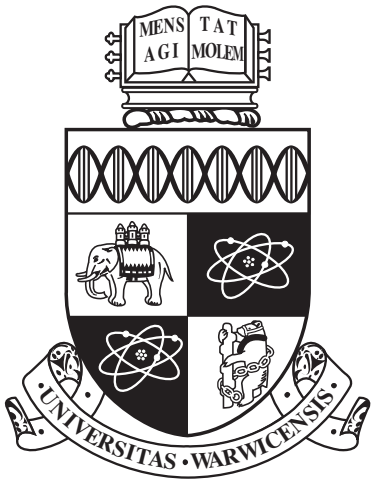


Common Projective Torsion Points of Pairs of Elliptic Curves and the Methods of Raynaud

by

David Hubbard

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Warwick Mathematics Institute

September 2025

THE UNIVERSITY OF
WARWICK

Acknowledgments

I would like to thank my supervisor Christian Böhning for his support throughout the PhD. He has taught me many things over the past four years, but the most invaluable lesson has been how to think about geometry with an unbiased view towards its connections with topology, number theory, group theory and analysis.

Thank you to Professor Alexei Skorobogatov for meeting with me at Imperial College London for a secondment in my third year, and to Professor Yuri Tschinkel and the Simons Foundation for hosting me in my final year where I finished writing this thesis. I would like to thank Professor David Holmes for our discussions on logarithmic geometry at GAeL in Turin. I feel that this was a turning point in my understanding of how to apply the techniques from logarithmic geometry to the methods of Raynaud discussed in this thesis. Thank you to Professors Damiano Testa and Gavin Brown who both spent many hours discussing calculations related to this thesis and taking time to answer any questions I had. I would also like to thank Martin Gallauer whom I met at Oxford when he gave classes on elliptic curves and category theory and is now a permanent member of the Warwick Mathematics Institute. As a master's student, I resonated very much with the higher level view he showed us of pure mathematics, and speaking to him as a graduate student, I feel that I can begin to appreciate more greatly the philosophy behind motives, infinity categories and other attempts to unify mathematics in a more general framework.

I would like to thank the many PhD students and other young researchers who have taken the times to discuss elements of this thesis and related problems. This is by no means an exhaustive list, but thank you to Daniel Marlowe, Margherita Pagano, Sara Veneziale, Michaela Barbieri, Marta Benozzo, Vanja Zuliani, Thomas Read, Dhruva Divate, Diana Mocanu, Bianca Gouthier, Alvaro Gonzalez Hernandez, Tommaso Faustini and Franco Giovenzana.

Thank you to my friends Gabe, James, Joe, Noah, Oscar, Tom B., Maddie, Jess, Indie, Alice, Ellie, Sam, Caspar, Dom, Tom G., Alex, Tom O., Caleb, Josh, Ollie, Fergus, Will, George, Ruby, Noah, Sophie, Lizzie and Olivia. Thank you to my mum, dad, and sister Isabella for their continued support over the last four years.

Declaration

The work presented in this thesis is my own except where I have stated otherwise. This work has not been presented for a degree at any other university. This thesis was written in my capacity as a PhD student at the Warwick Mathematics Institute. The author was funded by the UK Engineering and Physical Sciences Research Council: studentship code (EP/W523793/1).

Abstract

Suppose E_1, E_2 are elliptic curves over the complex numbers equipped with standard double coverings $\pi_i \colon E_i \to \mathbb{P}^1$; ramified in the two-torsion points of E_i. Let $E_i[\infty]$ be the torsion points on E_i. In [BFT18], Bogomolov, Fu and Tschinkel ask if the number of points in $\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])$ is uniformly bounded over all pairs of curves where the branch loci of π_1 and π_2 do not coincide. This was answered affirmatively in [DKY20, Kueh21, Gao21, DGH21, GGK21] and also [Poi22-1, Poi22-2], but realistic effective bounds are unknown.

In this thesis, we obtain such realistic bounds for common projective torsion points on elliptic curves under some mild extra assumptions on the reduction type of the input data at given primes. The method is based on Raynaud's original work on the Manin-Mumford conjecture [Ray83-1, Ray83-2]. In particular, we generalise several of his results to cases of bad reduction using techniques from logarithmic geometry.

The problem of Bogomolov-Fu-Tschinkel, along with the Manin-Mumford conjecture belong to the *unlikely intersections* of arithmetic geometry. We discuss some related problems in this area including Lang's conjecture on torsion points lying on curves in the 2-torus. Using the techniques of Beukers-Smyth, we give a much simpler and more conceptual proof of a result of Fu on roots of unity under projective equivalence that also falls under the umbrella of unlikely intersections.

Contents

Introduction **ix**

Common projective torsion of points of pairs of elliptic curves ix

Unlikely intersections and uniformity xii

Lang's problem on curves in the torus and projective equivalence of roots of unity xiii

Structure of this thesis xiv

I Lang's problem on torsion points of curves in the torus and projective equivalence of roots of unity **xvi**

Chapter 1 Torsion points on curves in the torus **1**

1.1 A problem of Lang 1

1.2 Uniformity and roots of unity on curves in the torus 2

Chapter 2 Projective equivalence and roots of unity **7**

2.1 Projective equivalence and roots of unity 7

2.2 Maximal examples 9

II The case of good reduction **13**

Chapter 3 Preliminaries **14**

3.1 Local fields 14

3.1.1 Background on local fields 14

3.1.2 Extensions of Dedekind domains 16

3.1.3 Galois extensions of local fields 17

3.1.4 Extensions of complete fields 18

3.1.5 Witt vectors 18

3.2 Abelian varieties and finite flat group schemes 20

3.2.1 Group schemes 20

3.2.2 Abelian varieties 22

3.2.3 Hopf algebras and affine group schemes 24

3.2.4 Finite flat group schemes and quotients . . . 25
3.2.5 The étale fundamental group . . . 27
3.2.6 The connected-étale sequence . . . 29
3.2.7 Cartier duality . . . 30
3.2.8 Prolongations of group schemes . . . 32
3.2.9 Tate modules . . . 33
3.3 p-divisible groups and formal groups . . . 36
3.3.1 p-divisible groups . . . 36
3.3.2 The p-divisible group of an elliptic curve . . . 42
3.4 Geometry of curves in characteristic $p > 0$ . . . 44
3.4.1 Frobenius and differentials . . . 44
3.4.2 The Cartier operator . . . 46
3.4.3 Lifts of Frobenius . . . 48
3.5 Mixed characteristic deformation theory . . . 50
3.5.1 Formal schemes . . . 50
3.5.2 Flat liftings . . . 51
3.5.3 Lifting schemes from characteristic p to characteristic 0 . . . 54
3.5.4 Lifting closed subschemes . . . 57
3.5.5 Lifting finite morphisms . . . 58
3.6 Serre-Tate moduli . . . 59
3.6.1 Serre-Tate theorem . . . 60
3.6.2 Serre-Tate formal moduli . . . 61
3.6.3 Properties of canonical liftings . . . 63
3.7 Inertia representations attached to elliptic curves . . . 65
3.7.1 The Néron-Ogg-Shafarevich criterion . . . 65
3.7.2 Galois theory of local fields . . . 67
3.7.3 Galois representations of the formal group of an elliptic curve . . . 69
3.7.4 Inertia representations of elliptic curves with supersingular reduction 72
3.7.5 Inertia representations of elliptic curves with good ordinary reduction 73

Chapter 4 Raynaud's proof of the Manin-Mumford conjecture 76
4.1 Raynaud's proof of the Manin-Mumford conjecture . . . 76
4.1.1 Normal bundles . . . 78
4.1.2 Lifting morphisms with zero k-differential . . . 84
4.1.3 Proof of Theorem II . . . 89
4.1.4 Refinements on the bounds . . . 100
4.1.5 Inertia actions and p-divisible groups . . . 102

Chapter 5 Bounds obtained for the Bogomolov-Fu-Tschinkel conjecture in the case of good reduction **106**
5.1 Bounds obtained for the Bogomolov-Fu-Tschinkel conjecture in the case of good reduction . . . 106
5.1.1 The Jacobian of the curve X . . . 109
5.1.2 Bounds on common coprime-to-p torsion . . . 112
5.1.3 Bounds on common torsion points of any order . . . 114

III The case of semistable reduction and methods from logarithmic geometry **116**

Chapter 6 Semistable reduction and Néron models **117**
6.1 Néron models of elliptic curves and Tate curves . . . 117
6.1.1 Properties of Néron models . . . 117
6.1.2 Néron models of elliptic curves . . . 118
6.1.3 Kodaira-Néron classification . . . 122
6.1.4 Tate curves . . . 124
6.2 Semistable reduction and Grothendieck's orthogonality theorem . . . 127
6.2.1 Semistable reduction theorem . . . 127
6.2.2 Grothendieck's orthogonality theorem . . . 128
6.2.3 Deligne-Rapoport generalised elliptic curves . . . 132

Chapter 7 Logarithmic geometry **133**
7.1 Toric geometry and monoids . . . 135
7.1.1 Toric geometry . . . 135
7.1.2 Monoids . . . 139
7.1.3 The étale topology . . . 141
7.2 Logarithmic geometry . . . 142
7.2.1 Logarithmic schemes . . . 142
7.3 Log smooth curves, log differentials and log deformation theory . . . 146
7.3.1 Log smooth curves . . . 146
7.3.2 Logarithmic differentials . . . 148
7.3.3 Logarithmic deformation theory . . . 150
7.3.4 Logarithmic geometry in positive characteristic . . . 151
7.3.5 Logarithmic blow-ups . . . 153

Chapter 8 Extending Raynaud's method to the semistable case and methods from log geometry **156**
8.1 Extending Raynaud's method to the semistable case . . . 156

8.1.1 Bounds obtained in the case of semistable reduction 159
8.1.2 Finiteness and methods from log geometry 164

IV Appendix **173**

Appendix A Estimating the Serre-Tate coordinate of an elliptic curve **174**
A.1 Canonical liftings modulo p^n 174
A.2 Estimating the Serre-Tate coordinate 175

Appendix B Bogomolov's result on homotheties **176**
B.1 Homotheties of the p-adic Tate module 176
B.2 Application to torsion points on curves 176

Bibliography **178**

Introduction

Common projective torsion of points of pairs of elliptic curves

Let E be an elliptic curve over the complex numbers. A *standard double cover* $\pi : E \to \mathbb{P}^1$ is a double cover of the projective line by E compatible with the inversion map $\iota : E \to E$ in the sense that $\pi \circ \iota = \pi$. A standard double cover is ramified in the 2-torsion points $E[2]$ of E. We write $\pi(E[2]) = \{a, b, c, d\} \subset \mathbb{P}^1$ for the set of branch points and let $E[\infty]$ denote the torsion subgroup of E. In [BFT18], Bogomolov-Fu-Tschinkel were interested in comparing the torsion points of pairs of elliptic curves over the complex numbers. To do this, they considered pairs of elliptic curves with standard double covers (π_i, E_i) for $i = 1, 2$ and studied the set of *common projective torsion points* $\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])$. The authors showed that, whenever the branch loci $\pi_1(E_1[2])$ and $\pi_2(E_2[2])$ do not coincide, this intersection is finite. Indeed, considering the curve:

$$\begin{array}{ccc} X & \hookrightarrow & E_1 \times E_2 \\ \downarrow & & \downarrow{\scriptstyle \pi_1 \times \pi_2} \\ \Delta_{\mathbb{P}^1} & \hookrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \end{array}$$

where $\Delta_{\mathbb{P}^1}$ is the diagonal and X is its preimage under the product of the standard double covers, an easy calculation shows that the condition on branch loci ensures that X is integral and of geometric genus ≥ 2. This places us in the situation of the *Manin-Mumford conjecture*:

Theorem. *Let $X \hookrightarrow A$ be an integral curve of geometric genus g in an abelian variety defined over $\mathbb{C}$. Let $A[\infty]$ denote the torsion subgroup of A. Then the intersection:*

$$X \cap A[\infty]$$

is finite unless $X = E + a$ where E is an elliptic curve, and $a \in A[\infty]$. In particular, if $g \geq 2$ then, the set of torsion points of X is finite.

The conjecture was raised independently by Manin and Mumford in the classical

setting of a smooth curve C of genus ≥ 2 embedded in its Jacobian $C \hookrightarrow J_C$ and was first proven by Raynaud [Ray83-1]. Bogomolov-Fu-Tschinkel conjectured that, among pairs (E_i, π_i) of standard double covers whose branch loci do not coincide, there is a *uniform bound* c, such that:

$$|\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])| \leq c$$

that does not depend on either curve E_i. Recently, several authors [DKY20,Kueh21,Gao21, DGH21,GGK21] managed to show, as a corollary of their work, that there exists a uniform constant c satisfying the above conjecture. Poineau in [Poi22-1, Poi22-2] also proved this using a different technique involving Berkovich spaces over the integers, and dynamics of Lattès maps.

To the best of our knowledge, these approaches have so far failed to determine the minimal possible c above and have not yielded *effective realistic* bounds. On the other hand, one knows pairs (E_i, π_i) for which the number of common projective torsion points $|\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])|$ is comparatively large [BF17, FS19]. The current record is 34 [FS19]. In this thesis, we aim to provide a realistic bound c on the common projective torsion points of pairs of elliptic curves, which holds when certain geometric conditions are met. To do so, we employ Raynaud's original proof of the Manin-Mumford conjecture [Ray83-1] applied to the curve $X = (\pi_1 \times \pi_2)^{-1}(\Delta_{\mathbb{P}^1}) \hookrightarrow E_1 \times E_2 = A$.

By a specialisation argument, one restricts to the case where the input data is defined over a number field. Raynaud then passes to an unramified extension K of $\mathbb{Q}_p$ with algebraically closed residue field k for some prime $p > 0$. Taking a model $\mathscr{X} \hookrightarrow \mathscr{A}$ over the ring of integers R of K, he thus degenerates the situation to positive characteristic. It is essential for Raynaud's method that R is an absolutely unramified discrete valuation ring, and that both $\mathscr{X}$ and $\mathscr{A}$ have *good reduction* at p. A simple argument then shows that the *coprime-to-p* torsion points of A, lying on X, inject into the image of the following intersection:

$$\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}(k)$$

where the map is given by specialisation to characteristic $p > 0$. Thus, it is sufficient to find a bound on the cardinality of this image. First, he verifies that the above image is indeed a finite set. When $\mathscr{A}$ has *good ordinary reduction*, this can be done by studying lifts of the Frobenius morphism on smooth curves in positive characteristic. Then, assuming finiteness, he describes a bound on the cardinality which is expressible in terms of an intersection number on the special fibre $\mathscr{A}_k$ when A has dimension 2. It is a non-trivial problem to extract tractable bounds from Raynaud's approach. We do this in the case where X is the preimage of the diagonal $(\pi_1 \times \pi_2)^{-1}(\Delta_{\mathbb{P}^1})$ embedded in the product of two elliptic curves $E_1 \times E_2$ to obtain the following realistic bounds on the number of common projective coprime-to-p torsion of pairs of elliptic curves in Theorem 5.1.8:

Theorem. *Let (E_i, π_i), $i = 1, 2$, be a pair of elliptic curves equipped with standard double covers $\pi_i : E_i \to \mathbb{P}^1$ defined over a number field L. Fix a place v of L lying over a prime $p > 2$ for which:*

i) v is unramified over p;

ii) E_1 and E_2 have good reduction at v;

iii) The scheme of common branch loci $\pi_1(E_1[2])) \cap \pi_2(E_2[2]))$ has rank < 4, and the rank remains constant after specialisation mod v.

Given the assumptions above, one obtains the following bound on the number of common projective torsion points of E_1 and E_2 of order coprime-to-p:

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})\right| \leq 2p^3 + 8.$$

Moreover, we show that this bound can be sharpened in a number of cases in Corollary 5.1.9. Combining this bound with information on the action of the inertia group I_K on the group of *p-primary* torsion points $(E_1 \times E_2)[\infty]^{(p)}$, one is able to extend the above result to a bound on the number of common projective torsion points of *any order*. This is the content of Theorem 5.1.10.

Of course, to show that the above bound is uniform, we need to say something about pairs of elliptic curves E_1 and E_2 with *bad reduction* at the given prime $p > 0$. Indeed, suppose that one or both of the elliptic curves E_i have *bad multiplicative reduction*, then there exists a proper *minimal Weierstrass model* $\mathscr{W}_i \to \mathrm{Spec}(R)$ of E_i. Let $\overline{\mathscr{A}}$ denote the product of the minimal Weierstrass models of E_1 and E_2 and let $\mathscr{A}$ denote the smooth locus over $\mathrm{Spec}(R)$. The main obstruction to extending the bounds obtained to the case of multiplicative reduction is that the special fibre of the proper model $\overline{\mathscr{A}}_k$ is no longer normal, and so one cannot hope to directly obtain the same intersection theoretic bounds in this case. To avoid this, we translate the situation to the smooth relative surface $\mathbb{P}^1_R \times_R \mathbb{P}^1_R$ by working with extensions $\pi_{i,R} : \mathscr{W}_i \to \mathbb{P}^1_R$ of our standard double covers. In this context, we are able to show that the following analogous bounds hold in Corollary 8.1.4:

Theorem. *Let (E_i, π_i), $i = 1, 2$, be a pair of elliptic curves equipped with standard double covers $\pi_i : E_i \to \mathbb{P}^1$ defined over a number field L. Fix a place v of L lying over a prime $p > 2$ for which v is unramified over p. Suppose that E_1 and E_2 have at worst bad multiplicative reduction at v and satisfy Assumption 8.1.2. Then one obtains the following bound on the number of common projective torsion points of E_1 and E_2 of order coprime-to-p:*

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_1(E_1[\infty]^{(p')})\right| \leq 2p^3 + 2.$$

As in the case of good reduction, these bounds are only valid when the image of:

$$\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}(k)$$

under reduction mod p is finite. To show this, the key idea is that many of Raynaud's arguments can be extended to the *log smooth* setting. Indeed, after endowing the minimal Weierstrass models $\mathscr{W}_i$ of E_i and $\mathrm{Spec}(R)$ with appropriate log structures, the models become log smooth. By extending a number of Raynaud's results to the log smooth setting, in particular his Frobenius lifting argument, we are able to show the desired finiteness result under certain mild geometric conditions (cf. Theorem 8.1.7).

Unlikely intersections and uniformity

Bogomolov-Fu-Tschinkel place their problem amongst the *unlikely intersections* of arithmetic geometry. This is an umbrella term for a collection of problems following the same very general set-up, and can be first attributed to Zannier [Zan12]. Let A be a geometric group object (e.g. an affine group variety, abelian variety or even a moduli stack of group schemes). First, we define what it means for a point $a \in A$ to be *special* (e.g. a torsion point). Then, we define what it means for a subspace $X \hookrightarrow A$ to be *special* (e.g. a torsion coset). Finally, we *qualitatively* describe the special subspaces by asserting that:

$$X \hookrightarrow A \text{ is special } \iff X \cap \{\text{special points of } A\} \subseteq X \text{ is Zariski dense.}$$

Consider a smooth curve X embedded in its Jacobian $J_X = A$ over a number field L. Suppose we take L-rational points as our *special* points. Of course the L-rational points of X form a dense subset if and only if they are infinite in number and we arrive at the Mordell conjecture (Falting's theorem [Fal86]). In this case, a curve X is *special* if and only if it is the translate of an elliptic curve of positive rank. If we change the notion of *special* point to mean a geometric torsion point, then we arrive at the Manin-Mumford conjecture. Both of these conjectures were unified into the *Mordell-Lang conjecture* [Lang65]. The first proof of the Mordell-Lang conjecture was given by McQuillan [McQ92].

This idea can be generalised in a number of directions. Replacing the curve $X \hookrightarrow A$ by a higher dimensional subvariety, we can still ask when X is a coset of a subgroup. Replacing A by any *semiabelian variety* B i.e. an extension of an abelian variety A by a torus $\mathbb{G}_m^r$:

$$0 \to \mathbb{G}_m^r \to B \to A \to 0$$

we obtain a generalised Mordell-Lang conjecture which was settled by Vojta [Voj98]. An even further abstraction is given by the André-Oort conjecture where we replace A by a *Shimura variety* $\mathscr{A}$. The definition of $\mathscr{A}$ is rather technical; informally it is a moduli

space of abelian varieties and arises from a quotient of a complex analytic domain by an arithmetic group. The 'special' points of a Shimura variety are so-called *CM points* corresponding to abelian varieties in the moduli space $\mathscr{A}$ with complex multiplication. The André-Oort conjecture attempts to classify the *special Shimura subvarieties* of $\mathscr{A}$ as closures of CM points. A proof was given by Klingler and Yafaev, conditional on the generalised Riemann hypothesis [Kli-Yaf14]. The final ingredients for a full proof were provided by Pila, Shankar and Tsimerman [PST21].

Each of the problems mentioned can be thought of as *qualitative* descriptions of the special subspaces. Conversely, one may ask if there is a *quantitative* description of the non-special subspaces. In the context of Falting's theorem, Mazur conjectured that there exists a constant $c = c(g, d)$ such that, for all smooth, irreducible, projective curves X of genus $g \geq 2$ defined over number fields L of degree d over $\mathbb{Q}$ we have $|X(L)| \leq c$ [Maz86, p. 234]. Coleman's theory of p-adic integration, combined with Chabauty's method gave a new proof Falting's theorem over $\mathbb{Q}$ [Col87], and also an effective bound c in the case where the *Mordell-Weil rank* r (i.e. rank of $J_X(\mathbb{Q})$) satisfies the inequality $r < g$. In more recent work of Katz, Rabinoff, Zureick-Brown [KRZ-B16], the authors were able to show that a constant $c = c(g, d)$ exists depending on g and the degree $d = [L : \mathbb{Q}]$, but again with some (less restrictive) conditions on the Mordell-Weil rank (in this case being 'small').

Mazur conjectured more generally that a 'uniform Mordell-Lang conjecture' should hold. Work of Dimitrov, Gao and Habbegger [DGH21] provide such a statement; improving the results of [KRZ-B16] by allowing any Mordell-Weil rank. Moreover, this gives us a uniform constant $c = c(g)$ such that for all smooth, irreducible, projective curves X of genus $g \geq 2$ defined over $\mathbb{C}$ we have $|X(\mathbb{C}) \cap J_X[\infty]| \leq c$ for any embedding $X \hookrightarrow J_X$ of X into its Jacobian. [DGH21] show the existence of a constant $c = c(g, d)$ when X is defined over a number field L of degree d. The degree hypothesis was removed by additional work of Kühne [Kueh21]. However, it should be noted that the bounds obtained are far from effective and computable and so do not provide the 'realistic' bounds we seek for the Bogomolov-Fu-Tschinkel conjecture.

Lang's problem on curves in the torus and projective equivalence of roots of unity

As a warm-up to our study of Raynaud's proof of the Manin-Mumford conjecture, and its application to the problem on projective torsion points of Bogomolov-Fu-Tschinkel, we consider the following problem of Lang. Given an irreducible curve X in the algebraic 2-torus $\mathbb{G}^2_{m,\mathbb{C}}$, Lang proved that the intersection $X \cap \mathbb{G}^2_{m,\mathbb{C}}[\infty]$ is finite if and only if X is not the translate of a sub-torus (isomorphic to $\mathbb{G}_{m,\mathbb{C}}$) by a pair of roots of unity (ζ_1, ζ_2) [Lang13]. This can be understood as the affine analogue of the Manin-Mumford conjecture. Indeed,

the proof is thematically similar, as it require some information of the Galois action on torsion points and an argument coming from intersection theory in the ambient space $\mathbb{G}^2_{m,\mathbb{C}}$.

As with the other unlikely intersections problems, one can ask if there is a uniformity statement. Namely, if one considers curves of a fixed degree $d > 0$ (by embedding $\mathbb{G}^2_{m,\mathbb{C}}$ in $\mathbb{P}^2_{\mathbb{C}}$), then is there a uniform constant c such that $|X \cap \mathbb{G}^2_{m,\mathbb{C}}[\infty]| \leq c$ for all non-special curves X of degree $d > 0$? A positive, and almost-optimal answer to this question was given by Beukers-Smyth [Beu-Smy02].

Again, drawing the analogy between the Manin-Mumford conjecture and Lang's problem, one can also ask the analogue of the Bogomolov-Fu-Tschinkel conjecture in the affine case. Namely, given two projective automorphisms $\gamma_1, \gamma_2 \in \mathrm{PGL}(2, \mathbb{C})$, when is the intersection $\gamma_1(\mu_\infty) \cap \gamma_2(\mu_\infty)$ finite? Moreover, among the pairs γ_1, γ_2 for which this intersection is finite, can one give a bound on the size of this intersection? An answer to this question was given by Fu [Fu22], where he was able to show that this intersection contains at most 14 points when it is finite, and he calculates the possibilities for this maximal intersection up to projective equivalence. Applying the methods of Beukers-Smyth we are able to provide a simple and conceptual proof of the following (slightly weaker) uniform bound in Corollary 2.1.3:

Theorem. *Let $\mu_\infty \subseteq \mathbb{P}^1_{\mathbb{C}}$ denote (an embedding of) the set of all roots of unity. Suppose that γ_1, γ_2 are projective automorphisms such that $\gamma_1(\mu_\infty) \cap \gamma_2(\mu_\infty)$ is a finite set. Then the following uniform bound holds:*

$$|\gamma_1(\mu_\infty) \cap \gamma_2(\mu_\infty)| \leq 18.$$

Structure of this thesis

This thesis is separated into three parts. In Part I, we discuss Lang's problem on torsion points lying on curves embedded in the 2-torus, the uniformity result of Beukers-Smyth and our simplified proof of Fu's result. In Part II, we develop the necessary background to describe Raynaud's proof of the Manin-Mumford conjecture in the most general setting. In Section 3.1, we state some basic properties of local fields and introduce the Witt vectors which will play an important role throughout.

In Section 3.2, we recall the basic properties of abelian varieties and how these notions behave in families by working with abelian schemes. We also study finite flat group schemes over discrete valuation rings and introduce the notions of Cartier duality and the connected-étale sequence with a view of studying the torsion subgroup schemes of abelian schemes.

We then study the p-divisible groups and formal groups associated to an abelian scheme in Section 3.3. These will turn out to be more refined invariants and play an

important role in the theory of Serre-Tate moduli in Section 3.6. In Section 3.4, we study curves in positive characteristic. Most notably, we discuss the nature of inseparable coverings and the Cartier operator which are unique to characteristic $p > 0$ geometry.

In Section 3.5, we introduce some classical results from deformation theory, paying particular attention to what happens in the mixed characteristic setting. In Section 3.7, we study the Galois representations of elliptic curves with good reduction. In particular, we want to use the Galois theory of local fields to give concrete descriptions of the images of inertia on the p-primary torsion of elliptic curves.

In the remainder of Part II, we detail Raynaud's proof of the Manin-Mumford conjecture. This can broadly be split into three parts:

i) We show that the image of the intersection $\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}(k)$ is *finite* by studying the normal bundle of $\mathscr{X}_k$ in $\mathscr{A}$ in Prop. 4.1.14.

ii) Assuming finiteness, we then provide a bound on the cardinality of this image in Cor. 4.1.16.

iii) We then extend this bound to a bound on the number of torsion points of an abelian variety A of *any* order that lies on an embedded curve X by studying the inertia action on p-primary torsion in Prop. 4.1.34.

Finally, returning to the setting of Bogomolov-Fu-Tschinkel, we calculate what bounds can be obtained for the number of common projective torsion points of elliptic curves with good reduction at a given prime $p > 0$ using Raynaud's method. This is the content of Thm. 5.1.8 and Thm. 5.1.10.

In Part III, we describe generalisations of the results in Part II to the semistable setting. In Section 6.1, we discuss Néron models $\mathscr{E}/R$ of elliptic curves E/K. In the semistable setting, $\mathscr{E}/R$ will not in general be an abelian scheme but a non-proper R-group scheme. Using the Tate uniformisations of elliptic curves with multiplicative reduction, we are able to study their associated torsion group schemes and inertia representations as in Part I. We then discuss the Semistable Reduction Theorem and Grothendieck's Semistability Criterion in Section 6.2. This generalises the Néron-Ogg-Shafarevich criterion, and is crucial to understanding how Raynaud's proof should extend to the semistable case.

The final piece of background we discuss is in Section 7.1 on the relevant facts used from logarithmic geometry for the results in Section 8.1. Furnishing the semistable models constructed in Section 6.1 with appropriate log structures, we show that they are *log smooth* and are able to extend many of Raynaud's results to the semistable case using this fact. Finally, we show that one may obtain analogous bounds on the number of common coprime-to-p torsion points of pairs of elliptic curves with at worst multiplicative reduction at a given prime $p > 0$ in Cor. 8.1.4.

Part I

Lang's problem on torsion points of curves in the torus and projective equivalence of roots of unity

Chapter 1

Torsion points on curves in the torus

1.1 A problem of Lang

Let $f \in \mathbb{C}[x,y]$ be an irreducible polynomial and let $\mu_\infty = \{\zeta \in \mathbb{C} \mid \zeta^n = 1 \text{ for some } n > 0\}$ denote the set of all roots of unity. In [Lang13], Lang posed the following problem. When is the set:

$$\{(\zeta_1, \zeta_2) \in \mu_\infty \times \mu_\infty \mid f(\zeta_1, \zeta_2) = 0\}$$

finite? As $\mu_\infty \subseteq \mathbb{G}_{m,\mathbb{C}}$, one may ask the same question for any Laurent polynomial $f \in \mathbb{C}[x, x^{-1}, y, y^{-1}]$. Setting $X = \{f = 0\} \subseteq \mathbb{G}^2_{m,\mathbb{C}}$, we may equivalently ask when the set:

$$X \cap \mathbb{G}^2_{m,\mathbb{C}}[\infty]$$

of torsion points of the algebraic 2-torus lying on X is finite. One may consider the above the *affine* analogue of the Manin-Mumford conjecture for curves in abelian surfaces. Recall that any 1-dimensional, connected subgroup of the 2-torus is a copy of $\mathbb{G}_{m,\mathbb{C}}$ embedded as a Laurent polynomial:

$$\mathbb{G}_{m,\mathbb{C}} \cong \{x^m y^n - 1 = 0\} \subseteq \mathbb{G}^2_{m,\mathbb{C}}$$

where $m, n \in \mathbb{Z}$ are coprime. Given a point $(a,b) \in \mathbb{G}^2_{m,\mathbb{C}}$ and a curve $X \subseteq \mathbb{G}^2_{m,\mathbb{C}}$, we define the *translate of* X *by* (a,b) to be the curve:

$$(a,b) \cdot X = \{(ax, by) \in \mathbb{G}^2_{m,\mathbb{C}} \mid (x,y) \in X\}.$$

If $X = \{f(x,y) = 0\}$, then $(a,b) \cdot X$ is the vanishing locus of the polynomial $f(a^{-1}x, b^{-1}y)$.

Definition 1.1.1. We say that a curve in the $X \subseteq \mathbb{G}^2_{m,\mathbb{C}}$ is a *torsion coset* if there is a 1-dimensional, connected subgroup $H \leq \mathbb{G}^2_{m,\mathbb{C}}$ and a pair of roots of unity $(\zeta_1, \zeta_2) \in \mu^2_\infty$ such that:

$$X = (\zeta_1, \zeta_2) \cdot H.$$

It is clear that, for any torsion coset X, the intersection $X \cap \mu^2_\infty$ is infinite. However,

the converse also holds:

Theorem 1.1.2. *Let $X \subseteq \mathbb{G}_{m,\mathbb{C}}^2$ be an irreducible curve. Then the intersection:*

$$X \cap \mathbb{G}_{m,\mathbb{C}}[\infty]^2$$

is infinite if and only if X is a torsion coset.

Proof. See [Lang13, Ch. 8, Theorem 6.1]. □

Let $\mathbb{Q}^{\mathrm{ab}}$ denote the maximal abelian extension of $\mathbb{Q}$; i.e. the union of all finite Galois extensions $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is abelian. This can be constructed by adjoining μ_∞ to $\mathbb{Q}$. Suppose that $X = \{f = 0\}$ is irreducible and, without loss of generality, assume that one of the coefficients is 1. Let K be the field obtained by adjoining the coefficients of f to $\mathbb{Q}^{\mathrm{ab}}$. Then, if $K \supsetneq \mathbb{Q}^{\mathrm{ab}}$, there exists some conjugate $\sigma : K \hookrightarrow \mathbb{C}$ such that $f^\sigma \neq f$, but $\sigma|_{\mathbb{Q}^{\mathrm{ab}}} = \mathrm{Id}_{\mathbb{Q}^{\mathrm{ab}}}$. This means that the irreducible curve $X^\sigma = \{f^\sigma = 0\}$ contains the intersection $X \cap \mathbb{G}_{m,\mathbb{C}}[\infty]^2$ and so:

$$X \cap \mathbb{G}_{m,\mathbb{C}}[\infty]^2 \subseteq X \cap X^\sigma.$$

As we normalised the coefficients of f, the curves X and X^σ are distinct and so by Bézout's theorem, this is a finite set, and so the problem of Lang only becomes interesting when we work over the algebraic extension $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$. Indeed, Lang's proof has two essential components, he studies the Galois theory of finite Kummer extensions and how this interplays with the intersection theory on the 2-torus coming from Bézout's theorem. We will see that the Manin-Mumford conjecture has a similar proof in spirit. Namely, the torsion points on an abelian variety are understood by their Galois action, and some type of intersection theory is required to prove the desired finiteness result.

1.2 Uniformity and roots of unity on curves in the torus

As with the Manin-Mumford conjecture, or the problem of Bogomolov-Fu-Tschinkel, one can ask whether there is a *uniform* version of Lang's problem. In general, when one's attention is restricted to irreducible curves X that are not torsion cosets, the size of the intersection $X \cap \mathbb{G}_{m,\mathbb{C}}[\infty]^2$ grows with the degree of X. Thus, it is an interesting question to ask whether the size of this intersection is *uniformly bounded* amongst curves of bounded degree. An affirmative answer was given by Beukers and Smyth [Beu-Smy02]. Given a Laurent polynomial $f = \sum_{i,j} a_{ij} x^i y^j$ one defines the *Newton polytope* to be:

$$\mathrm{Newt}(f) = \mathrm{Conv}(\{(i,j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}) \subseteq \mathbb{R}^2.$$

We let $\mathrm{Vol}(f)$ denote the area of the Newton polytope of f. Note that, if $f \in \mathbb{C}[x,y]$ has degree d, then $\mathrm{Newt}(f)$ is contained in the triangle with vertices $(0,0)$, $(d,0)$ and $(0,d)$, and so $\mathrm{Vol}(f) \leq \frac{1}{2}d^2$.

Theorem 1.2.1. *Let $f(x,y)$ be an irreducible Laurent polynomial, and let $X = \{f = 0\} \subseteq \mathbb{G}^2_{m,\mathbb{C}}$ denote the corresponding curve. If X is not a torsion coset, then we have that:*

$$|X \cap \mathbb{G}^2_{m,\mathbb{C}}| \leq 22\mathrm{Vol}(f).$$

We now illustrate the method of Beukers-Smyth. A crucial ingredient is the intersection theory on the 2-torus coming from mixed volumes. We first note the following invariants associated to a Laurent polynomial defined using convex geometry:

Definition 1.2.2. Let $g = \sum_{(i,j)\in\mathbb{Z}^2} a_{ij}x^iy^j$ be a Laurent polynomial.

i) The *support* of g is the set of lattice points:

$$\mathrm{Supp}(g) = \{(i,j) \in \mathbb{Z}^2 \mid a_{ij} \neq 0\}.$$

ii) The *lattice* associated to g is the abelian group generated by the set of differences:

$$\mathcal{L}(g) = \big\langle (i,j) - (i',j') \mid (i,j),(i',j') \in \mathrm{Supp}(g) \big\rangle.$$

iii) The rank of $\mathcal{L}(g)$ is either 1 or 2. When the rank is 2, we say $\mathcal{L}(g)$ is *full* if it generates $\mathbb{Z}^2$.

Note that the Newton polytope of g is the convex hull of its support. The following can be considered a 'toric' analogue of Bézout's theorem:

Lemma 1.2.3. *Suppose $f(x,y)$ and $g(x,y)$ are Laurent polynomials over $\mathbb{C}$ such that $X = \{f = 0\}$ and $Y = \{g = 0\}$ have no common component. Then:*

$$|X \cap Y| \leq \mathrm{Vol}(\mathrm{Newt}(f) + \mathrm{Newt}(g)) - \mathrm{Vol}(f) - \mathrm{Vol}(g).$$

Proof. See [Ful93, p. 122]. □

We now rule out certain degenerate cases based on the above definitions. Fix a Laurent polynomial f and write X for the associated curve. Suppose first that $\mathcal{L}(f)$ has rank 1. Then one can write $f(x,y) = g(x^ay^b)$ for some monomial x^ay^b, and some polynomial $g \in \mathbb{C}[z,z^{-1}]$. If g has a solution $g(\zeta) = 0$ for a root of unity $\zeta \in \mu_\infty$, then there are an infinite number of solutions $x^ay^b = \zeta$ and X is a torsion coset. On the other

hand, if g has no solutions in μ_∞ then $X \cap \mu_\infty^2 = \emptyset$. Again, if f is not defined over $\mathbb{Q}^{\mathrm{ab}}$, then there is some conjugate σ such that:

$$X \cap \mu_\infty^2 \subseteq X \cap X^\sigma.$$

By the toric Bézout theorem, this intersection is bounded by:

$$\mathrm{Vol}(\mathrm{Newt}(f) + \mathrm{Newt}(f^\sigma)) - \mathrm{Vol}(f) - \mathrm{Vol}(f^\sigma) = 2\mathrm{Vol}(f).$$

Based on this discussion, we make the following assumptions:

Assumption 1.2.4. *Let $f \in \mathbb{C}[x, x^{-1}, y, y^{-1}]$ be irreducible and write $X = \{f = 0\} \subseteq \mathbb{G}_{m,\mathbb{C}}^2$ denote the associated curve. We assume the following:*

i) After rescaling so that 1 is a coefficient of f, f is defined over $\mathbb{Q}^{\mathrm{ab}}$.

ii) The associated lattice $\mathcal{L}(f)$ is full.

We now illustrate the general method of Beukers-Smyth to bound the size of the intersection $X \cap \mu_\infty^2$ for a curve $X = \{f = 0\}$ satisfying Assumption 1.2.4. Note that, there is some ζ_N of order $N > 0$ such that X is defined over $\mathbb{Q}(\zeta_N)$. For ease of exposition, we will assume that $N = 1$, with the general case working similarly with some extra information about the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ (see for example [Beu-Smy02, p. 5]). Consider the following collection of polynomials:

$$\begin{aligned}
f_1(x, y) &= f(x, -y), \\
f_2(x, y) &= f(-x, y), \\
f_3(x, y) &= f(-x, -y), \\
f_4(x, y) &= f(x^2, y^2), \\
f_5(x, y) &= f(x^2, -y^2), \\
f_6(x, y) &= f(-x^2, y^2), \\
f_7(x, y) &= f(-x^2, -y^2)
\end{aligned}$$

and let $X_i = \{f_i = 0\}$ for $i = 1, ..., 7$. We claim that, with our assumptions on f, X has no common component with X_i (i.e. f and f_i are coprime), and if $(\zeta, \zeta') \in X \cap \mu_\infty^2$, then $(\zeta, \zeta') \in X_i$ for some i. Assuming this, we would have:

$$|X \cap \mu_\infty^2| \leq \sum_{i=1}^{7} |X \cap X_i|.$$

To prove the second point we use the following elementary lemma:

Lemma 1.2.5. *Suppose ζ_N is a primitive N-th root of unity. Then it is Galois conjugate to one of:*

$$\begin{aligned} -\zeta_N &\quad \text{if} \quad N \equiv 0 \pmod 4, \\ -\zeta_N^2 &\quad \text{if} \quad N \equiv 2 \pmod 4, \\ \zeta_N^2 &\quad \text{if} \quad N \text{ odd}. \end{aligned}$$

Proof. We have that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$. Moreover, an integer a is a unit modulo N if and only if $\gcd(a, N) = 1$ and so the last statement is clear. So suppose that N is even and write $N = 2M$. Then $-1 = \zeta_N^M$. If M is even then $\gcd(M+1, 2M) = \gcd(M+1, 2) = 1$ and so the first statement follows. Similarly, if M is odd then $\gcd(M+2, 2M) = \gcd(M+2, 2) = 1$, thus the second statement. □

If (ζ, ζ') are roots of unity on X, then for some $a, b, N > 0$ we can write:

$$(\zeta, \zeta') = (\zeta_N^a, \zeta_N^b).$$

Then, by the above, there exists an automorphism $\sigma : \mathbb{Q}(\zeta_N) \to \mathbb{Q}(\zeta_N)$ sending:

$$\zeta_N \mapsto -\zeta_N, \zeta_N^2 \quad \text{or} \quad -\zeta_N^2,$$

and therefore $\sigma(f(\zeta_N^a, \zeta_N^b)) = f_i(\zeta_N^a, \zeta_N^b) = 0$ for at least one i.

To show that X has no common component with X_i we note, for $i = 1, 2, 3$, that $f \mid f_i$ would imply $\mathcal{L}(f)$ is of rank 1. For example, if $f \mid f_1$ then $f = f_1$ and $f(x, y) = g(x, y^2)$ for some Laurent polynomial g and $\mathcal{L}(f)$ is not full. So assuming that f, f_1, f_2, f_3 have no common factors, if $f | f_4$ then similarly $f f_1 f_2 f_3 | f_4$ which is a contradiction by considering degrees. A similar argument shows that $f \nmid f_i$ for $i = 5, 6, 7$.

We have that $\mathrm{Vol}(f_i) = \mathrm{Vol}(f)$ for $i = 1, 2, 3$ and $\mathrm{Vol}(f_i) = 4\mathrm{Vol}(f)$ for $i = 4, 5, 6, 7$. Applying the toric Bézout theorem, we obtain the bound of:

$$|X \cap \mu_\infty^2| \leq \sum_{i=1}^{7} |X \cap X_i| \leq 22\mathrm{Vol}(f).$$

Remark 1.2.6. Suppose that f is a Laurent polynomial such that $\mathcal{L}(f)$ is not full, but has rank 2. Then there is an integer valued basis $(a, c), (b, d)$ of $\mathbb{R}^2$ such that:

$$\mathcal{L}(f) = \mathbb{Z} \cdot (a, c) \oplus \mathbb{Z} \cdot (b, d).$$

Then, after potentially re-ordering the basis, the index of $\mathcal{L}(f)$ in $\mathbb{Z}^2$ is given by the

determinant:

$$\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc.$$

Thus, there exists some Laurent polynomial g with $\mathcal{L}(g)$ full such that:

$$g(x^a y^c, x^b y^d) = f(x, y).$$

On one hand, the toric morphism:

$$\begin{aligned} \mathbb{G}_{m,\mathbb{C}}^2 &\longrightarrow \mathbb{G}_{m,\mathbb{C}}^2; \\ (x, y) &\longmapsto (x^a y^c, x^b y^d) \end{aligned}$$

is degree $ad - bc$, and sends pairs of roots of unity to pairs of roots unity. On the other hand, we have the equality:

$$\mathrm{Vol}(f) = |ad - bc|\mathrm{Vol}(g)$$

so we may assume without loss of generality that all lattices are full.

For the general case, when f is minimally defined over some field $\mathbb{Q}(\zeta_N)$, we refer to [Beu-Smy02, 3.4]. Indeed, there is a case-by-case analysis depending on the residue of N mod 4 that provides a similar collection of curves X_i sharing no common component with X, and that contain all pairs of roots of unity lying on X. In each case, one obtains at worst the bound $22\mathrm{Vol}(f)$.

Chapter 2

Projective equivalence and roots of unity

2.1 Projective equivalence and roots of unity

Recall that the projective automorphisms of $\mathbb{P}^1_{\mathbb{C}}$ are given by the Möbius transformations:

$$\mathrm{PGL}_2(\mathbb{C}) \cong \left\{ \gamma(z) = \frac{az+b}{cz+d} \mid ad - bc \neq 0 \right\}.$$

We say that two subsets $S, S' \subseteq \mathbb{P}^1_{\mathbb{C}}$ are *projectively equivalent* if $\gamma(S) = S'$ for some projective automorphism γ. If $S, S' \subseteq \mu_\infty$, we say that S and S' are *trivially equivalent* if $\gamma(S) = S'$ only when $\gamma(\mu_\infty) = \mu_\infty$. In [Fu22], Fu proves the following:

Theorem 2.1.1. *Suppose that $S, S' \subseteq \mu_\infty$ are non-trivially, projectively equivalent. Then:*

$$|S| = |S'| \leq 14.$$

Moreover, modulo projective equivalence, there are two distinct possibilities S_1, S_2 for which $|S_i| = 14$:

i)

$$S_1 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^9, \zeta^{11}, \zeta^{14}, \zeta^{18}, \zeta^{22}, \zeta^{25}, \zeta^{27}\},$$

where ζ is a primitive 30-th root of unity;

ii)

$$S_2 = \{1, \omega, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{12}, \omega^{22}, \omega^{31}, \omega^{40}, \omega^{50}, \omega^{54}, \omega^{56}, \omega^{58}\},$$

where ω is a primitive 60-th root of unity;

Fu's method is algorithmic in nature, however does provide explicitly the sharpest bounds, and computes the maximal examples.

Remark 2.1.2. The torsion subgroup $\mathbb{G}_{m,\mathbb{C}}[\infty]$ is given by μ_∞. To view the torsion subgroup in $\mathbb{P}^1_{\mathbb{C}}$, we make a choice of embedding $\mathbb{G}_{m,\mathbb{C}} \hookrightarrow \mathbb{P}^1_{\mathbb{C}}$ i.e. a choice of homogeneous coordinates:

$$\begin{aligned} \mathbb{G}_{m,\mathbb{C}} &\longrightarrow \mathbb{P}^1_{\mathbb{C}}; \\ z &\longmapsto [1:z]. \end{aligned}$$

Any such embedding is unique up to a projective automorphism of $\mathbb{P}^1_{\mathbb{C}}$ (i.e. a change of coordinates).

In view of this remark, we reframe Fu's result as follows: Let $\iota_j : \mathbb{G}_{m,\mathbb{C}} \hookrightarrow \mathbb{P}^1$ $(j = 1, 2)$ be two embeddings as above. Then there exists a uniform bound on the number of common torsion points:

$$\iota_1(\mathbb{G}_{m,\mathbb{C}}[\infty]) \cap \iota_2(\mathbb{G}_{m,\mathbb{C}}[\infty]),$$

as long as the intersection is not infinite. In this way, Fu's theorem is the analogue of the Bogomolov-Fu-Tschinkel conjecture where we replace pairs of elliptic curves with standard double covers with pairs of embeddings of the 1-torus in $\mathbb{P}^1_{\mathbb{C}}$.

By complete analogy, one may bound the number of common roots of unity of two projective embeddings by studying the diagonal $\Delta_{\mathbb{P}^1} \subseteq \mathbb{P}^1 \times \mathbb{P}^1$. Using homogeneous coordinates $([x_0 : x_1], [y_0 : y_1])$, the diagonal is given by $\Delta_{\mathbb{P}^1} = \{g = 0\}$ where:

$$g = x_0 y_1 - x_1 y_0.$$

Write $\gamma(x_0, x_1) = [ax_0 + bx_1 : cx_0 + dx_1]$ for a Möbius map γ and let:

$$f = (ax_0 + bx_1)y_1 - (cx_0 + dx_1)y_0.$$

Then the curve $X = \{f = 0\}$ fits into the following Cartesian diagram:

$$\begin{array}{ccc} X & \hookrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow & & \downarrow{\scriptstyle \gamma \times \mathrm{Id}} \\ \Delta_{\mathbb{P}^1} & \hookrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \end{array}$$

where the vertical arrows are isomorphisms. Then, to bound the intersection $\gamma(\mu_\infty) \cap \mu_\infty$, it is equivalent to bound the intersection:

$$X \cap \mu_\infty^2.$$

From this perspective, one may directly apply the results of Beukers-Smyth. Firstly, we

note that X is a torsion coset if and only if $\gamma \in H \leq \mathrm{PGL}_2(\mathbb{C})$ where:

$$H = \left\langle \zeta x, \frac{1}{x} \mid \zeta \in \mu_\infty \right\rangle.$$

As the method dictates, we consider the following collection of polynomials:

$$\begin{aligned}
f_1(x,y) &= f(x,-y) = (ax+b)+(cx+d)y,\\
f_2(x,y) &= f(-x,y) = (-ax+b)-(-cx+d)y,\\
f_3(x,y) &= f(-x,-y) = (-ax+b)+(-cx+d)y,\\
f_4(x,y) &= f(x^2,y^2) = (ax^2+b)-(cx^2+d)y^2,\\
f_5(x,y) &= f(x^2,-y^2) = (ax^2+b)+(cx^2+d)y^2,\\
f_6(x,y) &= f(-x^2,y^2) = (-ax^2+b)-(-cx^2+d)y^2,\\
f_7(x,y) &= f(-x^2,-y^2) = (-ax^2+b)+(-cx^2+d)y^2.
\end{aligned}$$

Noting that, the curves X and X_i have no common intersection in $\mathbb{G}_m^2$ for $i = 1, 2$, and that $\mathrm{Vol}(f) = 1$, we obtain the following as a corollary of Theorem 1.2.1:

Corollary 2.1.3. *Let $\gamma \in \mathrm{Möb}(\mathbb{C}) \setminus H$. Then we have the following uniform bound:*

$$|X \cap \mu_\infty^2| \leq 18,$$

where $X = (\gamma \times \mathrm{Id})^{-1}(\Delta_{\mathbb{P}^1})$. Moreover, if $\gamma \in H$ then $X \cap \mu_\infty^2$ is infinite.

This is not a sharp bound unlike the result of Fu, however, the proof of the above is considerably shorter than Fu's calculations.

2.2 Maximal examples

In the maximal examples of Fu, where the largest possible intersection of 14 points is attained, we can describe precisely how the method of Beukers-Smyth fails to be sharp:

Example 2.2.1. Let ζ be a primitive 30-th root of unity. We consider the matrix:

$$\gamma_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -\zeta^7 - \zeta^6 + \zeta^2 & \zeta^7 - \zeta^2 \\ 1 & -\zeta^6 - 1 \end{bmatrix}.$$

Note that, in $\mathbb{Q}(\zeta)$ we have the identity:

$$\zeta^9 = -\zeta^7 - \zeta^6 + \zeta^3 + \zeta^2 - 1,$$

thus we can write:

$$\gamma_1 = \begin{bmatrix} \zeta^9 - \zeta^6 - \zeta^3 + 1 & -\zeta^9 - \zeta^6 + \zeta^3 - 1 \\ 1 & -\zeta^6 - 1 \end{bmatrix}.$$

Writing $\xi = -\zeta^3$ (a primitve 5-th root), then A is defined over $\mathbb{Q}(\xi)$:

$$\gamma_1 = \begin{bmatrix} -\xi^3 - \xi^2 + \xi + 1 & \xi^3 - \xi^2 - \xi - 1 \\ 1 & -\xi^2 - 1 \end{bmatrix}.$$

Correspondingly we have the polynomial:

$$f(x, y) = (-\xi^3 - \xi^2 + \xi + 1)x + \xi^3 - \xi^2 - \xi - 1 - xy + (\xi^2 + 1)y.$$

Interpreting the calculations in [Fu22], one can check that the curve $X = \{f = 0\}$ contains the following pairs of roots of unity:

$$\begin{aligned} X \cap \mu_\infty^2 =& \{(1,1), (\zeta, \zeta^2), (\zeta^2, \zeta^5), (\zeta^3, \zeta^9), (\zeta^4, \zeta^{13}), (\zeta^5, \zeta^{16}), (\zeta^6, \zeta^{18}), (\zeta^9, \zeta^{21}), \\ & (\zeta^{11}, \zeta^{22}), (\zeta^{14}, \zeta^{23}), (\zeta^{18}, \zeta^{24}), (\zeta^{22}, \zeta^{25}), (\zeta^{25}, \zeta^{26}), (\zeta^{27}, \zeta^{27})\} \\ =& \{(z, \gamma_1(z)) \mid z \in S_1\}. \end{aligned}$$

Again, we consider a selection of polynomials:

$$\begin{aligned} f_1(x, y) &= f(x, -y), \\ f_2(x, y) &= f(-x, y), \\ f_3(x, y) &= f(-x, -y), \\ f_4(x, y) &= f^\sigma(x^2, y^2), \\ f_5(x, y) &= f^\sigma(x^2, -y^2), \\ f_6(x, y) &= f^\sigma(-x^2, y^2), \\ f_7(x, y) &= f^\sigma(-x^2, -y^2); \end{aligned}$$

where σ is given by $\xi \mapsto \xi^2$. Then, one may compute where the roots of unity that lie on

X are distributed amongst the curves $X_i = \{f_i = 0\} \subseteq (\mathbb{Q}(\xi)^*)^2$:

$$\begin{aligned}
&X \cap X_1 = \emptyset,\\
&X \cap X_2 = \emptyset,\\
&X \cap X_3 = \{(\zeta^3, \zeta^9), (\zeta^{18}, \zeta^{24})\},\\
&X \cap X_4 = \{(1,1), (\zeta^3, \zeta^9), (\zeta^6, \zeta^{18}), (\zeta^{18}, \zeta^{24})\},\\
&X \cap X_5 = \{(\zeta^2, \zeta^5), (\zeta^4, \zeta^{13}), (\zeta^{14}, \zeta^{23}), (\zeta^{22}, \zeta^{25})\},\\
&X \cap X_6 = \{(\zeta, \zeta^2), (\zeta^5, \zeta^{16}), (\zeta^{11}, \zeta^{22}), (\zeta^{25}, \zeta^{26})\},\\
&X \cap X_7 = \{(\zeta^3, \zeta^9), (\zeta^9, \zeta^{21}), (\zeta^{18}, \zeta^{24}), (\zeta^{27}, \zeta^{27})\}.
\end{aligned}$$

Note that the 18 points in the above intersections overcount the number of roots of unity precisely by the pairs $(\zeta^3, \zeta^9), (\zeta^{18}, \zeta^{24})$ appearing on X_3, X_4 and X_7.

Example 2.2.2. Let ω be a primitive 60-th root of unity. We consider the matrix:

$$\gamma_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -\omega^{14} - \omega^{12} - \omega^{10} + \omega^4 + \omega^2 + 1 & \omega^{14} + \omega^{12} + \omega^{10} - \omega^6 - \omega^4 - \omega^2 \\ \omega^{12} + \omega^{10} + \omega^8 - \omega^2 & -\omega^{12} - \omega^{10} - \omega^8 - \omega^6 + \omega^2 + 1 \end{bmatrix}.$$

Again, this matrix is defined over a subfield $\mathbb{Q}(\eta)$ where $\eta^2 = -\omega$ is a primitive 15-th root of unity:

$$\gamma_2 = \begin{bmatrix} \eta^7 + \eta^6 + \eta^5 - \eta^2 - \eta + 1 & -\eta^7 - \eta^6 - \eta^5 + \eta^3 + \eta^2 + \eta \\ -\eta^6 - \eta^5 - \eta^4 + \eta & \eta^6 + \eta^5 + \eta^4 + \eta^3 - \eta + 1 \end{bmatrix}.$$

Correspondingly, we have a polynomial:

$$\begin{aligned}
g(x,y) =& (\eta^7 + \eta^6 + \eta^5 - \eta^2 - \eta + 1)x - \eta^7 - \eta^6 - \eta^5 + \eta^3 + \eta^2 + \eta\\
&+ (\eta^6 + \eta^5 + \eta^4 - \eta)xy - (\eta^6 + \eta^5 + \eta^4 + \eta^3 - \eta + 1)y.
\end{aligned}$$

Again, using the results of [Fu22], one can check that the curve $Y = \{g = 0\}$ contains the following pairs of roots of unity:

$$\begin{aligned}
Y \cap \mu_\infty^2 =& \{(1,1), (\omega, \omega^9), (\omega^2, \omega^{18}), (\omega^4, \omega^{28}), (\omega^6, \omega^{32}), (\omega^8, \omega^{34}), (\omega^{12}, \omega^{36}),\\
&(\omega^{22}, \omega^{38}), (\omega^{31}, \omega^{39}), (\omega^{40}, \omega^{40}, (\omega^{50}, \omega^{42}), (\omega^{54}, \omega^{44}), (\omega^{56}, \omega^{46}), (\omega^{58}, \omega^{50})\}\\
=& \{(z, \gamma_2(z)) \mid z \in S_2\}.
\end{aligned}$$

We now have a selection of polynomials:

$$\begin{aligned}
g_1(x,y) &= g(x,-y),\\
g_2(x,y) &= g(-x,y),\\
g_3(x,y) &= g(-x,-y),\\
g_4(x,y) &= g^\tau(x^2,y^2),\\
g_5(x,y) &= g^\tau(x^2,-y^2),\\
g_6(x,y) &= g^\tau(-x^2,y^2),\\
g_7(x,y) &= g^\tau(-x^2,-y^2);
\end{aligned}$$

where τ is given by $\eta \mapsto \eta^2$. Again, one computes where the roots of unity on Y are distributed among the curves $Y_i = \{g_i = 0\} \subseteq (\mathbb{Q}(\omega)^*)^2$:

$$\begin{aligned}
Y \cap Y_1 &= \emptyset,\\
Y \cap Y_2 &= \emptyset,\\
Y \cap Y_3 &= \{(\omega,\omega^9),(\omega^{31},\omega^{39})\},\\
Y \cap Y_4 &= \{(1,1),(\omega^{40},\omega^{40}),(\omega^{12},\omega^{36}),(\omega^4,\omega^{28})\},\\
Y \cap Y_5 &= \{(\omega^8,\omega^{34}),(\omega^{56},\omega^{46})\},\\
Y \cap Y_6 &= \{(\omega^6,\omega^{32}),(\omega^{54},\omega^{44})\},\\
Y \cap Y_7 &= \{(\omega^{22},\omega^{38}),(\omega^{50},\omega^{42}),(\omega^2,\omega^{18}),(\omega^{58},\omega^{50})\}.
\end{aligned}$$

In contrast to Example 2.2.1, the above intersections consist of exactly 14 points in $(\mathbb{Q}(\omega)^*)^2$. However, the curves Y_5 and Y_6 both intersect Y in $(\mathbb{C}^*)^2$ in two additional points which are not pairs of roots of unity.

Part II

The case of good reduction

Chapter 3

Preliminaries

3.1 Local fields

3.1.1 Background on local fields

Here we discuss some background on local fields. In particular, we develop the basic Galois theory required to describe the local Galois representations attached to elliptic curves in Section 3.7. Our main reference will be [Ser13].

Completion of a ring

Let R be a commutative ring and I an ideal. Consider the inverse system:

$$... \to R/I^2 \to R/I,$$

given by projection. The inverse limit $\varprojlim R/I^n =: \hat{R}$ is called the *(I-adic) completion of R*. For each n, the natural map $R \to R/I^n$ induces a ring extension $R \to \hat{R}$ by the universal property. Alternatively phrased, one may define the *Krull topology* on R by declaring $\{I^n\}$ as a basis of open neighbourhoods of $0 \in R$. The I-adic completion $\hat{R}$ is then simply the completion of R with respect to the Krull topology.

Example 3.1.1. i) Let $p > 0$ be a prime. The p-adic integers $\mathbb{Z}_p$ are the completion of $\mathbb{Z}$ with respect to $\langle p \rangle$.

ii) Let R be a noetherian ring. The completion of $R[t_1, ..., t_n]$ with respect to $I = \langle t_1, ..., t_n \rangle$ is the ring of formal power series $R[\![t_1, ..., t_n]\!]$.

Definition 3.1.2. Let R be a principal ideal domain. We say that R is a *discrete valuation ring* (DVR) if it has a unique, non-zero prime (maximal) ideal $\mathfrak{m}$. Any generator π of $\mathfrak{m}$ is referred to as a *uniformiser* of R. Note that any two uniformisers differ multiplicatively by a unit.

The non-zero ideals of R are of the form $\mathfrak{m}^n$. In particular, if we fix a uniformiser π, we may express any non-zero element uniquely in the form $u \cdot \pi^n$ where $n \geq 0$ and $u \in R^*$. This defines the associated *discrete valuation* on R:

$$\begin{aligned} v : R \setminus \{0\} &\longrightarrow \mathbb{Z}_{\geq 0}; \\ (u \cdot \pi^n) &\longmapsto n. \end{aligned}$$

Let K denote the field of fractions of R. Then, again we have a unique expression:

$$K = \{u \cdot \pi^n \mid n \in \mathbb{Z} \text{ and } u \in R^*\} \cup \{0\}$$

and we extend our discrete valuation $v : K^* \to \mathbb{Z}$. Note that we have the properties:

i) $v : K^* \to \mathbb{Z}$ is a surjective homomorphism.

ii) For all $x, y \in K$ we have: $v(x + y) \geq \inf(v(x), v(y))$.

where by convention $v(0) := \infty$. It is not hard to see that the unique maximal ideal of R is given by:

$$\mathfrak{m} := \{x \in R \mid v(x) > 0\}.$$

We define the *residue field* of a valuation ring R as $k := R/\mathfrak{m} = R/\pi R$ for any uniformiser π. Given a field K with a discrete valuation v we may define the *completion of K with respect to v* denoted by $\widehat{K_v}$. Indeed, this may be defined as the fraction field of the $\mathfrak{m}$-adic completion of $\hat{R}$. However, it is often convenient to consider the associated *norm* on K (for some fixed $a \in (0, 1)$):

$$\begin{aligned} \|x\| &= a^{v(x)} \text{ when } x \neq 0, \\ \|0\| &= 0. \end{aligned}$$

One can verify that the norm on K satisfies the following, for every $x, y \in K$:

$$\begin{aligned} \|x \cdot y\| &= \|x\| \cdot \|y\|, \\ \|x + y\| &\leq \sup(\|x\|, \|y\|), \\ \|x\| &\geq 0. \end{aligned}$$

where we have equality in the last line if and only if $x = 0$. Then equivalently, $\widehat{K_v}$ is the completion of K as a normed space with respect to $\|\cdot\|$.

Example 3.1.3. Let p be a prime. We define the p-adic norm on $\mathbb{Q}$ by:

$$\|p^r \frac{a}{b}\|_p := p^{-r},$$

where $r \in \mathbb{Z}$ and a and b are coprime integers, not divisible by p. Then the completion of $\mathbb{Q}$ with respect to p is given by the p-adic numbers $\mathbb{Q}_p$.

3.1.2 Extensions of Dedekind domains

Let A be a Dedekind domain and K its field of fractions. Then, for every non-zero prime $\mathfrak{p} \subset A$, the localisation $A_\mathfrak{p}$ is a DVR. We denote by $v_\mathfrak{p}$ the corresponding valuation on K. Suppose that L is a finite separable extension of K and B is the integral closure of A in L. As L/K is separable, B is also a Dedekind domain [Ser13, I, §4, Prop. 9].

Remark 3.1.4. We say that a field k is *perfect* if all algebraic extensions are separable. Indeed, every characteristic 0 field is perfect, and a characteristic $p > 0$ field is perfect if and only if the Frobenius map $x \mapsto x^p$ is an automorphism. Thus, the 'first' example of an imperfect field where we must be careful about notions of separability is $k = \mathbb{F}_p(t)$. Note that when k is perfect, the notions of separable and algebraic closure coincide.

Let $\mathfrak{p} \subset A$ be a non-zero prime ideal. As B is Dedekind, we may decompose $\mathfrak{p}B$ into a product of prime ideals [Ser13, I, §3, Prop. 7]:

$$\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}},$$

where the image of $\mathfrak{p}B$ in $B_\mathfrak{q}$ is of the form $(\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q}}$. The integer $e_\mathfrak{q}$ is called the *ramification index* of $\mathfrak{q}$ in the extension L/K. We take the product over primes $\mathfrak{q} \subset B$ that *divide* $\mathfrak{p}$ in the sense that $\mathfrak{q} \cap A = \mathfrak{p}$. For such primes, there is an extension of residue fields:

$$\kappa(\mathfrak{p}) := A/\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \subseteq B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} = B/\mathfrak{q} =: \kappa(\mathfrak{q}).$$

Denote by $f_\mathfrak{q} = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]$ the *residue degree* of $\mathfrak{q}$ in L/K. When there is only one prime $\mathfrak{q}$ lying over $\mathfrak{p}$ and $f_\mathfrak{q} = 1$, we say the extension L/K is *totally ramified at* $\mathfrak{p}$. Conversely, when $e_\mathfrak{q} = 1$ and $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is separable, we say that the extension L/K is *unramified over* $\mathfrak{p}$.

Remark 3.1.5. We can define the same notion for extensions of local rings. Suppose that $(R, \mathfrak{m}) \subseteq (S, \mathfrak{n})$ is an extension of local rings with fraction fields $K \subseteq L$, residue fields $k(\mathfrak{m})$ and $k(\mathfrak{n})$, and valuations v and w respectively. Then, we define the *ramification index* e of R in S as the ramification index of $\mathfrak{m}$ in S; that is to say:

$$\mathfrak{m}S = \mathfrak{n}^e.$$

Equivalently, if π is a uniformiser of R, then $e = w(\pi)$. If $e = 1$ and the extension $k(\mathfrak{n})/k(\mathfrak{m})$ is separable, then we say the extension is *unramified*.

Proposition 3.1.6. *Let A be a Dedekind domain and $\mathfrak{p}$ a non-zero prime. Let L/K be a finite, separable extension of degree n and B the integral closure of A in L. We then have the equality:*

$$n = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}.$$

3.1.3 Galois extensions of local fields

Let L/K and $B \supseteq A$ be as in the previous subsection. Suppose now that L/K is Galois and let $\mathrm{Gal}(L/K)$ denote the corresponding Galois group.

Proposition 3.1.7. $\mathrm{Gal}(L/K)$ *acts transtively on the set of primes $\mathfrak{q}$ of B that lie over a fixed prime $\mathfrak{p} \subset A$. Moreover, for each prime $\mathfrak{q}$ over $\mathfrak{p}$, the integers $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}}$ depend only on $\mathfrak{p}$. We thus have the equality:*

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}},$$

where $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ are the integers above, and $g_{\mathfrak{p}}$ is the number of primes of B lying over $\mathfrak{p}$.

Proof. See [Ser13, I, §7]. □

Let $\mathfrak{p} \subset A$ be a non-zero prime and $\mathfrak{q}, \mathfrak{q}' \subset B$ be two primes lying over $\mathfrak{p}$. We define the *decomposition group* of $\mathfrak{q}$ in L/K as the subgroup $D_{\mathfrak{q}}(L/K) \subseteq \mathrm{Gal}(L/K)$ fixing $\mathfrak{q}$. As the action is transitive, $D_{\mathfrak{q}}(L/K)$ and $D_{\mathfrak{q}'}(L/K)$ are conjugate subgroups. As $D_{\mathfrak{q}}(L/K)$ fixes $\mathfrak{q}$, we have a well defined homomorphism:

$$D_{\mathfrak{q}}(L/K) \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})).$$

We denote the kernel of this homomorphism by $I_{\mathfrak{q}}(L/K)$ as the *inertia group of $\mathfrak{q}$ in L/K*. By transitivity of $\mathrm{Gal}(L/K)$ on the set of primes $\mathfrak{q} \subseteq B$ lying over a prime $\mathfrak{p} \subseteq A$, it is clear that:

$$g_{\mathfrak{p}} = [\mathrm{Gal}(L/K) : D_{\mathfrak{q}}(L/K)].$$

Let K^D denote the subgroup of L fixed by $D_{\mathfrak{q}}(L/K)$ and K^I the subgroup fixed by $I_{\mathfrak{q}}(L/K)$. Consider the field extensions:

$$L \supseteq K^I \supseteq K^D \supseteq K.$$

When the decomposition group is a normal subgroup, by the Galois correspondence we have:

$$[K^D : K] = g, \quad [L : K^I] = e, \quad [K^I : K^D] = f.$$

From this we obtain the following easy corollary:

Corollary 3.1.8. *Let A be a Dedekind domain, K its field of fractions, L/K a finite Galois extension, and B the integral closure of A in L. Then L/K is unramified at a prime $\mathfrak{p} \subseteq A$ if and only if $I_{\mathfrak{q}}(L/K)$ is trivial for some prime ideal $\mathfrak{q}_i \subseteq B$ lying over $\mathfrak{p}$.*

3.1.4 Extensions of complete fields

Let L/K be a finite separable extension of fields, and now suppose that K admits a discrete valuation v. Consider the valuation ring R and its integral closure B in L. As R is a principal ideal domain, B is a free R-module of rank $n = [L : K]$. Denote by $\mathfrak{q}_i$ the prime ideals of B. Each corresponds to a valuation w_i on L; extending v which we refer to as a *prolongation*.

Proposition 3.1.9. *Let K be a field with a discrete valuation v and valuation ring R. Let L/K be a finite separable extension of degree n, and let B be the closure of R in L.*

i) Suppose that K is complete with respect to v. Then v extends to a unique prolongation w on L such that B is a discrete valuation ring with respect to w, and L is complete with respect to w. In this case, if e denotes the ramification index of L/K (cf. Remark 3.1.5) and f the residue degree, then $n = ef$.

ii) More generally, let w_i denote the different prolongations of v to L, and let e_i, f_i be the corresponding ramification indices and residue degrees respectively. Then:

$$[\widehat{L_{w_i}} : \widehat{K_v}] = e_i f_i.$$

Moreover, if $\hat{w}_i$ is the unique prolongation of the valuation $\hat{v}$ on $\widehat{K_v}$ to $\widehat{L_{w_i}}$, then we have:

$$e_i = e(\widehat{L_{w_i}}/\widehat{K_v}) \text{ and } f_i = f(\widehat{L_{w_i}}/\widehat{K_v}).$$

Proof. See [Ser13, I, §3 and §4]. □

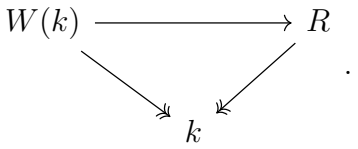
3.1.5 Witt vectors

Let R be a discrete valuation ring, complete with respect to a valuation v with a uniformiser π. Let K denote the field of fractions and k the residue field. Suppose that R is of characteristic 0 and k is of characteristic $p > 0$. Then, there is a copy of $\mathbb{Z}$ in R. By localising the extension $\mathbb{Z} \hookrightarrow R$ at p and taking the completion, one obtains an extension of complete local rings $\mathbb{Z}_p \subseteq R$ with ramification index e which we refer to as the *absolute ramification index* of R. Equivalently, if we normalise v so that $v(\pi) = 1$, then $v(p) = e$. We say that R is *absolutely unramified* if $e = 1$. In this case, we may take p as a uniformiser of R.

When the residue field k is finite of order p^f, R is a free, finitely generated module over $\mathbb{Z}_p$ of rank n where $n = ef$. In this case, $K \supseteq \mathbb{Q}_p$ is a finite extension of degree n.

Proposition 3.1.10. *Let k be a perfect field of characteristic $p > 0$. Then there exists a, unique up to isomorphism, complete DVR denoted by $W(k)$ of characteristic 0, which*

is absolutely unramified and has residue field k. Uniqueness is guaranteed by the following universal property: when R is a complete DVR of characteristic 0 and residue field k, there exists a unique homomorphism $W(k) \to R$ of local rings, which specialises to the identity on residue fields:



Furthermore, R is a free $W(k)$-module of rank e where e is the absolute ramification index of R.

Proof. See [Ser13, I, §5] for a proof. □

The ring $W(k)$ is referred to as the ring of *Witt vectors* associated to k. We omit the proof of the universal property and instead construct the Witt vectors in their usual representation. Let p be a prime number. We define the *Witt polynomials*:

$$W_0 = X_0,\ W_1 = X_0^p + pX_1,\ ...,\ W_n = X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n, ...$$

in $\mathbb{Z}[X_0, X_1, ...]$. The proof of the following can be found in [Ser13, II, §6]:

Lemma 3.1.11. *Given $\Phi \in \mathbb{Z}[X, Y]$, there exists a unique sequence $\varphi_0, \varphi_1, ...$ in the polynomial ring $\mathbb{Z}[X_0, X_1, ..., Y_0, Y_1, ...]$ such that:*

$$W_n(\varphi_0, ...) = \Phi(W_n(X_0, ...), W_n(Y_0, ...)), \quad n \geq 0.$$

Let $S_0, S_1, ...$ (respectively $P_0, P_1, ...$) denote the polynomials $\varphi_0, \varphi_1, ...$ from the Lemma associated to the polynomial $\Phi(X, Y) = X + Y$ (respectively $\Phi(X, Y) = XY$). Let A be an arbitrary commutative ring. Then, for each n, we define the multiplication $\cdot_{W_n}$ and addition $+_{W_n}$ on the set A^n by:

$$\begin{aligned} a +_{W_n} b &= (S_0(a, b), ..., S_n(a, b)); \\ a \cdot_{W_n} b &= (P_0(a, b), ..., P_n(a, b)). \end{aligned}$$

In fact, these define a commutative ring structure on A^n which we denote by $W_n(A) = (A^n, +_{W_n}, \cdot_{W_n})$. The zero element is denoted by $(0, ..., 0)$ and the unit by $(1, 0, ..., 0)$ in terms of coordinates of A^n. We refer to $W_n(A)$ as the ring of *Witt vectors associated to A of length n*. We denote a more general element $a \in W_n(A)$ by $(a_0, ..., a_n)$.

Example 3.1.12. For large n, the addition on $W_n(A)$ is hard to describe, but for $n = 2$

we have:

$$S_0(a,b) = a_0 + b_0, \qquad S_1(a,b) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0+b_0)^p}{p};$$
$$P_0(a,b) = a_0 b_0, \qquad P_1(a,b) = b_0^p a_1 + b_1 a_0^p + p a_1 b_1.$$

We have natural projections $W_{n+1}(A) \to W_n(A)$ and can take the projective limit to define the *Witt vectors* associated to A:

$$W(A) := \varprojlim W_n(A).$$

Of course, one defines the multiplication and addition on this ring by the polynomials S_n and P_n applied to $A^{\mathbb{N}}$.

Remark 3.1.13. Let k be a perfect field of characteristic $p > 0$. Then there is a lift of the Frobenius morphism $F_0 : k \to k$; $x \mapsto x^p$ given by:

$$F : W(k) \longrightarrow W(k);$$
$$(a_0, a_1, ...) \longmapsto (a_0^p, a_1^p, ...).$$

One may check that this is a ring homomorphism. Dually, there is a *Verschiebung* or *shift* operator:

$$V : W(k) \longrightarrow W(k);$$
$$(a_0, a_1, ...) \longmapsto (0, a_0, a_1, ...).$$

These maps are dual in the sense that $VF = \cdot p = FV$.

3.2 Abelian varieties and finite flat group schemes

3.2.1 Group schemes

Let Sch/S denote the category of S-schemes. The main reference for the properties of finite group schemes will be [Tate97]. A *group object* G in Sch/S (or equivalently an *S-group scheme*) is an object with the following morphisms (of S-schemes):

i) $m : G \times_S G \longrightarrow G$ the *multiplication* map;

ii) $i : G \longrightarrow G$ the *inversion* map;

iii) $e : S \longrightarrow G$ the *identity* section;

satisfying the usual group axioms. We may view G as a functor of points using the Yoneda embedding:

$$\begin{aligned} G : \mathrm{Sch}/S &\longrightarrow \mathrm{Set}; \\ T &\longmapsto G(T) := \mathrm{Hom}_S(T, G). \end{aligned}$$

Each set $G(T)$ is naturally a group using the group object structure on G and so we obtain a factorisation:

$$\begin{array}{ccc} \mathrm{Sch}/S & \xrightarrow{\exists} & \mathrm{Grp} \\ & \searrow^{G} & \downarrow \text{forgetful} \\ & & \mathrm{Set} \end{array}$$

where Grp is the category of groups. By the Yoneda lemma, conversely, any functor $H : \mathrm{Sch}/S \to \mathrm{Grp}$, with the functor (forgetful $\circ\, H$) being representable by an S-scheme, is also a group scheme. Importantly, this reduces the descriptions of many properties of group schemes to the usual definition for groups.

Definition 3.2.1. We say that an S-group scheme G is *commutative* if the following diagram commutes:

$$\begin{array}{ccc} G \times_S G & \xrightarrow{(\mathrm{pr}_2, \mathrm{pr}_1)} & G \times_S G \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & G & \end{array} .$$

Equivalently, $G(T)$ is a commutative group for each $T \to S$.

A *homomorphism* $f : G \to H$ of S-group schemes is a morphism of S-schemes such that the induced map:

$$f_T : G(T) \longrightarrow H(T)$$

is a group homomorphism for all $T \to S$.

Definition 3.2.2. Let $f : G \to H$ be a homomorphism of S-group schemes.

i) Consider the fibre product:

$$\begin{array}{ccc} K := G \times_H S & \longrightarrow & S \\ \downarrow & & \downarrow e_H \\ G & \xrightarrow[f]{} & H \end{array} .$$

Then, for each S-scheme T, $K(T)$ is the kernel of f_T and so is a group in a natural way. Using Yoneda's lemma, we then obtain a group scheme structure on K. We denote the corresponding group object by $\ker(f)$.

ii) It is not as simple to show that $\operatorname{coker}(f)$ exists or is an S-group scheme. Unlike the functor obtained by taking kernels, the cokernel functor is rarely representable.

For each positive integer n, we write by $[n]_G : G \longrightarrow G$ for the *multiplication-by-n* map which is given on points by the usual map:

$$\begin{aligned} G(T) &\longrightarrow G(T) \\ a &\longmapsto a^n \end{aligned}$$

We denote by $G[n]$ the kernel of $[n]_G$; the *n-torsion* subgroup of G.

3.2.2 Abelian varieties

We recall some facts about abelian varieties over a field k, and abelian schemes over a noetherian base scheme S. For statements about abelian varieties, we refer to [Mum74], and for statements about abelian S-schemes, we refer to [MFK-94, Ch. 6].

Definition 3.2.3. Suppose that A is a k-group variety. We say that A is an *abelian variety* if it is complete and geometrically connected.

More generally, if $\mathscr{A}$ is a proper S-group scheme with geometrically connected fibres, then we say $\mathscr{A}$ is an *abelian scheme*; i.e. the fibres of $\mathscr{A}$ over S are abelian varieties. Most authors do not assume commutativity in either definition, but this follows from properness:

Proposition 3.2.4. *Let $\mathscr{A}$ be an abelian scheme over S. Then $\mathscr{A}$ is commutative as an S-group scheme.*

Proof. See [MFK-94, Corollary 6.5]. □

Example 3.2.5. i) Suppose E is a projective, integral, smooth k-curve of genus 1 with a rational point $e \in E(k)$. Then there is a unique abelian variety structure on E with identity e. E is of course an *elliptic curve*. There is an isomorphism of groups:

$$\begin{aligned} E(k) &\longrightarrow \operatorname{Pic}^0_k(E); \\ P &\longmapsto [P - e] \end{aligned}$$

where $\operatorname{Pic}^0_k(E)$ is the group of (k-rational) degree 0 divisors of E, modulo linear equivalence.

ii) More generally, if C is a projective, integral, smooth k-curve of genus $g \geq 2$ with a rational point $P_0 \in C(k)$, then there is a (unique up to isomorphism) k-abelian variety J_C of dimension g such that:

$$J_C(\bar{k}) \cong \operatorname{Pic}^0_{\bar{k}}(C).$$

The rational point P_0 determines an embedding $C \hookrightarrow J_C$ which is given by:

$$C(\bar{k}) \hookrightarrow \mathrm{Pic}^0_{\bar{k}}(C) \cong J_C(\bar{k});$$
$$P \longmapsto [P - P_0]$$

on $\bar{k}$-points. J_C is the *Jacobian variety* of C.

iii) Let X be a smooth projective variety over k, then there is an associated *Albanese variety* $X \to \mathrm{Alb}(X)$ characterised by the property that, for all morphisms $g : X \to A$ from X to an abelian variety A/k, there exists a unique homomorphism of abelian varieties $f : A \to \mathrm{Alb}(X)$ such that:

$$\begin{array}{ccc} & & A \\ & \overset{g}{\nearrow} & \downarrow f \\ X & \longrightarrow & \mathrm{Alb}(X) \end{array}$$

commutes. Informally, the Albanese variety is the 'smallest' abelian variety associated to X. When X is a curve, the Jacobian variety and Albanese variety coincide.

A *homomorphism* $f : A \to B$ of k-abelian varieties A and B is simply a homomorphism of k-group schemes. A surjective homomorphism of abelian varieties $f : A \to B$ of the same dimension is an *isogeny*. In this case, $H := \ker(f)$ is a finite k-group scheme and B is the categorical quotient A/H. Conversely, the quotient of an abelian variety by a finite subgroup always exists:

Proposition 3.2.6. *i) Let A be an abelian variety and H a finite subgroup. Then there exists an abelian variety B and an isogeny $f : A \to B$ such that $\ker(f) = H$. We call $B = A/H$ the quotient of A by H.*

ii) Let $f : A \to C$ be an isogeny of abelian varieties and let $H \subseteq \ker(f)$ be a subgroup. Then there exists an isogeny $A/H \to C$ allowing the following diagram to commute:

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & C \\ & {\scriptstyle \text{quot.}} \searrow \quad \nearrow {\scriptstyle \exists} & \\ & A/H & \end{array} .$$

Proof. i) See [Mum74, II.7, Th. 6].

ii) Ibid., p. 118, Corollary 1.

□

Let k be a field of characteristic $p \geq 0$ and let n be a positive integer. We have the

following description of the geometric n-torsion points of an abelian variety A of dimension g *as a group*:

Proposition 3.2.7. *Consider the isogeny $[n]_A : A \to A$. We have the following:*

i) Suppose that $p \nmid n$. Then $[n]_A$ is separable of degree n^{2g} and moreover:

$$A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

ii) If $p > 0$ then there exists an integer $0 \leq i \leq g$, called the p-rank of A, such that:

$$A[p](\bar{k}) \cong (\mathbb{Z}/p\mathbb{Z})^{i}.$$

Proof. See [Mum74, p. 64]. □

When A is an elliptic curve, this leads to the following dichotomy:

Definition 3.2.8. Suppose that E is an elliptic curve over a field k of characteristic $p > 0$. Let r denote the p-rank of E.

i) If $r = 1$ we say that E is *ordinary*.

ii) If $r = 0$ we say that E is *supersingular*.

3.2.3 Hopf algebras and affine group schemes

Suppose now that $S = \mathrm{Spec}(R)$ is the spectrum of a ring R. We denote by Sch/R the category of R-schemes. Suppose $G = \mathrm{Spec}(A)$ is an *affine* R-group scheme. Then, dually, we obtain the following R-algebra homomorphisms:

i) $\mu : A \longrightarrow A \otimes_R A$ the *co-multiplication* map;

ii) $\iota : A \longrightarrow A$ the *antipodal* map;

iii) $\epsilon : A \longrightarrow R$ the *augmentation* or *co-unit* map.

We call an R-algebra equipped with these homomorphisms, satisfying the dual group axioms a *Hopf algebra*. Clearly, the spectrum of any Hopf algebra is an R-group scheme.

Example 3.2.9. i) Let G be a finite group. We denote by $G \times S$ the disjoint union of copies of S indexed by elements of G. The group structure on G induces a group scheme structure on the disjoint union via its indices. We call $G \times S$ the *constant* R-group scheme for the group G. When there is no risk of ambiguity, we will write G as shorthand for $G \times S$.

ii) Let $A = R[t]$. We define co-multiplication by $\mu(t) = a + b$ under the isomorphism:

$$A \otimes_R A \cong R[a, b].$$

This defines the *additive group* $\mathbb{G}_{a,R} := (\mathbb{A}^1_R, +)$. Note that, for any R-algebra B, the isomorphism:

$$\begin{aligned} \mathrm{Hom}_R(R[t], B) &\longrightarrow B; \\ f &\longmapsto f(t) \end{aligned}$$

identifies B with itself (as an additive group).

iii) Taking now $A = R[t, t^{-1}]$, we set $\mu(t) = ab$ using the notation above. This defines the *multiplicative group* $\mathbb{G}_{m,R} := (\mathbb{A}^1_R \setminus \{0\}, \times)$. Note that, for any R-algebra B, the isomorphism:

$$\begin{aligned} \mathrm{Hom}_R(R[t, t^{-1}], B) &\longrightarrow B^*; \\ f &\longmapsto f(t) \end{aligned}$$

gives the units of B (as a multiplicative group).

Let k be a field of characteristic $p \geq 0$ and $n > 0$ an integer. We define the multiplicative group scheme μ_n to be the kernel of $[n]_{\mathbb{G}_{m,k}}$:

$$\mathbb{G}_{m,k}[n] = \mu_n = \mathrm{Spec}\left(\frac{k[x]}{\langle x^n - 1\rangle}\right).$$

When $p > 0$, the p-torsion of $\mathbb{G}_{a,k}$ is non-reduced:

$$\alpha_p := \mathbb{G}_{a,k}[p] = \mathrm{Spec}\left(\frac{k[x]}{\langle x^p\rangle}\right).$$

3.2.4 Finite flat group schemes and quotients

Suppose that S is a locally noetherian, connected scheme. An S-scheme H is finite and flat over S if $\mathscr{O}_H$ is locally free of finite, constant rank n over $\mathscr{O}_S$. We denote the *rank* of H over S by $[H : S]$.

Suppose that G is a group scheme over S and H is a finite, flat closed subgroup scheme of G. We want to show that the categorical quotient G/H exists as an S-scheme. More generally, we can consider the *action* of a finite, flat group scheme H on a scheme $X \to S$:

Definition 3.2.10. An *action* of a finite, flat group scheme is a morphism of S-schemes:

$$\rho : H \times_S X \longrightarrow X,$$

such that, for all S-schemes T, we have a group action $H(T)$ on $X(T)$:

$$\rho_T : H(T) \times X(T) \longrightarrow X(T),$$

i.e. for each $h \in H(T)$ $\rho_{T,h} : X(T) \to X(T)$ is an automorphism and:

$$\rho_{T,h} \circ \rho_{T,h'} = \rho_{T,hh'} \text{ and } \rho_{T,e_{H(T)}} = \mathrm{Id},$$

for all $h, h' \in H(T)$.

We say that the action ρ is *strictly free* if the following morphism of S-schemes:

$$(\rho, \mathrm{Id}) : H \times_S X \longrightarrow X \times_S X,$$

sending $(h, x) \mapsto (h \cdot x, x)$ is injective and a closed immersion. Suppose that $f : X \to Y$ is a morpshism of schemes and that ρ gives an action of H on X. We say that f is *constant on orbits* if the following diagram commutes:

$$\begin{array}{ccc} H \times_S X & \xrightarrow{\mathrm{pr}_2} & X \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow[f]{} & Y \end{array}.$$

A concise proof of the following fact can be found in [Ray66]:

Proposition 3.2.11. *Suppose that H is a finite flat group scheme over a locally noetherian base S. Suppose further that H acts strictly freely on a finite type S-scheme X such that every orbit is contained in an affine open set. Then there exists an S-scheme Y and a morphism $f : X \to Y$, constant on orbits, such that for any other morphism $f' : X \to Y'$ that is constant on orbits, there exists a unique morphism $\varphi : Y \to Y'$ allowing the below diagram to commute:*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & {\scriptstyle f'}\searrow & \downarrow{\scriptstyle \varphi} \\ & & Y' \end{array}.$$

It follows that Y is unique up to isomorphism. We call $X/H := Y$ the quotient of X by H. Moreover:

i) The morphism $f : X \to X/H$ is finite flat of rank given by the rank of H/S.

ii) For every S-scheme T, the natural map $X(T)/H(T) \to (X/H)(T)$ is injective.

Suppose now that G is a finite flat S-group scheme and H a closed flat subgroup. Then, using the above we may construct the scheme of left cosets G/H. The rank of G/H over S is given by the difference of the ranks of G and H. Of course, G/H is a finite flat group scheme over S only when H is a normal subgroup (point-wise); for example when G is commutative.

3.2.5 The étale fundamental group

The following discussion can be found in [Mil80, I.3]. Let S be a locally noetherian, connected scheme. A morphism $f : Y \to S$ is *finite étale* if it is finite, flat and *unramified* i.e. for each point $s \in S$, the fibre Y_s is the spectrum of a separable algebra over the residue field $\kappa(s)$. Equivalently, Y_s is reduced and for each point $y \in Y_s$ we have that $\kappa(y)/\kappa(s)$ is a separable extension of fields. Suppose we fix a geometric point $\bar{s} \to S$ lying over s, namely a morphism $\mathrm{Spec}(\bar{k}) \to S$ induced by an algebraic closure $\bar{k}/\kappa(s)$. Denote by FEt/S the category of finite étale maps to S. We define the functor:

$$\begin{aligned} F_{\bar{s}} : \mathrm{FEt/S} &\longrightarrow \mathrm{Set}; \\ (Y \xrightarrow{f} S) &\longmapsto \mathrm{Hom}_S(\bar{s}, Y). \end{aligned}$$

Note that, if S is a variety over an algebraically closed field $\bar{k}$, then $F_{\bar{s}}(Y) = f^{-1}(\bar{s})$. If we could define a 'universal' étale cover $\tilde{S}$ of S, we would then obtain the following definition of étale fundamental group:

$$\pi_1^{\text{ét}}(S, \bar{s}) := \mathrm{Aut}_S(\tilde{S}).$$

By definition, such an object would represent the functor $F_{\bar{s}}$. However, in general no such universal object exists. To remedy this, we can define a partial ordering, via morphisms $S_j \to S_i$, on the finite étale covers of S and show that $F_{\bar{s}}$ is *pro-representable* with respect to this. Namely, we will have a projective system $(S_i)_{i \in I}$ and a natural isomorphism:

$$F_{\bar{s}}(Y) \cong \varprojlim_{i \in I} \mathrm{Hom}(S_i, Y).$$

Remark 3.2.12. In the projective system, it is possible to restrict to finite étale covers $S_i \to S$ that are *Galois* i.e. of degree equal to the order of $\mathrm{Aut}_S(S_i)$.

This allows us to define the *étale fundamental group* of S:

$$\pi_1^{\text{ét}}(S, \bar{s}) := \varinjlim_{i} \mathrm{Aut}_S(S_i).$$

Equipping each finite automorphism group with the discrete topology, we give $\pi_1^{\text{ét}}(S, \bar{s})$ the natural topology as an injective limit. The étale fundamental group acts trivially on the

projective system $(S_i)_{i\in I}$. This induces a (right) action of the étale fundamental group on $F_{\bar{s}}(Y) \cong \varprojlim_{i\in I}\mathrm{Hom}(S_i, Y)$ for each finite étale cover $Y \to S$. Moreover, if we give $F_{\bar{s}}(Y)$ the discrete topology, this action is continuous. Let $\mathrm{F}\pi_1^{\text{ét}}(S,\bar{s})-\mathrm{Set}$ denote that category of finite, discrete sets with a continuous $\pi_1^{\text{ét}}(S,\bar{s})$-action.

Theorem 3.2.13. *The functor:*

$$\begin{aligned}\mathrm{FEt}/S &\longrightarrow \mathrm{F}\pi_1^{\text{ét}}(S,\bar{s})-\mathrm{Set};\\ Y &\longmapsto F(Y)\end{aligned}$$

is an equivalence of categories.

When G is a finite flat group scheme over a noetherian, connected scheme S, we have an equivalence of categories:

$$\begin{aligned}\mathrm{FFGS}^{\text{ét}}/S &\longrightarrow \mathrm{F}\pi_1^{\text{ét}}(S,\bar{s})-\mathrm{Grp};\\ Y &\longmapsto F(Y)\end{aligned}$$

between the category of finite flat étale group schemes over S and finite groups equipped with a continuous $\pi_1^{\text{ét}}(S,\bar{s})$-action.

Example 3.2.14. Let k be a field. Then we have an isomorphism:

$$\mathrm{Gal}(k^{\mathrm{sep}}/k) \cong \pi_1^{\text{ét}}(\mathrm{Spec}(k),\bar{s})$$

where k^{sep} is a separable closure of k. This is clear from Remark 3.2.12.

Remark 3.2.15. Let G/S be a finite flat group scheme. Then the relative sheaf of differentials $\Omega^1_{G/S}$ coincides with $\mathscr{I}/\mathscr{I}^2$ where $\mathscr{I} \subseteq \mathscr{O}_G$ is the *augmentation ideal sheaf*. It is the ideal sheaf corresponding to the unit section $e : S \to G$ (cf. 3.2.3 iii)) viewed as a closed subscheme of G. Thus, $G \to S$ is étale if and only if $\Omega^1_{G/S} = 0$ i.e. $\mathscr{I} = \mathscr{I}^2$. By Nakayama's lemma, this is equivalent to $\mathscr{I}_x = 0$ for each $x \in e(S)$. Hence, the complement of $e(S)$ in G is the support of $\mathscr{I}$ and is closed. Therefore, G/S is étale if and only if the identity section $e : S \to G$ is open (and closed).

Consider now a henselian local ring R with residue field k. Denote $S = \mathrm{Spec}(R)$ and let $S_0 = \mathrm{Spec}(k) = \{s\}$ be its closed point. As R is henselian, the functor:

$$\begin{aligned}\mathrm{FEt}/S &\longrightarrow \mathrm{FEt}/S_0;\\ (Y \xrightarrow{f} S) &\longmapsto (Y \times_R k \to S_0)\end{aligned}$$

is an equivalence. Thus, we have an isomorphism

$$\pi_1^{\text{ét}}(S_0,\bar{x_0}) \to \pi_1^{\text{ét}}(S,\bar{x}),$$

induced by the inclusion $\{s\} \hookrightarrow S$, where $\bar{x}_0 : \mathrm{Spec}(\bar{k}) \to \mathrm{Spec}(k)$ is a geometric point and $\bar{x}$ its image in $\mathrm{Spec}(R)$. Importantly, a finite étale group scheme $\mathscr{G}/S$ is determined by $\mathscr{G}(\bar{x})$ and thus by its special fibre $\mathscr{G}_0 := \mathscr{G} \times_S S_0$:

Corollary 3.2.16. *Let R be a henselian local ring with residue field k. Let $\mathscr{G}_0$ be a finite étale group scheme over k. Then, there exists a unique finite étale group scheme $\mathscr{G}/R$ lifting $\mathscr{G}_0$ in the sense that:*

$$\mathscr{G}_k \cong \mathscr{G}_0.$$

Corollary 3.2.17. *Let k be a separably closed field and G a finite étale group scheme over k. Then G is a constant group scheme.*

Proof. Write $G = \mathrm{Spec}(A)$ so that A is a finite étale algebra over k. A is then a finite product of finite separable field extensions of k. However, as k is separably closed, A is a finite product of copies of k. It is then not hard to see that G is the constant group scheme associated to $G(k)$. □

3.2.6 The connected-étale sequence

We now restrict out attention to the category FFGS/S of finite flat commutative group schemes over a henselian local ring $S = \mathrm{Spec}(R)$. Let $\mathfrak{m}$ denote the maximal ideal of R, K the fraction field and $k = R/\mathfrak{m}$ the residue field. Let $\mathscr{G}$ be a finite flat group scheme over this ring and let $\mathscr{G}^\circ$ denote the connected component of the identity.

Lemma 3.2.18. *$\mathscr{G}^\circ$ is a normal subgroup scheme and the quotient:*

$$\mathscr{G}/\mathscr{G}^\circ =: \mathscr{G}_{\text{ét}}$$

is an étale group scheme.

Proof. See [Tate97, p. 139]. □

The induced short exact sequence of a finite flat commutative group scheme into its connected and étale parts is an important invariant:

Definition 3.2.19. Let $\mathscr{G}$ be a finite flat group scheme over a henselian local ring R. We refer to the short exact sequence:

$$0 \longrightarrow \mathscr{G}^\circ \longrightarrow \mathscr{G} \longrightarrow \mathscr{G}_{\text{ét}} \longrightarrow 0;$$

as the *connected-étale* sequence of $\mathscr{G}$.

Let $\mathscr{G}/R$ be a finite flat commutative group scheme. Suppose the residue field k has characteristic $p > 0$. We will see from the following results that $[\mathscr{G}^\circ : S]$ is always a power

of p. In particular, in characteristic 0 every finite commutative group scheme over a field is étale. So, in some sense, the connected-étale sequence is only relevant in positive and mixed characteristic.

Lemma 3.2.20. *Suppose that k is algebraically closed and of characteristic $p > 0$. Then the connected-étale sequence of a finite flat commutative group scheme G/k splits over k.*

Proof. Let $G = \mathrm{Spec}(A)$ be a finite commutative group scheme over k. As k is perfect, G_{red} is étale. Moreover, $G_{\mathrm{red}} \times G_{\mathrm{red}}$ is still reduced and so $G_{\mathrm{red}} \subseteq G$ is a closed subgroup scheme. Letting $\alpha : \mathrm{Spec}(\bar{k}) \to \mathrm{Spec}(A)$ be a geometric point as in 3.2.5, we have isomorphisms $G_{\mathrm{red}}(\alpha) \cong G(\alpha) \cong G_{\text{ét}}(\alpha)$. Therefore, the canonical map $G \to G_{\text{ét}}$ is an isomorphism when restricted to G_{red}; thus providing a splitting of the connected-étale sequence. □

Proposition 3.2.21. *Suppose that k is a field of characteristic $p > 0$ and G is a connected finite group scheme over k. Then the order of G is a power of p.*

Proof. See [Tate97, Lemma 3.7.1]. □

Corollary 3.2.22. *Let k be a field of characteristic $p \geq 0$ and let G be a finite k-group scheme of order coprime to p. Then G is étale. In particular, if $\mathrm{char}(k) = 0$ then every finite group scheme is étale.*

3.2.7 Cartier duality

Let R be as in the previous section and suppose that $\mathscr{G} = \mathrm{Spec}(A)$ is a finite flat commutative R-group scheme. As discussed in 3.2.3, A is a Hopf algebra. Denote by $A^* := \mathrm{Hom}_R(A, R)$ the dual R-module. As $\mathscr{G}$ is finite flat, A is locally free of finite constant rank. Thus, the operation $(-)^*$ is reflexive, i.e. there is a natural isomorphism:

$$A^{**} \cong A.$$

Remark 3.2.23. As A is commutative, one can endow $A^* := \mathrm{Hom}_R(A, R)$ with the structure of a Hopf algebra and thus $\mathscr{G}^\vee$ becomes a group scheme. For example, let $\eta : A \otimes_R A \to A$ be given by multiplication $a \otimes b \mapsto ab$. Then, dually we may define:

$$\mu^* : A^* \longrightarrow A^* \otimes_R A^* \cong (A \otimes_R A)^*,$$

where the isomorphism holds as A is locally free of finite type. This defines a comultiplication on A^* and one may check that it induces a Hopf algebra structure.

Definition 3.2.24. Let $\mathscr{G}$ be a finite flat commutative R group scheme. We denote by:

$$\mathscr{G}^\vee := \mathrm{Spec}(A^*),$$

the *Cartier* dual of $\mathscr{G}$.

As with other 'good' duality theories, the Cartier dual is a covariant functor:

$$(\mathrm{FFGS}/R)^{op} \longrightarrow \mathrm{FFGS}/R;$$

from the category of finite, flat commutative group schemes to itself. This is clear from the association:

$$\mathscr{G}^\vee \cong \mathrm{Hom}_R(\mathscr{G}, \mathbb{G}_{m,R}).$$

Explicitly, $\mathscr{G}^\vee$ represents the functor:

$$B \longmapsto \mathrm{Hom}_B(\mathscr{G}(B), \mathbb{G}_{m,R}(B)),$$

from R-algebras to sets. Moreover, we have a duality pairing:

$$\langle -, - \rangle : \mathscr{G} \times \mathscr{G}^\vee \longrightarrow \mathbb{G}_{m,R};$$

where for each R-algebra B, we have the natural evaluation map:

$$\begin{aligned} \mathscr{G}(B) \times \mathrm{Hom}_B(\mathscr{G}(B), \mathbb{G}_{m,R}(B)) &\longrightarrow \mathbb{G}_{m,R}(B); \\ (x, f) &\longmapsto f(x). \end{aligned}$$

Lemma 3.2.25. *Let $\mu_{n,R} := \mathrm{Spec}\left(\frac{R[x]}{\langle x^n - 1\rangle}\right)$ be the n-torsion of $\mathbb{G}_{m,R}$. Then the Cartier dual is given by:*

$$\mu_{n,R}^\vee = \mathbb{Z}/n\mathbb{Z}.$$

Proof. This is clear from the association $(\mathbb{Z}/n\mathbb{Z})^\vee \cong \mathrm{Hom}_R(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_{m,R}) = \mathbb{G}_{m,R}[n]$. □

The tangent space of a finite group scheme

Let G be a finite commutative group scheme over a field k and let $e \in G(k)$ denote the identity section. Let $\mathfrak{m}_{G,e}$ denote the maximal ideal of $\mathscr{O}_{G,e}$. Recall that the *tangent space* is given by the dual k-vector space:

$$T_{G,e} = (\mathfrak{m}_{G,e}/\mathfrak{m}_{G,e}^2)^*;$$

and that there is an isomorphism:

$$T_{G,e} \cong \ker\left(G\left(\frac{k[t]}{t^2}\right) \to G(k)\right).$$

Proposition 3.2.26. *There is a canonical isomorphism of k-vector spaces:*

$$T_{G,e} \cong \mathrm{Hom}_k(G^\vee, \mathbb{G}_{a,k})$$

where $G^\vee$ is the Cartier dual of G, and $\mathbb{G}_{a,k}$ is the additive group scheme (Ex. 3.2.9 (ii)). *The right hand side is a k-vector space by left multiplication on $\mathbb{G}_{a,k}$.*

Proof. See [Pink04, Prop. 13.1]. □

3.2.8 Prolongations of group schemes

Let R be a complete discrete valuation ring of mixed characteristic $(0, p)$. Let K be its field of fractions, $\pi \in R$ a uniformiser and $k = R/\pi R$. Let v denote the valuation on R, normalised so that $v(\pi) = 1$, and let $e = v(p)$ denote the *absolute ramification index*.

Definition 3.2.27. Let G be a finite group scheme over K. A *prolongation* of G to R is a finite, flat group scheme $\mathscr{G}/R$ such that $\mathscr{G}_K \cong G$.

The following is a fundamental result of [Ray66]:

Theorem 3.2.28. *Suppose that $e < p - 1$. Let $\mathscr{G}/R$ be a finite flat commutative group scheme of order a power of p. Then $\mathscr{G}$ is, up to isomorphism, the unique prolongation of its generic fibre $\mathscr{G}_K$.*

Let $\mathrm{FFGS}^{(p)}/R$ denote the category of finite flat commutative group schemes over R of p-primary order. Let $G_K = \mathrm{Gal}(\bar{K}/K)$ denote the absolute Galois group of K, where $\bar{K}$ is a choice of algebraic closure.

Corollary 3.2.29. *Suppose that $e < p - 1$. Then the additive functor:*

$$\begin{aligned} \mathrm{FFGS}^{(p)}/R &\longrightarrow G_K\text{−Mod}; \\ \mathscr{G} &\longmapsto \mathscr{G}_K(\bar{K}). \end{aligned}$$

is fully faithful.

Importantly, to study the connected-étale sequence of $\mathscr{G}/R$, it is enough to understand the Galois action on the geometric points of the generic fibre of $\mathscr{G}$.

Corollary 3.2.30. *Let $\mathscr{G}/R$ be a finite flat commutative group scheme and suppose that $e < p - 1$. Then the connected-étale sequence:*

$$0 \longrightarrow \mathscr{G}^\circ \longrightarrow \mathscr{G} \longrightarrow \mathscr{G}_{\text{ét}} \longrightarrow 0$$

of $\mathscr{G}$ splits if and only if the corresponding short exact sequence of Galois modules splits:

$$0 \longrightarrow \mathscr{G}^\circ(\bar{K}) \longrightarrow \mathscr{G}(\bar{K}) \longrightarrow \mathscr{G}_{\text{ét}}(\bar{K}) \longrightarrow 0.$$

Remark 3.2.31. Note that the condition $e < p-1$ is essential for Theorem 3.2.28 to hold. Suppose that ζ_p is a primitive p-th root of unity in R. Then $\mu_{p,K}$ and $(\mathbb{Z}/p\mathbb{Z})_K$ become isomorphic as group schemes:

$$\frac{K[x]}{\langle x^p - 1\rangle} \cong \frac{K[x]}{\langle x-1\rangle} \times \frac{K[x]}{\langle x-\zeta_p\rangle} \times ... \times \frac{K[x]}{\langle x-\zeta_p^{p-1}\rangle}.$$

However, $\mu_{p,R}$ and $(\mathbb{Z}/p\mathbb{Z})_R$ are non-isomorphic prolongations (the former is non-reduced and the latter is étale).

3.2.9 Tate modules

Dual abelian varieties

Returning to the study of abelian varieties over a field k, we introduce the *dual abelian variety*. Let A be an abelian variety over k. For simplicity, we assume k is algebraically closed throughout. Consider the following morphisms:

$$\begin{array}{ccccc} & & A \times_k A & & \\ & \swarrow^{\mathrm{pr}_1} & \downarrow m & \searrow^{\mathrm{pr}_2} & \\ A & & A & & A \end{array}$$

which are given by projection onto the first coordinate, multiplication on A, and projection onto the second coordinate respectively. Let $\mathscr{L}$ be a line bundle on A. We say that $\mathscr{L}$ is *degree zero* if:

$$m^*\mathscr{L} \cong \mathrm{pr}_1^*\mathscr{L} \otimes \mathrm{pr}_2^*\mathscr{L}.$$

Denote by $\mathrm{Pic}^0(A) \subseteq \mathrm{Pic}(A)$ the degree 0 part of the Picard group. Roughly speaking, the dual abelian variety $A^\vee$ parametrises degree 0 line bundles on A. In particular, we would like there to be an isomorphism:

$$\mathrm{Pic}^0(A) \cong A^\vee(k).$$

Example 3.2.32. Let E/k be an elliptic curve. It is not hard to check that the notion of degree zero line bundle above coincides with the usual notion of degree of divisors on smooth curves:

$$\begin{aligned} \mathrm{Pic}(E) \cong \frac{\mathrm{Div}(E)}{\sim} &\xrightarrow{\deg} \mathbb{Z} \\ \left[\sum_i a_i P_i\right] &\longmapsto \sum_i a_i \end{aligned}$$

The isomorphism $E(k) \cong \mathrm{Pic}^0(E)$ in Example 3.2.5 (i) shows that $E \cong E^\vee$ i.e. elliptic

curves are *self-dual*.

The dual abelian variety $A^\vee$ is a solution to the moduli problem of parametrising families of degree 0 line bundles on A. As such, there is a universal line bundle $\mathscr{P}$ on $A \times A^\vee$ which parametrises all degree 0 line bundles on A. We make this precise with the following proposition:

Proposition 3.2.33. *Let A be an abelian variety over k of dimension g. Then there exists a pair $(A^\vee, \mathscr{P})$ where $A^\vee$ is a k-abelian variety of dimension g and $\mathscr{P}$ is a line bundle on $A \times A^\vee$. The pair is unique up to isomorphism as it is universal among pairs $(T, \mathscr{L})$ of k-schemes T and line bundles $\mathscr{L}$ on $A \times T$ such that:*

i) $\mathscr{L}|_{A\times\{t\}} \in \mathrm{Pic}^0(A \times \{t\})$ for all $t \in T$;

ii) $\mathscr{L}|_{\{0\}\times T}$ is trivial.

Namely, given such a pair $(T, \mathscr{L})$ there exists a unique morphism $\alpha : T \to A^\vee$ such that $(\mathrm{Id} \times \alpha)^* \mathscr{P} \cong \mathscr{L}$.

Proof. See [Mum74, II.8]. □

$\mathscr{P} \in \mathrm{Pic}(A \times A^\vee)$ is referred to as the *Poincaré bundle*. It is universal in the sense that, for any degree 0 line bundle $\mathscr{L} \in \mathrm{Pic}^0(A)$, there exists a unique point $a \in A^\vee(k)$ such that:

$$\mathscr{P}|_{A\times\{a\}} \cong \mathscr{L}.$$

As with Cartier duality, taking the dual of an abelian variety is functorial:

Proposition 3.2.34. *Let $f : A \to B$ be an isogeny of degree d with kernel N. Then there exists a dual isogeny $f^\vee : B^\vee \to A^\vee$ also of degree d such that $f \circ f^\vee = [d]_B$ and $f^\vee \circ f = [d]_A$. On points, $f^\vee$ is given by the pullback of invertible sheaves $f^* : \mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$. Moreover, the exact sequence:*

$$0 \to N \to A \xrightarrow{f} B \to 0$$

gives rise to a dual exact sequence:

$$0 \to N^\vee \to B^\vee \xrightarrow{f^\vee} A^\vee \to 0$$

where $N^\vee$ is the Cartier dual of N.

Proof. See [Mum74, p. 143]. □

Polarisations

Let A be an abelian variety over k and let $\bar{k}$ be an algebraic closure of k. Suppose that $\mathscr{L}$ is an ample line bundle on $A_{\bar{k}}$. Consider the map:

$$\begin{aligned} A(\bar{k}) &\longrightarrow \mathrm{Pic}^0(A_{\bar{k}}); \\ a &\longmapsto t_a^*\mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned}$$

where t_a is translation by a. By the theorem of the square, this is a group homomorphism. In fact, it is surjective and, as $\mathscr{L}$ is ample, this map has finite kernel $K(\mathscr{L})$. Taking the quotient by this subgroup, we obtain the dual abelian variety $A^\vee$. This motivates the following definition:

Definition 3.2.35. A *polarisation* $\lambda : A \to A^\vee$ is an isogeny such that, over $\bar{k}$, $\lambda_{\bar{k}}$ corresponds to a quotient of the above form with respect to an ample line bundle $\mathscr{L} \in \mathrm{Pic}(A_{\bar{k}})$. The *degree* of the polarisation is the degree of λ. A *principal polarisation* is a polarisation of degree 1.

Example 3.2.36.

i) As discussed in Example 3.2.32, elliptic curves always admit principal polarisations.

ii) Let C be a smooth, projective integral curve of genus g over k and suppose that $C(k)$ is non-empty. Then $\mathrm{Jac}(C)$ is principally polarised by any *theta divisor*.

Weil pairing

Duality of abelian varieties over k satisfies many good properties, in particular, it is a reflexive duality i.e. $A^{\vee\vee}$ is naturally isomorphic to A for any abelian variety. However, there is no 'good' duality pairing on $A \times A^\vee$. Instead, for each integer $m > 0$, we have the *Weil pairing*:

$$e_m : A[m](k^{\mathrm{sep}}) \times A^\vee[m](k^{\mathrm{sep}}) \longrightarrow \mu_m(k^{\mathrm{sep}});$$

It is defined as follows, for simplicity we assume k is algebraically closed. Let $a \in A[m](k)$ and $a' \in A^\vee[m](k)$ which we think of as a degree 0 divisor D of A. Then, as D is m-torsion, we have $[m]_A^*D \sim mD \sim 0$ in $\mathrm{Div}(A)$. Thus, there are rational functions $f, g \in k(A)$ such that:

$$mD = \mathrm{div}(f) \text{ and } [m]_A^*D = \mathrm{div}(g);$$

and:

$$\mathrm{div}(f \circ [m]_A) = [m]_A^*(\mathrm{div}(f)) = [m]_A^*(mD) = m([m]_A^*D) = \mathrm{div}(g^m).$$

Therefore, $\frac{g^m}{f \circ [m]_A}$ is a constant function $c \in k$ on A and so, for each $x \in A$ we have:

$$g(x+a)^m = cf(mx + ma) = cf(mx) = g(x)^m.$$

Finally, $\frac{g}{g \circ t_a}$ is an m-th root of unity in $k(A)$ and in particular is constant. We denote this constant by $e_m(a, a')$.

Tate modules

Definition 3.2.37. Let A be an abelian variety over a field k. Let $l > 0$ denote a prime that is invertible in k and consider the injective system:

$$... \leftarrow A[l^n](k^{\text{sep}}) \xleftarrow{\cdot l} A[l^{n+1}](k^{\text{sep}}) \leftarrow ...$$

We then define the l-adic *Tate module* associated to A as the injective limit:

$$T_l(A) := \varprojlim A[l^n](k^{\text{sep}}).$$

Note that the formation of this limit commutes with the action of $G_k = \text{Gal}(k^{\text{sep}}/k)$ and so there is a well-defined Galois action on the l-adic Tate module. Note also that, as an abstract abelian group, if $\dim(A) = g$ then:

$$A[l^n](k^{\text{sep}}) \cong (\mathbb{Z}/l^n\mathbb{Z})^{2g}$$

and so, as a $\mathbb{Z}_l$-module, we have an isomorphism:

$$T_l(A) \cong \mathbb{Z}_l^{2g}$$

Setting $\mathbb{Z}_l(1) := \varprojlim \mu_{l^n}$, we may extend the Weil pairings e_{l^n} to a pairing:

$$\begin{aligned} e_l : T_l(A) \times T_l(A^\vee) &\longrightarrow \mathbb{Z}_l(1); \\ ((a_n), (a'_n)) &\longmapsto (e_{l^n}(a_n, a'_n)). \end{aligned}$$

Remark 3.2.38. Suppose that k is of characteristic $p > 0$. Then there are no non-trivial p^n-th roots of unity so any bilinear pairing $e_{p^n} : A[p^n](k^{\text{sep}}) \times A^\vee[p^n](k^{\text{sep}}) \to \mu_{p^n}(k^{\text{sep}})$ for an abelian variety A/k will be trivial.

3.3 p-divisible groups and formal groups

3.3.1 p-divisible groups

Our main reference for the study of p-divisible groups will be [Tate67].

Definition 3.3.1. Let R be a commutative ring. Let p be a prime number, and $h \geq 0$ an

integer. A *p-divisible group over R of height h* is an inductive system:

$$G = (G_n, i_n)_{n \geq 0}$$

such that:

i) G_n is a finite R-group scheme of rank p^{nh};

ii) For each $n \geq 0$ the sequence:

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}$$

is exact (i.e. G_n is associated with the kernel of p^n on G_{n+1} via the map i_n).

Note that, for group schemes, this would imply:

$$G_n \cong (\mathbb{Z}/p^n\mathbb{Z})^h \text{ and } G = \varinjlim_n G_n \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h.$$

A *homomorphism* $f : G \to H$ of p-divisible groups $G = (G_n, i_n)$ and $H = (H_n, j_n)$ is a collection of homomorphisms $f_n : G_n \to H_n$ such that:

$$\begin{array}{ccc} G_n & \xrightarrow{i_n} & G_{n+1} \\ \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n+1}} \\ H_n & \xrightarrow[j_n]{} & H_{n+1} \end{array}$$

commutes for all $n \geq 1$.

Example 3.3.2. i) Let A be an abelian scheme over R of dimension g. Then the system $(A[p^n], i_n)$, where $i_n : A[p^n] \to A[p^{n+1}]$ is inclusion, gives the p-divisible group $A[p^\infty]$ of A. Note that it is of height $h = 2g$.

ii) The p-divisible group of the torus $\mathbb{G}_{m,R}$ is given by:

$$\mu_{p^\infty,R} = (\mu_{p^n,R}, i_{p^n});$$

where i_{p^n} is again just inclusion.

Formal Lie groups

Suppose that R is a complete, noetherian local ring with residue field k of characteristic $p > 0$.

Definition 3.3.3. A (commutative) *formal Lie group* Γ *over* R is a homomorphism $f : R[\![X_1, ..., X_n]\!] \to R[\![Y_1, ..., Y_n]\!] \widehat{\otimes}_R R[\![Z_1, ..., Z_n]\!]$ satisfying the following axioms:

Write $f = f(Y,Z) = (f_i(Y,Z))$ where each $f_i(Y,Z)$ is a formal power series in $2n$ variables. Then we require:

i) $X = f(X,0) = f(0,X)$;

ii) $f(X,f(Y,Z)) = f(f(X,Y),Z)$ (associativity);

iii) $f(X,Y) = f(Y,X)$ (commutativity).

We take $\Gamma = \mathrm{Spf}(R[\![X_1,...,X_n]\!])$ (cf. Def. 3.5.1). The formal group law given by f gives Γ the structure of a group object in the category of formal schemes over R. Write $X * Y = f(X,Y)$. Set $\psi(X) := X * ... * X$ (p times). This corresponds to multiplication by p on Γ. We say that Γ is *divisible* if $[p]_\Gamma : \Gamma \to \Gamma$ is an *isogeny* or equivalently, if $\psi : R[\![X_1,...,X_n]\!] \to R[\![X_1,...,X_n]\!]$ is a finite and free homomorphism. In this case, we let $\Gamma[p^\infty]$ denote the p-divisible group $(\Gamma[p^n], i_n)$ of p^n-torsion with the usual inclusion. Note that $\Gamma[p]$ is a *connected* finite group scheme and so is of rank p^h (Prop. 3.2.21).

Proposition 3.3.4. *Let R be a complete noetherian local ring with residue field k of characteristic $p > 0$. Then, the assignment $\Gamma \mapsto \Gamma[p^\infty]$ is an equivalence between the category of divisible, commutative formal Lie groups over R and the category of connected p-divisible groups over R.*

Proof. See [Tate67, 2.2 Prop. 1] □

Example 3.3.5. Let $\mathbb{G}_{m,R} = \mathrm{Spec}(R[x,x^{-1}])$ denote the multiplicative group over R with coordinate x. The formal completion of $\mathbb{G}_{m,R}$ at the identity section $e : \mathrm{Spec}(R) \to \mathbb{G}_{m,R}$ corresponding to $x = 1$ defines a formal Lie group $\hat{\mathbb{G}}_{m,R}$ (cf. Ex. 3.5.2). Setting $X = x - 1$, and noting that $x^{-1} = \frac{1}{1+X} = 1 - X + X^2 - ...$, we may write $\hat{\mathbb{G}}_{m,R} = \mathrm{Spf}(R[\![X]\!])$. Then, the associated formal group law is:

$$f(X,Y) = X + Y + XY = (x-1)(y-1) - 1.$$

Let $G = (G_n, i_n)$ be any p-divisible group over a complete noetherian local ring R, with residue field k of characteristic $p > 0$. The connected components G_n° determine a connected p-divisible group. By considering the connected-étale sequence of G_n (cf. Def. 3.2.19), we obtain an exact sequence of p-divisible groups:

$$0 \longrightarrow G^\circ \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0.$$

We define the *dimension* of G to be the dimension of the formal Lie group associated to G°.

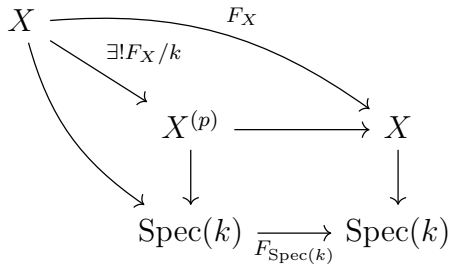
Frobenius and Verschiebung

Definition 3.3.6. Let X be a k-scheme where k is a perfect field of characteristic $p > 0$. The *absolute Frobenius morphism*:

$$F_X : X \longrightarrow X$$

is given by the identity on the topological space $|X|$, and the power of p map $x \mapsto x^p$ on the structure sheaf $\mathscr{O}_X$. Note that, in general this is not a morphism of k-schemes.

To obtain a morphism of k-schemes, we consider the following fibre product:



where $X^{(p)} = X \times_{F_{\mathrm{Spec}(k)}} \mathrm{Spec}(k)$ is the *Frobenius twist* of X. We call the morphism $F_{X/k} : X \to X^{(p)}$ the *relative Frobenius morphism*. Note that it is a purely inseparable, finite flat morphism of degree p.

Remark 3.3.7. Let k be a perfect field of characteristic $p > 0$. Let G/k be a finite commutative group scheme. The Frobenius twist $G^{(p)}$ is still a finite commutative group scheme, and the relative Frobenius $F_{G/k} : G \to G^{(p)}$ is a group homomorphism. Taking the Cartier dual $G^\vee$ we may also consider the relative Frobenius $F_{G^\vee/k} : G^\vee \to (G^\vee)^{(p)} \cong (G^{(p)})^\vee$. This corresponds dually to the *Verschiebung operator* $V_{G/k} : G^{(p)} \to G$.

Lemma 3.3.8. *Let G/k be a finite, commutative group scheme over a perfect field k of characteristic $p > 0$. Let $F_{G/k} : G \to G^{(p)}$ be the relative Frobenius morphism and $V_{G/k} : G^{(p)} \to G$ the Verschiebung operator. Then:*

$$V_{G/k} \circ F_{G/k} = [p] \quad \text{and} \quad F_{G/k} \circ V_{G/k} = [p];$$

i.e. the multiplication-by-p map on G and $G^{(p)}$ respectively.

Proof. See [Dem06, Prop., p. 29]. □

Note that if $G = (G_n, i_n)$ is a p-divisible group of height h, then so is $G^{(p)} := (G_n^{(p)}, i_n^{(p)})$. We then have induced morphisms of p-divisible groups:

$$\begin{array}{ccc} G & \xrightarrow{[p]} & G \\ {\scriptstyle F}\downarrow & \nearrow^{V} & \downarrow{\scriptstyle F} \\ G^{(p)} & \xrightarrow[[p]]{} & G^{(p)} \end{array} \qquad (\dagger)$$

where F and V are given by the Frobenius and Verschiebung respectively on G_v. The kernel of multiplication-by-p on G is given by G_1 and is of order p^h. Whereas the kernel of $F : G \to G^{(p)}$ is of order p^n where n is the dimension of G.

Duality for p-divisible groups

Let $G = (G_n, i_n)$ be a p-divisible group over R. We assume that each G_n is commutative so we may take the *Cartier dual* $G_n^\vee$ (cf. Def. 3.2.24). We define maps $i'_n : G_n^\vee \to G_{n+1}^\vee$ by taking the Cartier dual of the multiplication-by-p map $G_{n+1} \to G_n$. It is easy to check that $G^\vee = (G_n^\vee, i'_n)$ is a p-divisible group of the same height called the *dual* of G.

Proposition 3.3.9. *Let R be a complete noetherian local ring of residue characteristic $p > 0$. Let G be a p-divisible group over R of dimension n and height h. Then its dual $G^\vee$ is of dimension $h - n$.*

Proof. Dimension and height do not change after specialisation, so we may assume $R = k$ is a field of characteristic $p > 0$. By the diagram (†) we have an exact sequence:

$$0 \to \ker(F) \to \ker([p]) \to \ker(V) \to 0.$$

We have that $G_1 = \ker([p])$ has order p^h, and $\ker(F)$ has order p^n. Since $F_{G_v/k}$ and $V_{G_v/k}$ are dual morphisms, it follows that $\ker(V)^\vee$ is given by the cokernel of:

$$F_{G_1^\vee/k} : G_1^\vee \longrightarrow (G_1^\vee)^{(p)} \cong (G_1^{(p)})^\vee$$

and consequently has order p^{h-n}. □

Example 3.3.10. i) The p-divisible group μ_∞ has $h = n = 1$. Its dual is the étale p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$ which has $h = 1$ and $n = 0$.

ii) Let A be an abelian scheme over R of dimension g. Suppose that its dual $A^\vee$ exists over R. Then we have that:

$$(A[p^\infty])^\vee \cong (A^\vee)[p^\infty]$$

namely, the formation of duality of p-divisible groups commutes with duality of abelian schemes. Both $A[p^\infty]$ and $(A^\vee)[p^\infty]$ have height $2g$ and dimension g.

Moreover, the connected component $A[p^\infty]^\circ$ is the formal completion of A along the identity section e. The height of $A[p^\infty]^\circ$ coincides with the *p-rank* of A (cf. Prop. 3.2.7). We may interchange between the notation $\hat{A}$ and $A[p^\infty]^\circ$ to refer to the same object depending on the context.

Galois representations of p-divisible groups

Let R be a complete discrete valuation ring, with residue field $k = R/\mathfrak{m}$ of characteristic $p > 0$, and let K be the field of fractions of R. Let L be the completion of an algebraic extension of K and let S be the ring of integers of L. S is a complete valuation ring but the valuation on S may not be discrete. Let G be a p-divisible group over R. We define $G(S)$ the group of S-points of G to be:

$$G(S) := \varprojlim_i G(S/\mathfrak{m}^i S) \quad \text{where} \quad G(S/\mathfrak{m}^i S) := \varinjlim_n G_n(S/\mathfrak{m}^i S).$$

This gives $G(S)$ the structure of a $\mathbb{Z}_p$-module. Note that, by construction, the p^n-torsion subgroup of $G(S)$ is given by $\varprojlim_i G_n(S/\mathfrak{m}^i S) \cong G_n(S)$ and so the full torsion subgroup of $G(S)$ is given by $G(S)[\infty] \cong \varinjlim_n G_n(S)$.

Remark 3.3.11. If G is an étale p-divisible group over R, then the maps $G_n(S/\mathfrak{m}^{i+1}S) \to G_n(S/\mathfrak{m}^i S)$ are bijective for each i, and thus $G(S)$ is a torsion group.

On the other hand, if G is a connected p-divisible group associated to some formal Lie group Γ on $R[\![X_1, ..., X_n]\!]$ then $G(S)$ is an analytic group over L, which is given by points $(x_1, ..., x_n)$ where x_i lie in the maximal ideal of S (as a set).

Example 3.3.12.

i) If $G = \mathbb{G}_{m,R}[p^\infty]$, then $G(S)$ is the group of units of S congruent to 1.

ii) If A is an abelian scheme over R and $G = A[p^\infty]$, then $G(S) \subset A(S)$ is the subgroup of points whose reduction modulo the maximal ideal is a p-primary torsion point. Moreover, $G^\circ(S)$ is associated with the kernel of the reduction map.

The Galois modules associated to a p-divisible group

Keeping the notation of the previous section, we now let $\bar{K}$ be an algebraic closure of K. We define:

$$G(\bar{K}) := \varprojlim_n G_n(\bar{K}) \text{ with respect to } i_n : G_n \hookrightarrow G_{n+1};$$

$$T(G) := \varinjlim_n G_n(\bar{K}) \text{ with respect to } G_{n+1} \xrightarrow{\cdot p^n} G_n.$$

As $\mathrm{char}(K) = 0$, the group schemes $(G_n)_K$ are étale (Cor. 3.2.22), and so $G(\bar{K})$ and $T(G)$ are isomorphic to the $\mathbb{Z}_p$-modules $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ and $\mathbb{Z}_p^h$ respectively, where h is the height of G, both with a continuous G_K-action. Note that, as $\mathrm{Gal}(\bar{K}/K)$-modules they determine each other:

$$G(\bar{K}) \cong T(G) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \text{ and } T(G) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, G(\bar{K})).$$

Example 3.3.13. Let A/R be an abelian scheme of dimension g and G the p-divisible group of A. Then $T(G) = T_p(A_K)$; the p-adic Tate module of A_K (cf. 3.2.38).

We state without proof the main results on Galois representations associated to p-divisible groups:

Theorem 3.3.14. *Let R be an integrally closed, noetherian domain, with fraction field K of characteristic 0. Let G and H be p-divisible groups over R. Then any homomorphism $f : G \otimes_R K \to H \otimes_R K$ extends uniquely to a homomorphism $G \to H$.*

Proof. See [Tate67, 4.2]. □

Corollary 3.3.15. *The natural map:*

$$\mathrm{Hom}(G, H) \longrightarrow \mathrm{Hom}_{G_K}(T(G), T(H));$$

is a bijection.

This follows as the module $T(G)$ is determined by the generic fibre of the p-divisible group G.

Remark 3.3.16. These results should be viewed in conjuction with corresponding statement about prolongations of group schemes (cf. Theorem 3.2.28). Note that we don't require any conditions on ramification when the above theorem is applied to a local ring.

3.3.2 The p-divisible group of an elliptic curve

Let E/k be an elliptic curve over a separably closed field k of characteristic $p > 0$. Recall that the geometric p^n-torsion is given by $E[p^n](\bar{k}) \cong (\mathbb{Z}/p^n\mathbb{Z})^i$ where i is the p-rank of E. In particular, if $i = 1$ we say that E is *ordinary* and if $i = 0$ we say that p is *supersingular* (Def. 3.2.8). By contrast, the multiplication-by-p^n map is a finite flat morphism of degree p^{2n}, and so we know that, as a finite commutative group scheme, $E[p^n]$ still has rank p^{2n} and thus has some non-reduced connected component.

Theorem 3.3.17. *Let E/k be an elliptic curve over a separably closed field k of characteristic $p > 0$. Then the p-divisible group $E[p^\infty]$ is given by:*

i) The split exact sequence:

$$0 \to \mu_{p^\infty,k} \to E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0;$$

where $\mu_{p^\infty,k}$ is the p-divisible group of $\mathbb{G}_{m,k}$ (Example 3.3.2 (ii)), when E is ordinary.

ii) When E is supersingular, its p-divisible group $E[p^\infty]$ is connected, of height 2 and dimension 1 and so coincides with the formal group of E. In the Dieudonné-Manin classification, it is given by the p-divisible group $G_{1,1}$ [Man63].

Corollary 3.3.18. *The p-torsion group scheme $E[p]$ is given by:*

i) The split exact sequence:

$$0 \to \mu_{p,k} \to E[p] \to \mathbb{Z}/p\mathbb{Z} \to 0;$$

when E is ordinary.

ii) The unique non-split, self-dual exact sequence:

$$0 \to \alpha_{p,k} \to E[p] \to \alpha_{p,k} \to 0$$

when E is supersingular. Moreover, one can associate $E[p] \cong \ker(F^{(2)}_{E/k})$.

The supersingular case is most easily seen by the theory of Dieudonné modules which we will not explore here (see for example [Dem06]). We already have enough tools to illustrate the ordinary case however. Let E/k be an ordinary elliptic curve and consider its connected-étale sequence:

$$0 \to E[p]^\circ \to E[p] \to E[p]^{\text{ét}} \to 0.$$

As the p-rank of E is 1, we see that both $E[p]^\circ$ and $E[p]^{\text{ét}}$ are of rank p. As k is separably closed, $E[p]^{\text{ét}}$ is a constant group scheme so must be $\mathbb{Z}/p\mathbb{Z}$. Now, $E \cong E^\vee$ is self dual as an abelian variety (Ex. 3.2.32), and so $E[p] \cong E[p]^\vee$ is isomorphic to its Cartier dual (Prop. 3.2.34). Taking the Cartier dual commutes with finite products, thus $E[p]$ contains a copy of $(\mathbb{Z}/p\mathbb{Z})^\vee \cong \mu_{p,k}$ (Lemma 3.2.25). Thus we see that $E[p]^\circ \cong \mu_{p,k}$.

The same argument holds to show that $E[p^n] \cong \mu_{p^n,k} \times \mathbb{Z}/p^n\mathbb{Z}$ (the only abelian group of order p^n is given by $\mathbb{Z}/p^n\mathbb{Z}$ and it is clear from the description in Lemma 3.2.25 that it is dual to $\mu_{p^n,k}$) and thus we have determined the p-divisible group.

3.4 Geometry of curves in characteristic $p > 0$

3.4.1 Frobenius and differentials

Let k be an algebraically closed field of characteristic $p > 0$. The following discussion on differentials in positive characteristic and the Cartier operator can be found in [Il79] or [Bri-Kum07]. Let X/k be a smooth variety of dimension n. Recall that, the sheaf of Kähler differentials $\Omega^1_{X/k}$ on X/k is a locally free sheaf of rank n. Setting $\Omega^i_{X/k} := \bigwedge^i(\Omega^1_{X/k})$ to be the sheaf of *i-forms*, we obtain the (*algebraic*) *de Rham complex*:

$$\Omega^\bullet_{X/k} = \left[0 \to \mathscr{O}_X \xrightarrow{d} \Omega^1_{X/k} \xrightarrow{d} ... \xrightarrow{d} \Omega^n_{X/k} \to 0\right]$$

where in regular local coordinates $t_1, ..., t_n$, the derivative $\mathscr{O}_X \xrightarrow{d} \Omega^1_{X/k}$ is given by:

$$d(f(t_1, ..., t_n)) = \frac{\partial f}{\partial t_1} dt_1 + ... + \frac{\partial f}{\partial t_n} dt_n.$$

In fact, $\bigoplus_{i \geq 0} \Omega^i_{X/k}$ becomes a differential graded algebra under the wedge product:

$$\wedge : \Omega^i_{X/k} \otimes \Omega^j_{X/k} \to \Omega^{i+j}_{X/k};$$

where we note the following equality for local i-forms ω and j-forms η:

$$d(\omega \wedge \eta) = d\omega \wedge \eta + (-1)^i \omega \wedge d\eta.$$

Of course, the derivative d is not $\mathscr{O}_X$-linear; simply because of the Leibniz rule:

$$d(fg) = df \cdot g + f \cdot dg;$$

for local sections f, g. However, in positive characteristic, a striking feature of differentials is that they are $\mathscr{O}^p_X$-linear. Namely, if t is a local coordinate then we have the equality: $d(t^p) = pt^{p-1} = 0$ and more generally $d(f^p) = 0$ for a local section of $\mathscr{O}^p_X$. Thus, we see that, if ω is a local i-form and f a local section then:

$$d(f^p \omega) = d(f^p) \wedge \omega + f^p d\omega = f^p d\omega$$

We may phrase this linearity more concretely in terms of the relative Frobenius (Def. 3.3.6). Recall that if S is an $\mathbb{F}_p$-scheme, then the *absolute Frobenius* $F_S : S \to S$ is given by the identity on topological spaces, and the p-th power map on $\mathscr{O}_S$. Let $S = \mathrm{Spec}(k)$. Then the *Frobenius twist* $X^{(p)}$ of X is the fibre product $X^{(p)} = X \times_{F_S} S$. The relative Frobenius morphism $F_{X/k} : X \to X^{(p)}$ is the unique morphism of k-schemes induced by F_X.

Example 3.4.1. Let $X = \mathbb{A}^n_k = \mathrm{Spec}(k[t_1, ..., t_n])$. Then $X^{(p)} = \mathrm{Spec}(k[t_1^{(p)}, ..., t_n^{(p)}])$ for

some coordinates $t_i^{(p)}$ where $F_{X/k} : \mathbb{A}_k^n \longrightarrow \mathbb{A}_k^n$ is given by:

$$(t_1, ..., t_n) \longmapsto (t_1^p, ..., t_n^p) = (t_1^{(p)}, ..., t_n^{(p)}).$$

Suppose we have closed subscheme $Y \subseteq X$ with ideal generated by the polynomials $f_1, ..., f_m \in k[t_1, ..., t_n]$. If we express a polynomial in $f \in k[t_1, ..., t_n]$ as $f = \sum_{I \in \mathbb{N}^n} a_I t^I$, we define:

$$f^{(p)} := \sum_{I \in \mathbb{N}^n} a_I^p t^I;$$

so that:

$$Y^{(p)} = \{f_1^{(p)} = 0\,, ...\,, f_m^{(p)} = 0\} \quad \text{and} \quad F_{Y/k} = F_{X/k}|_Y.$$

Let $F_{X/k} : (X, \mathscr{O}_X) \to (X^{(p)}, \mathscr{O}_{X^{(p)}})$ be the relative Frobenius morphism. The natural morphism $\mathscr{O}_{X^{(p)}} \to (F_{X/k})_* \mathscr{O}_X$ allows us to view any $(F_{X/k})_* \mathscr{O}_X$-module as an $\mathscr{O}_{X^{(p)}}$-module.

Lemma 3.4.2. *Let k be an algebraically closed field of characteristic $p > 0$. Let X be a smooth k-variety of dimension n and let $F_{X/k} : X \to X^{(p)}$ be the relative Frobenius morphism.*

i) $F_{X/k}$ is a purely inseparable, finite, flat morphism of degree p^n.

ii) $(F_{X/k})_* \mathscr{O}_X$ is a locally free $\mathscr{O}_{X^{(p)}}$-module of rank p^n.

Proof. i) In fact, the relative Frobenius morphism is finite for any finite type k-scheme [stacks-project, Lemma 33.36.8]. By so-called 'miracle flatness' [Mats89, §23], X is regular so $F_{X/k}$ is flat.

ii) By [Mats89, Thm. 7.10], a flat and finite morphism is locally free. □

Let X be a regular k-variety of dimension n and $t_1, ..., t_n$ be local regular coordinates. To avoid confusion between local sections of $\mathscr{O}_X$ and $\mathscr{O}_{X^{(p)}}$, if f is a local section of $\mathscr{O}_X$ we write $f \otimes 1$ for the corresponding section of $\mathscr{O}_{X^{(p)}} = \mathscr{O}_X \otimes_{F_S} \mathscr{O}_S$. (ii) implies that any local section f of $\mathscr{O}_X$ has a unique expression:

$$f = \sum_{\substack{0 \le i < p \\ 1 \le j \le n}} f_{ij}^p t_j^i$$

for local sections f_{ij} of $\mathscr{O}_X$. Consider the de Rham complex $\Omega^\bullet_{X^{(p)}/k}$ of the Frobenius twist $X^{(p)}$. As $F_{X/k}$ is locally free, by pushing forward we obtain a complex of locally free $\mathscr{O}_{X^{(p)}}$-modules:

$$(F_{X/k})_* \Omega^\bullet_{X/k} = \left[0 \to (F_{X/k})_* \mathscr{O}_X \to (F_{X/k})_* \Omega^1_{X/k} \to ... \to (F_{X/k})_* \Omega^n_{X/k} \to 0\right].$$

By our previous discussion, the derivative maps in this complex are $\mathscr{O}_{X^{(p)}}$-linear and we can take cohomology to obtain the coherent $\mathscr{O}_{X^{(p)}}$-modules:

$$\mathscr{H}^i\left((F_{X/k})_*\Omega^\bullet_{X/k}\right).$$

Theorem 3.4.3 (Cartier isomorphism)**.** *Let k be an algebraically closed field of characteristic $p > 0$ and let X/k be a regular variety of dimension n. Then for $0 \leq i \leq n$ we have an isomorphism of coherent $\mathscr{O}_{X^{(p)}}$-modules:*

$$\mathscr{C}^{-1} : \Omega^i_{X^{(p)}/k} \longrightarrow \mathscr{H}^i\left((F_{X/k})_*\Omega^\bullet_{X/k}\right);$$

where, for a local section x of $\mathscr{O}_X$ we denote by $x \otimes 1$ the corresponding section of $\mathscr{O}_{X^{(p)}}$, and $\mathscr{C}^{-1}$ is the unique $\mathscr{O}_X^{(p)}$-linear morphism satisfying:

$$\mathscr{C}^{-1}(d(x \otimes 1)) = [x^{p-1}dx].$$

In fact, $\mathscr{C}^{-1}$ defines a well defined isomorphism of graded $\mathscr{O}_{X^{(p)}}$-algebras:

$$\mathscr{C}^{-1} : \bigoplus_{i=0}^{n} \Omega^i_{X^{(p)}/k} \longrightarrow \bigoplus_{i=0}^{n} \mathscr{H}^i\left((F_{X/k})_*\Omega^\bullet_{X/k}\right).$$

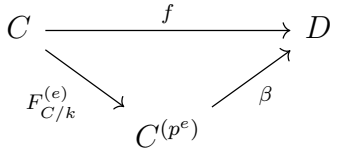
We refer to the inverse $\mathscr{C}$ as the Cartier isomorphism*.*

Proof. See [Il79, §2]. □

3.4.2 The Cartier operator

Let C be a smooth, complete curve over an algebraically closed field k of characteristic $p > 0$. Let $F_{C/k} : C \to C^{(p)}$ be the relative Frobenius of C. As discussed, $F_{C/k}$ is finite, flat and purely inseparable of degree p. In fact, the Frobenius is the prototypical inseparable map of curves in the following sense:

Proposition 3.4.4. *Let k be an algebraically closed field of characteristic $p > 0$ and let $f : C \to D$ be a finite morphism of smooth, projective curves over k. Then there exists an integer $e \geq 0$ and a finite, generically étale map $\beta : C^{(p^e)} \to D$ such that:*



commutes.

Proof. As the curves are smooth and projective, there is a (contravariant) equivalence between finite morphisms and finite field extensions, so we may work with functions fields.

There exists an intermediate field extension $k(C)/K/k(D)$ such that $k(C)/K$ is purely inseparable of degree p^e say, and $K/k(D)$ is separable. Precisely, K is the separable closure of $k(D)$ in $k(C)$. Then, the field extension $k(C)/K$ correspond to the e-th iterate of the Frobenius $F^{(e)}_{C/k} : C \to C^{(p^e)}$. The extension $K/k(D)$ is separable so that the corresponding morphism $C^{(e)} \to D$ is generically étale. □

More generally, when C and D are integral but not necessarily smooth over k, one can still write $[k(C) : k(D)] = [k(C) : K] \cdot [K : k(D)]$ where $k(C)/K$ is purely inseparable and $K/k(D)$ is separable. This motivates the following definition:

Definition 3.4.5. Let k be an algebraically closed field of characteristic $p > 0$ and let $f : C \to D$ be a finite morphism of integral curves. Then we may decompose the degree:

$$\deg(f) = \text{insep.deg}(f) \cdot \text{sep.deg}(f)$$

into the *(purely) inseparable degree* and *separable degree* respectively. When C and D are smooth, this comes from the unique decomposition:

$$f : C \xrightarrow{F^{(e)}_{C/k}} C^{(p^e)} \xrightarrow{\beta} D.$$

Note that $\text{insep.deg}(f) = p^e$ is always a power of p.

We note the following easy corollary:

Corollary 3.4.6. *Suppose that $f : C \to D$ is a finite morphism of smooth curves over an algebraically closed field of characteristic $p > 0$, and that $\deg(f)$ is coprime-to-p. Then f is generically étale (separable).*

Let $\Omega^1_{C/k}$ be the sheaf of Kähler differentials. Then the algebraic de Rham complex is given by:

$$0 \to \mathscr{O}_C \xrightarrow{d} \Omega^1_{C/k} \to 0.$$

The Cartier isomorphism is then given by:

$$\mathscr{C} : \text{coker}\left((F_{C/k})_*\mathscr{O}_C \xrightarrow{d} (F_{C/k})_*\Omega^1_{C/k}\right) \xrightarrow{\sim} \Omega^1_{C^{(p)}/k}.$$

Composing $\mathscr{C}$ with the natural map

$$(F_{C/k})_*\Omega^1_{C/k} \to \text{coker}\left((F_{C/k})_*\mathscr{O}_C \xrightarrow{d} (F_{C/k})_*\Omega^1_{C/k}\right)$$

we obtain the *Cartier operator*:

Definition 3.4.7. Let k be an algebraically closed field of characteristic $p > 0$. Let C/k be a complete, non-singular curve. The *Cartier operator* is the morphism of locally free

$\mathscr{O}_{C^{(p)}}$-modules:

$$\mathscr{C} : (F_{C/k})_* \Omega^1_{C/k} \longrightarrow \Omega^1_{C^{(p)}/k};$$

where, if t is a local coordinate of C, $t^{(p)}$ the corresponding local coordinate of $C^{(p)}$, and f a local section of $\mathscr{O}_C$ then there is a unique expression:

$$f = f_0^p + f_1^p t + ... + f_{p-1}^p t^{p-1};$$

for local sections f_i. Thus, for a local section $f \cdot dt$ of $\Omega^1_{C/k}$ we have:

$$\mathscr{C}(f \cdot dt) = (f_{p-1} \otimes 1) \cdot dt^{(p)}.$$

Remark 3.4.8. In the literature, the terms *Cartier operator* and *Cartier isomorphism* are often used interchangeably. We make the distinction between the two here; that the Cartier operator is the morphism of line bundles above. It is only defined for curves and is not in general an isomorphism.

3.4.3 Lifts of Frobenius

Let k be an algebraically closed field of characteristic $p > 0$ and let C_0/k be a smooth, complete curve of genus g. Let $W_2(k)$ denote the Witt vectors of length 2. Recall that by a *lift* of C_0 to $W_2(k)$ we mean a flat morphism $C_1 \to \mathrm{Spec}(W_2(k))$ such that $C_1 \times_{W_2(k)} k \cong C_0$ (cf. 3.5.2). Similarly, by a *lift of Frobenius*, we will mean a morphism $F_1 : C_1 \to D_1$ between flat R_1-schemes that restricts to $F_{C_0/k}$. There is a key relationship between liftings of Frobenius and the Cartier operator:

Proposition 3.4.9. *Let k be an algebraically closed field of characteristic $p > 0$ and let C_0/k be a smooth, complete curve. Then liftings of the Frobenius $F_{C_0/k} : C_0 \to C_0^{(p)}$ corrsepond to sections of the Cartier operator $\mathscr{C} : (F_{C_0/k})_* \Omega^1_{C_0/k} \to \Omega^1_{C_0^{(p)}/k}$. Namely, given a morphism $F_1 : C_1 \to D_1$ between flat R_1-schemes that restrict to $F_{C_0/k}$, there exists a morphism line bundles:*

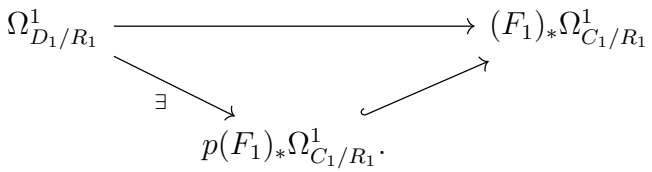
$$\tau : \Omega^1_{C_0^{(p)}/k} \longrightarrow (F_{C_0/k})_* \Omega^1_{C_0/k}$$

such that $\tau \circ \mathscr{C}$ is the identity.

Proof. The following calculations can be gleaned from [Maz73]. Suppose that x_1 is a local section of $\mathscr{O}_{D_1}$. By flatness, we may write $F_1^*(x_1) = x_1^p + p \cdot y_1$ for a local section y_1 of $\mathscr{O}_{C_1}$ (cf. Lemma 3.5.5). Thus, if $x_1 \cdot dt_1$ is a local section of $\Omega^1_{D_1/R_1}$, the derivative of F_1 is given by:

$$\begin{aligned} &\Omega_{D_1/R_1} \longrightarrow (F_1)_* \Omega_{C_1/R_1}; \\ &x_1 \cdot ds_1 \longmapsto F^*(x_1)(p s_1^{p-1} \cdot ds_1 + p \cdot dy_1), \end{aligned}$$

and so we have a factorisation:



Again, by flatness, we may associate the modules $p(F_1)_*\Omega^1_{C_1/R_1}$ and $(F_{C_0/k})_*\Omega^1_{C_0/k}$ and so obtain a morphism of sheaves:

$$\tau : \Omega_{C_0^{(p)}/k} \longrightarrow (F_{C_0/k})_*\Omega^1_{C_0/k}$$

By the local calculations above, if $(x_0 \otimes 1) \cdot dt_0^{(p)}$ is a local section of $\Omega_{C_0^{(p)}/k}$ then $\tau((x_0 \otimes 1) \cdot dt_0^{(p)}) = x_0^{p-1} \cdot dt_0$. By the local expression in Def. 3.4.7, it is easy to see that $\tau \circ \mathscr{C}$ is the identity. □

Raynaud employs this fact in [Ray83-2] to show that the Frobenius cannot be lifted on higher genus curves:

Corollary 3.4.10. *Suppose that C_0/k is a complete non-singular curve of genus $g \geq 2$. Then the Frobenius on C_0 cannot be lifted.*

Proof. The line bundles $\Omega_{C_0^{(p)}/k}$ and $(F_{C_0/k})_*\Omega^1_{C_0/k}$ are of degree $2g-2 > 0$ and $p(2g-2) > 0$ respectively. Thus, if the composition:

$$0 \to (F_{C_0/k})_*\Omega^1_{C_0/k} \xrightarrow{\mathscr{C}} \Omega_{C_0^{(p)}/k} \xrightarrow{\tau} (F_{C_0/k})_*\Omega^1_{C_0/k} \to 0$$

is the identity, then $\mathscr{C}$ is a monomorphism between sheaves of strictly decreasing degree, which is a contradiction. □

Remark 3.4.11. Let k be a perfect field and X_0/k a non-singular variety. Let $F_{X_0} : X_0 \to X_0$ denote the absolute Frobenius and let $F_{X_0/k} : X_0 \to X_0^{(p)}$ denote the relative Frobenius. Suppose that there exists a flat lifting X_1 over $S_1 := \mathrm{Spec}(W_2(k))$ of X_0 over $S_0 := \mathrm{Spec}(k)$. If there exists an endomorphism $F_1 : X_1 \to X_1$ extending the *absolute* Frobenius F_0, then we may take $X_1' := X_1 \times_{\varphi_1} S_1$ where $\varphi_1 : (a_0, a_1) \mapsto (a_0^p, a_1^p)$ lifts the Frobenius on k to $W_2(k)$ and there exists a unique morphism $X_1 \to X_1'$ lifting the relative Frobenius induced by F_1.

On the other hand, as k is perfect, there is an inverse φ_1^{-1} to the Frobenius on $W_2(k)$. Then, we may similarly associated $X_1 = X_1' \times_{\varphi_1^{-1}} S_1$ and so we see that lifts of the absolute Frobenius correspond to lifts of the relative Frobenius by symmetry. Thus we may interchange these notions.

3.5 Mixed characteristic deformation theory

We state (mostly without proof) the requisite facts from deformation theory used to deform a characteristic $p > 0$ variety or morphism to characteristic p^2 or to characteristic 0. The main reference will be [Har10].

3.5.1 Formal schemes

Let A be a noetherian ring and I an ideal. Recall that (cf. 3.1.1) the I-adic completion of A is given by the inverse system:

$$\hat{A} = \varprojlim \left(A/I \leftarrow A/I^2 \leftarrow ... \right).$$

Consider the corresponding affine scheme $X = \mathrm{Spec}(A)$ and closed subscheme $Y = \mathrm{Spec}(A/I)$. We can consider the corresponding sequence of spaces:

$$Y \hookrightarrow Y_1 \hookrightarrow Y_2 \hookrightarrow ...$$

where $Y_n := \mathrm{Spec}(A/I_n)$. These all have the same underlying topological space. We define the *formal completion* of X along Y to be the locally ringed space:

$$\hat{X} = \mathrm{Spf}(A) := \varinjlim Y_n.$$

The sheaf $\mathscr{O}_{\hat{X}}$ is defined on opens $D_f \subset X$ by:

$$\mathscr{O}_{\hat{X}}(D_f) := \varprojlim (A/I_n)_f.$$

More generally, for a noetherian scheme X and a closed subscheme Y, with sheaf of ideals $\mathscr{I}$, we define the *formal completion* of X along Y to be the locally ringed space $(\hat{X}, \mathscr{O}_{\hat{X}})$ where:

$$\mathscr{O}_{\hat{X}} := \varprojlim \mathscr{O}/\mathscr{I}^n.$$

Definition 3.5.1. A (noetherian) *formal scheme* $(\mathscr{X}, \mathscr{O}_{\mathscr{X}})$ is a locally ringed space admitting a finite open cover $\{\mathscr{U}_i\}$ such that, for each i, the pair $(\mathscr{U}_i, \mathscr{O}_{\mathscr{X}}|_{\mathscr{U}_i})$ is isomorphic to the completion of some noetherian scheme X_i along a closed subscheme Y_i. We say that $(\mathscr{X}, \mathscr{O}_{\mathscr{X}})$ is *algebraisable* if it arises as the completion of a single noetherian scheme along a closed subscheme.

Example 3.5.2. i) Let X be a noetherian scheme and x a closed point. Then $\hat{X}$ is topologically a one-point space with structure sheaf given by the completion of the local ring $\widehat{\mathscr{O}_{X,p}}$.

ii) Let A be an abelian variety over an algebraically closed field k and let $e \in A(k)$ be the identity section. The *formal Lie group* associated to A which we denote by Γ, is the completion of A along e. As A is smooth and projective, we have that:

$$\widehat{\mathscr{O}_{A,e}} \cong k[\![t_1, ..., t_g]\!];$$

where t_i are regular coordinates for A and g is the dimension. The multiplication map $m : A \times_k A \to A$ then induces, after passing to the completion, a formal group law:

$$f : k[\![x_1, ..., x_g]\!] \to k[\![s_1, ..., s_g]\!] \hat{\otimes}_k k[\![t_1, ..., t_g]\!].$$

This is called the *formal (Lie) group* attached to A. Note that, as in (i), $\mathrm{Spf}(\widehat{\mathscr{O}_{\mathrm{A,e}}})$ is just a point, so all the information of the formal Lie group is contained in the formal power series f.

We can carry through many of the usual definitions from schemes to formal schemes. We state some definitions that we will use later in our discussion of deformation theory:

Definition 3.5.3. Let X be a noetherian scheme, and Y a closed subscheme with corresponding ideal sheaf $\mathscr{I}$. Let $\hat{X}$ denote the formal completion of X along Y. Let $\mathscr{X}$ be a more general noetherian formal scheme.

i) Let $\mathscr{F}$ be a coherent sheaf on X. We define the *formal completion* of $\mathscr{F}$ along Y to be the sheaf on Y:

$$\widehat{\mathscr{F}} := \varinjlim_n \mathscr{F}/\mathscr{I}^n\mathscr{F}.$$

ii) A sheaf of $\mathscr{O}_{\mathscr{X}}$-modules $\mathscr{G}$ is said to be *coherent* if there exists some open cover $\hat{X}_i$ of formal completions of noetherian schemes (along some closed subscheme) such that $\mathscr{G}|_{\hat{X}_i} = \widehat{\mathscr{F}_i}$ for some coherent sheaf $\mathscr{F}_i$ of $\mathscr{O}_{X_i}$ modules.

3.5.2 Flat liftings

Let R be a complete DVR with uniformiser π, residue field $k = R/\pi$ of characteristic $p > 0$ and fraction field K of characteristic. We are mainly interested in the case $R = W(k)$ where we can take $p = \pi$. For each $n > 0$, we define the truncated rings $R_n := R/\pi^{n+1}R$. These are artinian local rings with residue field k.

Let X_0/k be a smooth, proper variety over k. By a *lifting* of X_0 to *order* n we will mean a flat scheme X_n/R_n such that $(X_n)_k \cong X_0$. Such liftings are referred to as *infinitesimal liftings* as the X_n are identical as topological spaces, but differ in their nilpotent structures as schemes. Suppose we have liftings X_n/R_n for each n and that they

are compatible in the sense that:

$$(X_{n+1})_{R_n} \cong X_n,$$

for each n. This then defines a formal scheme $\mathscr{X} := \varprojlim_n X_n$. We say that a flat scheme X/R is a *lifting* of X_0/k if $X_k \cong X_0$. Equivalently, $\mathscr{X}$ is *algebraisable* and $\mathscr{X} \cong \hat{X}$; the *formal completion* of X along the closed subscheme X_k (cf. Def. 3.5.1).

Given such a family $X \to \mathrm{Spec}(R)$, we have a flat deformation between the special fibre X_0 and the generic fibre X_K. We say that these two schemes are *deformation equivalent*. This gives the following diagram:

$$\begin{array}{ccc} X_0 & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k) & \longrightarrow & \mathrm{Spec}(R) \end{array} .$$

As X is flat over R, the fibres share certain properties like dimension and arithmetic genus, however, they can differ in subtle ways and other invariants do not tend to be preserved. We first note the criterion for flatness over R_1. Recall that a module M_1 over R_1 is flat if and only if the functor $- \otimes_{R_1} M_1$ is exact. It is automatically right exact, so one needs to only check if it preserves monomorphisms. The following lemma shows that we need only consider the exact sequence of R_1-modules:

$$0 \to \pi R_1 \longrightarrow R_1 \longrightarrow k \to 0.$$

Remark 3.5.4. If R is the ring $k[\![\pi]\!]$ then, $R_1 = \frac{k[\pi]}{\pi^2} =: k[\epsilon]$ gives the *dual numbers* over k and the exact sequence:

$$0 \longrightarrow \epsilon k[\epsilon] \longrightarrow k[\epsilon] \longrightarrow k \longrightarrow 0,$$

splits via the section $k \to k[\epsilon]$; $1 \mapsto 1 + 0 \cdot \epsilon$. On the other hand, if k has characteristic $p > 0$ and $R = W(k)$ then $R_1 = W_2(k)$ and the exact sequence:

$$0 \to pW_2(k) \longrightarrow W_2(k) \longrightarrow k \to 0$$

cannot split as there are no ring homomorphisms from k to $W_2(k)$. (The former is of characteristic p whereas the latter is of characteristic p^2). Note that, in either case we have an isomorphism of R_1-modules:

$$\begin{aligned} k &\longrightarrow \pi R_1; \\ a_0 &\longmapsto \pi \cdot a_1, \end{aligned}$$

where a_1 is any element of R_1 such that $a_1 \equiv a_0 \pmod{\pi}$.

Lemma 3.5.5. *Let M_1 be an R_1-module and $M_0 = M_1 \otimes_{R_1} k \cong M_1/\pi M_1$. Then M_1 is flat if and only if the natural map:*

$$M_0 \cong M_1/\pi M_1 \xrightarrow{\pi} M_1;$$
$$x + \pi M \mapsto \pi x$$

is injective. Equivalently, we can identify M_0 as the submodule $\pi M_1 \subseteq M_1$.

Proof. Recall that M_1 is flat if and only if $\mathrm{Tor}_1^{R_1}(M_1, N) = 0$ for all R_1-modules N. By the local criterion for flatness [Har10, Lemma 2.1] as R_1 is noetherian it is sufficient to check this for $N = R_1/\mathfrak{p}$ for every prime ideal $\mathfrak{p} \subset R_1$. However, the only prime ideal of R_1 is generated by π so M_1 is flat if and only if $M_1 \otimes -$ preserves flatness of the following exact sequence:

$$0 \to k \xrightarrow{\pi} R_1 \to k \to 0;$$

i.e. if and only if the following sequence is exact:

$$0 \to M_0 \xrightarrow{\pi} M_1 \to M_0 \to 0.$$

Finally, tensoring is always right exact so we only need to check injectivity. □

Recall that a morphism of schemes $f : X \to Y$ is *flat* if and only if, for every point $x \in X$ with $y = f(x) \in Y$, the local ring $\mathscr{O}_{X,x}$ is flat as a $\mathscr{O}_{Y,y}$-modules. Generalising the above criterion to schemes, if S_1 is an R_1-scheme and $S_0 := S_1 \times_{R_1} k$, we then have:

Corollary 3.5.6. *S_1 is a flat R_1-scheme if and only if the natural map:*

$$\theta : \mathscr{O}_{S_0} \to \pi\mathscr{O}_{S_1},$$

is an isomorphism, where π is used to denote the section of $\mathscr{O}_{S_1}$ generated by $\pi \in R_1$.

More generally, if $f : X \to Y$ is a morphism of schemes and $\mathscr{F}$ is a sheaf of $\mathscr{O}_X$-modules, then we say that $\mathscr{F}$ is *flat over* Y if $\mathscr{F}_x$ is flat as a $\mathscr{O}_{Y,f(x)}$-module for each $x \in X$. Similarly, if S_1 is an R_1-scheme and $\mathscr{F}_1$ a sheaf of $\mathscr{O}_{S_1}$-modules, then $\mathscr{F}_1$ is flat over R_1 if and only if there is an isomorphism $\mathscr{F}_0 \cong \pi\mathscr{F}_1$ where $\mathscr{F}_0 = \mathscr{F}_1 \otimes \mathscr{O}_{S_0}$ is viewed as an $\mathscr{O}_{S_1}$-module.

Infinitesimal lifting criterion

Let X/k be a variety over an algebraically closed field k of dimension n. We say that X is *non-singular* if for every point $x \in X$, the local rings $\mathscr{O}_{X,x}$ are regular local rings i.e. the maximal ideals $\mathfrak{m}_{X,x}$ can be generated (minimally) by n elements. By Nakayama's lemma, this is equivalent to the cotangent space of X at x: $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$ being of dimension n (as a

k-vector space). The infinitesimal lifting criterion is the statement that (as X/k is of finite type), X being non-singular is equivalent to it being formally smooth:

Proposition 3.5.7 (Infinitesimal lifting criterion)**.** *Let X/k be a non-singular variety and let $Y = \mathrm{Spec(A)}$ be an arbitrary affine scheme. An infinitesimal thickening $Y' = \mathrm{Spec(A')}$ is an affine scheme, such that $Y \subseteq Y'$ is closed and the ideal J of Y is nilpotent. Then for any morphism $f : Y \to X$ there exists a lifting:*

$$\begin{array}{ccc} Y' & & \\ \uparrow & \searrow^{f'} & \\ Y & \xrightarrow[f]{} & X \end{array} .$$

Proof. [Har10, Prop. 4.4] □

3.5.3 Lifting schemes from characteristic p to characteristic 0

We now state the first deformation theory problem we wish to consider. Let R be a complete DVR using the notation in the previous subsection, of mixed characteristic. Suppose that X_0 is a projective, non-singular variety over k. Assume further that k is perfect of characteristic $p > 0$. We wish to understand how to lift X_0 to a flat R-scheme X. Then X_K is of characteristic 0 and we have 'lifted' X_0 from characteristic p to characteristic 0. We do this in the following steps which we will see are essentially replicated in the other deformation theory problems we consider:

Proposition 3.5.8. *Suppose that there exists a flat scheme X_n over R_n that lifts X_0. Then the obstruction to lifting X_n to a flat scheme X_{n+1}/R_{n+1} lies in $H^2(X_0, \Theta_{X_0/k})$ where $\Theta_{X_0/k}$ is the tangent sheaf of X_0.*

Proof. See [Har10, Thm. 25.3]. □

If $H^2(X_0, \Theta_{X_0/k}) = 0$ then we say that deformations of X_0 are *unobstructed*. Suppose that we can lift X_0 to X_1. We will see that the different possibilities for X_1 are parametrised by a group.

Remark 3.5.9. Consider a perfect field k of characteristic $p > 0$ and the two rings $W_2(k)$ and $k[\epsilon]$ as in Remark 3.5.4. Suppose we have a smooth projective variety X_0/k and we want to lift it to X_1/R_1 where R_1 is one of the two rings above. If $R_1 = D$ then we always have a *trivial lifting*:

$$X_1^{\mathrm{triv}} := X_0 \times_k \mathrm{Spec}(k[\epsilon]);$$

which exists as $k[\epsilon]$ is a k-algebra. Indeed the lifting X_1^{triv} corresponds to the identity of the group of possible liftings. However, in the case $R_1 = W_2(k)$ there is no 'preferred lifting' of X_0.

Torsors

Definition 3.5.10. Let $G \times S \to S$ be a left action of a group G on a set S. We say that S is a *torsor* or *principal homogeneous space* for G if the action is free and transitive.

Equivalently, for each element $s \in S$, we have an isomorphism:

$$\begin{aligned} G \times \{s\} &\longrightarrow S; \\ (g, s) &\longmapsto g \cdot s. \end{aligned}$$

So that S is isomorphic to the group G, except has no preferred identity. However, once we fix an element $s_0 \in S$ we can consider S to be a group with identity s_0.

Proposition 3.5.11. *Let k be a perfect field of positive characteristic $p > 0$ and let X_0/k be a non-singular variety with lifting X_n/R_n for some $n > 0$. Then the set of isomorphism classes of possible liftings X_{n+1}/R_{n+1} is a torsor under the cohomology group $H^1(X_0, \Theta_{X_0/k})$.*

Proof. See [Har10, §25] □

Note that if X_0 cannot be lifted, then we should really refer to the set of possible liftings as a *pseudotorsor* where the set S in the above definition is empty.

Algebraicity criterion

Suppose now that we are able to lift our variety X_0/k compatibly to X_n/R_n for each $n > 0$. We then obtain a formal scheme $\mathscr{X} := \varinjlim X_n$. We would like to understand when $\mathscr{X}$ is *algebraisable* (cf. Def. 3.5.1), namely, when does there exist a locally noetherian scheme $X \to \mathrm{Spec}(R)$ whose formal completion $\hat{X} \to \mathrm{Spf}(R)$ coincides with $\mathscr{X}$?

Serre's GAGA principle [Ser56] relates the category of coherent sheaves on a complex algebraic variety and it's 'analytification' where we consider, more generally, sheaves of modules of holomorphic functions. Grothendieck proved the analogue of Serre's statement for formal schemes. As for complex manifolds, this provides tools for determining when an analytic/formal object can be constructed from an algebraic one i.e. arises from a scheme.

Theorem 3.5.12. *Let R be a complete DVR. Suppose that $f : X \to Y$ is a separated, finite type morphism of R-schemes. Let $\hat{X}$ (resp. $\hat{Y}$) denote the formal completion of X along its special fibre X_0 (resp. Y along Y_0). Then there is an equivalence of categories $\mathscr{F} \mapsto \widehat{\mathscr{F}}$ from the category of coherent sheaves $\mathscr{F}$ on X whose support is proper over Y, to the category of coherent sheaves on $\hat{X}$ whose support is proper over $\hat{Y}$.*

Proof. See [EGA, III, Thm. 5.1.4]. □

Corollary 3.5.13. *Let $f : X \to Y$ be as in the previous theorem, and let $\mathscr{X}$ be a general noetherian formal scheme over* $\mathrm{Spf}(R)$.

i) There is a bijection between closed formal subschemes $\mathscr{X} \subseteq \hat{Y}$ and closed subschemes $X \subseteq Y$, proper over Y under the assignment $X \mapsto \hat{X}$.

ii) Suppose that $f : X \to Y$ is finite. Then the assignment $f : X \to Y$ to $\hat{f} : \hat{X} \to \hat{Y}$ is an equivalence from the category of finite Y-schemes to the category of formal $\hat{Y}$-schemes, proper over $\hat{Y}$.

Proof. i) See [EGA, III, Thm. 5.1.8].

ii) See [Il05, Cor. 4.6]

□

It is a more subtle question to algebraise infinitesimal deformations of abstract varieties and it is for this reason that we restrict our attention to projective varieties X_0/k. Let $\mathscr{L}_0$ be a very ample line bundle on X_0 defining a closed embedding $X_0 \hookrightarrow \mathbb{P}^N_k$ for some $N > 0$. Consider $\mathbb{P}^N_R$ and its formal completion along $\mathbb{P}^N_k$. Then, to lift X_0 to an algebraic R-scheme, we can lift it infinitesimally along with the line bundle $\mathscr{L}_0$ and then apply (i) above to algebraise the lift to a projective R-scheme embedded in $\mathbb{P}^N_R$.

Theorem 3.5.14. *Let R be a complete DVR with residue field k and uniformiser π. Set $R_n := R/\pi^{n+1}$. Let X_0 be a proper variety over k and suppose that we have compatible liftings X_n for each $n > 0$ and set $\mathscr{X} := \varprojlim_n X_n$.*

i) Let $\mathscr{L}_0$ be an ample line bundle and suppose that $\mathscr{L}_n$ is an invertible $\mathscr{O}_{X_n}$-module such that $\mathscr{L}_n \otimes X_0 = \mathscr{L}_0$. Then, the obstruction to lifting $\mathscr{L}_n$ to an invertible sheaf on X_{n+1} lies in $H^2(X_0, \mathscr{O}_{X_0})$.

ii) Suppose that $\mathscr{M}$ is an invertible line bundle on $\mathscr{O}_{\mathscr{X}}$ such that $\mathscr{M} \otimes X_0$ is ample. Then $\mathscr{X} = \hat{X}$ is algebraisable and there exists a unique ample line bundle $\mathscr{L}$ on X such that $\widehat{\mathscr{L}} \cong \mathscr{M}$.

Proof. See [EGA, III, Thm. 5.4.5] □

Corollary 3.5.15. *Let X_0 be a projective variety over k with $H^2(X_0, \mathscr{O}_{X_0}) = 0$. Suppose that we can lift X_0 to a formal scheme $\mathscr{X}$ over R. Then $\mathscr{X}$ is algebraizable.*

Putting this all together, we have criteria for lifting smooth projective schemes from characteristic $p > 0$ to characteristic 0:

Theorem 3.5.16. *Let R be a complete DVR of characteristic 0 with residue field k of characteristic $p > 0$. Let X_0 be non-singular projective variety over k. Suppose that:*

$$H^2(X_0, \mathscr{O}_{X_0}) = 0 \quad \text{and} \quad H^2(X_0, \Theta_{X_0/k}) = 0.$$

Then there exists a flat R-scheme X such that $X_k \cong X_0$.

Proof. See [Har10, Thm. 25.3] □

Importantly for us, we can always lift curves:

Corollary 3.5.17. *Let X_0 be a smooth projective curve over k. Then there exists a lifting of X_0 to R.*

Proof. Suppose that X_0 is a smooth projective curve. As $\dim(X_0) = 1$ the cohomology groups $H^2(X_0, \mathscr{O}_{X_0})$ and $H^2(X_0, \Theta_{X_0/k})$ vanish. □

3.5.4 Lifting closed subschemes

Suppose that k is an algebraically closed field of characteristic $p > 0$ and that R is a complete DVR of characteristic 0 with residue field k. Suppose that A_0/k is a non-singular variety. Suppose that A_0/k admits a lift A/R and $i_0 : X_0 \hookrightarrow A_0$ is a local complete intersection. We have already discussed how to lift X_0 abstractly, but how can we lift X_0 to successive closed subschemes $i_n : X_n \hookrightarrow A_n$ over the ring R_n such that $i_n|_{X_0} = i_0$?

Let $\mathscr{I}_0 := \ker(\mathscr{O}_{A_0} \to (i_0)_*\mathscr{O}_{X_0})$ be the ideal sheaf of X_0 in A_0. We define the *conormal sheaf* to be $\mathscr{C}_{X_0/A_0} = \mathscr{I}_0/\mathscr{I}_0^2$ viewed as an $\mathscr{O}_{X_0}$-module. As X_0 is a local complete intersection, $\mathscr{C}_{X_0/A_0}$ is locally free of rank $\operatorname{codim}_{A_0}(X_0)$. Dually, we have the *normal sheaf* $\mathscr{N}_{X_0/A_0} = (\mathscr{C}_{X_0/A_0})^\vee$. Correspondingly, we have an exact sequence of sheaves of $\mathscr{O}_{X_0}$-modules:

$$0 \longrightarrow \Theta_{X_0/k} \longrightarrow \Theta_{A_0/k}|_{X_0} \longrightarrow \mathscr{N}_{X_0/A_0} \longrightarrow 0.$$

Proposition 3.5.18. *Suppose for some $n > 0$ that there is a flat lifting $i_n : X_n \hookrightarrow A_n$. Then the set of flat liftings $i_{n+1} : X_{n+1} \hookrightarrow A_{n+1}$ of i_n is naturally a torsor under the global sections of the normal sheaf $H^0(X_0, \mathscr{N}_{X_0/A_0})$.*

Proof. See [Har10, Thm. 6.3]. By Lemma 3.5.5 for $\mathscr{O}_{X_0}$-modules, a flat lifting $i_1 : X_1 \hookrightarrow A_1$ corresponds to a flat ideal sheaf $\mathscr{I}_1 \subseteq \mathscr{O}_{A_1}$ that fits into an exact sequence:

$$0 \longrightarrow \mathscr{I}_0 \longrightarrow \mathscr{I}_1 \longrightarrow \mathscr{I}_0 \longrightarrow 0.$$

Hartshorne shows that the difference of two such extensions $\mathscr{I}_1, \mathscr{I}_1' \in \operatorname{Ext}^1(\mathscr{I}_0, \mathscr{I}_0)$ induces a morphism $\mathscr{I}_0 \to \mathscr{O}_{X_0}$ that vanishes on $\mathscr{I}_0^2$. Namely, we have a section of the normal bundle:

$$H^0(X_0, \mathscr{N}_{X_0/A_0}) = \operatorname{Hom}(\mathscr{I}_0/\mathscr{I}_0^2, \mathscr{O}_{X_0}).$$

He then proceeds to show that this does indeed define a torsor. □

Again, as we are in the mixed characteristic case there is no 'preferred' lifting of X_0 to a closed subscheme $X_1 \subseteq A_1$. As in the case of an abstract lifting, there is a cohomological obstruction to the existence of a lift:

Proposition 3.5.19. *Suppose for some $n > 0$ that there is a flat lifting $i_n : X_n \hookrightarrow A_n$. Then the obstruction to lifting i_n to $i_{n+1} : X_{n+1} \hookrightarrow A_{n+1}$ is an element of the cohomology group $H^1(X_0, \mathscr{N}_{X_0/A_0})$.*

Proof. See [Har10, Thm. 6.3]. □

Applying the algebraicity criterion of Corollary 3.5.13 (i), if we have a comptabile system of closed subschemes $\mathscr{X} = \varprojlim X_n$ then this is automatically algebraisable and arises from a closed immersion $i : X \hookrightarrow A$ of a flat R-scheme lifting $i_0 : X_0 \hookrightarrow A_0$.

3.5.5 Lifting finite morphisms

Finally, we discuss lifting finite morphisms $f_0 : X_0 \to Y_0$ over k to the rings R_n and R. By considering the graph of f, we see that this is a special case of the previous subsection.

Theorem 3.5.20. *Let k be a perfect field of characteristic $p > 0$. Let $f_0 : X_0 \to Y_0$ be a finite flat morphism of projective k-schemes. Let X and Y be flat liftings of X_0 and Y_0 respectively to R.*

i) Suppose that $f_n : X_n \to Y_n$ is a finite flat morphism extending f_0. Then the obstruction to extending f_n to a finite flat morphism $f_{n+1} : X_{n+1} \to Y_{n+1}$ lies in $H^1(X_0, \mathscr{H}om(f_0^*(\Omega_{Y_0/k}), \mathscr{O}_{X_0}))$.

ii) If a lifting $f_n : X_n \to Y_n$ exists, then the set of possible extensions f_{n+1} of f_n (up to isomorphism) is a torsor under $H^0(X_0, \mathscr{H}om(f_0^*(\Omega_{Y_0/k}), \mathscr{O}_{X_0}))$.

iii) If there is a compatible set of liftings f_n for every $n > 0$ then the morphism of formal schemes $f : \mathscr{X} \to \mathscr{Y}$ is automatically algebraisable. Namely, there exists a finite flat morphism $g : X \to Y$ such that $f = \hat{g}$.

Proof. (i) and (ii) are in fact special cases of Prop. 3.5.18 and Prop. 3.5.19. For ease of exposition, we will only consider the problem of lifting $f_0 : X_0 \to Y_0$ to $f_1 : X_1 \to Y_1$. Let $\Gamma_{f_0} : X_0 \to X_0 \times_k Y_0$ denote the graph morphism (Id, f_0). This is a closed immersion. Taking $X_1 \times_{R_1} Y_1$ as the flat lifting of $X_0 \times_k Y_0$, the obstruction to lifting the graph of f_0 (and thus to lifting f_0) is given by the first cohomology group of the normal sheaf $\mathscr{N}_{\Gamma_{f_0}}$. On the other hand, there is an exact sequence:

$$0 \longrightarrow \mathscr{C}_{\Gamma_{f_0}} \longrightarrow \Gamma_{f_0}^* \Omega_{X_0 \times Y_0/k} \longrightarrow \Omega_{X_0/k} \longrightarrow 0;$$

noting that the graph is a complete intersection. We have the isomorphism:

$$\Gamma_{f_0}^* \Omega_{X_0 \times Y_0/k} \cong \Omega_{X_0/k} \oplus f_0^* \Omega_{Y_0/k}.$$

Moreover, the short exact sequence splits as the projection map $\mathrm{pr}_1 : X_0 \times_k Y_0 \to X_0$ induces a section. Overall, we have:

$$\mathscr{C}_{\Gamma_{f_0}} \cong f_0^*(\Omega_{Y_0/k});$$

and thus $\mathscr{N}_{\Gamma_{f_0}} \cong \mathscr{H}om(f_0^*(\Omega_{Y_0/k}), \mathscr{O}_{X_0})$. As in the case of closed subschemes, finite morphisms are also algebraisable (cf. Cor. 3.5.13). □

3.6 Serre-Tate moduli

Throughout this section, we fix an algebraically closed field k of characteristic $p > 0$. Our main reference will be [Ka78]. Let Art_k denote the category of artinian local rings $(R, \mathfrak{m}_R)$ with residue field $R/\mathfrak{m}_R = k$. Let A_0/k be an abelian variety of dimension g. An *infinitesimal deformation* or *infinitesimal lifting* of A_0 is a flat scheme $A \to \mathrm{Spec}(R)$ such that $A_k \cong A_0$. We restrict our attention to liftings that are additionally *abelian schemes*, namely, $A \to \mathrm{Spec}(R)$ is a proper, R-group scheme. We then define the *formal moduli functor* $\mathrm{Def}_{A_0/k} : \mathrm{Art}_k \longrightarrow \mathrm{Set}$ by:

$$R \longmapsto \{A \to \mathrm{Spec}(R) \mid A \text{ abelian } R\text{-scheme with } A_k \cong A_0\}/\cong .$$

We say that $\mathrm{Def}_{A_0/k}$ is *pro-representable* (cf. 3.2.5) if there exists some complete local noetherian ring $(\mathscr{R}, \mathfrak{m}_{\mathscr{R}})$ with residue field k such that:

$$\mathrm{Def}_{A_0/k} \cong \varinjlim_n \mathrm{Hom}(\mathscr{R}_n, -).$$

This implies that there exists a *universal formal deformation* $\mathscr{A}^u \to \mathrm{Spf}(\mathscr{R})$ (corresponding to $\mathrm{Id} \in \mathrm{Hom}(\mathscr{R}, \mathscr{R})$) where $\mathscr{A}^u$ is a noetherian formal scheme (Def. 3.5.1). i.e. for each $n > 0$, writing $\mathscr{R}_n := \mathscr{R}/\mathfrak{m}_{\mathscr{R}}^{n+1}$ and $\mathscr{A}_n^u := \mathscr{A}^u \times_{\mathscr{R}} \mathscr{R}_n$ we have an isomorphism:

$$\mathrm{Def}_{A_0/k}(R) \cong \varinjlim_n \mathrm{Hom}(\mathscr{R}_n, R)$$

that is natural for $R \in \mathrm{Art}_k$. Then, if $A \to \mathrm{Spec}(R)$ is some infinitesimal deformation, there exists an integer $N > 0$ and a pullback diagram:

$$\begin{array}{ccc} A & \longrightarrow & \mathscr{A}_N^u \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\mathscr{R}_N) \end{array} .$$

Recall that the *p-rank* of A_0 is the integer $0 \leq i \leq g$ such that $|A[p](k)| = p^i$ (Prop. 3.2.7). When $i = g$ we say that A_0 is *ordinary*. The theory of Serre-Tate is split into two parts:

i) Liftings of A_0 to $A \to \mathrm{Spec}(R)$ for some local artinian ring R are in correspondence with liftings of the p-divisible group $A_0[p^\infty]$ to some p-divisible group $G \to \mathrm{Spec}(R)$.

ii) When A_0 is ordinary, $\mathrm{Def}_{A_0/k}$ is *pro-representable* by a formal moduli space $\widehat{\mathscr{M}}_{A_0/k}$ which carries the structure of a formal torus $(\hat{\mathbb{G}}_{m,W(k)})^{g^2}$ over the Witt vectors $W(k)$.

A striking consequence of (ii) is that, for an artinian local ring R, there is a distinguished *canonical lifting* A^{can}/R corresponding to the identity element of $(\hat{\mathbb{G}}_m)^{g^2}(R) = (1+\mathfrak{m}_R)^{g^2}$. This is in stark contrast to the general set-up of deformations in mixed characteristic where there is no 'preferred' lifting of a general variety to characteristic zero, and the space of possible liftings is a torsor under a certain cohomology group (Prop. 3.5.11).

Remark 3.6.1. Note that there are counterexamples for non-ordinary abelian varieties A_0/k being liftable to a flat scheme $A/W(k)$ [Oort-Norm80]. However, there always exists a *ramified* extension $R \supseteq W(k)$ over which a given non-ordinary abelian variety A_0 is liftable to a flat scheme A/R.

On the other hand, it follows from Serre-Tate theory that *ordinary* abelian varieties always admit *unramified* liftings, i.e. liftings to the Witt vectors. However, we are primarily interested in elliptic curves, and by Cor. 3.5.17 supersingular elliptic curves E_0/k still admit unramified liftings.

3.6.1 Serre-Tate theorem

The main statement of the Serre-Tate theorem describes the infinitesimal deformation theory of *any* abelian variety A_0/k. The key observation of Serre was that infinitesimal deformations of A_0 are in 1:1 correspondence with deformations of the *p-divisible group* $A_0[p^\infty]$ (Def. 3.3.1). We make this precise by phrasing this as an equivalence of categories.

Theorem 3.6.2 (Serre-Tate Theorem)**.** *Let k be an algebraically closed field of characteristic $p > 0$. Let R be an artinian local ring with residue field k. Let* AbSch/R *denote the category of abelian schemes over R, and let $\mathscr{D}$ denote the category of triples (A_0, G, ϵ) where A_0 is an abelian variety over k, G is a p-divisible group over R and $\epsilon : G_k \xrightarrow{\sim} A_0[p^\infty]$ is an isomorphism of p-divisible groups. Then there is an equivalence:*

$$\begin{aligned} \mathrm{AbSch}/R &\longrightarrow \mathscr{D}; \\ A &\longmapsto (A_k, A[p^\infty], (A[p^\infty])_k \xrightarrow{\text{nat.}} A_k[p^\infty]) \end{aligned}$$

i.e. deformations of A_0 are determined by deformations of $A_0[p^\infty]$.

Proof. See [Ka78, Theorem 1.2.1]. □

3.6.2 Serre-Tate formal moduli

Let k be an algebraically closed field of characteristic $p > 0$ and let A_0 be an ordinary abelian variety over k of dimension g. Let $A_0^\vee$ denote the dual abelian variety. Note that $A_0^\vee$ is also ordinary as it is isogenous to A_0. Denote by:

$$T_p A_0 := \varprojlim A_0[p^n](k)$$

the p-adic Tate module (cf. Def. 3.2.37). Similarly, we denote by $T_p A_0^\vee$ the Tate module of $A_0^\vee$. By the ordinary assumption, these are free $\mathbb{Z}_p$-module of rank g. Denote by $\hat{\mathbb{G}}_{m,W(k)}$ the formal completion of $\mathbb{G}_{m,W(k)}$ at the identity section. Suppose we choose coordinates $\mathbb{G}_{m,W(k)} = \mathrm{Spec}(W(k)[t^{\pm 1}])$, and using the notation of Ex. 3.3.5 we take:

$$\hat{\mathbb{G}}_{m,W(k)} = \mathrm{Spf}(W(k)[\![T]\!])$$

where $T = t - 1$. Thus, if $(R, \mathfrak{m}_R)$ is a complete noetherian local ring, or an artinian local ring with residue field k, $\hat{\mathbb{G}}_m(R)$ is the set of morphisms $W(k)[\![t-1]\!] \to R$ such that t gets sent to the maximal ideal $\mathfrak{m}_R$. Thus we have:

$$\hat{\mathbb{G}}_m(R) = 1 + \mathfrak{m}_R$$

sometimes referred to as the *principal units* of R. We are now ready to state the main result on formal moduli of ordinary abelian varieties:

Theorem 3.6.3. *Let k be an algebraically closed field of characteristic $p > 0$ and let A_0/k be an ordinary abelian variety.*

i) Let R be an artinian local ring with residue field k. Then there is natural isomorphism:

$$\begin{aligned} \mathrm{Def}_{A_0/k}(R) &\longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(T_p A_0 \otimes T_p A_0^\vee, \hat{\mathbb{G}}_m(R)); \\ (A \to \mathrm{Spec}(R)) &\longmapsto q(A/r; -, -). \end{aligned}$$

ii) Moreover, the infinitesimal deformation functor $\mathrm{Def}_{A_0/k}$ is pro-representable by a formal moduli space $\hat{\mathscr{M}}_{A_0/k}$ with the structure of a formal torus of rank g^2:

$$\hat{\mathscr{M}}_{A_0/k} \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_p A_0 \otimes T_p A_0^\vee, \hat{\mathbb{G}}_m).$$

Proof. See [Ka78, Theorem 2.1]. □

Suppose we fix an infinitesimal deformation A/R of A_0/k. We may think of the

associated bilinear map:

$$q(A/R; -, -) : T_pA_0 \times T_pA_0^\vee \longrightarrow \hat{\mathbb{G}}_m(R)$$

as a 'lifting' of the Weil pairing. Recall that any notion of Weil pairing on the p-adic Tate module of an abelian variety in characteristic $p > 0$, taking values in k is trivial (Remark 3.2.38), and so Katz 'lifts' the values of his pairing to $\hat{\mathbb{G}}_m(R) = 1 + \mathfrak{m}_R$ where there are non-trivial p^n-th roots of unity. By fixing $\mathbb{Z}_p$-bases of T_pA_0 and $T_pA_0^\vee$, it is clear that specifying such a bilinear pairing is equivalent to specifying g^2 principal units. These are referred to as the *Serre-Tate coordinates* of the lifting A/R. Let $\hat{A}_0$ denote the formal group attached to A_0 (cf. Ex. 3.3.10). We first note the following lemma:

Lemma 3.6.4. *Let k be an algebraically closed field of characteristic $p > 0$ and let A_0/k be an ordinary abelian variety. Then, for each $n > 0$, the connected-étale sequence of $A_0[p^n]$ is given by:*

$$0 \to (\mu_{p^n,k})^g \to A_0[p^n] \to (\mathbb{Z}/p\mathbb{Z})^g \to 0$$

and so $\hat{A}_0[p^n]$ and $A_0[p^n](k)$ are dual under Cartier duality.

Proof. This essentially follows from Theorem 3.3.17. We have that $A_0[p^n]^{\text{ét}} \cong A_0[p^n](k) \cong (\mathbb{Z}/p\mathbb{Z})^g$ as a constant group scheme. Then, as taking the Cartier dual commutes with finite products we have the lemma. □

Thus, the connected-étale sequence of the p-divisible group of A_0 is given by the split extension (cf. Ex. 3.3.10):

$$0 \to \hat{A}_0 \to A_0[p^\infty] \to T_pA_0 \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \to 0.$$

For each $n > 0$, Cartier duality induces an isomorphism:

$$\hat{A}_0[p^n] \xrightarrow{\sim} \text{Hom}(A_0^\vee[p^n](k), \mu_{p^n,k}).$$

Taking the limit we see that:

$$\hat{A}_0 \xrightarrow{\sim} \text{Hom}_{\mathbb{Z}_p}(T_pA_0^\vee, \hat{\mathbb{G}}_{m,k}).$$

After a choice of $\mathbb{Z}_p$-basis of $T_pA_0^\vee$, we have an isomorphism $\hat{A}_0 \cong (\hat{\mathbb{G}}_{m,k})^g$ and thus we refer to $\hat{A}_0$ as a *toroidal formal group*. Similarly, after a choice of $\mathbb{Z}_p$-basis of T_pA_0, $T_pA_0 \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g$ is the étale, constant p-divisible group of height g. $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ admits a unique lifting to the same constant group scheme over R as it is étale. Thus, $\hat{A}_0$ also admits a unique lifting to the toroidal formal group $\text{Hom}_{\mathbb{Z}_p}(T_pA_0^\vee, \hat{\mathbb{G}}_{m,R})$ by duality. Overall, we obtain the following:

Proposition 3.6.5. *Let k be an algebraically closed field and let A_0 be an ordinary abelian variety over k, of dimension g. Suppose that R is an artinian local ring with residue field k and that A/R is an infinitesimal deformation of A_0. Then, the p-divisible group $A[p^\infty]$ is given by an extension:*

$$0 \to \hat{A} \to A[p^\infty] \to T_p A_0 \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \to 0;$$

where $\hat{A}$ is the formal group associated to A. Moreover, we have an isomorphism $\hat{A} \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_p A_0^\vee, \hat{\mathbb{G}}_{m,R})$ so that, after a choice of $\mathbb{Z}_p$-basis for $T_p A_0$ and $T_p A_0^\vee$, we have isomorphisms:

$$\hat{A} \cong (\hat{\mathbb{G}}_{m,R})^g \quad \text{and} \quad A[p^\infty]^{\text{ét}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g.$$

The q-pairing associated to the lifting A/R can be described as follows. As R is artinian with residue field k of characteristic $p > 0$, there exists some integer $n > 0$ such that $\mathfrak{m}_R^{n+1} = 0$. In particular, $p^n \hat{A}(R) = 0$ (as $\hat{A}(R)$ takes values in $\mathfrak{m}_R$ and $k = R/\mathfrak{m}_R$ is of characteristic $p > 0$). Thus, there exists a well defined 'lifting' homomorphism:

$$\begin{aligned} A_0(k) &\longrightarrow A(R); \\ x_0 &\longmapsto p^n x \end{aligned}$$

where $x \in A(R)$ is any lift of x_0. Note that, a lift always exists as A/R is smooth (this is Prop. 3.5.7 applied to $\mathrm{Spec}(R)$). Moreover, the map is well-defined as for any other lifting $x' \in A(R)$, the difference $x - x'$ is in the kernel of reduction, and so is contained in $\hat{A}(R)$ (Ex. 3.3.12 (ii)). This lifting homomorphism, restricted to p^n-torsion for each $n > 0$, induces a homomorphism of $\mathbb{Z}_p$-modules:

$$\varphi_{A/R} : T_p A_0 \longrightarrow \hat{A}(R) \cong \mathrm{Hom}_{\mathbb{Z}_p}(T_p A_0^\vee, \hat{\mathbb{G}}_m(R))$$

Specifying such a homomorphism is equivalent to defining a pairing:

$$\begin{aligned} q(A/R; -, -) : T_p A_0 \times T_p A_0^\vee &\longrightarrow \hat{\mathbb{G}}_m(R); \\ (\alpha, \alpha') &\longmapsto \varphi_{A/R}(\alpha)(\alpha'). \end{aligned}$$

3.6.3 Properties of canonical liftings

Let k an algebraically closed field of characteristic $p > 0$ and let $W(k)$ be the Witt vectors associated to k. For an ordinary abelian variety A_0/k, as described there is a universal formal deformation $\mathscr{A}^u$ over $\hat{\mathbb{G}}_m$ and the canonical lifting corresponds to the unit section. By Thm. 3.5.14, this formal scheme is algebraisable and we refer to it as the canonical lifting $\mathscr{A}^{\text{can}} \to \mathrm{Spec}(W(k))$ of A_0 to $W(k)$. As discussed, the p-divisible group of A_0 is

given by the split short exact sequence:

$$0 \to \hat{A}_0 \to A_0[p^\infty] \to (\mathbb{Q}_p/\mathbb{Z}_p)^g \to 0;$$

where $\hat{A}_0$ is the formal completion of A_0 at the identity. We know that $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ and $\hat{A}_0$ are Cartier dual. As $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ is étale, it admits a unique lifting to $W(k)$, and by duality so does $\hat{A}_0$. Thus, any other abelian scheme $\mathscr{A} \to \mathrm{Spec}(W(k))$ lifting A_0, by the Serre-Tate theorem, is determined by an extension:

$$0 \to \hat{\mathscr{A}} \to \mathscr{A}[p^\infty] \to (\mathbb{Q}_p/\mathbb{Z}_p)^g \to 0.$$

By the associated bilinear pairing in Theorem 3.6.3, the canonical lifting can be characterised as the unique up to isomorphism lifting of A_0 corresponding to the trivial extension $\hat{\mathscr{A}} \times (\mathbb{Q}_p/\mathbb{Z}_p)^g$. The following provides another important characterisation of the canonical lifting of an ordinary abelian variety:

Proposition 3.6.6. *Let k be an algebraically closed field of characteristic $p > 0$ and let $W(k)$ denote the Witt vectors of k. Suppose that A_0 is an ordinary abelian variety. Then there is a unique up to isomorphism lifting $\mathscr{A}^{\mathrm{can}}/W(k)$ of A_0 such that the natural map:*

$$\mathrm{End}(\mathscr{A}^{\mathrm{can}}) \longrightarrow \mathrm{End}(A_0)$$

is a bijection. This is the canonical lifting.

Proof. [Mess06, Ch. V, Thm. 3.3]. □

Corollary 3.6.7. *Let A_0 and B_0 be two ordinary abelian varieties over k and let $\mathscr{A}^{\mathrm{can}}$ and $\mathscr{B}^{\mathrm{can}}$ denote their respective canonical liftings. Then the natural map:*

$$\mathrm{Hom}(\mathscr{A}^{\mathrm{can}}, \mathscr{B}^{\mathrm{can}}) \longrightarrow \mathrm{Hom}(A_0, B_0)$$

is a bijection.

In fact, to check whether a particular lifting of an ordinary abelian variety is the canonical one, one need only determine whether the Frobenius morphism lifts:

Proposition 3.6.8. *Let A_0 be an ordinary abelian variety over k and $\mathscr{A}/W(k)$ a lifting. Then $\mathscr{A} \cong \mathscr{A}^{\mathrm{can}}$ if and only if there exists a morphism:*

$$F : \mathscr{A} \longrightarrow \mathscr{A}'$$

that extends the relative Frobenius $F_{A_0/k} : A_0 \to A_0^{(p)}$ where $\mathscr{A}'$ is the base change of $\mathscr{A}$ by the Frobenius on the Witt vectors $W(k) \to W(k)$ sending $(a_0, a_1, ...) \mapsto (a_0^p, a_1^p, ...)$.

Proof. [Mess06, App., Cor. 1.2]. □

This should be compared with Cor. 3.4.10. Let E_0/k be an ordinary elliptic curve and let $\mathscr{E}/W(k)$ be a lifting. Then, the rank p, connected group scheme $\hat{E}_0[p]$ lifts uniquely to a rank p connected group scheme over $\hat{\mathscr{E}}[p]/W(k)$ and the Frobenius can always be lifted in the weak sense, namely, the quotient map:

$$\mathscr{E} \longrightarrow \mathscr{E}/\hat{\mathscr{E}}[p]$$

restricts to the relative Frobenius on E_0. However, this does not provide a lifting of the absolute Frobenius unless $\mathscr{E}$ is canonical. In this case, the base change $\mathscr{E}'$ of $\mathscr{E}$ with respect to the Frobenius on $W(k)$ coincides with the quotient $\mathscr{E}/\hat{\mathscr{E}}[p]$.

3.7 Inertia representations attached to elliptic curves

3.7.1 The Néron-Ogg-Shafarevich criterion

Let v be a finite place of a number field L. Denote by $\mathscr{O}_{L,v}$ the localisation at v and k_v the corresponding residue field. We say that an abelian variety A/L has *good reduction* at v if there exists an abelian scheme $\mathscr{A} \to \mathrm{Spec}(\mathscr{O}_{L,v})$ such that $\mathscr{A}_L \cong A$.

Theorem 3.7.1. *Let L be a number field, v a finite place and A/L an abelian variety. Suppose that the residue field k_v has characteristic $p > 0$. The following are equivalent:*

i) A has good reduction at v;

ii) For some prime $l \neq p$, the l-adic Tate module is unramified;

iii) For all primes $l \neq p$, the l-adic Tate module is unramified.

Proof. See [ST03, Theorem 1]. □

Let K/L be a finite extension and suppose w is an extension of v to K. Recall that the decomposition group $D_w(K/L) \subseteq \mathrm{Gal}(K/L)$ is the subgroup of automorphisms which preserve w (cf. 3.1.3). We then have an epimorphism:

$$D_w(K/L) \longrightarrow \mathrm{Gal}(k_w/k_v);$$

where k_w is the residue field of K at w. We denote the kernel of this map by $I_w(K/L)$; the *inertia group* of K/L at w. Now let $\bar{L}/L$ be an algebraic closure of L. We can make sense of these definitions for an infinite extension by noting that the *absolute Galois group* is naturally an inverse limit:

$$\mathrm{Gal}(\bar{L}/L) \cong \varprojlim_{K \supset L} \mathrm{Gal}(K/L)$$

taken over all finite Galois extensions K/L which are partially ordered by inclusion; inducing natural restriction maps on Galois groups. Let $\bar{v}$ be an extension of v to $\bar{L}$. We then define:

i) The *decomposition group* of $\bar{L}/L$ at $\bar{v}$:

$$D_{\bar{v}} := \varprojlim_{K \supset L} D_w(K/L).$$

ii) The *inertia group* of $\bar{L}/L$ at $\bar{v}$:

$$I_{\bar{v}} := \varprojlim_{K \supset L} I_w(K/L).$$

where for each finite extension K/L, the valuation w is the restriction of $\bar{v}$. Note that we still have an exact sequence:

$$1 \longrightarrow I_{\bar{v}} \longrightarrow D_{\bar{v}} \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1$$

where $\bar{k}$ is some algebraic closure of k. Recall that the extension K/L is unramified at w if $I_w(K/L)$ is trivial (Cor. 3.1.8). More generally, if S is a set with an action of $\mathrm{Gal}(\bar{L}/L)$, we say it is *unramified at* v if $I_{\bar{v}}$ acts trivially. Let A be an abelian variety of dimension g over L and $n > 0$ a positive integer. The multiplication-by-n map $[n]_A : A \to A$ is L-rational with finite kernel of rank n^{2g}. Thus, the (geometric) n-torsion

$$A[n](\bar{L}) := [n]_A^{-1}(0)$$

admits a $G_L = \mathrm{Gal}(\bar{L}/L)$-action (i.e. one can check that if $x \in A[n](\bar{L})$ and $\sigma \in G_L$ then $nx^\sigma = (nx)^\sigma = e$). Thus, we have a representation of G_L attached to the n-torsion points of A:

$$\rho_{n,A} : G_L \longrightarrow \mathrm{Aut}(A[n](\bar{L})) \cong \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

For each prime $l > 0$, one may consider the limit of the representations above for l^n and obtain a representation of the l-adic Tate module (Def. 3.2.37):

$$\rho_{l^\infty,A} : G_L \longrightarrow \mathrm{Aut}(T_l(A)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_l).$$

Suppose that the place v of L has residue characteristic $p > 0$ and $l \neq p$ is another prime. Then, the Néron-Ogg-Shafarevich criterion says one need only verify that $\rho_{l^\infty,A}(I_{\bar{v}}) = \{1\}$ to see that A has good reduction at v. We note the following consequence:

Corollary 3.7.2. *Let $f : A \to B$ be an isogeny of abelian varieties over a number field L. Let v be a finite place of L for which A has good reduction. Then B has good reduction at*

v also.

Proof. See [ST03, Corollary 2]. □

3.7.2 Galois theory of local fields

The main reference for the discussion on representations of inertia groups and elliptic curves will be [Ser72]. For the remainder of this section, we fix a number field L and a finite place v. Let K be the completion of L with respect to v. Let R be the corresponding valuation ring and $\mathfrak{m}$ the maximal ideal of R. Suppose that $k = R/\mathfrak{m}$ is of characteristic $p > 0$. We *normalise* v in the sense that, for a uniformiser $\pi \in R$ we take $v(\pi) = 1$. Then $v(p) = e$ gives the *absolute ramification index* of R (3.1.5).

Fixing an algebraic closure $\bar{K}/K$, v extends uniquely to a (no longer discrete) valuation on $\bar{K}$ which we still denote by v (cf. Prop. 3.1.9). Note that the absolute Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$ coincides with the decomposition group $D_{\bar{v}}$ and so without ambiguity, we denote by $I \subseteq G_K$ the inertia group. Note also that the residue field of $\bar{K}$ with respect to v is an algebraic closure $\bar{k}$ of k and that we have the exact sequence:

$$1 \longrightarrow I \longrightarrow \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Let K^{nr} denote the *maximal unramified extension* of K i.e. the union of finite unramified extensions L/K. In fact, one may describe K^{nr} explicitly:

$$K^{\mathrm{nr}} = \bigcup_{p \nmid m} K(\zeta_m) = \bigcup_{n>0} K(\zeta_{p^n-1}).$$

Indeed, finite unramified extensions of K correspond to finite separable extensions of k. As k is a finite field of characteristic $p > 0$ these are all of the form $\mathbb{F}_{p^n}$. So that $\mathbb{F}_{p^n}^*$ is cyclic of order $p^n - 1$. It is not hard to see that if L/K is finite and unramified with residue field $\mathbb{F}_{p^n} \supseteq k$, then $L = K(\zeta_{p^n-1})$ for some primitive $(p^n - 1)$-th root of unity (in $\bar{K}$). The inertia group is then given by:

$$I = \mathrm{Gal}(\bar{K}/K^{\mathrm{nr}}).$$

Definition 3.7.3. Let K be a field of characteristic 0, complete with respect to a discrete, normalised valuation v, and residue characteristic $p > 0$. Let K'/K be a finite extension of K of ramification degree e'. We say that K'/K is *tamely ramified* if $p \nmid e'$.

Similarly, we can let $\bar{K} \supseteq K^{\mathrm{t}} \supseteq K^{\mathrm{nr}}$ denote the *maximal tamely ramified extension* of K. We define the *wild inertia group* to be the Galois subgroup:

$$I_p = \mathrm{Gal}(\bar{K}/K^{\mathrm{t}}) \subseteq I.$$

We denote by $I_{\mathrm{t}} := I/I_p$ the *tame inertia group* with Galois group $\mathrm{Gal}(K^{\mathrm{t}}/K^{\mathrm{nr}})$.

Remark 3.7.4. In fact, the wild inertia and inertia subgroups $I_p \subseteq I \subseteq G_K$ belong to a filtration of the absolute Galois group:

$$G_K \supseteq G_0 \supseteq G_1 \supseteq ...$$

where G_n is the subgroup of G_K fixing $\bar{R}/\bar{\mathfrak{m}}^{n+1}$. It is then clear that $G_0 = I$ and moreover $G_1 = I_p$ [Ser13, IV, §1]. In fact, I_p is the largest *pro-p-subgroup* of I i.e. for each finite Galois extension L/K, the subgroup $I_p(L/K) \subseteq I(L/K)$ is the largest p-subgroup (i.e. of p-primary order) [Ser13, IV, §2, Cor. 3] and I_p is given by the limit:

$$I_p = \varprojlim_{L \supset K} I_p(L/K).$$

The wild inertia group is, in some sense, the hardest part of the Galois group to describe. Luckily, the representations of I that we will study are trivial when restricted to I_p, and so we need only understand representations of I_{t}:

Proposition 3.7.5. *Let k' be some field of characteristic $p > 0$ and let V be a finite dimensional vector space over k'. Suppose that $\rho : G_K \to \mathrm{GL}(V)$ is a continuous, semisimple representation (with the respect to the profinite topology). Then:*

$$\rho(I_p) = \{\mathrm{Id}\}.$$

Proof. See [Ser72, Prop. 5]. □

Structure of the tame inertia group

Let $\bar{K} \supseteq K^{\mathrm{t}} \supseteq K^{\mathrm{nr}} \supseteq K$ be as before. As with the maximal unramified extension, we can explicitly construct the maximal tamely ramified extension. Let $d > 0$ be an integer coprime to p and let $\mu_d \subseteq K^{\mathrm{nr}}$ denote the d-th roots of unity. These are all of valuation 1 and so specialise injectively into $\bar{k}$. Let $\pi \in K$ be a uniformiser and consider the extension:

$$K^d := K^{\mathrm{nr}}(\pi^{1/d}).$$

These are tamely ramified extensions of K^{nr} of degree d with Galois group μ_d. Specifically, if $\sigma \in \mathrm{Gal}(K^d/K^{\mathrm{nr}})$ then $\sigma(\pi^{1/d}) = \theta_d(\sigma)\pi^{1/d}$ for a unique root of unity $\theta_d(\sigma) \in \mu_d$. This defines an isomorphism:

$$\theta_d : \mathrm{Gal}(K^d/K^{\mathrm{nr}}) \longrightarrow \mu_d.$$

In fact, it is sufficient to adjoin $\pi^{1/d}$ only for integers of the form $d = q - 1$ where $q = p^h$ is a p-th power. Specifically, we have:

$$I_{\mathrm{t}} = \mathrm{Gal}(K^{\mathrm{t}}/K^{\mathrm{nr}}) \cong \varprojlim_{q} \mathrm{Gal}(K^{q-1}/K^{\mathrm{nr}});$$

and an isomorphism:

$$\theta : \mathrm{Gal}(K^{\mathrm{t}}/K^{\mathrm{nr}}) \longrightarrow \varprojlim_{q} \mu_{q-1}$$

induced by the isomorphisms θ_{q-1} where $q = p^h$, for each $h > 0$. Let $X = \mathrm{Hom}(I_{\mathrm{t}}, \bar{k}^*)$ denote the characters of I_{t} (1-dimensional representations). For each $d > 0$ coprime to p, viewing $\mu_d \subseteq \bar{k}$, we have defined elements $\theta_d \in X$. When $d = q - 1$ where $q = p^h$, we may associate $\mu_{q-1} \cong \mathbb{F}_q^*$ where $\mathbb{F}_q \subseteq \bar{k}$ is the unique subfield of $\bar{k}$ with $q = p^h$ elements. We refer to any composition of θ_{q-1} with an automorphism of $\mathbb{F}_q$ as a *fundamental character*.

Remark 3.7.6. In fact, Serre shows that the characters θ_d generate X [Ser72, Prop. 6]. Consider the group $\mathbb{Q}/\mathbb{Z}$ under addition. This is a torsion group and so can be decomposed into its p-primary and coprime-to-p components:

$$\mathbb{Q}/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p \oplus (\mathbb{Q}/\mathbb{Z})^{(p')};$$

where:

$$(\mathbb{Q}/\mathbb{Z})^{(p')} = \bigoplus_{l \neq p} \mathbb{Q}_l/\mathbb{Z}_l.$$

Each element $\alpha \in (\mathbb{Q}/\mathbb{Z})^{(p')}$ may be expressed as $\alpha = a/d$ where $a, d \in \mathbb{Z}$ and $\gcd(p, d) = 1$. Serre shows that we have an isomorphism $(\mathbb{Q}/\mathbb{Z})^{(p')} \cong X$ by assigning $\alpha \mapsto (\theta_d)^a$.

3.7.3 Galois representations of the formal group of an elliptic curve

Let K be a field of characteristic zero, complete with respect to a discrete valuation v of residue characteristic $p > 0$. Let E/K be an elliptic curve with good reduction at v. The rest of this section will be devoted to describing the image of the inertia representations:

$$\rho_{p^n,E} : I \longrightarrow \mathrm{Aut}(E[p^n](\bar{K})) \cong \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

as subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. For our purposes, we will only need to do this in the case where R is *absolutely unramified* i.e. p is a uniformiser. Let k be the residue field of K and let E_0/k be the reduction of E mod v. We say that E has *good ordinary reduction* if E_0 is ordinary and *good supersingular reduction* if E_0 is supersingular (cf. Def. 3.2.8). In the ordinary reduction case, the connected-étale sequence of $\mathscr{E}[p^\infty]$ is given by:

$$0 \longrightarrow \hat{\mathscr{E}} \longrightarrow \mathscr{E}[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0;$$

whereas in the supersingular reduction case we have $\hat{\mathscr{E}} \cong \mathscr{E}[p^\infty]$ (Thm. 3.3.17). In either case, we will first have to consider the Galois representations attached to the formal group of an elliptic curve, where the latter reduction type will be slightly more challenging as the

formal group of an elliptic curve with supersingular reduction is of height 2.

Representations of 1-dimensional formal groups

Let (K, v, R, k) be as before and suppose for now that R has absolute ramification index $e = 1$. The valuation on K extends uniquely to an algebraic closure $\bar{K}$. Denote by $\bar{R}$ and $\bar{k} = \bar{R}/\bar{\mathfrak{m}}$ the corresponding valuation ring and residue field respectively. Recall that a *1-dimensional formal group* on R is given by a power series (Def. 3.3.3):

$$f(X, Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j;$$

with $c_{ij} \in R$. The multiplication-by-p map is then given by:

$$[p](X) = \sum_{i \geq 1} a_i X^i$$

for some $a_i \in R$. As the leading terms of f are given by $X + Y + ...$, it is easy to see that $a_1 = p$. Moreover, the *height* of the formal group (viewed as a connected p-divisible group (Def. 3.3.1)) is the integer $h > 0$ such that:

$$[p](X) \equiv X^{p^h} + ... \,(\text{mod } \pi).$$

Denote by Γ the formal group associated to f and by $\Gamma[p]$ the p-torsion subgroup. Recall that the set of $\bar{K}$-points of Γ is given by the maximal ideal $\bar{\mathfrak{m}}$ (Remark 3.3.11). As $\bar{K}$ is algebraically closed, $\Gamma[p](\bar{R})$ consists of p^h points in $\bar{\mathfrak{m}}$. We will sketch Serre's proof [Ser72, 1.8, p. 267] of the following:

Proposition 3.7.7. *Let K be a characteristic 0 field, complete with respect to a discrete valuation v. Let $(R, \mathfrak{m})$ denote the valuation ring, and assume that the residue field k is of characteristic $p > 0$. Let $\bar{K}$ denote an algebraic closure of K. Extending v uniquely to K, we obtain a valuation ring $(\bar{R}, \bar{\mathfrak{m}})$ with residue field $\bar{k}$. Suppose that $f(X, Y) \in R[\![X, Y]\!]$ defines a formal group law of height h. Let $V = \Gamma[p](\bar{R})$. We have the following:*

i) V has the structure of an $\mathbb{F}_q$-vector space of dimension 1 (where $q = p^h$);

ii) The wild inertia group I_p acts trivially on V;

iii) The induced action of I_t on V is $\mathbb{F}_q$-linear and given by the fundamental character θ_{q-1}:

$$\theta_{q-1} : I_t \longrightarrow \text{Aut}_{\mathbb{F}_q}(V) \cong \mathbb{F}_q^*.$$

Proof. Note that we normalised $v : K^* \to \mathbb{Z}$ so that it is surjective. Thus, $v : \bar{K}^* \to \mathbb{Q}$ is also surjective. For $\alpha \in \mathbb{Q}$, we denote by $\bar{\mathfrak{m}}_\alpha$ the set of $x \in \bar{K}$ with $v(x) \geq \alpha$ and by $\bar{\mathfrak{m}}_\alpha^+$

the subset with $v(x) > \alpha$. Then the quotient $V_\alpha = \bar{\mathfrak{m}}_\alpha/\bar{\mathfrak{m}}_\alpha^+$ is a 1-dimensional vector space over $\bar{k}$. Moreover, there is a natural action of G_K on V_α:

$$\bar{R}/\bar{\mathfrak{m}} \times \bar{\mathfrak{m}}_\alpha/\bar{\mathfrak{m}}_\alpha^+ \longrightarrow \bar{\mathfrak{m}}_\alpha/\bar{\mathfrak{m}}_\alpha^+;$$
$$(\lambda, x) \longmapsto \lambda x.$$

This is well defined as, if $v(\lambda) \geq 0$ (resp. > 0) and $v(x) \geq \alpha$ (resp. $> \alpha$), then $v(\lambda x) \geq \alpha$ (resp. $> \alpha$). Note that two elements of $\bar{K}$ that are conjugate under G_K have the same valuation [Ser13, §2, Cor. 3] so that the action:

$$\rho : G_K \longrightarrow \mathrm{Aut}(V_\alpha)$$

is well-defined. Moreover, if $s \in G_K$ and $\sigma \in G_k = \mathrm{Gal}(\bar{k}/k)$ is its image, then we have the relation:

$$s(\lambda x) = s(\lambda)s(x) = \sigma(\lambda)s(x);$$

for all $\lambda \in \bar{k}$ and $x \in V_\alpha$; i.e. the automorphism $s : V_\alpha \to V_\alpha$ is σ-linear. Thus, if we restrict the representation to $I \subseteq G_K$, then it is $\bar{k}$-linear i.e. is given by:

$$\rho|_I : I \longrightarrow \bar{k}^*.$$

We note then that (ii) follows as $\bar{k}^*$ has no non-trivial p-torsion and so $\rho|_I$ induces a 1-dimensional representation of the tame inertia group:

$$\varphi_\alpha : I_t \longrightarrow \bar{k}^*$$

and thus is a character of the type considered in Remark 3.7.6. Indeed, Serre shows that $\varphi_\alpha = \chi_\alpha$. Returning to the kernel $V = \Gamma[p](\bar{R})$, suppose that $0 \neq x \in V$ and consider:

$$[p](x) = px + a_2x^2 + ... + a_qx^q + ... = x(p + ... + a_qx^{q-1} + ...) = 0.$$

Considering valuations, we have that $v(x) = \frac{1}{q-1}$. Setting $\alpha = v(x)$ and noting that $f(X, Y) \equiv X + Y \pmod{\bar{\mathfrak{m}}_\alpha^+}$ we have an injective homomorphism of abelian groups:

$$V \subseteq \bar{\mathfrak{m}}_\alpha \longrightarrow \bar{\mathfrak{m}}_\alpha/\bar{\mathfrak{m}}_\alpha^+ = V_\alpha.$$

Moreover, this homomorphism is G_K-equivariant. Finally, as I_p acts trivially on V we can consider the induced action of I_{t} and we have:

$$s(x) = \theta_{q-1}(s)x \quad \text{for all} \quad s \in I_{\mathrm{t}}, x \in V.$$

More specifically, the image of $I_t \to \mathrm{Aut}_{\bar{k}}(V)$ is given by the homotheties $x \mapsto \lambda x$ for each

$\lambda \in \mathbb{F}_q^*$ and is surjective onto $\mathbb{F}_q^*$. $\square$

3.7.4 Inertia representations of elliptic curves with supersingular reduction

As before, let K be a characteristic 0 field complete with respect to a discrete valuation v of absolute ramification index $e = 1$. Let R be the valuation ring with maximal ideal $\mathfrak{m}$ and residue field k of characteristic $p > 0$. Suppose that E/K is an elliptic curve with good supersingular reduction. Then there exists a model $\mathscr{E}/R$ such that $\mathscr{E}_K \cong E$ and $\mathscr{E}_k = E_0/k$ is a supersingular elliptic curve. We then have that $\hat{\mathscr{E}} \cong \mathscr{E}[p^\infty]$. Consider the inertia representation:

$$\rho_p : I \longrightarrow \mathrm{Aut}(E[p](\bar{K})) = \mathrm{Aut}(\hat{\mathscr{E}}[p](\bar{R})).$$

By results of the last subsection, one can furnish $\hat{\mathscr{E}}[p](\bar{R})$ with the structure of a 1-dimensional $\mathbb{F}_{p^2}$-vector space and the image $\rho_p(I)$ is the cyclic group $\mathbb{F}_{p^2}^*$. One cannot repeat the same analysis to given the image of $\rho_{p^n}(I)$ when $n > 1$ but we can still describe the size of the orbits:

Proposition 3.7.8. *Let K be a characteristic 0 field complete with respect to a discrete valuation v of absolute ramification index $e = 1$ (cf. 3.1.5), and residue characteristic $p > 0$. Let E/K be an elliptic curve with good supersingular reduction. Then the image of the inertia representation:*

$$\rho_p : I \longrightarrow \mathrm{Aut}(E[p](\bar{K}))$$

is a cyclic subgroup of order $q - 1$ where $q = p^2$. Suppose that $x \in E[p^n](\bar{K}) \cong \hat{E}[p^n](\bar{K})$ is of exact order p^n. Then $v(x) = \frac{1}{q^n - q^{n-1}}$ and moreover:

$$|I \cdot x| = [K^{\mathrm{nr}}(x) : K^{\mathrm{nr}}] = q^n - q^{n-1}.$$

Proof. Note that $\mathbb{F}_{p^2}$ is a 2-dimensional $\mathbb{F}_p$-vector space and so there is an inclusion:

$$\mathbb{F}_{p^2}^* \cong \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Let $x \in E[p^n](\bar{K}) \setminus E[p^{n-1}](\bar{K})$. Denote by $K^{\mathrm{nr}}(x)/K^{\mathrm{nr}}$ the smallest field extension of K^{nr} over which x is defined. Then, we have that $|I \cdot x| = [K^{\mathrm{nr}}(x) : K^{\mathrm{nr}}]$ where $I \cdot x = \{s(x) \mid s \in I\} \subset E[p^n](\bar{K})$ is the inertia orbit of x. As the extension $K^{\mathrm{nr}}(x)/K^{\mathrm{nr}}$ is totally ramified, the degree of the extension is given by the reciprocal of the valuation $v(x)$. To see that $v(x) = \frac{1}{q^n - q^{n-1}}$, one looks at the formal multiplication map $[p](X)$ again and applies an induction argument. Suppose that $y = [p](x)$ and $v(y) = \frac{1}{q^{n-1} - q^{n-2}}$. Then:

$$y = px + a_2x^2 + ... + a_qx^q + ...$$

and so $v(y) = v(x^q) = qv(x)$ and we're done. $\square$

3.7.5 Inertia representations of elliptic curves with good ordinary reduction

Let $(R, \mathfrak{m}, K, k, \pi)$ be as in the previous subsection (in particular, we still assume $e = 1$). Let E/K be an elliptic curve with good ordinary reduction. Let $\mathscr{E}/R$ be a model of E and $E_0 = \mathscr{E}/R$. Then, E_0 is an ordinary elliptic curve, and $\mathscr{E}$ is uniquely determined as a lifting of E_0 by its p-divisible group $\mathscr{E}[p^\infty]$ (cf. Thm. 3.6.2). Recall that the p-divisible group of E_0 is given by the product (Prop. 3.6.5):

$$E_0[p^\infty] = \hat{E}_0 \times (\mathbb{Q}_p/\mathbb{Z}_p).$$

Then, as these components both lift uniquely to R, $\mathscr{E}[p^\infty]$ is determined as an extension:

$$1 \to \hat{\mathscr{E}} \to \mathscr{E}[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

On the other hand, the formal moduli space of liftings of E_0 is pro-represented by $\hat{\mathbb{G}}_{m,R}$ (Thm. 3.6.3) and so this extension is parametrised by a unique element:

$$\lambda \in \hat{\mathbb{G}}_{m,R}(R) = 1 + \mathfrak{m}$$

the *Serre-Tate* coordinate of $\mathscr{E}$. In [Kr97, App.], Kraus determines this extension in the following precise sense. For any finite extension L/K, we uniquely extend the valuation v on K to L. Let $(R_L, \mathfrak{m}_L, k_L)$ denote the corresponding discrete valuation ring. We then obtain the following diagram by taking R_L-points:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 1 + \mathfrak{m}_L R_L & \xhookrightarrow{j_L} & \mathscr{E}[p^\infty](R_L) & \twoheadrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle \exists \psi_L} & & \uparrow{\scriptstyle \text{can.}} & & \\ & & & & & & \mathbb{Q}_p & & \end{array}$$

where j_L is inclusion and $\psi_L : \mathbb{Q}_p \to \mathscr{E}[p^\infty](R_L)$ is the unique homomorphism of p-divisible groups allowing the diagram to commute [Kr97, App. Lemme 1]. Then $\lambda \in 1 + \mathfrak{m}_L R_L$ is the unique element satisfying $j_L(\lambda^{-1}) = \psi_L(1)$ (independently of L). Moreover, we have a surjective morphism of $\mathrm{Gal}(L/K)$-modules:

$$f_L : (1 + \mathfrak{m}_L R_L) \times \mathbb{Q}_p \twoheadrightarrow \mathscr{E}[p^\infty](R_L)$$

with kernel $\langle \lambda, 1 \rangle$ generated by elements (λ^x, x) for $x \in \mathbb{Z}_p$. Then, the torsion subgroup $E[p^n](\bar{K})$ is isomorphic to:

$$\left\{ \left[\left(\zeta_{p^n}^i \lambda^{1/p^n}, \frac{j}{p^n} \right) \right] \,\middle|\, 0 \leq i, j < p \right\}$$

where for $(a, x) \in (1 + \mathfrak{m}_L R_L) \times \mathbb{Q}_p$ we denote by $[(a, x)] = (a, x) \pmod{\langle \lambda, 1 \rangle}$ and λ^{1/p^n} (resp. ζ_{p^n}) is a p^n-th root of λ (resp. of unity) in $\bar{K}$. In particular, we can see that the field of definition of the p^n-torsion is $L = K(E[p^n]) = K(\zeta_{p^n}, \lambda^{1/p^n})$ and $E[p^n](L)$ fits in the short exact sequence:

$$0 \to \mu_{p^n}(L) \hookrightarrow E[p^n](L) \hookrightarrow \mathbb{Z}/p^n\mathbb{Z} \to 0.$$

Picking a generator of $\mu_{p^n}(L)$ and $\mathbb{Z}/p^n\mathbb{Z}$, we can then think of the representation of I in terms of matrices:

$$\rho_{p^n} : I \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

where for $\sigma \in I$:

$$\rho_{p^n}(\sigma) = \begin{bmatrix} \chi_{p^n}(\sigma) & \psi_{p^n}(\sigma) \\ 0 & 1 \end{bmatrix}$$

where $\chi_{p^n} : I \to (\mathbb{Z}/p^n\mathbb{Z})^*$ is the cyclotomic character (or equivalently the fundamental character θ_{p^n-1} (Remark 3.7.6)) and $\psi_{p^n} : I \to (\mathbb{Z}/p^n\mathbb{Z})$ is given by the formula:

$$\zeta_{p^n}^{\psi(\sigma)} \lambda^{1/p^n} = \sigma(\lambda^{1/p^n}).$$

Remark 3.7.9. By Theorem 3.2.28, as we work over an absolutely unramified discrete valuation ring R, the extensions:

$$0 \to \mu_{p^n,R} \hookrightarrow \mathscr{E}[p^n] \hookrightarrow \mathbb{Z}/p^n\mathbb{Z} \to 0$$

are determined by knowing the Galois representation above. For example, we can write the p-torsion group scheme of $\mathscr{E}$ in terms of λ:

$$\mathscr{E}[p] = \mathrm{Spec}\left(\frac{R[X_0]}{\langle X_0^p - 1 \rangle} \times \ldots \times \frac{R[X_{p-1}]}{\langle X_{p-1}^p - \lambda^{p-1} \rangle} \right).$$

Note that if $\lambda^{1/p} \in R$ or equivalently if $v(\lambda - 1) > 1$, then $\mathscr{E}[p] \cong \mu_{p^n,R} \times \mathbb{Z}/p^n\mathbb{Z}$.

Let $N = v(\lambda - 1)$. As $e = 1$ we may take p to be a uniformiser of R. Thus $\lambda^{1/p^n} \in K$ if and only if $\lambda \in (1+pR)^{p^n} = 1 + p^{n+1}R$ and N is the unique integer such that $\lambda^{1/p^{N-1}} \in K$ but $\lambda^{1/p^N} \notin K$. By the description of the inertia action, whenever $n < N$ we have that:

$$E[p^n](\bar{K}) = \mu_{p^n,K}(\bar{K}) \times \mathbb{Z}/p^n\mathbb{Z}$$

splits as an inertia representation and the extension $K(\zeta_{p^n}, \lambda^{1/p^n}) = K(\zeta_{p^n})/K$ is degree $p^n - p^{n-1}$. When $n \geq N$ the extension $K(\zeta_{p^n}, \lambda^{1/p^n})/K$ is of degree $(p^n - p^{n-1})p^{n-N+1}$ and the extension of inertia representations is no longer split. We explicitly write down the images of inertia in the next proposition. Note that, when $\lambda = 1$, by convention we take $v(0) = \infty$, in which case the extension is split for all orders p^n, and E is the *canonical lifting* of its special fibre in the sense of Serre-Tate (cf. Thm. 3.6.3).

Proposition 3.7.10. *Let K be a characteristic 0 field complete with respect to a discrete valuation v of absolute ramification index $e = 1$, and residue characteristic $p > 0$. Write R for the valuation ring and $\mathfrak{m}$ for the maximal ideal. Let E/K be an elliptic curve with good ordinary reduction and Serre-Tate coordinate $\lambda \in 1 + \mathfrak{m}$. Write $N = v(\lambda - 1)$. Then the image of the inertia representation:*

$$\rho_{p^n} : I \to \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

is given by the subgroup:

$$\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \;\middle|\; a \in (\mathbb{Z}/p^n\mathbb{Z})^*, b \in p^{N-1}(\mathbb{Z}/p^n\mathbb{Z}) \right\}$$

where by convention, if $\lambda = 1$ and $N = \infty$ then we take $p^{N-1}(\mathbb{Z}/p^n\mathbb{Z}) = 0$.

Using this description it is easy to understand how the inertia orbits grow:

Corollary 3.7.11. *Let E/K be an elliptic curve with good ordinary reduction and Serre-Tate coordinate $\lambda \in 1 + \mathfrak{m}$. Write $N = v(\lambda - 1) \geq 0$ and suppose that $x \in E[p^n](\bar{K})$ is a point of exact order n. If $n < N$ then $E[p^n](\bar{K}) = \mu_{p^n}(\bar{K}) \times \mathbb{Z}/p^n\mathbb{Z}$ splits as an I-representation and:*

$$|I \cdot x| = \begin{cases} 1 & \text{if } x \in \mathbb{Z}/p^n\mathbb{Z} \\ p^n - p^{n-1} & \text{otherwise} \end{cases}$$

Whereas, if $n \geq N$ then $E[p^n](\bar{K})$ is no longer split and we have:

$$|I \cdot x| \geq p^{n-N+1}.$$

When E is a canonical lifting i.e. $\lambda = 1$ then we interpret the above with $N = \infty$.

Chapter 4

Raynaud's proof of the Manin-Mumford conjecture

4.1 Raynaud's proof of the Manin-Mumford conjecture

We will now describe Raynaud's proof of the Manin-Mumford conjecture in [Ray83-1]. We do this in part to see what bounds one can obtain for the conjecture of Bogomolov-Fu-Tschinkel in certain cases, as they rely carefully on several elements of his proof, but also to elucidate the more technical parts of his proof using examples, and with the hindsight of his later paper [Ray83-2] which provides a simpler proof of certain finiteness results in special cases.

Let $i : X \hookrightarrow A$ be the closed embedding of a projective, integral curve X of geometric genus $g \geq 2$ in an abelian variety A over the complex numbers. Let $A[\infty]$ denote the torsion subgroup of A. The Manin-Mumford conjecture is the following statement:

Theorem I. The set $A[\infty] \cap X(\mathbb{C})$ of torsion points of A lying on X is finite.

This is slightly more general than the classical situation, considered independently by Manin and Mumford, where X is non-singular and $A = J_X$ is the Jacobian of X. We sketch Raynaud's proof now. We first note that it is sufficient to *specialise* to the case where $i : X \hookrightarrow A$ is defined over a number field L:

Lemma 4.1.1. *Let $i : X \hookrightarrow A$ be defined over $\mathbb{C}$ as above. Then there exists some number field L and an embedding of an integral curve of geometric genus ≥ 2 into an abelian variety: $\mathscr{X}_s \hookrightarrow \mathscr{A}_s$ defined over L such that one obtains an injection:*

$$X(\mathbb{C}) \cap A[\infty] \longrightarrow \mathscr{X}_s(\bar{L}) \cap \mathscr{A}_s[\infty];$$

under an appropriate specialisation map.

Proof. Indeed, there exists some field F, finitely generated over $\mathbb{Q}$ and contained in $\mathbb{C}$ over which $i : X \hookrightarrow A$ is defined. Abusing notation, we write $i : X \hookrightarrow A$ for the corresponding morphism of F-schemes. F is the function field of some affine variety $S = \mathrm{Spec}(E)$. There exists a projective S-scheme $\mathscr{A} \to S$ such that $\mathscr{A}_F \cong A$ (for example, taking a projective embedding $A \subseteq \mathbb{P}^n_E$ and setting $\mathscr{A}$ to be the closure of A in $\mathbb{P}^n_S$). Let $\mathscr{X}$ denote the scheme-theoretic closure of X in $\mathscr{A}$. By restricting to a non-empty open subscheme U of S, we may assume that:

i) $\mathscr{A}$ is an abelian U-scheme;

ii) $\mathscr{X}$ is a proper, flat U-curve with geometrically integral fibres, and that i is a closed immersion;

iii) The normalisation $\widetilde{\mathscr{X}}$ of $\mathscr{X}$ is a proper, smooth U-curve with geometric fibres of genus ≥ 2.

Consider a closed point s of $U_{\mathbb{Q}} \subseteq S_{\mathbb{Q}}$ and let $n > 0$ be an integer. As $S_{\mathbb{Q}}$ is characteristic 0 and $\mathscr{A}_{\mathbb{Q}}$ is an abelian $S_{\mathbb{Q}}$-scheme, the group scheme $\mathscr{A}_{\mathbb{Q}}[n]$ is finite étale (Cor. 3.2.22), and thus the intersection $\mathscr{X}_{\mathbb{Q}} \cap \mathscr{A}_{\mathbb{Q}}[n]$ is also finite étale over $U_{\mathbb{Q}}$. Then, the cardinality of $X(\bar{F}) \cap A[\infty]$ is given by the rank of $\mathscr{X}_{\mathbb{Q}} \cap \mathscr{A}_{\mathbb{Q}}[n]$ over $U_{\mathbb{Q}}$. This rank is locally constant (using the étale assumption), and thus is equal to the rank of $(\mathscr{X} \cap \mathscr{A}[n])_s$. On the other hand, this is a subset of $\mathscr{X}_s \cap \mathscr{A}_s[n]$. □

Thus, we see that it is sufficient to replace X with the curve $\mathscr{X}_s$ above, for a closed point $s \in S_{\mathbb{Q}}$. Moreover, the above proof constructs a model $\mathscr{X} \hookrightarrow \mathscr{A}$ of $X \hookrightarrow A$ over U; a non-empty open subset of $\mathrm{Spec}(\mathscr{O}_L)$ where L is now a number field. Then, there exists a finite place v of L, corresponding to a closed point in U lying over a prime $p > 0$ with the following properties:

Assumption 4.1.2. *Let $i : X \hookrightarrow A$ be the embedding of an integral curve in an abelian variety A defined over a number field L. Let $\alpha : \tilde{X} \to X$ denote the normalisation, and let v be a finite place of L. Assume that:*

i) v is unramified over a prime $p > 0$;

ii) A has good reduction at v;

iii) There is a proper flat model $\mathscr{X} \to \mathrm{Spec}(\mathscr{O}_{L,v})$ of X such that the normalisation $\widetilde{\mathscr{X}} \to \mathscr{X}$ is a smooth $\mathscr{O}_{L,v}$-curve with integral fibres of genus ≥ 2.

Let R denote the complete discrete valuation ring obtained by completing the maximal unramified extension of $\widehat{\mathscr{O}}_{L,v}$ (3.7.2). Let K be the fraction field and k the residue field. Then, by construction, k is algebraically closed of characteristic $p > 0$ and p is a uniformiser of R (i.e. R is absolutely unramified (cf. 3.1.5)). Abusing notation and letting

$\mathscr{X} \hookrightarrow \mathscr{A}$ denote the corresponding morphism of R-schemes and $i : X \hookrightarrow A$ the restriction to K, it is sufficient to show that the following intersection is finite:

$$X(\bar{K}) \cap A[\infty].$$

Let $A[\infty]^{(p)}$ denote the subgroup of torsion points of order a power of p, and let $A[\infty]^{(p')}$ denote the subgroup of points of order coprime-to-p. Then, there is a direct sum decomposition:

$$A[\infty] = A[\infty]^{(p)} \oplus A[\infty]^{(p')}.$$

By the Néron-Ogg-Shafarevich criterion (Thm. 3.7.1), the inertia group I_K acts trivially on $A[\infty]^{(p')}$. However, as K is maximally unramified, the absolute Galois group $G_K = \mathrm{Gal}(\bar{K}/K)$ coincides with I_K (3.7.2) and thus $A[\infty]^{(p')}$ is K-rational. On the other hand, as $A[\infty]^{(p')}$ is a torsion group, with all elements of order coprime-to-p, the multiplication-by-p map acts bijectively (for group-theoretic reasons), and so we have an inclusion:

$$A[\infty]^{(p')} \cap X(\bar{K}) \subseteq pA(\bar{K}) \cap X(\bar{K}) = pA(K) \cap X(K).$$

As $\mathscr{A}/R$ is proper, we have that $pA(K) \cap X(K) = p\mathscr{A}(R) \cap \mathscr{X}(R)$. As A has good reduction at v, the torsion points of $\mathscr{A}$ of order coprime-to-p specialise injectively into the special fibre $\mathscr{A}_k$ (using Ex. 3.3.12 (ii) for example). Overall, to show that the intersection $X(\bar{K}) \cap A[\infty]^{(p')}$ is finite, it suffices to prove the following:

Theorem II. The image of the following intersection:

$$\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{A}(k),$$

is finite under reduction modulo p.

4.1.1 Normal bundles

We will give the following definitions now in view of our discussion on the normal bundle later:

Definition 4.1.3. Let $i : X \hookrightarrow Y$ be a closed immersion of codimension r. We say that i is a *regular embedding* if the ideal sheaf $\mathscr{I}$ of X in Y is globally generated by r sections. We say that i is a *local complete intersection* (*lci*) if it factorises into $i : X \xrightarrow{i'} Y' \xrightarrow{p} Y$ where i' is a regular embedding and p is smooth. Write $\mathscr{I}_{X/Y}$ for the ideal sheaf and $\mathscr{C}_{X/Y} = \mathscr{I}_{X/Y}/\mathscr{I}^2_{X/Y}$ for the conormal sheaf. Note that, when $i : X \hookrightarrow Y$ is lci, the conormal sheaf, and dually the normal sheaf $\mathscr{N}_{X/Y} = \mathscr{C}^\vee_{X/Y}$ are locally free of rank r.

Suppose that $X \xrightarrow{i} Y \xrightarrow{j} Z$ are regular (resp. lci) embeddings. Note that the composition $j \circ i$ is regular (resp. lci), and the corresponding exact sequence of ideal

sheaves:

$$j^*\mathscr{I}_{Y/Z} \longrightarrow j^*\mathscr{I}_{X/Z} \longrightarrow \mathscr{I}_{X/Y} \longrightarrow 0;$$

(resp. conormal sheaves:

$$i^*\mathscr{C}_{Y/Z} \longrightarrow \mathscr{C}_{X/Z} \longrightarrow \mathscr{C}_{X/Y} \longrightarrow 0;$$

) is left exact [Ful-Lang13, Prop. 3.4].

Relative Proj and Relative Spec

Definition 4.1.4. Let S be a scheme and $\mathscr{H}$ a quasi-coherent sheaf of $\mathscr{O}_S$-algebras.

i) There exists an affine morphism $\pi : \underline{\mathrm{Spec}}_S(\mathscr{H}) \to S$ with the property that, for every affine open $U = \mathrm{Spec}(A) \subset S$ we have that $\pi^{-1}(U) \cong \mathrm{Spec}(\mathscr{H}(U))$. We call $\underline{\mathrm{Spec}}_S(-)$ the *relative spectrum* functor.

ii) Similarly, if $\mathscr{H} = \bigoplus_{d\geq 0} \mathscr{H}_d$ is a quasi-coherent sheaf of graded $\mathscr{O}_S$-algebras then there exists a projective morphism $\pi : \underline{\mathrm{Proj}}_S(\mathscr{H}) \to S$ such that, for every affine open $U = \mathrm{Spec}(A) \subset S$ we have that $\pi^{-1}(U) \cong \mathrm{Proj}(\mathscr{H}(U))$. We call this the *relative Proj construction.*

Example 4.1.5. For $\mathscr{E}$ a quasi-coherent sheaf of $\mathscr{O}_S$-modules, the sheaf $\mathscr{H} = \mathrm{Sym}(\mathscr{E})$ is naturally a sheaf of graded $\mathscr{O}_S$-algebras under the symmetric product. For example, if $\mathscr{E} \cong \mathscr{O}_S^{\oplus(n+1)}$ then $\mathrm{Sym}(\mathscr{E}) \cong \mathscr{O}_S[T_0, T_1, ...T_n]$ with $\deg(T_i) = 1$. Let $\mathbb{P}(\mathscr{E})$ (resp. $\mathbb{V}(\mathscr{E})$) denote $\underline{\mathrm{Proj}}_S(\mathscr{H}) \to S$ (resp. $\underline{\mathrm{Spec}}_S(\mathscr{H}) \to S$). Note that by convention, the sheaf of sections of the morphism $\mathbb{V}(\mathscr{E}) \to S$ is given by the *dual* $\mathscr{E}^\vee$. We note the following properties:

i) Both $\mathbb{V}$ and $\mathbb{P}$ are contravariant functors.

ii) If $\mathscr{L}$ is an invertible sheaf on S, then $\mathbb{P}(\mathscr{L}) \cong S$.

iii) Moreover, if $\mathscr{E}$ is a quasi-coherent $\mathscr{O}_S$-module then:

$$\mathbb{P}(\mathscr{E} \otimes_{\mathscr{O}_S} \mathscr{L}) \cong \mathbb{P}(\mathscr{E}).$$

Given a a quasi-coherent sheaf of $\mathscr{O}_S$-modules $\mathscr{E}$, there is a natural 'compactification' of $\mathbb{V}(\mathscr{E})$ given by $\mathbb{P}(\mathscr{E}\oplus\mathscr{O}_S)$; the *projective cone* of $\mathbb{V}(\mathscr{E})$ [Ful-Lang13, p. 68]. Indeed, we have that $\mathrm{Sym}(\mathscr{E} \oplus \mathscr{O}_S) \cong \mathrm{Sym}(\mathscr{E})[T]$ as a sheaf of graded $\mathscr{O}_S$-algebras by setting $\deg(T) = 1$. The projection $\mathscr{E} \oplus \mathscr{O}_S \to \mathscr{E}$ corresponds to a closed immersion $\mathbb{P}(\mathscr{E}) \hookrightarrow \mathbb{P}(\mathscr{E} \oplus \mathscr{O}_S)$ which one can think of as the *hyperplane at infinity* corresponding to $T = 0$. Conversely, the locus $T \neq 0$ corresponds to an open immersion $\mathbb{V}(\mathscr{E}) \hookrightarrow \mathbb{P}(\mathscr{E} \oplus \mathscr{O}_S)$. The projective cone

comes naturally equipped with a *zero section* $S \to \mathbb{V}(\mathscr{E}) \hookrightarrow \mathbb{P}(\mathscr{E} \oplus \mathscr{O}_S)$ induced by the second projection $\mathscr{E} \oplus \mathscr{O}_S \to \mathscr{O}_S$. Overall, we have a decomposition into open and closed subschemes:

$$\mathbb{P}(\mathscr{E} \oplus \mathscr{O}_S) \cong \mathbb{V}(\mathscr{E}) \sqcup \mathbb{P}(\mathscr{E}).$$

Lemma 4.1.6. *Let $\mathscr{E}$ be a quasi-coherent sheaf of $\mathscr{O}_S$-modules. Consider the functor:*

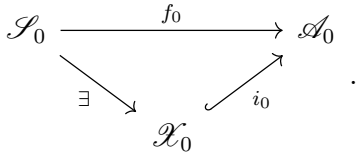
$$\begin{aligned} F : (\mathrm{Sch}/S)^{\mathrm{op}} &\longrightarrow \mathrm{Set}; \\ (f : T \to S) &\longmapsto \mathrm{Hom}_{\mathscr{O}_T}(f^*\mathscr{E}, \mathscr{O}_T) \end{aligned}$$

Then F is represented by $\mathbb{V}(\mathscr{E})$.

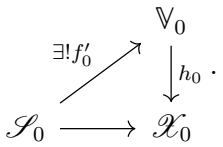
Proof. See [stacks-project, Definition 27.4.5]. □

Let R be a discrete valuation ring with maximal ideal $\mathfrak{m}$, π a uniformiser, and residue field k. For each $n > 0$ write $R_n := R/\mathfrak{m}^{n+1}$. If $\mathscr{S}$ is an R-scheme, we will denote by $\mathscr{S}_n$ the restriction to R_n and $\mathscr{S}_0$ the special fibre over k. Similarly, for a morphism of R-schemes $f : \mathscr{S} \to \mathscr{S}'$ we use the notations $f_n : \mathscr{S}_n \to \mathscr{S}'_n$ and $f_0 : \mathscr{S}_0 \to \mathscr{S}'_0$ for the corresponding restrictions. Recall that an R_1-scheme $f_1 : \mathscr{S}_1 \to \mathrm{Spec}(R_1)$ is flat if and only if the natural map $\mathscr{O}_{\mathscr{S}_0} \to \pi\mathscr{O}_{\mathscr{S}_1}$ is an isomorphism (Cor. 3.5.6). Let $\mathscr{A}_1$ be an R_1-scheme and suppose that $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ is a closed embedding. We will construct an affine morphism $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ with the following lifting property:

Proposition 4.1.7. *There exists an affine morphism $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ such that, for every morphism of flat R_1-schemes $f_1 : \mathscr{S}_1 \to \mathscr{A}_1$ where the restriction $f_0 : \mathscr{S}_0 \to \mathscr{A}_0$ factorises as:*



There exists a unique morphism $f'_0 : \mathscr{S}_0 \to \mathbb{V}_0$ such that the following diagram commutes:



Before constructing $\mathbb{V}_0$, we immediately note the following properties:

i) There is a one-to-one correspondence between flat liftings $i_1 : \mathscr{X}_1 \hookrightarrow \mathscr{A}_1$ of i_0 and sections of $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$.

ii) Denote by $(\mathscr{A}_1, \mathscr{X}_0)(R_1) \subseteq \mathscr{A}_1(R_1)$ the subset of R_1-points of $\mathscr{A}_1$ that reduce mod $\mathfrak{m}$ to k-points of $\mathscr{X}_0$. Then there exists a commutative diagram:

$$\begin{array}{ccc} (\mathscr{A}_1, \mathscr{X}_0)(R_1) & \xrightarrow{\tau} & \mathbb{V}_0(k) \\ & \searrow & \downarrow h_0 \\ & & \mathscr{X}_0(k) \end{array} .$$

Proof of Prop. 4.1.7. For ease of exposition, we will assume first that there exists a morphism of flat R_1-schemes $i_1 : \mathscr{X}_1 \hookrightarrow \mathscr{A}_1$ lifting i_0, and that i_0 is lci. Let $\mathscr{I}_0$ denote the ideal sheaf of $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ which lifts to the ideal sheaf $\mathscr{I}_1$ of $\mathscr{X}_1 \hookrightarrow \mathscr{A}_1$. We denote by $\mathscr{I}_1'$ the ideal sheaf of $\mathscr{X}_0 \hookrightarrow \mathscr{A}_0 \hookrightarrow \mathscr{A}_1$. Then there exists an exact sequence of ideal sheaves:

$$\mathscr{O}_{\mathscr{A}_0} \longrightarrow \mathscr{I}_1' \longrightarrow \mathscr{I}_0 \longrightarrow 0;$$

and an exact sequence of conormal sheaves:

$$0 \longrightarrow \mathscr{O}_{\mathscr{X}_0} \longrightarrow \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1} \longrightarrow \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0} \longrightarrow 0. \qquad (*)$$

Note that we assumed $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ to be a local complete intersection so this sequence is left exact. The flat lifting $i_1 : \mathscr{X}_1 \hookrightarrow \mathscr{A}_1$ of i_0 corresponds to a splitting of this exact sequence so we obtain a (non-canonical) decomposition:

$$\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1} \cong \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0} \oplus \mathscr{O}_{\mathscr{X}_0}.$$

Indeed, if we let $\mathscr{I}_1$ denote the ideal sheaf of i_1, then there is another exact sequence of conormal sheaves corresponding to $\mathscr{X}_0 \hookrightarrow \mathscr{X}_1 \hookrightarrow \mathscr{A}_1$:

$$0 \longrightarrow \mathscr{C}_{\mathscr{X}_1/\mathscr{A}_1}|_{\mathscr{X}_0} \longrightarrow \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1} \xrightarrow{r} \mathscr{O}_{\mathscr{X}_0} \longrightarrow 0.$$

The morphism of sheaves r provides a retraction of the short exact sequence $(*)$. Using the projective cone construction, we then obtain a decomposition of the associated projective bundle:

$$\mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \cong \mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \sqcup \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}).$$

We denote by $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ the affine bundle corresponding to the image of the open immersion:

$$\mathbb{V}_0 = \mathrm{Im}(\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \hookrightarrow \mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1})).$$

Recall that the sections of $\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \mathscr{X}_0$ are in bijection with the global sections of the normal bundle $\mathscr{N}_{\mathscr{X}_0/\mathscr{A}_0}$. Informally, one should think of $\mathbb{V}_0$ as the affine bundle corresponding to normal vectors of $\mathscr{X}_0 \hookrightarrow \mathscr{A}_1$ that *do not* lie in the special fibre $\mathscr{A}_0$. Recall

that $\mathbb{V}(\mathscr{I}_1') \to \mathscr{A}_1$ represents the following functor:

$$\begin{aligned} F : (\mathrm{Sch}/\mathscr{A}_1)^{\mathrm{op}} &\longrightarrow \mathrm{Set}; \\ (f : T \to \mathscr{A}_1) &\longmapsto \mathrm{Hom}_{\mathscr{O}_T}(f^*(\mathscr{I}_1'), \mathscr{O}_T). \end{aligned}$$

Consider the subfunctor $F'(T) = \{u \in F(T) \mid u(\pi) = 1\}$ where, abusing notation, π denotes the section of $f^*(\mathscr{I}_1')$ corresponding to the chosen uniformiser π of R. Raynaud shows that this functor is representable by an $\mathscr{A}_1$-scheme $V_0 \subseteq \mathbb{V}(\mathscr{I}_1')$. Note that if $u : f^*(\mathscr{I}_1') \to \mathscr{O}_T$ is a point of $F'(T)$ then $0 = u(\pi^2) = \pi \cdot u(\pi) = \pi \cdot 1$ and thus $\pi \cdot \mathscr{O}_T = 0$. Moreover, $\mathscr{I}_1' \cdot \mathscr{O}_T = u(\pi \mathscr{I}_1') = \pi \cdot u(\mathscr{I}_1') = 0$ so, in fact, the morphism u factors as:

$$u : f^*(\mathscr{I}_1') \longrightarrow f^*(\mathscr{I}_1'/(\mathscr{I}_1')^2) \longrightarrow \mathscr{O}_T;$$

i.e. $V_0 \subseteq \mathbb{V}(\mathscr{I}_1'/(\mathscr{I}_1')^2) = \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1})$ and V_0 is an $\mathscr{X}_0$-scheme. From this description, one can see that the schemes V_0 and $\mathbb{V}_0$ coincide. Indeed, given a splitting $\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1} \cong \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0} \oplus \mathscr{O}_{\mathscr{X}_0}$, we see that:

$$\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \cong \underline{\mathrm{Spec}}_{\mathscr{X}_0}(\mathrm{Sym}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})[t]);$$

where the parameter t corresponds to the generator $\pi \in \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}$. The sublocus $V_0 \subseteq \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1})$ is given by setting the coordinate $t = 1$. On the other hand, there is a rational map $\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \dashrightarrow \mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1})$ defined away from the zero section (this is analagous to the quotient map $\mathbb{A}^{n+1} \dashrightarrow \mathbb{P}^n$). Again, identifying:

$$\mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \cong \underline{\mathrm{Proj}}_{\mathscr{X}_0}(\mathrm{Sym}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})[T]);$$

we see that the sublocus $\mathbb{V}_0 \subseteq \mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1})$ is given by setting the (homogeneous) coordinate $T \neq 0$. So we see that, as V_0 and $\mathbb{V}_0$ are defined away from the zero section, they become identified under this rational map. The upshot of this approach is that the lifting property of $\mathbb{V}_0$ is now clear. Let $f_1 : \mathscr{S}_1 \to \mathscr{A}_1$ be a morphism of flat R_1-schemes and suppose that the restriction to k factorises as $f_0 : \mathscr{S}_0 \to \mathscr{X}_0 \hookrightarrow \mathscr{A}_1$. Then, we have that $\mathscr{I}_1' \cdot \mathscr{O}_{\mathscr{S}_1} = \pi \cdot \mathscr{O}_{\mathscr{S}_1}$. By flatness, we may associate $\pi \cdot \mathscr{O}_{\mathscr{S}_1} \cong \mathscr{O}_{\mathscr{S}_0}$ sending π to 1. Overall, this gives us a morphism of $\mathscr{O}_{\mathscr{S}_0}$-modules:

$$f_0^*(\mathscr{I}_1') \to \mathscr{I}_1' \cdot \mathscr{O}_{\mathscr{S}_1} = \pi \cdot \mathscr{O}_{\mathscr{S}_1} \cong \mathscr{O}_{\mathscr{S}_0};$$

sending $\pi \mapsto 1$, and thus we obtain a morphism $f_1' : \mathscr{S}_1 \to \mathbb{V}_0$ as required. □

Note that the above construction shows that $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ is a torsor (cf. Def.

3.5.10) under $\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$. Indeed, there is an additive action:

$$\begin{array}{ccc} \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \times \mathbb{V}_0 & \longrightarrow & \mathbb{V}_0 \\ & \searrow & \downarrow h_0 \\ & & \mathscr{X}_0 \end{array}$$

which may be seen from the functor of points perspective. Recall that $\mathbb{V}_0 \to \mathscr{X}_0$ represents the functor F' from the Proposition. Similarly, $\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$ represents the functor $F_0(T) = \mathrm{Hom}_{\mathscr{O}_T}(g^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}), \mathscr{O}_T)$ where $g : T \to \mathscr{X}_0$ is a morphism of schemes. If $f : T \to \mathscr{A}_1$, then one obtains the exact sequence:

$$f^*(\mathscr{O}_{\mathscr{X}_0}) \longrightarrow f^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \xrightarrow{\theta} f^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \longrightarrow 0$$

noting that the pushforward is right exact. If $u, u' \in F'(T)$, then $u' - u : f^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}) \to \mathscr{O}_T$ sends π to 0 and thus corresponds to a unique morphism of $\mathscr{O}_T$-modules $v : f^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \mathscr{O}_T$ such that $u' - u = v \circ \theta$. This defines an additive group action:

$$F_0(T) \times F'(T) \longrightarrow F'(T)$$

sending $(v, u) \mapsto u + v \circ \theta$ that is natural in T. The action is free and transitive by the uniqueness of v; and thus defines a torsor.

Remark 4.1.8. Recall that, given a scheme X and quasi-coherent *ideal sheaf* $\mathscr{I} \subseteq \mathscr{O}_X$, one defines the *blow-up* of X with *centre* $\mathscr{I}$ via the relative Proj construction:

$$\pi : \mathrm{Bl}_{\mathscr{I}}(X) = \mathbb{P}(\mathscr{I}) = \underline{\mathrm{Proj}}_X(\mathscr{O}_X \oplus \mathscr{I} \oplus \mathscr{I}^2 \oplus ...) \longrightarrow X.$$

Then, if $Y \subseteq X$ is the corresponding closed subscheme, the exceptional divisor $\pi^{-1}(Y)$ corresponds naturally to $\mathbb{P}(\mathscr{I}/\mathscr{I}^2) = \mathbb{P}(\mathscr{C}_{X/Y})$.

This gives a more geometric description of the scheme $\mathbb{V}_0$ in the case where we have a lift of $\mathscr{A} \to \mathrm{Spec}(R)$ of $\mathscr{A}_1$. Let $\mathscr{I}_0$ denote the ideal sheaf of $\mathscr{X}_0$ in $\mathscr{A}_0$ as before, but now let $\mathscr{I}'$ denote the ideal sheaf of $\mathscr{X}_0$ in $\mathscr{A}$. Write $\mathscr{V} \subset \mathrm{Bl}_{\mathscr{X}_0}(\mathscr{A}) = \mathbb{P}(\mathscr{I}') \to \mathscr{A}$ for the open subscheme of the blow-up of $\mathscr{A}$ at $\mathscr{X}_0$ where the homogeneous coordinate in $\mathbb{P}(\mathscr{I}')$ corresponding to the generator $\pi \in \mathscr{I}'$ becomes invertible. Then, associating $\mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}})$ with the exceptional divisor, we obtain an $\mathscr{X}_0$-scheme $\mathscr{V}_0 = \mathscr{V}_0 \cap \mathbb{P}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}}) \to \mathscr{X}_0$. One may check that this coincides with the affine morphism $\mathbb{V}_0 \to \mathscr{X}_0$.

Example 4.1.9. The blow-up construction in the previous Remark allows one to write down the affine bundle $\mathbb{V}_0$ explicitly in certain cases. For example, if $\mathscr{A} = \mathbb{A}^2_R$ with coordinates x and y, and $\mathscr{X}$ is given by an irreducible polynomial $f \in R[x, y]$, then the

ideal defining $\mathscr{X}_0$ in $\mathscr{A}$ is given by $I = \langle \pi, f \rangle$. Thus we have:

$$\mathrm{Bl}_{\mathscr{X}_0}(\mathscr{A}) = \mathrm{Proj}\left(\frac{R[x,y][T_0,T_1]}{\langle fT_0 - \pi T_1 \rangle}\right).$$

The open set where the generator T_0 corresponding to π is invertible is given by $\mathscr{V} = \mathrm{Spec}\left(\frac{R[x,y][t]}{\langle f - \pi t \rangle}\right)$. We then see that the special fibre is $\mathscr{V}_0 = \mathrm{Spec}\left(\frac{k[x,y][t]}{\langle f_0 \rangle}\right) \cong \mathscr{X}_0 \times \mathbb{A}^1_k$. Unsurprisingly, the affine bundle $\mathbb{V}_0$ is trivial as $\mathscr{X}_0$ is an affine, lci curve in $\mathbb{A}^2_k$. Suppose that $(a_1, b_1) \in (\mathbb{A}^2_{R_1}, \mathscr{X}_0)(R_1)$. Then $f_0(a_0, b_0) = 0$ and so $f_1(a_1, b_1) = \pi e_1$ for some $e_1 \in R_1$. Thus, the map τ can be written explicitly as:

$$\begin{aligned} \tau : (\mathbb{A}^2_{R_1}, \mathscr{X}_0)(R_1) &\longrightarrow \mathscr{X}_0(k) \times \mathbb{A}^1(k); \\ (a_1, b_1) &\longmapsto ((a_0, b_0), e_0) \end{aligned}$$

where we identify $\pi e_1 \mapsto e_0$ under the isomorphism $\pi R_1 \xrightarrow{\sim} k$ of R_1-modules.

4.1.2 Lifting morphisms with zero k-differential

Keeping the notation of the previous section, we now assume that p is a generator of the maximal ideal of R_1, and that k is algebraically closed of characteristic p for some prime $p > 0$. Suppose that $u_1 : \mathscr{B}_1 \to \mathscr{A}_1$ is a morphism of smooth (in particular, flat) R_1-schemes. Suppose further that the restriction $u_0 : \mathscr{B}_0 \to \mathscr{A}_0$ has zero k-differential. Let $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ be a closed immersion. As the differential of u_0 is zero, the scheme-theoretic preimage $u_0^{-1}(\mathscr{X}_0)$ is automatically non-reduced. Let $j_0 : \mathscr{Y}_0 = u_0^{-1}(\mathscr{X}_0)^{\mathrm{red}} \hookrightarrow \mathscr{B}_0$ denote the same closed subspace with the reduced induced subscheme structure. Let $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ denote the affine morphism from the previous section. We will show that it enjoys another lifting property:

Proposition 4.1.10. *Let $u_1 : \mathscr{B}_1 \to \mathscr{A}_1$, $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ and $j_0 : \mathscr{Y}_0 \hookrightarrow \mathscr{B}_0$ be as above. Write $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ for the restriction of u_0 to $\mathscr{Y}_0$. Then, there exists a unique morphism $v_0' : \mathscr{Y}_0 \to \mathbb{V}_0$ such that the following diagram commutes:*

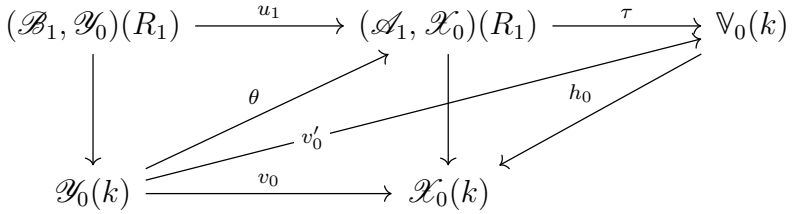
$$\begin{array}{ccc} & & \mathbb{V}_0 \\ & \overset{v_0'}{\nearrow} & \big\downarrow {\scriptstyle h_0} \\ \mathscr{Y}_0 & \xrightarrow[v_0]{} & \mathscr{X}_0 \end{array}.$$

On points, the existence of such a lifting is not hard to see. Firstly, we note that

there is a unique map $\theta : \mathscr{B}_0(k) \to \mathscr{A}_1(R_1)$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathscr{B}_1(R_1) & \xrightarrow{u_1} & \mathscr{A}_1(R_1) \\ \downarrow & \overset{\theta}{\nearrow} & \downarrow \\ \mathscr{B}_0(k) & \xrightarrow[u_0]{} & \mathscr{A}_0(k) \end{array}$$

where the vertical maps are given by specialisation. Indeed, by the infinitesimal lifting criterion (Prop. 3.5.7), if $\sigma_0 \in \mathscr{B}_0(k)$ then there exists a (non-unique) choice of lifting $\sigma_1 \in \mathscr{B}_1(R_1)$. We define θ by setting $\theta(\sigma_0) = u_1(\sigma_1)$. If this is well-defined, then commutativity of the above diagram is clear. Suppose $\sigma_1' \in \mathscr{B}(R_1)$ also lifts σ_0. Then, by flatness of $\mathscr{B}_1$, we have that $\sigma_1 - \sigma_1' = ps_1$ for some section $s_1 \in \mathscr{B}(R_1)$. Recall that, we may naturally associate $T_{\sigma_0}\mathscr{B}_0 \cong \ker(\mathscr{B}_1(R_1) \longrightarrow \mathscr{B}_0(k))$. Thus, as the differential of u_0 is zero, we have that $u_1(ps_1) = 0$ and θ is well defined. Reprising the notation $(\mathscr{A}_1, \mathscr{X}_0)(R_1) \subseteq \mathscr{A}_1(R_1)$ to denote points in $\mathscr{A}_1$ that specialise to points of $\mathscr{X}_0$, and defining $(\mathscr{B}_1, \mathscr{Y}_0)(R_1) \subseteq \mathscr{B}_1(R_1)$ similarly, we obtain a commutative diagram:



where we define $v_0' = \tau \circ \theta$ using the unique map τ from property (ii) of Prop. 4.1.7. It will require slightly more work to show that v_0' is induced by a morphism of schemes. First, we will require the following fact:

Lemma 4.1.11. *Let k be a perfect field of characteristic $p > 0$. Suppose that $\varphi : N \to M$ is a homomorphism of finitely generated k-algebras such that the induced morphism of modules of Kähler differentials:*

$$\Omega_{N/k} \otimes_N M \longrightarrow \Omega_{M/k}$$

is zero. Then, for any $a \in N$, $\varphi(a)$ is a p-th power in M.

Proof. Consider the commutative diagram:

$$\begin{array}{ccc} \Omega_{N/k} \otimes_N M & \xrightarrow{0} & \Omega_{M/k} \\ \uparrow & & \uparrow \\ N & \xrightarrow{\varphi} & M \end{array}$$

where the vertical maps are the respective universal derivations. By commutativity, $\varphi(a) \in \ker(d)$; the kernel of the universal derivation $d : M \to \Omega_{M/k}$. We then conclude by noting

$\ker(d) = M^p$ [stacks-project, Lemma 10.158.2]. $\square$

Suppose that $\varphi_1 : M_1 \to N_1$ is a morphism of finitely generated, flat R_1-algebras such that $\varphi_0 : M_0 = M_1 \otimes_{R_1} k \to N_1 \otimes_{R_1} k = N_0$ has zero k-differential. Let $a_1 \in M_1$ and $a_0 \in M_0$ its reduction mod p. Then $\varphi_0(a_0) = \alpha_0^p$ is a p-th power for some element $\alpha_0 \in N_0$. Picking some lifting $\alpha_1 \in N_1$ of α_0, we define the *Teichmüller lift* of a_0 to be $\tau(a_0) = \alpha_1^p$. This is well defined as if α_1' is another lift of α_0, then by flatness we have that $\alpha_1' = \alpha_1 + p\beta_1$ for some $\beta_1 \in N_1$ and $(\alpha_1')^p = \alpha_1^p$. The Teichmüller lift fits in the following diagram:

$$\begin{array}{ccc} N_1 & \xrightarrow{\varphi_1} & M_1 \\ \downarrow & \overset{\tau}{\nearrow} & \downarrow \\ N_0 & \xrightarrow[\varphi_0]{} & M_0 \end{array}$$

It satisfies the following properties:

i) $\tau(a_0 b_0) = \tau(a_0)\tau(b_0)$;

ii) $\tau(a_0 + b_0) = \tau(a_0) + \tau(b_0) + pS(\alpha_0, \beta_0)$;

where $a_0, b_0 \in M_0$, $\varphi_0(a_0) = \alpha_0^p$, $\varphi_0(b_0) = \beta_0^p$, and $S \in \mathbb{Z}[U, V]$ is the homogeneous polynomial given by:

$$S(U, V) = \frac{(U+V)^p - U^p - V^p}{p}.$$

Proof. Note that, on local sections, we have a Teichmüller lifting:

$$\begin{array}{ccc} \mathscr{O}_{\mathscr{A}_1} & \xrightarrow{u_1^\#} & \mathscr{O}_{\mathscr{B}_1} \\ \downarrow & \overset{\tau}{\nearrow} & \downarrow \\ \mathscr{O}_{\mathscr{A}_0} & \xrightarrow[u_0^\#]{} & \mathscr{O}_{\mathscr{B}_0} \end{array}.$$

Specifically, for a local section $a_1 \in \mathscr{O}_{\mathscr{A}_1}$ with image $a_0 \in \mathscr{O}_{\mathscr{A}_1}$, we have that $u_0^\#(a_0) = \alpha_0^p$ as u_0 has zero differential. Then, by smoothness of $\mathscr{B}_1$, there exists a lift $\alpha_1 \in \mathscr{O}_{\mathscr{B}_1}$ of $\alpha_0 \in \mathscr{O}_{\mathscr{B}_0}$. The Teichmüller lift is then given by $\beta_1^p \in \mathscr{O}_{\mathscr{B}_1}$. By flatness of $\mathscr{B}_1$, we can compare the Teichmüller lift with the image $u_1^\#(a_1)$ to obtain the *p-derivation* (associated to u_1) on local sections:

$$\delta = \frac{u_1^\# - \tau}{p} : \mathscr{O}_{\mathscr{A}_1} \longrightarrow p\mathscr{O}_{\mathscr{B}_1} \cong \mathscr{O}_{\mathscr{B}_0}.$$

Concretely, if $a_1, b_1 \in \mathscr{O}_{\mathscr{A}_1}$ are local sections such that $u_0^\#(a_0) = \alpha_0^p$ and $u_0^\#(b_0) = \beta_0^p$ for some local sections $\alpha_0, \beta_0 \in \mathscr{O}_{\mathscr{B}_0}$ then there are unique sections $\delta(a_1), \delta(b_1) \in \mathscr{O}_{\mathscr{B}_0}$ such that:

$$u_1^\#(a_1) = \tau(a_0) + p\delta(a_1) \quad \text{and} \quad u_1^\#(b_1) = \tau(b_0) + p\delta(b_1);$$

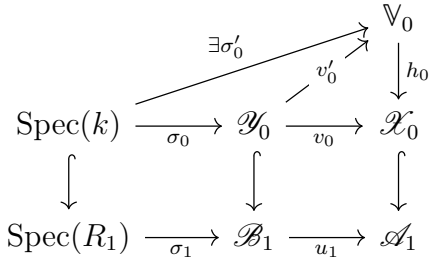
where we write $p\delta(a_1), p\delta(b_1)$ for the sections of $p\mathscr{O}_{\mathscr{B}_1} \cong \mathscr{O}_{\mathscr{B}_0}$ corresponding to $\delta(a_1), \delta(b_1)$ respectively. We note the following properties of δ:

$$\begin{aligned}\delta(a_1 + b_1) &= \delta(a_1) + \delta(b_1) + S(\alpha_0, \beta_0);\\ \delta(a_1 b_1) &= \delta(a_1) u_0^{\#}(b_0) + u_0^{\#}(a_0)\delta(b_1);\\ \delta(p) &= 1.\end{aligned}$$

Note that the second condition is a Leibniz rule, twisted by u_0, hence the name p-derivation. In fact, one can deduce the third condition from the first two and the fact that $\delta(1) = 0$. Let $\mathscr{I}_0$ denote the sheaf of ideals of $\mathscr{X}_0$ in $\mathscr{A}_0$ and $\mathscr{J}_0$ denote the sheaf of ideals of $\mathscr{Y}_0$ in $\mathscr{B}_0$. Again, we use the notation $\mathscr{I}_1'$ to define the ideal sheaf of $\mathscr{X}_0$ in $\mathscr{A}_1$. Using the p-derivation, we can construct a morphism of $\mathscr{O}_{\mathscr{Y}_0}$-modules $\nu : u_1^*(\mathscr{I}_1') \to \mathscr{O}_{\mathscr{Y}_0}$ such that $\nu(p) = 1$, and thus obtain a morphism $v_0' : \mathscr{Y}_0 \to \mathbb{V}_0$ by the lifting property of $\mathbb{V}_0$. Let:

$$\begin{aligned}\nu : u_1^*(\mathscr{I}_1') &\longrightarrow \mathscr{O}_{\mathscr{Y}_0};\\ u_1^*(a_1) &\longmapsto \delta(a_1) \,(\mathrm{mod}\ \mathscr{J}_0).\end{aligned}$$

To see this is well-defined, note that if $a_1 \in \mathscr{I}_1'$ is a local section, then $u_0^{\#}(a_0) = \alpha_0^p \in \mathscr{J}_0$. Since $\mathscr{Y}_0$ is reduced, we have that $\alpha_0 \in \mathscr{J}_0$ and therefore $u_0^{\#}(a_0) \in \mathscr{J}_0^p$. Using this fact, and the conditions of δ, one sees that ν is $\mathscr{O}_{\mathscr{Y}_0}$-linear, and that $\nu(p) = 1$. We conclude by showing that $v_0' : \mathscr{Y}_0 \to \mathbb{V}_0$ coincides with the map we constructed earlier on k-points. Indeed, the above process is functorial with respect to morphisms of R_1-schemes whose restriction to k has zero differential, so if we have a section $\sigma_1 : \mathrm{Spec}(R_1) \to \mathscr{B}_1$ fitting into the following diagram:



then there exists a section $\sigma_0' : \mathrm{Spec}(k) \to \mathbb{V}_0$ allowing the diagram to commute. Thus, $\tau(u_1 \circ \sigma_1) = v_0' \circ \sigma$. □

Remark 4.1.12. Note that, if M_1, N_1 are flat R_1-algebras and $u_0 : M_0 \to N_0$ is a k-algebra morphism with zero differential, then one may define a p-derivation $\delta : M_1 \to N_0$ using the conditions from the above proof. Then, a lifting $u_1 : M_1 \to N_1$ of u_0 is equivalent to specifying a p-derivation:

$$u_1 = \tau + p\delta$$

by noting that the Teichmüller lifting τ depends only on u_0. In fact, we have formalised this result already in Theorem 3.5.20 (ii). If $f_0 : X_0 \to Y_0$ is a finite flat morphism of projective k-schemes with respective liftings X_1 and Y_1 to R_1, then the space of liftings of f_0 to R_1 is a torsor under $H^0(X_0, \mathscr{H}om(f_0^*(\Omega_{Y_0/k}), \mathscr{O}_{X_0}))$. Recalling that $\mathrm{Der}_k(\mathscr{O}_{Y_0}) \cong \mathscr{H}om(\Omega_{Y_0/k}, \mathscr{O}_{Y_0})$ we see that these global sections can be thought of as *twisted derivations*.

Example 4.1.13. Returning to Example 4.1.9, we reprise the notation $\mathscr{X} = \{f = 0\} \subseteq \mathbb{A}^2_R$ for some irreducible polynomial $f \in R[x, y]$. Suppose further that $\mathscr{X}$ is a smooth R-curve, and consider the morphism $u : \mathbb{A}^2_R \to \mathbb{A}^2_R$ given by $u(x, y) = (x^p, y^p)$. Then $u_0 : \mathbb{A}^2_k \to \mathbb{A}^2_k$ has zero k-differential. The preimage $u_0^{-1}(\mathscr{X}_0) = \{f_0(x^p, y^p) = 0\}$ is non-reduced in general as:

$$f_0(x_0^p, y_0^p) = (g_0(x, y))^p$$

for some polynomial $g_0 \in k[x, y]$, in characteristic $p > 0$. We repeat this factorisation process until $g_0 \notin k[x, y]^p$ so that $\mathscr{Y}_0 = \{g_0 = 0\}$ is the reduced preimage. Pick some arbitrary smooth lifting $\mathscr{Y}_1 = \{g_1 = 0\}$ where $g_1 \in R_1[x, y]$. Then, as $R_1[x, y]$ is a flat R_1-module, we have that:

$$u_1^*(f_1) - g_1^p = f_1(x^p, y^p) - g_1^p = p \cdot \beta_1(x, y)$$

for some polynomial $\beta_1 \in R_1[x, y]$. Note that, the polynomial $p \cdot \beta_1 \in pR_1[x, y] \cong k[x, y]$ is independent of the lifting g_1. Overall, one can check that Raynaud's lifting construction defines a unique morphism of k-schemes:

$$\begin{aligned} v_0' : \mathscr{Y}_0 &\longrightarrow \mathbb{V}_0 \cong \mathscr{X}_0 \times \mathbb{A}^1_k; \\ (c_0, d_0) &\longmapsto ((c_0^p, d_0^p), \beta_0(c_0, d_0)) \end{aligned}$$

that, on points, is given by the composition:

$$\mathscr{Y}_0(k) \longrightarrow (\mathscr{A}_1, \mathscr{X}_0)(R_1) \xrightarrow{\tau} \mathbb{V}_0(k).$$

Indeed, as $\mathscr{Y}_1$ is smooth, there exists $(c_1, d_1) \in \mathscr{Y}_1(R_1)$ lifting $(c_0, d_0) \in \mathscr{Y}_0(k)$. Then the above composition is given by:

$$(c_0, d_0) \longmapsto (c_1^p, d_1^p) \longmapsto ((c_0^p, d_0^p), e_0)$$

where $f_1(c_1^p, d_1^p) = pe_1$ for some unique element $pe_1 \in p \cdot R_1$. By construction, we have that:

$$f_1(c_1^p, d_1^p) = f_1(c_1^p, d_1^p) - g_1(c_1, d_1)^p = p \cdot h_1(c_1, d_1);$$

so these maps coincide.

4.1.3 Proof of Theorem II

Let us return to the situation where R is an absolutely unramified ($e = 1$) complete discrete valuation ring with fraction field K of characteristic 0 and algebraically closed residue field k of characteristic $p > 0$. Suppose that $i : \mathscr{X} \hookrightarrow \mathscr{A}$ is the closed immersion of a flat R-curve in an abelian R-scheme such that the fibres of $\mathscr{X}$ are integral curves of geometric genus ≥ 2. We need to show that the image of:

$$\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}_0(k)$$

is finite under specialisation. Reprising the notation of the previous subsections, it is enough to show that:

Proposition 4.1.14. *The image of:*

$$\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k)$$

is finite under reduction mod p.

Remark 4.1.15. Using [Mess06, 7, Ch. III], as we assume the absolute ramification index is 1, the kernel of specialisation map $\mathscr{A}(R) \to \mathscr{A}_1(R_1)$ is contained in $p\mathscr{A}(R)$ and so it is in fact equivalent to working modulo p^2.

The closed immersion $i_1 : \mathscr{X}_1 \hookrightarrow \mathscr{A}_1$ corresponds to a section of the affine bundle $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ and a non-canonical isomorphism $\mathbb{V}_0 \cong \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$. Write $\mathscr{X}_0' \subseteq \mathbb{V}_0$ for the isomorphic copy of $\mathscr{X}_0$ corresponding to the zero section of the normal bundle. Recall that we have a factorisation:

$$\begin{array}{ccc} (\mathscr{A}_1, \mathscr{X}_0)(R_1) & \xrightarrow{\tau} & \mathbb{V}_0(k) \\ & \searrow & \downarrow{\scriptstyle h_0} \\ & & \mathscr{X}_0(k) \end{array} .$$

Note that $\tau(\mathscr{X}_1(R_1)) \subseteq \mathscr{X}_0'(k)$ by construction. On the other hand, by the results of the previous section, if we let $[p]_{\mathscr{A}_1} : \mathscr{A}_1 \to \mathscr{A}_1$ denote the multiplication-by-p map on $\mathscr{A}_1$, and set $j_0 : \mathscr{Y}_0 \hookrightarrow \mathscr{A}_0$ to be the reduced preimage of $\mathscr{X}_0$ under $[p]_{\mathscr{A}_0}$, then we obtain a lifting:

$$\begin{array}{ccc} & & \mathbb{V}_0 \\ & \overset{v_0'}{\nearrow} & \downarrow{\scriptstyle h_0} \\ \mathscr{Y}_0 & \xrightarrow[v_0]{} & \mathscr{X}_0 \end{array}$$

where $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ is the restriction of the multiplication-by-p map to $\mathscr{Y}_0$. Write $\mathscr{Y}_0' \subseteq \mathbb{V}_0$ for the scheme theoretic image of v_0'. Then we see that $\tau(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1)) = \mathscr{X}_0'(k) \cap$

$\mathscr{Y}_0'(k)$ and so, identifying $\mathscr{X}_0'$ with $\mathscr{X}_0$ under h_0, we obtain the following Corollary of Proposition 4.1.14:

Corollary 4.1.16. *Suppose that $\mathscr{A}_0$ is an abelian surface. Then the cardinality of the image of:*

$$\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k)$$

is finite under reduction mod p, and is bounded by:

$$|\mathscr{X}_0'(k) \cap \mathscr{Y}_0'(k)| \leq (\mathscr{X}_0 \cdot \mathscr{X}_0) \deg(h_0')$$

where $h_0' : \mathscr{Y}_0' \to \mathscr{X}_0$ is the restriction of h_0 to $\mathscr{Y}_0'$, and $\mathscr{X}_0 \cdot \mathscr{X}_0$ is the self intersection of $\mathscr{X}_0$ in $\mathscr{A}_0$.

Remark 4.1.17. In fact, if the desired image is finite, then the intersection $\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1)$ is finite. This follows as the kernel of the specialisation map $p\mathscr{A}_1(R_1) \to \mathscr{A}_0(k)$ is finite (cf. the 'lifting' homomorphism of Prop. 3.6.5).

More generally, let $\widetilde{\mathscr{Y}_0'} \to \mathscr{Y}_0'$ denote the normalisation of $\mathscr{Y}_0' \subseteq \mathbb{V}_0$, and $\tilde{h_0'} : \widetilde{\mathscr{Y}_0'} \to \mathscr{Y}_0' \xrightarrow{h_0'} \mathscr{X}_0$. By associating $\mathbb{V}_0 \cong \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$, the inclusion $\mathscr{Y}_0' \hookrightarrow \mathbb{V}_0$ corresponds to a morphism of $\mathscr{O}_{\mathscr{Y}_0'}$-modules $(h_0')^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \mathscr{O}_{\mathscr{Y}_0'}$ that is zero precisely over the intersection $\mathscr{X}_0' \cap \mathscr{Y}_0'$. Let $\mathscr{M}_0$ denote the quotient of the pullback sheaf $(\tilde{h_0'})^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$ by its torsion subsheaf. Then we obtain a non-zero morphism of locally free sheaves on $\widetilde{\mathscr{Y}_0'}$:

$$\epsilon : \mathscr{M}_0 \longrightarrow \mathscr{O}_{\widetilde{\mathscr{Y}_0'}}.$$

Dually, we have an injective morphism of locally free sheaves $\epsilon^\vee : \mathscr{O}_{\widetilde{\mathscr{Y}_0'}} \to \mathscr{M}_0^\vee$ with image $\mathscr{O}_{\widetilde{\mathscr{Y}_0'}}(D)$ corresponding to some divisor D on $\widetilde{\mathscr{Y}_0'}$ of positive degree, supported on the preimage of $\mathscr{X}_0'(k) \cap \mathscr{Y}_0'(k)$ in $\widetilde{\mathscr{Y}_0'}$.

Remark 4.1.18. Overall, we obtain a bound:

$$|\mathrm{Im}(\mathscr{X}_1(R_1) \cap \mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k))| \leq \mu_0$$

where:

$$\mu_0 = \sup_{\mathscr{L} \subseteq \mathscr{M}_0^\vee} \deg(\mathscr{L})$$

and we take the maximum degree of invertible sheaves $\mathscr{L} \subseteq \mathscr{M}_0^\vee$. This coincides with the intersection number $\mathscr{X}_0' \cdot \mathscr{Y}_0' = \deg(\mathscr{M}_0^\vee)$ when $\mathscr{A}_0$ is an abelian surface.

Finiteness in the smooth ordinary case

We first show the desired finiteness result in the idealised situation when $\mathscr{X}$ is a smooth R-curve and $\mathscr{A}$ has good ordinary reduction using the subsequent paper of Raynaud [Ray83-

2]. Recall that the connected-étale sequence of $\mathscr{A}[p]$ is given by:

$$0 \longrightarrow \mathscr{A}[p]^\circ \longrightarrow \mathscr{A}[p] \longrightarrow \mathscr{A}[p]_{\text{ét}} \longrightarrow 0$$

where $\text{rank}(\mathscr{A}[p]^\circ) = \text{rank}(\mathscr{A}[p]_{\text{ét}}) = p^g$ and $g = \dim(\mathscr{A}_0)$. Let $\mathscr{B} = \mathscr{A}/\mathscr{A}[p]^\circ$ and denote by:

$$[p]_{\mathscr{A}} : \mathscr{A} \xrightarrow{\alpha} \mathscr{B} \xrightarrow{\beta} \mathscr{A}$$

the factorisation of the multiplication-by-p map where α is the quotient morphism and β is the dual isogeny. Note that β is étale by construction. Denote by $\mathscr{Z} = \beta^{-1}(\mathscr{X}) \subseteq \mathscr{B}$ the smooth R-curve which is an étale cover of $\mathscr{X}$ under β. Reducing modulo p^2 we obtain the factorisation:

$$[p]_{\mathscr{A}_1} : \mathscr{A}_1 \xrightarrow{\alpha_1} \mathscr{B}_1 \xrightarrow{\beta_1} \mathscr{A}_1$$

and specialising to k we obtain the factorisation:

$$[p]_{\mathscr{A}_0} : \mathscr{A}_0 \xrightarrow{\alpha_0} \mathscr{B}_0 \xrightarrow{\beta_0} \mathscr{A}_0.$$

As we have constrained that $\mathscr{A}_0$ is an ordinary k-abelian variety, we see that $\mathscr{B}_0 \cong \mathscr{A}_0^{(p)}$ and α_0 corresponds to the relative Frobenius under this isomorphism. As before, let $\mathscr{Y}_0$ denote the reduced preimage of $\mathscr{X}_0$ under $[p]_{\mathscr{A}_0}$ (or equivalently, the reduced preimage of $\mathscr{Z}_0$ under α_0). Let $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ denote the restriction of $[p]_{\mathscr{A}_0}$ to $\mathscr{Y}_0$, and let $w_0 : \mathscr{Y}_0 \to \mathscr{Z}_0$ denote the restriction of α_0 to $\mathscr{Y}_0$. By construction, we may associate $\mathscr{Z}_0 \cong \mathscr{Y}_0^{(p)}$ and w_0 with the relative Frobenius on $\mathscr{Y}_0$. Let $(\mathscr{B}_1, \mathscr{Z}_0)(R_1)$ denote the set of points of $\mathscr{B}(R_1)$ that specialise to $\mathscr{Z}_0(k)$, and consider the set of points $\alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1)) \cap \mathscr{Z}_1(R_1) \subseteq (\mathscr{B}_1, \mathscr{Z}_0)(R_1)$. Then we have:

$$\beta_1(\alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1))) = p(\mathscr{A}_1, \mathscr{Y}_0)(R_1) \cap \mathscr{X}_1(R_1) = p\mathscr{A}_1(R_1) \cap \mathscr{X}_1(R_1).$$

Thus, to prove Proposition 4.1.14, it suffices to show the following:

Proposition 4.1.19. *The image of:*

$$\alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1)) \cap \mathscr{Z}_1(R_1) \longrightarrow \mathscr{Z}_0(k)$$

under reduction mod p is finite.

Replacing $\mathscr{Z}_1$ by any irreducible component, we may assume that $\mathscr{Z}_1$ and $\mathscr{Y}_0$ are irreducible. We proceed by contradiction. Suppose that this image is infinite and choose an abstract smooth lifting $\mathscr{Y}_1 \to \text{Spec}(R_1)$ of $\mathscr{Y}_0$. We will use this infinite set of points to lift the relative Frobenius $w_0 : \mathscr{Y}_0 \to \mathscr{Z}_0$ to a morphism of R_1-curves $w_1 : \mathscr{Y}_1 \to \mathscr{Z}_1$. As $\mathscr{Z}_0 \to \mathscr{X}_0$ is an étale cover of a non-singular curve of genus $g \geq 2$ we obtain the desired contradiction by Corollary 3.4.10.

Lemma 4.1.20. *Suppose that Prop. 4.1.19 is false. Then, there exists a morphism of R_1-curves $w_1 : \mathscr{Y}_1 \to \mathscr{Z}_1$ lifting the relative Frobenius $w_0 : \mathscr{Y}_0 \to \mathscr{Z}_0$.*

Proof. Let $\mathscr{U}_1 \subseteq \mathscr{Y}_1$ denote an affine open. By the infinitesimal lifting property on $\mathscr{A}_1$, there exists a local lifting $f_1 : \mathscr{U}_1 \to \mathscr{A}_1$ of the composition $\mathscr{U}_0 \hookrightarrow \mathscr{Y}_0 \hookrightarrow \mathscr{A}_0$. Such a local lifting is not unique, and may be modified by a derivation (cf. Remark 4.1.12). However, as α_0 is the relative Frobenius, it has zero differential and so these local liftings may be composed with $\alpha_1 : \mathscr{A}_1 \to \mathscr{B}_1$ to give a well defined R_1-morphism $g_1 : \mathscr{Y}_1 \to \mathscr{B}_1$:

$$\begin{array}{ccccc} & & \overset{\exists g_1}{\curvearrowright} & & \\ \mathscr{Y}_1 & & \mathscr{A}_1 & \xrightarrow[\alpha_1]{} & \mathscr{B}_1 \\ \uparrow & & \uparrow & & \uparrow \\ \mathscr{Y}_0 & \hookrightarrow & \mathscr{A}_0 & \xrightarrow[\alpha_0]{} & \mathscr{B}_0 \end{array}$$

that lifts the composition $\mathscr{Y}_0 \hookrightarrow \mathscr{A}_0 \xrightarrow{\alpha_0} \mathscr{B}_0$. By construction, g_1 locally factors through $\mathscr{A}_1$ so we have that:

$$g_1(\mathscr{Y}_1(R_1)) \subseteq \alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1)).$$

On the other hand, if $\sigma_1 \in (\mathscr{A}_1, \mathscr{U}_0)(R_1)$ for some affine open $\mathscr{U}_1 \subseteq \mathscr{Y}_1$, then we can modify the local lifting $f_1 : \mathscr{U}_1 \to \mathscr{A}_1$ by a translation of $\mathscr{A}_1$ so that $\sigma_1 \in f_1(\mathscr{U}_1(R_1))$; thus $\alpha_1(\sigma_1) \in g_1(\mathscr{Y}_1(R_1))$ and we have that:

$$g_1(\mathscr{Y}_1(R_1)) = \alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1)).$$

Let $\mathscr{Y}_1' = \mathscr{Z}_1 \times_{\mathscr{B}_1} \mathscr{Y}_1$ denote the pullback of $\mathscr{Z}_1 \hookrightarrow \mathscr{B}_1$ by $g_1 : \mathscr{Y}_1 \to \mathscr{B}_1$:

$$\begin{array}{ccc} \mathscr{Y}_1' & \xrightarrow{w_1} & \mathscr{Z}_1 \\ \downarrow & & \downarrow \\ \mathscr{Y}_1 & \xrightarrow[g_1]{} & \mathscr{B}_1 \end{array}.$$

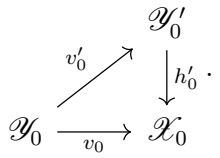
Then $\mathscr{Y}_1' \subseteq \mathscr{Y}_1$ is a closed subscheme. We assume for contradiction that the image of:

$$\alpha_1((\mathscr{A}_1, \mathscr{Y}_0)(R_1)) \cap \mathscr{Z}_1(R_1) = g_1(\mathscr{Y}_1(R_1)) \cap \mathscr{Z}_1(R_1)$$

is infinite in $\mathscr{Z}_0(k)$. Therefore, $\mathscr{Y}_1'(R_1)$ has infinite image in $\mathscr{Y}_0(k)$. As $\mathscr{Y}_0$ is an irreducible curve, the image is dense, and thus the set $\mathscr{Y}_1'(R_1)$ is dense in $\mathscr{Y}_1$. Thus $\mathscr{Y}_1' = \mathscr{Y}_1$ and the morphism $w_1 : \mathscr{Y}_1' = \mathscr{Y}_1 \to \mathscr{Z}_1$ provides a lift of Frobenius. □

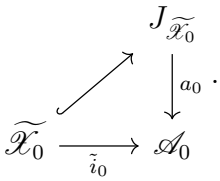
Finiteness in general

We now provide the proof of Prop. 4.1.14 in the general case. Recall that we have a commutative diagram:



To prove the proposition, it is sufficient to show that the curves $\mathscr{X}_0', \mathscr{Y}_0' \subseteq \mathbb{V}_0$ are distinct integral curves. We show that $\mathscr{Y}_0$ is integral using characteristic $p > 0$ geometry. To show the curves are distinct, we prove that the morphism $v_0' : \mathscr{Y}_0 \to \mathscr{Y}_0'$ is generically étale. Then, as v_0 is inseparable, the cover $h_0' : \mathscr{Y}_0' \to \mathscr{X}_0$ must also be inseparable, and so the curves $\mathscr{X}_0', \mathscr{Y}_0'$ are distinct (as the morphism $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ restricts to an isomorphism $\mathscr{X}_0' \xrightarrow{\sim} \mathscr{X}_0$).

Let $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ denote the closed immersion of the integral curve $\mathscr{X}_0$ into the k-abelian variety $\mathscr{A}_0$. Let $\alpha_0 : \widetilde{\mathscr{X}_0} \to \mathscr{X}_0$ denote the normalisation and write $\tilde{i}_0 : \widetilde{\mathscr{X}_0} \xrightarrow{\alpha_0} \mathscr{X}_0 \xrightarrow{i_0} \mathscr{A}_0$. Given an embedding of $\widetilde{\mathscr{X}_0}$ into its Jacobian $\widetilde{\mathscr{X}_0} \hookrightarrow J_{\widetilde{\mathscr{X}_0}}$, there is an *Albanese morphism* $a_0 : J_{\widetilde{\mathscr{X}_0}} \to \mathscr{A}_0$ fitting into the commutative diagram:



(cf. Ex. 3.2.5 (iii)). We make the following assumptions:

Assumption 4.1.21. *Let k be an algebraically closed field of characteristic $p > 0$. Let $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ be the closed immersion of a curve in an abelian variety defined over k. Write $\alpha_0 : \widetilde{\mathscr{X}_0} \to \mathscr{X}_0$ for the normalisation and N for the kernel of the Albanese morphism $a_0 : J_{\widetilde{\mathscr{X}_0}} \to \mathscr{A}_0$. We assume that:*

i) a_0 is surjective;

ii) N is smooth over k;

iii) The order of the group of connected components N/N° is coprime to p (where N° is the connected component of the identity of N).

Note that, although the assumptions above seem rather technical, they are automatic in the case where $\mathscr{X}_0$ is smooth and $\mathscr{A}_0$ coincides with the Jacobian. Note that, when we specialise to the case of Bogomolov-Fu-Tschinkel where $\mathscr{A}_0$ is the product of two elliptic curves (i) follows immediately for dimension reasons, and we will see that taking $p > 2$ will be sufficient for (ii) and (iii) (cf. Remark 5.1.7).

Lemma 4.1.22. *Let $u_0 : \mathscr{B}_0 \to \mathscr{A}_0$ be an isogeny of k-abelian varieties such that $\mathscr{G}_0 = \ker(u_0)$ is of p-primary order. Let $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ denote the closed immersion of an integral curve of geometric genus ≥ 2 satisfying Assumption 4.1.21 above. Let $\mathscr{Y}_0$ denote the reduced preimage of $\mathscr{X}_0$ under u_0. Then $\mathscr{Y}_0$ is integral.*

Proof. Let $j_0 : \mathscr{Y}_0 \hookrightarrow \mathscr{B}_0$ denote the corresponding closed immersion and let $\beta_0 : \widetilde{\mathscr{Y}_0} \to \mathscr{Y}_0$ be the normalisation of $\mathscr{Y}_0$. As $\mathscr{Y}_0$ is reduced, it is enough show irreducibility, or equivalently that $\widetilde{\mathscr{Y}_0}$ is connected. Consider the diagram:

$$\begin{array}{ccc} \mathscr{B}_0 \times_{\mathscr{A}_0} \widetilde{\mathscr{X}_0} & \longrightarrow & \widetilde{\mathscr{X}_0} \\ \downarrow & & \downarrow \\ \mathscr{B}_0 \times_{\mathscr{A}_0} J_{\widetilde{\mathscr{X}_0}} & \longrightarrow & J_{\widetilde{\mathscr{X}_0}} \\ \downarrow & & \downarrow{\scriptstyle a_0} \\ \mathscr{B}_0 & \xrightarrow[u_0]{} & \mathscr{A}_0 \end{array}.$$

Conditions (i) and (iii) imply that the fibre product is connected, thus $\mathscr{B}_0 \times_{\mathscr{A}_0} J_{\widetilde{\mathscr{X}_0}}$ is an abelian variety (as properness and smoothness are preserved under base change). Thus, to show that $\widetilde{\mathscr{Y}_0}$ is connected, we may assume that $\mathscr{X}_0 = \widetilde{\mathscr{X}_0}$ and $\mathscr{A}_0 = J_{\widetilde{\mathscr{X}_0}}$, and show that the fibre product $\mathscr{B}_0 \times_{\mathscr{A}_0} \widetilde{\mathscr{X}_0}$ is irreducible. By dividing out by the connected component of $\ker(u_0)$, we may assume that u_0 is a separable isogeny (as the reduced preimage of an integral subvariety under a purely inseparable cover will still be irreducible). Then, we conclude by noting that abelian étale covers (and in particular, separable isogenies) of the Jacobian $J_{\widetilde{\mathscr{X}_0}}$ are in direct correspondence with connected étale covers of $\widetilde{\mathscr{X}_0}$ via the fibre product [Mil86, Prop. 9.1]. □

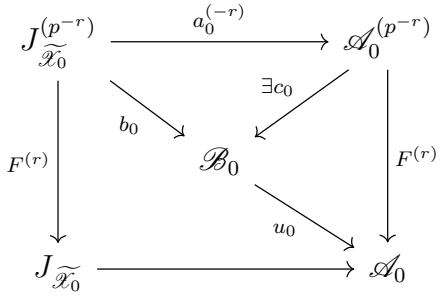
Lemma 4.1.23. *Suppose that $u_0 : \mathscr{B}_0 \to \mathscr{A}_0$ is a purely inseparable isogeny. Then $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ has degree p^r for some $r > 0$. Suppose that Assumption 4.1.21 holds. Then there exists a factorisation of the iterated relative Frobenius:*

$$F^{(r)} : \mathscr{A}_0^{(p^{-r})} \longrightarrow \mathscr{B}_0 \xrightarrow{u_0} \mathscr{A}_0.$$

Proof. Firstly, we note that the morphism $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ is purely inseparable, so that the induced map $\tilde{v}_0 : \widetilde{\mathscr{Y}_0} \to \widetilde{\mathscr{X}_0}$ coincides with the iteration of the relative Frobenius of the same degree (cf. Prop. 3.4.4) and so we may associate $\widetilde{\mathscr{Y}_0} \cong \widetilde{\mathscr{X}_0}^{(p^{-r})}$ and $\tilde{v}_0 = F^{(p^r)}$. We summarise this in the following diagram:

$$\begin{array}{ccc} \widetilde{\mathscr{X}_0}^{(p^{-r})} & \longrightarrow & \mathscr{Y}_0 \\ {\scriptstyle F^{(r)}}\downarrow & & \downarrow{\scriptstyle v_0} \\ \widetilde{\mathscr{X}_0} & \longrightarrow & \mathscr{X}_0 \end{array}$$

where the horizontal arrows are normalisations. Note additionally that $J_{\widetilde{\mathscr{X}_0^{(p^{-r})}}} \cong J^{(p^{-r})}_{\widetilde{\mathscr{X}_0}}$. We then obtain the following diagram:



where b_0 is the Albanese morphism associated to $\tilde{j}_0 : \widetilde{\mathscr{X}_0^{(p^{-r})}} = \widetilde{\mathscr{Y}_0} \to \mathscr{B}_0$. By assumption, $\ker(a_0^{(-r)}) = N^{(-r)}$ is smooth, so that its image $b_0(N^{(-r)}) \subseteq \ker(u)$ is smooth also. However, as u_0 is purely inseparable, or equivalently as $\ker(u_0)$ is connected, this image is zero and so there exists a homomorphism of abelian varieties $c : \mathscr{A}_0^{(p^{-r})} \to \mathscr{B}_0$ allowing the diagram to commute; providing the desired factorisation. □

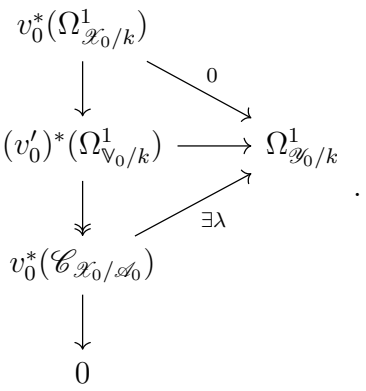
Suppose now we take u_0 to be the multiplication-by-p map $[p]_{\mathscr{A}_0} : \mathscr{A}_0 \to \mathscr{A}_0$. We show that $v_0' : \mathscr{Y}_0 \to \mathscr{Y}_0'$ is generically étale.

Proposition 4.1.24. *Let $[p]_{\mathscr{A}_0} : \mathscr{A}_0 \to \mathscr{A}_0$ denote the multiplication-by-p map on $\mathscr{A}_0$. Let $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ be an integral curve of geometric genus ≥ 2, and $\mathscr{Y}_0$ the reduced preimage of $\mathscr{X}_0$ under $[p]_{\mathscr{A}_0}$. Then the morphism $v_0' : \mathscr{Y}_0 \to \mathscr{Y}_0'$ defined in Proposition 4.1.10 is generically étale.*

Consider the differential $(v_0')^*(\Omega^1_{\mathscr{Y}_0'/k}) \to \Omega^1_{\mathscr{Y}_0/k}$. We will show that this morphism vanishes on a finite set. By the construction of $\mathbb{V}_0$, we have an isomorphism $\mathbb{V}_0 \cong \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \xrightarrow{h_0} \mathscr{X}_0$. By the definition of the conormal sheaf, we have the exact sequence:

$$h_0^*(\Omega^1_{\mathscr{X}_0/k}) \longrightarrow \Omega^1_{\mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})/k} \longrightarrow h_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \longrightarrow 0$$

Considering the factorisation $v_0 = h_0' \circ v_0'$. Pulling back along v_0', we obtain the diagram:



As the differential of v_0' is 0, we obtain a morphism of sheaves $\lambda : v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \Omega^1_{\mathscr{Y}_0/k}$. It is sufficient to show that λ is zero at only finitely many points of $\mathscr{Y}_0$. We now compute λ in terms of local sections. Reprising the notation of Prop. 4.1.10, let $\mathscr{I}_0$ be the ideal sheaf of $\mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ and a_0 a local section. Denote by $\mathscr{I}_1'$ the ideal sheaf of $\mathscr{X}_0 \hookrightarrow \mathscr{A}_1$ and choose a local lift a_1 of a_0. Write $\bar{a}_0$ for the image of a_0 in $\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}$. By construction, the morphism $v_0' : \mathscr{Y}_0' \to \mathbb{V}_0 \cong \mathbb{V}(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0})$ is induced by the morphism of sheaves:

$$\begin{aligned} v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) &\longrightarrow \mathscr{O}_{\mathscr{Y}_0}; \\ v_0^*(\bar{a}_0) &\longmapsto \delta|_{\mathscr{Y}_0}(a_1). \end{aligned}$$

Then we have that $\lambda(v_0^*(\bar{a}_0)) = d\delta|_{\mathscr{Y}_0}(a_1)$ where $\delta : \mathscr{O}_{\mathscr{A}_1} \to \mathscr{O}_{\mathscr{A}_0}$ is the p-derivation constructed in the proof. On the other hand, the morphism $[p]_{\mathscr{A}_0} : \mathscr{A}_0 \to \mathscr{A}_0$ has zero differential, so the image of $[p]^*_{\mathscr{A}_1}\Omega_{\mathscr{A}_1/R_1} \to \Omega_{\mathscr{A}_1/R_1}$ lies in $p\Omega_{\mathscr{A}_1/R_1} \cong \Omega_{\mathscr{A}_0/k}$. Specifically, for the local section $a_1 \in \mathscr{I}_1' \subseteq \mathscr{O}_{\mathscr{A}_1}$ we have $u_1^*(a_1) = \alpha_1^p + p\delta(a_1)$ for some local section $\alpha_1 \in \mathscr{O}_{\mathscr{A}_1}$, and so:

$$du_1^*(a_1) = u_1^*(da_1) = p(d\alpha_1^{p-1} + d\delta(a_1)).$$

Writing $\mathscr{J}_0$ for the ideal sheaf of $\mathscr{Y}_0$ in $\mathscr{A}_0$, we have that $\alpha_0 \in \mathscr{J}_0$, and so $p(d\alpha_1^{p-1}) = 0$. Overall, we have proved the following:

Lemma 4.1.25. *Under the isomorphism $p\Omega_{\mathscr{A}_1/R_1} \cong \Omega_{\mathscr{A}_0/k}$ one may associate:*

$$\begin{aligned} p\Omega_{\mathscr{A}_1/R_1} &\longrightarrow \Omega_{\mathscr{A}_0/k}; \\ [p]^*_{\mathscr{A}_1}(da_1) &\longmapsto \lambda(v_0^*(\bar{a}_0)) \end{aligned}$$

for a local section $a_1 \in \mathscr{I}_1'$.

Gauss maps

We show that $\frac{d[p]_{\mathscr{A}_1}}{p}$ is generically non-zero by studying the *Gauss map*. Suppose first that $\mathscr{X}_0/k$ is smooth of genus $g \geq 2$. Note that $\Omega^1_{\mathscr{A}_0/k} \cong \mathscr{O}_A^{\oplus d}$ is trivial, where $d = \dim(\mathscr{A}_0)$, and so we can define an associated projective space $\mathbb{P}_{\mathscr{A}_0} := \mathbb{P}(\Omega^1_{\mathscr{A}_0/k})$. After a choice of basis $\omega_1, ..., \omega_d \in H^0(\mathscr{A}_0, \Omega^1_{\mathscr{A}_0/k})$, we obtain an isomorphism $\mathbb{P}_{\mathscr{A}_0} \cong \mathbb{P}^{d-1}_k \times \mathscr{A}_0$. The closed immersion i_0 has an associated conormal exact sequence:

$$\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0} \longrightarrow i_0^*\Omega^1_{\mathscr{A}_0/k} \longrightarrow \Omega^1_{\mathscr{X}_0/k} \longrightarrow 0.$$

The morphism of sheaves $i_0^*\Omega^1_{\mathscr{A}_0/k} \to \Omega^1_{\mathscr{X}_0/k}$ induces the corresponding *Gauss map*:

$$\gamma_{\mathscr{X}_0} : \mathscr{X}_0 \cong \mathbb{P}(\Omega^1_{\mathscr{X}_0/k}) \longrightarrow \mathbb{P}_{\mathscr{A}_0}.$$

Informally, given a closed point $x \in \mathscr{X}_0$, we obtain an associated tangent vector in $\Theta_{\mathscr{A}_0/k,x}$, unique up to scaling. Translating this direction to the identity $e \in \mathscr{A}_0$ we obtain a 1-dimensional subspace of $\Theta_{\mathscr{A}_0/k,e}$ corresponding to a well-defined point of $\mathbb{P}_{\mathscr{A}_0}$. More generally, if $\mathscr{X}_0$ is singular, then on the smooth locus $\mathscr{X}_0^{\mathrm{sm}} \subseteq \mathscr{X}_0$, we still obtain a morphism $\mathscr{X}_0^{\mathrm{sm}} \to \mathbb{P}_{\mathscr{A}_0}$. Let $\alpha : \widetilde{\mathscr{X}_0} \to \mathscr{X}_0$ be the normalisation of $\mathscr{X}_0$. Then as $\widetilde{\mathscr{X}_0}$ is non-singular, this morphism extends uniquely:

$$\begin{array}{ccc} \widetilde{\mathscr{X}_0} & & \\ \downarrow{\scriptstyle \alpha} & \searrow^{\gamma_{\widetilde{\mathscr{X}_0}}} & \\ \mathscr{X}_0 & \dashrightarrow & \mathbb{P}_{\mathscr{A}_0} \end{array}$$

to the *Gauss map* of $\widetilde{\mathscr{X}_0}$. Rephrasing this in terms of sheaves, we can pullback the conormal sequence of $\mathscr{X}_0$ in $\mathscr{A}_0$ by the normalisation α_0 to obtain:

$$\alpha_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \longrightarrow (\tilde{i}_0)^*\Omega^1_{\mathscr{A}_0/k} \longrightarrow \alpha_0^*\Omega^1_{\mathscr{X}_0/k} \longrightarrow 0.$$

Let $\widetilde{\Omega}_{\mathscr{X}_0}$ denote the quotient of $\alpha_0^*\Omega^1_{\mathscr{X}_0/k}$ by its torsion subsheaf, and let $\widetilde{\mathscr{C}}_{\mathscr{X}_0/\mathscr{A}_0}$ denote the cokernel of the natural morphism $(\tilde{i}_0)^*\Omega^1_{\mathscr{A}_0/k} \to \widetilde{\Omega}_{\mathscr{X}_0}$. Then we obtain an exact sequence:

$$0 \longrightarrow \widetilde{\mathscr{C}}_{\mathscr{X}_0/\mathscr{A}_0} \longrightarrow (\tilde{i}_0)^*\Omega^1_{\mathscr{A}_0/k} \longrightarrow \widetilde{\Omega}_{\mathscr{X}_0} \longrightarrow 0$$

and, associated to the morphism $(\tilde{i}_0)^*\Omega^1_{\mathscr{A}_0/k} \to \widetilde{\Omega}_{\mathscr{X}_0}$, we have the Gauss map of $\mathscr{X}_0$:

$$\gamma_{\widetilde{\mathscr{X}_0}} : \widetilde{\mathscr{X}_0} \cong \mathbb{P}(\widetilde{\Omega}_{\mathscr{X}_0}) \longrightarrow \mathbb{P}((\tilde{i}_0)^*\Omega^1_{\mathscr{A}_0/k}) \cong \mathbb{P}_{\mathscr{A}_0}.$$

Reprising the notation $j_0 : \mathscr{Y}_0 \hookrightarrow \mathscr{A}_0$ for the inclusion of the reduced preimage of $\mathscr{X}_0$ under $[p]_{\mathscr{A}_0}$ and letting $\beta_0 : \widetilde{\mathscr{Y}_0} \to \mathscr{Y}_0$ denote normalisation, we obtain the analogous exact sequences:

$$\mathscr{C}_{\mathscr{Y}_0/\mathscr{A}_0} \longrightarrow j_0^*\Omega^1_{\mathscr{A}_0/k} \longrightarrow \Omega^1_{\mathscr{Y}_0/k} \longrightarrow 0$$

and:

$$0 \longrightarrow \widetilde{\mathscr{C}}_{\mathscr{Y}_0/\mathscr{A}_0} \longrightarrow (\tilde{j}_0)^*\Omega^1_{\mathscr{Y}_0/k} \longrightarrow \widetilde{\Omega}_{\mathscr{Y}_0} \longrightarrow 0$$

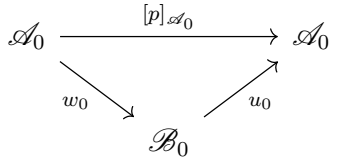
and an associated Gauss map $\gamma_{\widetilde{\mathscr{Y}_0}} : \widetilde{\mathscr{Y}_0} \longrightarrow \mathbb{P}_{\mathscr{A}_0}$.

Lemma 4.1.26. *Suppose that the inclusion $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ satisfies Assumption 4.1.21 and that $\mathscr{X}_0$ is of geometric genus $g \geq 2$. Then:*

$$\deg(\gamma_{\widetilde{\mathscr{Y}_0}}) < \deg(\gamma_{\widetilde{\mathscr{X}_0}} \circ \tilde{v}_0).$$

Proof. Let $\mathscr{G}_0 = \ker([p]_{\mathscr{A}_0})$ and $\mathscr{G}_0^{\text{ét}}$ be the étale part. Setting $\mathscr{B}_0 = \mathscr{A}_0/\mathscr{G}_0^{\text{ét}}$, we obtain a

factorisation:



where u_0 is purely inseparable and w_0 is the étale quotient. Clearly, it is sufficient to prove the analogous statement with u_0 in place of $[p]_{\mathscr{A}_0}$. By Lemma 4.1.23, there is a factorisation:

$$F^{(r)} : \mathscr{A}_0^{(p^{-r})} \longrightarrow \mathscr{B}_0 \xrightarrow{u_0} \mathscr{A}_0$$

where p^r is the degree of $\mathscr{Y}_0 \to \mathscr{X}_0$. As in the proof of the Lemma, we may associate $\widetilde{\mathscr{X}_0^{(p^{-r})}} = \widetilde{\mathscr{Y}_0}$. We then obtain inclusions:

$$\widetilde{\Omega}_{\mathscr{Y}_0} \hookrightarrow \widetilde{\Omega}_{\mathscr{X}_0^{(p^{-r})}} \hookrightarrow \Omega^1_{\widetilde{\mathscr{X}_0^{(p^{-r})}}}$$

and therefore:

$$\deg(\gamma_{\widetilde{\mathscr{Y}_0}}) \leq \deg(\gamma_{\widetilde{\mathscr{X}_0^{(p^{-r})}}}) \leq \deg(\gamma_{\widetilde{\mathscr{X}_0}}).$$

On the other hand:

$$\deg(\gamma_{\widetilde{\mathscr{X}_0}}) < p^r \deg(\gamma_{\widetilde{\mathscr{X}_0}}) = \deg(\gamma_{\widetilde{\mathscr{X}_0}} \circ \tilde{v}_0)$$

as $[p]_{\mathscr{A}_0}$ has zero differential which forces $r > 0$. □

Fixing a basis $\omega_1, ..., \omega_d \in H^0(\mathscr{A}_0, \Omega^1_{\mathscr{A}_0/k})$, we obtain a (non-canonical) isomorphism:

$$[p]^*_{\mathscr{A}_0}(\Omega^1_{\mathscr{A}_0/k}) \xrightarrow{\sim} \Omega^1_{\mathscr{A}_0/k}$$

by noting that the sections $[p]^*_{\mathscr{A}_0}(\omega_1), ..., [p]^*_{\mathscr{A}_0}(\omega_d)$ trivialise $[p]^*_{\mathscr{A}_0}(\Omega^1_{\mathscr{A}_0/k})$. Pulling back the conormal exact sequences of $\mathscr{X}_0$ and $\mathscr{Y}_0$, we obtain a commuting diagram:

$$\begin{array}{ccccccc} v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) & \longrightarrow & (j_0 \circ [p]_{\mathscr{A}_0})^*\Omega^1_{\mathscr{A}_0/k} & \longrightarrow & v_0^*\Omega^1_{\mathscr{X}_0/k} & \longrightarrow & 0 \\ & & \downarrow\sim & & & & \\ \mathscr{C}_{\mathscr{Y}_0/\mathscr{A}_0} & \longrightarrow & j_0^*\Omega^1_{\mathscr{A}_0/k} & \longrightarrow & \Omega^1_{\mathscr{Y}_0/k} & \longrightarrow & 0 \end{array} .$$

Let $\gamma : v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \Omega^1_{\mathscr{Y}_0/k}$ denote the composition from top left to bottom right in the above diagram.

Corollary 4.1.27. *Under the hypotheses of Lemma 4.1.26, the morphism of sheaves γ is generically non-zero.*

Proof. By pulling back along normalisations, we obtain the analogous diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \tilde{v}_0^*(\widetilde{\mathscr{C}}_{\mathscr{X}_0}) & \longrightarrow & ([p]_{\mathscr{A}_0} \circ \tilde{j}_0)^* \Omega^1_{\mathscr{A}_0/k} & \longrightarrow & \tilde{v}_0^* \widetilde{\Omega}^1_{\mathscr{X}_0} & \longrightarrow & 0 \\ & & & & \downarrow \sim & & & & \\ 0 & \longrightarrow & \widetilde{\mathscr{C}}_{\mathscr{Y}_0/\mathscr{A}_0} & \longrightarrow & \tilde{j}_0^* \Omega^1_{\mathscr{A}_0/k} & \longrightarrow & \widetilde{\Omega}^1_{\mathscr{Y}_0} & \longrightarrow & 0 \end{array} .$$

Let $\tilde{\gamma} : \tilde{v}_0^*(\widetilde{\mathscr{C}}_{\mathscr{X}_0}) \to \widetilde{\Omega}^1_{\mathscr{Y}_0}$ denote the analogous morphism of sheaves. Note that $\tilde{\gamma}$ is equal to γ over the smooth locus of $\mathscr{Y}_0$ so it is sufficient to prove the claim for $\widetilde{\mathscr{Y}_0}$. Suppose for contradiction that $\tilde{\gamma} = 0$. Then, the vertical isomorphism in the above diagram would induce an isomorphism on the quotient $\tilde{v}_0^* \widetilde{\Omega}^1_{\mathscr{X}_0} \xrightarrow{\sim} \widetilde{\Omega}^1_{\mathscr{Y}_0/k}$. On the other hand, by Lemma 4.1.26, we have that:

$$\deg(\widetilde{\Omega}^1_{\mathscr{Y}_0/k}) = \deg(\gamma_{\widetilde{\mathscr{Y}_0}}) < \deg(\gamma_{\widetilde{\mathscr{X}_0}} \circ \tilde{v}_0) = \deg(\tilde{v}_0^* \widetilde{\Omega}^1_{\mathscr{X}_0})$$

providing the desired contradiction. □

Finally, we describe $\gamma : v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \Omega^1_{\mathscr{Y}_0/k}$ locally, over the smooth locus of $\mathscr{X}_0$. Let $a_0 \in \mathscr{I}_0$ be a local section and $\bar{a}_0$ its image in $\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}$. We may write $da_0 = \sum_{i=1}^d f_i \omega_i$ for some local sections $f_i \in \mathscr{O}_{\mathscr{A}_0}$ with respect to the basis ω_i. We then have that:

$$\gamma(v^*(\bar{a}_0)) = \sum_{i=1}^d [p]^*_{\mathscr{A}_0}(f_i)\, \omega_i|_{\mathscr{Y}_0}.$$

We finish the proof of Proposition 4.1.24 by showing the following:

Lemma 4.1.28. *The maps $\gamma, \lambda : v_0^*(\mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0}) \to \Omega^1_{\mathscr{Y}_0/k}$ coincide.*

Proof. Lift the basis ω_i of $\Omega_{\mathscr{A}_0/k}$ to a basis ω_i' of $\Omega_{\mathscr{A}_1/R_1}$. Then, if $a_1 \in \mathscr{I}_1'$ is a local section with image $\bar{a}_0 \in \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_1}$ we can write $da_1 = \sum_{i=1}^d f_i' \omega_i'$ for some local sections $f_i' \in \mathscr{O}_{\mathscr{A}_1}$ and we have that:

$$\gamma(v^*(\bar{a}_0)) = \sum_{i=1}^d [p]^*_{\mathscr{A}_0}(f_i)\, \omega_i|_{\mathscr{Y}_0}$$

where $f_i \equiv f_i' \pmod p$. On the other hand, $[p]^*_{\mathscr{A}_1}(\omega_i') = p\omega_i'$, thus:

$$[p]^*_{\mathscr{A}_1}(da_1) = p \left(\sum_{i=1}^d [p]^*_{\mathscr{A}_1}(f_i')\, \omega_i' \right)$$

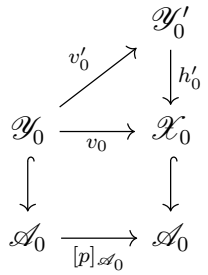
and by Lemma 4.1.25, we have that:

$$\lambda(v_0^*(\bar{a}_0)) = \sum_{i=1}^d [p]^*_{\mathscr{A}_0}(f_i)\, \omega_i|_{\mathscr{Y}_0}$$

thus the morphisms of sheaves coincide. □

4.1.4 Refinements on the bounds

We now discuss refinements on the bounds discussed in Remark 4.1.18 when $\mathscr{A}_0$ is an *abelian surface*. Recall that, from the previous subsections we have a diagram of the form:



where $h_0 : \mathbb{V}_0 \to \mathscr{X}_0$ is an affine morphism with distinct integral curves $\mathscr{X}_0', \mathscr{Y}_0' \subseteq \mathbb{V}_0$ such that $h_0|_{\mathscr{X}_0'} : \mathscr{X}_0' \to \mathscr{X}_0$ is an isomorphism. We wish to describe the bound:

$$|\mathscr{X}_0'(k) \cap \mathscr{Y}_0'(k)| \leq \mu_0 = \deg(h_0') \cdot (\mathscr{X}_0 \cdot \mathscr{X}_0).$$

Note that $\deg(v_0) = \deg(h_0') \cdot \deg(v_0')$ so as a first step we describe the degree of the restriction $[p]_{\mathscr{A}_0}|_{\mathscr{Y}_0}$. To do this, we recall that if $f_0 : C_0 \to D_0$ is a finite morphism of integral k-curves, then there is a factorisation:

$$\deg(f_0) = \text{insep.deg}(f_0) \cdot \text{sep.deg}(f_0)$$

(cf. Prop. 3.4.4) corresponding to the decomposition of the finite extension $k(C_0)/k(D_0)$ into a purely inseparable and separable field extension.

Proposition 4.1.29. *Let k be an algebraically closed field of characteristic $p > 0$ and $u_0 : \mathscr{B}_0 \to \mathscr{A}_0$ an isogeny of abelian varieties over k. Let $\mathscr{G}_0 = \ker(u_0)$ and write:*

$$\mathscr{G}_0 = \mathscr{G}_0^\circ \times_k \mathscr{G}_0^{\text{ét}}$$

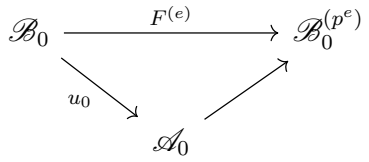
for the connected-étale decomposition. Suppose that $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{A}_0$ is the closed immersion of an integral curve satisfying Assumption 4.1.21 and $j_0 : \mathscr{Y}_0 \hookrightarrow \mathscr{B}_0$ is the reduced preimage of $\mathscr{X}_0$ under u_0. Then, writing $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ for the restriction of u_0 to $\mathscr{Y}_0$, we have that:

i) $\text{sep.deg}(v_0) = \text{rk}(\mathscr{G}_0^{\text{ét}})$*;*

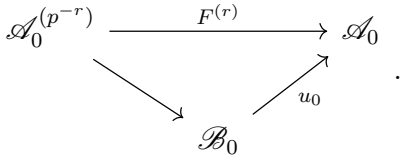
ii) $\text{insep.deg}(v_0) = p^e$ *where $e > 0$ is the smallest integer such that $F^{(e)}$ annihilates $\mathscr{G}_0^\circ$.*

Proof. To prove (i), we may divide $\mathscr{A}_0$ by $\mathscr{G}_0^\circ$ and assume that u_0 is a separable isogeny. Then $\mathscr{Y}_0$ is the preimage of $\mathscr{X}_0$ under u_0 and $\deg(v_0) = \deg(u_0)$. To prove (ii) we similarly

divide through by $\mathscr{G}_0^{\text{ét}}$ and assume that u_0 is purely inseparable. Write $p^r = \text{insep.deg}(v_0)$. We assume that $F^{(e)}(\mathscr{G}_0^\circ) = 0$ so that we have a factorisation:



hence $r \leq e$. To obtain the reverse inequality we use the factorisation of the geometric Frobenius from Lemma 4.1.23:



A fortiori, $F^{(r)}(\mathscr{G}_0^\circ) = 0$. □

The above information allows us to compute the degree of $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$. However, to optimise the bounds of Remark 4.1.18, we would like to describe the degree of $h_0' : \mathscr{Y}_0' \to \mathscr{X}_0$. Recall that, from Proposition 4.1.24, the morphism $v_0' : \mathscr{Y}_0 \to \mathscr{Y}_0'$ is generically étale i.e. separable and thus:

$$\text{insep.deg}(h_0') = \text{insep.deg}(\text{v}_0);$$

and so we need only describe the separable degree of h_0'.

Refining the bounds for canonical lifts

Suppose that $\mathscr{A}_0$ is ordinary. Recall that $\mathscr{A}_1$ is the *canonical lifting* of $\mathscr{A}_0$ (cf. 3.6.3) if the connected-étale sequence splits:

$$0 \longrightarrow \mathscr{G}_1^\circ \longrightarrow \mathscr{G}_1 \longrightarrow \mathscr{G}_1^{\text{ét}} \longrightarrow 0$$

as a short exact sequence of finite flat R_1-group schemes where $\mathscr{G}_1 = \mathscr{A}_1[p]$. More generally, suppose that there is some non-trivial finite étale subgroup scheme:

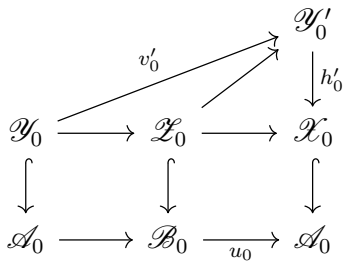
$$\mathscr{H}_1 \subseteq \mathscr{G}_1.$$

Then we can consider the factorisation:

$$[p]_{\mathscr{A}_1} : \mathscr{A}_1 \longrightarrow \mathscr{B}_1 \xrightarrow{u_1} \mathscr{A}_1$$

where $\mathscr{A}_1 \to \mathscr{A}_1/\mathscr{H}_1 = \mathscr{B}_1$ is the étale quotient and u_1 is the dual isogeny. Let $\mathscr{Z}_0 \hookrightarrow \mathscr{B}_0$ be the reduced preimage of $\mathscr{X}_0$ under u_0. Then, as the differential of u_0 is still zero, we

obtain the following diagram:



by applying the lifting property of $\mathbb{V}_0$ described in Proposition 4.1.10 and noting that it is natural. Applying Prop. 4.1.29 again, we obtain the bound:

$$\text{sep.deg}(h_0') \leq \text{sep.deg}(\mathscr{Z}_0 \to \mathscr{X}_0) = \text{rk}(\mathscr{G}_1^{\text{ét}}/\mathscr{H}_1).$$

4.1.5 Inertia actions and p-divisible groups

Let R, K, k be as in the previous subsections. Recall that we have a closed immersion $i : X \hookrightarrow A/K$ of a curve in an abelian variety and we wish to show that the intersection $X(\bar{K}) \cap A[\infty]$ is finite, and bounded by some tractable constant $c > 0$. So far, we have been able to provide a bound on the *coprime-to-p* torsion $A[\infty]^{(p')}$ of A lying on X:

$$|X(\bar{K}) \cap A[\infty]^{(p')}| \leq |\text{Im}(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \to \mathscr{X}_0(k))| \leq \mu_0.$$

We now show how this bound can be used to infer a bound on the number of torsion points of *any order* lying on X. First, we show that the above bound holds for all *translates* of X:

Proposition 4.1.30. *Let $a \in A(\bar{K})$ and $X + a \hookrightarrow A$ denote the $\bar{K}$-curve $t_a(X)$ where $t_a : A \to A$ denote translation by a. Then there exists a bound:*

$$|(X + a)(\bar{K}) \cap A[\infty]^{(p')}| \leq \mu_0$$

where μ_0 is independent of $a \in A(\bar{K})$.

Proof. Suppose first that $a \in A(\bar{K}) \setminus A(K)$. Let $H \leq A$ denote the subgroup scheme of translations which fix X. As X has geometric genus $g \geq 2$, $H \hookrightarrow \text{Aut}(X)$ is a finite group. Let $\mathscr{H} \subseteq \mathscr{A}$ denote the closure of H in $\mathscr{A}$ and let $\widetilde{\mathscr{X}} \to \mathscr{X}$ denote the normalisation. By assumption, $\widetilde{\mathscr{X}}$ is a smooth R-curve. There is an action of $\mathscr{H}$ on $\mathscr{X}$ which extends to $\widetilde{\mathscr{X}}$. Consider the special fibre $\mathscr{H}_0 \hookrightarrow \text{Aut}(\widetilde{\mathscr{X}_0})$. The Lie algebra of $\text{Aut}(\widetilde{\mathscr{X}_0})$ at the identity is given by $H^0(\widetilde{\mathscr{X}_0}, \omega_{\widetilde{\mathscr{X}_0}/k}^{\vee})$ where $\omega_{\widetilde{\mathscr{X}_0}/k}$ is the canonical sheaf of $\widetilde{\mathscr{X}_0}$. As $\widetilde{\mathscr{X}_0}$ has genus $g \geq 2$, $\omega_{\widetilde{\mathscr{X}_0}/k}$ is ample and so $H^0(\widetilde{\mathscr{X}_0}, \omega_{\widetilde{\mathscr{X}_0}/k}^{\vee}) = 0$. Therefore, $\mathscr{H}_0$ is étale and $\mathscr{H}$ is unramified. In

particular, there is some $\sigma \in G_K = I_K$ such that $(X+a)^\sigma \neq X+a$. Thus:

$$(X+a)(\bar{K}) \cap A[\infty]^{(p')} \subseteq (X+a)(\bar{K}) \cap \sigma((X+a)(\bar{K})).$$

The right hand side consists of the intersection of two distinct integral curves and so is finite and bounded independently of a and σ. Indeed, we may take μ_0 to be the maximum of this number, and the bound from Remark 4.1.17. In the case when A is an abelian surface, we have that $|(X+a)(\bar{K}) \cap \sigma((X+a)(\bar{K}))| \leq X \cdot X = \mathscr{X}_0 \cdot \mathscr{X}_0$. Now suppose that $a \in A(K) \cong \mathscr{A}(R)$ so that $X+a$ is a K-curve. It is sufficient to show that:

$$|\mathrm{Im}((\mathscr{X}_1 + a_1)(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow (\mathscr{X}_0 + a_0)(k))| \leq \mu_0.$$

As k is algebraically closed, there exists an element $b_0 \in \mathscr{A}_0(k)$ such that $pb_0 = a_0$. Picking any lifting $b_1 \in \mathscr{A}_1(R_1)$ of b_0, we have that $a_1 = pb_1 + c_1$ where c_1 is in the kernel of reduction. Write $\Lambda(a_1) = \mathrm{Im}((\mathscr{X}_1 + a_1)(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow (\mathscr{X}_0 + a_0)(k))$. The case $\Lambda(0)$ is of course Prop. 4.1.14. We split into two cases:

(i) First we assume that $a_1 = pb_1$. Then we see that $\Lambda(pb_1) = \Lambda(0) + pb_0$ and so these sets are of the same cardinality.

(ii) Now assume that $a_1 = c_1$ is in the kernel of reduction. Then, we can replicate the proof of Prop. 4.1.14 and construct a bundle $\mathbb{V}_0 \to \mathscr{X}_0 = (\mathscr{X}_1 + c_1)_0$ and a curve $\mathscr{Y}_0'$ which remain unchanged (as they depend only on the special fibre). On the other hand, $\mathscr{X}_1 + c_1$ is a different lifting of $\mathscr{X}_0$, and so the trivialising section $\mathscr{X}_0'$ of $\mathbb{V}_0$ changes. However, one can check that the bounds obtained in Remark 4.1.17 still hold for the size of $\Lambda(c_1)$. Indeed, one simply replaces the morphism of sheaves $\epsilon : \mathscr{M}_0 \longrightarrow \mathscr{O}_{\widetilde{\mathscr{Y}_0'}}$ with a morphism $\epsilon + (\tilde{h}_0')^*(v)$ for a unique morphism $v : \mathscr{C}_{\mathscr{X}_0/\mathscr{A}_0} \to \mathscr{O}_{\mathscr{X}_0}$ as given by the torsor description of $\mathbb{V}_0$ in Prop. 4.1.7, thus giving the same bound μ_0. □

Note that, as we assumed our initial input data $X \hookrightarrow A$ were defined over a number field L, there are an infinite number of finite places of L satisfying Assumption 4.1.2. Choosing another finite place w satisfying the same conditions, and lying over a distinct prime $q \neq p$, one obtains a bound:

$$|X(\bar{L}) \cap A[\infty]^{(q')}| \leq \mu_1$$

where μ_1 is the bound obtained in Remark 4.1.17 when we work over the prime q instead of p. It is clear that $X(\bar{L}) \cap A[\infty]^{(p)} \subseteq X(\bar{L}) \cap A[\infty]^{(q')}$ as $p \neq q$ so we obtain the following as a corollary of Prop. 4.1.30:

Proposition 4.1.31. *For all $a \in A(\bar{K})$, there exists a bound:*

$$|(X + a)(\bar{K}) \cap A[\infty]^{(p)}| \leq \mu_1$$

where μ_1 is independent of $a \in A(\bar{K})$.

Remark 4.1.32. Alternatively, one may obtain a bound μ_1 as above by studying *homotheties* of the p-adic Tate module of A (cf. [Bog80]). In this way, one may obtain bounds on the number of p-primary torsion points of A lying on (any translate of) X without the extra assumption of good reduction at another place w. We discuss this in the Appendix (Prop. B.2.1).

We now describe how to combine the bounds on coprime-to-p and p-primary torsion into a single bound on the size of $X(\bar{K}) \cap A[\infty]$.

Definition 4.1.33. Let K be a characteristic 0 field, complete with respect to a discrete valuation, with residue characteristic $p > 0$. Let A/K be an abelian variety. We say that the inertia action on A is *large* if for all $N > 0$ there exists an integer $r > 0$ such that, whenever $x \in A[\infty]^{(p)}$ has order $> p^r$, then the size of the orbit $I_K \cdot x$ is $> N$.

Informally, the size of the I_K-orbits of points of $A[\infty]^{(p)}$ tend to infinity as their order tends to infinity. We show immediately that when A/K has a large inertia action, we can bound the torsion points lying on X:

Proposition 4.1.34. *Suppose that A has large inertia action. Then there exists a constant $c > 0$, depending on the residue characteristic $p > 0$ and a distinct prime $q \neq p$, such that:*

$$|X(\bar{K}) \cap A[\infty]| \leq c.$$

Proof. Suppose that $x \in X(\bar{K}) \cap A[\infty]$. Then there exists a unique decomposition $x = x' + x''$ where $x' \in (X - x'')(\bar{K}) \cap A[\infty]^{(p')}$ and $x'' \in (X - x')(\bar{K}) \cap A[\infty]^{(p)}$. As $x' \in A(K)$ we have that $X - x'$ is a K-curve and thus:

$$G_K \cdot x'' \subseteq (X - x')(\bar{K}) \cap A[\infty]^{(p)}.$$

Then, using Prop. 4.1.31, we have that $|G_K \cdot x''| \leq \mu_1$. As the inertia action is large, there exists some $r > 0$ such that the order of x'' is at most p^r (depending on μ_1). There are at most $|A[p^r](\bar{K})| = p^{2gr}$ possibilities for x'' where $g = \dim(A)$. For each such possibility, the number of possibilities for x' is bounded by

$$|(X - x'')(\bar{K}) \cap A[\infty]^{(p')}| \leq \mu_0$$

by Prop. 4.1.30. In total:

$$|X(\bar{K}) \cap A[\infty]| \leq c := p^{2gr} \cdot \mu_0. \qquad \square$$

Let $\mathscr{A}[p^\infty]$ denote the p-divisible group of $\mathscr{A}$ over R. Recall that $\mathscr{A}[p^\infty]$ has an associated connected-étale sequence:

$$0 \longrightarrow \mathscr{A}[p^\infty]^\circ \longrightarrow \mathscr{A}[p^\infty] \longrightarrow \mathscr{A}[p^\infty]^{\text{ét}} \longrightarrow 0.$$

The failure of the action on $A[\infty]^{(p)} = \mathscr{A}[p^\infty](\bar{K})$ to be large precisely occurs when $\mathscr{A}[p^\infty](K)$ has a non-trivial, p-divisible sub-group:

Lemma 4.1.35. *Let T'_p be the maximal p-divisible subgroup of $\mathscr{A}[p^\infty](K)$. Then there exists a p-divisible subgroup $T'' \subseteq A[\infty]^{(p)}$ such that:*

$$A[\infty]^{(p)} \cong T'_p \oplus T''$$

as Galois modules. Moreover, the inertia action on T'' is large.

Proof. See [Ray83-1, Lemma 5.2.1]. $\square$

We conclude the chapter by giving a proof of the Manin-Mumford conjecture in general:

Theorem 4.1.36. *[Manin-Mumford Conjecture] Suppose that $X \hookrightarrow A/L$ is an integral curve of geometric genus $g \geq 2$ embedded in an abelian variety defined over a number field L. Suppose that there are places v, w of L, unramified over distinct primes p, q respectively such that X and A have good reduction at both v and w. Then there exists a constant $c > 0$, depending on p and q such that:*

$$|X(\bar{K}) \cap A[\infty]| \leq c.$$

Proof. Consider the new decomposition of the torsion points of A:

$$A[\infty] = T' \oplus T''$$

where T'' is the supplement from Lemma 4.1.35 and $T' = T'_p \oplus A[\infty]^{(p')}$. Then we still have that T' is unramified and $pT' = T'$ by construction. We may then repeat the proof of Proposition 4.1.34 to obtain a bounds μ_0 on the cardinality of $X(\bar{K}) \cap T'$. As the inertia action on T'' is now large, we may obtain a bound on $X(\bar{K}) \cap T''$ as in Prop. 4.1.31 respectively and then produce a total bound $c > 0$ on $X(\bar{K}) \cap A[\infty]$ by repeating the proof of Proposition 4.1.34 with respect to the new decomposition. $\square$

Chapter 5

Bounds obtained for the Bogomolov-Fu-Tschinkel conjecture in the case of good reduction

5.1 Bounds obtained for the Bogomolov-Fu-Tschinkel conjecture in the case of good reduction

We now return to the conjecture of Bogmolov-Fu-Tschinkel and describe the bounds one may obtain from Raynaud's proof of the Manin-Mumford conjecture in the good reduction case. Suppose that $\pi_i : E_i \to \mathbb{P}^1$, $i = 1, 2$ are standard double covers of elliptic curves defined over some algebraically closed field k. Write:

$$\pi_i(E_i[2](k)) = \{a_i, b_i, c_i, d_i\}.$$

We consider the curve $i : X \hookrightarrow E_1 \times E_2$ given by the preimage of the diagonal $\Delta_{\mathbb{P}^1}$ under the product of the standard projections $\pi_1 \times \pi_2$ (i.e. the fibre product):

$$\begin{array}{ccc} E_1 \times E_2 & \longleftarrow & X \\ \downarrow{\scriptstyle \pi_1 \times \pi_2} & & \downarrow \\ \mathbb{P}^1 \times \mathbb{P}^1 & \longleftarrow & \Delta_{\mathbb{P}^1} \end{array} .$$

Using Raynaud's proof of the Manin-Mumford conjecture, we can obtain a bound $c > 0$ on the torsion points of $E_1 \times E_2$ lying on X:

$$\left| X(\bar{L}) \cap E_1[\infty] \times E_2[\infty] \right| \leq c$$

when the standard double covers (E_i, π_i) satisfy certain conditions that we will explain later.

Remark 5.1.1. The morphism $X \to \Delta_{\mathbb{P}^1}$ is degree four, and branched at the points:

$$\{(a_1, a_1), (b_1, b_1), (c_1, c_1), (d_1, d_1), (a_2, a_2), (b_2, b_2), (c_2, c_2), (d_2, d_2)\}.$$

Generically, this is a set of 8 distinct points in $\mathbb{P}^1(k)$ and so a bound $c > 0$ above would lend itself to the following bound on the number of common projective torsion points:

$$|\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])| \leq \frac{c}{4} + 8.$$

Letting h_1 and h_2 represent classes of $\mathbb{P}^1 \times \{*\}$ and $\{*\} \times \mathbb{P}^1$ in $\mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1)$ respectively, we have that $\mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z}h_1 \oplus \mathbb{Z}h_2$. Then $\Delta \sim h_1 + h_2$ and as each E_i is a double cover of $\mathbb{P}^1$, we have that:

$$X \sim 2(E_1 + E_2) \in \mathrm{Pic}(E_1 \times E_2) \quad \text{and so} \quad X^2 = X \cdot X = 8(E_1 \cdot E_2) = 8.$$

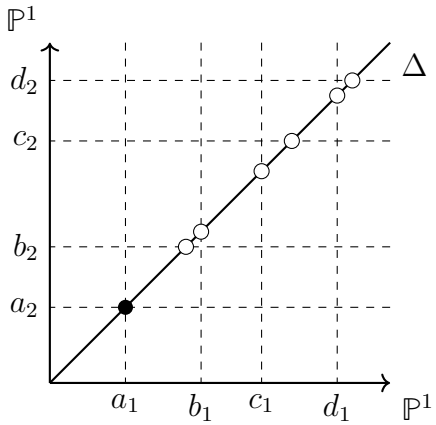
Then, using the adjunction formula [Har13, V, Prop. 1.5] we have that:

$$p_a(X) = \frac{1}{2}(X \cdot (X + \mathcal{K}_{E_1 \times E_2}) + 2) = \frac{1}{2}(X^2 + 2) = 5$$

as $E_1 \times E_2$ is an abelian surface so has trivial canonical divisor. To apply the Manin-Mumford conjecture to $X \hookrightarrow E_1 \times E_2$, we need to verify when $p_g(X) \geq 2$. To do this, we compute the singularities of X. As $\Delta_{\mathbb{P}^1} \cong \mathbb{P}^1$ is non-singular, X can only have singularities over the branch points:

$$\{(a_1, a_1), (b_1, b_1), (c_1, c_1), (d_1, d_1), (a_2, a_2), (b_2, b_2), (c_2, c_2), (d_2, d_2)\}.$$

The number of branch points is given by: $8 - |\pi_1(E_1[2](k)) \cap \pi_2(E_2[2](k))|$. We use an analytic argument to determine which of these branch points correspond to singularities of X. Consider the diagram of $\mathbb{P}^1 \times \mathbb{P}^1$ below:



Working analytically (over $\mathbb{C}$ for example) we can pick local complex coordinates $(z_1, z_2) \in E_1 \times E_2$ and $w_i \in \mathbb{P}^1$ such that $z_i^2 = w_i$ if w_i is a branch point of π_i, and $z_i = w_i$

otherwise. Suppose that two branch points $a_1 = a_2$ coincide (i.e. the point $\bullet$ above). Then $X \subseteq E_1 \times E_2$ is locally analytically given by the equation:

$$\{z_1^2 - z_2^2 = 0\} \subseteq E_1 \times E_2$$

and so there is a node of X lying over $(a_1, a_2) \in \Delta_{\mathbb{P}^1}$. On the other hand, if b_1 is a branch point of $\pi_1 : E_1 \to \mathbb{P}^1$ but $b_1 \notin \pi_2(E_2[2])$ is not a branch points of π_2 (i.e. a point $\circ$), then X is given locally analytically by the equation:

$$\{z_1^2 - z_2 = 0\} \subseteq E_1 \times E_2$$

and so X is smooth over a neighbourhood of $(b_1, b_1) \in \Delta_{\mathbb{P}^1}$. Overall, we have shown the following:

Lemma 5.1.2. *Let (E_i, π_i), $i = 1, 2$ be a pair of standard double covers defined over a field of characteristic $\neq 2$. Let $X = (\pi_1 \times \pi_2)^{-1}(\Delta_{\mathbb{P}^1})$ be the preimage of the diagonal. Then X has arithmetic genus $p_a(X) = 5$. Moreover, X has nodes over the points:*

$$\pi_1(E_1[2]) \cap \pi_2(E_2[2]);$$

and thus has geometric genus:

$$p_g(X) = 5 - |\pi_1(E_1[2]) \cap \pi_2(E_2[2])|\,.$$

In particular, when $\pi_1(E_1[2]) \cap \pi_2(E_2[2]) = \emptyset$, X is smooth.

Let $\sigma_1 = \iota_1 \times \mathrm{Id}$ and $\sigma_2 = \mathrm{Id} \times \iota_2$ denote the respective involutions of the first and second component of $E_1 \times E_2$. This defines a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ action on $E_1 \times E_2$. By construction X is invariant under this action and so we obtain a subgroup:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong H \subseteq \mathrm{Aut}(X).$$

Note that $X/\sigma_1 = E_2$ and $X/\sigma_2 = E_1$.

Lemma 5.1.3. *Suppose that $\pi_1(E_1[2]) \neq \pi_2(E_2[2])$. Then X is integral.*

Proof. As X is a double cover of E_i, either X is irreducible or it has two components C_1 and C_2 such that $C_1 \cong C_2 \cong E_1 \cong E_2$. Assume for contradiction that we are in the latter case and $X = C_1 \cup C_2$. Then, as any automorphism $g \in H$ permutes C_1 and C_2, we obtain a group homomorphism:

$$H \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

where $g(C_1) = C_{\sigma(1)}$, $g(C_2) = C_{\sigma(2)}$ for some permuation $\sigma \in \mathrm{Aut}\{1, 2\} \cong \mathbb{Z}/2\mathbb{Z}$. This group homomorphism has a non-trivial kernel, and so there exists some $g \neq \mathrm{Id}$ such that

$g(C_1) = C_1$ and $g(C_2) = C_2$. As g is non-trivial, without loss of generality, we may assume that g induces the involution $\iota_2 : E_2 \to E_2$. On the other hand, by assumption, there is some branch point $b_1 \in \pi_1(E_2[2])$ such that $b_1 \notin \pi_2(E_2[2])$. X is smooth over some neighbourhood of b_1 and so there are distinct points $P_1 \in C_1$ and $P_2 \in C_2$ lying over b_1. By assumption $g(P_1) = P_2$ and $g(P_2) = P_1$ as g corresponds to the involution of E_2 and P_1, P_2 correspond to non-2-torsion points, thus contradicting the assumption that $g(C_1) = C_1$ and $g(C_2) = C_2$. □

Remark 5.1.4. On the other hand, if $\pi_1(E_1[2]) = \pi_2(E_2[2])$ there is no contradiction and X has two elliptic components. Indeed, considering Weierstrass equations, this implies that $E_1 \cong E_2$ and so X is isomorphic to two copies of $E_1 \cong E_2$.

5.1.1 The Jacobian of the curve X

Consider the automorphism $\iota = \sigma_1\sigma_2 = \sigma_2\sigma_1$ of X. This is induced by the involution on the abelian surface $E_1 \times E_2$ and thus fixes the singularities of X:

$$\mathrm{Sing}(X) = X \cap (E_1[2] \times E_2[2]).$$

Let $X' = X/\iota$ denote the quotient curve and denote by $\tilde{X}$ and $\tilde{X}'$ the respective normalisations of X and X'. As the fixed locus of ι is precisely the singular locus of X, the curve X' has the same number of nodes as X. Consider the induced quotient map on the normalisations: $\tilde{X} \to \tilde{X}/\tilde{\iota} = \tilde{X}'$ where $\tilde{\iota} : \tilde{X} \to \tilde{X}$ extends ι. We may take local parameters z_i of E_i such that any singularity of X is analytically locally cut out of $E_1 \times E_2$ by the equation $z_1^2 - z_2^2 = 0$. In these coordinates, ι is given by $(z_1, z_2) \mapsto (-z_1, -z_2)$ and so the two local components $z_1 = z_2$ and $z_1 = -z_2$ are preserved by ι. This implies that the fixed locus of $\tilde{\iota}$ is given by the pairs of preimage points of $\tilde{X}$ lying over the nodes of X. Then, by the Riemann-Hurwitz formula we have:

$$2p_g(X) - 2 = 2(2p_g(X') - 2) + 2r$$

where $r = |\mathrm{Sing}(X)|$. Thus, the arithmetic and geometric genus of X' are given by the formula:

$$p_a(X') = r + p_g(X') = \frac{1}{2}(p_g(X) + r + 1) = 3.$$

We will now describe the Jacobian $J_{\tilde{X}}$ and the associated Albanese morphism:

$$a : J_{\tilde{X}} \longrightarrow E_1 \times E_2$$

with a view towards verifying that Assumption 4.1.21 holds in the present situation. The main tool we have in decomposing $J_{\tilde{X}}$ is the following [Kani-Ros89, Thm. C]:

Theorem 5.1.5. *Let C be a smooth, projective, geometrically connected curve defined over a field K. Suppose that $H \subseteq \mathrm{Aut}_K(C)$ is a finite subgroup and $H_1, ..., H_r \subseteq H$ are a collection of further subgroups such that $H_i \cdot H_j = H_j \cdot H_i$ for all i, j. Let g_{ij} denote the genus of $C/H_i \cdot H_j$. Suppose that:*

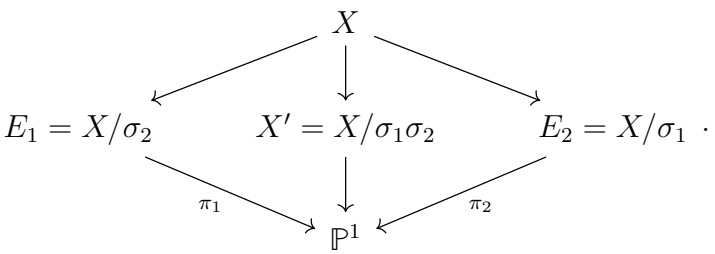
i) $g_{ij} = 0$ for all $1 \leq i < j \leq r$;

ii) $g_C = g_{C/H_1} + ... + g_{C/H_r}$.

Then there is an isogeny:

$$J_C \sim J_{C/H_1} \times ... \times J_{C/H_r}.$$

Recall that there is a subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong H \subseteq \mathrm{Aut}(X)$ generated by the automorphisms $\sigma_1, \sigma_2 : E_1 \times E_2 \to E_1 \times E_2$ which give the involution on E_1 and E_2 respectively. These automorphisms extend uniquely to $\tilde{X}$. We sum up the corresponding quotients in the below diagram:



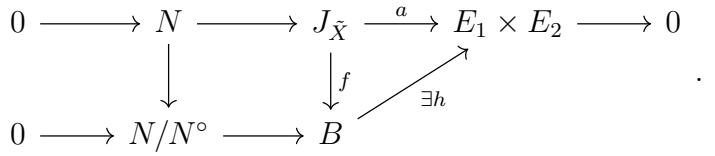
Taking $H_1 = \langle \sigma_1 \rangle, H_2 = \langle \sigma_2 \rangle, H_3 = \langle \sigma_1 \sigma_2 \rangle$ then $H_i \cdot H_j = H$ whenever $i \neq j$ so that $C/H_i \cdot H_j = \mathbb{P}^1$. Moreover, using the equality $g_{\tilde{X}} = g_{\tilde{X}'} + 2 = g_{\tilde{X}'} + g_{E_1} + g_{E_2}$, we obtain the following decomposition:

$$J_{\tilde{X}} \sim J_{\tilde{X}'} \times E_1 \times E_2$$

We now calculate the kernel $N = \ker(a)$ of the Albanese morphism $a : J_{\tilde{X}} \to E_1 \times E_2$ in each case $g(\tilde{X}) = 2, 3, 4, 5$ as in [BFT18, p. 7]:

Lemma 5.1.6. *The kernel of the Albanese morphism $N = \ker(a)$ is smooth in characteristic $\neq 2$. Moreover, if $N^\circ \subseteq N$ is the connected component of the identity, then the number of connected components of N: $|N/N^\circ|$ is a power of 2.*

Proof. The connected component of the identity $N^\circ \subseteq N$ is an abelian variety of dimension $g - 2$; isomorphic to $J_{\tilde{X}'}$. Let $f : J_{\tilde{X}} \to B = J_{\tilde{X}}/N^\circ$ denote the quotient, and consider the Stein factorisation:



Now $h : B \to E_1 \times E_2$ is an isogeny with kernel N/N°. Let $Z = f(\tilde{X})$. Let $n = \deg(h)$ and consider the preimage curve $h^{-1}(X) \subseteq B$. On one hand, the self intersection is given by $h^{-1}(X) \cdot h^{-1}(X) = n(X \cdot X) = 8n$. On the other hand, we have that:

$$[h^{-1}(X)] = \sum_{x \in N/N^\circ} [Z + x]$$

and so $h^{-1}(X) \cdot h^{-1}(X) = n^2(Z \cdot Z)$. Overall we have that:

$$|N/N^\circ| = \frac{8}{(Z \cdot Z)} \quad \text{and} \quad (Z \cdot Z) = 2p_a(Z) - 2 = 2(g(\tilde{X}) + \#(\text{nodes of } Z)) - 2$$

by the adjunction formula.

$g = 2$: In this case X' is rational and so $J_{\tilde{X}} \sim E_1 \times E_2$ and the Albanese morphism is an isogeny (in particular, it is surjective), so we have $a = h$ and $Z = \tilde{X}$. Up to projective transformation, we may assume:

$$\{a_1, b_1, c_1, d_1\} \cap \{a_1, b_1, c_1, d_1\} = \{0, 1, \infty\}.$$

By the adjunction formula $\tilde{X} \cdot \tilde{X} = 2g(\tilde{X}) - 2 = 2$. Therefore $2n^2 = 8n$ and $n = 4$. Moreover, one sees that $N \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ by noting that the ramification points $\{0, 1, \infty\}$ of $X \to \mathbb{P}^1$ correspond to 3 nodes $\{P_0, P_1, P_\infty\} \subseteq X$ and so to 6 points $\{Q_0, Q_0', Q_1, Q_1', Q_\infty, Q_\infty'\} \subseteq \tilde{X} \hookrightarrow J_{\tilde{X}}$ of the normalisation. We then obtain the elements: $[Q_0 - Q_0'], [Q_1 - Q_1'], [Q_\infty - Q_\infty'] \in \mathrm{Pic}^0(\tilde{X}) \cong J_{\tilde{X}}$ which can be easily seen to generate the kernel N with the relation:

$$[Q_0 - Q_0'] + [Q_1 - Q_1'] + [Q_\infty - Q_\infty'] = 0.$$

$g = 3$: In this case $\tilde{X}' = E_3$ is an elliptic curve and we have that:

$$J_{\tilde{X}} \sim E_1 \times E_2 \times E_3$$

and so it is clear that the kernel $N = \ker(a)$ contains E_3. Writing $\pi_i(E_i[2]) = \{a_i, b_i, c_i, d_i\}$ for $i = 1, 2$, without loss of generality we may take $a_1 = a_2 = 0$ and $b_1 = b_2 = \infty$ so that X has two nodes P_0 and P_∞. In fact, Z is non-singular so:

$$N/N^\circ \cong \mathbb{Z}/2\mathbb{Z}.$$

$g = 4$: In this case X' is a genus 2 curve. One can see from the equality:

$$8 = n(2(g(\tilde{X}) + \#(\text{nodes of } Z)) - 2) = n(6 + 2\#(\text{nodes of } Z))$$

that we have $n = 1$ and that Z has a single node, so lies isomorphically over X.

$g = 5$: In this case, $X = \tilde{X}$ is a smooth genus 5 curve and $X' = \tilde{X}'$ is smooth, hyperelliptic genus 3 curve. The double cover $X \to X'$ is unramified. We then see that $Z \cong X$ so that $(Z \cdot Z) = 8$ and again N/N° is trivial. □

Remark 5.1.7. The above discussion holds over any algebraically closed field of characteristic 0 or $p > 2$ as we utilise the fact that the finite covers of degrees 2 and 4 above are separable. Thus, to verify Assumption 4.1.21 for the reduction of $i : X \hookrightarrow E_1 \times E_2$ modulo p, one need only take $p > 2$.

5.1.2 Bounds on common coprime-to-p torsion

Let (E_i, π_i) be a pair of standard double covers defined over a number field L. Write $\pi_i(E_i[2])(\bar{L}) = \{a_i, b_i, c_i, d_i\}$. Fix a finite place v of L over a prime $p > 2$. Write R for the complete maximal unramified extension of $\mathscr{O}_{L,v}$ constructed in Assumption 4.1.2, K for the fraction field and k for the residue field.

Theorem 5.1.8. *Let (E_i, π_i), $i = 1, 2$ be a pair of standard double covers defined over a number field L. Write $\pi_i(E_i[2])(\bar{L}) = \{a_i, b_i, c_i, d_i\}$. Fix a finite place v of L over a prime $p > 2$. Suppose the following hold:*

i) v is unramified over p;

ii) E_1 and E_2 have good reduction at v;

iii) $\pi_1(E_1[2]) \cap \pi_2(E_2[2])$ has constant rank < 4 after reduction at v (i.e. these sets of branch points don't coincide, and the number of geometric points in the intersection does not increase after specialisation).

Then we have that:

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})\right| \leq 2p^3 + 8.$$

Proof. Let $X \hookrightarrow E_1 \times E_2$ be the curve given by the preimage of the diagonal under the product of the standard double covers. As the branch loci of π_1, π_2 do not coincide, as discussed in Lemma 5.1.2, X is integral of geometric genus ≥ 2. As we assume that E_1 and E_2 have good reduction, there exist abelian R-schemes $\mathscr{E}_1$ and $\mathscr{E}_2$ respectively extending the curves where R is the completion of the maximally unramified extension of $\widehat{\mathscr{O}}_{L,v}$. We then take $i : \mathscr{X} \hookrightarrow \mathscr{E}_1 \times_R \mathscr{E}_2$ to be the scheme-theoretic closure of X in $\mathscr{E}_1 \times_R \mathscr{E}_2$. Condition (iii) ensures that the normalisation of $\widetilde{\mathscr{X}}$ of $\mathscr{X}$ is smooth over R and so Assumption 4.1.2 is satisfied for $X \hookrightarrow E_1 \times E_2$ and so we may apply Corollary 4.1.16:

Consider the reduction mod p of the closed embedding $i_0 : \mathscr{X}_0 \hookrightarrow \mathscr{E}_{1,0} \times_k \mathscr{E}_{2,0}$. By flatness, the self intersection of $\mathscr{X}_0$ is still given by $(\mathscr{X}_0 \cdot \mathscr{X}_0) = (X \cdot X) = 8$. Recall that, the bounds from Corollary 4.1.16 depend on the degree of $h_0' : \mathscr{Y}_0' \to \mathscr{X}_0$ where:

$$\begin{array}{ccc} & & \mathscr{Y}_0' \\ & \overset{v_0'}{\nearrow} & \downarrow{\scriptstyle h_0'} \\ \mathscr{Y}_0 & \xrightarrow[v_0]{} & \mathscr{X}_0 \\ \downarrow & & \downarrow \\ \mathscr{E}_{1,0} \times_k \mathscr{E}_{2,0} & \xrightarrow[[p]]{} & \mathscr{E}_{1,0} \times_k \mathscr{E}_{2,0} \end{array}$$

$\mathscr{Y}_0 \hookrightarrow \mathscr{E}_{1,0} \times_k \mathscr{E}_{2,0}$ is the reduced preimage of $\mathscr{X}_0$ under the multiplication-by-p map, and $v_0 : \mathscr{Y}_0 \to \mathscr{X}_0$ is the restriction of the multiplication-by-p map to $\mathscr{Y}_0$. To bound $\deg(h_0')$, we need to understand the connected-étale sequence of $\mathscr{G}_0 = \mathscr{E}_{1,0}[p] \times_k \mathscr{E}_{2,0}[p]$. Recall that:

i) If $\mathscr{E}_0/k$ is a supersingular elliptic curve then $\mathscr{E}_0[p] = \mathscr{E}_0[p]^\circ$ is of rank p^2, and coincides with $\ker(F^{(2)}_{\mathscr{E}_0/k})$.

ii) If $\mathscr{E}_0/k$ is an ordinary elliptic curve then:

$$\mathscr{E}_0[p] \cong \mu_{p,k} \times_k \mathbb{Z}/p\mathbb{Z}$$

(cf. Cor. 3.3.18). Applying Proposition 4.1.29 to the above situation, we have that:

i) If $\mathscr{E}_{1,0}$ and $\mathscr{E}_{2,0}$ are both supersingular then:

$$\deg(v_0) = \text{insep.deg}(v_0) = p^2.$$

As v_0' is separable, it is an isomorphism and overall $\deg(h_0') = p^2$.

ii) If exactly one of $\mathscr{E}_{1,0}$ and $\mathscr{E}_{2,0}$ is ordinary then:

$$\text{sep.deg}(v_0) = p \quad \text{and} \quad \text{insep.deg}(v_0) = p^2.$$

Thus we have that $\deg(h_0') \leq p^3$.

iii) If $\mathscr{E}_{1,0}$ and $\mathscr{E}_{2,0}$ are both ordinary then:

$$\text{sep.deg}(v_0) = p^2 \quad \text{and} \quad \text{insep.deg}(v_0) = p$$

and so $\deg(h_0') \leq p^3$.

Thus, in all cases we obtain the bound:

$$|X(\bar{K}) \cap (E_1[\infty]^{(p')} \times E_2[\infty]^{(p')})| \leq 8p^3$$

and by the considerations in Remark 5.1.1 we can infer the bound $2p^3 + 8$ on common projective torsion points. □

Overall, we obtain the bound $2p^3 + 8$ in all cases. However, we obtain a slight sharpening of the bound on $\deg(h_0')$ when one or both of $\mathscr{E}_{i,R_1}$ is the canonical lifting of $\mathscr{E}_{i,0}$ (cf. 4.1.4):

i) If exactly one of $\mathscr{E}_{1,R_1}$ and $\mathscr{E}_{2,R_1}$ is a canonical lifting, then we have that $\deg(h_0') \leq p^2$.

ii) If both $\mathscr{E}_{1,R_1}$ and $\mathscr{E}_{2,R_1}$ are canonical liftings, then we have that $\deg(h_0') = p$.

We sum up the sharpenings we can make depending on the reduction type of the curves, and whether one or both is a canonical lifting modulo p^2 as follows:

Corollary 5.1.9. *Keeping the assumptions as above, we obtain the following sharpenings of the bound given:*

i) Suppose that both curves E_1 and E_2 have supersingular reduction. Then:

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})\right| \leq 2p^2 + 8.$$

ii) Suppose that exactly one of the curves is the canonical lifting of its reduction mod v. Then:

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})\right| \leq 2p^2 + 8.$$

iii) Suppose that both curves are the canonical liftings of their reductions mod v. Then:

$$\left|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})\right| \leq 2p + 8.$$

5.1.3 Bounds on common torsion points of any order

Let $X \hookrightarrow E_1 \times E_2/L$ be as in the previous subsection. We have the bound on the coprime-to-p torsion lying on X:

$$\left|X(\bar{K}) \cap E_1[\infty]^{(p')} \times E_2[\infty]^{(p')}\right| \leq 8p^i$$

where $i = 1, 2$ or 3. Suppose that we take a second finite place w of L over a prime $q \neq p$ satisfying Assumption 4.1.2, then we obtain similar bounds on the p-primary torsion:

$$\left|X(\bar{K}) \cap E_1[\infty]^{(p)} \times E_2[\infty]^{(p)}\right| \leq 8q^j$$

again for some $j = 1, 2$ or 3. Using the results of Prop. 3.7.8 and Cor. 3.7.11, as long as E_1 and E_2 are not canonical liftings, there is some explicit function $N(r)$ such that, if

$x \in E_1[\infty]^{(p)} \times E_2[\infty]^{(p)}$ has order $\geq p^r$ then we have a lower bound:

$$|I_K \cdot x| \geq N(r).$$

Applying the proof of Prop. 4.1.34 with $\mu_0 = 8p^3$, $\mu_1 = 8q^3$ and $N(r)$, one obtains a tractable bound for the common projective torsion points of two elliptic curves:

Theorem 5.1.10. *Let (E_i, π_i), $i = 1, 2$ be a pair of standard double covers defined over a number field L. Write $\pi_i(E_i[2])(\bar{L}) = \{a_i, b_i, c_i, d_i\}$. Fix a finite place v of L over a prime $p > 2$. Suppose the following hold:*

i) v is unramified over p;

ii) E_1 and E_2 have good reduction at v;

iii) $\pi_1(E_1[2]) \cap \pi_2(E_2[2])$ has constant rank < 4 after reduction at v (i.e. these sets of branch points don't coincide, and the number of geometric points in the intersection does not increase after specialisation).

Suppose that w is another finite place of L satisfying the above, and lying over a prime $q \neq p$. Then we have that:

$$|\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty])| \leq \frac{c}{4} + 8$$

where:

$$c = 8p^3 \cdot p^{4r}$$

and r is the smallest positive integer such that $N(r) \leq 8q^3$.

Remark 5.1.11. When one of the component curves E_i is a canonical lifting, then as explained in Lemma 4.1.35, one can still obtain the bound above by re-running the arguments in Prop. 4.1.34 with the decomposition described in Lemma 4.1.35.

It is a purely combinatorial problem to determine the constant $c > 0$ in each of the cases described (depending on the reduction type of E_1 and E_2), and depending on the primes p, q. In the case where one of the curves E_i has ordinary reduction, the constant $N(r)$ depends on the Serre-Tate coordinate λ_i of E_i (cf. Cor. 3.7.11). More specifically, one needs to know the valuation $v(\lambda_i - 1)$ to write $N(r)$ explicitly. We discuss in the Appendix (Prop. A.2.1) how one may determine this valuation for small primes.

Part III

The case of semistable reduction and methods from logarithmic geometry

Chapter 6

Semistable reduction and Néron models

Until now, we have primarily been concerned with the common torsion points of pairs of elliptic curves with good reduction. In the next part, we will extend some of the methods of Raynaud to the case of *bad reduction* of one or both of the elliptic curves in question to obtain new bounds for the Bogomolov-Fu-Tschinkel conjecture.

6.1 Néron models of elliptic curves and Tate curves

6.1.1 Properties of Néron models

The standard reference for Néron models is [BLR-12], however, when we restrict our attention to elliptic curves, the main reference will be [Sil94] with some auxiliary results from [Liu02]. Let S be a Dedekind scheme i.e. a noetherian integral scheme of dimension 1 whose local rings are all regular. Examples to keep in mind are non-singular algebraic curves, the spectra of Dedekind domains, and their localisations at non-zero primes. Suppose that K is the fraction field of S and that X is a smooth, separated K-scheme of finite type. By a *model* of X over S, we will mean a flat S-scheme $\mathscr{X}$ such that $\mathscr{X}_K \cong X$.

Definition 6.1.1 (Néron Mapping Property)**.** Let X be a smooth, separated K-scheme of finite type. A *Néron model* for X over S (if it exists) is a smooth, separated S-model $\mathscr{X}$ of finite type satisfying the *Néron Mapping Property* (NMP):

For each smooth S-scheme $\mathscr{Y}$ with a morphism of K-schemes $u_K : \mathscr{Y}_K \to \mathscr{X}_K$, there exists a unique S-morphism $u : \mathscr{Y} \to \mathscr{X}$ extending u_K.

We note the following immediate consequences of the NMP:

Proposition 6.1.2. *Let X be a smooth, separated K-scheme of finite type.*

i) A Néron model for X over S is unique up to isomorphism, if it exists.

ii) Suppose that the Néron model $\mathscr{X}/S$ of X exists. Then there is a natural bijection:

$$\mathscr{X}(S) \cong X(K).$$

iii) Suppose that X is a K-group scheme. Then $\mathscr{X}$ is an S-group scheme; extending the group structure on X.

Example 6.1.3. Suppose that R is a complete DVR with fraction field K and set $S = \mathrm{Spec}(R)$. The following are *non-examples* of Néron models.:

i) $\mathbb{P}^1_R$ fails to be a Néron model of $\mathbb{P}^1_K$ precisely because there exists automorphisms of $\mathbb{P}^1_K$ that fail to extend to $\mathbb{P}^1_R$. Suppose for contradiction that $\mathbb{P}^1_R$ is a Néron model, and consider the automorphism $\gamma \in \mathrm{PGL}(2, K)$ given by:

$$\gamma = \begin{bmatrix} \pi & 0 \\ 0 & 1 \end{bmatrix}$$

where $\pi \in R$ is a uniformiser. If $\gamma_R : \mathbb{P}^1_R \to \mathbb{P}^1_R$ is the R-morphism given by the same matrix, then this must be the unique extension of γ. However, the restriction $\gamma_k : \mathbb{P}^1_k \to \mathbb{P}^1_k$ is no longer invertible, and thus γ_R is not an R-automorphism.

On the other hand, from the NMP, it is clear that any K-automorphism should extend uniquely to an R-automorphism (the inverse must also extend uniquely, and the composite extends uniquely to the identity).

ii) Similarly, $\mathbb{G}_{m,R}$ fails to be the Néron model of $\mathbb{G}_{m,K}$. This is most easily seen on points:

$$\mathbb{G}_{m,R}(R) = R^* = R \setminus \pi R \ncong K^* = \mathbb{G}_{m,K}(K).$$

6.1.2 Néron models of elliptic curves

Let R be a complete discrete valuation ring with fraction field K and residue field k. Assume that K is characteristic 0 and that k is separably closed of characteristic $p > 0$. Let π be a uniformiser of R and let $\mathfrak{m} = \pi R$ denote the maximal ideal. In this subsection we will primarily be concerned with elliptic curves E/K with multiplicative reduction. The main reference will be [Sil94]. The following construction [Sil94, Example 5.4.4] will turn out to be prototypical for the models we wish to consider and so we provide it here:

Example 6.1.4. Let $\mathscr{W}/R$ be defined to be the following Weierstrass curve:

$$\mathscr{W} : y^2 + xy = x^3 + \pi^N \subseteq \mathbb{P}^2_R$$

where $N > 0$ is an integer. Letting $E = \mathscr{W}_K$, we see that E has multiplicative reduction at π as:

$$\mathscr{W}_k : y^2 + xy = x^3$$

is the rational curve with a single node $\gamma = (0,0) \in \mathscr{W}_k$. Let $\mathscr{W}^{\mathrm{sm}} = \mathscr{W} \setminus \{\gamma\}$. By properness, it is clear that $\mathscr{W}(R) \cong E(K)$. So suppose that $(a,b) \in \mathscr{W}(R)$ specialises to $\gamma = (0,0)$. Then we can write $(a,b) = (\pi a', \pi b')$ such that $a', b' \in R$ satisfy:

$$\pi(b')^2 + \pi^2 a'b' = \pi^2(a')^3 + \pi^{N-1}.$$

Thus, if $N = 1$, by considering valuations, we see that no such point can exist and $\mathscr{W}^{\mathrm{sm}}(R) = E(K)$ and in fact $\mathscr{W}^{\mathrm{sm}}$ is the Néron model for E. On the other hand, if $N > 1$ there is no contradiction and in fact $\mathscr{W}^{\mathrm{sm}}$ is not the Néron model of E. This is explained in part because $\mathscr{W}$ is not regular. Indeed, the point $\gamma \in \mathscr{W}$ behaves like a cyclic quotient singularity in the sense that there is an étale chart:

$$\mathscr{U} = \mathrm{Spec}\left(\frac{R[u,v]}{\langle uv - \pi^N \rangle}\right) \longrightarrow \mathscr{W}$$

where $\mathscr{U}$ is obtained from the $\mathbb{A}^1_{\mathbb{Z}}$-scheme $X = \mathrm{Spec}\left(\frac{\mathbb{Z}[u,v,t]}{\langle uv - t^N \rangle}\right)$ via the base change:

$$\begin{array}{ccc} \mathscr{U} & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathbb{A}^1_{\mathbb{Z}} \end{array}$$

sending $t \mapsto \pi$. On the other hand, applying the base change $\mathrm{Spec}(\mathbb{C}[t]) \to \mathbb{A}^1_{\mathbb{Z}}$ we obtain the usual cyclic quotient singularity of type A_{N-1}. We will see that there exists a *minimal resolution* $\mathscr{C} \to \mathscr{W}$ of this singularity to a regular, proper model of E and that its smooth locus $\mathscr{C}^{\mathrm{sm}}$ is the Néron model of E.

We make the above construction concrete with the following definitions and propositions. Let E/K be an elliptic curve in Weierstrass form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$. By performing a change of coordinates, one may take the values $a_i \in R$. We say that the corresponding projective R-scheme in $\mathbb{P}^2_R$ is a *minimal Weierstrass model* $\mathscr{W}$ of E if the discriminant $\Delta = \Delta(a_i)$ is minimal with respect to its valuation $v(\Delta) \geq 0$. Let $\mathscr{W}^{\mathrm{sm}} \subseteq \mathscr{W}$ denote the maximal smooth subscheme of $\mathscr{W}$; i.e. we remove the singular point of $\mathscr{W}_k$ if it exists. In general, this is not the Néron model of E but still enjoys certain desirable properties:

Proposition 6.1.5. *Let R be discrete valuation ring with fraction field K. Let E/K be an elliptic curve and $\mathscr{W}/R$ its minimal Weierstrass model. Let $\mathscr{W}^{sm}$ denote the largest smooth subscheme of $\mathscr{W}$.*

i) $\mathscr{W}^{\mathrm{sm}}$ is an R-group scheme with generic fibre isomorphic to E;

ii) The addition map on $\mathscr{W}^{\mathrm{sm}}$ extends to an R-group scheme action:

$$\mathscr{W}^{\mathrm{sm}} \times_R \mathscr{W} \longrightarrow \mathscr{W};$$

iii) If $\mathscr{W}$ is regular then $\mathscr{W}^{\mathrm{sm}}(R) \cong E(K)$.

Proof. See [Sil94, IV, §5, Theorem 5.3]. □

In general, the minimal Weierstrass model is not the Néron model of E. To obtain the Néron model we would like to desingularise the *arithmetic surface* $\mathscr{W} \to \mathrm{Spec}(R)$, minimally, so that the resulting resolution of singularities can still satisfy the Néron Mapping Property.

Relatively minimal arithmetic surfaces

Let S be a Dedekind scheme with fraction field K. An *arithmetic surface* $\mathscr{C}$ is an integral, normal, excellent scheme which is flat and finite type over S whose generic fibre $C = \mathscr{C}_K$ is a smooth, integral, projective curve of genus $g \geq 1$. Note that, by flatness, for each closed point $s \in S$ the curve $\mathscr{C}_s$ has arithmetic genus $p_a(\mathscr{C}_s) = g$. Moreover, the normality assumption ensures that the singularities of $\mathscr{C}$ lie in codimension 2 i.e. are a finite set of points, lying only on a finite set of closed fibres $\mathscr{C}_s$.

Theorem 6.1.6. *Let R be a Dedekind domain with fraction field K, and let C/K be a smooth, projective, integral curve of genus $g \geq 1$.*

i) There exists an arithmetic surface $\mathscr{C}/R$ with generic fibre C that is regular and proper over R. We call $\mathscr{C}$ a proper regular model for C.

ii) There exists a proper regular model $\mathscr{C}^{\min}/R$ for C that is (relatively) minimal in the sense that, for any other proper regular model $\mathscr{C}$ of C, the induced birational map $\mathscr{C} \dashrightarrow \mathscr{C}^{\min}$ extends to an R-morphism.

Proof. See [Sil94, IV, §4, Theorem 4.5]. □

We refer to the (unique up to R-isomorphism) model $\mathscr{C}^{\min}$ as the (relatively) *minimal proper regular model* of C. The construction of $\mathscr{C}^{\min}$ works much like the classical case of minimal models of compact complex surfaces. Indeed, given a normal, proper model $\mathscr{C}$ of C, there exists a finite sequence of blow-ups $\tilde{\mathscr{C}} \to \mathscr{C}$, centered at the singular points of $\mathscr{C}$ such that $\tilde{\mathscr{C}}$ is regular. We then perform a series of *contractions* on $\tilde{\mathscr{C}}$ that terminate at a unique proper regular model.

Let $S = \mathrm{Spec}(R)$ where R is a discrete valuation ring and suppose $\mathscr{C} \to S$ is a proper arithmetic surface. $\mathscr{C}$ is normal so admits a good notion of a Weil divisor. Let $\mathrm{Div}(\mathscr{C})$ denote the free abelian group generated by the irreducible Weil divisors of $\mathscr{C}$ i.e. integral closed subschemes of dimension 1. Viewing $\mathscr{C}$ as a fibred surface, there are two main classes of divisors. Any section $\sigma : S \to \mathscr{C}$ has closed image which we view as a *horizontal divisor*. On the other hand, letting $0 \in S$ denote the closed point, we may write:

$$\mathscr{C}_0 = \sum_i n_i F_i;$$

where $F_i \subseteq \mathscr{C}_0$ are irreducible curves and n_i are a finite set of non-zero integers. This defines a subgroup of *fibral divisors*:

$$\mathrm{Div}_f(\mathscr{C}) \subset \mathrm{Div}(\mathscr{C});$$

generated by the divisors F_i.

Theorem 6.1.7. *Let R be a discrete valuation ring with residue field k, $S = \mathrm{Spec}(R)$ and $\mathscr{C}/S$ a regular, proper arithmetic surface. There exists a unique bilinear pairing:*

$$\begin{aligned} \mathrm{Div}(\mathscr{C}) \times \mathrm{Div}_f(\mathscr{C}) &\longrightarrow \mathbb{Z}; \\ (D, F) &\longmapsto D \cdot F. \end{aligned}$$

satisfying the following properties:

i) If $D \in \mathrm{Div}(\mathscr{C})$ and $F \in \mathrm{Div}_f(\mathscr{C})$ are irreducible, then:

$$D \cdot F = \sum_{x \in D \cap F} I_x(D, F);$$

where:

$$I_x(D, F) = \dim_k \frac{\mathscr{O}_{\mathscr{C},x}}{\langle f, g \rangle};$$

and $f, g \in \mathscr{O}_{\mathscr{C},x}$ are local equations for D, F respectively.

ii) If $D_1, D_2 \in \mathrm{Div}(\mathscr{C})$ are linearly equivalent then for any fibral divisor F we have:

$$D_1 \cdot F = D_2 \cdot F.$$

iii) The restriction of $\cdot$ to fibral divisors is symmetric.

Proof. See [Sil94, IV, §7, Theorem 7.2]. □

Note that, for any rational function $f \in K(\mathscr{C})$ the associated principal divisor:

$$\mathrm{div}(f) = \sum_D \mathrm{ord}_D(f) D$$

is, by definition, linearly equivalent to 0 and so $\mathrm{div}(f) \cdot F = 0$ for all fibral divisors F by (ii). In particular, $\mathscr{C}_0 = \mathrm{div}(\pi)$ is linearly equivalent to 0, where $\pi \in R$ is a uniformiser. Thus $\mathscr{C}_0 \cdot \mathscr{C}_0 = 0$. We now state Castelnuovo's criterion, adapted for arithmetic surfaces, in the case where the residue field k is *algebraically closed*. Note that, if $\mathscr{C}$ is a proper, regular model and $x \in \mathscr{C}_0$ is a closed point, then the blow-up at x: $\varphi : \mathrm{Bl}_x(\mathscr{C}) \to \mathscr{C}$ is also a proper regular model, isomorphic to $\mathscr{C} \setminus \{x\}$ away from a copy of $\mathbb{P}^1_k \subset (\mathrm{Bl}_x(\mathscr{C}))_k$ with self intersection $\mathbb{P}^1_k \cdot \mathbb{P}^1_k = -1$. In general, we say that an irreducible fibral divisor is an *exceptional curve* if it is rational, and has self intersection -1.

Proposition 6.1.8 (Castelnuovo's criterion)**.** *Let R be a discrete valuation ring with fraction field K and algebraically closed residue field k. Let C be a non-singular projective of genus $g \geq 1$.*

i) Let $\mathscr{C}'/R$ be a proper regular model for C and $D \in \mathrm{Div}_f(\mathscr{C}')$ an exceptional curve. Then the contraction:

$$\varphi : \mathscr{C}' \longrightarrow \mathscr{C}$$

of $\mathscr{C}'$ at D exists.

ii) The minimal proper regular model for C/K contains no exceptional curves.

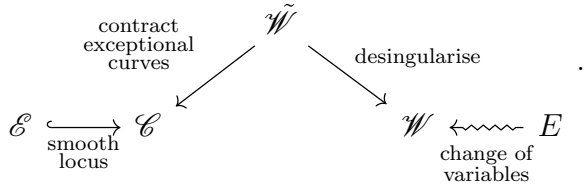
Proof. See [Sil94, IV, §7, Proposition 7.5]. □

Thus, given a non-singular projective curve C/K of genus $g \geq 1$, one may take any proper, normal model $\mathscr{C}/R$ (i.e. clearing denominators of some projective equations and normalising). Then there exists a desingularisation $\tilde{\mathscr{C}} \to \mathscr{C}$ from a finite sequence of blow-ups and the minimal model is obtained by contracting any (-1)-curves.

6.1.3 Kodaira-Néron classification

Let R be a complete DVR with fraction field K and algebraically closed residue field k. Let E/K be an elliptic curve. Recall that the minimal proper regular model $\mathscr{C}$ is obtained as the minimal desingularisation of the minimal Weierstrass model $\mathscr{W}$. Then the Néron model $\mathscr{E}$ of E is the maximal smooth subscheme of $\mathscr{C}$. We sum this up in the following

diagram (adapted from [Liu02, p. 457]):



Independently, Kodaira and Néron classified the possible special fibres of the minimal proper regular model $\mathscr{C}$ of E [Kod63], [Ner64]. We will only discuss the minimal proper regular models $\mathscr{C}$ of elliptic curves $E = \mathscr{C}_K$ with multiplicative reduction.

Remark 6.1.9. If k is a not necessarily algebraically closed field, with an algebraic closure $\bar{k}$, then a *k-torus* $\mathbb{T}$ of *rank* $r > 0$ is any k-group scheme which admits a $\bar{k}$-isomorphism $\mathbb{T}_{\bar{k}} \cong (\mathbb{G}_{m,\bar{k}})^r$. We say that $\mathbb{T}$ is *split* (over k) if there exists a k-rational isomorphism:

$$\mathbb{T} \cong (\mathbb{G}_{m,k})^r.$$

Otherwise, we say that $\mathbb{T}$ is *non-split*. In the classification of Néron-Kodaira, they distinguish between *split multiplicative reduction* and *non-split multiplicative reduction* of the Néron model of an elliptic curve. In what follows, we will keep the assumption that k is algebraically closed and only refer to *multiplicative reduction*.

Definition 6.1.10. Let k be an algebraically closed field and $N > 0$ a positive integer. Let $\mathbb{P}^1_k \times \mathbb{Z}/N\mathbb{Z}$ be N disjoint copies of the projective line. Suppose we make a choice of projective coordinate $z_i = (z, i) \in \mathbb{P}^1_k \times \{i\}$ for each $i \in \mathbb{Z}/N\mathbb{Z}$. The (standard) *Néron N-gon* is the algebraic curve $P_{N,k}$ given by identifying:

$$(\infty, i) \sim (0, i+1) \text{ for each } i \in \mathbb{Z}/N\mathbb{Z}.$$

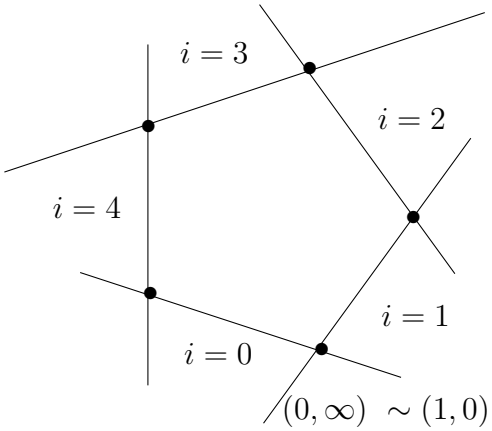
$P_{N,k}$ is of arithmetic genus 1 with trivial dualising sheaf and normalisation $\tilde{P}_{N,k} = \mathbb{P}^1_k \times \mathbb{Z}/N\mathbb{Z}$. Note that we allow the nodal rational curve $P_{1,k}$.

The above definition should really be a proposition. In [Del-Rap72, II, Lemme 1.3], the authors show that any connected, reduced algebraic curve C/k of arithmetic genus one, with at worst nodal singularities, and trivial dualising sheaf ω_C is a Néron N-gon or an elliptic curve.

Example 6.1.11. Let k be an algebraically closed field.

i) The nodal cubic $y^2 + xy = x^3 \subseteq \mathbb{P}^2_k$ is the Néron 1-gon.

ii) We illustrate the Néron 5-gon below:



We are now ready to state the Kodaira-Néron classification for elliptic curves with multiplicative reduction:

Theorem 6.1.12. *Let R be a complete DVR with fraction field K and algebraically closed residue field k. Let E/K be an elliptic curve with minimal proper regular model $\mathscr{C}$ and Néron model $\mathscr{E}$.*

i) If E has good reduction, then $\mathscr{E} = \mathscr{C}$ and $\mathscr{C}_k$ is an elliptic curve. We denote this reduction type by I_0.

ii) If E has (split) multiplicative reduction then $\mathscr{C}_k \cong P_{N,k}$ is a Néron N-gon where $N = -v(j(E))$. We denote this reduction type by I_N.

In case (ii), $\mathscr{C}_k$ has N nodes and $\mathscr{E}_k \cong \mathbb{G}_{m,k} \times \mathbb{Z}/N\mathbb{Z}$.

Proof. See [Sil94, IV, §8, Theorem 8.2]. □

6.1.4 Tate curves

Our main reference for Tate curves is [Ser97, Appendix A.1]. Let K be a field, complete with respect to a discrete valuation v. Let R denote the corresponding valuation ring and k the residue field. Given any *Tate parameter* $q \in K^*$ such that $v(q) > 0$, we have the associated *Tate curve*:

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where we define the power series:

$$\begin{aligned} s_k(q) &= \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n}, \quad (k \geq 1); \\ a_4(q) &= -5s_3(q); \\ a_6(q) &= -\left(\frac{5s_3(q) + 7s_5(q)}{12}\right); \end{aligned}$$

which converge with respect to v. E_q is then an elliptic curve in Weierstrass form. Note that the j-invariant is given by the convergent power series:

$$j(q) = \frac{(1+48a_4(q))^3}{q\prod(1-q^n)^{24}} = \frac{1}{q} + 744 + 1964884q + ...$$

so that $v(q) = -v(j(E_q))$. By considering valuations, the coefficients of E_q are integral. Moreover, the reduction mod v is given by the nodal cubic with singular point $(0,0)$:

$$\tilde{E_q} : y^2 + xy = x^3.$$

The fundamental observation of Tate was that *any* elliptic curve E/K with split multiplicative reduction could be expressed as a Tate curve (up to isomorphism) for a *unique* Tate parameter $q \in K^*$:

Proposition 6.1.13. *Let K be a field complete with respect to a discrete valuation v. Suppose that E/K is an elliptic curve with split multiplicative reduction mod v. Then there exists a unique element $q \in K^*$ with $v(q) > 0$ such that:*

$$E \cong E_q;$$

via a K-rational isomorphism.

Proof. See [Sil94, V, Theorem 3.1]. □

In the classical setting, one often defines an elliptic curve over the complex numbers as a 1-dimensional complex torus $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau \subseteq (\mathbb{C},+)$ is a free abelian subgroup of rank 2. Such a complex torus is shown to be algebraic by defining a closed embedding into $\mathbb{CP}^2$ using the Weierstrass $\wp$-function. This perspective is important as it realises $\mathbb{C}$ as the universal cover, and holomorphic functions on $\mathbb{C}/\Lambda$ are equivalent to Λ-periodic functions on $\mathbb{C}$. On the other hand, if K is a non-Archimedean field, then $(K,+)$ admits no non-trivial free subgroups, and so one cannot hope to uniformise an elliptic curve E/K with K. Considering the exponential exact sequence:

$$1 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{C} \longrightarrow \mathbb{C}^* \longrightarrow 1,$$

one can show that $\mathbb{C}/\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\tau$ is biholomorphic to $\mathbb{C}^*/s^{\mathbb{Z}}$ for the complex parameter $s = \exp(2\pi i\tau)$. The upshot of this approach is that there are many discrete subgroups of $(K^*,\times)$ for a non-Archimedean field K, and in fact, there is at least an analytic uniformisation of Tate curves:

Theorem 6.1.14. *Let K be a field complete with respect to a discrete valuation v. Let $q \in K^*$ be a parameter with $v(q) > 0$ and denote by E_q/K the corresponding Tate curve.*

Let $\bar{K}$ be an algebraic closure of K and set $G_K = \mathrm{Gal}(\bar{K}/K)$. Then there is a surjective group homomorphism:

$$\phi : \bar{K}^* \longrightarrow E_q(\bar{K});$$
$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & u \notin q^{\mathbb{Z}} \\ e & u \in q^{\mathbb{Z}} \end{cases}$$

where X and Y are convergent power series (with respect to the unique extension of v to $\bar{K}$) for $u \notin q^{\mathbb{Z}}$ given by:

$$X(u,q) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q);$$
$$Y(u,q) = \sum_{n \in \mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q).$$

The kernel of this homomorphism is $q^{\mathbb{Z}}$ and, moreover, it is G_K-equivariant.

Proof. See [Sil94, V, Theorem 3.1]. □

This perspective makes it very easy to understand the torsion subgroups $E_q[m](\bar{K})$ as Galois modules. Indeed, given a point $x \in \bar{K}^*$ we write $[x] \in \bar{K}^*/q^{\mathbb{Z}}$ for its image in the quotient. Then it is clear that the m-torsion subgroup is given by:

$$\{[\zeta_m^i \cdot q^{\frac{j}{m}}] \mid 0 \leq i, j < m\};$$

where $\zeta_m \in \bar{K}$ is a primitive m-th root of unity and $q^{\frac{1}{m}}$ is an m-th root of q. As the uniformisation map is G_K-equivariant, we have the following:

Proposition 6.1.15. *Let K be a field complete with respect to a discrete valuation v. Let $q \in K^*$ be a parameter with $v(q) > 0$ and denote by E_q/K the corresponding Tate curve. Let $\bar{K}$ be an algebraic closure of K and set $G_K = \mathrm{Gal}(\bar{K}/K)$. Suppose that $m > 0$ is an integer. Then there is an exact sequence of Galois modules:*

$$0 \longrightarrow \mu_m(\bar{K}) \longrightarrow E_q[m](\bar{K}) \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$

Moreover, the above sequence splits if and only if $q^{\frac{1}{m}} \in K$.

Proof. See [Ser97, A.1.2]. □

Recall that isogenous abelian varieties share the same reduction type. Isogenies between Tate curves can be read off easily from their uniformisations. We say that two Tate parameters $q, q' \in K^*$ are *multiplicatively associated* if there exist positive integers $A, B > 0$ such that:

$$q^A = (q')^B$$

Theorem 6.1.16. *Let K be a field complete with respect to a discrete valuation v. Suppose that $q, q' \in K^*$ are parameters with $v(q), v(q') > 0$. Then the corresponding Tate curves are isogenous if and only if q and q' are multiplicatively associated.*

Proof. See [Ser97, A.1.4 Theorem]. □

Again, this statement can be seen more clearly by working with uniformisations. Let E_q be a Tate curve and $A > 0$ an integer. Then the multiplication by A map admits a factorisation:

$$[A] : E_q \longrightarrow E_{q^A} \longrightarrow E_q;$$

which on uniformisations corresponds to:

$$\bar{K}^*/q^{\mathbb{Z}} \longrightarrow \bar{K}^*/q^{A\cdot\mathbb{Z}} \longrightarrow \bar{K}^*/q^{\mathbb{Z}};$$

where the first morphism is induced by $x \mapsto x^A$ on $\bar{K}^*$ and the second is induced by the identity. This describes an isogeny $E_q \to E_{q^A}$.

6.2 Semistable reduction and Grothendieck's orthogonality theorem

We describe the Semistable Reduction Theorem for abelian varieties as proved by Grothendieck [SGA7]. Grothendieck goes further to prove an analogue of the Néron-Ogg-Shafaverich to determine when an abelian variety over a local field has semistable reduction in terms of the action of inertia on the l-adic Tate module [ibid.]. Much of the exposition of Grothendieck's orthogonality theorem and semistable reduction criterion has been taken from [Con22].

6.2.1 Semistable reduction theorem

Let k be an algebraically closed field. A *semiabelian* variety A/k is a connected k-group scheme that fits into an exact sequence:

$$1 \longrightarrow T \longrightarrow A \longrightarrow B \longrightarrow 0;$$

where T is a torus i.e. admits an isomorphism $T \cong \mathbb{G}_{m,k}^r$ for some $r > 0$ and B is an abelian variety. This motivates the following definition:

Definition 6.2.1. Let R be a DVR with algebraically closed residue field k and fraction field K. We say that an abelian variety A/K has *semistable* reduction if $\mathscr{A}_k^\circ$ is a semiabelian variety where $\mathscr{A}/R$ is the Néron model of A and $\mathscr{A}_k^\circ \subseteq \mathscr{A}_k$ is the connected component of the identity.

In this case, we denote by $\Phi = \mathscr{A}_k/\mathscr{A}_k^\circ$ the group of connected components. Note that Φ is finite étale even when k has positive characteristic.

Example 6.2.2. An elliptic curve E/K has semistable reduction if and only if it has reduction type I_N for $N \geq 0$. Let $\mathscr{E}/R$ denote the Néron model of E and suppose that $N > 0$. Then $\mathscr{E}_k^\circ \cong \mathbb{G}_{m,k}$ and there is a split exact sequence:

$$1 \longrightarrow \mathbb{G}_{m,k} \longrightarrow \mathscr{E}_k \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow 0$$

Let R be a discrete valuation ring with residue field k and fraction field K. Suppose that A/K is an abelian variety. We say that A has *potentially good reduction* (resp. *potentially semistable reduction*) if there exists a finite separable extension $K' \supseteq K$ such that $A_{K'}$ has good reduction (resp. semistable reduction).

Theorem 6.2.3 (Semistable Reduction Theorem)**.** *Let R be a discrete valuation ring with residue field k and fraction field K. Suppose that A/K is an abelian variety. Then A/K has potentially semistable reduction.*

Proof. [SGA7, Théorème 3.6, p. 351] □

Proposition 6.2.4. *Let $f : A \to B$ be an isogeny of abelian varieties over a local field K. Then A has semistable reduction if and only if B has semistable reduction.*

Proof. See [Con22, Prop. 4.1] □

Remark 6.2.5. The formation of the Néron model $\mathscr{A}/R$ of A/K has a nice compatibility with étale base change [BLR-12, Prop. 2 (c) p. 13]. Namely, let $R \subseteq R'$ be a flat, unramified extension. Let $K \subseteq K'$ be the corresponding extension of fraction fields. Then the Néron model of $A_{K'}$ is given by $\mathscr{A}_{R'}$. In particular, if A does not acquire semistable reduction over K, then the extension K'/K from the Semistable Reduction Theorem is necessarily ramified.

6.2.2 Grothendieck's orthogonality theorem

In analogy to the Néron-Ogg-Shafarevich criterion (cf. Thm. 3.7.1), there is an inertial criterion on the l-adic Tate modules for determining when A has semistable reduction due to Grothendieck. Suppose that A has semistable reduction and let $\mathscr{A}/R$ denote the Néron model. Then there is an exact sequence of k-group schemes:

$$1 \longrightarrow T \longrightarrow \mathscr{A}_k^\circ \longrightarrow B \longrightarrow 0;$$

where T is a torus and B is an abelian variety. Write $h = \dim(B)$ and $r = \operatorname{rank}(T)$ so that, if $g = \dim(A)$, then $g = h + r$. Let $n > 0$ be an integer and consider the multiplication-by-n

morphism:

$$[n]_{\mathscr{A}} : \mathscr{A} \longrightarrow \mathscr{A}$$

We would like to apply our study of finite flat group schemes to the kernel $\mathscr{A}[n]$ but unfortunately, if A has bad reduction, then in general $[n]_{\mathscr{A}}$ fails to be finite. An easy way to see this is the following criterion of Deligne [Del-Rap72, Lemme 1.19]. Recall that a morphism of schemes $f : X \to S$ is *quasi-finite* if it is locally of finite type and every fibre $f^{-1}(s)$ of a closed point $s \in S$ is a finite set.

Lemma 6.2.6. *Let $f : X \to S$ be a quasi-finite, separated, flat morphism. If the rank of the fibres of f is constant, then it is finite.*

By the semiabelian hypothesis, $[n]_{\mathscr{A}}$ is flat and quasi-finite. However, in general, the rank of $\mathscr{A}_k[n]$ will be lower than that of the generic fibre $A[n]$. Indeed, by the exact sequence above, the rank of $\mathscr{A}_k^\circ[n]$ is n^{r+2h} whereas the rank of $A[n]$ is of course $n^{2g} = n^{2r+2h}$. Thus, as Φ is a finite étale group scheme, if n does not divide the rank of Φ, then the rank of $\mathscr{A}[n]$ drops after specialisation, and so $\mathscr{A}[n]$ is not finite.

Example 6.2.7. Let E/K be an elliptic curve with I_N-reduction and let $\mathscr{E}/R$ be the Néron model. Let $n > 0$ be an integer. Then $\mathscr{E}[n]$ is finite if and only if $n \mid N$. Indeed if $\gcd(N, n) = 1$ then it is easy to see that $\mathscr{E}_k^\circ[n] \cong \mathbb{G}_{m,k}[n]$ is of rank n, whereas the rank of $E[n]$ is n^2.

The upshot of this is that there is always a largest finite subscheme $\mathscr{A}[n]_f \subseteq \mathscr{A}[n]$ which is in fact a subgroup. This is essentially a consequence of Zariski's Main Theorem:

Theorem 6.2.8 (Zariski's Main Theorem)**.** *Let $f : X \to S$ be a quasi-finite, separated morphism of noetherian schemes. Then there is a factorisation:*

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & S \\ & {\scriptstyle j}\searrow \quad \nearrow{\scriptstyle g} & \\ & \bar{X} & \end{array}$$

into an open immersion $j : X \hookrightarrow \bar{X}$ into some finite S-scheme $\bar{X}$.

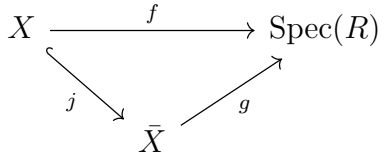
Proof. See [EGA, IV, 8.12.6]. □

Corollary 6.2.9. *Let $f : X \to \mathrm{Spec}(R)$ be a quasi-finite, separated morphism where R is a henselian local ring with residue field k. Then there is a unique decomposition:*

$$X = X_f \sqcup X';$$

where $X_f \to \mathrm{Spec}(R)$ is finite and $(X')_k = \emptyset$. Moreover, the assignment $X \mapsto X_f$ is functorial and commutes with products. In particular, if X is an R-group scheme then X_f is a subgroup scheme.

Proof. We sketch the construction of X_f. See [Con22, Thm. 4.10] for the uniqueness, functoriality and compatibility with products. By Zariski's main theorem there is diagram:



where $X \hookrightarrow \bar{X}$ is an open immersion into a finite R-scheme. As R is henselian, there is a decomposition $\bar{X} = \bigsqcup_i \mathrm{Spec}(R_i)$ where R_i are finite, local R-algebras. Thus we may write $X = \bigsqcup_i X_i$ where either $X_i = \mathrm{Spec}(R_i)$ or $(X_i)_k = \emptyset$. We then set X_f to be the disjoint union of the former components, and X' to be the disjoint union of the latter. □

Let $\mathscr{A}[n]_f \subseteq \mathscr{A}[n]$ denote the finite part of the n-torsion of the Néron model $\mathscr{A}$. As noted, this is a finite flat R-group scheme.

Remark 6.2.10. Suppose that R is a complete DVR with algebraically closured residue field k of characteristic $p > 0$ and let K denote the fraction field of R with algebraic closure $\bar{K}$. Suppose that n is coprime to p. Then $\mathscr{A}[n]_f$ is a finite flat étale group scheme. As k is algebraically closed, $\mathscr{A}[n]_f$ is a constant R-group scheme. By construction of the 'finite part' we have that $\mathscr{A}[n]_f(R) = \mathscr{A}[n](R)$ and so by the Néron Mapping Property $\mathscr{A}[n]_f(K) = \mathscr{A}[n](K) = \mathscr{A}[n](\bar{K})^{I_K}$. Thus, we see that $\mathscr{A}[n]_f$ is the 'inertial fixed part' of $\mathscr{A}[n]$.

Let $\mathscr{A}_k[n]_t := \mathrm{Im}(T[n] \hookrightarrow \mathscr{A}_k^\circ[n])$ denote the *toric part* of the torsion. We have the following filtration of k-group schemes:

$$\mathscr{A}_k[n]_t \subseteq \mathscr{A}_k[n]_f^\circ \subseteq \mathscr{A}_k[n]_f.$$

As $\mathscr{A}_k[n]_t$ is a multiplicative group scheme and $\mathscr{A}_k[n]_f^\circ$ is the connected component, this filtration lifts uniquely to R:

$$\mathscr{A}[n]_t \subseteq \mathscr{A}[n]_f^\circ \subseteq \mathscr{A}[n]_f$$

(cf. Def. 3.2.19). Taking the limit of the above over l^n for $n > 0$ on $\bar{K}$-points, we obtain the corresponding filtration for l-adic Tate modules. This forms the context for Grothendieck's inertial criterion on semistable reduction:

Lemma 6.2.11. *Let R be a henselian DVR with fraction field K of characteristic 0 and residue field k of characteristic $p > 0$. Let A/K be an abelian variety with semistable reduction and $\mathscr{A}/R$ its Néron model. Let $l \neq p$ be a prime. Then there is a filtration of G_K-equivariant $\mathbb{Z}_l$-submodules:*

$$T_l(A)_t \subseteq T_l(A)_f \subseteq T_l(A).$$

Moreover, $T_l(A)^{I_K} = T_l(A)_f$ where $I_K \subseteq G_K$ is the inertia subgroup.

This follows from Remark 6.2.10. Let $A^\vee$ denote the dual abelian variety. Then $A^\vee$ also has semistable reduction (cf. Prop. 6.2.4) and there is an analogous filtration of $T_l(A^\vee)$. Let:

$$\mu_{l^\infty} : T_l(A) \times T_l(A^\vee) \longrightarrow \mathbb{Z}_l(1)$$

denote the l-adic Weil pairing.

Theorem 6.2.12 (Orthogonality theorem)**.** *Let R be a henselian DVR with fraction field K of characteristic 0 and residue field k of characteristic $p > 0$. Let A/K be an abelian variety and $\mathscr{A}/R$ its Néron model. Let $l \neq p$ be a prime. If A has semistable reduction then, under the l-adic Weil pairing, the orthogonal complement of $T_l(A)_f$ is $T_l(A^\vee)_t$. In particular, we may pick a complement:*

$$T_l(A) = T_l(A)_f \oplus U$$

as $\mathbb{Z}_l$-modules. Then $U \cong T_l(A)/T_l(A)_f$ is Cartier dual to $T_l(A^\vee)_t$ and so both U and $T_l(A)_f$ are I_K-trivial modules.

Proof. See [SGA7, Exp. IX, 2.4, 5.2]. □

Thus, if we pick a $\mathbb{Z}_l$-basis of $T_l(A)_f$ and extend it to $T_l(A)$, then the image of the inertia representation $\rho_{l^\infty} : I_K \longrightarrow \mathrm{Aut}(T_l(A)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_l)$ is represented by block matrices of the form:

$$\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}.$$

In particular, for each $\sigma \in I_K$ we have that $(\sigma - 1)^2 = 0$ i.e. the representation ρ_{l^∞} is *unipotent* of *height* at most 2. Like the Néron-Ogg-Shafarevich criterion, the converse also holds:

Theorem 6.2.13 (Inertial criterion for semistable reduction)**.** *Let R be a henselian DVR with fraction field K of characteristic 0 and residue field k of characteristic $p > 0$. Let A/K be an abelian variety and $l \neq p$ be a prime. Then A has semistable reduction if and only if the inertia group I_K acts unipotently of height at most 2 on $T_l(A)$.*

Proof. See [SGA7, Exp. IX, 3.5]. □

Let K be a complete local field of characteristic 0 and residue characteristic $p > 0$. Recall that if E/K is an elliptic curve with multiplicative reduction then it is isomorphic to a Tate curve, for each $n > 0$, the l^n-torsion is given by the exact sequence:

$$0 \longrightarrow \mu_{l^n}(\bar{K}) \longrightarrow E_q[l^n](\bar{K}) \longrightarrow \mathbb{Z}/l^n\mathbb{Z} \longrightarrow 0$$

(cf. Prop. 6.1.15). If $l \neq p$, then we see that I_K acts trivially on $\mu_{l^n}(\bar{K})$ and so the representation on $T_l(E)$ is indeed unipotent of height at most 2.

6.2.3 Deligne-Rapoport generalised elliptic curves

For completeness, we introduce Deligne and Rapoport's notion of *generalised elliptic curves* [Del-Rap72].

Definition 6.2.14. Let S be a connected scheme. A *stable genus* 1 *curve* over S is a morphism $f : \mathscr{C} \longrightarrow S$ with each geometric fibre a proper, smooth and connected curve of genus 1, or a Néron polygon (cf. Def. 6.1.10).

Let $C = P_{N,k}$ be the Néron N-gon over an algebraically closed field k. Recall that the normalisation is given by $\tilde{C} = \mathbb{P}^1_k \times \mathbb{Z}/N\mathbb{Z}$ and the non-singular locus of C is given by $C^{\mathrm{reg}} = \mathbb{G}_{m,k} \times \mathbb{Z}/N\mathbb{Z}$. There is a natural action:

$$C^{\mathrm{reg}} \times \tilde{C} \longrightarrow \tilde{C};$$
$$((z,i),(w,j)) \longmapsto (z \cdot w, i+j)$$

that descends to a well-defined action $C^{\mathrm{reg}} \times C \to C$.

Definition 6.2.15. Let S be a connected scheme. A *generalised elliptic curve* over S is a triple $(\mathscr{C}, +, e)$ where $f : \mathscr{C} \to S$ is a stable genus 1 curve, $+ : \mathscr{C}^{\mathrm{sm}} \times \mathscr{C} \to \mathscr{C}$ a morphism and $e : S \to \mathscr{C}$ a section satisfying:

i) The restriction of $+$ to $\mathscr{C}^{\mathrm{reg}}$ makes $\mathscr{C}^{\mathrm{reg}}$ an S-group scheme with identity section e.

ii) The morphism $+$ defines an S-group scheme action.

iii) For each geometric point $\bar{s} \in S$ such that $\mathscr{C}_{\bar{s}}$ is singular, the action $+$ over $\bar{s}$ acts by rotations on the *dual graph* $\Gamma(\mathscr{C}_{\bar{s}})$ (i.e. the graph whose vertices correspond to components of $\mathscr{C}_{\bar{s}}$ and whose edges correspond to intersections of components).

Let $(\mathscr{C}, +, e)$ be a generalised elliptic curve over S and let $\bar{s}$ be a closed point with residue field k. Note that the multiplication map $[n] : \mathscr{C}^{\mathrm{sm}} \longrightarrow \mathscr{C}^{\mathrm{sm}}$ is flat over S, but not in general finite by Lemma 6.2.6. Suppose that $C = \mathscr{C}_{\bar{s}}$ is a Néron N-gon. Then, given an integer $n > 0$ we have that $C^{\mathrm{reg}}[n] \cong \mu_n \times \mathbb{Z}/\gcd(n,N)\mathbb{Z}$. In view of Deligne's characterisation of finiteness (cf. Lemma 6.2.6), we have the following easy Corollary:

Corollary 6.2.16. *Let $f : \mathscr{C} \to S$ be a generalised elliptic curve over S and let $n > 0$ be an integer. Suppose that for each geometric point $\bar{s} \in S$, we have that $\mathscr{C}_{\bar{s}}$ is non-singular, or a Néron N-gon with $n \mid N$. Then $\mathscr{C}^{\mathrm{sm}}[n]$ is a finite flat S-group scheme with rank n^2.*

Chapter 7

Logarithmic geometry

Logarithmic geometry was introduced by Fontaine and Illusie with the idea of studying crystalline cohomology in semistable families, however, Kato was responsible for putting many of the ideas in a concrete and general framework [K.Kat19]. Our main references for the study of logarithmic geometry will be [Gr11], [Og18] and [K.Kat94].

Let k be an algebraically closed field and X a variety over k of dimension n. If X is non-singular, then for each closed point $p \in X$ we have that $\mathscr{O}_{X,p}$ is regular i.e. there exists *local coordinates* $t_1, .., t_n \in \mathscr{O}_{X,p}$ that generate the maximal ideal $\mathfrak{m}_{X,p}$. We can equivalently characterise when X is singular in terms of the sheaf of Kähler differentials:

Theorem 7.0.1. *Let X be a variety over an algebraically closed field k. Then X is non-singular if and only if the sheaf of (relative) Kähler differentials $\Omega_{X/k}$ is locally free of rank $n = \dim(X)$.*

Proof. See [Har13, Theorem 8.15]. □

When X is singular, the sheaf of differential forms $\Omega^1_{X/k}$ fails to be locally free of constant rank. However, there is an important class of singularities called *strict normal crossings* which allow for a well-defined notion of *logarithmic forms*.

Definition 7.0.2. Let X be a non-singular variety over an algebraically closed field k. Let D be a reduced, Cartier divisor. We say that D has *strict normal crossings* or is a *strict normal crossings divisor*, if for some regular local coordinates $x_1, ..., x_n$ of X, D is given by the equation $x_1 \cdot ... \cdot x_r = 0$ for some $1 \leq r \leq n$.

Suppose that $\mathrm{char}(k) = 0$ and that X is non-singular and quasi-projective. Then, taking the closure in some projective space, we obtain a projective variety $\bar{X}$ with (possibly non-empty) singular locus supported within a proper subvariety $Z = \bar{X} \setminus X$. The relevance of strict normal crossings is seen by (the weak version of) Hironaka's theorem. Namely, there is a resolution of singularities $\pi : \tilde{X} \to \bar{X}$ centred in D such that $\pi^{-1}(Z)$ is a strict normal crossings divisor [Bog-Pan96].

So assume that X is non-singular, $\bar{X}$ is projective, $D = \bar{X} \setminus X$ is a strict normal crossings divisor and let $i : X \hookrightarrow \bar{X}$ denote the open immersion given by inclusion. We define the sheaf of *log differentials* $\Omega^1_{\bar{X}}(\log D) \subseteq i_*\Omega^1_X$ to be the subsheaf locally generated by differentials of the form:

$$\frac{dx_1}{x_1}, ..., \frac{dx_r}{x_r}, dx_{r+1}, ..., dx_n$$

where $x_1, ..., x_n$ are regular local coordinates and $n = \dim(X)$. The differentials of the form $\frac{dx_i}{x_i}$ are referred to as *logarithmic forms* or forms with at worst *logarithmic poles*, where a hypothetical 'log' regular function $\log(x_i)$ would have differential $d(\log(x_i)) = \frac{dx_i}{x_i}$. Importantly, the sheaf of log differential forms can be used to give information about the open subscheme X. For example, Deligne was able to compute the (singular) cohomology groups of a quasi-projective variety $X/\mathbb{C}$ by working with log differential forms on the projective variety $\bar{X}$:

$$\mathbb{H}^i(\bar{X}, \Omega^\bullet_{\bar{X}}(\log D)) \cong H^i(X, \mathbb{C})$$

where $\Omega^\bullet_{\bar{X}}(\log D) = \bigwedge^\bullet \Omega^1_{\bar{X}}(\log D)$ and $\mathbb{H}^i$ denotes hypercohomology [Del06]. Let S be a connected scheme. More generally, a morphism of schemes $f : \mathscr{X} \to S$ of locally finite presentation is *smooth* if and only if it is flat and the sheaf of relative differentials $\Omega^1_{\mathscr{X}/S}$ is locally free of rank equal to the *relative dimension* of X/S [EGA, IV, 16.10.2]. Informally, a flat family of non-singular schemes will give rise to a smooth morphism. Working over an algebraically closed field k, suppose that f is a morphism of k-schemes, and that S is a non-singular, geometrically connected and dimension one scheme. Suppose additionally that, for a fixed closed point $0 \in S$, the fibre $\mathscr{X}_0 \subseteq \mathscr{X}$ is a strict normal crossings divisor, and that for every closed point $s \neq 0$ we have that $\mathscr{X}_s$ is non-singular. Recall that there is an exact sequence:

$$f^*\Omega^1_{S/k} \longrightarrow \Omega^1_{\mathscr{X}/k} \longrightarrow \Omega^1_{\mathscr{X}/S} \longrightarrow 0$$

[Har13, Prop. 8.11]. We define the sheaf of *relative log differentials* of $f : \mathscr{X} \to S$ by:

$$\Omega^1_{\mathscr{X}/S}(\log \mathscr{X}_0) = \Omega^1_{\mathscr{X}/k}(\log \mathscr{X}_0)/f^*\Omega^1_{S/k}(\log\{0\}).$$

Importantly, even though f fails to be smooth and so $\Omega^1_{\mathscr{X}/S}$ cannot be free of rank $\dim(\mathscr{X}) - 1$, one can check that the sheaf of relative log differentials satisfies this property. Let $j : \mathscr{X}_0 \hookrightarrow \mathscr{X}$ denote the natural closed immersion. Then moreover, the pullback $j^*\Omega^1_{\mathscr{X}/S}(\log \mathscr{X}_0)$ is a locally free sheaf of rank $\dim(\mathscr{X}_0)$ even though $\mathscr{X}_0$ is singular. As we will see, $\mathscr{X}_0$ is a *log smooth* scheme (in an appropriate sense), allowing one to make analogous statements about $\mathscr{X}_0$ that would hold for a smooth scheme.

Both of these examples can be viewed in the framework of *Iitaka's philosophy*; that any statement about a smooth variety X involving the sheaf of differentials Ω^1_X should find its counterpart for pairs (X, D) where X is a smooth variety and D a strict normal

crossings divisor using the sheaf of log differentials $\Omega^1_X(\log D)$ [Mat13, p. 110].

7.1 Toric geometry and monoids

7.1.1 Toric geometry

Kato's original definition of a logarithmic scheme was one that is étale-locally *toric*. For this statement to be well defined, one needs a notion of *toric scheme* which does not depend on a base ring. We first discuss toric varieties over an algebraically closed field k of characteristic 0. We can then generalise from toric varieties over k to toric schemes. Our main reference will be [Ful93] with some auxiliary results from [CLS-24].

Definition 7.1.1. Let k be an algebraically closed field of characteristic 0. A *toric variety* X is a normal variety with a dense open subset $T \subseteq X$ isomorphic to a torus $T \cong \mathbb{G}^r_{m,k}$ such that multiplication $T \times T \to T$ extends to an action:

$$T \times X \longrightarrow X.$$

Note that all toric varieties are rational, the simplest examples being $\mathbb{G}^r_{m,k} \subseteq \mathbb{A}^r_k \subseteq \mathbb{P}^r_k$. Consider the character lattice of T:

$$M = \mathrm{Hom}(\mathbb{G}^r_{m,k}, \mathbb{G}_{m,k}).$$

This is a free abelian group of rank r. Dually, we have the lattice of 1-parameter subgroups:

$$N = \mathrm{Hom}(\mathbb{G}_{m,k}, \mathbb{G}^r_{m,k}).$$

These lattices are dual under the perfect bilinear pairing:

$$\langle -, - \rangle : M \times N \longrightarrow \mathbb{Z} \quad \text{where} \quad \langle \chi, \lambda \rangle = \chi(\lambda(1)).$$

Definition 7.1.2. Let M be a lattice of rank r, $N = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ the dual lattice and $\langle -, - \rangle : M \times N \to \mathbb{Z}$ the bilinear pairing $\langle v, u \rangle = u(v)$. Let $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$ and $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}$. A *cone* $\sigma \subseteq N_{\mathbb{R}}$ is any subset of the form:

$$\sigma = \mathrm{Cone}(u_1, ..., u_s) = \{a_1 u_1 + ... + a_s u_s \mid a_1, ..., a_s \geq 0\}$$

for a finite subset $\{u_1, ..., u_s\} \subseteq N_{\mathbb{R}}$. Any such subset that produces the same cone is a generating set. We say that σ is *rational* if there exists a generating set of lattice points in N. Note that $\langle -, - \rangle$ extends uniquely to $M_{\mathbb{R}} \times N_{\mathbb{R}}$. The *dual cone* $\sigma^\vee \subseteq N_{\mathbb{R}}$ is given by:

$$\sigma^\vee = \{v \in M_{\mathbb{R}} \mid \langle v, u \rangle \geq 0 \text{ for all } u \in \sigma\}.$$

Given $v \in \sigma^\vee$, we define the *supporting hyperplane* H_v to be the orthogonal complement:

$$H_v = \langle v \rangle^\perp = \{u \in N_\mathbb{R} \mid \langle v, u \rangle = 0\}.$$

A *face* τ of σ is the intersection $\tau = H_v \cap \sigma$ of σ with a supporting hyperplane. We use the symbol $\tau \preceq \sigma$ to denote a face. We say that σ is *strongly convex* if $\{0\} \preceq \sigma$. Let $e_1, ..., e_r \in M$ be a $\mathbb{Z}$-basis. Write $k[M]$ for the polynomial algebra generated by the characters χ^m for $m \in M$, over k, with the relation:

$$\chi^m \cdot \chi^{m'} = \chi^{m+m'}$$

for each $m, m' \in M$. Then if $t_i = \chi^{e_i}$ it is clear that $k[M] \cong k[t_1^{\pm 1}, ..., t_r^{\pm 1}]$. Similarly, given a rational cone $\sigma \subseteq N_\mathbb{R}$ we can associate a k-algebra $k[\sigma^\vee \cap M]$. Importantly, for a strictly convex rational cone, this is a finitely generated k-algebra:

Lemma 7.1.3 (Gordon's lemma)**.** *Let M be a lattice of finite rank with dual lattice N. Suppose that $\sigma \subseteq N_\mathbb{R}$ is a strictly convex rational polyhedral cone. Then the k-algebra $k[\sigma^\vee \cap M]$ is finitely generated.*

Proof. See [Ful93, p. 18 Prop. 1]. □

Definition 7.1.4. Let k be an algebraically closed field. An *affine toric variety* X_σ is the spectrum of a k-algebra $k[\sigma^\vee \cap M]$ where $\sigma \subseteq N_\mathbb{R}$ is a strictly convex rational polyhedral cone, M is a lattice of finite rank and $N = M^\vee$ is the dual lattice.

Gordon's lemma ensures that X_σ is a finite type k-scheme. Note that, if $\tau \preceq \sigma$ is a face corresponding to the supporting hyperplane H_v for $v \in \sigma^\vee$, then we obtain the expression:

$$k[\tau^\vee \cap M] = k[\sigma^\vee \cap M] + \mathbb{N} \cdot (-v)$$

and X_τ is the localisation of χ^v in X_σ; in particular, it is open [Ful93, p. 18 Lemma]. Thus, if σ is strongly convex then $\{0\} \preceq \sigma$ and we obtain a torus embedding $\mathbb{G}_{m,k}^r \hookrightarrow X_\sigma$.

Constructing toric varieties from fans

Of course, one would like to define toric varieties that aren't necessarily affine, still using combinatorial data. This requires a way to 'glue' affine toric varieties, such that the result is still toric.

Definition 7.1.5. Let N be a lattice. A *fan* Σ in N is a collection of strongly convex rational polyhedral cones σ in $N_\mathbb{R}$ satisfying the following:

i) Any face $\tau \preceq \sigma$ lies in Σ.

ii) If $\sigma_1, \sigma_2 \in \Sigma$ then $\sigma_1 \cap \sigma_2$ is a face of both.

To every fan Σ in a lattice N, we can associate a normal toric variety X_Σ. Specifically, for each $\sigma \in \Sigma$ we have an affine toric variety X_σ. Then, X_Σ is the scheme obtained by gluing each pair of affine schemes X_{σ_1} and X_{σ_2} by noting that $\sigma_1 \cap \sigma_2$ is a face of both σ_1 and σ_2 and so we glue along the open subscheme $X_{\sigma_1 \cap \sigma_2}$.

Suppose that N_1 and N_2 are lattices and T is a lattice homomorphism $T : N_1 \to N_2$ (i.e. a $\mathbb{Z}$-linear map). Let Σ_1 and Σ_2 be fans in N_1 and N_2 respectively. We say that T is a *morphism of fans* if, for all $\sigma_1 \in \Sigma_1$ there exists $\sigma_2 \in \Sigma_2$ such that $T_\mathbb{R}(\sigma_1) \subseteq \sigma_2$ where:

$$T_\mathbb{R} : M_\mathbb{R} \longrightarrow N_\mathbb{R}$$

is the induced $\mathbb{R}$-linear map. Let X_{Σ_1} and X_{Σ_2} denote the corresponding toric varieties. Then there is an induced morphism:

$$f : X_{\Sigma_1} \longrightarrow X_{\Sigma_2};$$

where the restriction $T_\mathbb{R} : \sigma_1 \to \sigma_2$ corresponds to a morphism of k-algebras $k[\sigma_2^\vee \cap M_2] \to k[\sigma_1^\vee \cap M_1]$ which in turn corresponds to a morphism of affine schemes $X_{\sigma_1} \to X_{\sigma_2}$. One can check that these morphisms glue compatibly. On the other hand, there is another special class of morphisms $f : X_1 \to X_2$ of toric varieties. Let T_1 and T_2 denote the respective tori of X_1 and X_2. We say that a morphism $f : X_1 \to X_2$ is *torus equivariant* if it fits into the following commutative diagram:

$$\begin{array}{ccc} T_1 \times X_1 & \longrightarrow & X_1 \\ {\scriptstyle f|_{T_1} \times f}\downarrow & & \downarrow{\scriptstyle f} \\ T_2 \times X_2 & \longrightarrow & X_2 \end{array}$$

where the horizontal arrows are given by the respective torus actions. In other words, f is compatible with the torus actions of X_1 and X_2.

Lemma 7.1.6. *Let Σ_1 and Σ_2 be fans in lattices N_1 and N_2 respectively, and let X_{Σ_1} and X_{Σ_2} denote the corresponding toric varieties. Then a morphism $f : X_{\Sigma_1} \to X_{\Sigma_2}$ is torus equivariant if and only if it is induced by a morphism of fans $\Sigma_1 \to \Sigma_2$.*

Proof. See [CLS-24, Prop. 1.3.14]. □

Such a morphism of toric varieties will be referred to as a *toric morphism*.

Toric surface singularities

Let $N = \mathbb{Z}^2$ with basis e_1, e_2. Let X_σ/k be an affine toric surface given by a cone $\sigma \subseteq \mathbb{R}^2$. After a change of basis, we may assume σ is of the form:

$$\sigma = \mathrm{Cone}(e_2, re_1 - ae_2) \subseteq \mathbb{R}^2;$$

where $0 \leq a < r$ are coprime [CLS-24, Prop. 10.1.1]. Write $u_1 = e_2$ and $u_2 = re_1 - ae_2$ and let $N' \subseteq N$ be the sublattice generated by these lattice point. Note that:

$$N' = \mathbb{Z}e_2 \oplus \mathbb{Z}(re_1 - ae_2) = r\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$$

so that the quotient is given by $G = N/N' \cong \mathbb{Z}/r\mathbb{Z}$. Let M be the dual lattice of N and e_1^* and e_2^* the corresponding dual basis. Then the dual lattice M' of N' is given by:

$$M \subseteq M' = \frac{1}{r}\mathbb{Z}e_1^* \oplus \mathbb{Z}e_2^*.$$

The inclusion of lattices $N' \hookrightarrow N$ induces a morphism of affine toric varieties:

$$f : \mathbb{A}_k^2 = \mathrm{Spec}(k[M']) \longrightarrow \mathrm{Spec}(k[\sigma^\vee \cap M]) = X_\sigma.$$

Write $U = \chi^{\frac{1}{r}e_1^*}$ and $Y = \chi^{e_2^*}$ so that $u_1^* = \frac{1}{r}e_2^*$ and $u_2^* = \frac{a}{r}e_1^* + e_2^*$ and $k[M'] = k[U, U^aY] = k[U, V]$ by setting $V = U^aY$. On the other hand, setting $X = \chi^{e_1^*} = U^r$ we have that:

$$k[\sigma^\vee \cap M] = \bigoplus k \cdot X^iY^j;$$

where $0 \leq j \leq \frac{r}{a}i$. So we see that $k[\sigma^\vee \cap M] = k[U, V]^G$ where the group $G \cong \mu_r$ acts on $k[U, V]$ by $\zeta_r \cdot (U, V) = (\zeta_r U, \zeta_r^a V)$ and the morphism f is induced by the inclusion $k[U, V]^G \subseteq k[U, V]$. Overall, $X_\sigma = \mathbb{A}_k^2/\mu_r$ is the cyclic quotient singularity $\frac{1}{r}(1, a)$ in the notation of [Rei12] and we have proved the following:

Proposition 7.1.7. *Let X be a normal toric surface. Then X has at worst cyclic quotient singularities.*

Example 7.1.8. Consider the case $a = r - 1$. Then the invariant polynomial ring is given by:

$$k[U, V]^{\mu_r} = k[U^r, V^r, UV].$$

Setting $X = U^r$, $Y = V^r$ and $Z = UV$ we can write this quotient as follows:

$$\begin{aligned} \mathbb{A}_k^2 &\longrightarrow \mathrm{Spec}\left(\frac{k[X, Y, Z]}{\langle XY - Z^r\rangle}\right); \\ (U, V) &\longmapsto (U^r, V^r, UV). \end{aligned}$$

Resolution of toric singularities

Let N be a lattice and $\sigma \subseteq N_\mathbb{R}$ a strongly convex rational polyhedral cone. Let X_σ denote the corresponding affine toric variety. Suppose that σ *spans* $N_\mathbb{R}$ in the sense that there exists a generating set for σ which is a basis of $N_\mathbb{R}$. Then there exists a unique *toric fixed point* $x_\sigma \in X_\sigma$. Namely, if $T \times X_\sigma \to X_\sigma$ denotes the torus action, then x_σ is unique in

satisfying $z \cdot x_\sigma = x_\sigma$ for all $z \in T$ [CLS-24, Prop. 1.3.2]. In fact, either X_σ is non-singular or it has an isolated singularity at the unique toric fixed point $x_\sigma \in X_\sigma$.

Definition 7.1.9. Let N be a lattice and Σ a fan. A *refinement* Σ' of Σ is any morphism of fans $\Sigma' \to \Sigma$ where the underlying morphism of lattices is the identity.

In other words, Σ' is a fan in N such that, for each cone $\sigma' \in \Sigma'$, there exists a cone $\sigma \in \Sigma$ such that $\sigma' \subseteq \sigma$. Let $f : X_{\Sigma'} \to X_\Sigma$ be the morphism induced by a refinement. As f is induced by the identity on N, it restricts to the identity on the tori of $X_{\Sigma'}$ and X_Σ and so f is birational and in particular a blow-up. We refer to any blow-up induced by a refinement of fans as a *toric blow-up*. Note that, as f restricts to the identity on tori, a toric blow-up is centred in torus fixed points. It is well known that any singularity of a projective variety (over an algebraically closed field of characteristic 0) can be resolved by a sequence of blow-ups. In fact, one can show that singularities on toric varieties can be resolved by toric blow-ups:

Proposition 7.1.10. *Let X be a normal toric variety. Then there exists a desingularisation $\tilde{X} \to X$ given by a toric blow-up. In particular, $\tilde{X}$ is a toric variety.*

Proof. See [Ful93, p. 48 Prop.]. □

Example 7.1.11. Let X_σ denote the cyclic quotient singularity from Example 7.1.8. The refinement Σ' of the single cone σ to resolve the singularity is given by inserting the rays generated by the (primitive) lattice points:

$$u_0 = (0,1) \quad u_1 = (1,0) \quad ... \quad u_i = (i, -(i-1)) \quad ... \quad u_r = (r, -(r-1)).$$

Note that $X_\Sigma = X_{\sigma'_1} \cup ... \cup X_{\sigma'_r}$ where each $X_{\sigma'_i} \cong \mathbb{A}^2$ as each pair $\{u_i, u_{i+1}\}$ generate the lattice N. One may verify that this subdivision agrees with the resolution of singularities detailed in [Rei12].

7.1.2 Monoids

Definition 7.1.12. A (commutative) *monoid* is a triple $(P, +, 0)$ where:

$$+ : P \times P \longrightarrow P$$

is a (commutative) associative binary operation with neutral element $0 \in P$.

Example 7.1.13.
i) Let R be a commutative unital ring. Then R^* is a monoid under multiplication.

ii) For any integer $r > 0$, $\mathbb{N}^r$ is a monoid under addition (where by convention we take $0 \in \mathbb{N}$).

iii) Let M be a free abelian group of finite rank and $N = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ the dual lattice. Write $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$, $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R}$ and $\langle -, - \rangle : M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$ for the standard bilinear pairing. Suppose that $\sigma \subseteq M_{\mathbb{R}}$ is a strictly convex rational polyhedral cone with dual cone:

$$\sigma^{\vee} = \{n \in N_{\mathbb{R}} \mid \langle n, m \rangle \geq 0\}.$$

We say $P_{\sigma} = \sigma^{\vee} \cap N$ is the monoid associated to σ.

A homomorphism $f : P \to Q$ of monoids satisfies $f(0_P) = 0_Q$ and $f(x + y) = f(x) + f(y)$ for all $x, y \in P$. We say that P is *finitely generated* if there exists a surjective homomorphism $\mathbb{N}^r \to P$ for some $r > 0$. The *Grothendieck group* of P is the abelian group:

$$P^{\mathrm{gp}} = P \times P / \sim$$

with addition given coordinate-wise and where $(x, x') \sim (y, y')$ if and only if, for some element $z \in P$ we have $z + x + x' = z + y + y'$. Let $P \to P^{\mathrm{gp}}$ be the natural map $x \mapsto (x, 0)$. We say that P is *integral* if this is an injective map. We say that P is *saturated* if additionally, whenever $x \in P^{\mathrm{gp}}$ and there exists $n > 0$ such that $nx \in P$, then we have $x \in P$ also.

Definition 7.1.14. Let P be an integral monoid and take $P \subseteq P^{\mathrm{gp}}$ to be the inclusion. We define the *saturation* P^{sat} of P to be:

$$P^{\mathrm{sat}} = \{x \in P^{\mathrm{gp}} \mid nx \in P \text{ for some } n > 0\}.$$

Finally, we say that P is *torsion-free* if P^{gp} is a torsion free group.

Definition 7.1.15. A monoid P is *fine* if it is finitely generated and integral. We say that P is *toric* if it is fine, saturated and torsion-free; in particular P^{gp} is a free abelian group of finite rank.

Let N be a lattice, M its dual and $\sigma \subseteq N_{\mathbb{R}}$ a strictly convex rational polyhedral cone. Note that the associated monoid $P_{\sigma} = \sigma^{\vee} \cap M$ is indeed toric. It is finitely generated by Gordon's lemma and $P^{\mathrm{gp}} = M$ so it is saturated by construction.

Lemma 7.1.16. *Let P be a toric monoid. Then there exists a strongly convex rational polyhedral cone $\sigma \subseteq N_{\mathbb{R}}$ such that $P = P_{\sigma}$ where $M = P^{\mathrm{gp}}$ is a lattice and N its dual.*

Let P be toric and take $M = P^{\mathrm{gp}}$. We define:

$$\sigma^{\vee} = \{\lambda x \mid \lambda \in \mathbb{R},\, x \in M\} \subseteq M_{\mathbb{R}}.$$

Then, letting N be the dual lattice and $\langle -, - \rangle$ the standard pairing, we set:

$$\sigma = \{u \in N_{\mathbb{R}} \mid \langle u, v \rangle \geq 0 \,\text{for all}\, v \in \sigma^{\vee}\}.$$

P being saturated is equivalent to the fact that $P = \sigma^\vee \cap M$.

7.1.3 The étale topology

We are almost ready to define the category of logarithmic schemes. Of significant importance will be the category of *fine saturated log schemes* which will be modeled on the affine schemes $\mathrm{Spec}(R[P])$ where P is a fine saturated monoid and R is a base ring. However, if a scheme X is affine-locally isomorphic to such a scheme, then this is already too restrictive a definition. For example, if P is a toric monoid and R is an algebraically closed field of characteristic 0, then X will be rational.

To rectify this, we work in the *étale site* $X_{\text{ét}}$ where a fine saturated log scheme will only be étale-locally isomorphic to an affine scheme $\mathrm{Spec}(R[P])$. Again, if we restrict our attention to k algebraically closed of characteristic 0 and P a toric monoid, then every smooth variety is étale-locally isomorphic to $\mathbb{A}^n_k$, and is a fine saturated log scheme in an appropriate sense.

Definition 7.1.17. Let $\mathscr{C}$ be a category. A *Grothendieck topology* on $\mathscr{C}$ is the data of a set of families of morphisms $(U_i \to U)_{i\in I}$ for each object $U \in \mathscr{C}$ called the *coverings* of U satisfying:

i) For any covering $(U_i \to U)_{i\in I}$ and morphism $V \to U$ in $\mathscr{C}$, the fibre products $V_i = V \times_U U_i$ exist in $\mathscr{C}$ and $(V_i \to V)_{i\in I}$ is a covering of V.

ii) If $(U_i \to U)_{i\in I}$ is a covering of U, and if for each $i \in I$ we have a covering $(V_{ij} \to U_i)_{j\in J_i}$ of U_i, then $(V_{ij} \to U)_{i,j}$ is also a covering of U.

iii) For any $U \in \mathscr{C}$ the family $(U \xrightarrow{\mathrm{Id}} U)$ consisting of the identity is a covering.

A category $\mathscr{C}$ endowed with a Grothendieck topology will be referred to as a *site*.

Example 7.1.18. i) Let X be a scheme. The *Zariski* site is the category $\mathrm{Top}(X)$ of open subschemes $U \subseteq X$ with morphisms given by inclusions. A covering of $U \subseteq X$ is a family of open immersions $(j_i : U_i \to U)_{i\in I}$ such that $U = \bigcup_{i\in I} j_i(U_i)$ i.e. the family is *surjective*.

ii) The *étale site* has underlying category Et/X consisting of étale morphisms $U \to X$. The coverings are the families of étale morphisms $(U_i \to U)$ that are surjective in the same sense as the Zariski site.

A *presheaf* of sets on a category $\mathscr{C}$ with a Grothendieck topology is a functor:

$$\mathscr{F} : \mathscr{C}^{\mathrm{op}} \longrightarrow \mathrm{Set}$$

We say that a presheaf $\mathscr{F}$ is a *sheaf* if for every covering $(U_i \to U)_{i\in I}$ the sequence:

$$\mathscr{F}(U) \to \prod_{i\in I} \mathscr{F}(U_i) \rightrightarrows \prod_{(i,j)\in I\times I} \mathscr{F}(U_i \times_U U_j)$$

is exact. A morphism of (pre-)sheaves is simply a natural transformation of contravariant functors. Let X be a scheme. Recall that a geometric point $\bar{x} \to X$ is the induced morphism given by a choice of algebraic closure $\bar{k}$ of the residue field $\kappa(x)$ of a point $x \in X$. We say that an étale cover $\varphi : U \to X$ is an *étale neighbourhood* of x if $x \in \varphi(U)$.

Definition 7.1.19. Let X be a scheme and $\mathscr{F}$ a presheaf on $X_{\text{ét}}$. The *stalk* at a geometric point $\bar{x} \to X$ is:

$$\mathscr{F}_{\bar{x}} = \varinjlim_{(U\to X)} \mathscr{F}(U);$$

where the limit is taken over étale neighbourhoods of $x \in X$.

7.2 Logarithmic geometry

7.2.1 Logarithmic schemes

Definition 7.2.1. A *pre-log structure* on a scheme X is a sheaf of monoids $\mathscr{M}_X$ on the étale site $X_{\text{ét}}$, along with a morphism of sheaves of monoids:

$$\alpha_X : \mathscr{M}_X \longrightarrow \mathscr{O}_X;$$

where $\mathscr{O}_X$ is a sheaf of monoids under multiplication. A pre-log structure is a *log structure* if:

$$\alpha_X : \alpha_X^{-1}(\mathscr{O}_X^\times) \longrightarrow \mathscr{O}_X^\times$$

is an isomorphism. A *log scheme* $X^\dagger$ is a triple $(X, \mathscr{M}_X, \alpha_X)$ where $\alpha_X : \mathscr{M}_X \to \mathscr{O}_X$ is a log structure on a scheme X.

A morphism of log schemes $f : X^\dagger \to Y^\dagger$ is a morphism of schemes $f : X \to Y$ along with a morphism of sheaves of monoids $f^\# : f^{-1}\mathscr{M}_Y \to \mathscr{M}_X$ such that the following diagram:

$$\begin{array}{ccc} f^{-1}\mathscr{M}_Y & \longrightarrow & \mathscr{M}_X \\ {\scriptstyle f^{-1}\alpha_Y}\downarrow & & \downarrow{\scriptstyle \alpha_X} \\ f^{-1}\mathscr{O}_Y & \xrightarrow{f^*} & \mathscr{O}_X \end{array}$$

is commutative.

Example 7.2.2. i) If X is a scheme, we can always define the *trivial log structure* where we take $\mathscr{M}_X = \mathscr{O}_X^\times$ and α_X is inclusion.

ii) Let X be a scheme and $D \subseteq X$ an effective divisor. Let $U = X \setminus D$ and $j : U \hookrightarrow X$ denote the corresponding open immersion. We define the *divisorial log structure* on X induced by D via the sheaf of monoids:

$$\mathscr{M}_{(X,D)} = (j_* \mathscr{O}_U^\times) \cap \mathscr{O}_X.$$

This is the sheaf of regular function on X which are invertible on U; clearly it is closed under multiplication. We take α_X to be inclusion.

iii) Let k be a field and $X = \mathrm{Spec}(k)$. Defining a sheaf of monoids on X is equivalent to defining a monoid homomorphism:

$$P \longrightarrow k.$$

The *standard log point* is the log scheme given by the monoid homomorphism $\alpha : k^* \oplus \mathbb{N} \to k$ where:

$$\alpha(a, n) = \begin{cases} a & \text{if } n = 0; \\ 0 & \text{otherwise.} \end{cases}$$

As with the *sheafification* $\mathscr{F}^+$ of a presheaf $\mathscr{F}$ on a scheme X, one can always minimally produce a log structure on X from a pre-log structure:

Definition 7.2.3. Let $\alpha : \mathscr{M}_X \to \mathscr{O}_X$ be a pre-log structure on a scheme X. The *log structure associated to* $\mathscr{M}_X$ is given by the sheaf of monoids:

$$\mathscr{M}_X^+ = \frac{\mathscr{M}_X \oplus \mathscr{O}_X^\times}{\{(m, \alpha_X(m)^{-1}) \mid m \in \alpha_X^{-1}(\mathscr{O}_X^\times)\}}$$

and the morphism of monoids:

$$\begin{aligned} \alpha_X^+ : \mathscr{M}_X^+ &\longrightarrow \mathscr{O}_X; \\ (m, f) &\longmapsto \alpha_X^+(m) f. \end{aligned}$$

It is often easier in practice to describe a pre-log structure on a scheme. For example, suppose that P is a monoid and $\underline{P}$ is the constant sheaf on a scheme X with stalk P. Then we say that the pre-log structure $\underline{P} \to \mathscr{O}_X$ is a *chart* for the induced log structure on X.

Example 7.2.4. Let k be a field. Then the morphism of monoids $\mathbb{N} \to k$ sending $0 \mapsto 1$ and $n \mapsto 0$ for $n > 0$ is a *global chart* for the standard log point.

Another important class of log structures are the *pullback log structures*. Given a log scheme $Y^\dagger$ and a morphism of schemes $f : X \to Y$, there is a natural way to induce a log structure $X^\dagger$ on X:

Definition 7.2.5. Let $f : X \to Y$ be a morphism of schemes and $\alpha_Y : \mathscr{M}_Y \to \mathscr{O}_Y$ a log structure on Y. Then the *pullback log structure* on X is the log structure associated to the pre-log structure:

$$f^{-1}(\mathscr{M}_Y) \xrightarrow{\alpha_Y} f^{-1}(\mathscr{O}_Y) \xrightarrow{f^*} \mathscr{O}_X.$$

We denote this log structure by $f^*\mathscr{M}_Y$.

Remark 7.2.6. Let R be a discrete valuation ring with residue field k. Let $S = \mathrm{Spec}(R)$ and $0 \in S$ the closed point corresponding to $\mathrm{Spec}(k)$. Then the divisorial log structure corresponding to $(S, \{0\})$ is given by the global chart:

$$\begin{aligned} \mathbb{N} &\longrightarrow R; \\ n &\longmapsto \pi^n. \end{aligned}$$

The pullback log structure to the closed point $\mathrm{Spec}(k)$ then agrees with the global chart in Ex. 7.2.4.

Definition 7.2.7. Let $f : X^\dagger \to Y^\dagger$ be a morphism of log schemes. We say that f is *strict* if the pullback log structure $f^*\mathscr{M}_Y$ coincides with the log structure $\mathscr{M}_X$ on X.

We say a chart $\underline{P} \to \mathscr{O}_X$ is a *global chart* if the induced map of log schemes $X^\dagger \to \mathrm{Spec}(\mathbb{Z}[P])^\dagger$ is strict. Let P be a monoid and R a ring. We denote by $R[P]$ the monoid ring which is the polynomial algebra generated by P. We use the notation χ^m to denote the image of $m \in P$ under the natural map $\varphi : P \to R[P]$ and thus have the relation $\chi^m \cdot \chi^{m'} = \chi^{m+m'}$ for all $m, m' \in P$. We say that $X^\dagger$ is an *affine logarithmic R-scheme* if $X = \mathrm{Spec}(R[P])$ for a monoid P, and φ is a global chart.

Example 7.2.8. Let k be an algebraically closed field and $P = \sigma^\vee \cap M$ a toric monoid. Then a global chart for the affine toric variety X_σ/k is given by the natural map:

$$\begin{aligned} P &\longrightarrow k[P]; \\ m &\longmapsto \chi^m. \end{aligned}$$

Let $T \subseteq X_\sigma$ denote the torus and $\partial X_\sigma = X_\sigma \setminus T$ the *toric boundary*. Then in fact, the divisorial log structure $\mathscr{M}_{(X_\sigma, \partial_\sigma)}$ coincides with the log structure for this global chart.

Let $X^\dagger = (X, \mathscr{M}_X)$ be a log scheme. As $\alpha_X : \mathscr{M}_X \to \mathscr{O}_X$ is a log structure, $\mathscr{O}_X^\times$ is a submonoid of $\mathscr{M}_X$. We denote by:

$$\overline{\mathscr{M}_X} = \mathrm{coker}(\alpha_X^{-1} : \mathscr{O}_X^\times \to \mathscr{M}_X)$$

the *ghost sheaf* of $X^\dagger$. Given a scheme X, there are many different choices for a log structure and it is hard to make any meaningful statements about a generic log scheme

without putting some constraints on the log structure. We say that $X^\dagger$ is *fine saturated (fs)* if étale-locally it admits a chart modeled on a fine saturated monoid. In fact, one may take this monoid to be torsion free. This justifies the claim that logarithmic schemes are étale-locally toric. For any fs log scheme $X^\dagger$, there exists an étale cover by affine toric $\mathbb{Z}$-schemes $\mathrm{Spec}(\mathbb{Z}[P])$.

Definition 7.2.9. Let $f : X^\dagger \to Y^\dagger$ be a morphism of fine log schemes. We say that f is *log smooth* if étale-locally on X and Y there is a commutative diagram:

$$\begin{array}{ccc} X & \longrightarrow & \mathrm{Spec}(\mathbb{Z}[P]) \\ {\scriptstyle f}\downarrow & & \downarrow \\ Y & \longrightarrow & \mathrm{Spec}(\mathbb{Z}[Q]) \end{array}$$

satisfying the following conditions:

i) The horizontal maps induce charts $\underline{P} \to \mathscr{O}_X$ and $\underline{Q} \to \mathscr{O}_Y$ for $X^\dagger$ and $Y^\dagger$ respectively.

ii) The induced morphism:

$$X \to Y \times_{\mathrm{Spec}(\mathbb{Z}[Q])} \mathrm{Spec}(\mathbb{Z}[P])$$

is a smooth morphism of schemes.

iii) The vertical arrow on the right is induced by a monoid homomorphism $Q \to P$ with $\ker(Q^{\mathrm{gp}} \to P^{\mathrm{gp}})$ and the torsion part of $\mathrm{coker}(Q^{\mathrm{gp}} \to P^{\mathrm{gp}})$ both finite groups of orders invertible in X.

A diagram as in the above definition is a *chart* for the morphism $f : X^\dagger \to Y^\dagger$.

Example 7.2.10. i) Let $f : X \to S$ be a morphism of smooth schemes. Then if we endow X and S with the trivial log structure and take $P = Q = 0$ in the above, we see that f becomes log smooth.

ii) Let k be a field and P a toric monoid. Set $X = \mathrm{Spec}(k[P])$ with the toric log structure and endow $Y = \mathrm{Spec}(k)$ with the trivial log structure. Taking $Q = 0$ in the above definition, we see that $X^\dagger \to \mathrm{Spec}(k)^\dagger$ becomes log smooth; even though X may not be a nonsingular variety.

iii) Let $f : \mathscr{X} \to \mathbb{A}^1_k$ be a flat morphism where $\mathscr{X}$ is regular, k is a field and for all $t \neq 0$, the fibre $\mathscr{X}_t$ is a non-singular variety. Suppose further that $\mathscr{X}_0$ is a strict normal crossings divisor so that étale-locally we may take $\mathscr{X} = \{x_1 \cdot \ldots \cdot x_r = t\}$ in $\mathbb{A}^n \times \mathbb{A}^1$. Taking $P = \mathbb{N}^r$ and $Q = \mathbb{N}$ and defining the morphism of monoids $Q \to P$

by $1 \mapsto (1, ..., 1)$, we then obtain a chart for f by:

$$\begin{aligned} \mathbb{N}^r &\longrightarrow \frac{k[x_1, ..., x_n, t]}{\langle x_1 \cdot ... \cdot x_r - t \rangle}; \\ e_i &\longmapsto x_i \end{aligned}$$

and $\mathbb{N} \to k[t]$ by $1 \mapsto t$. Then we can see that $f : \mathscr{X}^\dagger \to (\mathbb{A}^1_k)^\dagger$ is log smooth. Moreover, we can endow $f|_{\mathscr{X}_0} : \mathscr{X}_0^\dagger \to \mathrm{Spec}(k)^\dagger$ with the pullback log structure so that $\mathrm{Spec}(k)^\dagger$ is the standard log point and $\mathscr{X}_0^\dagger$ is log smooth over this point even though it has strict normal crossings singularities.

7.3 Log smooth curves, log differentials and log deformation theory

7.3.1 Log smooth curves

A *log smooth curve* is a log smooth integral morphism $f : \mathscr{C}^\dagger \to S^\dagger$ of relative dimension 1.

Definition 7.3.1. Let R be a complete discrete valuation ring with algebraically closed residue field k and π a uniformiser. By an R-curve we mean a flat morphism $f : \mathscr{C} \to \mathrm{Spec}(R)$ of relative dimension 1. Suppose that R has fraction field K and $C = \mathscr{C}_K$ is a non-singular curve. We say that $\mathscr{C}$ has *semistable reduction* if, for at worst a finite set of closed points $x \in \mathscr{C}(k)$, there exists an étale neighbourhood $\mathscr{U} \to \mathscr{C}$ of x given by:

$$\mathscr{U} \cong \mathrm{Spec}\left(\frac{R[s,t]}{\langle st - \pi^e \rangle}\right)$$

for some integer $e > 0$. Otherwise, $x \in \mathscr{C}(k)$ is a non-singular point and there is an étale neighbourhood $\mathscr{U} \to \mathscr{C}$ of x given by:

$$\mathscr{U} \cong \mathrm{Spec}(R[t])$$

Importantly, there is a natural way of endowing a log structure on a semistable curve $f : \mathscr{C} \to S$. First, we choose a log structure on the base $S^\dagger$ by a chart $\sigma : Q \to R$. We have an étale cover by the two types of charts above, and so need only define log structures on each:

i) For the chart $\mathscr{U} = \mathrm{Spec}(R[t]) \to S$ we take the log structure induced by the following

chart of monoids:

$$\begin{aligned} Q &\longrightarrow R[t]; \\ q &\longmapsto f^*(\sigma(q)). \end{aligned}$$

ii) For the chart $\mathscr{U} \cong \operatorname{Spec}\left(\frac{R[s,t]}{\langle st-\pi^e\rangle}\right) \to S$ we take the following chart of monoids:

$$\begin{aligned} \mathbb{N}^2 \oplus_{\mathbb{N}} Q &\longrightarrow \operatorname{Spec}\left(\frac{R[s,t]}{\langle st-\pi^e\rangle}\right); \\ ((a,b),q) &\longmapsto s^a t^b f^*(\sigma(q)) \end{aligned}$$

where the pushout of monoids is induced by the morphisms $\mathbb{N} \to Q$ sending 1 to an element $\alpha \in Q$ such that $\sigma(\alpha) = \pi^e$, and the diagonal $\mathbb{N} \to \mathbb{N}^2$.

Example 7.3.2. Suppose we take the chart $\mathbb{N} \to R$ as in Remark 7.2.6 sending $1 \to \pi$ so that the pullback log structure on $\operatorname{Spec}(k)$ gives the standard log point. Define the monoids S_e for $e > 0$ as the pushouts $S_e = \mathbb{N}^2 \oplus_{\mathbb{N}} \mathbb{N}$ induced by the diagonal $\mathbb{N} \to \mathbb{N}^2$ and the multiplication by e map $\mathbb{N} \xrightarrow{\cdot e} \mathbb{N}$. Then taking $Q = \mathbb{N}$ and $\alpha = e$ in (ii) we obtain a chart for the morphism $f : \mathscr{U} = \operatorname{Spec}\left(\frac{R[s,t]}{\langle st-\pi^e\rangle}\right) \to S$.

Let $\mathscr{U}_0^\dagger$ denote the closed fibre $\operatorname{Spec}\left(\frac{k[s,t]}{\langle st\rangle}\right)$ with the pullback log structure. Of course, without the log structure, the fibre $\mathscr{U}_0$ is independent of e, however, $\mathscr{U}_0^\dagger$ 'remembers' that it sits in the family $\mathscr{U}$ via the monoid S_e. Equivalently, one can note that S_e is a toric monoid and consider the corresponding toric variety $X = \operatorname{Spec}(k[S_e])$. In fact, this is precisely the affine toric surface singularity $\frac{1}{e}(1, e-1)$ considered in Prop. 7.1.7. Moreover, it follows that the boundary divisor ∂X coincides with $\mathscr{U}_0$ and the toric logarithmic structure on ∂X coincides with $\mathscr{U}_0^\dagger$. Alternatively phrased, $\mathscr{U}$ is étale-locally a cyclic quotient singularity of type A_{e-1}, and the log scheme $\mathscr{U}_0^\dagger$ 'remembers' the singularity of the family.

It turns out that any log smooth curve $f : \mathscr{C}^\dagger \to S^\dagger$ is covered by charts of the form (i), (ii) or the chart of a *log marked point* (iii):

Definition 7.3.3. Let R be a discrete valuation ring with residue field k and let $Q \to R$ be a monoid homomorphism with $S^\dagger = \operatorname{Spec}(R)^\dagger$ the induced log scheme. A point $x \in \mathscr{C}(k)$ on a log R-curve $f : \mathscr{C}^\dagger \to S^\dagger$ is a *log marked point* if there is an étale neighbourhood $\mathscr{U} \to \mathscr{C}$ of x given by $\mathscr{U} = \operatorname{Spec}(R[t]) \to S$ with chart:

$$\begin{aligned} \mathbb{N} \oplus Q &\longrightarrow R[t]; \\ (n,q) &\longmapsto t^n f^*(\sigma(q)). \end{aligned}$$

If $f : \mathscr{C}^\dagger \to S^\dagger$ is a log curve and $x \in \mathscr{C}(k)$ is a log marked point then $\mathscr{C}_k$ is non-singular at x, but the pullback log structure of $\mathscr{C}^\dagger$ to x is a log point given by the monoid $Q \to k$.

Theorem 7.3.4. *Let R be a discrete valuation ring with algebraically closed residue field. Let $S = \mathrm{Spec}(R)$ and let $f : \mathscr{C}^\dagger \to S^\dagger$ be a log smooth curve. Then there is an étale covering of f by charts of the form $(i) - (iii)$; where charts of the form $(ii) - (iii)$ occur over only a finite set of points of $\mathscr{C}(k)$.*

Proof. See [F.Kat00, Theorem 1.3]. □

7.3.2 Logarithmic differentials

Definition 7.3.5. Let $f : X^\dagger \to Y^\dagger$ be a morphism of log schemes and $\mathscr{E}$ an $\mathscr{O}_X$-module. A *log derivation* of $X^\dagger$ over $Y^\dagger$ with values in $\mathscr{E}$ is a pair $(D, D\log)$ where $D : \mathscr{O}_X \to \mathscr{E}$ is a usual derivation and $D\log : \mathscr{M}_X^{\mathrm{gp}} \to \mathscr{E}$ is a morphism of sheaves of abelian groups satisfying:

i) For every local section m of $\mathscr{M}_X$ we have:

$$D(\alpha_X(m)) = \alpha_X(m) \cdot D\log(m).$$

ii) For every local section n of $f^{-1}\mathscr{M}_Y$ we have $D\log(f^\#(n)) = 0$.

Write $\mathrm{Der}_{X^\dagger/Y^\dagger}(\mathscr{E})$ for the sheaf of log derivations of $f : X^\dagger \to Y^\dagger$ with values in $\mathscr{E}$, and $\Theta_{X^\dagger/Y^\dagger} = \mathrm{Der}_{X^\dagger/Y^\dagger}(\mathscr{O}_X)$. Roughly speaking, the sheaf $\mathscr{M}_X$ tells us which regular functions we may apply $D\log$ to, and we ask that $D\log$ is trivial on the base.

Definition 7.3.6. Let $f : X^\dagger \to Y^\dagger$ denote a morphism of log schemes. The sheaf of *log differentials* is given by:

$$\Omega^1_{X^\dagger/Y^\dagger} = \frac{\Omega^1_{X/Y} \oplus (\mathscr{O}_X \otimes_{\mathbb{Z}} \mathscr{M}_X^{\mathrm{gp}})}{\mathscr{K}}$$

where $\mathscr{K}$ is the $\mathscr{O}_X$-module generated by elements $(d(\alpha_X(m)), -\alpha_X(m) \otimes m)$ and $(0, 1 \otimes f^*(n))$ for all $m \in \mathscr{M}_X$ and $n \in f^{-1}\mathscr{M}_Y$. We obtain a log derivation taking values in $\Omega^1_{X^\dagger/Y^\dagger}$ via the natural maps:

$$d : \mathscr{O}_X \longrightarrow \Omega^1_{X/Y} \longrightarrow \Omega^1_{X^\dagger/Y^\dagger}; \tag{7.1}$$

$$d\log : \mathscr{M}_X^{\mathrm{gp}} \longrightarrow \mathscr{O}_X \otimes_{\mathbb{Z}} \mathscr{M}_X^{\mathrm{gp}} \longrightarrow \Omega^1_{X^\dagger/Y^\dagger}. \tag{7.2}$$

Lemma 7.3.7. *Let $f : X^\dagger \to Y^\dagger$ be a morphism of log schemes. The sheaf of log differentials is universal in the sense that, for all $\mathscr{O}_X$-modules $\mathscr{E}$ with a log derivation $(D, D\log)$, there exists a unique morphism of $\mathscr{O}_X$-modules $\Phi : \Omega^1_{X^\dagger/S^\dagger} \to \mathscr{E}$ such that:*

$$D = \Phi \circ d \quad \text{and} \quad D\log = \Phi \circ d\log.$$

In particular, we have:

$$\Theta_{X^\dagger/Y^\dagger} \cong \mathscr{H}om_{\mathscr{O}_X}(\Omega^1_{X^\dagger/S^\dagger}, \mathscr{O}_X).$$

Proof. See [Gr11, Lemma 3.33]. □

Example 7.3.8. i) Let $f : X^\dagger \to Y^\dagger$ be a log smooth morphism. Then $\Omega^1_{X^\dagger/Y^\dagger}$ is a locally free sheaf on X.

ii) Let k be an algebraically closed field, X/k a non-singular variety and $D \subseteq X$ an effective, strict normal crossings divisor. Suppose that we endow X with the divisorial log structure $\mathscr{M}_{(X,D)}$ and $\mathrm{Spec}(k)$ with the trivial log structure. Then we have that:

$$\Omega^1_{X^\dagger/k} \cong \Omega^1_{X/k}(\log D).$$

iii) Let R be a complete discrete valuation ring with algebraically closed residue field k. Let $C_0^\dagger \to \mathrm{Spec}(k)^\dagger$ be the special fibre of a log smooth curve as in Thm. 7.3.4. We can write:

$$C_0 = \sum_i D_i$$

for the irreducible components which we assume to be reduced. Then, if $x_1, ..., x_n \in D_i$ are the closed points which are either nodes or log marked points, then we have that:

$$\Theta_{C_0^\dagger/k^\dagger}|_{D_i} \cong \Theta_{D_i/k}(-\sum_{j=1}^{n} x_i).$$

In fact, if $\omega_{C_0/k}$ is the dualising sheaf, then we have an isomorphism:

$$\Omega^1_{C_0^\dagger/k^\dagger} \cong \omega_{C_0/k}(s_1 + ... + s_r)$$

where $s_1, ..., s_r \in C_0$ are the log marked points [F.Kat00, Prop. 1.13].

Lemma 7.3.9. *Given a morphism $f : X^\dagger \to Y^\dagger$ of log schemes over $S^\dagger$ there is a natural morphism:*

$$f^* : f^*(\Omega^1_{Y^\dagger/S^\dagger}) \longrightarrow \Omega^1_{X^\dagger/S^\dagger}$$

induced by the usual pullback on differential forms $f^*\Omega^1_{Y/S} \to \Omega^1_{X/S}$ and the morphism of sheaves:

$$f^* \otimes f^\# : f^{-1}(\mathscr{O}_Y \otimes \mathscr{M}_Y^{\mathrm{gp}}) \longrightarrow \mathscr{O}_X \otimes \mathscr{M}_X^{\mathrm{gp}}.$$

Proof. See [Gr11, Def. 3.35] □

7.3.3 Logarithmic deformation theory

Let k be an algebraically closed field and let $f_0 : X_0^\dagger \to \mathrm{Spec}(k)^\dagger$ be a log smooth variety. Let R_n be an artinian local ring with uniformiser π and residue field k. Suppose that $\pi^n \neq 0$ but $\pi^{n+1} \cdot R_n = 0$ and denote by $R_{n-i} = R_n/\pi^i$. The study of log deformation theory, in analogy to deformation theory of schemes, involves understanding when a log smooth morphism $X_0^\dagger \to \mathrm{Spec}(k)^\dagger$ extends to a log smooth morphism $X_n^\dagger \to \mathrm{Spec}(R_n)^\dagger$.

The key difference between deformation theory of schemes versus deformations of log schemes is that log deformations are not necessarily locally trivial. In fact, a local lifting is completely determined by choosing a log structure on $\mathrm{Spec}(R_n)$. This is illustrated by the following proposition:

Proposition 7.3.10. *Let $f_0 : X_0^\dagger \to \mathrm{Spec}(k)^\dagger$ be a log smooth affine variety, where $\mathrm{Spec}(k)^\dagger$ is the standard log point. Given a fine log structure on $\mathrm{Spec}(R_n)^\dagger$, there is a unique up to isomorphism (if it exists) log smooth lifting $f_n : X_n^\dagger \to \mathrm{Spec}(R_n)^\dagger$.*

Proof. See [Gr11, Prop. 3.38]. □

On the other hand, as in the case of deformation of schemes, there is a cohomological description of the obstruction to lifting a log smooth morphism $f_{n-1} : X_{n-1}^\dagger \to \mathrm{Spec}(R_{n-1})^\dagger$ to $\mathrm{Spec}(R_n)^\dagger$ globally (given a choice of fine log structure), and the space of possible liftings has a torsor description:

Proposition 7.3.11. *Suppose $f_0 : X_0^\dagger \to \mathrm{Spec}(k)^\dagger$ is a log smooth variety. Suppose there exists a log smooth deformation $f_{n-1} : X_{n-1}^\dagger \to \mathrm{Spec}(R_{n-1})^\dagger$. Given a log structure on R_n, there exists an obstruction in $H^2(X_0, \Theta_{X_0^\dagger/k^\dagger})$ that vanishes if and only if there exists a log smooth deformation $f_n : X_n^\dagger \to \mathrm{Spec}(R_n)^\dagger$ extending f_0. In this case, the set of log smooth deformations is a torsor over $H^1(X_0, \Theta_{X_0^\dagger/k^\dagger})$.*

Proof. See [Gr11, Prop. 3.40]. □

In particular, log smooth curves are unobstructed. There is also an analogue of the infinitesimal lifting criterion for log smooth morphisms due to F. Kato. We say that a morphism of log schemes $t : (T', \mathscr{M}_{T'}) \to (T, \mathscr{M}_T)$ is an *infinitesimal thickening* of *order at most n* if it is a strict, closed immersion and the corresponding ideal sheaf $\mathscr{I}$ is nilpotent with $\mathscr{I}^{n+1} = 0$.

Proposition 7.3.12 (Log smooth infinitesimal lifting criterion)**.** *Let $f : (X, \mathscr{M}_X) \to (Y, \mathscr{M}_Y)$ be a morphism of fine log schemes, locally of finite presentation. Then f is log*

smooth if and only if it is infinitesimally log smooth, namely, for all diagrams of the form:

$$\begin{array}{ccc} (T', \mathscr{M}_{T'}) & \xrightarrow{\sigma'} & (X, \mathscr{M}_X) \\ {\scriptstyle t}\downarrow & \overset{\exists g}{\nearrow} & \downarrow{\scriptstyle f} \\ (T, \mathscr{M}_T) & \xrightarrow[\sigma]{} & (Y, \mathscr{M}_Y) \end{array}$$

where t is a thickening of order at most 1, there exists a unique morphism of log schemes $g : (T, \mathscr{M}_T) \to (X, \mathscr{M}_X)$ such that the diagram commutes.

Proof. See [F.Kat96, Thm. 4.1]. □

7.3.4 Logarithmic geometry in positive characteristic

Let k be a perfect field of characteristic $p > 0$. Recall that, if X is a k-scheme then we define the absolute Frobenius morphism $F_X : (X, \mathscr{O}_X) \to (X, \mathscr{O}_X)$ as the identity on topological spaces and the power-of-p map $F^{\#} : \mathscr{O}_X \to \mathscr{O}_X$. If $\alpha : \mathscr{M}_X \to \mathscr{O}_X$ is a log structure on X, then we can define the *absolute log Frobenius morphism* $F_{X^\dagger} : X^\dagger \to X^\dagger$ by defining $F_X^\flat : \mathscr{M}_X \to \mathscr{M}_X$ to be the multiplication-by-p map.

Suppose that we endow $\mathrm{Spec}(k)$ with a log structure and $X^\dagger$ is a $k^\dagger$-log scheme. Similarly, one can define the *log Frobenius twist* $(X^\dagger)^{(p)}$ of $X^\dagger$ as the fibre product in the category of log schemes:

$$\begin{array}{ccc} (X^\dagger)^{(p)} & \longrightarrow & X^\dagger \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k)^\dagger & \xrightarrow[F_{\mathrm{Spec}(k)^\dagger}]{} & \mathrm{Spec}(k)^\dagger \end{array} .$$

And by the universal property, the *relative log Frobenius morphism* $F_{X^\dagger/k^\dagger} : X^\dagger \to (X^\dagger)^{(p)}$ is the unique morphism of $k^\dagger$-log schemes induced by the absolute log Frobenius morphism on $X^\dagger$.

Example 7.3.13. Let R be a discrete valuation ring of characteristic 0 with residue field k, algebraically closed of characteristic $p > 0$. Consider the log smooth morphism:

$$f : \mathscr{U}^\dagger = \mathrm{Spec}\left(\frac{R[x,y]}{\langle xy - \pi\rangle}\right)^\dagger \to \mathrm{Spec}(R)^\dagger$$

with log structure defined in Example 7.3.2 where π is a uniformiser of R. Let $f_0 : \mathscr{U}_k^\dagger \to \mathrm{Spec}(k)^\dagger$ be the restriction to the special fibre with the pullback log structure. Let $g_0 : (\mathscr{U}_k^\dagger)^{(p)} \to \mathrm{Spec}(k)^\dagger$ denote the log Frobenius twist of $\mathscr{U}_k^\dagger$. Then $\mathscr{U}_k \cong \mathscr{U}_k^{(p)}$ as

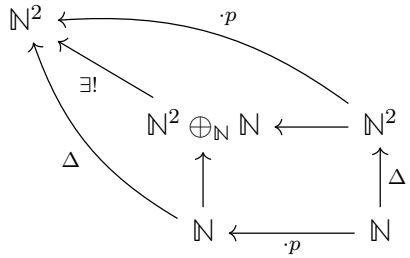
k-schemes, but the log structure on $\mathscr{U}_k^{(p)}$ is now given by the pushout of monoids:

$$\begin{array}{ccc} \mathbb{N}^2 \oplus_{\mathbb{N}} \mathbb{N} & \longleftarrow & \mathbb{N}^2 \\ \uparrow & & \uparrow \Delta \\ \mathbb{N} & \xleftarrow[\cdot p]{} & \mathbb{N} \end{array}.$$

This is the monoid S_p from Definition 7.3.1 (ii). Thus, if we consider the morphism of log schemes $\mathscr{V}^\dagger = \mathrm{Spec}\left(\frac{R[u,v]}{\langle uv-\pi^p\rangle}\right)^\dagger \to \mathrm{Spec}(R)^\dagger$ with chart given by the above pushout, then the restriction to the special fibre with the pullback log structure gives the log Frobenius twist of $\mathscr{U}_k^\dagger$. Moreover, the quotient map:

$$\begin{aligned} F : \mathscr{U}^\dagger &\longrightarrow \mathscr{V}^\dagger; \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

with chart given by the unique morphism $\mathbb{N}^2 \oplus_{\mathbb{N}} \mathbb{N} \to \mathbb{N}^2$:



provides a lifting of the relative log Frobenius morphism:

$$F_k : \mathscr{U}_k^\dagger \longrightarrow \mathscr{V}_k^\dagger \cong (\mathscr{U}_k^\dagger)^{(p)}.$$

Let $f : X^\dagger \to \mathrm{Spec}(k)^\dagger$ be a log smooth morphism where X/k is a variety, k is perfect of characteristic $p > 0$, and the log structures are fine. Then the sheaf of log differentials $\Omega^1_{X^\dagger/k^\dagger}$ is locally free of rank $\dim(X)$. Set $\Omega^i_{X^\dagger/k^\dagger} = \bigwedge^i \Omega^1_{X^\dagger/k^\dagger}$. The *logarithmic de Rham complex* is given by the exterior derivatives:

$$d : \Omega^i_{X^\dagger/k^\dagger} \longrightarrow \Omega^{i+1}_{X^\dagger/k^\dagger};$$

which are defined uniquely by the first exterior derivative $d : \mathscr{O}_X \to \Omega^1_{X^\dagger/k^\dagger}$ as in Def. 7.3.6 and by constraining that:

i) $d^2\omega = 0$ for all sections ω in $\Omega^i_{X^\dagger/k^\dagger}$;

ii) $d(d\log(m)) = 0$ for all sections m of $\mathscr{M}_X$;

iii) $d(\omega \wedge \eta) = d\omega \wedge \eta + (-1)^i \omega \wedge d\eta$ if $\omega \in \Omega^i_{X^\dagger/k^\dagger}$ and $\eta \in \Omega^j_{X^\dagger/k^\dagger}$.

It is not hard to see that d is still $\mathscr{O}_{X^{(p)}}$-linear as in 3.4.1. Moreover, there is a natural extension of the Cartier operator/isomorphism to logarithmic differentials, the key being that the Cartier operator is constant on differential forms with logarithmic poles.

Theorem 7.3.14. *[Log Cartier isomorphism] Let k be an algebraically closed field of characteristic $p > 0$ and let $X^\dagger/k^\dagger$ be a log smooth variety of dimension n. Then for $0 \leq i \leq n$ we have an isomorphism of $\mathscr{O}_{X^{(p)}}$-modules:*

$$\mathscr{C}^{-1}_{X^\dagger/k^\dagger} : \Omega^i_{(X^\dagger)^{(p)}/k^\dagger} \longrightarrow \mathscr{H}^i\left((F_{X^\dagger/k^\dagger})_*\Omega^\bullet_{X^\dagger/k^\dagger}\right);$$

where, for a local section x of $\mathscr{O}_X$ (resp. m of $\mathscr{M}_X$) we denote by $x^{(p)}$ the corresponding section of $\mathscr{O}_{X^{(p)}}$ (resp. $m^{(p)}$ of $\mathscr{M}_{X^{(p)}}$), and $\mathscr{C}^{-1}_{X^\dagger/k^\dagger}$ is the unique $\mathscr{O}^{(p)}_X$-linear morphism satisfying:

$$\mathscr{C}^{-1}_{X^\dagger/k^\dagger}(dx^{(p)}) = [x^{p-1}dx] \quad \text{and} \quad \mathscr{C}^{-1}_{X^\dagger/k^\dagger}(d\log(m^{(p)})) = d\log(m)$$

In fact, $\mathscr{C}^{-1}_{X^\dagger/k^\dagger}$ defines a well defined isomorphism of graded $\mathscr{O}_{X^{(p)}}$-algebras:

$$\mathscr{C}^{-1}_{X^\dagger/k^\dagger} : \bigoplus_{i=0}^{n} \Omega^i_{(X^\dagger)^{(p)}/k^\dagger} \longrightarrow \bigoplus_{i=0}^{n} \mathscr{H}^i\left((F_{X^\dagger/k^\dagger})_*\Omega^\bullet_{X^\dagger/k^\dagger}\right).$$

Proof. See [Og18, Prop. 4.1.1]. □

Suppose that $C^\dagger \to \mathrm{Spec}(k)^\dagger$ is a log smooth curve without log marked points. Then we may identify $\Omega^1_{C^\dagger/k^\dagger} \cong \omega_{C/k}$ where $\omega_{C/k}$ is the dualising sheaf. As in the smooth case, we define the morphism of locally free sheaves of rank 1 on $C^{(p)}$ induced by the log Cartier isomorphism on $C^\dagger$ to be the *log Cartier operator*:

$$\mathscr{C} : (F_{C^\dagger/k^\dagger})_*\omega_{C/k} \to \mathrm{coker}((F_{C^\dagger/k^\dagger})_*\mathscr{O}_C \xrightarrow{d} (F_{C^\dagger/k^\dagger})_*\omega_{C/k}) \xrightarrow[\sim]{\mathscr{C}_{C^\dagger/k^\dagger}} \omega_{C^{(p)}/k}.$$

7.3.5 Logarithmic blow-ups

There is a special class of blow-ups on fine saturated log schemes called *logarithmic blow-ups*. Their construction can be considered the 'coordinate-free' analogue of a toric blow-up. There is a more general notion of a fan of monoids, and a subdivision of a fan that similarly produces logarithmic blow-ups from combinatorial data. Unlike a classical blow-up, a logarithmic blow-up is a log smooth morphism, even though it is not flat (in general, a log smooth morphism need not be flat).

Definition 7.3.15. Let P be a monoid. A subset $I \subseteq P$ is an *ideal* if $I \cdot P \subseteq I$. I is a *prime ideal* if $P \setminus I$ is a submonoid. Write $\mathrm{Spec}(P)$ for the set of all prime ideals of P.

Note that $\emptyset$ and P are trivially ideals of P. Suppose that $I \subseteq P$ is non-trivial for a fine saturated monoid P. Let $\langle I \rangle \subseteq \mathbb{Z}[P]$ denote the ideal of the ring $\mathbb{Z}[P]$ generated by I. We define the *logarithmic blow-up* of $X^\dagger = \mathrm{Spec}(\mathbb{Z}[P])^\dagger$ with *centre* I to be the blow-up map:

$$\pi : Y^\dagger = \mathrm{Proj}_X \left(\bigoplus \langle I \rangle^n \right)^\dagger \longrightarrow \mathrm{Spec}(\mathbb{Z}[P])^\dagger.$$

We define the log structure on Y as follows. First note that Y has an open affine cover by:

$$U_a = \mathrm{Spec}(\mathbb{Z}[P_a]);$$

where $a \in I$ and $P_a \subseteq P^{\mathrm{gp}}$ is the submonoid generated by elements of the form $\frac{b}{a}$ for $b \in I$. In general, the canonical log structure on U_a is not necessarily saturated so we take the saturation $U_a^{\mathrm{sat}} = \mathrm{Spec}(\mathbb{Z}[P_a^{\mathrm{sat}}])$ (Def. 7.1.14) and use this to define the log structure on Y.

Definition 7.3.16. Let $X^\dagger = (X, \mathscr{M}_X)$ be a log scheme and $\mathscr{I} \subseteq \mathscr{M}_X$ an ideal sheaf (of monoids). We say that $\pi : Y^\dagger \to X^\dagger$ is the *log blow-up* of $X^\dagger$ with *centre* $\mathscr{I}$ if étale locally on X there is a chart $\underline{P} \to \mathscr{O}_X$ by a fine saturated monoid such that $Y^\dagger$ is the pull-back:

$$\begin{array}{ccc} Y^\dagger & \longrightarrow & \mathrm{Proj}_X \left(\bigoplus \langle I \rangle^n\right)^\dagger \\ {\scriptstyle f}\downarrow & & \downarrow \\ X^\dagger & \longrightarrow & \mathrm{Spec}(\mathbb{Z}[P])^\dagger \end{array}$$

where $I = \mathscr{I}(\mathrm{Spec}(\mathbb{Z}[P]))$ and the saturated log structure on $\mathrm{Proj}_X \left(\bigoplus \langle I \rangle^n\right)^\dagger$ is the one defined above.

Remark 7.3.17. Let X be a scheme and $\mathscr{I} \subseteq \mathscr{O}_X$ a quasi-coherent ideal sheaf. Consider the classical blow-up of X along the corresponding closed subscheme Z:

$$\pi : Y = \mathrm{Proj}_X \left(\bigoplus_{n \geq 0} \mathscr{I}^n \right) \longrightarrow X.$$

One can show that the exceptional divisor $\pi^{-1}(Z) \subseteq Y$ is a Cartier divisor. Indeed, over an open affine $U = \mathrm{Spec}(A)$ where $\mathscr{I}(U) = I \subseteq A$ we have that $\pi^{-1}(U)$ is covered by open affines of the form:

$$U_a = \mathrm{Spec}\left(A \left[\frac{I}{a} \right] \right);$$

where $a \in I$. In fact, $\pi : Y \to X$ is the minimal X-scheme such that $\pi^{-1}(Z)$ is Cartier [stacks-project, Lemma 31.32.5].

Analogously, if P is a finite saturated monoid we say that an ideal $I \subseteq P$ is *invertible* if it is generated by a single element. More generally, an ideal sheaf $\mathscr{I} \subseteq \mathscr{M}_X$ of a finite saturated log scheme $X^\dagger = (X, \mathscr{M}_X)$ is *fractional* if X is covered by charts $\underline{P} \to \mathscr{O}_X$ such that $\mathscr{I}$ is locally invertible.

By the étale-local construction above, it is not hard to see that if $\mathscr{I} \subseteq \mathscr{M}_X$ is an ideal sheaf of a finite saturated log scheme $X^\dagger = (X, \mathscr{M}_X)$ then the ideal sheaf $\mathscr{J} = \mathscr{I} \cdot \mathscr{M}_Y$ of the log blow-up $Y^\dagger \to X^\dagger$ at $\mathscr{I}$ is fractional. Similarly, the log blow-up of $\pi : Y^\dagger \to X^\dagger$ with centre $\mathscr{I}$ is the minimal fine saturated log-scheme over $X^\dagger$ such that $\mathscr{I} \cdot \mathscr{M}_Y$ is fractional [Niz06, Prop. 4.2].

Proposition 7.3.18. *Let $X^\dagger = (X, \mathscr{M}_X)$ be a finite saturated log scheme and $\mathscr{I} \subseteq \mathscr{M}_X$ and ideal sheaf. Write $\pi : Y^\dagger \to X^\dagger$ for the log blow-up of $X^\dagger$ at $\mathscr{I}$. Then π is log smooth.*

Proof. The question is local on $X^\dagger$ so we need only verify condition (iii) of Def. 7.2.9 for the natural monoid homomorphism:

$$P \longrightarrow P_a$$

where P is a fine saturated monoid, $I \subseteq P$ is a non-trivial ideal and P_a is the submonoid of P^{gp} generated by some $a \in I$. This is immediate as $(P_a)^{\mathrm{gp}} = P^{\mathrm{gp}}$ □

We conclude our discussion on logarithmic blow-ups by noting that they generalise toric blow-ups. The following can be found in [K.Kat94]. Recall that if N is a lattice, a fan Σ in N is a collection of strictly convex rational polyhedral cones $\sigma \subseteq N_{\mathbb{R}}$ such that any face τ of σ lies in Σ and any intersection of cones $\sigma_1 \cap \sigma_2$ in Σ is a face of both. From a fan Σ, we can construct the log scheme $X^\dagger_\Sigma$ by gluing the affine log schemes:

$$X_{P_\sigma} = \mathrm{Spec}(\mathbb{Z}[P_\sigma])$$

where $P_\sigma = \sigma^\vee \cap M$ for the dual lattice $M = N^\vee$ with the induced log structure by the monoids P_σ. Moreover, if Σ' is a subdivison of Σ, then we obtain a morphism of log schemes $X^\dagger_{\Sigma'} \to X^\dagger_\Sigma$ by noting that, for a cone $\sigma' \in \Sigma'$, there exists some cone $\sigma \in \Sigma$ such that $\sigma' \subseteq \sigma \subseteq N_{\mathbb{R}}$. This induces an epimorphism of monoids:

$$P_\sigma \to P_{\sigma'}$$

giving a chart for the morphism.

Lemma 7.3.19. *Let Σ' be a refinement of a fan Σ in a lattice N. Then the resulting morphism of log schemes:*

$$X^\dagger_{\Sigma'} \longrightarrow X^\dagger_\Sigma$$

is a logarithmic blow-up, and in particular is log smooth.

Proof. See [Niz06, Theorem 4.7]. □

Chapter 8

Extending Raynaud's method to the semistable case and methods from log geometry

8.1 Extending Raynaud's method to the semistable case

We now return to the problem of Bogomolov-Fu-Tschinkel. Recall that we consider pairs of standard double covers:

$$\pi_i : E_i \longrightarrow \mathbb{P}^1$$

$i = 1, 2$, defined over a number field L and wish to describe the cardinality of the intersection:

$$\pi_1(E_1[\infty]) \cap \pi_2(E_2[\infty]).$$

As before, we can equivalently bound the torsion points of the abelian surface $E_1 \times E_2$ that lie on the curve $X = (\pi_1 \times \pi_2)^{-1}(\Delta_{\mathbb{P}^1})$:

$$X(\bar{L}) \cap (E_1[\infty] \times E_2[\infty]).$$

We would like to weaken Assumption 4.1.2 to say something about this intersection when the elliptic curves E_1 and E_2 have at worst multiplicative reduction (i.e. semistable reduction) at some finite place v of L over a prime $p > 0$. Let R be the maximally unramified extension of $\mathscr{O}_{L,v}$ constructed in Part II, and suppose that E/K is an elliptic curve with semistable reduction. We will be interested in the models $\mathscr{E}$, $\mathscr{C}$ and $\mathscr{W}$ of E defined below; recall that when E has good reduction they coincide:

i) Let $\mathscr{E}/R$ be the Néron model of E/K. Recall that this is an R-group scheme satisfying $\mathscr{E}(R) \cong E(K)$.

ii) Let $\mathscr{C}/R$ denote the minimal proper regular model of E/K. Recall that if $\mathscr{C}^{\mathrm{sm}}/R$ is the smooth locus over R, then this coincides with the Néron model. Note that $\mathscr{C}_k \cong P_{N,k}$ is the standard Néron N-gon where $N = -v(j(E))$ when $N > 0$.

iii) Let $\mathscr{W}/R$ denote the minimal Weierstrass model for E/K. This is the model of E obtained by contracting the (-2)-curves of $\mathscr{C}/R$. Thus, $\mathscr{W}_k$ is the projective rational curve with a single node. $\mathscr{W}$ is regular if and only if $N \leq 1$ in which case it coincides with $\mathscr{C}$. We let $\mathscr{W}^{\mathrm{sm}}$ denote the smooth locus of $\mathscr{W}$ over R. This is an R-group scheme.

Write $\overline{\mathscr{A}} = \mathscr{W}_1 \times_R \mathscr{W}_2$ for the product of the minimal Weierstrass models and $\mathscr{A}$ for the smooth locus over $\mathrm{Spec}(R)$. We then obtain models $\overline{\mathscr{X}} \hookrightarrow \overline{\mathscr{A}}$ and $\mathscr{X} = \overline{\mathscr{X}} \cap \mathscr{A} \hookrightarrow \mathscr{A}$ for $X \hookrightarrow A$ by taking the scheme theoretic closure of X in $\overline{\mathscr{A}}$ and $\mathscr{A}$ respectively. As in the good reduction case, we consider the image of the intersection:

$$\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}_k(k)$$

under reduction modulo p. By precisely the same reasoning as 4.1, there are injections:

$$\begin{array}{ccc} X(\bar{K}) \cap (A[\infty]^{(p')})^{I_K} & \hookrightarrow & \mathscr{X}(R) \cap p\mathscr{A}(R) \\ & \searrow & \downarrow \\ & & \mathscr{X}_k(k) \end{array}$$

where $(A[\infty]^{(p')})^{I_K}$ is the *inertial fixed part* of the coprime-to-p torsion of $A(\bar{K})$, and so we seek to bound the image of this intersection. As we do not assume that A has good reduction, it is no longer true that $A[\infty]^{(p')}$ is unramified (has trivial inertia action). Indeed, if $m > 0$ is an integer, coprime to p, and E_i has bad multiplicative reduction then we have a filtration:

$$\mathscr{E}_i[m]_t \subseteq \mathscr{E}_i[m]_f \subseteq \mathscr{E}_i[m];$$

where these are the *toric* and *finite* parts of the group scheme respectively. We then have that $\mathscr{E}_i[m]_f(R) \cong E_i[m](\bar{K})^{I_K} = E_i[m](K)$ (cf. Remark 6.2.10). Concretely, $E_i[m]$ is of rank m^2 and the toric part $E_i[m]_t$ is of rank m. In general, the finite part $E_i[m]_f$ coincides with the toric part, however if $\mathscr{E}_{i,k}$ has N components and $(N, m) \neq 1$, then $\mathscr{E}_i[m]_f$ will be strictly larger than the toric part. Under the contraction $\mathscr{C}_i \longrightarrow \mathscr{W}_i$ the toric part of $\mathscr{E}_i[m]$ gets sent isomorphically to the finite part of $\mathscr{W}_i^{\mathrm{sm}}[m]$.

Remark 8.1.1. Consider the case when E_1 has good reduction and E_2 has bad multiplicative reduction. Then, it is still true that the common projective torsion points of order coprime-to-p is an unramified set:

$$\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')}) \subseteq \mathbb{P}^1(K)$$

simply by noting that $E_1[\infty]^{(p')}$ is unramified. As π_i are double covers, the set $X(\bar{K}) \cap (E_1[\infty]^{(p')} \times E_2[\infty]^{(p')})$ is unramified, except possibly at the points of order 2.

On the other hand, suppose that E_i both have bad multiplicative reduction and that the standard double covers $\pi_i : E_i \to \mathbb{P}^1$ extend to morphisms $\pi_{i,R} : \mathscr{W}_i \to \mathbb{P}^1_R$. Suppose further that the images $\pi_{1,k}(\gamma_1) \neq \pi_{2,k}(\gamma_2)$ do not coincide where γ_i is the node of $\mathscr{W}_{i,k}$. Then, if $x_i \in E_i[\infty]^{(p')}$ are two coprime-to-p torsion points, not defined over K (i.e. ramified), then we cannot have $\pi_1(x_1) = \pi_2(x_2)$ as these points specialise to γ_1 and γ_2 respectively. Thus, in this case we also have that:

$$\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')}) \subseteq \mathbb{P}^1(K).$$

In light of the above Remark, we make the following assumptions in the case of semistable reduction:

Assumption 8.1.2. *Suppose that we have pairs $(E_1, \pi_1), (E_2, \pi_2)$, where E_1, E_2 are elliptic curves defined over a number field L and π_1, π_2 are standard double covers of $\mathbb{P}^1$, also defined over L. Let v be a finite place of L, unramified over a prime $p > 0$ and write R for the completion of the maximal unramified extension of $\widehat{\mathscr{O}}_{L,v}$ with residue field k and fraction field K. For both curves E_i $(i = 1, 2)$, we assume that one of the below scenarios holds:*

i) If E_i has good reduction at v, then there is an abelian scheme:

$$\mathscr{E} \to \mathrm{Spec}(R)$$

with generic fibre isomorphic to the given elliptic curve E, and there exists an R-morphism:

$$\pi_{i,R} : \mathscr{E}_i \longrightarrow \mathrm{Spec}(R)$$

that is compatible with the involution on $\iota_{i,R} : \mathscr{E}_i \to \mathscr{E}_i$ in the sense that $\pi_{i,R} \circ \iota_{i,R} = \pi_{i,R}$, and that extends the morphism of K-schemes $\pi_i : E_i \to \mathbb{P}^1$.

ii) If E_i has bad reduction at v, then there is a minimal Weierstrass model:

$$\mathscr{W}_i \to \mathrm{Spec}(R)$$

with nodal rational central fibre $\mathscr{W}_k$, and an R-morphism

$$\pi_{i,R} : \mathscr{W}_i \longrightarrow \mathrm{Spec}(R)$$

that extends the morphism of K-schemes $\pi_i : E_i \to \mathbb{P}^1$. Note that the involution $\iota_{i,R} : \mathscr{W}_i^{sm} \to \mathscr{W}_i^{sm}$ extends uniquely to the node. We denote again by $\iota_{i,R}$ this extension and we require that $\pi_{i,R} \circ \iota_{i,R} = \pi_{i,R}$.

iii) The set of branch points in $\mathbb{P}^1$ of the morphisms induced by the morphisms $\pi_{1,R}$ and $\pi_{2,R}$ on the geometric generic fibres are distinct. In addition, the set of branch points in $\mathbb{P}^1$ of the morphisms induced by $\pi_{1,R}$ and $\pi_{2,R}$ on the normalisations of the special fibres are distinct also, and disjoint from the images in $\mathbb{P}^1_k$ of the nodes of the special fibres, which are additionally required to be distinct.

First, we will assume finiteness of the image of:

$$\mathrm{Im}(\mathscr{X}(R) \cap p\mathscr{A}(R) \longrightarrow \mathscr{X}_k(k));$$

and show that, under Assumption 8.1.2, we can still obtain bounds on the cardinality of this image. Note that, an obstruction to obtaining bounds analogous to Corollary 4.1.16 in the present context is that the special fibre of $\mathscr{A}$ is no longer proper, and so one cannot talk about degrees of curves on this surface. On the other hand, the special fibre of the proper model $\overline{\mathscr{A}}$ is no longer non-singular (nor normal), and it is more subtle to describe an intersection theory on this surface.

In the next subsection, we transfer the entire argument based on the ideas in [Ray83-1] to $\mathbb{P}^1_R \times_R \mathbb{P}^1_R$ using the morphism of R-schemes $\pi_{1,R} \times \pi_{2,R}$ and then obtain analogous bounds on the size of the image by working in this projective, R-smooth ambient space. Note that, even though the compactification $\mathscr{A} \subseteq \overline{\mathscr{A}}$ is not smooth, one can show that it is *log smooth* in an appropriate sense. Using this idea, we describe a log Frobenius lifting argument, completely analogous to Theorem 4.1.3, to give finiteness of the image under certain mild restrictions.

8.1.1 Bounds obtained in the case of semistable reduction

Reprising the notation of Part II, we let R_1 denote the truncated ring R/p^2 and use the subscript $_1$ for the base change of an R-scheme to R_1 and subscript $_0$ for base change to k. Throughout this subsection, we will assume that we have pairs of standard double covers (E_i, π_i) satisfying Assumption 8.1.2, and that the image of the intersection:

$$\mathrm{Im}(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k))$$

is finite. We first need to introduce some further notation and definitions. For $i = 1, 2$ we write:

$$[p]_{\mathscr{W}_i} : \mathscr{W}_i \dashrightarrow \mathscr{W}_i$$

for the multiplication-by-p map, which is in general only a rational map defined on $\mathscr{W}_i^{\mathrm{sm}}$. Since the multiplication-by-p map commutes with the involutions, we obtain an induced

rational map, which we will denote by:

$$\widetilde{[p]}_{\mathscr{W}_i} : \mathbb{P}^1_R \dashrightarrow \mathbb{P}^1_R.$$

By taking products, we have rational maps:

$$[p]_{\mathscr{A}} : \overline{\mathscr{A}} \dashrightarrow \overline{\mathscr{A}}$$

and:

$$\widetilde{[p]}_{\mathscr{A}} : \mathbb{P}^1_R \times_R \mathbb{P}^1_R \dashrightarrow \mathbb{P}^1_R \times_R \mathbb{P}^1_R$$

where $\widetilde{[p]}_{\mathscr{A}} = \widetilde{[p]}_{\mathscr{W}_1} \times \widetilde{[p]}_{\mathscr{W}_2}$. Note that, over k, the above rational maps all extend uniquely to morphisms. In particular, we obtain a morphism of k-schemes:

$$\widetilde{[p]}_{\mathscr{A}_0} : \mathbb{P}^1_k \times_k \mathbb{P}^1_k \longrightarrow \mathbb{P}^1_k \times_k \mathbb{P}^1_k.$$

Finally, we denote by $\mathscr{Y}_0 \subset \mathscr{A}_0$ the reduced preimage of $\mathscr{X}_0$ under $[p]_{\mathscr{A}_0}$, which is a curve lying over the reduced preimage $\nabla_0 \subset \mathbb{P}^1_k \times \mathbb{P}^1_k$ of the diagonal $\Delta_0 \subset \mathbb{P}^1_k \times_k \mathbb{P}^1_k$ under $\widetilde{[p]}_{\mathscr{A}_0}$. Let $\mathscr{U} \subseteq \mathbb{P}^1_R \times_R \mathbb{P}^1_R$ denote the open subscheme that is the complement of the images of the node(s) of $\mathscr{W}_i$ under $\pi_{i,R}$ or equivalently:

$$\mathscr{U} = (\pi_{1,R} \times \pi_{2,R})(\mathscr{A}) \subseteq \mathbb{P}^1_R \times_R \mathbb{P}^1_R.$$

Then, by construction, $\widetilde{[p]}_{\mathscr{A}}$ defines an R-morphism on $\mathscr{U}$. Let Δ_1 be the diagonal in $\mathbb{P}^1_{R_1} \times_{R_1} \mathbb{P}^1_{R_1}$ and $\Delta_1^\circ = \Delta_1 \cap \mathscr{U}_1$. Our main finiteness result is the following:

Theorem 8.1.3. *The image of the intersection:*

$$\Delta_1^\circ(R_1) \cap \widetilde{[p]}_{\mathscr{A}_1}(\mathscr{U}_1(R_1)) \longrightarrow \Delta_0^\circ(k)$$

under reduction modulo p is bounded by $2p^3$.

We note immediately the bounds on common projective coprime-to-p torsion points we obtain from the Theorem:

Corollary 8.1.4. *Suppose that we have a pair (E_1, π_1) and (E_2, π_2) of elliptic curves with standard double covers satisfying Assumption 8.1.2, and that the image of the intersection:*

$$\mathrm{Im}(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k))$$

is finite. Then:

$$|\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})| \leq 2p^3 + 2.$$

Proof. By Assumption 8.1.2 and the discussion in Remark 8.1.1, we know that the intersection $\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})$ is unramified. Consider the set:

$$(\pi_1 \times \pi_2)(X(K) \cap (E_1[\infty]^{(p')} \times E_2[\infty]^{(p')})).$$

This differs from the intersection $\pi_1(E_1[\infty]^{(p')}) \cap \pi_2(E_2[\infty]^{(p')})$ by at most 2 points. Indeed, without loss of generality, this only occurs when we have points $\pi_1(x_1) = \pi_2(x_2)$ where $x_1 \in E_1[\infty]^{(p')}$ specialises to a node but, by assumption, $x_2 \in E_2[\infty]^{(p')}$ does not specialise to a node and so is K-rational. Thus, $\pi_1(x_1)$ is K-rational and $x_1 \in E_1[2] \setminus E_1[2]^{I_K}$ which consists of at most 2 points. Now, arguing similarly to 4.1, we have that the intersection $X(K) \cap E_1[\infty]^{(p')} \times E_2[\infty]^{(p')}$ injects into the image of:

$$\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k).$$

Moreover, by commutativity of the diagram:

$$\begin{array}{ccc} \mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) & \longrightarrow & \mathscr{X}_0(k) \\ \downarrow{\scriptstyle \pi_{1,R_1} \times \pi_{2,R_1}} & & \downarrow{\scriptstyle \pi_{1,k} \times \pi_{2,k}} \\ \Delta_1^\circ(R_1) \cap \widetilde{[p]}_{\mathscr{A}_1}(\mathscr{U}_1(R_1)) & \longrightarrow & \Delta_0^\circ(k) \end{array}$$

we have that $(\pi_1 \times \pi_2)(X(K) \cap (E_1[\infty]^{(p')} \times E_2[\infty]^{(p')}))$ injects into the image of:

$$\Delta_1^\circ(R_1) \cap \widetilde{[p]}_{\mathscr{A}_1}(\mathscr{U}_1(R_1)) \longrightarrow \Delta_0^\circ(k). \qquad \square$$

Before we supply the proof of the theorem, we note the following:

Lemma 8.1.5. *The curve ∇_0 is nonsingular.*

Proof. Let $\widetilde{\mathscr{W}_{i,k}}$ be the normalisation of $\mathscr{W}_{i,k}$ and write:

$$\tilde{\pi}_{i,k} : \widetilde{\mathscr{W}_{i,k}} \longrightarrow \mathbb{P}^1_k$$

for the induced double coverings. By Assumption 8.1.2 (iii), the preimage $(\tilde{\pi}_{1,k} \times \tilde{\pi}_{2,k})^{-1}(\Delta_0)$ is the normalisation $\widetilde{\mathscr{X}_0}$ of the curve $\overline{\mathscr{X}}_0$. Now, the morphisms $\widetilde{\mathscr{W}_{i,k}} \to \widetilde{\mathscr{W}_{i,k}}$ induced by $[p]_{\mathscr{W}_{i,k}} : \mathscr{W}_{i,k} \to \mathscr{W}_{i,k}$ each factor as a purely inseparable map, followed by an étale map. Thus, the reduced preimage $\widetilde{\mathscr{Y}_0}$ of $\widetilde{\mathscr{X}_0}$ under the product of these maps is also non-singular (it is some geometric Frobenius twist of an étale cover of $\widetilde{\mathscr{X}_0}$ and in fact is the normalisation of $\overline{\mathscr{Y}}_0$; the closure of $\mathscr{Y}_0$ in $\overline{\mathscr{A}}_0$). Now ∇_0 is a quotient of $\widetilde{\mathscr{Y}_0}$ by a $\mathbb{Z}/2 \times \mathbb{Z}/2$-action, with at most $\mathbb{Z}/2$ stabilisers, hence non-singular. $\square$

Remark 8.1.6. Consider the following projective model:

$$\mathscr{W} : y^2 = x^3 + x^2 + p \subseteq \mathbb{P}^2_R.$$

When $p > 2$, $\mathscr{W}_k$ is the nodal rational curve with node given by $\gamma = (0,0) \in \mathbb{P}^2_k$. One obtains a standard double cover by considering:

$$\begin{aligned} \pi_R : \mathscr{W} &\longrightarrow \mathbb{P}^1_R; \\ (x,y) &\longmapsto x. \end{aligned}$$

By analysing the *division polynomials* [Sil09, Ex. 3.7, p. 105] associated to $E = \mathscr{W}_K$, one obtains iterative formulae for the multiplication-by-p map:

$$\begin{aligned} [p]_{\mathscr{W}} : \mathscr{W} &\dashrightarrow \mathscr{W}; \\ (x,y) &\mapsto \left(\frac{\phi_p(x)}{\psi^2_p(x)}, \frac{\omega_p(x,y)}{\psi^3_p(x,y)} \right) \end{aligned}$$

where $\phi_p(x), \psi^2_p(x) \in R[x]$ and $\omega_p(x,y), \psi^3_p(x,y) \in R[x,y]$. Note that:

$$\begin{aligned} \phi_p(x) &= x^{p^2} + ... \\ \psi^2_p(x) &= p^2 x^{p^2-1} + ... \end{aligned}$$

One can see that this morphism does not extend to the node $\gamma = (0,0)$ by noting that, even though $\phi_p(x), \psi^2_p(x)$ are coprime in $K[x]$, their images modulo p (which we denote using $\widetilde{\ }$) have a common factor. Indeed, one can calculate that:

$$\widetilde{\psi}^2_p(x) \mid \widetilde{\phi}_p(x) \quad \text{and} \quad \frac{\widetilde{\phi}_p(x)}{\widetilde{\psi}^2_p(x)} = x^p.$$

Thus, if one considers the associated Lattè's map in terms of projective coordinates $[T_0 : T_1] \in \mathbb{P}^1_R$, there exists homogeneous polynomials $F, G \in R[T_0, T_1]$ of degree p^2 such that $F(1,x) = \phi_p(x)$ and $G(1,x) = x\psi^2_p(x)$ giving the expression:

$$\begin{aligned} \overline{[p]}_{\mathscr{W}} : \mathbb{P}^1_R &\dashrightarrow \mathbb{P}^1_R; \\ [T_0 : T_1] &\mapsto [F(T_0,T_1) : G(T_0,T_1)]. \end{aligned}$$

F, G are coprime in $K[T_0, T_1]$, but modulo p we have that:

$$[\widetilde{F}(T_0,T_1) : \widetilde{G}(T_0,T_1)] = [T_0^p : T_1^p].$$

Proof of Theorem 8.1.3. First, we note that the image is finite by the commutativity of

the diagram, the finiteness assumption on the top row and the surjectivity of the vertical arrows. In essence, we replicate Example 4.1.13, but instead work with bihomogeneous polynomials in $\mathbb{P}^1_R \times_R \mathbb{P}^1_R$. As the k-differential of $\widetilde{[p]}_{\mathscr{A}_0}$ is zero and $\mathscr{U}_1$ is a smooth R_1-scheme we may apply Prop. 4.1.10 to the morphism $\widetilde{[p]}_{\mathscr{A}_1} : \mathscr{U}_1 \longrightarrow \mathscr{U}_1$ and the curve $\Delta_1^\circ \hookrightarrow \mathscr{U}_1$. As in the Proposition, we have the following diagram on points:

$$\begin{array}{ccc} (\mathscr{U}_1, \nabla_0^\circ)(R_1) & \longrightarrow & (\mathscr{U}_1, \Delta_0^\circ)(R_1) \\ \downarrow & \overset{\exists!}{\nearrow} & \downarrow \\ \nabla_0^\circ(k) & \longrightarrow & \Delta_0^\circ(k) \end{array}$$

where ∇_0° is the reduced preimage of Δ_0° under $\widetilde{[p]}_{\mathscr{A}_0}$, and the top row consists of R_1-points of $\mathscr{U}_1$ which specialise to ∇_0° and Δ_0° respectively. Let $([T_0 : T_1], [S_0 : S_1])$ be bihomogeneous coordinates for $\mathbb{P}^1_{R_1} \times_{R_1} \mathbb{P}^1_{R_1}$. Then we may write $\Delta_1 = \{f_1 = 0\}$ for the bihomogeneous polynomial $f_1 = T_0S_1 - T_1S_0$ of bidegree $(1,1)$. We may also write the induced maps of $\mathscr{W}_i$ in terms of bihomogeneous polynomials with coefficients in R_1:

$$\begin{aligned} [p]_{\mathscr{W}_{1,R_1}}([T_0 : T_1]) &= [F(T_0, T_1) : G(T_0, T_1)]; \\ [p]_{\mathscr{W}_{2,R_1}}([S_0 : S_1]) &= [F'(S_0, S_1) : G'(S_0, S_1)] \end{aligned}$$

where F, G have bidegree $(p^2, 0)$ and F', G' have bidegree $(0, p^2)$. We use the subscript $_0$ to denote the reduction mod p of these polynomials. We assume that, without loss of generality, $\mathscr{W}_1$ has bad reduction, and so $\mathscr{W}_{1,k}^{\mathrm{sm}} \cong \mathbb{G}_{m,k}$. Thus, $[p]_{\mathscr{W}_{1,k}}$ drops to degree p on $\mathbb{G}_{m,k}$. Consequently, F_0 and G_0 have a common factor of bidegree $(p^2 - p, 0)$. In the case when $\mathscr{W}_{2,R_1}$ has good reduction, F_0' and G_0' are coprime. The curve ∇_0 is defined to be the reduced preimage of the pullback curve:

$$\{F_0G_0' - F_0'G_0 = 0\} \subseteq \mathbb{P}^1_k \times_k \mathbb{P}^1_k.$$

As the differential of both $[p]_{\mathscr{W}_{i,k}}$ is zero, there is some bihomogeneous polynomial g_0 such that $g_0^p = F_0G_0' - F_0'G_0$. Then, $\nabla_0 = \{g_0 = 0\}$ and we may pick some lifting $\nabla_1 = \{g_1 = 0\}$ such that bidegree(g_1) = bidegree(g_0). By Lemma 8.1.5, ∇_1 is smooth and so the specialisation map $\nabla_1(R_1) \longrightarrow \nabla_0(k)$ is surjective. Thus, we have that:

$$\Delta_1^\circ(R_1) \cap \widetilde{[p]}_{\mathscr{A}_1}(\mathscr{U}_1(R_1)) = \Delta_1^\circ(R_1) \cap \widetilde{[p]}_{\mathscr{A}_1}(\nabla_1(R_1)).$$

Now, as g_1^p and $F_1G_1' - F_1'G_1$ are congruent modulo p, there is some bihomogeneous polynomial h_1 such that:

$$F_1G_1' - F_1'G_1 - g_1^p = p \cdot h_1.$$

From this expression it is clear that h_1 has bidegree (p^2, p^2). Suppose that $b_1 \in \Delta_1^\circ(R_1) \cap$

$\widetilde{[p]}_{\mathscr{A}_1}(\nabla_1(R_1))$. Then $f_1(b_1) = 0$ and there exists some $a_1 \in \nabla_1(R_1)$ (i.e. $g_1(a_1) = 0$) such that $\widetilde{[p]}_{\mathscr{A}_1}(a_1) = b_1$. This implies that $h_0(a_0) = 0$ and thus, the set of points b_0 that arise this way comprise the set:

$$\widetilde{[p]}_{\mathscr{A}_0}\left(\{b_0 \in \mathscr{U}_0(k) \mid h_0(a_0) = 0 \text{ and } f(a_0) = 0\}\right).$$

By the finiteness assumption, the bihomogeneous polynomials h_0 and f_0 have no common component and so a bound on the cardinality of the above set is given by the intersection number:

$$(p, p) \cdot (p^2, p^2) = 2p^3.$$

□

8.1.2 Finiteness and methods from log geometry

Extending the multiplication-by-p map to proper models

We will now discuss the finiteness of the image:

$$\mathrm{Im}(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k))$$

as was assumed in the previous subsection.

Theorem 8.1.7. *Suppose that (E_1, π_1) and (E_2, π_2) are two elliptic curves together with standard projections defined over a number field L. Assume that E_1 has bad multiplicative reduction with the standard projection extending to the minimal Weierstrass model:*

$$\begin{array}{ccc} \mathscr{W}_1 & \xrightarrow{\pi_{1,R}} & \mathbb{P}^1_R \\ & \searrow \quad \swarrow & \\ & \mathrm{Spec}(R) & \end{array}$$

and that E_2 has good ordinary reduction with standard projection extending to the Néron model:

$$\begin{array}{ccc} \mathscr{E}_2 & \xrightarrow{\pi_{2,R}} & \mathbb{P}^1_R\,. \\ & \searrow \quad \swarrow & \\ & \mathrm{Spec}(R) & \end{array}$$

We further assume that the elliptic curve E_1 over K has a Tate parameter $q \in K^*$ that is a p-th power of a uniformiser in K. Then Assumption 8.1.2 implies the image:

$$\mathrm{Im}(\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k))$$

is finite.

To prove Theorem 8.1.7 we will follow the structure of Raynaud's argument illustrated in Lemma 4.1.20 and generalise it to log smooth curves. The proof requires a number of preparations. The non-liftability of the Frobenius used in Raynaud's argument only holds if one works with proper curves, so as a first step, we will extend the multiplication-by-p map for certain elliptic curves with bad multiplicative reduction to some proper models of these curves over $\mathrm{Spec}(R)$; this will justify the somewhat technical assumption that the Tate parameter q above is a p-th power of a uniformiser.

Definition 8.1.8. An *admissible factorisation* of the multiplication-by-p map on a projective model $\mathscr{E} \to \mathrm{Spec}(R)$ of an elliptic curve E/K consists of the following data:

i) An R-morphism $\varphi\colon \mathscr{E} \to \mathscr{E}''$ whose restriction to the generic fibre is the multiplication-by-p map $[p]_E\colon E \to E$.

ii) A flat, projective R-scheme $\mathscr{E}' \to \mathrm{Spec}(R)$ with R-morphisms

$$\mathscr{E} \xrightarrow{\alpha_{\mathscr{E}}} \mathscr{E}' \xrightarrow{\beta_{\mathscr{E}}} \mathscr{E}''$$

such that $\varphi = \beta_{\mathscr{E}} \circ \alpha_{\mathscr{E}}$, the morphism $\alpha_{\mathscr{E},0}\colon \mathscr{E}_0 \to \mathscr{F}_0$ induced by restricting α to the special fibres is the relative Frobenius morphism (so that $\mathscr{F}_0$ is the Frobenius twist of $\mathscr{E}_0$), and that the morphism $\beta_{\mathscr{E}}$ is étale.

Proposition 8.1.9. *Let $\mathscr{C}/R$ be the minimal proper regular model of an elliptic curve E/K. Suppose that either the special fibre $\mathscr{C}_k$ is an ordinary elliptic curve, or that it is a Néron N-gon with p dividing N. Then E admits an admissible factorisation.*

Proof. In the case when $\mathscr{C}_k$ is a nonsingular ordinary elliptic, this has already been observed in 4.1.3. Indeed, $\mathscr{C}$ coincides with the Néron model $\mathscr{E}/R$ and we set $\mathscr{E}' = \mathscr{E}/\mathscr{E}[p]^\circ$. Then if we set $\alpha_{\mathscr{E}} : \mathscr{E} \to \mathscr{E}'$ to be the quotient, one obtains a factorisation:

$$[p]_{\mathscr{E}} : \mathscr{E} \xrightarrow{\alpha_{\mathscr{E}}} \mathscr{E}' \xrightarrow{\beta_{\mathscr{E}}} \mathscr{E}$$

where $\beta_{\mathscr{E}}$ is the separable isogeny dual to $\alpha_{\mathscr{E}}$. Consider now the case when $\mathscr{C}_k = P_{N,k}$ is a Néron N-gon with $N = p \cdot m$ for some integer $m > 0$. The main point is that, since p divides N, the kernel of multiplication-by-p, $\mathscr{E}[p]$ on the Néron model $\mathscr{E} \subseteq \mathscr{C}$, is a *finite flat* R-group scheme that acts on $\mathscr{C}$ (cf. 6.2.3). Then by [Ray66], we obtain a quotient $\mathscr{C}'' := \mathscr{C}/\mathscr{E}[p]$ that is an integral, projective, flat R-scheme (by part (i) of the Theorem in loc. cit.), and the quotient morphism $\mathscr{C} \to \mathscr{C}''$ restricts to the multiplication-by p on the generic fibre. Moreover, the connected-étale sequence of $\mathscr{E}[p]$ is given by:

$$0 \longrightarrow \mu_{p,R} \longrightarrow \mathscr{E}[p] \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

by considering the exact sequence of G_K-modules in Prop. 6.1.15 for example. Letting $\mathscr{C}' = \mathscr{C}/\mu_{p,R}$ we then obtained the desired factorisation:

$$\mathscr{C} \longrightarrow \mathscr{C}' \longrightarrow \mathscr{C}''.$$

□

The geometry of preimages of the diagonal under certain covering maps

We work over an algebraically closed field k of characteristic $p > 2$ and consider:

i) A nodal rational cubic C_0/k with a degree 2 covering $\tau\colon C_0 \to \mathbb{P}^1$. Let $\alpha_0 : \mathbb{P}^1 \cong \tilde{C}_0 \to C_0$ be the normalisation morphism. Then the composition $\widetilde{\tau} = \alpha_0 \circ \tau : \mathbb{P}^1 \to \mathbb{P}^1$ is branched in two points which we may take to be $0, \infty \in \mathbb{P}^1$. Let $\beta\colon P_{N,k} \to C_0$ be the étale, degree N cover of C_0 by the Néron N-gon.

ii) An elliptic curve E_0 over k with a standard double covering $\pi\colon E_0 \to \mathbb{P}^1$ branched in four points a, b, c, d. We assume the branch loci $\{a, b, c, d\}$ and $\{0, \infty\}$ are disjoint. Let $\gamma \in C_0$ denote the singular point. We also assume that:

$$\tau(\gamma) \notin \{a, b, c, d\}.$$

Let $\Delta_0 \subset \mathbb{P}^1 \times \mathbb{P}^1$ be the diagonal. We wish to understand the geometry of the preimage curve:

$$\Gamma = \left((\gamma \circ \tau) \times \pi\right)^{-1}(\Delta_0) \subset P_{N,k} \times E_0.$$

This can be reduced to determining the geometry of:

$$\overline{\Gamma} = \left(\widetilde{\tau} \times \pi\right)^{-1}(\Delta_0) \subset \widetilde{C}_0 \times E_0.$$

Proposition 8.1.10. *The curve Γ is a connected curve with N connected components, each of which is a non-singular curve of genus 3. The nodes of Γ are precisely the pairwise, consecutive, transverse intersections of the components.*

Proof. It is easy to see that, since the sets of branch points for $\widetilde{\tau}$ and π are disjoint, the curve $\overline{\Gamma}$ is non-singular and irreducible. Indeed, non-singularity can be checked étale-locally, and irreducibility holds because, again looking étale-locally one sees that, if $\overline{\Gamma}$ were reducible, it would split into two components permuted by the covering group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, but again since the sets of branch points for $\widetilde{\tau}$ and π are disjoint, a local argument shows that no subgroup $\mathbb{Z}/2\mathbb{Z}$ of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ acts trivially on the set of components. As $\overline{\Gamma}$ is a double cover of both $\widetilde{C}_0$ and E_0 we see that:

$$\overline{\Gamma} \sim 2(\widetilde{C}_0 + E_0) \in \mathrm{Div}(\widetilde{C}_0 \times E_0).$$

The canonical class K_S of $S = \widetilde{C}_0 \times E_0$ being $-2\widetilde{C}_0$, we can calculate the genus of $\overline{\Gamma}$:

$$g(\overline{\Gamma}) = \frac{1}{2}\overline{\Gamma} \cdot (\overline{\Gamma} + K_S) + 1 = 3$$

by adjunction. Let $\{\nu_1, \nu_2\} = \alpha_0^{-1}(\gamma)$. Since we assumed that $\tau(\gamma) \notin \{a, b, c, d\}$, it follows that $\overline{\Gamma}$ intersects $\{\nu_1\} \times E_0$ and $\{\nu_2\} \times E_0$ transversely in S. □

The connection to torsion points

Suppose now that we are given two elliptic curves E_1, E_2 over K with standard projections π_i as in Theorem 8.1.7. Then, with the hypotheses and notation of 8.1.2, the minimal proper regular model $\mathscr{C}_1 \to \mathrm{Spec}(R)$ of E_1 has special fibre given by a Néron p-gon, whereas $\mathscr{E}_2 \to \mathrm{Spec}(R)$ has special fibre given by an ordinary elliptic curve. Using Proposition 8.1.9, we produce admissible factorisations:

$$\mathscr{C}_1 \xrightarrow{\alpha_{\mathscr{W}_1}} \mathscr{C}_1' \xrightarrow{\beta_{\mathscr{W}_1}} \mathscr{W}_1;$$

$$\mathscr{E}_2 \xrightarrow{\alpha_{\mathscr{E}_2}} \mathscr{E}_2' \xrightarrow{\beta_{\mathscr{E}_2}} \mathscr{E}_2;$$

where $\mathscr{W}_1$ is the minimal Weierstrass model of E_1. We set:

i) $\overline{\mathscr{B}} = \mathscr{C}_1 \times_R \mathscr{E}_2$, $\overline{\mathscr{B}}' = \mathscr{C}_1' \times_R \mathscr{E}_2'$, $\overline{\mathscr{A}} = \mathscr{W}_1 \times_R \mathscr{E}_2$.

ii) $\alpha = \alpha_{\mathscr{W}_1} \times_R \alpha_{\mathscr{E}_2}$, $\beta = \beta_{\mathscr{W}_1} \times_R \beta_{\mathscr{E}_2}$.

to obtain a composition of morphisms of R-schemes:

$$\overline{\mathscr{B}} \xrightarrow{\alpha} \overline{\mathscr{B}}' \xrightarrow{\beta} \overline{\mathscr{A}}$$

where $\beta \circ \alpha$ restricted to the generic fibre is the multiplication-by-p map on the abelian surface $E_1 \times E_2$, β is étale, and α restricts to the relative Frobenius on the special fibre of $\overline{\mathscr{B}}$. By the assumptions made in Theorem 8.1.7, we are also given standard double covers $\pi_i : E_i \to \mathbb{P}^1_K$, $i = 1, 2$, extending to double covers:

$$\pi_{1,R} : \mathscr{W}_1 \to \mathbb{P}^1_R \quad \text{and} \quad \pi_{2,R} : \mathscr{E}_2 \to \mathbb{P}^1_R.$$

Writing $\Delta_R \subset \mathbb{P}^1_R \times \mathbb{P}^1_R$ for the diagonal, we take $\overline{\mathscr{X}} = (\pi_{1.R} \times \pi_{2,R})^{-1}(\Delta_R) \hookrightarrow \overline{\mathscr{A}}$. We then define:

$$\overline{\mathscr{Z}} := \beta^{-1}(\overline{\mathscr{X}}) \subseteq \overline{\mathscr{B}}'.$$

Furthermore, we write $\overline{\mathscr{Y}_0}$ for the *reduced* preimage of $\overline{\mathscr{Z}}_0$ under $\alpha_0 \colon \mathscr{A}_0 \to \mathscr{B}_0$. (Again, we denote $R_n := R/p^{n+1}R$, and use a subscript $_n$ to denote the base change of an R-scheme

to R_n.) $\mathscr{C}_1^{\mathrm{sm}} = \mathscr{E}_1$ is the Néron model of E_1 and we write $\mathscr{E}_1' = \mathscr{E}_1/\mu_{p,R} = (\mathscr{C}_1')^{\mathrm{sm}}$. Then we obtain the abelian R-schemes:

$$\mathscr{B} = \mathscr{E}_1 \times_R \mathscr{E}_2,\ \mathscr{B}' = \mathscr{E}_1' \times_R \mathscr{E}_2',\ \mathscr{A} = \mathscr{W}_1^{\mathrm{sm}} \times_R \mathscr{E}_2.$$

Let $\mathscr{X} = \overline{\mathscr{X}} \cap \mathscr{A}$ and $\mathscr{Z} = \overline{\mathscr{Z}} \cap \mathscr{B}'$ denote the corresponding curves in $\mathscr{A}$ and $\mathscr{B}'$ respectively. We would like to show the finiteness of the image of:

$$\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1) \longrightarrow \mathscr{X}_0(k).$$

Let $\Sigma = (\mathscr{B}_1, \mathscr{Y}_0)(R_1)$ denote the set of points in $\mathscr{B}_1(R_1)$ that specialise to the curve $\mathscr{Y}_0 = \overline{\mathscr{Y}_0} \cap \mathscr{B}_0 \subseteq \mathscr{B}_0$. We also write $\Lambda = \alpha_1(\Sigma) \subseteq \mathscr{B}_1'(R_1)$. Then, by construction:

$$p\Sigma = \beta_1(\Lambda) = (\mathscr{A}_1, \mathscr{X}_0)(R_1) \cap p\mathscr{A}_1(R_1)$$

and so:

Lemma 8.1.11. *If the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is finite, then the image of $\mathscr{X}_1(R_1) \cap p\mathscr{A}_1(R_1)$ in $\mathscr{X}_0(k)$ is finite.*

In Theorem 8.1.7 we assumed that the elliptic curve E_1 over K has Tate parameter $q \in K^*$ that is a p-th power of a uniformiser $q' \in K$: $q = (q')^p$. This assumption is essential for the following density statement:

Proposition 8.1.12. *If the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is infinite, then this image is infinite in every irreducible component of $\overline{\mathscr{Z}}_0$.*

Proof. This follows from the rotational symmetry of the situation. By Prop. 6.1.15, the short exact sequence of G_K-modules:

$$0 \longrightarrow \mu_p(\bar{K}) \longrightarrow E_1[p](\bar{K}) \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

is split. On the Néron model $\mathscr{E}_1$, this corresponds to the existence of an étale subgroup scheme $\mathscr{E}_1[p]^{\text{ét}} \subseteq \mathscr{E}_1$, where the p sections $\mathscr{E}_1[p]^{\text{ét}}(R)$ respectively pass through the p components of the special fibre $\mathscr{E}_{1,k} \cong \mathbb{G}_{m,k} \times \mathbb{Z}/p\mathbb{Z}$. Restricting to R_1 and taking the image of these sections under $\alpha_1 : \overline{\mathscr{B}}_1 \to \overline{\mathscr{B}}_1'$, we obtain an action on $\mathscr{B}_1'$ by translation by $\mathscr{E}_1[p]^{\text{ét}} \times \{\mathrm{Id}\}$. If the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is infinite, then clearly it is dense on some component of $D_0 \subseteq \overline{\mathscr{Z}}_0$. However, for any other component of $\overline{\mathscr{Z}}_0$, there are sections $\sigma_1 \in \alpha_1(\mathscr{E}_1[p]^{\text{ét}} \times \{\mathrm{Id}\})$ and $x_1 \in \mathscr{Z}_1(R_1)$ such that $x_0 \in D_0(k)$ and $\sigma_1 + x_1$ specialises to this component. □

Log deformation theory and Frobenius liftings

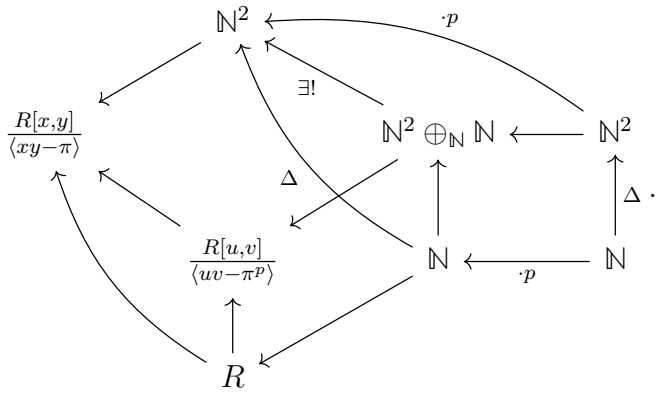
We now define log structures on the models of curves and abelian varieties we have constructed. Recall the construction in Example 7.3.13. We give $\mathrm{Spec}(R)$ the divisorial log structure and then define the morphism of $R^\dagger$-log schemes:

$$F : \mathscr{U}^\dagger \longrightarrow \mathscr{V}^\dagger;$$

where the underlying morphism of schemes is given by:

$$F : \mathscr{U} = \mathrm{Spec}\left(\frac{R[x,y]}{\langle xy-\pi\rangle}\right) \longrightarrow \mathrm{Spec}\left(\frac{R[u,v]}{\langle uv-\pi^p\rangle}\right) = \mathscr{V};$$
$$(x,y) \longmapsto (x^p, y^p)$$

and the log structure is given by the chart of monoids:



As discussed, $\mathscr{U}^\dagger$ and $\mathscr{V}^\dagger$ are both log smooth over $\mathrm{Spec}(R)^\dagger$ and the restriction of F to the standard log point $\mathrm{Spec}(k)^\dagger$ is given by the log relative Frobenius $F_0 : \mathscr{U}_k^\dagger \to \mathscr{V}_k^\dagger$. As the curve E_2 has good reduction, the proper regular model $\mathscr{E}_2/R$ is smooth and so continues to be log smooth with the trivial log structure. On the other hand, the minimal proper regular model $\mathscr{C}_1$ of E_1 fails to be smooth at the p nodes of $\mathscr{C}_k$. For each such node, there is an étale neighbourhood $\mathscr{U} \to \mathscr{C}$. We define the log structure on $\mathscr{C}^\dagger$ by taking an étale cover by p copies of $\mathscr{U}$ and then taking the trivial log structure on the smooth locus of $\mathscr{C}_1$ over R.

Similarly, the images of the nodes of $\mathscr{C}_k$ in $\mathscr{C}' = \mathscr{C}/\mu_{p,R}$ correspond to p cyclic quotient singularities of the arithmetic surface, and we can define a log structure as above using the charts $\mathscr{V} \to \mathscr{C}'$ in neighbourhoods of these singular points. The morphism of log schemes $F : \mathscr{U}^\dagger \to \mathscr{V}^\dagger$ then furnishes the quotient $\mathscr{C} \to \mathscr{C}'$ with the structure of a morphism of log schemes. We take the product log structure on $\overline{\mathscr{B}}^\dagger$ and $(\overline{\mathscr{B}}')^\dagger$, and as the morphism $\overline{\mathscr{B}}' \to \overline{\mathscr{A}}$ is finite étale, we also obtain a log structure for $\overline{\mathscr{A}}$. Finally, we take $\overline{\mathscr{Z}}$ and $\overline{\mathscr{X}}$ to have the respective pullback log structures as closed subschemes. Note that,

by the description of the étale charts, all log schemes are log smooth over $\mathrm{Spec}(R)^\dagger$.

Consider the reduced preimage curve $\overline{\mathscr{Y}_0}^\dagger \hookrightarrow (\overline{\mathscr{B}}'_0)^\dagger$ (again with the pullback log-structure). Étale-locally around the nodes of $\overline{\mathscr{Y}_0}^\dagger$, there is a chart given by $\mathscr{U}_0^\dagger$ by construction. Thus, $\overline{\mathscr{Y}_0}^\dagger \hookrightarrow (\overline{\mathscr{B}}'_0)^\dagger$ is log smooth and we may pick an abstract log smooth lifting:

$$\overline{\mathscr{Y}_1}^\dagger \longrightarrow \mathrm{Spec}(R_1)^\dagger$$

by Prop. 7.3.11. We will show that there exists a lifting $\overline{\mathscr{Y}_1}^\dagger \to \overline{\mathscr{Z}_1}^\dagger$ of the log relative Frobenius on $\overline{\mathscr{Y}_0}^\dagger$ when the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is infinite. As a first step we note that:

Lemma 8.1.13. *There exists a canonical morphism of log schemes:*

$$\begin{array}{ccccc}
\overline{\mathscr{Y}_1}^\dagger & & \overset{\exists g_1}{\longrightarrow} & & \\
\uparrow & & \overline{\mathscr{B}_1}^\dagger & \xrightarrow[\alpha_1]{} & (\overline{\mathscr{B}_1}')^\dagger \\
\uparrow & & \uparrow & & \uparrow \\
\overline{\mathscr{Y}_0}^\dagger & \hookrightarrow & \overline{\mathscr{B}_0}^\dagger & \xrightarrow[\alpha_0]{} & (\overline{\mathscr{B}_0}')^\dagger
\end{array}$$

such that the diagram commutes, and satisfying $g_1(\mathscr{Y}_1(R_1)) = \Lambda$ where $\mathscr{Y}_1$ is the smooth locus of $\overline{\mathscr{Y}_1}$ over R_1.

Proof. We wish to mimic Lemma 4.1.20 in the present log setting. As $\overline{\mathscr{B}}_1^\dagger \to \mathrm{Spec}(R_1)^\dagger$ is log smooth, applying Prop. 7.3.12, there is a lifting:

$$\begin{array}{ccc}
 & & \overline{\mathscr{B}}_0^\dagger \\
 & \nearrow & \downarrow \\
\overline{\mathscr{Y}}_0^\dagger & \longrightarrow & \overline{\mathscr{B}}_1^\dagger \\
\downarrow & \overset{\exists h_1}{\nearrow} & \downarrow \\
\overline{\mathscr{Y}}_1^\dagger & \longrightarrow & \mathrm{Spec}(R_1)^\dagger
\end{array}$$

that exists *étale-locally*. Two such lifts differ by a derivation [Ser06, Section 1.1], but since the differential of $\alpha_0 \colon \overline{\mathscr{B}}_0 \to \overline{\mathscr{B}}'_0$ is zero, we get a well-defined map to $\overline{\mathscr{B}}'_1$ if we post-compose with α_1. Since these morphisms are defined étale-locally on the source, these local lifts glue to a morphism:

$$g_1 : \overline{\mathscr{Y}}_1^\dagger \longrightarrow (\overline{\mathscr{B}}'_1)^\dagger.$$

The property $g_1(\mathscr{Y}_1(R_1)) = \Lambda$ can be seen from the local construction. Indeed, the inclusion $g_1(\mathscr{Y}_1(R_1)) \subseteq \Lambda$ is clear. To see the reverse inclusion, if we take $\alpha_1(x_1) \in \Lambda$, then $x_0 \in \mathscr{Y}_0$. As we are in the smooth locus, we may take some $w_1 \in \mathscr{Y}_1(R_1)$ such that $w_0 = x_0$. By altering the local lifting h_1 by a translation, we may assume that $h_1(w_1) = g_1(x_1)$. □

Lemma 8.1.14. *Suppose that the assumptions of Proposition 8.1.12 are satisfied, in particular, the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is infinite. Then, the morphism α_1 induces a first order infinitesimal lifting of the log relative Frobenius:*

$$u_1 : \overline{\mathscr{Y}}_1^{\dagger} \longrightarrow \overline{\mathscr{Z}}_1^{\dagger}$$

Proof. We wish to show that the morphism g_1 of Lemma 8.1.13 factors through the closed subscheme $\overline{\mathscr{Z}}_1^{\dagger}$ in $(\overline{\mathscr{B}}_1')^{\dagger}$. We denote by $\overline{\mathscr{Y}}_1'$ the fibre product:

$$\begin{array}{ccc} \overline{\mathscr{Y}}_1' & \longrightarrow & \overline{\mathscr{Y}}_1 \\ \downarrow & & \downarrow g_1 \\ \overline{\mathscr{Z}}_1 & \hookrightarrow & \overline{\mathscr{B}}_1' \end{array}.$$

This is a closed subscheme of $\overline{\mathscr{Y}}_1$. We will show that in fact $\overline{\mathscr{Y}}_1 = \overline{\mathscr{Y}}_1'$ and so the first projection gives the desired lifting. Since we assume that the image of $\Lambda \cap \mathscr{Z}_1(R_1)$ in $\mathscr{Z}_0(k)$ is infinite, this image is infinite in every irreducible component of $\overline{\mathscr{Z}}_0$ by Proposition 8.1.12. Therefore, there is a set of sections in $\overline{\mathscr{Y}}_1'(R_1)$ with Zariski dense image in every irreducible component of the special fibre of $\overline{\mathscr{Z}}_0$. Then $\overline{\mathscr{Y}}_1'$ is schematically dense in $\overline{\mathscr{Y}}_1$ by [EGA, IV, 11.10.9]; and so these schemes are equal. □

We conclude by showing that such a log smooth curve cannot admit a lifting of the log relative Frobenius.

Lemma 8.1.15. *Suppose $C_1^{\dagger} \to \mathrm{Spec}(R_1)^{\dagger}$ is a log smooth curve. Assume that there is a non-singular component $C_0' \subseteq C_0$ for which:*

$$\Omega^1_{C_0^{\dagger}/k^{\dagger}}|_{C_0'} \cong \omega_{C_0'}(x_1 + ... + x_r)$$

has positive degree on C_0', where $x_1, ..., x_r$ are either log marked points of C_0', or nodes of C_0. Let $F_{C_0^{\dagger}/k^{\dagger}} : C_0^{\dagger} \to (C_0^{\dagger})^{(p)}$ denote the log relative Frobenius. Then there exists no morphism of log schemes $F_1 : C_1^{\dagger} \longrightarrow D_1^{\dagger}$ that restricts to $F_{C_0^{\dagger}/k^{\dagger}}$ (where $D_1^{\dagger}/R$ is some log smooth curve specialising to $(C_0^{\dagger})^{(p)}/k^{\dagger}$).

Proof. We argue similarly to [Ray83-2, Lemma I.5.4]. First, since $C_1^{\dagger} \to \mathrm{Spec}(R_1)^{\dagger}$ and $D_1^{\dagger} \to \mathrm{Spec}(R_1)^{\dagger}$ are log smooth curves, the sheaves of log differentials $\Omega^1_{C_1^{\dagger}/R_1^{\dagger}}$ and $\Omega^1_{D_1^{\dagger}/R_1^{\dagger}}$ are locally free of rank 1 and we have a natural functorial morphism of these lines bundles:

$$F_1^* : F_1^*(\Omega^1_{D_1^{\dagger}/R_1^{\dagger}}) \to \Omega^1_{C_1^{\dagger}/R_1^{\dagger}};$$

(cf. [Gr11, p. 115-116]). Since the differential of F_0^* is zero, the morphism of line bundles

F_1^* factors through $p\Omega^1_{C^\dagger/R_1^\dagger}$. Dividing by p, we obtain a morphism:

$$\tau' \colon F_0^*(\Omega^1_{D_0^\dagger/k^\dagger}) \longrightarrow \Omega^1_{C_0^\dagger/k^\dagger};$$

which corresponds to a morphism $\tau \colon \Omega^1_{D_0^\dagger/k^\dagger} \longrightarrow (F_0)_*(\Omega^1_{C_0^\dagger/k^\dagger})$ by adjunction. On the other hand, we have the log Cartier operator:

$$\mathscr{C} : (F_0)_*(\Omega^1_{C_0^\dagger/k^\dagger}) \longrightarrow \Omega^1_{D_0^\dagger/k^\dagger}.$$

Again, we have that liftings of the log Frobenius correspond to sections of the Cartier operator in the sense that $\tau \circ \mathscr{C} = \mathrm{Id}$. Indeed, away from log marked points and singular points, the equality is clear from Prop. 3.4.9 where the log Cartier operator coincides with Cartier operator on non-singular curves. On the other hand, the log Cartier operator is constant on log differential forms $d\log(m)$ (Theorem 7.3.14). The description of F_1^* in Lemma 7.3.9 tells us that:

$$F_1^*(d\log(m)) = d\log(F_1^{\#}(m)) = p(d\log(\mathrm{m}))$$

and so τ' is also constant on such log differential forms. In particular, both of these maps are non-zero. Now, $\Omega^1_{C_0^\dagger/k^\dagger}$ restricted to C_0' is nothing but $\omega_{C_0'}\left(\sum_{i=1}^r x_i\right)$, which we assumed to have positive degree $d > 0$ say. Then $F_0^*(\Omega^1_{C_0^\dagger/k^\dagger})$ will have degree $p \cdot d$ on the corresponding component $D_0' = (C_0')^{(p)}$ of D_0. This is a contradiction as $\Omega^1_{D_0^\dagger/k^\dagger}$ has the same degree d when restricted to D_0', but there cannot be a nonzero morphism from a line bundle of degree $p \cdot d$ to one of degree d when $d > 0$. □

We can now finally put everything together:

Proof of Theorem 8.1.7. If the conclusion of the Theorem does not hold, then in particular, by Proposition 8.1.12 and Lemma 8.1.11, we are in the context of Lemma 8.1.14. The curve Γ from Proposition 8.1.10 has p components consisting of non-singular curves of genus 3, arranged in a chain. Thus, $\Omega^1_{\Gamma^\dagger/k^\dagger}$ restricted to an irreducible component has positive degree. The finite étale cover:

$$P_{p,k} \times \mathscr{E}'_{2,k} \overset{\mathrm{Id}\times\beta_{\mathscr{E}_2,k}}{\longrightarrow} \mathscr{W}_{1,k} \times \mathscr{E}_{2,k}$$

restricts to an étale cover $\overline{\mathscr{Z}}_0 \to \Gamma$ of degree p. Thus, $\Omega^1_{\overline{\mathscr{Z}}_0^\dagger/k^\dagger}$ restricted to an irreducible component still has positive degree, contradicting Lemma 8.1.15. □

Part IV

Appendix

Appendix A

Estimating the Serre-Tate coordinate of an elliptic curve

A.1 Canonical liftings modulo p^n

Let K be a field of characteristic 0 that is complete with respect to a discrete valuation v extending the p-adic valuation. Suppose that E/K is an elliptic curve with good ordinary reduction. Recall that one has a short exact sequence of I_K-modules:

$$0 \longrightarrow \mu_{p^n}(\bar{K}) \longrightarrow E[p^n](\bar{K}) \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

for each $n > 0$. To obtain tractable bounds for Theorem 5.1.10, it was important to understand when this sequence is split. This is completely determined by the Serre-Tate coordinate λ associated to E. Write $\mathfrak{m} \subseteq R = \mathscr{O}_{K,v}$ for the valuation ring and k for the residue field. We assume that K is maximally unramified i.e. k is separably closed.

Proposition A.1.1. *Let E/K be an elliptic curve with good ordinary reduction. Write $\mathscr{E}/R$ for the Néron model and $\mathscr{E}_n/R_n$ for the base change to $R_n = R/\mathfrak{m}^{n+1}$ for an integer $n > 0$. Writing $\lambda \in 1 + \mathfrak{m}$ for the corresponding Serre-Tate coordinate, the following are equivalent:*

i) $v(\lambda - 1) > n$.

ii) λ *is a* p^n*-th root in* R.

iii) The short exact sequence of G_K*-modules splits:*

$$0 \longrightarrow \mu_{p^n}(\bar{K}) \longrightarrow E[p^n](\bar{K}) \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0.$$

iv) The short exact sequence of R*-group schemes splits:*

$$0 \longrightarrow \mu_{p^n,R} \longrightarrow \mathscr{E}[p^n] \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0.$$

v) The corresponding short exact sequence of R_n-group schemes splits.

vi) The absolute Frobenius $F_{\mathscr{E}_0/k} : \mathscr{E}_0 \to \mathscr{E}_0$ lifts to a morphism $F_n : \mathscr{E}_n \longrightarrow \mathscr{E}_n$.

When any of the equivalent conditions hold for the model $\mathscr{E}/R$ of an elliptic curve E/K, we say that $\mathscr{E}_n/R_n$ is the *canonical lifting* of $\mathscr{E}_0/k$ modulo p^n.

A.2 Estimating the Serre-Tate coordinate

As far as we are aware, there are no explicit formulae for the Serre-Tate coordinate λ of an elliptic curve E/K, however, one can say something about the valuation $v(\lambda - 1)$:

Proposition A.2.1. *Let E/K be the elliptic curve:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and consider the invariants:

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4 \quad \text{and} \quad b_6 = a_3^2 + 4a_6;$$
$$c_4 = b_2^2 = 24b_4 \quad \text{and} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Suppose that E specialises to an ordinary elliptic curve $\mathscr{E}_0/k$. Write $\mathscr{E}^{\text{can}}/R$ for the canonical lifting of $\mathscr{E}_0$ and λ for the Serre-Tate coordinate of $\mathscr{E}$. We then have:

$$v(\lambda - 1) = \begin{cases} v(c_4) & \text{if} \quad j(\mathscr{E}_0) = 0; \\ v(c_6) & \text{if} \quad j(\mathscr{E}_0) = 1728; \\ v(j(E) - j(\mathscr{E}^{\text{can}})) & \text{if} \quad j(\mathscr{E}_0) \neq 0, 1728. \end{cases}$$

Proof. See [Kr97, Appendix, Prop. 3]. □

Writing $j_0 = j(\mathscr{E}_0)$, as $\mathscr{E}^{\text{can}}$ is definable over $W(k)$, we can express $j(\mathscr{E}^{\text{can}}) = (j_0, j_1, j_2, ...)$ as a Witt vector. $\mathscr{E}^{\text{can}}$ is determined by $\mathscr{E}_0$, so one can view each j_i as a function of j_0. Tate was able to prove the following formulae hold for small primes:

$$j_1 = J_1(j_0) = \begin{cases} 3j_0^3 + j_0^4 & \text{if} \quad p = 5; \\ 3j_0^5 + 5j_0^6 & \text{if} \quad p = 7. \end{cases}$$

In fact, J_i is always a rational function in $\mathbb{F}_p(X)$ when $p \geq 5$ [Fin10].

Appendix B

Bogomolov's result on homotheties

B.1 Homotheties of the p-adic Tate module

Let A be an abelian variety over a number field L. Let $p > 0$ be a prime number and set:

$$V_p(A) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A);$$

where $T_p(A) = \varprojlim_n A[p^n](\bar{L})$ is the p-adic Tate module. Note that $\dim_{\mathbb{Q}_p} V_p(A) = 2g$ where $g = \dim(A)$. There is an associated p-adic representation:

$$\rho : G_L \longrightarrow \mathrm{Aut}(V_p(A));$$

where $G_L = \mathrm{Gal}(\bar{L}/L)$. We say that an element $s \in G_L$ is a *homothety* if it acts on $V_p(A)$ by scaling. Namely, there exists some element $\lambda \in \mathbb{Q}_p^*$ such that:

$$s(x) = \lambda x \quad \text{for all} \quad x \in V_l(A).$$

Theorem B.1.1. *There exists an integer $m > 0$ and an element $s \in G_L$ such that:*

$$s(x) = lx;$$

for all $x \in A[\infty]^{(p)}$ where $l = 1 + p^m$.

Proof. See [Bog80, Cor. 2]. □

B.2 Application to torsion points on curves

Let $X \hookrightarrow A$ be an integral curve in an abelian variety defined over a number field L. Suppose that $X \neq X + a$ for any element $a \in A(\bar{L})$. Using the existence of the homotheties in Theorem B.1.1, we are able to prove the following without any assumption on the

reduction type of A at a prime $p > 0$:

Proposition B.2.1. *Let $p > 0$ be a prime number. For all $a \in A(\bar{L})$, the intersection:*

$$(X + a) \cap A[\infty]^{(p)}$$

is finite, of cardinality bounded by some integer $N > 0$ where N is independent of a.

Proof. The following proof is adapted from [Ray83-3, Section 7]. Fix some positive integer $l > 0$. For all points $a, b \in A(\bar{L})$ we iteratively define the closed subschemes $U_{a,b}^{(n)} \subseteq A$ as follows:

i) $U_{a,b}^{(0)} := X$;

ii) $U_{a,b}^{(n+1)} + a = (U_{a,b}^{(n)} + a) \cap [l]_A^{-1}(U_{a,b}^{(n)} + b)$.

Note that $U_{a,b}^{(n+1)} \subseteq U_{a,b}^{(n)}$ form a decreasing sequence of closed subschemes and so become stationary at some closed subscheme $U_{a,b}$ satisfying:

$$[l]_A(U_{a,b} + a) \subseteq U_{a,b} + b.$$

We now show that $U_{a,b}$ is finite. Take a point $x \in A(\bar{L})$ such that $(l-1)x = a - b$ and set:

$$W = U_{a,b} + a + x.$$

Then $[l]_A(W) \subseteq W$. Suppose that $W' \subseteq W$ is an irreducible component of maximum dimension. Then we also have $[l]_A(W')$ is an irreducibile component of maximum dimension, and so we may assume $[l]_A^r(W') = W'$ without loss of generality, for some $r > 0$. But then W' is a translate of an abelian subvariety of A and by assumption on X, we have that W' is dimension 0.

Let $s \in G_L$ be the homothety from Theorem B.1.1. Abusing notation, we extend s to an automorphism of $A(\bar{L})$. Suppose that $x \in (X + a)(\bar{L}) \cap A[\infty]^{(p)}$. Then $x = u + a$ for some $u \in X(\bar{L})$ and $s(u + a) = s(u) + s(a) = l(u + a)$. On the other hand:

$$s(u + a) = s(u) + s(a) \in X + s(a)$$

as X is defined over L. Thus $u \in U_{a,s(a)}$ and so the desired intersection is finite. □

Bibliography

[Art69] Artin, Michael, *Algebraization of formal moduli. I.*, Global analysis (papers in honor of K. Kodaira), 21-71: (1969).

[Beu-Smy02] Beukers F., and Smyth C.J., *Cyclotomic points on curves*, Number theory for the millennium, I: (2002).

[BF17] Bogomolov, F., and Fu, H., *Elliptic curves with large intersection of projective torsion points*, Eur. J. Math. **4**, 555-560: (2018).

[BFT18] Bogomolov, F., Fu, H., and Tschinkel, Y., *Torsion of elliptic curves and unlikely intersections*, Geometry and physics. Vol. I, Oxford Univ. Press, Oxford, 19-37: (2018).

[BLR-12] Bosch, Siegfried, Lütkebohmert, Werner, and Raynaud, Michel. *Néron models*. Vol. 21. Springer Science & Business Media: (2012).

[Bog80] Bogomolov, Fedor, *Sur l'algébricité des représentations l-adiques*, Comptes Rendus de l'Académie des Sciences Ser. A-B 290.15, A701-A703: (1980).

[BHvB24] Böhning, Christian, Hans-Christian, Graf von Bothmer, and Hubbard, David, *Explicit bounds on common projective torsion points of elliptic curves*, arXiv preprint arXiv:2412.20174: (2024).

[Bog-Pan96] Bogomolov, Fedor, and Pantev, Tony. *Weak Hironaka theorem.* arXiv preprint alg-geom/9603019: (1996).

[Bri-Kum07] Brion, Michel, and Kumar, Shrawan, *Frobenius splitting methods in geometry and representation theory*, Vol. 231. Springer Science & Business Media: (2007).

[Bu96] Buium, Alexandru, *Geometry of p-jets*: (1996).

[Bu05] Buium, Alexandru, *Arithmetic differential equations.* No. 118. American Mathematical Soc.: (2005).

[CLS-24] Cox, David A., Little, John B., and Schenck, Henry K., *Toric varieties.* Vol. 124. American Mathematical Society: (2024).

[Col87] Coleman, Robert F., *Ramified torsion points on curves*: (1987).

[Con22] Conrad, Brian. *Semistable reduction for abelian varieties.* Seminar Lecture Notes available at the webpage `http://math.stanford.edu/~akshay/ntslearn.html`: (2022).

[Del06] Deligne, Pierre, *Équations différentielles à points singuliers réguliers.* Vol. 163. Springer: (2006).

[Del-Ill87] Deligne, Pierre, and Luc Illusie. *Relèvements modulo p^2 et décomposition du complexe de de Rham*, Inventiones mathematicae 89, 247-270: (1987).

[Del-Rap72] Deligne, Pierre, and Rapoport, Michael, *Les schémas de modules de courbes elliptiques.* Modular Functions of One Variable II: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972. Berlin, Heidelberg: Springer Berlin Heidelberg, 143-316: (1973).

[Dem06] Demazure, Michel, *Lectures on p-divisible groups*. Vol. 302. Springer: (2006).

[DKY20] DeMarco, L., Krieger, H., and Ye, H., *Uniform Manin-Mumford for a family of genus* 2 *curves*, Ann. of Math. (2) **191**, no. 3, 949-1001: (2020).

[DGH21] Dimitrov V., Gao Z., and Habegger P., *Uniformity in Mordell–Lang for curves*, Annals of Mathematics, 237–98: (2021).

[EGA] Dieudonne, Jean Alexandre, and Grothendieck, Alexandre, *Éléments de géométrie algébrique*. Vol. 166. Berlin Heidelberg New York: Springer: (1971).

[Fal86] Faltings, Gerd, *Finiteness theorems for abelian varieties over number fields*,Arithmetic geometry, 9-26, Springer: (1986).

[Fin10] Finotti, Luís R.A., *Lifting the j-invariant: Questions of Mazur and Tate*, Journal of Number Theory 130.3, 620-638: (2010).

[FS19] Fu, H., and Stoll, M., *Elliptic curves with common torsion x-coordinates and hyperelliptic torsion packets*, Proc. Amer. Math. Soc. **150**, no. 12, 5137–5149: (2022).

[Ful93] Fulton, William, *Introduction to toric varieties.* No. 131. Princeton university press: (1993).

[Ful-Lang13] Fulton, William, and Lang, Serge, *Riemann-Roch algebra.* Vol. 277. Springer Science & Business Media: (2013).

[Fu22] Fu, H., *Projective equivalence for the roots of unity.* Journal of Algebraic Combinatorics, 56(3), pp.823-871: (2022)

[Gao21] Gao, Z., *Recent developments of the uniform Mordell-Lang conjecture*, `https://arxiv.org/abs/2104.03431v4`https://arxiv.org/abs/2104.03431v4: (2021).

[GGK21] Gao, Z., Ge, T., and Kühne, L., *The uniform Mordell-Lang conjecture*, `https://arxiv.org/abs/2105.15085v2`https://arxiv.org/abs/2105.15085v2: (2021).

[Gr11] Gross, Mark, *Tropical geometry and mirror symmetry.* No. 114. American Mathematical Soc.: (2011).

[H24] Hubbard, David, *Roots of unity and projective equivalence*, arXiv preprint arXiv:2410.17412: (2024).

[Har13] Hartshorne, Robin, *Algebraic geometry.* Vol. 52. Springer Science & Business Media: (2013).

[Har10] Hartshorne, Robin, *Deformation theory.* Vol. 257. New York: Springer: (2010).

[Il79] Illusie, Luc, *Complexe de de Rham-Witt*, Astérisque 63, 83-112: (1979).

[Il94] Illusie, Luc, *Logarithmic spaces (according to K. Kato)*, Barsotti symposium in algebraic geometry. Academic Press: (1994).

[Il05] Illusie, Luc, *Grothendieck's existence theorem in formal geometry with a letter of Jean-Pierre Serre*, Mathematical surveys and monographs 123, 179: (2005).

[Kani-Ros89] Kani, Ernst, and Rosen, Michael, *Idempotent relations and factors of Jacobians.* Mathematische Annalen 284.2, 307-327: (1989).

[Ka78] Katz, Nicholas, *Serre-Tate local moduli*, Surfaces Algébriques: Séminaire de Géométrie Algébrique d'Orsay 1976–78. Springer Berlin Heidelberg, (1981).

[F.Kat96] Kato, Fumiharu, *Log smooth deformation theory*, Tohoku Mathematical Journal, Second Series 48.3, 317-354: (1996).

[F.Kat00] Kato, Fumiharu, *Log smooth deformation and moduli of log smooth curves*, International Journal of Mathematics 11.02, 215-232: (2000).

[K.Kat94] Kato, Kazuya, *Toric singularities*, American Journal of Mathematics 116.5, 1073-1099: (1994).

[K.Kat19] Kato, Kazuya, *Logarithmic structures of Fontaine-Illusie. II*, arXiv preprint arXiv:1905.10678: (2019).

[Kli-Yaf14] Klingler B., and Yafaev A., *the André-Oort conjecture*, Annals of mathematics, Nov 1;180(3):867–925: (2014).

[Kob12] Koblitz, Nea,. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Vol. 58. Springer Science & Business Media: (2012)

[Kod63] Kodaira, Kunihiko, *On compact analytic surfaces: II*, Annals of Mathematics 77.3, 563-626: (1963).

[Kon95] Kontsevich, Maxim, *Lecture at Orsay.*, (1995).

[Kr97] Kraus, Alain, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Polska Akademia Nauk, Instytut Matematyczny: (1997).

[KRZ-B16] Katz, Eric, Rabinoff, Joseph, and Zureick-Brown, David, *Uniform bounds for the number of rational points on curves of small Mordell–Weil rank*, 3189–3240, : (2016).

[Kueh21] Kühne, L., *Equidistribution in families of abelian varieties and uniformity*, `https://arxiv.org/abs/2101.10272v2`: (2021).

[Kunz69] Kunz, Ernst, *Characterizations of regular local rings of characteristic p*, American Journal of Mathematics 91.3, 772-784: (1969).

[Lang65] Lang, Serge, *Division points on curves*, Annali di Matematica Pura ed Applicata, 229-34: (1965).

[Lang13] Lang, Serge, *Fundamentals of Diophantine geometry*, Springer Science & Business Media: (2013).

[Liu02] Liu, Q., *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press: (2002), reprint: (2010).

[Man63] Manin, Yu I., *The theory of commutative formal groups over fields of finite characteristic*, Russian Mathematical Surveys 18.6, 1: (1963).

[Mat13] Matsuki, K., *Introduction to the Mori program*, Springer Science & Business Media: (2013).

[Mats89] Matsumura, Hideyuki, *Commutative ring theory*, No. 8. Cambridge university press, (1989).

[Maz73] Mazur, Barry, *Frobenius and the Hodge filtration (estimates)*, Annals of Mathematics 98.1, 58-95: (1973).

[Maz86] Mazur B., *Arithmetic on curves*, Bulletin of the American Mathematical Society, 14(2):207-59: (1986).

[McQ92] McQuillan M.L., *Division points on semi-abelian varieties*, Harvard University: (1992)

[Mess06] Messing, William, *The crystals associated to Barsotti-Tate groups*, The crystals associated to Barsotti-Tate groups: with applications to abelian schemes, 112-149: (2006).

[MFK-94] Mumford, David, Fogarty, John, and Kirwan, Frances, *Geometric invariant theory*, Vol. 34. Springer Science & Business Media: (1994).

[Mil80] Milne, James S., *Etale cohomology*, (PMS-33). Princeton university press: (1980).

[Mil86] Milne, James S., *Jacobian varieties*, Arithmetic geometry. New York, NY: Springer New York, 167-212: (1986).

[Mum74] Mumford, David, Ramanujam, Chidambaran Padmanabhan, and Manin, Jurij Ivanovič, *Abelian varieties*, Vol. 5. Oxford: Oxford university press: (1974).

[Ner64] Néron, André, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publications Mathématiques de l'IHÉS 21, 5-128: (1964).

[Niz06] Nizioł, Wiesława. *Toric singularities: log-blow-ups and global resolutions*, Journal of algebraic geometry 15.1, 1-29: (2006).

[Og18] Ogus, Arthur, *Lectures on logarithmic algebraic geometry*, Vol. 178. Cambridge University Press, (2018).

[Oort-Norm80] Norman, Peter, and Oort, Frans, *Moduli of abelian varieties*, Annals of Mathematics 112.2, 413-439: (1980).

[Pink04] Pink, Richard, *Finite group schemes*, Notes de Cours, `http://www.math.ethz.ch/pink/FiniteGroupSchemes.html`: (2004).

[Poi22-1] Poineau, J., *Dynamique analytique sur $\mathbb{Z}$. I : Mesures d'équilibre sur une droite projective relative*, `https://arxiv.org/abs/2201.08480`: (2022).

[Poi22-2] Poineau, J., *Dynamique analytique sur $\mathbb{Z}$. II : Écart uniforme entre Lattès et conjecture de Bogomolov-Fu-Tschinkel*, `https://arxiv.org/abs/2207.01574`: (2022).

[PST21] Pila, J., Shankar, A. N., Tsimerman, J., Esnault, H., and Groechenig, M., *Canonical Heights on Shimura Varieties and the André-Oort Conjecture*, arXiv preprint arXiv:2109.08788: (2021).

[Ray66] Raynaud, Michel, *Passage au quotient par une relation d'équivalence plate*, Proceedings of a Conference on Local Fields: NUFFIC Summer School held at Driebergen (The Netherlands) in 1966. Springer Berlin Heidelberg: (1967).

[Ray83-1] Raynaud, M., *Courbes sur une variété abélienne et points de torsion*, Invent. math. **71**, 207-233: (1983).

[Ray83-2] Raynaud, M., *Around the Mordell conjecture for function fields and a conjecture of Serge Lang*, in: "Algebraic Geometry", Raynaud, M., Shioda, T. (eds.), Lecture Notes in Mathematics **1016** Springer (Berlin, Heidelberg): (1983).

[Ray83-3] Raynaud, Michel, *Sous-variétés d'une variété abélienne et points de torsion*, Arithmetic and Geometry: Papers Dedicated to IR Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic, 327-352: (1983).

[Rei12] Reid, Miles, *Surface cyclic quotient singularities and Hirzebruch-Jung resolutions*, manuscript available at `http://www.warwick.ac.uk/masda/surf`: (2012).

[Ser56] Serre, Jean-Pierre, *Géométrie algébrique et géométrie analytique*, Annales de l'institut Fourier. Vol. 6: (1956).

[Ser58] Serre, Jean-Pierre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposion Internacional de topologia algebraica, 24-53: (1958).

[Ser72] Serre, Jean-Pierre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. math 15, 259-331: (1972).

[Ser97] Serre, Jean-Pierre. *Abelian l-adic representations and elliptic curves*, AK Peters/CRC Press: (1997).

[Ser06] Sernesi, E., *Deformations of algebraic schemes*, Grundlehren der math. Wissenschaften **334**, Springer: (2006)

[Ser13] Serre, Jean-Pierre, *Local fields*, Vol. 67. Springer Science & Business Media: (2013).

[SGA7] Grothendieck, Alexandre, *Groupes de Monodromie en Géométrie Algébrique: SGA 7*, Springer-Verlag: (1972).

[Sil09] Silverman, J.H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, 2nd Edition, Springer-Verlag: (2009)

[Sil94] Silverman, Joseph H., *Advanced topics in the arithmetic of elliptic curves*, Vol. 151. Springer Science & Business Media: (1994).

[Sri-Meh87] Mehta, Vikram B., and Srinivas, Vasudevan, *Varieties in positive characteristic with trivial tangent bundle*, Compositio Mathematica 64.2, 191-212: (1987).

[stacks-project] Authors, The Stacks Project, *Stacks Project*.

[ST03] Serre, Jean-Pierre, and Tate, John, *Good reduction of abelian varieties*, Oeuvres-Collected Papers II. Springer, Berlin, Heidelberg, 472-497: (2003).

[Tate67] Tate, John T., *p-Divisible groups*, Proceedings of a Conference on Local Fields: NUFFIC Summer School held at Driebergen (The Netherlands) in 1966. Berlin, Heidelberg: Springer Berlin Heidelberg: (1967).

[Tate97] Tate, John, *Finite flat group schemes*, Modular forms and Fermat's last theorem. New York, NY: Springer New York, 121-154: (1997).

[Voj98] Vojta, P., *Integral points on subvarieties of semiabelian varieties II*, American Journal of Mathematics 121.2, 283-313: (1998)

[Zan12] Zannier, Umberto, *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Princeton University Press: (2012)