example 5.2.6. Assume the notation in Example 5.1.9. We now show that P_1, P_2, P_5, P_6 generate $Y_0(K_0)/5Y_0(K_0)$ by using Proposition 5.2.5. The points P_1 and P_2 map to

$$\frac{(2+3u)du}{v} \qquad \text{and} \qquad \frac{u\,du}{v}$$

in Ω_{K_0/k_0} respectively. These are $\mathbb{F}_5$-linearly independent, so P_1 and P_2 generate $Y_0(K_0)/F(Y_0(K_0))$.

Now, $F \circ F = -5$ on Y_0, so we have an exact sequence of $\mathbb{F}_5$-vector spaces

$$0 \longrightarrow \frac{Y_0(K_0)}{F(Y_0(K_0))} \xrightarrow{F} \frac{Y_0(K_0)}{5Y_0(K_0)} \longrightarrow \frac{Y_0(K_0)}{F(Y_0(K_0))} \longrightarrow 0.$$

From this it follows that P_1, P_2, P_5, P_6 generate $Y_0(K_0)/5Y_0(K_0)$. The same argument can be applied to show that $P_1, \ldots, P_8$ generate $Y_0(K)/5Y_0(K)$.

To talk about Selmer groups, it will be helpful to recall the notion of torsors and their basic properties. See [25, Section 6.5] for more details.

Definition 5.2.7. Let S be a scheme and G be an fppf group scheme over S. A *G-torsor over S* is an fppf S-scheme X equipped with a right G-action $X \times_S G \to X$ such that there exists an fppf morphism $S' \to S$ such that $X_{S'}$ together with its $G_{S'}$-action is isomorphic over S' to $G_{S'}$ together with the $G_{S'}$-action of multiplication on the right. We say that X is the *trivial* torsor if S' can be taken to be S.

All group schemes we will be working with will be commutative. Let S be a scheme and A be a commutative fppf group scheme over S. There is a injective function

$$\big\{\text{Isomorphism classes of } A\text{-torsors over } S\big\} \to H^1(S, A) \tag{5.14}$$

that goes as follows. Let T be an A-torsor over S and $S' \to S$ an fppf morphism with an isomorphism $\phi\colon A_{S'} \to T_{S'}$. Let ϕ_1 and ϕ_2 denote the induced isomorphisms $A_{S' \times_S S'} \to T_{S' \times_S S'}$ gotten by extending to $S' \times_S S'$ with respect to projection to the first factor and second factor respectively. The composition $\phi_2^{-1} \circ \phi_1$ is multiplication by some $a \in A(S' \times_S S')$. The image of T in $H^1(S, A)$ is given by the Čech 1-cocycle a with respect to the cover $S' \to S$. In all of the cases that concern us, (5.14) is a bijection (see [25, Theorem 6.5.10]). The following conditions are equivalent:

(i) T is trivial,

(ii) $T(S) \neq \emptyset$, and

(iii) T corresponds to the identity element of $H^1(S, A)$.

Suppose that $f\colon A \to B$ is a morphism of fppf group schemes over S, and let f_* denote the induced homomorphism $H^1(S, A) \to H^1(S, B)$. Let T be an A-torsor over S also thought of as an element of $H^1(S, A)$. Then the B-torsor corresponding to $f_*(T)$ is the contracted product $T \overset{A}{\times} B$, i.e., the quotient of $T \times_S B$ by the A-action $a \cdot (t, b) := (ta^{-1}, ab)$. There exists a natural S-morphism $T \to f_*(T)$ defined by $t \mapsto (t, 1)$.

Briefly return to the case of a general isogeny of elliptic curves $\phi\colon Y \to Y'$ over K, and let $\iota\colon \ker\phi \to Y$ denote the inclusion of the kernel of ϕ. Let T be a $(\ker\phi)$-torsor over K. Then $\iota_*(T)$ is a Y-torsor over K with a natural K-morphism $\iota_*(T) \to \phi_*\iota_*(T) \cong Y'$. This gives $\iota_*(T)$ the structure of $(\ker\phi)$-torsor over Y' that is the trivial Y-torsor over K if and only if T is in the image of $Y'(K) \to H^1(K, \ker\phi)$. We will now describe how to explicitly construct $\iota_*(T)$ in the case where Y is ordinary and ϕ is either V or F.

If Y is ordinary and $\phi = V$ (and Hasse invariant $A \in K^{\times(p-1)}$), then we have $H^1(K, \ker V) \cong K/\wp(K)$. For $\alpha \in K$, we can describe the $\mathbb{Z}/p\mathbb{Z}$-torsor T over K corresponding to its class $\overline{\alpha} \in K/\wp(K)$ and the $\mathbb{Z}/p\mathbb{Z}$-torsor $\iota_*(T) \to Y$. For the former, $T = \operatorname{Spec} K[z]/(z^p - z - \alpha)$ with the action of $\mathbb{Z}/p\mathbb{Z}$ given by $w \cdot z = z + w$. For the latter, first suppose that Y is given by a Weierstrass equation, and let ω be the corresponding invariant differential as in (5.8). By making a change of variables, we can assume that the Hasse invariant with respect to ω is $A = 1$. Then $\iota_*(T)$ is the cover of Y given by

$$z^p - z = s + \alpha \tag{5.15}$$

(see Proposition 5.2.2). The descent homomorphism $Y(K) \to K/\wp(K)$ as given by Voloch maps a K-point P to 0 if $P = O$ and the class of $-s(P)$ otherwise. We see easily from (5.15) that if $\alpha = -s(P)$ for some $P \in Y(K)$, then $\iota_*(T)$ is isomorphic over K to $Y^{(p)}$.

If $\phi = F$, then let $\omega^{(p)}$ be the usual invariant differential (5.8) on $Y^{(p)}$ coming from its

Weierstrass equation. Using Proposition 3.2.6, construct a function $f \in K^p(Y^{(p)})$ such that $\omega^{(p)} = df/f$. The cover of $Y^{(p)}$ given by $z^p = f$ is isomorphic to Y. For $\alpha \in K^\times$, the μ_p-torsor T over K corresponding to its class $\overline{\alpha} \in K^\times/K^{\times p}$ is $T = \operatorname{Spec} K[z]/(z^p - \alpha)$ with the action of μ_p given by $w \cdot z = wz$. Then $\iota_*(T)$ is the cover of $Y^{(p)}$ given by

$$z^p = \alpha f. \tag{5.16}$$

For some $g \in K(Y^{(p)})$ and nontrivial point $P_0 \in (\ker V)(K)$, we have $\operatorname{div}(fg^p) = p(P_0 - O)$. Set $f' := fg^p$. Then the cover $z^p = \alpha f$ is isomorphic to $z^p = \alpha f'$ and $\omega^{(p)} = df'/f'$. We see that for any $(x_0, y_0)_{xy} \in Y^{(p)}(K)$, we have the following equality of elements of $\Omega_{K/k}$:

$$\frac{d\big(f'(x_0, y_0)\big)}{f'(x_0, y_0)} = \begin{cases} 0 & \text{if } (x_0, y_0)_{xy} = (0,0)_{wz} = O \\ \dfrac{dx_0}{2y_0 + a_1^p x_0 + a_3^p} & \text{if } 2y_0 + a_1^p x_0 + a_3^p \neq 0 \\ \dfrac{dy_0}{a_1^p y_0 - 3x_0^2 - 2a_2^p x_0 - a_4^p} & \text{if } a_1^p y_0 - 3x_0^2 - 2a_2^p x_0 - a_4^p \neq 0. \end{cases}$$

By Proposition 5.2.5 and the paragraph before Lemma 5.2.4, it follows that the descent homomorphism $Y^{(p)}(K) \to K^\times/K^{\times p}$ maps a point $P \in Y^{(p)}(K)$ to 1 if $P = O$, to the class of $f'(-P_0)$ if $P = P_0$, and to the class of $f'(P)^{-1}$ otherwise. This is the inverse of the homomorphism shown by Voloch directly.

Ulmer explicitly describes the Selmer groups $\operatorname{Sel}(K, F)$ and $\operatorname{Sel}(K, V)$ in the case where k is a finite field ([35]). These results extend to the case where k is algebraically closed. When Y is ordinary, the group $\operatorname{Sel}(K, F)$ is finite, but $\operatorname{Sel}(K, V)$ is usually infinite when k is algebraically closed, as we will show. When Y is supersingular, $\operatorname{Sel}(K, F)$ is either zero or infinite when k is algebraically closed (see Proposition 5.2.9). Ulmer uses the fact that k is a finite field in his Lemma 1.2. We now show that this lemma holds for k algebraically closed as well.

Lemma 5.2.8. *Let R be a complete discrete valuation ring with residue field k and fraction*

field K, and assume k is algebraically closed. Let $\phi\colon Y \to Y'$ be an isogeny of elliptic curves over K with good reduction. Then $H^1(R, \ker\phi) \to H^1(K, \ker\phi)$ is an injection and its image is the image of $Y'(K)/\phi(Y(K))$.

Proof. Choose an element in $H^1(R, \ker\phi)$ thought of as a $(\ker\phi)$-torsor T over R. Because $\ker\phi$ is proper over K, we have $T(K) = T(R)$. Therefore, if T_K is a trivial torsor, then T must also be trivial. This shows that $H^1(R, \ker\phi) \to H^1(K, \ker\phi)$ is injective. Spread Y and Y' out to elliptic schemes $\mathcal{Y}$ and $\mathcal{Y}'$ over R.

If T is a $\mathcal{Y}$-torsor over R, then $T(k) \neq \emptyset$ because k is algebraically closed. By Hensel's lemma ([25, Theorem 3.5.63]), $T(R) \neq 0$ as well. This shows that $H^1(R, \mathcal{Y}) = 0$ and $\mathcal{Y}'(R) \to H^1(R, \ker\phi)$ is surjective. By properness, $\mathcal{Y}'(R) = Y'(K)$. We therefore have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\mathcal{Y}(R) & \longrightarrow & \mathcal{Y}'(R) & \twoheadrightarrow & H^1(R, \ker\phi) & \longrightarrow & H^1(R, \mathcal{Y}) = 0 \\
\big\updownarrow\wr & & \big\updownarrow\wr & & \big\downarrow & & \big\downarrow \\
Y(K) & \longrightarrow & Y'(K) & \longrightarrow & H^1(K, \ker\phi) & \longrightarrow & H^1(K, Y).
\end{array}$$

The last claim of the lemma follows from the middle square. □

Proposition 5.2.9. *Let k be an algebraically closed field of characteristic p, C be a connected smooth projective curve over k, and $K := k(C)$. Let Y_0 be a supersingular elliptic curve over k and $Y := (Y_0)_K$. Fix an isomorphism $\ker F \cong \alpha_p$ defined over k. Then the image of*

$$\mathrm{Sel}(K, F) \subset H^1(K, \ker F) \cong H^1(K, \alpha_p) \cong K/K^p \xrightarrow{d} \Omega_{K/k}$$

is $H^0(C, \Omega_C)^{C=0}$.

Proof. By Lemma 5.2.8, the image of $Y^{(p)}(K_v)$ in $H^1(K_v, \ker F)$ is the image of $H^1(\mathcal{O}_v, \ker F) \cong$

$\mathcal{O}_v/\mathcal{O}_v^p$ for each place v of K. Thus, the image of $\mathrm{Sel}(K,F)$ in K/K^p is the set

$$\{\alpha \in K/K^p \mid \alpha \in \mathcal{O}_v/\mathcal{O}_v^p \text{ for all } v\}.$$

Take some $\alpha \in K/K^p$ and place v of K. If the image of α in K_v/K_v^p lies in $\mathcal{O}_v/\mathcal{O}_v^p$, then $\mathrm{ord}_v\,\alpha \geq 0$. Conversely, suppose $\mathrm{ord}_v\,\alpha \geq 0$. Writing α as a Laurent series with respect to a uniformizer, one sees that α can be written as the sum of an element of $\mathcal{O}_v$ and an element of K_v^p. That is, α is in the image of $\mathcal{O}_v/\mathcal{O}_v^p$. Therefore, the image of $\mathrm{Sel}(K,F)$ in $\Omega_{K/k}$ is

$$\{d\alpha \in \Omega_{K/k} \mid \mathrm{ord}_v\,d\alpha \geq 0 \text{ for all } v\} = H^0(C,\Omega_C) \cap d(K) = H^0(C,\Omega_C)^{\mathcal{C}=0}$$

by Proposition 3.2.6. □

As before, assume that Y is given by a Weierstrass equation with ω as in (5.8) such that the Hasse invariant of Y with respect to ω is 1. Let Δ be the discriminant of this Weierstrass equation. To compute the Selmer groups for F and V, Ulmer defines the following Weil divisors of C:

$$D = \sum_v i_v v, \qquad \text{where} \qquad i_v = \begin{cases} 1 & \text{if } \mathrm{ord}_v(\Delta) > 0 \\ \left\lfloor \frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor + 1 & \text{if } \mathrm{ord}_v(\Delta) < 0 \text{ and } p \nmid \left\lfloor \frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor \\ \left\lfloor \frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor & \text{otherwise,} \end{cases}$$

$$\mathfrak{m} = \sum_v j_v v, \qquad \text{where} \qquad j_v = \begin{cases} 0 & \text{if } \mathrm{ord}_v(\Delta) > 0 \\ \left\lfloor -\frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor + 1 & \text{if } \mathrm{ord}_v(\Delta) < 0 \text{ and } p \nmid \left\lfloor -\frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor \\ \left\lfloor -\frac{p}{12}\,\mathrm{ord}_v(\Delta) \right\rfloor & \text{otherwise.} \end{cases}$$

Suppose that $\overline{\alpha} \in K/\wp(K)$, and let $\alpha \in K$ be a coset representative. Define $\mathrm{ord}_v\colon K/\wp(K) \to$

$\mathbb{Z}_{\leq 0}$ by $\mathrm{ord}_v(\overline{\alpha}) = 0$ if there exists some $\beta \in K$ such that $\mathrm{ord}_v(\alpha + \wp(\beta)) \geq 0$ and

$$\mathrm{ord}_v(\overline{\alpha}) = \max_{\beta \in K} \left\{ \mathrm{ord}_v(\alpha + \wp(\beta)) \right\}$$

otherwise. By writing α as a Laurent series with respect to a uniformizer at v, one sees that if $\mathrm{ord}_v(\overline{\alpha}) \neq 0$, then $p \nmid \mathrm{ord}_v(\overline{\alpha})$.

Proposition 5.2.10. *Let k be a field of characteristic p, and assume that k is either algebraically closed or finite. Let C be a geometrically integral smooth projective curve over k, and $K := k(C)$. Let Y be an ordinary elliptic curve over K, and assume the notation in the preceding paragraph. If $p \leq 3$, assume also that Y has either good reduction or split multiplicative reduction at every place of K. Then the image of $\mathrm{Sel}(K, F)$ in $\Omega_{K/k}$ is $H^0(C, \Omega_C(D))^{\mathcal{C}=1}$, and $\mathrm{Sel}(K, V)$ is the set*

$$\mathrm{Sel}(K, V) = \{\overline{\alpha} \in K/\wp(K) \mid \mathrm{ord}_v(\overline{\alpha}) \geq -j_v \text{ for all } v\}.$$

Proof. For the case where k is finite, see [35, Section 3]. The proof follows exactly the same in the case where k is algebraically closed by replacing [35, Lemma 1.2] with Lemma 5.2.8. □

5.3 Proof of main theorem for $\widetilde{g} = 1$ and $j(\widetilde{X_{\overline{K}}}) \in K$

Proof of Theorem 1.0.2(ii). Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data, where $g(Y) = \widetilde{g} = 1$ and $j(\widetilde{X_{\overline{K}}}) \in K$. We will invoke Remark 3.4.8 multiple times and replace k_0 and K_0 by finite extensions. First, enlarge k_0 and K_0 to assume that Y has a K_0-point, making Y into an elliptic curve as in the proof of Proposition 3.5.4. Next, use Proposition 3.5.4 to determine if Y is isotrivial. First, consider the case where Y is isotrivial, in which case we have ℓ_0, L_0, and $\phi\colon Y \to (Y_0)_{L_0}$ from Proposition 3.5.4. Enlarge k_0 and K_0 to assume that Y_0 is defined over k_0 and $Y = (Y_0)_{K_0}$. Using Corollary 5.1.5, compute a set of generators for

$Y_0(K)/Y_0(k)$, and then compute the finite group

$$\frac{Y_0(K)/Y_0(k)}{p(Y_0(K)/Y_0(k))} = \frac{Y_0(K)}{pY_0(K)}.$$

Compute $X(K)$ using Proposition 5.1.1.

Now, consider the case where Y is ordinary (note that if Y is nonisotrivial, then Y is ordinary because $j(Y) \notin k$). Compute the Hasse invariant A for Y with respect to an invariant differential, and enlarge k_0 and K_0 to assume $A^{1/(p-1)} \in K_0$. If $p \leq 3$, use Corollary 3.5.12 to enlarge k_0 and K_0 so that Y has a semistable model, i.e., Y has either good reduction or split multiplicative reduction at every $v \in C$. Note that $j(Y) \in K^p$ because π induces a degree p inseparable morphism of elliptic curves $\widetilde{X_{\overline{K}}} \to Y_{\overline{K}}$. So, $j(Y) \in K_0 \cap K^p = k_0 K_0^p$. Enlarge k_0 if necessary to ensure that $j(Y) \in K_0^p$, and so the equivalent conditions in Proposition 5.2.3 hold. Construct an elliptic curve Y' over K_0 such that $j(Y') = j(Y)^{1/p}$. Proposition 5.2.3(ii) implies that there is some choice of Y' such that $(Y')^{(p)} \cong Y$. In any case, $(Y')^{(p)}$ is isomorphic to Y after passing to some computable finite separable extension of K_0. Thus, enlarge k_0 and K_0 to assume $Y = (Y')^{(p)}$.

Consider the relative Frobenius morphism $F\colon Y' \to Y$. Compute the divisor D in the paragraph before Proposition 5.2.10 (note that the Y used there is our Y' here). Then use Corollary 3.2.8 to compute $H^0(C, \Omega_C(D))^{\mathcal{C}=1}$ and use Proposition 3.2.6(ii) to compute coset representatives $\alpha_1, \ldots, \alpha_N \in K^\times$ for its preimage in $K^\times/K^{\times p}$. Then compute the corresponding μ_p-torsors $T_1, \ldots, T_N$ over Y together with maps $F_i\colon T_i \to Y$ for each i as in (5.16). Then

$$\bigcup_{i=1}^{N} F_i(T_i(K)) = Y(K).$$

The morphisms F_i are inseparable, so apply Proposition 3.4.6 to compute

$$\bigcup_{i=1} F_i(T_i(K)) \cap \pi(X(K)) = \pi(X(K)).$$

Lastly, compute $X(K)$ by taking preimages. $\square$

Remark 5.3.1. Suppose $(p, k_0, C, K_0, X, Y, \pi)$ is Input 3.4.3 data such that $g(Y) = 1$ and X is isotrivial. Then Y is also isotrivial, so $j(X_{\overline{K}}) \in k \subset K$. Therefore $j(X_{\overline{K}}) \in K$ and X is in case (ii) of Theorem 1.0.2.

5.4 Case when $j(\widetilde{X_{\overline{K}}}) \notin K$

For this section, recall the notation from Proposition 5.2.10 and the paragraph before it. The algorithm to compute $X(K)$ in the previous section could be extended to the case $j(\widetilde{X_{\overline{K}}}) \notin K^p$ if $\mathrm{Sel}(K, V)$ were finite and we could compute coset representatives $\alpha_1, \ldots, \alpha_M$ in K for its image in $K/\wp(K)$, as we now explain. Assume that we have $\alpha_1, \ldots, \alpha_M$. Then compute their corresponding $\mathbb{Z}/p\mathbb{Z}$-torsors $T_1, \ldots, T_M$ over Y together with maps $V_i \colon T_i \to Y$ for each i as in (5.15). Compute the pullback $\pi_i \colon X_i \to T_i$ of $\pi \colon X \to Y$ along V_i. Denote the corresponding pullback of V_i by $g_i \colon X_i \to X$. Note that V_i is separable and π is purely inseparable, so $\overline{K}(T_i)$ and $\overline{K}(X)$ are linearly disjoint over $\overline{K}(Y)$. This implies that X_i is geometrically integral. Furthermore, X is regular and g_i is étale because V_i is étale, so X_i is regular. On the other hand, X_i maps to X, so X_i cannot be smooth ([32, Tag 0CCW]). The morphism π_i is purey inseparable of degree p, so $(p, k_0, C, K_0, X_i, Y_i, \pi_i)$ are valid Input 3.4.3 data. Furthermore,

$$j(\widetilde{(X_i)_{\overline{K}}}) = j\big((T_i)_{\overline{K}}\big)^{1/p} = j(Y^{(p)})^{1/p} = j(Y) \in K.$$

Use Section 5.3 to compute $X(K_i)$ for all i. Pulling back

$$\bigcup_i V_i(T_i(K)) = Y(K)$$

via π gives

$$\bigcup_i g_i(X_i(K)) = X(K).$$

To finish, compute the left hand side to compute $X(K)$.

Unfortunately, if k is algebraically closed and $j_v > 0$ for some place v of K, then $\mathrm{Sel}(K, V)$ can be infinite, as we show throughout this section.

Example 5.4.1. Suppose that k is finite or algebraically closed. Let $C := \mathbb{P}^1_k$ and $K := k(C) = k(t)$. Let Y be an ordinary elliptic curve over K. For each finite place v of $\mathbb{P}^1_k$, let $u_v \in K$ be a function with a simple pole at v and with no other poles. Then, using Proposition 5.2.10,

$$\begin{aligned}\mathrm{Sel}(K, V) &= \{\overline{\alpha} \in K/\wp(K) \mid \mathrm{ord}_v(\overline{\alpha}) \geq -j_v \text{ for all } v\} \\ &= \sum_v \sum_{\substack{1 \leq i \leq j_v \\ p \nmid i}} k u_v^i \pmod{\wp(K)} \\ &\subset K/\wp(K).\end{aligned}$$

If k is algebraically closed and $j_v > 0$ for some v, then this set is infinite. If k is finite, then this gives us an explicit description for $\mathrm{Sel}(K, V)$. Using the preceding paragraph, this proves Theorem 1.0.2(iii).

If k is finite and $g(C) \geq 1$, there are some things we can say about $\mathrm{Sel}(K, V)$ using facts about generalized Jacobians. We mostly follow Serre in [29]. For the next proposition, we introduce some notation. For each place v of K, let $U_v \subset K^\times$ be the subgroup of elements α such that $\mathrm{ord}_v \alpha = 0$, and for each integer $n \geq 0$, let $U_v^{(n)} \subset U_v$ denote the subgroup of α such that $\mathrm{ord}_v(\alpha - 1) \geq n$. Define the group

$$R_{\mathfrak{m}} = \prod_v U_v / U_v^{(j_v)}$$

(note that the factors where $j_v = 0$ are trivial). The groups $U_v/U_v^{(j_v)}$ can be given structures of algebraic group over k, and there is a subgroup of $R_{\mathfrak{m}}$ isomorphic to $\mathbb{G}_m$ given by diagonally

embedded constant functions. Define the group

$$L_{\mathfrak{m}} = R_{\mathfrak{m}}/\mathbb{G}_m.$$

Proposition 5.4.2. *Assume the hypotheses of Proposition 5.2.10 and the notation in the paragraph preceding it. There is an exact sequence of groups*

$$0 \to H^1_{\acute{e}t}(C, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Sel}(K, V) \to \mathrm{Ext}(L_{\mathfrak{m}}, \mathbb{Z}/p\mathbb{Z}) \to 0.$$

Proof. Let J be the Jacobian of C. There exists a commutative algebraic group $J_{\mathfrak{m}}$ over k, known as a generalized Jacobian, together with an exact sequence

$$0 \to L_{\mathfrak{m}} \to J_{\mathfrak{m}} \to J \to 0.$$

From this, we obtain an exact sequence

$$0 \to \mathrm{Ext}(J, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}(J_{\mathfrak{m}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}(L_{\mathfrak{m}}, \mathbb{Z}/p\mathbb{Z}) \to 0$$

[29, Theorem VII.23.13 and the subsequent example]. The left term parameterizes unramified covers of C of degree p, and the middle term parameterizes cyclic covers of C of degree p with conductor at most $\mathfrak{m}$ ([29, Sections VI.11 and VI.12]). The left term can therefore be identified with $H^1_{\acute{e}t}(C, \mathbb{Z}/p\mathbb{Z})$, and the middle term can be identified with $\mathrm{Sel}(K, V)$ by [29, Example 2 at the end of Section VI.12]. □

The subgroup $H^1_{\acute{e}t}(C, \mathbb{Z}/p\mathbb{Z})$ of $\mathrm{Sel}(K, V)$ is always finite. We now give an algorithm to compute its image in $K/\wp(K)$. For this, we introduce some more background on the Cartier operator $\mathcal{C}$ and the Hasse-Witt matrix; see [28, Sections 8-10] for more details. Let k be an algebraically closed field of characteristic p, and let C be a geometrically integral smooth projective curve over k with function field $K := k(C)$. Let $\mathcal{R}$ denote the *ring of repartitions*

on C, i.e., the elements $r = (r_P) \in \prod_{P \in C(k)} K$ such that r_P is regular at P for all but finitely many $P \in C(k)$. Let $\mathcal{R}(0)$ denote the subring of repartitions such that r_P is regular at all $P \in C(k)$. There is an isomorphism

$$\phi\colon \frac{\mathcal{R}}{\mathcal{R}(0)+K} \to H^1(C, \mathcal{O}_C) \tag{5.17}$$

that goes as follows. Let $r \pmod{\mathcal{R}(0)+K}$ be an element of the group on the left hand side. We can assume that $r_P \neq 0$ only for P in some finite set of points $\{P_1, \ldots, P_n\}$. For $1 \leq i \leq n$, let U_i be the open subset of C containing P_i and all points other than $P_1, \ldots, P_n$ at which r_{P_i} is regular, and let $U_{n+1} := C \setminus \{P_1, \ldots, P_n\}$. Then $\phi(r)$ is the Čech 1-cocycle for the open cover $U_1, \ldots, U_{n+1}$ of C whose value on $U_i \cap U_j$ for $1 \leq i < j \leq n+1$ is

$$f_{ij} := \begin{cases} r_{P_i} - r_{P_j} & \text{if } 1 \leq i, j \leq n \\ r_{P_i} & \text{if } j = n+1. \end{cases} \tag{5.18}$$

Let F denote the Frobenius operator on $\mathcal{R}$ sending r to (r_P^p). If F_* is the operator on $H^1(C, \mathcal{O}_C)$ induced by the pth power Frobenius map on $\mathcal{O}_C$, then ϕ satisfies $\phi(F(r)) = F_*(\phi(r))$.

Serre duality is explicitly described by the pairing

$$\langle \cdot, \cdot \rangle\colon \frac{\mathcal{R}}{\mathcal{R}(0)+K} \times H^0(C, \Omega_C) \to k, \qquad \langle r, \omega \rangle = \sum_{P \in C(k)} \operatorname{res}_P(r_P \omega).$$

The Frobenius operator on $\mathcal{R}/(\mathcal{R}(0)+K)$ and the Cartier operator on $H^0(C, \Omega_C)$ are related by the following formula:

$$\langle F(r), \omega \rangle = \langle r, \mathcal{C}(\omega) \rangle^p. \tag{5.19}$$

If $r_1, \ldots, r_g$ is a basis for $\mathcal{R}/(\mathcal{R}(0)+K)$, then the *Hasse-Witt matrix* with respect to this basis is a g-by-g matrix (a_{ij}) such that $F(r_i) = \sum_j a_{ij} r_j$. Suppose that $P_1, \ldots, P_g$ are g distinct points on C such that the divisor $D := P_1 + \cdots + P_g$ is nonspecial, i.e.,

$\dim H^0(C, \Omega_C(-D)) = 0$. If $u_1, \ldots, u_g$ are respective uniformizers for $P_1, \ldots, P_g$, then the repartitions $r_1, \ldots, r_g$ defined by

$$(r_i)_P := \begin{cases} 0 & \text{if } P \neq P_i \\ 1/u_i & \text{if } P = P_i \end{cases}$$

form a basis for $\mathcal{R}/(\mathcal{R}(0) + K)$.

Lemma 5.4.3. *There exists an algorithm that takes as input a finitely generated field k_0 and a geometrically integral smooth projective curve C over k_0 (set $k := \overline{k_0}$) of genus g and returns distinct points $P_1, \ldots, P_g \in C(k)$ such that the divisor $P_1 + \cdots + P_g$ is nonspecial.*

Proof. We choose the points $P_i \in C(k)$ one at a time such that for each i,

$$\dim_k H^0\big(C_k, \Omega_{C_k}(-P_1 - \cdots - P_i)\big) = g - i. \tag{5.20}$$

When $i = 0$, we have $\dim_k H^0(C_k, \Omega_{C_k}) = g$. Suppose $0 \leq i \leq g-1$ and that we have chosen i points such that (5.20) is true. Compute a nonzero element $\omega \in H^0(C_k, \Omega_{C_k}(-P_1 - \cdots - P_i))$, and choose a point $P_{i+1} \in C(k)$ at which ω does not vanish. This guarantees that

$$\dim_k H^0\big(C_k, \Omega_{C_k}(-P_1 - \cdots - P_i - P_{i+1})\big) = g - i - 1.$$

Once we have chosen $P_1, \ldots, P_g$, the divisor $P_1 + \cdots + P_g$ is nonspecial. Return $P_1, \ldots, P_g$. $\square$

Lemma 5.4.4. *There exists an algorithm that takes as input a finitely generated field k_0 (set $k := \overline{k_0}$), a geometrically integral smooth projective curve C over k_0, distinct points $P_1, \ldots, P_n \in C(k)$, and functions $r_1, \ldots, r_n \in k(C)$ and returns a function $s \in k(C)$ such that, if we define the repartition r on C_k by*

$$r_P := \begin{cases} r_i & \text{if } P = P_i \\ 0 & \text{otherwise,} \end{cases}$$

then $r + s \in \mathcal{R}(0)$, or determines that no such s exists.

Proof. Enlarge k_0 so that $P_1, \ldots, P_n$ and $r_1, \ldots, r_n$ are all defined over k_0. Compute $d_i := \operatorname{ord}_{P_i} r_i$, and compute a basis $v_1, \ldots, v_m$ for the Riemann-Roch space

$$H := H^0\big(C, \mathcal{O}_C(d_1 P_1 + \cdots + d_n P_n)\big).$$

If such an s exists, then $s \in H$ because its poles must lie in the set $\{P_1, \ldots, P_n\}$ and $\operatorname{ord}_{P_i} s = d_i$ for each i. The condition that $\operatorname{ord}_{P_i}(r_i + s) \geq 0$ is equivalent to s and $-r_i$ having the same principal part in their Laurent series expansions with respect to a uniformizer at P_i. That is, s lies on an affine linear subspace H_i cut out by d_i linear equations in $v_1, \ldots, v_n$. Compute H_i for every i, and return any $s \in H_1 \cap \cdots \cap H_n$ (if the intersection is empty, then no such s exists). □

Lemma 5.4.5. *Let S be a scheme and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of affine commutative group schemes over S. We then have the exact sequence

$$H^1(S, A) \xrightarrow{f_*} H^1(S, B) \xrightarrow{g_*} H^1(S, C).$$

Let T be a B-torsor over S such that $g_*(T)$ is the trivial C-torsor. Let $\sigma \colon S \to g_*(T)$ be any section, and consider the Cartesian square

$$\begin{array}{ccc} T_\sigma & \longrightarrow & S \\ \downarrow{\scriptstyle \sigma'} & & \downarrow{\scriptstyle \sigma} \\ T & \longrightarrow & g_*(T). \end{array}$$

Then T_σ is an A-torsor over S such that $f_*(T_\sigma) = T$.

Proof. One can check that the S-morphism $\mu\colon A \times_S T_\sigma \to T$ defined by $(a,t) \mapsto a \cdot \sigma'(t)$ lifts to a morphism $A \times_S T_\sigma \to T_\sigma$ and that this defines an A-action on T_σ. There is a well defined S-morphism

$$\phi\colon T_\sigma \overset{A}{\times} B \to T, \qquad (t,b) \mapsto b \cdot \sigma'(t),$$

which has the property that

$$\phi(t, b'b) = b'b \cdot \sigma'(t) = b' \cdot \phi(t,b).$$

So, if we can verify that T_σ is an A-torsor, then ϕ must be an isomorphism of B-torsors. For this, replace S by some fppf cover S' of S to assume that T_σ has an S-point. This means T has an S-point as well, which forces T to be the trivial torsor, so we can assume that T is B, $g_*(T)$ is C, and σ is the identity section. This then means T_σ is the kernel of g, which is A. □

Proposition 5.4.6. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0) and returns a coset representative in K for each element in the image of*

$$H^1_{\acute{e}t}(C_k, \mathbb{Z}/p\mathbb{Z}) \to H^1(K, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} K/\wp(K).$$

Proof. Use Lemma 5.4.3 to find distinct points $P_1, \ldots, P_g \in C(k)$ such that $P_1 + \cdots + P_g$ is nonspecial. Compute uniformizers $u_1, \ldots, u_g$ for $P_1, \ldots, P_g$ respectively to get a basis $r_1, \ldots, r_g$ for $\mathcal{R}/(\mathcal{R}(0) + K)$ as described in the paragraph after (5.19). Compute a basis $\omega_1, \ldots, \omega_g$ for $H^0(C, \Omega_C)$ and a matrix for the Cartier operator (Remark 3.2.3). Then use (5.19) to compute the Hasse-Witt matrix H with respect to the basis $r_1, \ldots, r_g$.

Consider the Artin-Schreier short exact sequence on the étale site of C_k:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \longrightarrow 0.$$

The map $\wp : k \to k$ is surjective, so we have the exact sequence

$$0 \longrightarrow H^1_{\acute{e}t}(C_k, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1_{\acute{e}t}(C_k, \mathbb{G}_a) \xrightarrow{\wp_*} H^1_{\acute{e}t}(C_k, \mathbb{G}_a).$$

Furthermore, we have the canonical isomorphism $H^1(C_k, \mathcal{O}_{C_k}) \cong H^1_{\acute{e}t}(C_k, \mathbb{G}_a)$. The kernel of $\wp_*$ on $H^1(C_k, \mathcal{O}_{C_k}) \cong \mathcal{R}/(\mathcal{R}(0) + K)$ is in bijection with

$$W := \{v \in k^g \mid Hv^p = v\}.$$

Compute this finite set W using Lemma 3.2.7(ii). The last thing we need to show is how to go from an element of W to its corresponding element of $K/\wp(K)$.

Consider an element of W, and let $r \in \mathcal{R}$ be the corresponding k-linear combination of $r_1, \ldots, r_g$. Then $r_P = 0$ if $P \neq P_1, \ldots, P_g$. Determine the Čech 1-cocycle $\phi(r)$ as described in the paragraph containing (5.17), with cover $U_1, \ldots, U_{g+1}$ of C_k and values f_{ij} on $U_i \cap U_j$. Let T denote the $\mathbb{G}_a$-torsor over C_k corresponding to r. Above U_i, for each $1 \leq i \leq n+1$, $T|_{U_i}$ and $\wp_*(T)|_{U_i}$ are both isomorphic to $U_i \times \mathbb{A}^1_k$, and their transition maps $(U_i \cap U_j) \times \mathbb{A}^1_k \to (U_i \cap U_j) \times \mathbb{A}^1_k$ are given by adding f_{ij} and $f_{ij}^p - f_{ij}$, respectively, to the $\mathbb{A}^1_k$ factors. Furthermore, the morphism $T|_{U_i} \to \wp_*(T)|_{U_i}$ is given by

$$(P, x) \mapsto (P, x^p - x). \tag{5.21}$$

We know that $\wp_*(T)$ is trivial because the class of r in $\mathcal{R}/(\mathcal{R}(0) + K)$ is in the kernel of $\wp_*$; our immediate goal is to compute a section $C_k \to \wp_*(T)$.

The repartition $\wp_*(r) = F(r) - r$ is in $\mathcal{R}(0) + K$. Use Lemma 5.4.4 to compute a function $s \in K$ such that $F(r) - r + s \in \mathcal{R}(0)$. It follows that for each $1 \leq i \leq g$, the function $h_i := r_{P_i}^p - r_{P_i} + s$ is regular on U_i, and the function $h_{g+1} := s$ is regular on U_{g+1}.

By (5.18), the Čech 1-cocycle $\phi(F(r)-r) = F_*(\phi(r)) - \phi(r)$ has value on $U_i \cap U_j$ equal to

$$f_{ij}^p - f_{ij} = \begin{cases} (r_{P_i}^p - r_{P_i}) - (r_{P_j}^p - r_{P_j}) & \text{if } 1 \le i, j \le g \\ r_{P_i}^p - r_{P_i} & \text{if } j = g+1 \end{cases}$$
$$= h_i - h_j.$$

Therefore, there is a section $\sigma\colon C_k \to \wp_*(T)$ given on U_i by

$$P \mapsto (P, h_i(P)). \tag{5.22}$$

According to Lemma 5.4.5, pulling back $T \to \wp_*(T)$ along σ gives us a $\mathbb{Z}/p\mathbb{Z}$-torsor T_σ over C_k that maps to T in $H^1(C_k, \mathcal{O}_{C_k})$. Comparing (5.21) and (5.22), we see that $T_\sigma|_{U_i}$ is given as the cover $x^p - x = h_i$. The class of h_i in $K/\wp(K)$, for any i, therefore corresponds to the class of r in $\mathcal{R}/(\mathcal{R}(0) + K)$. □

If k is algebraically closed and $\deg \mathfrak{m} \neq 0$, then $\mathrm{Ext}(L_\mathfrak{m}, \mathbb{Z}/p\mathbb{Z})$ can be infinite, as in Example 5.4.1. If k is finite, then $\mathrm{Ext}(L_\mathfrak{m}, \mathbb{Z}/p\mathbb{Z})$ is finite. In the latter case, I suspect that $\mathrm{Ext}(L_\mathfrak{m}, \mathbb{Z}/p\mathbb{Z})$ can be computed, but it is less clear how to lift elements to $\mathrm{Sel}(K, V)$. We can at least bound its size. For this, we introduce factor systems. Let A and B be commutative algebraic groups over k. A *factor system* for A with values in B is a morphism $f\colon A \times A \to B$ over k satisfying $f(x,y) = f(y,x)$ and

$$f(y,z) - f(x+y,z) + f(x,y+z) - f(x,y) = 0$$

for all points x, y, z on A. The factor system is *trivial* if there exists a k-morphism $g\colon A \to B$ such that $f(x,y) = g(x+y) - g(x) - g(y)$. If A and B are linear algebraic groups, then $\mathrm{Ext}(A, B)$ is isomorphic to the group of factor systems for A with values in B modulo the trivial factor systems ([29, Chapter VII, Proposition 7]).

Lemma 5.4.7. $\mathrm{Ext}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) \cong k$ *and* $\mathrm{Ext}(\mathbb{G}_m, \mathbb{Z}/p\mathbb{Z}) = 0$.

Proof. Let A be a commutative algebraic group. From the Artin-Schreier sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \to \mathbb{G}_a \to 0$$

we have the exact sequence

$$0 \to \mathrm{Hom}(A, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{G}_a) \to \mathrm{Hom}(A, \mathbb{G}_a) \to \mathrm{Ext}(A, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}(A, \mathbb{G}_a) \to \mathrm{Ext}(A, \mathbb{G}_a).$$

In terms of factor systems, $\mathrm{Ext}(\mathbb{G}_a, \mathbb{G}_a)$ is the k-vector space with basis the p^ith powers of the following polynomial

$$F(x, y) = \frac{1}{p}\big(x^p + y^p - (x + y)^p\big)$$

for $i = 0, 1, 2, \ldots$ ([29, Chapter VII, Proposition 8]). The Artin-Schreier map on $\mathrm{Ext}(\mathbb{G}_a, \mathbb{G}_a)$ sends F^{p^i} to $F^{p^{i+1}} - F^{p^i}$ and is therefore injective. The k-vector space $\mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_a)$ has basis the p^ith powers of $g(x) = x$. Therefore, the cokernel of the Artin-Schreier map on $\mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_a)$ is one-dimensional with basis $g(x)$. By the exact sequence above, $\mathrm{Ext}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) \cong k$.

Now, $\mathrm{Ext}(\mathbb{G}_m, \mathbb{G}_a) = 0$ by [29, Proof of Proposition VII.6.7]. It is also true that $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_a) = 0$, so by the exact sequence, $\mathrm{Ext}(\mathbb{G}_m, \mathbb{Z}/p\mathbb{Z}) = 0$. □

Lemma 5.4.8. *Let A be a commutative algebraic group over $\mathbb{F}_q$, where $q = p^n$, that admits a composition series whose successive quotients are isomorphic to $\mathbb{G}_a$. Then $\#\,\mathrm{Ext}(A, \mathbb{Z}/pZ) \leq q^{\dim A}$.*

Proof. We prove this by induction on the dimension of A. If $\dim A = 0$, then $\#\,\mathrm{Ext}(A, \mathbb{Z}/p\mathbb{Z}) = 1$. Let $n := \dim A \geq 1$, and suppose

$$0 \subset A_1 \subset A_2 \subset \cdots \subset A_n = A$$

is a composition series whose successive quotients are isomorphic to $\mathbb{G}_a$. From the exact sequence

$$0 \to A_{n-1} \to A \to \mathbb{G}_a \to 0,$$

we get the exact sequence

$$\begin{aligned} 0 \to \mathrm{Hom}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(A_{n-1}, \mathbb{Z}/p\mathbb{Z}) \\ \to \mathrm{Ext}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}(A, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}(A_{n-1}, \mathbb{Z}/p\mathbb{Z}). \end{aligned}$$

Using $\#\,\mathrm{Ext}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) = q$ by Lemma 5.4.7 and $\#\,\mathrm{Ext}(A_{n-1}, \mathbb{Z}/p\mathbb{Z}) \leq q^{n-1}$ by induction, we have

$$\#\,\mathrm{Ext}(A, \mathbb{Z}/p\mathbb{Z}) \leq \#\,\mathrm{Ext}(\mathbb{G}_a, \mathbb{Z}/p\mathbb{Z}) \times \#\,\mathrm{Ext}(A_{n-1}, \mathbb{Z}/p\mathbb{Z}) = q^n. \qquad \square$$

Proposition 5.4.9. *Assume the hypotheses of Proposition 5.2.10, and assume $k = \mathbb{F}_q$, where $q = p^n$. If S is the set of places v of C such that $j_v > 0$, then*

$$\#\,\mathrm{Ext}(L_{\mathfrak{m}}, \mathbb{Z}/p\mathbb{Z}) \leq q^{\sum_{v \in S}(j_v - 1)}.$$

Proof. The algebraic group $L_{\mathfrak{m}}$ factors as

$$L_{\mathfrak{m}} = \mathbb{G}_m^{\#S-1} \times \prod_{v \in S} U_v^{(1)}/U_v^{(j_v)}.$$

The group $U_v^{(1)}/U_v^{(j_v)}$ admits a composition series

$$0 \subset U_v^{(j_v-1)}/U_v^{(j_v)} \subset U_v^{(j_v-2)}/U_v^{(j_v)} \subset \cdots \subset U_v^{(2)}/U_v^{(j_v)} \subset U_v^{(1)}/U_v^{(j_v)}$$

with successive quotients isomorphic to $\mathbb{G}_a$. By Lemmas 5.4.7 and 5.4.8,

$$\#\,\mathrm{Ext}(L_{\mathfrak{m}}, \mathbb{Z}/p\mathbb{Z}) = \prod_{v \in S} \#\,\mathrm{Ext}(U_v^{(1)}/U_v^{(j_v)}, \mathbb{Z}/p\mathbb{Z}) \leq q^{\sum_{v \in S}(j_v - 1)}. \qquad \square$$

6 Curves of absolute genus at least 2

6.1 Isotrivial case

In the case where Y has genus at least 2 and is isotrivial, we make use of the de Franchis-Severi theorem. The proof of a computable version of the de Franchis-Severi theorem over a number field or $\overline{\mathbb{Q}}$ was given in [3, Theorem 5.5]. We show that it can be slightly modified to work over any field k_0 finitely generated over its prime field.

Theorem 6.1.1 (Computable de Franchis-Severi)**.** *There exists an algorithm that takes as input a finitely generated field k_0 (set $k := \overline{k_0}$) and an integral smooth projective curve X over k_0 and computes the set of pairs (Y, π) where Y is a smooth curve over k with $g(Y) \geq 2$ and $\pi\colon X_k \to Y$ is a separable k-morphism, up to isomorphism (pairs (Y, π) and (Y', π') are considered isomorphic if and only if there is a k-isomorphism $\theta\colon Y \to Y'$ with $\theta \circ \pi = \pi'$).*

Proof. Because $2 \leq g(Y) \leq g(X)$, it suffices to show that, for fixed $g \geq 2$, the set $\mathcal{C}_g$ of isomorphism classes of (Y, π) with $g(Y) = g$ is computable. Embed X in $\mathbb{P}H(X, \Omega_X^{\otimes 3})$. Let $(Y, \pi) \in \mathcal{C}_g$, and embed Y in $\mathbb{P}H(Y, \Omega_Y^{\otimes 3})$. If K_X and K_Y are divisors representing Ω_X and Ω_Y and R is the ramification divisor of π, then $3K_X - \pi^*(3K_Y)$ is linearly equivalent to $3R$, which is an effective divisor. This implies that $H^0(X, \pi^*\Omega_Y^{\otimes 3})$ is a vector subspace of $H^0(X, \Omega_X^{\otimes 3})$, so π is the restriction to X_k of a projection $\pi_L\colon \mathbb{P}H^0(X, \Omega_X^{\otimes 3}) \dashrightarrow \mathbb{P}H(Y, \Omega_Y^{\otimes 3})$ with respect to a linear subspace $L \subset \mathbb{P}H^0(X, \Omega_X^{\otimes 3})$ of dimension $d := 5g(X) - 5g(Y) - 1$. Let G be the Grassmannian variety of d-dimensional subspaces of $\mathbb{P}H^0(X, \Omega_X^{\otimes 3})$. If θ is an isomorphism from (Y, π) to (Y', π'), then $\pi^*\Omega_Y^{\otimes 3} = (\pi^*\theta^*\Omega_{Y'})^{\otimes 3} = \pi'^*\Omega_{Y'}^{\otimes 3}$. Thus, $(Y, \pi) \mapsto L$ is a well defined function $\iota\colon \mathcal{C}_g \to G(k)$. If $\iota(Y, \pi) = \iota(Y', \pi')$, then Y and Y' map isomorphically to the same curve in $\mathbb{P}H^0(X, \Omega_X^{\otimes 3})$ such that π and π' are induced by the same projection. Hence, ι is injective.

Conversely, if $s \in G_k$ has residue field $k(s)$, then let L be the corresponding subspace of $\mathbb{P}H^0(X_{k(s)}, \Omega_{X_{k(s)}}^{\otimes 3})$, let Y_s be the Zariski closure of the projection of $X_{k(s)} - L$ with respect

to L, and let $\pi_s \colon X_{k(s)} \to Y_s$ denote the morphism induced by this projection. The $s \in G(k)$ that are in the image of ι are precisely the points that satisfy the following three conditions:

(i) Y_s is a smooth curve over k,

(ii) π_s is a separable morphism, and

(iii) the subspace $L \subset \mathbb{P}H^0(X_k, \Omega_{X_k}^{\otimes 3})$ is equal to the linear subspace $L' \subset \mathbb{P}H^0(X_k, \Omega_{X_k}^{\otimes 3})$ defined as the zero locus of the sections in the image of $H^0(Y_s, \Omega_{Y_s}^{\otimes 3}) \to H^0(X_k, \Omega_{X_k}^{\otimes 3})$.

In [3], the authors first prove the following claim. Their proof holds in our case as well, so we will assume it.

Claim 1. G can be computably partitioned into a finite number of integral locally closed subsets H_i such that for each i, either

(1) for all $s \in H_i$, the curve Y_s is not smooth over the residue field of s, or

(2) there is a smooth family $\mathcal{Y} \to H_i$ of curves, and an H_i-morphism $X \times_k H_i \to \mathcal{Y}$ whose fiber above $s \in H_i$ is $\pi_s \colon X \to Y_s$.

We now prove the following claim.

Claim 2. Let H be a locally closed subset of G satisfying (2) in Claim 1. Then H can be computably partitioned into a finite number of integral locally closed subsets H_i' such that for each i, either (1) π_s is inseparable for all $s \in H_i'$ or (2) π_s is separable for all $s \in H_i'$.

To prove this claim, we use induction on the dimension of H. First, compute the irreducible components of H to reduce to the case where H is irreducible. The claim is clearly true if $\dim H = 0$. Suppose $\dim H \geq 1$, and let $\eta \in H$ be the generic point of H. By assumption, Y_η is smooth over $\kappa := k(\eta)$, so in particular, it is geometrically reduced. Compute some $f \in \kappa(Y_\eta)$ such that $\kappa(Y_\eta)$ is a finite separable extension of $\kappa(f)$. But, $\kappa(Y_\eta)$ is the function field of $\mathcal{Y}$, so compute a nonempty open subset $V \subset \mathcal{Y}$ on which f spreads out to a well defined k-morphism $\widetilde{f} \colon V \to \mathbb{A}_k^1$. Compute the image $U \subset H$ of V under $\mathcal{Y} \to H$. Then

$\widetilde{f}$ specializes to a well defined element f_s of $k(s)(Y_s)$ for all $s \in U$. Now, $df \neq 0 \in \Omega_{\kappa(Y_\eta)/\kappa}$ because $\kappa(Y_\eta)$ is separable over $\kappa(f)$, so we may replace U by a smaller nonempty open set to assume that $df_s \neq 0 \in \Omega_{k(s)(Y_s)/k(s)}$ for all $s \in U$. If $d(\pi_\eta^* f) = 0 \in \Omega_{\kappa(X_\eta)/\kappa}$, then $d(\pi_s^* f_s) = 0 \in \Omega_{k(s)(X_{k(s)})/k(s)}$ for all $s \in U$, meaning π_s is inseparable for all $s \in U$. If $d(\pi_\eta^* f) \neq 0 \in \Omega_{\kappa(X_\eta)/\kappa}$, we may again replace U by a smaller nonempty open set such that $d(\pi_s^* f_s) \neq 0 \in \Omega_{k(s)(X_{k(s)})/k(s)}$ for all $s \in U$, meaning π_s is separable for all $s \in U$. The irreducible components of $H \setminus U$ have smaller dimension than H, so, by induction, we have proved Claim 2.

In [3], the authors then prove the following claim. Because they work over $\overline{\mathbb{Q}}$, there is no mention of separability of π_s, but the proof of the claim stated here is exactly the same, so we will asume it.

Claim 3. Let H be a locally closed subset of G satisfying (2) in Claim 1 and (2) in Claim 2. Let J be the set of $s \in H$ for which the linear subspace $L \subset \mathbb{P}H^0(X_{k(s)}, \Omega_{X_{k(s)}}^{\otimes 3})$ is equal to the linear subspace $L' \subset \mathbb{P}H^0(X_{k(s)}, \Omega_{X_{k(s)}}^{\otimes 3})$ defined as the zero locus of the sections in the image of $H^0(Y_s, \Omega_{Y_s}^{\otimes 3}) \to H^0(X_{k(s)}, \Omega_{X_{k(s)}}^{\otimes 3})$. Then J is constructible and computable.

Claims 1, 2, and 3 together tell us that the set of $s \in G(k)$ satisfying (i), (ii), and (iii) above are the k-points of a constructible subset J of G. By the de Franchis-Severi theorem, there are finitely many such s, so $\dim J = 0$. Compute its k-points and their corresponding maps $\pi\colon X_k \to Y$. □

Corollary 6.1.2. *There exists an algorithm that takes as input a finitely generated field k_0 (set $k := \overline{k_0}$) and geometrically integral smooth projective curves X and Y over k_0 with $g(Y) \geq 2$ and returns the set of separable k-morphisms $X_k \to Y_k$.*

Proof. Compute the set of all pairs $(Y_1, \pi_1), \ldots, (Y_a, \pi_a)$ described in Theorem 6.1.1. Using Lemma 3.5.2, compute for all $1 \leq i \leq a$ the set of all k-isomorphisms $\psi_{i1}, \ldots, \psi_{ib_i}$ from $(Y_i)_k$ to Y_k. Then return the set of all $\psi_{ij} \circ \pi_i$ for $1 \leq i \leq a$ and $1 \leq j \leq b_i$. □

Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data, with $g(Y) = \widetilde{g} \geq 2$ and Y isotrivial. As

in the case $\widetilde{g} = 1$, we break the proof of 1.0.2 into the cases where Y is isotrivial and Y is nonisotrivial. Which case we are in can be detected using Proposition 3.5.4.

Proof of Theorem 1.0.2(iv), assuming Y is isotrivial. Using Proposition 3.5.4 and Remark 3.4.8, replace k_0 and K_0 by finite extensions and identify Y with $(Y_0)_{K_0}$ for some curve Y_0 over k_0. Thus

$$\begin{aligned} Y_0(K) &= \{\text{morphisms } \operatorname{Spec} K \to Y_0\} \\ &= \{k\text{-morphisms } C_k \to (Y_0)_k\} \\ &= Y_0(k) \cup \{\text{nonconstant } k\text{-morphisms } C_k \to (Y_0)_k\}. \end{aligned}$$

Using Corollary 6.1.2, compute the finitely many separable k-morphisms $g_1, \ldots, g_n \colon C_k \to (Y_0)_k$, and let $Q_1, \ldots, Q_n$ denote the corresponding elements of $Y_0(K)$. Let F denote the relative Frobenius $(Y_0)_k^{(1/p)} \to (Y_0)_k$. We claim that each point $P \in Y_0(K)$ falls into one of the following cases:

(i) $P = Q_i$ for some i, or

(ii) $P = F(Q)$ for some $Q \in (Y_0)_k^{(1/p)}(K)$.

To see this, suppose $P \in Y_0(K)$. If $P \in Y_0(k)$, then because k is algebraically closed, P satisfies (ii). Now, assume that $P \notin Y_0(k)$ and P does not satisfy (i). Then P can be identified with a nonconstant inseparable k-morphism $f \colon C_k \to (Y_0)_k$. This implies f factors as $g \circ F$ for some k-morphism $g \colon C_k^{(p)} \to (Y_0)_k$ (here we are using F to also denote the relative Frobenius $C_k \to C_k^{(p)}$). Taking the pth root of all coefficients in g gives us a k-morphism $g^{(1/p)} \colon C_k \to (Y_0)_k^{(1/p)}$, corresponding to a point $Q \in Y_0^{(1/p)}(K)$. Furthermore,

$$f = g \circ F = F \circ g^{(1/p)},$$

meaning $P = F(Q)$.

The set of P satisfying (i) is finite, so determine which ones lift to K-points of X. Compute $F\big((Y_0)_k^{(1/p)}(K)\big) \cap \pi(X(K))$ using Proposition 3.4.6, and compute $X(K)$ by taking preimages. □

6.2 Szpiro's height bound

Theorem 6.2.1 (Szpiro)**.** *Let k be a field of characteristic p, C be a geometrically integral smooth projective curve over k, $K := k(C)$, and Y be a geometrically integral smooth projective curve over K with $g(Y) \geq 2$. Let $\phi\colon \mathcal{Y} \to C$ be a semistable model for Y. Suppose $s\colon C \to \mathcal{Y}$ is a section of ϕ, and set $E := s(C)$. Let f be the number of nonsmooth fibers of ϕ and e be the modular inseparability exponent of Y. Then*

$$-E.E \leq p^e \frac{8}{3} 3^{3g(Y)+2} (g(Y)-1)^2 \left(f + 1 + \frac{2g(C)-2}{3^{g(Y)}} + \frac{1}{3^{3g(Y)}} \right). \tag{6.1}$$

Proof. See [34, Corollaire 2]. □

Remark 6.2.2. Given Input 3.4.3 data (p, k_0, C, K_0, Y) and a semistable model $\phi\colon \mathcal{Y} \to C$ for Y as in Theorem 6.2.1, we can use Corollary 3.5.8 to compute e, so we can compute the number on the right hand side of (6.1).

Theorem 6.2.3 (Szpiro)**.** *Let k, K, C, Y, and $\phi\colon \mathcal{Y} \to C$ be as in Theorem 6.2.1. The relative dualizing sheaf $\omega_{\mathcal{Y}/C} = \omega_{\mathcal{Y}} \otimes (\phi^*\Omega_C)^{-1}$ satisfies*

(i) $\omega_{\mathcal{Y}/C}.\omega_{\mathcal{Y}/C} \geq 0$, with equality if and only if Y is isotrivial, and

(ii) $\omega_{\mathcal{Y}/C}.D \geq 0$ for all effective divisors D on $\mathcal{Y}$, with equality if and only if D is supported on the rational curves of self-intersection -2 contained in the fibers of ϕ.

If Y is nonisotrivial, $\omega_{\mathcal{Y}/C}$ is big.

Proof. See [34, Théorème 1 and Théorème 2]. Bigness of $\omega_{\mathcal{Y}/C}$ follows from [21, Theorem 2.2.16]. □

6.3 Effective Mordell and proof of main theorem for $\widetilde{g} \geq 2$

Theorem 6.3.1 (Samuel)**.** *Let k be a field of characteristic p, C be a geometrically integral smooth projective curve over k, and $K := k(C)$. If Y is a geometrically integral smooth projective nonisotrivial curve over K with $g(Y) \geq 2$, then $Y(K)$ is finite.*

Proof. See [27, Théorème 4]. □

Lemma 6.3.2. *There exists an algorithm that takes as input a finitely generated field k_0, a polynomial $P \in \mathbb{Q}[t]$, and an integer m and returns the Hilbert scheme H of closed subschemes of $\mathbb{P}^m_{k_0}$ with Hilbert polynomial P as well as its universal family $\mathcal{H} \subset \mathbb{P}^m_{k_0} \times H$.*

Proof. This is a consequence of work by Gotzmann in [12, Section 3]. See [26, Lemma 8.23] for details. □

Theorem 6.3.3. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y) with $g(Y) \geq 2$ and Y nonisotrivial and returns $Y(K)$.*

Proof. First, use Corollary 3.5.12 to enlarge k_0 and K_0 such that Y has a semistable model and compute such a semistable model $\phi\colon \mathcal{Y} \to C$. For the remainder of this proof, it will be convenient to work over k instead of k_0, so by base changing, we will consider $\mathcal{Y}$ and C as varieties over k. Suppose that $\mathcal{Y}$ is embedded in $\mathbb{P}^m_k$, and let P be a hyperplane section on $\mathcal{Y}$. Compute the number N on the right hand side of (6.1) (see Remark 6.2.2). Compute divisors $K_{\mathcal{Y}}$ and K_C on $\mathcal{Y}$ such that $\omega_{\mathcal{Y}} \cong \mathcal{O}_{\mathcal{Y}}(K_{\mathcal{Y}})$ and $\phi^*\Omega_C \cong \mathcal{O}_{\mathcal{Y}}(K_C)$, and set $K_{\mathcal{Y}/C} := K_{\mathcal{Y}} - K_C$. By Theorem 6.2.3 and Kodaira's lemma ([21, Proposition 2.2.6]), $H^0(\mathcal{Y}, nK_{\mathcal{Y}/C} - P)$ is nonzero for sufficiently large n. Compute some positive integer n and effective divisor D on $\mathcal{Y}$ such that $nK_{\mathcal{Y}/C}$ is linearly equivalent to $P + D$. Compute the irreducible components $C_1, \ldots, C_r$ of D, and compute the nonnegative integer

$$M := \max\{0, -C_1.D, -C_2.D, \ldots, -C_r.D\}$$

(intersection numbers can be computed; see [26, Lemma 8.7 and Remarks 8.8 and 8.9]).

Note that if C' is an integral curve on $\mathcal{Y}$, then $C'.D \geq -M$. A point $Q \in Y(K)$ corresponds to a section s_Q of ϕ. Let $E := s_Q(C) \subset \mathcal{Y}$. First, note that

$$\begin{aligned} E.K_{\mathcal{Y}/C} &= E.K_{\mathcal{Y}} - E.K_C \\ &= (2g(C) - 2 - E.E) - (2g(C) - 2) \qquad \text{(adjunction formula)} \\ &= -E.E, \end{aligned} \tag{6.2}$$

from which we have

$$\begin{aligned} E.P &= E.(nK_{\mathcal{Y}/C} - D) \\ &= -nE.E - E.D \\ &\leq nN + M \qquad \text{(Theorem 6.2.1).} \end{aligned} \tag{6.3}$$

Therefore, the degree of E as a closed subvariety of $\mathbb{P}^m_k$ is at most $nN + M$.

Now, for each $1 \leq d \leq nN + M$, compute the Hilbert scheme H of 1-dimensional k-subschemes of $\mathbb{P}^m_k$ of genus $g(C)$ and degree d as well as the universal family $\psi\colon \mathcal{H} \to H$ embedded in $\mathbb{P}^m_k \times_k H$. Our goal will be to compute the $h \in H(k)$ such that

(i) $\mathcal{H}_h$ is integral and smooth,

(ii) $\mathcal{H}_h \subset \mathcal{Y}$ as subvarieties of $\mathbb{P}^m_k$, and

(iii) ϕ restricts to an isomorphism $\mathcal{H}_h \to C$.

We will compute the locus of points that satisfy these three properties step by step.

Step (i).

Compute the open subset $H_{sm} \subset H$ on which $\mathcal{H} \to H$ restricts to a smooth morphism. The function $H_{sm}(k) \to \mathbb{Z}_{\geq 0}$ given by

$$h \mapsto \#\text{ of connected components of } (\mathcal{H}_{sm})_h$$

is locally constant because $\psi^{-1}(H_{sm}) \to H_{sm}$ is flat, proper, and smooth ([7, Theorem 4.17(iii)]). Compute the union $H_{sm,int}$ of the connected components of H_{sm} on which the above function is identically 1. Thus, $H_{sm,int}$ is the open subset of h in H such that $\mathcal{H}_h$ is smooth and integral.

Step (ii).

Claim 1. Let H' be a reduced locally closed subvariety of $H_{sm,int}$, and let H'' be the locus of $h \in H'$ such that $\mathcal{H}_h \subset \mathcal{Y}_{k(h)} \subset \mathbb{P}^m_{k(h)}$. Then H'' is a computable closed subset of H'.

We prove Claim 1 by induction on the dimension of H'. It suffices to assume that H' is irreducible and affine, say $H' = \operatorname{Spec} A$. Let $\mathcal{H}' \subset \mathcal{H}$ be the preimage of H'. Let F denote the fraction field of A. Let $S := A[x_0, \ldots, x_m]$ be the homogeneous coordinate ring of $\mathbb{P}^m_A$ and I be the homogeneous ideal for $\mathcal{H}' \subset \mathbb{P}^m_A$.

Now consider the following procedure given a homogeneous element f in S of degree e. Compute a projection $p_F \colon S_e \otimes_A F \to I_e \otimes_A F$ (here S_e and I_e denote the graded pieces of degree e in S and I respectively). Write p_F as a matrix with entries in F, and compute the localization A' of A by inverting the denominators of these entries. Thus, p_F spreads out to an A'-homomorphism $p_{A'} \colon S_e \otimes_A A' \to I_e \otimes_A A'$ that is the identity when restricted to $I_e \otimes_A A'$. Compute

$$f - p_{A'}(f) = \sum_\alpha a_\alpha(f) x^\alpha$$

(here we are again using multi-index notation, i.e., if $\alpha = (\alpha_0, \ldots, \alpha_m)$ with $\alpha_0 + \cdots + \alpha_m = e$, then $x^\alpha := x_0^{\alpha_0} \cdots x_m^{\alpha_m}$).

Let $f_1, \ldots, f_\ell$ be homogeneous generators for the ideal for $\mathcal{Y}$ thought of as elements of S. Let J be the radical of the ideal of A' generated by all the $a_\alpha(f_i)$, and let $A'' := A'/J$. A point $h \in \operatorname{Spec} A'(k)$ is such that $\mathcal{H}_h \subset \mathcal{Y}$ if and only if $a_\alpha(f_i)$ vanish at h for all α and i. Thus, $\operatorname{Spec} A''$ is the intersection of the desired closed subvariety H'' with $\operatorname{Spec} A'$. The complement $H' \setminus \operatorname{Spec} A'$ has dimension less than the dimension of H', so by induction, we have proved Claim 1.

Apply Claim 1 to $H' := H_{sm,int}$ to compute the locally closed subvariety $Z \subset H$ of points

$h \in H$ such that $\mathcal{H}_h$ is a smooth integral curve contained in $\mathcal{Y}$, and let $\mathcal{Z} \subset \mathcal{H}$ be the preimage of Z.

Step (iii).

Let ϕ' be the composition of Z-morphisms $\mathcal{Z} \to \mathcal{Y} \times_k Z \to C \times_k Z$. We now wish to determine the set of $h \in Z(k)$ such that $\phi'_h \colon \mathcal{Z}_h \to C$ is an isomorphism.

Claim 2. Let $h \in Z(k)$ be a point such that $\phi'_h \colon \mathcal{Z}_h \to C$ is an isomorphism. Then h is an isolated point of Z.

To see this, let h be such a point. Let ε denote the generic point of C and consider the pullback morphism $\phi'_\varepsilon \colon \mathcal{Z}_\varepsilon \to \varepsilon \times Z$. Notice that the set of $h' \in Z(k)$ such that $\phi'_{h'}$ is a nonconstant morphism is the set of $h' \in Z(k)$ in the image of ϕ'_ε. But, ϕ'_ε is the composition of flat morphisms $\mathcal{Z}_\varepsilon \to \mathcal{Z} \to Z$, so the image of ϕ'_ε is an open subset U of Z containing h. Let $\mathcal{U} \subset \mathcal{Z}$ be the preimage of U. Then $\phi'|_{\mathcal{U}} \colon \mathcal{U} \to C \times_k U$ is quasi-finite. Furthermore, $\phi'|_{\mathcal{U}}$ is proper because $C \times_k U \to U$ is separated and the composition $\mathcal{U} \to C \times_k U \to U$ is proper, so $\phi'|_{\mathcal{U}}$ is finite. It follows that the function $\delta \colon C \times_k U \to \mathbb{Z}_{\geq 1}$ given by

$$y \mapsto \dim_{k(y)} \mathcal{O}_{\mathcal{U},\phi'^{-1}(y)} \otimes_{\mathcal{O}_{C \times_k U,y}} k(y)$$

is upper semicontinuous ([14, Exercise II.5.8]). The function $U \to \mathbb{Z}_{\geq 1}$ given by $h' \mapsto \delta(\varepsilon, h')$ is therefore upper semicontinuous. But $\delta(\varepsilon, h')$ is equal to the degree of $\phi'_{h'}$, so there exists some open $V \subset U$ containing h such that $\phi'_{h'}$ is an isomorphism for all $h' \in V$. For such h', the inverse $C \to \mathcal{Z}_{h'}$ composed with $\mathcal{Z}_{h'} \to \mathcal{Y}$ defines a section of ϕ. There can only be finitely many such sections by Theorem 6.3.1, so V is 0-dimensional. This proves Claim 2.

To compute $Y(K)$, compute the 0-dimensional irreducible components $h_1, \ldots, h_s$ of Z and determine which give rise to isomorphisms $\mathcal{Z}_{h_i} \to C$. Lastly, compute their inverses $C \to \mathcal{Z}_{h_i}$ and their corresponding elements of $Y(K)$. □

Proof of Theorem 1.0.2(iv), assuming Y is nonisotrivial. Let $(p, k_0, C, K_0, X, Y, \pi)$ be Input 3.4.3 data with $g(Y) = \widetilde{g} \geq 2$ and Y nonisotrivial. Compute $Y(K)$ using Theorem 6.3.3,

and then compute $X(K)$ as the set of K-points in $\pi^{-1}(Y(K))$. □

6.4 Purely inseparable points

Kim proves the following generalization of Theorem 6.3.1.

Theorem 6.4.1 (Kim)**.** *Let k be a field of characteristic p, C be a geometrically integral smooth projective curve over k, and $K := k(C)$. Let K^{1/p^∞} denote the union inside $\overline{K}$ of K^{1/p^n} for all n. If Y is a geometrically integral smooth projective nonisotrivial curve over K with $g(Y) \geq 2$, then $Y(K^{1/p^\infty})$ is finite.*

Proof. See [17, Corollary 1]. □

Here we show that his proof can be made effective.

Theorem 6.4.2. *There exists an algorithm that takes Input 3.4.3 data (p, k_0, C, K_0, Y) with $g(Y) \geq 2$ and Y nonisotrivial and returns $Y(K^{1/p^\infty})$.*

Proof. We start off with much of the same computation as in the proof of Theorem 6.3.3. Enlarge k_0 and K_0 and compute a semistable model $\phi\colon \mathcal{Y} \to C$. Compute the number f of nonsmooth fibers of ϕ. Suppose that $\mathcal{Y}$ is embedded in $\mathbb{P}^m_{k_0}$, and let P be a hyperplane section on $\mathcal{Y}$. Compute a positive integer n and effective divisor D on $\mathcal{Y}$ such that $nK_{\mathcal{Y}/C}$ is linearly equivalent to $P + D$. Compute the irreducible components $C_1, \ldots, C_r$ of D, and compute the nonnegative integer $M := \max\{0, -C_i.D\}$.

We now compute a nonnegative integer e_0 such that $Y(K^{1/p^\infty}) = Y(K^{1/p^{e_0}})$. For $e \geq 1$, an element of $Y(K^{1/p^e}) \setminus Y(K^{1/p^{e-1}})$ corresponds to a morphism $s\colon C_k \to \mathcal{Y}_k$ such that $\phi \circ s = F^e$ (here, F denotes the absolute Frobenius $C_k \to C_k$) and $s^*\Omega_{\mathcal{Y}} \to \Omega_C$ is nonzero. Let $E := s(C_k) \subset \mathcal{Y}_k$. Kim establishes the bound

$$E.K_{\mathcal{Y}/C} \leq 2g(C) - 2 + f. \tag{6.4}$$

Therefore,

$$E.P = nE.K_{\mathcal{Y}/C} - E.D \leq n(2g(C) - 2 + f) + M. \tag{6.5}$$

Also, as in (6.2), we have $E.E = -E.K_{\mathcal{Y}/C}$. Let R be the $\mathbb{Q}$-divisor

$$R := E - \frac{E.P}{P.P}P.$$

Then, combining everything,

$$-(2g(C) - 2 + f) \leq -E.K_{\mathcal{Y}/C} = E.E = \frac{(E.P)^2}{P.P} + R.R \leq \frac{(n(2g(C) - 2 + f) + M)^2}{P.P} + R.R,$$

so

$$-R.R \leq \frac{(n(2g(C) - 2 + f) + M)^2}{P.P} + 2g(C) - 2 + f =: \rho. \tag{6.6}$$

Let $c \in C(k)$, set $Z := \phi^{-1}(c)$, and let

$$S := Z - \frac{Z.P}{P.P}P.$$

Now,

$$p^e = \deg(F^{e*}c) = \deg Z|_E = E.Z = \frac{(E.P)(Z.P)}{P.P} + R.S. \tag{6.7}$$

The Hodge index theorem tells us that R and S lie on a subspace of $\mathrm{NS}(\mathcal{Y}) \otimes \mathbb{Q}$ on which the intersection pairing is negative definite. By Cauchy-Schwarz and (6.6),

$$(R.S)^2 \leq (R.R)(S.S) \leq -\rho S.S. \tag{6.8}$$

Combining (6.5), (6.7), and (6.8) gives

$$p^e \leq (n(2g(C) - 2 + f) + M)\frac{Z.P}{P.P} + \sqrt{-\rho S.S}. \tag{6.9}$$

Compute the largest integer e_0 less than or equal to the base p logarithm of the last expression above. To finish, compute $Y(K^{1/p^{e_0}})$ using Theorem 6.3.3. $\square$

A Sample code

The following Sage code was used to compute $\#X_n(K_0)$ from Example 4.3.1 in the case $p = 3$ and $1 \leq n \leq 79$, $3 \nmid n$. It is an implementation of the algorithm described in Section 4.3.

```
from sage.geometry.newton_polygon import NewtonPolygon
from numpy import ndindex

#The characteristic.
p = 3

#We are taking K to be the rational function field F_p(t).
O = PolynomialRing(GF(p,'c'),'t')
t = O.gen()
K = FractionField(O)

R = PolynomialRing(K,'x')
x = R.gen()

for n in range(1,80):
    if n%p==0: continue

#We are counting points on the curve y^p = r
    r = x^(p-1)-(t^n-1)^(p-1)

    facts = r.factor()
    deg = r.degree()

#Compute two rational points on P^1 at which r has valuation not
#divisible by p.
    fact1 = x
    fact2 = 1
    for tu in facts:
        if diff(tu[0],x)!=0 and tu[1]%p!=0:
            fact1 = tu[0]
            break;
    else:
        print "There are no separable factors of r"

    if deg%p==0:
        for tu in facts:
            if diff(tu[0],x)!=0 and tu[1]%p!=0 and tu[0]!=fact1:
```

```
                fact2 = tu[0]
                break;

#Let s be r composed with a linear fractional transformation so that s has
#valuations at 0 and infinity not divisible by p.
    s = r
    if fact2==1:
        s = r(x-fact1(0))
    else:
        s = r((fact2(0)*x-fact1(0))/(-x+1))

#Create a dictionary whose keys are the places v of K supported on
#coefficients a_i of s and whose values are dictionaries whose keys are
#integers i and whose values are ord_v(a_i).
    placedict = {}
    for i in range(s.degree()+1):
        if s[i]==0: continue
        afacts = s[i].factor()
        if len(afacts)==0: continue

        for tu in afacts:
            if not tu[0] in placedict:
                placedict[tu[0]] = {i:tu[1]}
            else:
                placedict[tu[0]][i] = tu[1]

    for i in range(s.degree()+1):
        if s[i]==0: continue
        for place in placedict:
            if not i in placedict[place]: placedict[place][i] = 0

#Create a dictionary whose keys are the places v as above and whose values
#are the possible numbers ord_v(x) mod p for solutions of y^p=s(x)
#according to the Newton polygon at v.
    xvals = {}
    for place in placedict:
        vals = map(lambda k: (k,placedict[place][k]), placedict[place].keys())
        np = NewtonPolygon(vals)
        xvals[place] = []
        slopes = uniq(np.slopes())
        verts = np.vertices()
        numverts = len(verts)
        for mu in slopes:
            if(mu%1==0): xvals[place].append((-mu)%p)
        for i in range(numverts):
```

```
            mu = verts[i][1]/verts[i][0]
            if mu%1!=0: continue
            if i==0 or i==numverts-1 or \
            floor((verts[i][1]-slopes[i]*verts[i][0])/p) > \
            floor((verts[i-1][1]-slopes[i-1]*verts[i-1][0])/p):
                xvals[place].append((-mu)%p)

#Solve y^p=s(alpha*x^p), where alpha runs through a complete set of
#representatives of elements of K whose valuations mod p at each v are the
#ones prescribed by xvals.
    sprime = diff(s,x)
    sdelta = diff(s,t)
    points = set({-fact1(0)})
    numplaces = len(placedict.keys())
    numexps = []
    for place in xvals: numexps.append(len(xvals[place]))
    exps = ndindex(tuple(numexps))
    tocheck = 1
    for i in numexps: tocheck = tocheck * i

    for exp in exps:
        alpha = 1
        for i in range(numplaces):
            place = placedict.keys()[i]
            alpha = alpha*place^xvals[place][exp[i]]
        salpha = sprime(alpha*x^p)*diff(alpha,t)*x^p+sdelta(alpha*x^p)
        salpharoots = salpha.roots()

        if fact2==1:
            points.update(map(lambda tu: \
                alpha*tu[0]^p-fact1(0),salpha.roots()))
        else:
            points.update(map(lambda tu: \
                (fact2(0)*alpha*tu[0]^p-fact1(0))/(-alpha*tu[0]^p+1), \
                salpha.roots()))

#Output the number of solutions.
    print str(n)+": "+str(len(points))
```

References

[1] G.W. Anderson. Abeliants and their application to an elementary construction of Jacobians. *Advances in Mathematics*, 172:169–205, 2002.

[2] E. Artin. *Algebraic numbers and algebraic functions*. Gordon and Breach, New York/London/Paris, 1967.

[3] M. H. Baker, E. González-Jiménez, Josep González, and B. Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127:1325–1387, 2005.

[4] D. Bayer and M. Stillman. Computation of Hilbert functions. *J. Symbolic Computation*, 14:31–50, 1992.

[5] B. Conrad. Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. *Enseign. Math.*, 52:37–108, 2006.

[6] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, 2007.

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

[8] B. Dwork. On the rationality of the zeta function of an algbraic variety. *Amer. J. Math.*, 82:631–648, 1960.

[9] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer, New York, 2004.

[10] D. Eisenbud, D. R. Grayson, M. Stillman, and B. Sturmfels. *Computations in algebraic geometry with Macaulay2*, volume 8 of *Algorithms and computation in mathematics*. Springer-Verlag, New York, 2002.

[11] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Computation*, 6:149–167, 1988.

[12] G. Gotzmann. Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes. *Mathematische Zeitschrift*, 158:61–70, 1978.

[13] H. Grauert. Mordells vermutung über rationale punkte auf algebraischen kurven und funktionenkörper. *Publications Mathématiques de l'IHÉS*, 25:131–149, 1965.

[14] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[15] S. Jambor. Primary decomposition of zero-dimensional ideals over arbitrary fields. Unpublished preprint, 2014.

[16] S. T. Jeong. Rational points on algebraic curves that change genus. *Journal of Number Theory*, 67:170–181, 1997.

[17] M. Kim. Purely inseparable points on curves of higher genus. *Mathematical Research Letters*, 4:663–666, 1997.

[18] S. Lang. Algebraic groups over finite fields. *American Journal of Mathematics*, 78:555–563, 1956.

[19] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1987.

[20] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[21] R. Lazarsfeld. *Positivity in algebraic geometry I*, volume 48 of *A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin Heidelberg, 2004.

[22] R. Matsumoto. Computing the radical of an ideal in positive characteristic. *J. Symbolic Computation*, 32:263–271, 2001.

[23] J. S. Milne. Jacobian varieties. In *Arithmetic geometry*, Storrs, Conn., pages 167–212. Springer-Verlag, New York, 1984.

[24] L. Moret-Bailly. Piceaux de variétés abéliennes. *Astérisque*, 129, 1985.

[25] B. Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, 2017.

[26] B. Poonen, D. Testa, and R. Van Luijk. Computing Néron-Severi groups and cycle class groups. *Compositio Mathematica*, 151:713–734, 2015.

[27] P. Samuel. Compléments à un article de Hans Grauert sur la conjecture de Mordell. *I.H.E.S. Publ. Math.*, 29:55–62, 1966.

[28] J.-P. Serre. Sur la topologie des variétés algébriques en caractéristique p. *Symposium Internacional de Topología Algebraica*, pages 24–53, 1958.

[29] J.-P. Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer, New York, 1988.

[30] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, New York, 1994.

[31] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2009.

[32] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2019.

[33] G. Stolzenberg. Constructive normalization of an algebraic variety. *Bull. Amer. Math. Soc.*, 74:595–599, 1968.

[34] L. Szpiro. Séminaire sur les pinceaux de courbes de genre au moins deux. *Astérisque*, 86, 1981.

[35] D. L. Ulmer. p-descent in characteristic p. *Duke Math. J.*, 62:237–265, 1991.

[36] D. L. Ulmer. Curves and Jacobians over function fields. Centre de Recerca Mathemàtica, February 2010.

[37] D. L. Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011.

[38] J. F. Voloch. Explicit p-descent for elliptic curves in characteristic p. *Compositio Mathematica*, 74:247–258, 1990.

[39] J. F. Voloch. A diophantine problem on algebraic curves over function fields of positive characteristic. *Bull. Soc. Math. Frace*, 119:121–126, 1991.