Topics In The Theory Of Selmer Varieties

Netan Dogra
Merton College
University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2015

Acknowledgements

This thesis is a poor reflection of the assistance and guidance I have received from several people over the past four years.

It has been a wonderful privilege to be a student of Minhyong Kim, and I have benefited mathematically and personally from his generosity, patience and encouragement and from many inspiring conversations. Much of the work in this thesis has been facilitated by collaboration with Jennifer Balakrishnan, and aside from the mathematics I have learned from her I have benefited enormously from her perseverance in experimentally verifying the results mentioned in this thesis (and falsifying countless previous mistaken formulae). Many of the ideas of this thesis were informed by endless hours of conversation with Jan Vonk, whose mathematical enthusiasm and curiosity have proved a constant source of encouragement. This thesis was greatly influenced by a lecture course I attended given by Amnon Besser. I am indebted to my examiners, Victor Flynn and Guido Kings, for suggesting numerous improvements to the exposition of the present work and for pointing out several inaccuracies.

Finally I would like to thank Lizzie for her love and support.

Abstract

The Selmer varieties of a hyperbolic curve X over $\mathbb{Q}$ are refinements of the Selmer group arising from replacing the Tate module of the Jacobian with higher quotients of the unipotent étale fundamental group. It is hoped that these refinements carry extra arithmetic information. In particular the nonabelian Chabauty method developed by Kim uses the Selmer variety to give a new method to find the set $X(\mathbb{Q})$.

This thesis studies certain local and global properties of the Selmer varieties associated to finite dimensional quotients of the unipotent fundamental group of a curve over $\mathbb{Q}$. We develop new methods to prove finiteness of the intersection of the Selmer varieties with the set of local points (and hence of the set of rational points) and new methods to implement this explicitly, giving the first examples of explicit nonabelian Chabauty theory for rational points on projective curves.

Contents

Chapter 1

Introduction

A basic goal of arithmetic geometry is to give some kind of additional algebraic or geometric structure to the set of rational points of a variety X over $\mathbb{Q}$. For example, let X be a curve of genus $g > 1$ over $\mathbb{Q}$, with a fixed rational point $x \in X(\mathbb{Q})$. This choice of a basepoint determines a *Kummer map*

$$\kappa : X(\mathbb{Q}) \to H^1_f(G_T, V)$$

of $X(\mathbb{Q})$ into a vector space of extensions of Galois representations (here, and throughout, $V := H^1_{ét}(\overline{X}, \mathbb{Q}_p)^*$, and p is be a prime of good reduction) satisfying certain finiteness conditions. These finiteness conditions arise from the commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\kappa} & H^1(G_T, V) \\ \downarrow & & \downarrow \mathrm{loc}_p \\ \prod_{v \in T} X(\mathbb{Q}_v) & \xrightarrow{\kappa_p} & \prod H^1(G_v, V) \end{array}$$

The theorem of Chabauty [17] says that if the rank of the span of κ is less than g, then the intersection $\mathrm{loc}_p(H^1_f(G_T, V)) \cap \kappa_p(X(\mathbb{Q}_p))$ is finite, and given by analytic equations which can often be computed explicitly [22]. The underlying principle may be summarised as reducing understanding the set $X(\mathbb{Q})$ to an analytic question (that of describing κ_p), and a 'motivic' question (that of understanding loc_p).

The nonabelian Chabauty method, introduced in [41] and developed in [42], proposes to study the set of points $X(\mathbb{Q})$ by assigning to a point z a family of

Galois equivariant torsors $P_n(x,z)$ over a unipotent group $U_n(x)$ coming from the geometric fundamental group of X. These $P_n(x,y)$ are étale incarnations of spaces of homotopy classes of paths from x to z on $X(\mathbb{C})$. This determines a sequence of *unipotent Kummer maps*

$$X(\mathbb{Q}) \to H^1_{f,\mathcal{L}}(G_T, U_n(x))$$

from rational points on X to the sets $H^1_f(G_T, U_n(x))$ of isomorphism classes of Galois equivariant torsors satisfying certain local conditions [4]. In fact these set have the structure of the $\mathbb{Q}_p$-points of a variety, giving a sequence of *Selmer varieties* of X:

$$\begin{array}{ccccccc} & & \ldots & & X(\mathbb{Q}) & & \\ & \swarrow & & \swarrow & \downarrow j_2^{\acute{e}t} & \searrow j_1^{\acute{e}t} & \\ \ldots \longrightarrow & H^1_{f,\mathcal{L}}(G_T, U_3) & \longrightarrow & & H^1_{f,\mathcal{L}}(G_T, U_2) & \longrightarrow & H^1_{f,\mathcal{L}}(G_T, U_1) \end{array}$$

where $j_1^{\acute{e}t}$ can be identified with κ via $U_1 \simeq V$. Again we have a 'Chabauty principle': there is a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{j_n^{\acute{e}t}} & H^1_{f,\mathcal{L}}(G_T, U_n) \\ \downarrow & & \downarrow \mathrm{loc}_{p,n} \\ X(\mathbb{Q}_p) & \xrightarrow{j_{n,p}^{\acute{e}t}} & H^1_f(G_p, U_n) \end{array}$$

and an analytic characterisation of $j_{n,p}^{\acute{e}t}$ via p-adic Hodge theory guarantees that the image of $j_{n,p}^{\acute{e}t}$ is Zariski dense and given by Coleman functions [42]. The 'motivic' story is more complicated, but assuming conjectures on the cohomology of geometric Galois representations [39] [15] the localisation map $\mathrm{loc}_{p,n}$ will be non-dense for all $n \gg 0$, giving a finite intersection $\mathrm{loc}_p(H^1_f(G_T, U_n)) \cap j_{n,p}^{\acute{e}t} X(\mathbb{Q}_p)$ (denoted $X(\mathbb{Q}_p)_n$) containing the set of rational points.

1.1 Understanding the Selmer variety

The price of replacing abelian cohomology with nonabelian cohomology is the loss of a group structure, which introduces two subtleties to the theory. The first is the question of how to determine when the localisation map is not dense (and hence when the nonabelian Chabauty method defines a finite set containing the set of rational points) and the second is the question of explicitly describing the sets $X(\mathbb{Q}_p)_n$.

There are several instances where the first problem has been solved. The starting point of Kim's work, in [41], was the case of the set of S-integral points of $\mathbb{P}^1 - \{0, 1, \infty\}$ over $\mathbb{Z}$, using Soulé's results on the Galois cohomology of Tate motives. In [38], Hadian gave a modification of Kim's method which enabled a proof of Siegel's theorem over totally real fields (for an alternative approach, see [44]). In [20], Coates and Kim use results of Greenberg on the Galois cohomology of CM fields to prove that $X(\mathbb{Q}_p)_n$ is finite for large n when X is a hyperbolic curve with Jacobian isogenous to a product of CM abelian varieties.

For the second problem, explicit equations were given in work of Kim and Balakrishnan, Kedlaya and Kim in [43] and [7] in the case of the set of integral points on an elliptic curve of rank 0 ot 1. In [24] Dan-Cohen and Wewers treat explicit Chabauty theory for certain quotients of the fundamental group of $\mathbb{P}^1$ minus three points. In [45] a general approach is outlined to describing the localisation maps on nonabelian cohomology.

In this thesis we describe new results in both directions. For the first problem, new methods are developed to prove non-density of the localisation map in situations where it cannot be seen for dimension reasons. For the second problem, the same global results can be used to describe equations satisfied by the localisations of global nonabelian cohomology classes. We also introduce new local results. Developing on the characterisation of the local unipotent Kummer map at primes of bad reduction given by Kim and Tamagawa [46], Oda's method is used to give a description in terms of the dual graph of a semistable model. It is then proved that the local unipotent Kummer map factors through the irreducible components of the special fibre of a semistable model. Using new explicit formulae proved at p, together with the global methods developed earlier in the thesis, we are able to produce the first examples of explicit non-abelian Chabauty theory for rational points on projective curves in situations where Chabauty's theorem doesn't apply. We focus on what is perhaps the simplest nontrivial case: that of a genus 2 curve with Jacobian isogenous to a product of elliptic curves each of rank at least 1. See the last chapter for the precise definitions involved.

Theorem 1. *Let X be a genus 2 curve with Jacobian isogenous to a product of two elliptic curves E_1 and E_2. Define*

$$\begin{aligned}\rho :& X(\mathbb{Q}_p) \to \mathbb{Q}_p \\ & z \mapsto 2\lambda_{p,E_1}(f_1(z)) - 2\frac{\log_{E_1}(f_1(z))^2}{\log_{E_1}(z_1)^2} h_{E_1}(z_1) - \\ & \lambda_{p,E_2}(f_2(z) - (0,1)) - \lambda_{p,E_2}(f_2(z) + (0,1)) \\ & + \frac{\log_{E_2}(f_2(z) - (0,1))^2 + \log_{E_2}(f_2(z) + (0,1))^2}{\log_{E_2}(z_2)^2} h_{E_2}(z_2)\end{aligned} \tag{1.1}$$

Then $X(\mathbb{Q}_p)_2$ is finite, and is contained in the finite set of z in $X(\mathbb{Q}_p)$ such that

$$\rho(z) = \sum_{v \in T_0} \beta_v$$

where β_v ranges over the finite set of possible values of

$$2\lambda_{E_1,v}(x(f_1(z))) - \lambda_{E_2,v}(x(f_2(z)) + (0,1)) - \lambda_{E_2,v}(x(f_2(z)) - (0,1))$$

for z in $X(\mathbb{Q})_v$.

Theorem 2. *Let X be a genus two curve of the form*

$$y^2 = x^6 + ax^4 + ax^2 + 1$$

such that

$$E : y^2 = x^3 + ax^2 + ax + 1$$

is an elliptic curve of rank 2. Define

$$\begin{aligned}F_1(z) =& \int_b^z (\omega_0\omega_1 - \omega_1\omega_0) \\ F_2(z) =& 2\int_b^z (-\omega_0\omega_3 + a\omega_1\omega_2 + 2\omega_1\omega_4) + \frac{1}{2}(x(b) - x(z)) \\ & - (\int_b^z \omega_0)(\int_{b^-}^b \omega_3) + a(\int_b^z \omega_1)(\int_{b^-}^b \omega_2) + 2(\int_b^z \omega_1)(\int_{b^-}^b \omega_3)\end{aligned}$$

Then $X(\mathbb{Q})$ is contained in the set of z in $X(\mathbb{Q}_p)$ satisfying

$$F_2(w)(F_1(z) - \frac{1}{2}(\int_b^z \omega_0)(\int_{b^-}^b \omega_1)) = F_2(z)(F_1(z) - \frac{1}{2}(\int_b^w \omega_0)(\int_{b^-}^b \omega_1))$$

1.2 Outline

The approach taken in this thesis is to replace the nonabelian torsors $P_n(b,z)$ by a filtered Galois representation obtained from $P_n(b,z)$ by twisting. Equivalently, for *any* unipotent lisse $\mathbb{Q}_p$ sheaf $\mathcal{F}$ on X, one obtains for each rational point x a Galois representation $x^*\mathcal{F}$, which is filtered, with graded pieces independent of x, and it is this parametrisation which is studied. The approach is similar in spirit to the work of Dan-Cohen and Wewers mentioned earlier, but with categories of mixed Tate motives replaced by extensions of Galois representations coming from the Tate module of the Jacobian of X. We specialise almost exclusively to the case where $n=2$, so that U_n will be a central extension of a vector group V by a vector group $\overline{\wedge^2 V}$. To give an oversimplified sketch of the approach, we introduce maps, which we denote by Ψ,

$$\Psi : \mathbb{Q}_p[X(\mathbb{Q})] \to \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U_2)] \to H^1_{f,T}(G_T, E(V,[L,L]))$$

from $\mathbb{Q}_p$-divisors of rational points to abelian cohomology classes. Here $E(V,[L,L])$ is a filtered Galois representation, with $\overline{\wedge^2 V}$ as a subobject.

There are also local analogues

$$\Psi_p : \mathbb{Q}_p[X(\mathbb{Q}_p)] \to \mathbb{Q}_p[H^1_f(G_p, U_2)] \to H^1_f(G_p, E_p(V,[L,L]))$$

Roughly, we identify conditions under which an element $\sum \mu_i(c_i)$ in $\mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T,U_2)]$ defines an element of $H^1_f(G_T,\overline{\wedge^2 V})$. In situations where $H^1_f(G_T,\overline{\wedge^2 V})$ is smaller than $H^1_f(G_p,\overline{\wedge^2 V})$, this is then used to identify conditions under which an element of $H^1_f(G_p,U)$ comes from a global class.

The structure of the thesis is as follows. In chapter 2 foundational results on fundamental groups and Selmer varieties are recalled, and the basic 'linearisation' process is described. It produces a map Θ (or rather various versions of a map Θ) which reduces a description of the localisation map to some multilinear algebra. Although the construction is quite elementary, it produces some surprising new results, and is applied to prove non-density of the localisation map in situations where non-density cannot be seen on graded pieces. At the end of the chapter we prove relations between the unipotent Kummer map for '$\mathbb{Q}_p(1)$-quotients' of the fundamental group and p-adic heights, following previous results of Balakrishan and Besser [6] and Balakrishnan, Besser and Muller [5] for the local unipotent Kummer map at p for affine elliptic and hyperelliptic curves, and work of Balakrishnan, Dan-Cohen, Kim and Wewers [4] for the local unipotent Kummer map at primes away from from p for affine elliptic curves. Our approach is cohomological, and amounts to identifying Beilinson's description of the extensions arising from the unipotent Kummer map [27] with Nekovar's description of the height pairing [50].

The next chapter discusses the local theory. We review the method of Oda for studying the action of inertia on the fundamental group at primes of bad reduction, and then describe how to use this to compute the local unipotent Kummer map. This is then used to give conditions under which the local unipotent Kummer map at depth 2 distinguishes the irreducible components of the special fibre of a semistable model, and examples where the local unipotent Kummer map at depth 2 is trivial even though the dual graph is not. The rest of the chapter is devoted to explicit computation of the local unipotent Kummer map at p. We recall the description of this map given in [42], and then introduce methods to compute the Hodge filtration and the local version of the map Θ introduced in the first chapter.

In the final chapter, we describe joint work with Jennifer Balakrishnan on the explicit non-abelian Chabauty method for bi-elliptic genus two curves, and give examples. These computations depend on several results on the global and local structure of the unipotent Kummer map established in previous chapters.

Chapter 2

Global Structure

In this chapter we prove the main results on the global structure of Selmer varieties. In the first two sections we review the foundational definitions and results on unipotent fundamental groups and Selmer varieties. We also note some cases not currently mentioned in the literature where $X(\mathbb{Q}_p)_2$ is finite. In section 3 we introduce some new ideas for studying the depth 2 Selmer variety. This is then used to prove non-density of the localisation map in situations where it cannot be seen on the level of the Galois cohomology of the graded pieces. The last section, which is largely independent of the preceding two sections, proves a relation between p-adic heights and certain pieces of the unipotent Kummer map, which is used in the explicit formulae for bielliptic curves obtained in the last chapter.

2.1 Galois representations arising from fundamental groups

We first define some elementary notation. For a vector space W over a field F define W^* to be the dual vector space. Define $T(W)$ to be the tensor algebra $\oplus_{n\geq 0} W^{\otimes n}$. Define $\wedge^2 W$ to be the second exterior product. Define $G_{\mathbb{Q}}$ to be the Galois group of $\mathbb{Q}$. For a finite set of primes S of $\mathbb{Q}$ define G_S to be the maximal quotient of $G_{\mathbb{Q}}$ unramified outside S. For S a set of primes of $\mathbb{Q}$ and K a finite extension of $\mathbb{Q}$ define $G_{K,S}$ to be the maximal quotient of G_K unramified outside all primes of K lying above an element of S.

We recall some constructions and notation in the continuous Galois cohomology of profinite groups (see [59]). Let G be an arbitrary profinite group, U a G-group (in the category of topological groups). Let V be a continuous representation of G, with an equivariant action of U. Then, for any G-equivariant left U-torsor P, we may form the *twist of V by P*, defined as follows:
Let $\sim$ denote the equivalent relation on $V \times P$ given by

$$(v,p) \sim (vu, u^{-1}p)$$

for all $v \in V, u \in U, p \in P$. Then $V \times P/\sim$ has a natural continuous G-representation structure, and we denote this G-representation by $V^{(P)}$.

Definition 1. For representations $V_1, \ldots, V_n$, we define a mixed representation with graded pieces $V_1, \ldots, V_n$ to be a Galois representation W admitting a filtration

$$M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$$

and isomorphisms

$$M_{i-1}/M_i \simeq V_i$$

For finite dimensional continuous $\mathbb{Q}_p$-representations W_1, W_2, we shall frequently identify
$H^1(G, W_1^* \otimes W_2)$ with $\mathrm{Ext}^1(W_1, W_2)$ as follows: given

$$0 \to W_2 \to W_3 \to W_1 \to 0$$

take W_4 to be the pull-back of $W_3 \otimes W_1^*$ by $\mathbb{Q}_p \to W_1^* \otimes W_1$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & W_1^* \otimes W_2 & \longrightarrow & W_4 & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W_1^* \otimes W_2 & \longrightarrow & W_1^* \otimes W_3 & \longrightarrow & W_1^* \otimes W_1 & \longrightarrow & 0
\end{array}$$

This gives a well-defined map

$$\mathrm{Ext}^1(W_1, W_2) \to H^1(G, W_1^* \otimes W_2)$$

which is an isomorphism with inverse given by sending an extension W_4 of $\mathbb{Q}_p$ by $W_1^* \otimes W_2$ by the pushforward of $W_1 \otimes W_4$ by $W_1^* \otimes W_1 \to \mathbb{Q}_p$.

A group G below shall always be either $G_{K,T}$ for a number field K and a finite set of primes T (i.e. the maximal quotient of $\mathrm{Gal}(\overline{K}|K)$ unramified outside T) or G_{K_v} for v a prime of K. For $\mathbb{Q}_p$- representations W_1 and W_2 of $G_{\mathbb{Q}_p}$, we say that $[W_3] \in \mathrm{Ext}^1(W_1, W_2)$ is crystalline if the induced extension of $W_1 \otimes B_{\mathrm{cr}}$ by $W_2 \otimes B_{\mathrm{cr}}$ admits a splitting. The subspace of such extensions is denoted $\mathrm{Ext}^1_f(W_1, W_2)$. Similarly for $\mathbb{Q}_p$ representations W_1 and W_2 of $G_T = G_{\mathbb{Q},T}$ we write $\mathrm{Ext}^1_f(W_1, W_2)$ for the space of classes of extensions which are crystalline at p and which split when restricted to the intertia group at v for all other primes.

We denote by $H^1_{f,T}(G_T, W) \subset H^1(G_T, W)$ the space of G_T cohomology classes which are crystalline at p (with no hypotheses at $v \in T - \{p\}$), and similarly define $\mathrm{Ext}^1_{f,T}(W_1, W_2)$.

Finally we define $H^1_g(G_p, W)$ to denote the kernel of

$$H^1_g(G_p, W) \to H^1_g(G_p, W \otimes B_{\mathrm{dR}})$$

and $H^1_g(G_T, W)$ to denote the kernel of the composite

$$H^1(G_T, W) \to H^1_g(G_p, W) \to H^1_g(G_p, W \otimes B_{\mathrm{dR}}).$$

2.1.1 $\mathbb{Q}_p$-local systems and Malcev Completions

We briefly recall the definition and basic properties of the $\mathbb{Q}_p$-unipotent fundamental group of a scheme X, as developed in [26]. The $\mathbb{Q}_p$-unipotent fundamental group of a scheme X is an object that can be viewed as coming from the étale fundamental group, but which admits more structure than the étale fundamental group:

The category of $\mathbb{Q}_p$ local systems, (or locally constant $\mathbb{Q}_p$ sheaves), on X has the structure of a rigid tensor category, with the obvious definition of tensor product and unit object. The fibres of a locally constant $\mathbb{Q}_p$ sheaf naturally have the structure of $\mathbb{Q}_p$ vector spaces, hence for each point x of W we have an associated fibre functor ω_x. Hence, noting that (as explained below) the groups of endomorphisms of the constant sheaf $\underline{\mathbb{Q}_p}$ is isomorphic to $\mathbb{Q}_p$, we obtain a neutral Tannakian category of $\mathbb{Q}_p$-local systems on X. This thesis will only consider *unipotent* local systems on X - that is, $\mathbb{Q}_p$-local systems on X equipped with filtration all of whose graded pieces are constant sheaves. Let $\mathcal{U}n^{\mathbb{Q}_p}(X)$ denote the category of unipotent étale $\mathbb{Q}_p$ local systems on X. The $\mathbb{Q}_p$-unipotent étale fundamental group $\pi_1^{ét,\mathbb{Q}_p}(X,x)$ at a fibre functor x is then defined to be the Tannakian fundamental group of the category $\mathcal{U}n^{\mathbb{Q}_p}(X)$ with fibre functor ω_x defined above. The relationship between this category and the étale fundamental group is as follows (see [30]):

Theorem 3. *We have an equivalence of categories between the category of $\mathbb{Q}_p$-local systems on X and the category of continuous $\mathbb{Q}_p$-representations of $\pi_1^{ét}(X,x)$*

Hence for any $x \in X$, $\mathcal{U}n^{\mathbb{Q}_p}(X)$ is equivalent to the category of continuous unipotent $\mathbb{Q}_p$ representations of the profinite fundamental group $\pi_1^{ét}(X,x)$. In particular, it is a neutral Tannakian category, and any point x of X defines a fibre functor, corresponding to the forgetful functor for $\pi_1^{ét}(X,x)$. Hence the unipotent étale fundamental group is simply the universal (pro-)object in the category of continuous homomorphisms from $\pi_1^{ét}(\overline{X},x)$ to unipotent algebraic groups. In order to 'compute' the Tannakian fundamental group, it is be enough to find a functor from profinite groups to unipotent pro-algebraic groups which is universal for group homomorphisms to unipotent pro-algebraic groups in the appropriate sense. Such a functor is given by Malcev completion [55]. We sketch how this works in our case of interest below:

Unless otherwise stated X will henceforth be an arbitrary smooth projective curve over $\mathbb{Q}$ of genus $g > 1$ with good reduction at p. T_0 will be the set of primes of bad reduction and $T := T_0 \cup \{p\}$. We work not with the unipotent étale fundamental group of X but that of the $\overline{X}$, the base change to $\overline{\mathbb{Q}}$. For rational points x and y the profinite set $\pi_1^{ét}(\overline{X};x,y)$ has a continuous action of $G_{\mathbb{Q}}$. For all primes l of good reduction, the $G_{\mathbb{Q}}$-action on

$$\pi_1^{ét,(l)}(\overline{X};x,y) := \pi_1^{ét,(l)}(\overline{X};x) \times_{\pi_1^{ét}(\overline{X};x)} \pi_1^{ét}(\overline{X};x,y)$$

is unramified at l. Hence the $G_{\mathbb{Q}}$-action on

$$\pi_1^{ét,p}(\overline{X};x,y) := \pi_1^{ét,p}(\overline{X};x) \times_{\pi_1^{ét}(\overline{X};x)} \pi_1^{ét}(\overline{X};x,y)$$

is unramified at all primes outside T and hence the $G_{\mathbb{Q}}$-action factors through G_T. $\mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X};x,y)]$ denote the G_T-representation freely generated by the G_T-set $\pi_1^{\acute{e}t,p}(\overline{X};x,y)$. The left action of $\pi_1^{\acute{e}t,p}(\overline{X},x)$ induces a G_T-equivariant left action

$$\mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X},x)] \otimes \mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X};x,y)] \to \mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X};x,y)]$$

Let I denote the kernel of the augmentation map

$$\mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X},x)] \to \mathbb{Q}_p$$

$$\sum \lambda_\gamma \gamma \mapsto \sum \lambda_\gamma$$

We obtain an nilpotent $\mathbb{Q}_p$-algebra object

$$A_n(x) := \mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X},x)]/I^{n+1}$$

in the category of $\mathbb{Q}_p$-Galois representations, and a finite dimensional $\mathbb{Q}_p$ Galois representation

$$A_n(x,y) := A_n(x) \otimes_{\mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X},x)]} \mathbb{Q}_p[\pi_1^{\acute{e}t,p}(\overline{X};x,y)]$$

which will be referred to in this thesis as a *path space*. $A_n(x,y)$ has the structure of a G_T equivariant rank 1 $A_n(x)$-module. It may also be viewed as the fibre at y of a $\mathbb{Q}_p$-local system $\mathcal{A}_n$, which corresponds to the $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},x)$ representations $A_n(x)$ via Tannakian duality. The I-adic filtration gives an associated graded $gr^\bullet A_n(x)$, which is naturally a quotient of $T(V)/V^{\otimes(n+1)}$, and is canonically isomorphic to $gr^\bullet A_n(x,y)$. We similarly have

$$I^i A_n(x,y) = \ker(A_n(x,y) \to A_{i-1}(x,y))$$

and

$$A[n](x,y) := I^n A_n(x,y) \simeq (I^n/I^{n+1})$$

By the above $A[n](x,y)$ is naturally a summand of $V^{\otimes n}$.

We have the following cohomological description of $A_n(x,y)$ [27].

Theorem 4 (Beilinson). *Let $X_i \subset X^n$ denote the divisor*

$$\{(x_1, \ldots, x_n) \in X^n : x_i = x_{i+1}\}$$

Then

$$A_n(x) \simeq H^n_{\acute{e}t}(\overline{X}^n; (x \times \overline{X}^{n-1}) \cup (\overline{X}^{n-1} \times y) \cup (\bigcup_{i=1}^{n-1} \overline{X}_i))^* \oplus \mathbb{Q}_p$$

and if $x \neq y$

$$A_n(x, y) \simeq H^n_{\acute{e}t}(\overline{X}^n; (x \times \overline{X}^{n-1}) \cup (\overline{X}^{n-1} \times y) \cup (\bigcup_{i=1}^{n-1} \overline{X}_i))^*$$

We define $A_\infty(x)$ to be the inverse limit of the $A_n(x)$. $A_\infty(x)$ is isomorphic to the completion of a free associative algebra on $2g$ generators modulo the two-sided ideal generated by one quadratic relation (which can be viewed as coming from the quadratic relation in the standard presentation of the fundamental group of a surface of genus g) by the augmentation ideal.

The Tannakian fundamental group of the category of locally constant $\mathbb{Q}_p$ sheaves on $\overline{X}$ at the fiber functor x, $\pi_1^{\acute{e}t, \mathbb{Q}_p}(\overline{X}, x)(\mathbb{Q}_p)$, has an explicit description as the subgroup of $A_\infty(x)^\times$ of *grouplike* elements [26], and its Lie algebra $L_\infty(x)$ has an explicit description as a sub-Lie algebra of *primitive* elements in the Lie algebra $A_\infty(x)$ (where the Lie bracket is the commutator). The finite dimensional quotients $U_n(x)$ are naturally subgroups of $A_n(x)^\times$. We recall the following results which are explained in [42] (see section 1 for the de Rham version, and section 2 for the étale version):

$$\mathrm{Hom}(b^*, z^*) \simeq A_\infty(b, z)$$

$$\mathrm{Iso}(b^*, z^*) \simeq A_\infty(b, z) - IA_\infty(b, z)$$

$$\mathrm{Iso}^\otimes(b^*, z^*) \simeq P_\infty(b, z)$$

In particular

$$P_\infty(b, z) \subset A_\infty(b, z) \tag{2.1}$$

Define $L_\infty(x)^{(1)} := [L_\infty(x), L_\infty(x)]$, $U_\infty(x)^{(1)} := [U_\infty(x), U_\infty(x)]$, and extend this inductively by

$$L_\infty(x)^{(n)} := [L_\infty(x), L_\infty(x)^{(n-1)}]$$

$$U_\infty(x)^{(n)} := [U_\infty(x), U_\infty(x)^{(n-1)}]$$

Our main objects of interest will be the finite dimensional quotients and subquotients

$$L_n(x) := L_\infty(x)/L_\infty(x)^{(n)}$$

$$U_n(x) := U_\infty(x)/U_\infty(x)^{(n)}$$

We also define

$$U[n] := \mathrm{Ker}(U_n \to U_{n-1})$$

and

$$A[n] := \mathrm{Ker}(A_n \to A_{n-1})$$

The action of $U_n(x)$ on $A_n(x)$ allows us to associate to any G_T-equivariant left-$U_n(x)$-torsor P a Galois representation $A_n(x)^{(P)}$ which will again have a canonical G_T-filtration with associated graded isomorphic to $gr^\bullet A_n(x)$. When P is the pushout $P_n(x,y) := U_n(x) \times_{\pi_1^{\acute{e}t}(\overline{X},x)} \pi_1^{\acute{e}t}(\overline{X};x,y)$ there is a canonical isomorphism

$$A_n(b,z) \simeq A_n(b)^{(P_n(b,z))}$$

hence the twisting construction may be thought of as giving a generalisation of $A_n(x,y)$ for the 'virtual path' associated to an arbitrary nonabelian cohomology class. ($P_n(b,z)$ is a left $U_n(b)$-torsor as we write composition of paths from left to right). For another (similar) characterisation of the sheaves $\mathcal{A}_n$ see [1]

Note that as a corollary of equation (2.1) $P_n(b,z)$ is naturally a subvariety of $A_n(b,z)$.

When we want to distinguish the objects A_n, P_n, U_n defined above from their other motivic realisations (i.e. de Rham, crystalline, Betti) we will denote them by as $A_n^{\acute{e}t}, P_n^{\acute{e}t}, U_n^{\acute{e}t}$. When comparing the fundamental groups of different curves X and Y, we write $A_n^{\acute{e}t}(X)(x_1,x_2)$, $A_n^{\acute{e}t}(Y)(y_1,y_2)$, etc.

2.1.2 The universal enveloping algebra at depth 2

When $n=1$ the map

$$z \mapsto [A_1(b,z)]$$

is exactly the parametrisation of points z given by the étale Abel-Jacobi map

$$\kappa : \mathrm{Div}^0(X)(\mathbb{Q}) \to H^1_f(G_T, V)$$

To describe the case $n = 2$ we introduce some notation.

Definition 2. Define $\overline{\wedge^2 V}$ and $\overline{V^{\otimes 2}}$ to be the quotients of $\wedge^2 V$ and $V^{\otimes 2}$ respectively by the image of the Weil pairing

$$\mathbb{Q}_p(1) \to \wedge^2 V \subset V^{\otimes 2}$$

The representation $A_2(b,z)$ is an extension of $A_1(b,z)$ by $\overline{V^{\otimes 2}}$. Define the representation $\overline{A}_2(b,z)$ to be the quotient of $A_2(b,z)$ by $\mathrm{Sym}^2(V)$. Hence $\overline{A}_2(b,z)$ has graded pieces $\mathbb{Q}_p, V$ and $\overline{\wedge^2 V}$, and there are short exact sequences

$$0 \to \overline{\wedge^2 V} \to \overline{A}_2(b,z) \to A_1(b,z) \to 0$$

$$0 \to I\overline{A}_2(b,z) \to \overline{A}_2(b,z) \to \mathbb{Q}_p \to 0$$

$\overline{A}_2(b,z)$ satisfies the following properties:

Lemma 1. *(i): $\overline{A_2}(b,z)$ is the fibre at z of a locally constant sheaf $\overline{\mathcal{A}_2}^{\acute{e}t}$ on X.*
(ii): $\overline{A_2}(b)$ is an algebra object in the category of continuous crystalline $\mathbb{Q}_p$ -representations of G_T.
(iii): There are G_T-equivariant inclusions

$$\begin{aligned} U_2(b) &\hookrightarrow \overline{A}_2(b)^\times \\ P_2(b,z) &\hookrightarrow \overline{A}_2(b,z) \\ L_2(z) &\hookrightarrow I\overline{A}_2(b) \end{aligned}$$

(iv): $\overline{A}_2(b,z)$ is isomorphic to the twist of $\overline{A}_2(b)$ by the $U_2(b)$-torsor $P_2(b,z)$.

Proof. (i) and (ii) are induced from the corresponding properties of $\mathcal{A}_2^{\acute{e}t}$ and $A_2(b)$ respectively. The injectivity results in (iii) follow from the fact that $U_2(b)$ acts faithfully on $\overline{A}_2(b)$. □

This thesis shall mostly consider quotients of $U_2(b)$. Let U be a quotient of U_2 such that $U^{\mathrm{ab}} = V$. Let L denote the Lie algebra of U. Then U sits in an exact sequence

$$1 \to [L, L] \to U \to V \to 1$$

Let $A = A(b)$ denote the quotient of $\overline{A}_2(b)$ by $\ker(\overline{\wedge^2 V} \to [L, L])$. Then A is a nilpotent algebra object in the category of p-adic Galois representations, with maximal ideal I. We may similarly define $A(b, z)$ to be the quotient of $\overline{A}_2(b, z)$ by $\ker(\overline{\wedge^2 V} \to [L, L])$, and define

$$P(z) = P(b, z) := U(b) \times_{U_2(b)} P_2(b, z)$$

As before we obtain exact sequences

$$0 \to [L, L] \to A(b, z) \to A_1(b, z) \to 0$$

$$0 \to IA(b, z) \to A(b, z) \to \mathbb{Q}_p \to 0$$

and the analogue of Lemma 1 holds (with the same proof):

Lemma 2. *(i): $A(b, z)$ is the fibre at z of a locally constant sheaf $\mathcal{A}^{\acute{e}t}$ on X.*
(ii): $A(b)$ is an algebra object in the category of continuous crystalline $\mathbb{Q}_p$ -representations G_T.
(iii): There are G_T-equivariant inclusions

$$U(b) \hookrightarrow A(x)^{\times}$$
$$P(b, z) \hookrightarrow A(b, z)$$
$$L(b) \hookrightarrow IA(b)$$

(iv): $A(b, z)$ is isomorphic to the twist of $A(b)$ by the $U(b)$-torsor $P(b, z)$.

2.1.3 Basic properties of $A(b, z)$

We now describe the $\mathrm{Ext}^1(V, [L, L])$ class associated to $A(b, z)$. As in the previous section U is taken to be a Galois stable quotient of U_2 whose abelianisation equals V.

Definition 3.

$$\tau : V \to \mathrm{Hom}(V, [L, L])$$

to be the homomorphism coming from the left action of V on $\wedge^2 V$

$$v \mapsto (w \mapsto v \wedge w)$$

Note that this differs by a factor of a half from the commutator homomorphism

$$v \mapsto (w \mapsto [v, w])$$

Define

$$\overline{V^* \otimes [L, L]} := \mathrm{coker}(\tau)$$

In the case $U = U_2$, τ is an injection and the map $V \to V^* \otimes \overline{\wedge^2 V}$ splits, giving a decomposition

$$H^1(G_T, V^* \otimes \overline{\wedge^2 V}) \simeq H^1(G_T, V) \oplus H^1(G_T, \overline{V^* \otimes [L, L]})$$

Definition 4. For a rational point z, define $c_1(z) \in H^1(G_T, V)$ and $c_2(z) \in H^1(G_T, \overline{V^* \otimes [L_2, L_2]})$ by

$$[I\overline{A}_2(z, x)] \simeq (c_1(z), c_2(z))$$

via the decomposition above. When we want to specify the basepoint we will write these as $c_1(b, z)$ and $c_2(b, z)$ respectively.

By comparing the left and right actions of U_2 on A, the relation between $IA(b, z)$ for varying b and z is as follows:

Lemma 3. *The $H^1_f(G_T, \overline{V^* \otimes [L_2, L_2]})$ class $c_2(z)$ associated to $I\overline{A}_2(b, z)$ is independent of b and z. For rational points x_1, x_2, z_1, z_2,*

$$c_1(z_1, x_1) - c_1(z_2, x_2) = \tau_* \kappa(z_1 + x_1 - z_2 - x_2)$$

Proof. First suppose $x_1 = x_2$. Then

$$[IA(x_1, z_1)] = [IA(x_1, z_2)^{\kappa(z_1 - z_2)}].$$

By definition of the twisting construction

$$[IA(x_1,z_2)^{\kappa(z_1-z_2)}] = [IA(x_1,z_2)] + \tau_*\kappa(z_1-z_2).$$

Similarly

$$[IA(x_1,z_1)] = [IA(x_2,z_1)^{\kappa(x_1-x_2)}] = [IA(x_2,z_1)] + \tau_*\kappa(x_1-x_2).$$

□

In general $c_2(z)$ can be nontrivial [25]. One special case where c_2 is trivial is that of a projective hyperelliptic curve

$$X : y^2 = f(x) = x^{2g+2} + \sum a_i x^i$$

of genus g.

Lemma 4. *Let $\alpha_1, \ldots, \alpha_{2g+2}$ be the roots of f. Let D denote the $\mathbb{Q}$-divisor $\frac{1}{g+1}\sum_i(\alpha_i,0)$. Then the extension class is $[IA(b,z)]$ is given by the image of $\kappa(z+b-D)$ under the natural map*

$$H^1(G_T,V) \to \mathrm{Ext}^1(V,\overline{\wedge^2 V})$$

coming from the nilpotent left action of V on $V \oplus \wedge^2 V$

Proof. First note that it will be enough to prove that the two classes are equal in $H^1(G_{K,T}, V^* \otimes \overline{\wedge^2 V})$, for K some finite extension of $\mathbb{Q}$, since the restriction map is injective. Let K be an extension containing all roots of f. For any i,j, the divisor $(\alpha_i,0)-(\alpha_j,0)$ is torsion, and so in particular

$$\kappa_K((\alpha_i,0)-(\alpha_j,0)) = 0.$$

Hence it is enough to show that the $H^1(G_{K,T}, V^* \otimes \overline{\wedge^2 V})$ class obtained from $A_2(b,z)$ agrees with that of $z+b-2(\alpha_i,0)$ for some i. We prove this in three stages:
(i): Suppose $z=b=(\alpha_i,0)$. Then the hyperelliptic involution gives an action of $\mathbb{Z}/2\mathbb{Z}$ on $A_2(b)$. This acts on the V-graded piece as -1 and on the $\overline{\wedge^2 V}$-graded piece as the identity. Hence we obtain a splitting of $A_2(b)$.

(ii): Now let b be arbitrary. By the Lemma 3 the extension class of $IA_2(b)$ is just the twist of $IA_2(\alpha_i)$ by the $H^1(G_T, V)$ class of $b-(\alpha_i, 0)$. Since this twist is via the conjugation action of U on A, the corresponding extension class is $2\kappa(b-(\alpha_i, 0))$.
(iii): Now we consider the general case. Now consider the right action of V on $IA_2(b)$. The representation $IA_2(b, z)$ is simply obtained by twisting by the $H^1(G_T, V)$ torsor associated to $z - b$. Hence the class is $z + b - 2(\alpha_i, 0)$. □

2.2 Selmer varieties and conjectures on the unipotent Kummer map

In this section we recall the notion of the Selmer variety and its key properties. We also recall some basic properties of nonabelian Galois cohomology [59]. For convenience everything below will be described for the case of $\mathbb{Q}$-rational basepoints, and we will not assiduously mention the analogous results over local fields, see [41] and [42] for more details.

2.2.1 Cohomology varieties and Selmer varieties

Fix a basepoint $b \in X(\mathbb{Q})$. In this subsection U will denote an arbitrary Galois stable quotient of U_n. The unipotent fundamental group allows us to define the following refinement of the Kummer map:

Definition 5. Let U be as above. Define

$$j : X(\mathbb{Q}) \to H^1(G_T, U)$$

$$x \mapsto [P(x)]$$

where

$$H^1(G_T, U) := U \backslash Z^1(G_T, U)$$

is the pointed set of isomorphism classes of U-valued G_T-cocycles. In the case $U = U_n$, we write $j = j_n$.

Recall that $P(b, x)$ is not merely a G-equivariant torsor, but a G-equivariant *bitorsor* (with a left action of $U(b)$ and a right action of $U(x)$), giving an identification of the Galois cohomology spaces of $U(b_1)$ and $U(b_2)$:

Lemma 5. *Let b_1, b_2 be $\mathbb{Q}$-points of X. Then we obtain an isomorphism*

$$H^1(G, U(b_1)) \simeq H^1(G, U(b_2))$$

defined by sending a left $U(b_1)$-torsor P to the left $U(b_2)$ -torsor $P(b_2, b_1) \times_{U(b_1)} P$

Proof. See Serre,[59], Proposition 35. □

One of the fundamental insights of the theory of Selmer varieties is that the cohomology spaces $H^1(G, U(b))$ carry a much richer structure than merely that of a pointed set, and that this extra structure has Diophantine applications. For the following theorem we take G to be either G_v or G_T:

Theorem 5 (Kim, [41])**.** *Let U be a finite dimensional unipotent group over $\mathbb{Q}_p$, admitting a continuous action of G. Suppose $H^0(G, U^i/U^{i+1})(\mathbb{Q}_p) = 0$ for all i. Then the functor*

$$R \mapsto H^1(G, U(R))$$

is represented by an affine algebraic variety over $\mathbb{Q}_p$, such that the six term exact sequence in nonabelian cohomology is a diagram of schemes over $\mathbb{Q}_p$.

In this thesis we will never distinguish between a cohomology variety and its $\mathbb{Q}_p$-points. Note that since the abelianisation of $U(\mathbb{Q}_p)$ has weight -1, it satisfies the hypotheses of the Theorem, and hence $H^1(G, U)$ has the structure of the $\mathbb{Q}_p$-points of an algebraic variety over $\mathbb{Q}$.

To go from the cohomology varieties $H^1(G_T, U)$ to Selmer varieties, one must add local conditions. For each $v \neq p$, there is a *local unipotent Kummer map*

$$j_v : X(\mathbb{Q}_v) \to H^1(G_v, U)$$

$$x \mapsto P(x)$$

which is trivial when v is a prime of good reduction and has finite image in general [46]. For $v = p$, the assignment $x \mapsto [P(x)]$ lands inside the subspace of *crystalline* torsors $H^1_f(G_p, U)$ (see the next chapter), and we define j_p to be the map

$$X(\mathbb{Q}_p) \to H^1_f(G_p, U)$$

There is then a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & H^1(G_T, U_n(x)) \\ \downarrow & & \downarrow \prod \mathrm{loc}_v \\ \prod_{v \in T} X(\mathbb{Q}_v) & \longrightarrow & \prod_{v \in T} H^1(G_v, U_n(x)) \end{array}$$

It is also shown in [41] that the localisation morphisms are morphisms of varieties, and the set of crystalline cohomology classes has the structure of the $\mathbb{Q}_p$ -points of a variety. Since at any prime $l \neq p$ the image of $X(\mathbb{Q}_l)$ in $H^1(G_l, U_n(x))$ is finite ([46]) we may define a subvariety $H^1_{f,\mathcal{L}}(G_T, U_n(x))$ of $H^1(G_T, U_n(x))$ to be the set of cohomology classes c satisfying

- $\mathrm{loc}_l(c)$ comes from an element of $X(\mathbb{Q}_l)$ for all $l \neq p$
- $\mathrm{loc}_p(c)$ is crystalline.
- The projection of c to $H^1(G_T, V)$ lies in the image of $\mathrm{Jac}(X)(\mathbb{Q}) \otimes \mathbb{Q}_p$

We have included the last condition to avoid any finiteness of Ш assumptions in the statement of our results. Of course from a computational perspective all the methods we outline in this paper depend on finding the Mordell-Weil rank of the Jacobian, and hence on knowing finiteness of Ш.

2.2.2 Diophantine applications of Selmer varieties

To use the Selmer variety constructed above to study the set of rational points of X, one needs to understand the diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{j_n^{\acute{e}t}} & H^1_{f,\mathcal{L}}(G_T, U_n(x)) \\ \downarrow & & \downarrow \mathrm{loc}_p \\ X(\mathbb{Q}_p) & \xrightarrow{j_{n,p}^{\acute{e}t}} & U_n^{dR}/F^0 \end{array}$$

It is hoped that, in a very general context, the Selmer variety is a sufficient refinement of the Selmer group of the Jacobian to detect the finiteness of the set of rational points $X(\mathbb{Q})$ of a hyperbolic curve. It follows from the finiteness of the kernel of the étale Abel-Jacobi map

$$\kappa : \mathrm{Jac}(X)(\mathbb{Q}_p) \to H^1(G_p, V)$$

that this would be implied by finiteness of the image of $X(\mathbb{Q})$ in $H^1_f(G_p, U)$.

Definition 6. Define $X(\mathbb{Q}_p)_n \subset X(\mathbb{Q}_p)$ to be the preimage under $j_{n,p}$ of the intersection of $j_{n,p}(X(\mathbb{Q}_p)$ with $\mathrm{loc}_p\, H^1_{f,\mathcal{L}}(G_T, U_n)$ in $H^1_f(G_p, U_n)$.

This gives a decreasing of subsets of $X(\mathbb{Q}_p)$

$$X(\mathbb{Q}_p)_1 \supset X(\mathbb{Q}_p)_2 \supset \dots$$

Note that by construction, $X(\mathbb{Q}) \subset X(\mathbb{Q}_p)_n$ for all n, hence one may hope that the additional nonabelian information contained in $X(\mathbb{Q}_p)_n$ for n large may be sufficient to detect arithmetic properties of the set $X(\mathbb{Q})$. For example:

Conjecture 1. *[Kim, [42]] Let X be a curve of genus greater than 1. For $n \gg 0$, $X(\mathbb{Q}_p)_n$ is finite.*

In fact, in [4] it is conjectured that for n large enough, one can recover $X(\mathbb{Q})$ from $X(\mathbb{Q}_p)_n$.

Conjecture 2. *[Kim, [4]] For $n \gg 0$,*

$$X(\mathbb{Q}_p)_n = X(\mathbb{Q})$$

As is explained in [42], Conjecture 1 is implied by the following conjecture, which is a special case of part of the Bloch-Kato conjectures on the Galois cohomology of motives:

Conjecture 3 (Bloch,Kato [15], Conjecture 5.3)**.** *For any smooth projective variety Z over $\mathbb{Q}$, any $n > 0$ and $2r - 1 \neq n$,*

$$ch_{n,r} : K^{(r)}_{2r-1-n}(Z) \otimes \mathbb{Q}_p \xrightarrow{\simeq} H^1_g(G_{\mathbb{Q}}, H^n(\overline{Z}, \mathbb{Q}_p(r))$$

is an isomorphism.

On the other hand, the relationship between Conjecture 2 and other conjectures on Galois cohomology is more mysterious. For instance, although in appearance it is very similar to Grothendieck's section conjecture there is no obvious implication in either direction.

To pass from controlling the size of global Galois cohomology inside local cohomology to obtaining finiteness of $X(\mathbb{Q}_p)_n$, one needs to understand the maps

$$j_{n,p} : X(\mathbb{Q}_p) \to H^1_f(G_p, U_n)$$

Theorem 6 (Kim,[42]). *The local unipotent Kummer maps $j_{n,p}$ are Zariski dense, and on each residue disc are given by p-adic power series.*

An immediate consequence is that whenever the localisation map

$$H^1_{f,\mathcal{L}}(G_T, U_n) \to H^1_f(G_p, U_n)$$

is not Zariski dense, then the intersection of $H^1_{f,\mathcal{L}}(G_T, U_n)$ with $X(\mathbb{Q}_p)$ is finite, as on each residue disc it is given by the zeroes of a non-unital p-adic power series, which have only have finitely many zeroes by p-adic Weierstrass preparation.

Corollary 1 (Kim,[42]). *Conjecture 1 holds whenever*

$$\mathrm{loc}_p\, H^1_{f,\mathcal{L}}(G_T, U) \to H^1_f(G_p, U)$$

is not Zariski dense.

Hence it is known that the nonabelian Chabauty method gives an analytic description of a finite set containing the set of rational points of X whenever one can show that the image of the global Selmer variety in the local Selmer variety is small.

This motivates the following definition:

Definition 7. Say that a finite dimensional G_T-stable quotient U' of $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$ *satisfies the dimension hypothesis* if the graded pieces $U'[i]$ satisfy

$$\mathrm{rk}\,\mathrm{Jac}(X)(\mathbb{Q}) + \sum_{i>1} \dim_{\mathbb{Q}_p} H^1_f(G_T, U'[i]) < \sum_{i>0} \dim_{\mathbb{Q}_p} H^1_f(G_p, U'[i])$$

where $U'[i]$ denotes the ith graded piece of the central series filtration of U' (so $U'[1] = U'^{\mathrm{ab}}$, $U'[2] = [U', U']/[U', [U', U']]$ etc).

We recall a standard method for proving non-density of the localisation map.

Proposition 1. *Conjecture 1 holds for U whenever U satisfies the dimension hypothesis.*

Proof. Recall the sequence of pointed varieties

$$H^1_f(G_T, U[i]) \to H^1_f(G_T, U_i) \to H^1_f(G_T, U_{i-1})$$

is exact, hence

$$\dim H^1_f(G_T, U) \leq \sum \dim H^1_f(G_T, U[i]) \tag{2.2}$$

Since the local conditions at primes away from p define a finite subset of $\prod_{v \in T_0} H^1(G_v, U)$, the dimension of $H^1_f(G_T, U)$ equals that of $H^1_{f,\mathcal{L}}(G_T, U)$. On the other hand, the dimension of $H^1_f(G_p, U)$ will be equal to that of its graded pieces (see [42], or [15] for the abelian analogue). □

2.2.3 Diophantine Application of $H^1_{f,\mathcal{L}}(G_T, U_2)$

Before introducing new methods to study the localisation map on Selmer variety, we pause to record some examples where one can prove non-density of the localisation map for the Selmer variety using the dimension hypothesis. This subsection will only concern the unipotent Kummer map at depth 2, and below U will denote a quotient of U_2. As this thesis is almost entirely concerned with the fundamental group at depth 2, we briefly note that, as well as predicting that for a fixed curve X, $X(\mathbb{Q}_p)_n$ is finite for n large, the Bloch-Kato conjectures also predict that for a given X one can find a suitably large l-primary cover X' for which $X'(\mathbb{Q}_p)_2$ is finite. In fact rather more is true. Recall that given a finite étale cover

$$X' \to X,$$

Galois with group Γ, we have a surjection

$$\sqcup_\alpha X'^{(\alpha)}(\mathbb{Q}) \to X(\mathbb{Q})$$

where α is an $H^1(G_\mathbb{Q}, \Gamma)$ class coming from a rational point on X via

$$X(\mathbb{Q}) \to H^1(G_\mathbb{Q}, \Gamma),$$

and $X'^{(\alpha)}$ is the twist of X' by α. Hence the problem of describing $X(\mathbb{Q})$ is subsumed in the problem of describing $X'^{(\alpha)}(\mathbb{Q})$ for all α coming from $X(\mathbb{Q})$. We show that there is a cover X' such that the Bloch-Kato conjectures predict that $X'^{(\alpha)}(\mathbb{Q}_p)_2$ is finite for all α - so that taking the union over all α gives a finite set containing $X(\mathbb{Q})$. The depth 1 version of this - i.e. applying Chabauty's theorem to covers of X - is used in by Flynn and Wetherell in [63], [33],[34] to study $X(\mathbb{Q})$ in situations where Chabauty's theorem cannot be applied, hence the generalisation to studying $X(\mathbb{Q})$ via nonabelian Chabauty on covers is a natural approach.

Proposition 2. *Let (X, b) be a smooth pointed curve over $\mathbb{Q}$, of genus $g > 1$. Fix a prime l not equal to p, and let K be the fixed field of $J[l]$, where J denotes the Jacobian variety of X. Let $r = \dim_{\mathbb{F}_p} H^1(G_{K,T\cup\{l\}}, \mathbb{Z}/l\mathbb{Z})$. Let*

$$(X', b') \to (X, b)$$

be an unramified Galois cover (defined over $\mathbb{Q}$) of degree l^b, for some $b > 0$. Then the Bloch-Kato conjectures imply that $X'(\mathbb{Q}_p) \cap H^1_{f,\mathcal{L}}(G_{T\cup l}, U_2)$ is finite whenever

$$l^b > \frac{2r-1}{g-1}$$

To prove this Proposition it will be useful to recall some more implications of the conjecture of Bloch and Kato above. Our reference is the article of Fontaine and Perrin-Riou [35]. In particular we make use all the following corollary of Fontaine and Perrin-Riou (see [35], Remark 2.2.2, following Proposition 2.2.1)

Proposition 3. *Let W be a finite dimensional $\mathbb{Q}_p$-representation of G_T. Then*

$$\begin{aligned}&\dim_{\mathbb{Q}_p}(H^0(G_T, W)) - \dim_{\mathbb{Q}_p}(H^1_f(G_T, W)) + \dim_{\mathbb{Q}_p}(H^1_f(G_T, W^*(1))) \\ &- \dim_{\mathbb{Q}_p}(H^0_f(G_T, W^*(1))) = -\dim_{\mathbb{Q}_p}(D_{dR}(W)/F^0) + \dim_{\mathbb{Q}_p}(H^0(\mathbb{R}, W)).\end{aligned}$$

For the ease of the reader we note that the terminology is somewhat different from that used in Fontaine Perrin-Riou: in their notation

$$\begin{aligned}
&\widetilde{H}^0_f(F,V) = H^0(F,V),\\
&\widetilde{H}^1_f(F,V) = H^1_f(F,V),\\
&\widetilde{H}^2_f(F,V) = (H^1_f(F,V^*(1)))^*,\\
&\widetilde{H}^3_f(F,V) = (H^0(F,V^*(1)))^*\\
&t_p = D_{\mathrm{dR}}(W)/F^0.
\end{aligned}$$

Lemma 6. *The conjecture of Bloch and Kato (conjecture [15]) implies*

$$H^1_f(G_T, \overline{\wedge^2 V}^*(1)) = 0.$$

Proof. Since $\overline{\wedge^2 V}^*$ is a direct summand of $H^1_{ét}(\overline{X}, \mathbb{Q}_p)^{\otimes 2}$ it is enough to prove this for

$$H^1_{ét}(\overline{X}, \mathbb{Q}_p)^{\otimes 2},$$

which by the Kunneth formula is a direct summand of $H^2_{ét}(\overline{X \times X}, \mathbb{Q}_p)$. The conjecture of Bloch and Kato implies that $H^1_g(G_T, H^2_{ét}(\overline{X \times X}, \mathbb{Q}_p))$ is isomorphic to $K^{(1)}_{-1}(X) \otimes \mathbb{Q}_p$, which is zero. Hence $H^1_f(G_T, H^2_{ét}(\overline{X \times X}, \mathbb{Q}_p))$ is zero. □

The formula of Fontaine and Perrin-Riou imply the following:

Corollary 2. *The dimensions of* $H^1_f(G_p, \overline{\wedge^2})$ *and* $H^1_f(G_T, \overline{\wedge^2})$ *satisfy the inequality*

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, \overline{\wedge^2 V}) - \dim_{\mathbb{Q}_p} H^1_f(G_T, \overline{\wedge^2 V}) \geq g(g-1) \tag{2.3}$$

Proof. By the formula of Fontaine and Perrin-Riou above we have

$$\begin{aligned}
&\dim_{\mathbb{Q}_p} H^1_f(G_p, \wedge^2 V) - \dim_{\mathbb{Q}_p} H^1_f(G_T, \wedge^2 V) = \dim H^0(G_{\mathbb{R}}, \wedge^2 V)\\
&- \dim H^0(G_T, \wedge^2 V) + \dim H^0(G_T, \wedge^2 V^*(1)) + \dim H^1_f(G_T, \wedge^2 V^*(1))
\end{aligned}$$

By Lemma 6 conjecture of Bloch and Kato implies $H^1_f(G_T, \wedge^2 V^*(1)) = 0$. By Poincaré duality the dimension of $H^0(G_{\mathbb{R}}, V)$ is equal to the dimension of the minus eigenspace of V under complex conjugation, hence they both have dimension g. This implies that

$$\dim_{\mathbb{Q}_p} H^0(G_{\mathbb{R}}, \wedge^2 V) = g(g-1)$$

For weight reasons $\dim H^0(G_T, \wedge^2 V) = 0$, and since $\mathbb{Q}_p(1)$ is a direct summand of $\wedge^2 V$,

$$\dim H^0(G_T, \wedge^2 V^*(1)) \geq 1$$

Hence

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, \wedge^2 V) - \dim_{\mathbb{Q}_p} H^1_f(G_T, \wedge^2 V) \geq g(g-1)+1$$

Finally note that

$$\dim H^1_f(G_p, \overline{\wedge^2 V}) = \dim H^1_f(G_p, \wedge^2 V) - 1$$

and

$$\dim H^1_f(G_T, \overline{\wedge^2 V}) = \dim H^1_f(G_T, \wedge^2 V)$$

again using the decomposition $\wedge^2 V \simeq \overline{\wedge^2 V} \oplus \mathbb{Q}_p(1)$. □

Proof of Proposition 2. Let $V' := H^1_{\acute{e}t}(\overline{X'}, \mathbb{Q}_p)^*$. As X has good reduction outside T and the cover $X' \to X$ is l-primary the curve X' has good reduction outside $T \cup \{l\}$. We want to show that X' as in the Theorem satisfies the dimension hypothesis

$$\dim H^1_f(G_p, \overline{\wedge^2 V'}) - \dim H^1_f(G_{T\cup\{l\}}, \overline{\wedge^2 V'}) > \operatorname{rk}\operatorname{Jac}(X') - \dim H^1_f(G_p, V')$$

The key step is the bound on the Mordell-Weil rank of the Jacobian of an l-primary cover, given by Ellenberg in [31]. We recall the argument: first note for that any finite $G_{\mathbb{Q}}$-stable quotient Γ of $\pi_1^{\acute{e}t,l}(\overline{X}, b)$, the central series gives a descending filtration whose graded pieces $\Gamma[i]$ are abelian $G_{\mathbb{Q}}$-representations factoring through $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ factoring through $\mathrm{Gal}(K|\mathbb{Q})$.

To bound the Mordell-Weil rank of X' over $\mathbb{Q}$, it is enough to bound the Mordell-Weil rank over K, and to bound this it is enough to bound $H^1(G_{K,T\cup\{l\}}, H^1(\overline{X}', \mu_l))$. Since $H^1(\overline{X}', \mu_l) \simeq \pi_1^{\acute{e}t,l}(\overline{X}', b')^{ab} \otimes \mathbb{Z}/l\mathbb{Z}$, and $\pi_1^{\acute{e}t,l}(\overline{X}', b')$ is a subgroup of $\pi_1^{\acute{e}t,l}(\overline{X}, b)$ (as the degree of the cover is a power of l), using the Jordan-Holder series for the pro-l group $\pi_1^{\acute{e}t,l}(\overline{X}, b)$, we see that $H^1(\overline{X}', \mu_l)$ admits a filtration whose associated graded $\mathrm{gr}\, H^1(\overline{X}', \mu_l)$ has a G_K action which factors through the action of G_K on $H^1(\overline{X}, \mu_l)$, and is hence trivial.

Lemma 7. *The rank of the group* $\mathrm{Jac}(X')(\mathbb{Q})$ *is bounded by* $2g'r$.

Proof. In fact we will show that that the larger group $\mathrm{Jac}(X')(K)$ satisfies this inequality. By the Kummer map for $\mathrm{Jac}(X')$ we have, for any field extension F of $\mathbb{Q}$ the inequality

$$\mathrm{rk}_{\mathbb{Z}} \mathrm{Jac}(X')(F) \leq \dim_{\mathbb{F}_l} H^1(G_{K,T\cup\{l\}}, \mathrm{Jac}(X')[l]) \tag{2.4}$$

is satisfied. Arguing as above

$$\dim_{\mathbb{F}_l} H^1(G_{K,T\cup\{l\}}, \mathrm{Jac}(X')[l]) \leq (\dim_{\mathbb{F}_l} \mathrm{Jac}(X')[l]).r \tag{2.5}$$

Putting all these together proves the lemma. □

To complete the proof of the Proposition it is sufficient to prove

$$\begin{aligned} g'(g'-1) &> 2g'r - \dim H^1_f(G_p, V) \\ &= 2g'r - g' \end{aligned}$$

and hence to prove that

$$g' > 2r$$

which follows from the fact that, by Riemann-Hurwitz, $g' = l^b(g-1)+1$. □

The rest of this section contains examples where one can prove finiteness of $X(\mathbb{Q}_p)_2$ unconditionally. Hence we restrict attention to curves admitting quotients U of U_2 for which bounding the size of $H^1_f(G_T, [U,U])$ is tractable.

Definition 8. For a weight -2 Galois representation W, a quotient U of U_2 is said to be a W-quotient of U_2 if $[L,L] \simeq W$.

Since $H^1_f(G_T, \mathbb{Q}_p(1)) = 0$, and $H^1_f(G_p, \mathbb{Q}_p(1)) = 1$, $\mathbb{Q}_p(1)^{\oplus n}$-quotients are a natural source of examples of curves where the non-abelian Chabauty method refines Chabauty's method. $\mathbb{Q}_p(1)^{\oplus n}$ quotients of U arise from the Jacobian of X having extra endomorphisms.

Lemma 8. *Let* $V = H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p(1))$. *Then*

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_{G_T}(\mathbb{Q}_p(1), V^{\otimes 2}) \geq \dim_{\mathbb{Q}} \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X), \mathrm{Jac}(X)) \otimes \mathbb{Q}$$

Proof.

$$\begin{aligned}\mathrm{Hom}_{G_T}(\mathbb{Q}_p(1), V^{\otimes 2}) &\simeq \mathrm{Hom}_{G_T}(\mathbb{Q}_p, V^* \otimes V)\\ &\simeq \mathrm{End}_{G_T}(V, V)\end{aligned}$$

and we have an inclusion

$$\mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(X), \mathrm{Jac}(X)) \otimes_{\mathbb{Q}} \mathbb{Q}_p \hookrightarrow \mathrm{End}_{G_T}(V, V)$$

□

Of course, by Faltings' theorem this inclusion is an isomorphism, but we won't need this. To study the Selmer variety, we actually want to calculate

$$\mathrm{Hom}_{G_T}(\mathbb{Q}_p(1), \wedge^2 V)$$

Lemma 9. *Suppose* $\mathrm{Jac}(X)$ *is isogenous over* $\mathbb{Q}$ *to* $A_1^{n_1} \times \ldots \times A_m^{n_m}$*, where the* A_i *are polarised abelian varieties. Then*

$$\dim \mathrm{Hom}_{G_T}(\mathbb{Q}_p(1), \wedge^2 V) \geq \sum_i n_i(n_i+1)/2$$

Proof. Let $V_i := T_p A_i \otimes \mathbb{Q}_p$. The polarisation shows $\mathrm{Hom}_{G_T}(\mathbb{Q}_p(1), \wedge^2 V)$ is nonzero [49]. Since

$$\oplus_i \wedge^2 (V_i^{\oplus n_i}) \hookrightarrow \wedge^2 V,$$

and

$$\wedge^2 (V_i^{\oplus n_i}) \simeq (\wedge^2 V_i)^{\oplus n_i(n_i+1)/2} \oplus (\mathrm{Sym}^2 V_i)^{\oplus n(n-1)/2}$$

the result follows. □

2.2.4 Non-$\mathbb{Q}_p(1)$-examples

In general it is hard to find examples of Galois representations of weight -2 whose Galois cohomology can be bounded that are not Artin-Tate. One example is $\mathrm{Sym}^2 V_E$, where $V_E = T_p E \otimes \mathbb{Q}_p$ is the $\mathbb{Q}_p$-Tate module of an elliptic curve over $\mathbb{Q}_p$, by the following theorem:

Theorem 7 (Flach, [32]). *Let E be an elliptic curve, and let p be a prime of good reduction for which*

$$G_{\mathbb{Q}} \to GL(E[p])$$

is surjective. Then $\dim H^1_f(G_T, \mathrm{Sym}^2 V_E) = 0$.

Note that by Serre's open image theorem all but finitely many primes satisfy the hypotheses of the theorem.

Corollary 3. *Let X be a curve with Jacobian isogenous over $\mathbb{Q}$ to $E^n \times \prod A_i^{n_i}$, with E an elliptic curve over $\mathbb{Q}$ whose mod p Galois representation has full image, and A_i a polarised abelian variety. Suppose the Mordell-Weil rank of X is less than $n(2n-1)/2 + \sum n_i(n_i+1)/2$. Then the localisation map for the Selmer variety of U_2 is not dense.*

Proof. This follows from the arguments of the previous subsection, together with Flach's theorem, and the fact that

$$\dim_{\mathbb{Q}_p} H^1_f(G_p, \mathrm{Sym}^2 V_E) = \dim_{\mathbb{Q}_p} D_{dR}(\mathrm{Sym}^2 V_E)/F^0 = 2$$

and hence there is a quotient of U_2 satisfying the dimension estimate. □

Remark 1. In fact, we shall show in section 2.4 that for X as above, it is possible to prove non-density of the Selmer variety in situations where the dimension estimate is not satisfied for U.

2.3 Universal extensions and linearisation of Selmer varieties

In this section we explain how can relate the nonabelian cohomology varieties defined above with objects of linear algebra. This amounts to replacing the unipotent torsor $P(z,b)$ with the Galois representation $A(b,z)$. We construct a nontrivial morphism

$$\Psi : H^1_{f,\mathcal{L}}(G_T, U(b)) \to H^1_{f,T}(G_T, E(V, [L, L]))$$

of the nonabelian cohomology variety $H^1_{f,\mathcal{L}}(G_T, U_2(b))$ into a vector space

$$H^1_{f,T}(G_T, E(V, [L, L]))$$

of *abelian* cohomology classes, giving a way to add nonabelian cohomology classes. The space $E(V,[L,L])$ has a $[L,L]$ as a subobject, giving a way to construct elements of $H^1_{f,T}(G_T,[L,L])$ by taking suitable linear combinations of $\Psi(z_i)$ whose image in $H^1_f(G_T, E(V,[L,L])/[L,L])$ is trivial. This will then be used to define a map

$$\begin{aligned}\Theta :&(H^1_f(G_p,U)\times\prod_{v\in T_0}H^1(G_v,U))\times_{H^1_f(G_p,V)}H^1_f(G_T,V)\\ &\to H^1_f(G_p,[L,L])\times\prod_{v\in T_0}H^1(G_v,[L,L])\end{aligned}$$

such that

$$\Theta\circ(\mathrm{loc}\times\pi_*)H^1_{f,\mathcal{L}}(G_T,U)\subset \mathrm{loc}\,H^1_{f,T}(G_T,[L,L])$$

2.3.1 Definitions and basic properties

Lemma 10. *Let W_1 and W_2 be finite dimensional continuous $\mathbb{Q}_p$-representations of G, such that*

$$\mathrm{Hom}_G(W_1,W_2)=\mathrm{Hom}_G(W_2,W_1)=0.$$

Then there is a universal extension $\widetilde{E}(W_1,W_2)$ in the category of finite dimensional representations of $\mathbb{Q}_p$-representations of G, such that:

- *$\widetilde{E}(W_1,W_2)$ lies in an exact sequece*

$$0\to W_2\to\widetilde{E}(W_1,W_2)\to W_1\otimes\mathrm{Ext}^1(W_1,W_2)\to 0$$

- *For an extension*

$$0\to W_2\xrightarrow{\iota}W_3\xrightarrow{\pi}W_1\to 0$$

  there is a unique morphism $e_{(W_3,\iota,\pi)}=e_{W_3}:W_3\to E(W_1,W_2)$ fitting in a commutative diagram of Galois representations

$$\begin{array}{ccccccccc}0 & \longrightarrow & W_2 & \longrightarrow & W_3 & \longrightarrow & W_1 & \longrightarrow & 0\\ & & \| & & \downarrow & & \downarrow{\scriptstyle 1_{W_1}\otimes[W_3]} & & \\ 0 & \longrightarrow & W_2 & \longrightarrow & \widetilde{E}(W_1,W_2) & \longrightarrow & W_1\otimes\mathrm{Ext}^1(W_1,W_2) & \longrightarrow & 0\end{array}$$

- $\widetilde{E}(W_1, W_2)$ *is unique up to unique isomorphism - that is, for any other* E' *satisfying the above two conditions, there is a unique isomorphism* $E' \to \widetilde{E}(W_1, W_2)$ *which is the indentity on the subspaces* W_2 *and the quotients* $\mathrm{Ext}^1(W_1, W_2) \otimes W_1$.

Proof. The construction is standard: take $\widetilde{E}(W_1, W_2)$ to be a representative of the class $[E]$ in $\mathrm{Ext}^1(W_1 \otimes \mathrm{Ext}^1(W_1, W_2), W_2)$ corresponding to the identity via

$$\mathrm{Ext}^1(W_1 \otimes \mathrm{Ext}^1(W_1, W_2), W_2) \simeq \mathrm{Ext}^1(W_1, W_2)^* \otimes \mathrm{Ext}^1(W_1, W_2)$$

□

We shall repeatedly make use of a minor variant of the space $E(W_1, W_2)$, which keeps track of extra endomorphisms in the Jacobian of X: let R be a finite $\mathbb{Q}_p$-algebra, and W_1 a continuous G_T-representation with a commuting left action of R. For any continuous G_T-representation W_2, we define a right action of R on $W_1 \otimes W_2 = \mathrm{Hom}(W_1, W_2)$ by taking $\psi.r$ to be the homomorphism

$$w \mapsto \psi(r.w)$$

Lemma 11. *Let* W_1, W_2 *and* R *be as above. There is a Galois representations* $\widetilde{E}_R(W_1, W_2)$, *sitting in a short exact sequence*

$$0 \to W_2 \to \widetilde{E}_R(W_1, W_2) \to W_1 \otimes_R \mathrm{Ext}^1(W_1, W_2) \to 0$$

such that for any short exact sequence of Galois representations

$$0 \to W_2 \to W_3 \to W_1 \to 0$$

there is a unique morphism

$$e_{R,(W_3,\iota,\pi)} = e_{R,W_3} : W_3 \to \widetilde{E}_R(W_1, W_2)$$

extending to a commutative diagram of Galois representations

$$\begin{array}{ccccccccc}
0 & \longrightarrow & W_2 & \longrightarrow & W_3 & \longrightarrow & W_1 & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow {\scriptstyle 1_{W_1} \otimes [W_3]} & & \\
0 & \longrightarrow & W_2 & \longrightarrow & \widetilde{E}_R(W_1, W_2) & \longrightarrow & W_1 \otimes_R \mathrm{Ext}^1(W_1, W_2) & \longrightarrow & 0
\end{array}$$

where the short exact sequences are as before.

Proof. The proof is exactly as in the previous Lemma: take $\widetilde{E}_R(W_1, W_2)$ to be a representative of the class $[E]$ in $\mathrm{Ext}^1(W_1 \otimes_R \mathrm{Ext}^1(W_1, W_2), W_2)$ corresponding to the identity via

$$\mathrm{Ext}^1(W_1 \otimes_R \mathrm{Ext}^1(W_1, W_2), W_2) \simeq \mathrm{Ext}^1(W_1, W_2)^* \otimes_R \mathrm{Ext}^1(W_1, W_2)$$

□

The extension $\widetilde{E}_R(W_1, W_2)$ contains representations which do not come from geometry, so it will be convenient to replace it with a subobject.

Definition 9. Define $E_R(W_1, W_2)$ to be the extension of $\mathrm{Ext}^1_f(W_1, W_2) \otimes W_1$ by W_2 obtained by pulling $\widetilde{E}_R(W_1, W_2)$ back by

$$\mathrm{Ext}^1_f(W_1, W_2) \otimes W_1 \to \mathrm{Ext}^1(W_1, W_2) \otimes W_1$$

Replacing G_T by $G_{\mathbb{Q}_p}$, one may similarly construct an extension of $H^1_f(G_p, W_1^* \otimes W_2) \otimes W_1$ by W_2, which will be denoted by $E_{p,R}(W_1, W_2)$.

In fact the map e_R is independent of π, in the following sense. Let R be a subalgebra of $\mathrm{End}_{G_T}(W_1)$. Let W_3 be an extension of W_1 by W_2:

$$0 \to W_2 \xrightarrow{\iota} W_3 \xrightarrow{\pi} W_1 \to 0 \tag{2.6}$$

and let α be an element of $R^\times$. Then α induces a new short exact sequence

$$0 \to W_2 \xrightarrow{\iota} W_3 \xrightarrow{\alpha \circ \pi} W_1 \to 0 \tag{2.7}$$

Lemma 12.

$$e_{R,(W_3,\iota,\pi)} = e_{R,(W_3,\iota,\alpha\circ\pi)}$$

Proof. The short exact sequence 2.6 is exactly the pull-back of 2.7 by the morphism α. Hence

$$[(W_3, \iota, \pi)] = [(W_3, \iota, \alpha \circ \pi)]\alpha$$

This gives the identity in $H^1(G, W_1^* \otimes W_2) \otimes \mathrm{Hom}(W_1, W_1)$

$$\begin{aligned}[(W_3, \iota, \pi)] \otimes_R 1_{W_1} &= [(W_3, \iota, \alpha \circ \pi)]\alpha \otimes_R 1_{W_1} \\ &= [(W_3, \iota, \alpha \circ \pi)] \otimes_R \alpha 1_{W_1}\end{aligned}$$

Let $\overline{e}_{R,W_3}$ denote the composite of e_{R,W_3} with the projection

$$E_R(W_1, W_2) \to \mathrm{Ext}^1_f(W_1, W_2) \otimes_R W_1$$

Then by commutativity

$$\begin{aligned}
\overline{e}_{R,(W_3,\iota,\alpha\circ\pi)} &= ([(W_3, \iota, \alpha \circ \pi)] \otimes_R 1_{W_1}) \circ \alpha \circ \pi \\
&= ([(W_3, \iota, \alpha \circ \pi)] \otimes_R \alpha.1_{W_1}) \circ \pi \\
&= [(W_3, \iota, \pi)] \otimes_R 1_{W_1}) \circ \pi = \overline{e}_{R,(W_3,\iota,\pi)}
\end{aligned}$$

Hence by uniqueness of the lift of $\overline{e}_{R,(W_3,\iota,\pi)}$ to W_3 the two homomorphisms are equal.

□

Remark 2. The case of interest for this thesis is where W_1 is taken to be the representation $V = T_p \,\mathrm{Jac}(X) \otimes \mathbb{Q}_p$. Suppose that the Jacobian of X is isogenous to $A_1^{n_1} \times \ldots \times A_m^{n_m}$, where A_i is simple with endomorphism algebra an order in K_i, and the A_i are pairwise non-isogenous. Let $V_i := \mathbb{Q}_p \otimes T_p(A_i)$. Then we may take as our algebra R the associative algebra $\prod_{i=1}^m \mathrm{Mat}_{n_i}(K_i \otimes \mathbb{Q}_p)$. $H^1(G_T, V^* \otimes [L, L]) \otimes_R V$ is then isomorphic to $\oplus_{i=1}^m H^1(G_T, V_i) \otimes_{K_i \otimes \mathbb{Q}_p} H^1(G_T, V_i^* \otimes [L, L])$, by the following lemma:

Lemma 13. *Let V and W be K-vector spaces. Then*

$$V^{\oplus n} \otimes_{\mathrm{Mat}_n(K)} W^{\oplus n} \simeq V \otimes_K W$$

and the contraction morphism

$$V^{\oplus_n} \otimes_K W^{\oplus n} \to V^{\oplus n}_{\mathrm{Mat}_n(R_0)} W^{\oplus n} \simeq V \otimes_K W$$

sends

$$(v_1, \ldots, v_n) \otimes_K (w_1, \ldots, w_n) \tag{2.8}$$

to $\sum_{i,j} v_i \otimes w_i$.

Proof. By definition

$$V^{\oplus n} \otimes_{\mathrm{Mat}_n(K)} W^{\oplus n} \simeq V^{\oplus n} \otimes_K W^{\oplus n}/Z$$

where Z is the span of $vM \otimes w - v \otimes Mw$, where $v \in V^{\oplus n}$, $w \in W^{\oplus n}$ and $M \in \mathrm{Mat}_n(K)$. Let π_i denote the projections $V^{\oplus n} \to V$ and $W^{\oplus n} \to W$ to the ith factor, and ι_i the inclusions into the ith factor, and let e_{ij} denote the n by n matrix with i,j-th entry equal to 1 and all others equal to 0. Then Z is spanned by the images of the morphisms

$$V \otimes_K W \to V^{\oplus n} \otimes_K W^{\oplus n}$$

$$v \otimes w \mapsto (\iota_i v)e_{kl} \otimes \iota_j w - (\iota_i v) \otimes e_{kl}(\iota_j w)$$

It's easy to see that this is spanned by the images of the maps

$$\iota_i \otimes \iota_j : V \otimes_K W \to V^{\oplus n} \otimes_K W^{\oplus n}$$

for $i \neq j$ and

$$\iota_i \otimes \iota_i - \iota_j \otimes \iota_j : V \otimes_K W \to V^{\oplus n} \otimes_K W^{\oplus n}$$

which completes the proof. □

In this thesis $W_1 = V$, and $W_2 = [L, L]$, and the extensions of V by $[L, L]$ coming from the twists of $IA(b)$ by equivariant V-torsors. This motivates the following definition:

Definition 10. Let W_0, W_1, W_2 be crystalline G_T-representations such that $\mathrm{Hom}(W_1, W_2) = \mathrm{Hom}(W_2, W_1) = 0$. Let

$$\tau : W_0 \to \mathrm{Hom}(W_1, W_2)$$

be a homomorphism of Galois representations. Define the extension

$$0 \to W_2 \to E(\tau, W_1, W_2) \to H^1_f(G_T, W_0) \otimes W_1 \to 0$$

to be an extension corresponding to

$$\tau_* : H^1_f(G_T, W_0) \to H^1_f(G_T, \mathrm{Hom}(W_1, W_2))$$

via

$$\mathrm{Ext}^1_f(H^1_f(G_T, W_0) \otimes W_1, W_2) \simeq \mathrm{Hom}(H^1_f(G_T, W_0), H^1_f(G_T, \mathrm{Hom}(W_1, W_2)))$$

As before, $E(\tau, W_1, W_2)$ has the property that for any c in $H^1_f(G, W_0)$, and extension

$$0 \to W_2 \to W_3 \to W_1 \to 0$$

such that $[W_3] = \tau_*(c)$ for c in $H^1_f(G_T, W_0)$, there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_2 & \longrightarrow & W_3 & \longrightarrow & W_1 & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow {\scriptstyle 1_{W_1} \otimes [c]} & & \\ 0 & \longrightarrow & W_2 & \longrightarrow & E(,\tau, W_1, W_2) & \longrightarrow & W_1 \otimes H^1_f(G_T, W_0) & \longrightarrow & 0 \end{array}$$

We similarly define the $G_{\mathbb{Q}_p}$ -representation $E_p(\tau, W_1, W_2)$ to be the corresponding extension of $H^1_f(G_p, W_0) \otimes W_1$ by W_2.

2.3.2 Linearising Selmer varieties

The use of the universal extension $E(W_1, W_2)$ is that it gives a way to linearise the algebra of mixed objects with fixed graded pieces. Suppose we are given a representation M, admitting a G_T-stable filtration

$$M = M_0 \supset M_1 \supset M_2 \supset M_3 = 0$$

and isomorphisms

$$\alpha_1 : M_0/M_1 \simeq \mathbb{Q}_p$$

$$\alpha_2 : M_1/M_2 \simeq W_1$$

$$\alpha_3 : M_2 \simeq W_2$$

Such a datum will be referred to as a mixed representation with graded pieces $\mathbb{Q}_p, W_1$ and W_2. The isomorphisms α_i will be referred to as the *frames* of the mixed extension M. The first isomorphism determines an element $[M]$ of $H^1(G, M_1)$. On the other hand, the other isomorphisms define a map

$$e_{M_1} : M_1 \to E(W_1, W_2)$$

Hence this determines a class $e_{M_1 *}[M]$ in $H^1(G, E(W_1, W_2))$. This will often simply be denoted by $[M]$. The image in $H^1_f(G_T, W_1) \otimes \mathrm{Ext}^1_f(W_1, W_2)$ will be denoted by

$\overline{[M]}$. Recall that by Lemma 2.6, the extension class $[M]$ is *independent* of α_2, and only depends on α_1 and α_3. In the formalism of [36] we may say that $[M]$ is an invariant of M as a '2-framed object'.

These constructions are now applied in the case $W_1 = V, W_2 = \overline{\wedge^2 V}$. Each 'universal extension' E defined above will give maps Ψ and Ψ_p from $H^1_f(G_T, U)$ to $H^1_f(G_T, E)$ and $H^1_f(G_p, U)$ to $H^1_f(G_p, E)$ respectively.

Lemma 14. *The extension* $[IA_2(b)]$ *in* $\mathrm{Ext}^1(V, \overline{\wedge^2 V})$ *is crystalline at* p *and splits at all* v *not equal to* p.

Proof. For $v = p$ this is proved by Olsson [53]. For v in T_0, it follows from the weight monodromy conjecture for curves, since $V^* \otimes \overline{\wedge^2 V}$ has weight -1. □

Hence for any P in $H^1_{f,\mathcal{T}}(G_T, U)$, $[A(b)^{(P)}]$ defines an element of $H^1_{f,T}(G_T, E(V, [L, L]))$.

Definition 11. Define

$$\Psi : \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U(b))] \to H^1_{f,T}(G_T, E(V, [L, L]))$$

$$P \mapsto [A(b)^{(P)}]$$

If the cohomology class is the torsor of paths from b to z then $\Psi(P)$ will be denoted $\Psi(z)$, or sometimes by $\Psi(b, z)$. Define $\overline{\Psi}$ to be the composite

$$\mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U(b))] \to H^1_{f,T}(G_T, E(V, [L, L])) \to H^1_f(G_T, V) \otimes H^1_f(G_T, V^* \otimes [L, L])$$

Similarly define

$$\Psi_p : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p E(V, [L, L]))$$

and

$$\overline{\Psi}_p : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p, V) \otimes H^1_f(G_p, V^* \otimes [L, L])$$

We have similar definitions for the modified versions of E:

Definition 12. For a unital $\mathbb{Q}_p$-algebra $R \subset \mathrm{End}_{G_T}(V)$, define

$$\Psi_R : \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U)] \to H^1_{f,T}(G_T, E_R(V, [L, L]))$$
$$P \mapsto [A(b)^{(P)}]$$
$$\overline{\Psi}_R : \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U)] \to H^1_f(G_T, V) \otimes_R H^1_f(G_T, V^* \otimes [L, L])$$
$$P \mapsto \overline{[A(b)^{(P)}]}$$
$$\Psi_{R,p} : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p, E_R(V, [L, L]))$$
$$P \mapsto [A(b)^{(P)}]$$
$$\overline{\Psi}_{R,p} : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p, V) \otimes_R H^1_f(G_p, V^* \otimes [L, L])$$
$$P \mapsto \overline{[A(b)^{(P)}]}$$

Recall that when X is a hyperelliptic curve the extension class $[IA(b)]$ was in the image of $H^1_f(G_T, V)$ under τ_*. Hence in this situation $E(IA(b))$ may be replaced by the subspace $E(\tau, V, [L, L])$.

Definition 13. Suppose U is such that there is c_0 in $H^1_f(G_T, V)$ such that

$$[IA(b)] = \tau_*(c)$$

Then define

$$\Psi_\tau : \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U)] \to H^1_{f,T}(G_T, E(\tau, V, [L, L])) \tag{2.9}$$
$$P \mapsto e_{\tau,IA(b)*}[A(b)^{(P)}]$$
$$\overline{\Psi}_\tau : \mathbb{Q}_p[H^1_{f,\mathcal{L}}(G_T, U)] \to H^1_f(G_T, V) \otimes H^1_f(G_T, V) \tag{2.10}$$
$$P \mapsto \overline{e_{\tau,IA(b)*}[A(b)^{(P)}]}$$
$$\Psi_{\tau,p} : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p, E(\tau, V, [L, L])) \tag{2.11}$$
$$P \mapsto e_{\tau,IA(b)*}[A(b)^{(P)}]$$
$$\overline{\Psi}_{\tau,p} : \mathbb{Q}_p[H^1_f(G_p, U)] \to H^1_f(G_p, V) \otimes H^1_f(G_p, V) \tag{2.12}$$
$$P \mapsto \overline{e_{\tau,IA(b)*}[A(b)^{(P)}]}$$

Lemma 15. *Suppose* $V \simeq V_1^{\oplus n_1} \oplus \ldots \oplus V_k^{\oplus n_k}$, *and* $R = \prod_{i=1}^k \mathrm{Mat}_{n_i}(\mathbb{Q}_p)$. *Let*

$$\iota_{ij} : V_i \to V$$

$$\pi_{ij} : V \to V_i$$

be the inclusions and projections for the j*th copy of* V_i, *so that* $\sum_{i,j} \iota_{ij} \circ \pi_{ij} = 1$. *Then*

$$\overline{\Psi}_R(c) = \sum_{i,j} (\pi_{ij*}(\pi_*(P)) \otimes_{\mathbb{Q}_p} (\iota_{ij*}([IA(b)] + \tau_*(\pi_*(P)))$$

in $H^1_f(G_T, V) \otimes_R \mathrm{Ext}^1_f(V, [L, L]) \simeq \oplus_i H^1_f(G_T, V_i) \otimes \mathrm{Ext}^1(V_i, [L, L])$. *In particular, if for all* i,

$$\sum_j (\pi_{ij*}(\pi_*(P)) \otimes_{\mathbb{Q}_p} (\iota_{ij*}([IA(b)] + \tau_*(\pi_*(P)))) = 0$$

in $H^1_f(G_T, V_i) \otimes \mathrm{Ext}^1(V_i, [L, L])$, *then*

$$\Psi_R(c) \in H^1_f(G_T, [L, L])$$

Proof. By definition,

$$\overline{\Psi}_R(c) = \pi_*(P) \otimes_R ([IA(b)] + \tau_* \pi_*(P))$$

By Lemma 13, this equals

$$\sum_{i,j} \pi_{ij*} \pi_*(P) \otimes_{\mathbb{Q}_p} \iota_{ij*}([IA(b)] + \tau_* \pi_*(P))$$

as required. □

2.3.3 Construction of other mixed extensions

In this section we construction some other mixed extensions, which are used to give further modifications to the maps Ψ above. The intuition behind the construction comes from the theory of height pairings: one may view p-adic height pairings (as constructed in [50]) on the group $H^1_f(G_T, V)$ as arising from obstructions in $\mathrm{Sym}^2 H^1_f(G_T, V)$ to the construction of $H^1_f(G_T, \mathbb{Q}_p(1))$ cohomology classes. In the previous section the obstruction to constructing a $\mathbb{Q}_p(1)$-cohomology class (or an $\overline{\wedge^2 V}$ cohomology class in the hyperelliptic case) came from $H^1_f(G_T, V)^{\otimes 2}$. This subsection gives a precise way to remove the $\wedge^2 H^1_f(G_T, V)$-component. This is used later to give explicit formulae for the image of $H^1_{f,\mathcal{L}}(G_T, U)$ in $H^1_f(G_p, U)$.

Definition 14. Let W_1, W_2 be extensions of $\mathbb{Q}_p$ by V. Define $\overline{W_1W_2}$ to be the quotient of $W_1 \otimes W_2$ by $\ker(V \otimes V \to \overline{\wedge^2 V})$. Then $\overline{W_1W_2}$ is a mixed representation with graded pieces $\mathbb{Q}_p, V^{\oplus 2}$ and $\overline{\wedge^2 V}$.

An easy computation shows:

Lemma 16. *The image* $[\overline{W_1W_2}]$ *in* $H^1_f(G_T, V)^{\otimes 2}$ *is given by*

$$[W_1] \otimes [W_2] - [W_2] \otimes [W_1]$$

In particular, it lies in the image of $\wedge^2_R H^1_f(G_T, V)$*, and the induced morphism*

$$H^1_f(G_T, V) \otimes H^1_f(G_T, V) \to \wedge^2_R H^1_f(G_T, V)$$

is onto.

Proof. The extension classes in $\mathrm{Ext}^1(\mathbb{Q}_p, V \oplus V)$ is equal to $([W_1], [W_2])$, and via the inclusion

$$V \hookrightarrow V^* \otimes \overline{\wedge^2 V})$$

the extension class in $\mathrm{Ext}^1(V \oplus V, \overline{\wedge^2 V})$ is identified with $([W_1], -[W_2])$, completing the proof. □

The mixed extensions $\overline{W_1W_2}$ arise when comparing the different path spaces that can be obtained from three points on X:

Lemma 17.

$$\Psi(z, y) = \Psi(z, x) + \Psi(x, y) + \overline{\kappa(z - y)\kappa(z - x)}$$

Proof. This follows from the composition of paths morphism

$$A_2(z, x) \otimes A_2(x, y) \to A_2(z, y)$$

□

Let

$$0 \to V \to E_i \to \mathbb{Q}_p \to 0$$

$i = 1, 2$ be extensions of $\mathbb{Q}_p$ by V. Then $E_1 \otimes E_2$ is mixed with graded pieces $\mathbb{Q}_p$, $V^{\oplus 2}$ and $V \otimes V$. Via the isomorphism above, $V \otimes V$ admits a surjective morphism

$\mathbb{Q}_p(1)$, hence by pushing out we obtain a mixed extension with graded pieces $\mathbb{Q}_p$, $V^{\oplus 2}$, and $\mathbb{Q}_p(1)$, and hence an element of $H^1(G_T, E(V, \mathbb{Q}_p(1)))$, which is easily seen to given a well-defined function

$$H^1(G_T, V) \otimes H^1(G_T, V) \to H^1(G_T, E(V, \mathbb{Q}_p(1)))$$

denoted

$$c_1 \otimes c_2 \mapsto \overline{c_1 c_2}^{(+)}$$

The projection $\pi : V \otimes V \to \mathbb{Q}_p(1)$ defines a map

$$\mathrm{Ext}^1(V, V \otimes V) \to \mathrm{Ext}^1(V, \mathbb{Q}_p(1))$$

There are two natural maps

$$H^1(G_T, V) \to \mathrm{Ext}^1(V, V \otimes V)$$

The following lemma is proved as in 16:

Lemma 18. *Suppose the projection $\pi : V \otimes V \to \mathbb{Q}_p(1)$ factors through $\wedge^2 V$. Then under the map*

$$H^1(G_T, E(V, \mathbb{Q}_p(1))) \to H^1(G_T, V) \otimes H^1(G_T, V)$$

$\overline{c_1 c_2}^{(+)}$ *mapsto* $c_1 \otimes c_2 - c_2 \otimes c_1$.

Definition 15. Let U be a $\mathbb{Q}_p(1)^{\oplus n}$ quotient of U_2. Define

$$\Gamma : H^1_f(G_T, V) \to H^1(G_T, V)^{\otimes 2}$$

to be the map

$$c \mapsto c \otimes_R IA(b)^{(c)}$$

By definition we have the identity

$$\overline{\Psi(c)} = \Gamma(\pi_*(P)) \tag{2.13}$$

for any $P \in H^1_f(G_T, U)$.

Definition 16. Define $H^1_f(G_T, E(V, \mathbb{Q}_p(1)))^{\mathrm{Sym}}$ to be the pull-back of $H^1_f(G_T, E(V, \mathbb{Q}_p(1)))$ by $\mathrm{Sym}^2 H^1_f(G_T, V_E) \to H^1(G_T, V_E)^{\otimes 2}$:

$$0 \to H^1(G_T, \mathbb{Q}_p(1)) \to H^1(G_T, E(V_E, \mathbb{Q}_p(1)))^{\mathrm{Sym}} \to \mathrm{Sym}^2 H^1_f(G_T, V_E) \to 0$$

Define

$$\Psi_R^{\mathrm{Sym}} : H^1_f(G_T, U) \to H^1_f(G_T, E(V, \mathbb{Q}_p(1)))^{\mathrm{Sym}}$$
$$P \mapsto \Psi_R(P) - \frac{1}{2}\sum[\overline{W_i Z_i}^{(+)}]$$

where

$$\overline{\Psi}(P) = \sum W_i \otimes Z_i$$

2.3.4 Equations for the localisation map

We now use the above to produce equations for $\mathrm{loc}\, H^1_{f,\mathcal{L}}(G_T, U) \subset H^1_f(G_p, U)$. The construction described in this subsection is entirely tautological, but it is useful for the more subtle questions of non-density of localisation maps and of computing the sets $X(\mathbb{Q}_p)_n$ defined in section 2. Define s to be a section of

$$H^1_{f,T}(G_T, E(V, [L, L])) \to \mathrm{Im}(H^1_{f,T}(G_T, E(V, [L, L])) \to H^1_f(G_T, V) \otimes \mathrm{Ext}^1_f(V, [L, L]))$$

Define

$$\begin{aligned} \Theta :& (H^1_f(G_p, U) \times \prod_{v \in T_0} H^1(G_v, U)) \times_{H^1_f(G_p, V)} \pi_*(H^1_f(G_T, U)) \\ &\to H^1_f(G_p, [L, L]) \times \prod_{v \in T_0} H^1(G_v, [L, L]) \\ &((P_p, (P_v)), c) \mapsto (\Psi_p(P_p), (\Psi_v(P_v))) - \mathrm{loc}(s(\overline{\Psi}(c))) \end{aligned} \tag{2.14}$$

Here the fibre product is via the maps

$$\mathrm{loc}_p : H^1_f(G_T, V) \to H^1_f(G_p, V)$$

and

$$\pi_* \times 0 : H^1_f(G_p, U) \times \prod_{v \in T_0} H^1(G_v, U) \to H^1_f(G_p, V)$$
$$(P_p, (P_v)) \mapsto \pi_* P_p$$

Lemma 19. *(i): The composite map*

$$\Theta \circ (\mathrm{loc}, \pi_*) : H^1_{f,\mathcal{L}}(G_T, U) \to (H^1_f(G_p, U) \times \prod_{v \in T_0} H^1(G_v, U)) \times_{H^1_f(G_p,V)} H^1_f(G_T, V)$$
$$\to H^1_f(G_p, [L, L]) \times \prod H^1(G_v, [L, L])$$

lands inside the image of $H^1_{f,T}(G_T, [L, L])$ *in* $H^1(G_p, [L, L]) \times \prod_v H^1(G_v, [L, L])$.

(ii): In particular, when

$$J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^1_f(G_p, V) \tag{2.15}$$

is an isomorphism, the image of the localisation map

$$\mathrm{loc}\, H^1_{f,\mathcal{L}}(G_T, U) \subset H^1_f(G_p, U) \times \prod H^1(G_v, U) \tag{2.16}$$

is contained inside the subvariety of $(P_p, (P_v))$ *satisfying*

$$\Theta((P_p, (P_v)), \pi_*(P)) \in \mathrm{loc}\, H^1_{f,T}(G_T, [L, L])$$

where Θ *is viewed as a map with source* $H^1_f(G_p, U) \times \prod_{v \in T_0} H^1(G_v, U)$ *via the isomorphism (2.15).*

Proof. By construction the image of $[A_2(b)]^(P) - s \circ \Gamma \circ \pi_*(P)$ in $H^1_f(G_T, V) \otimes \mathrm{Ext}^1_f(V, [L, L])$ is zero, hence $[A_2(b)]^(P) - s \circ \Gamma \circ \pi_*(P)$ defines an element of $H^1_f(G_T, [L, L])$, whose localisation is then given by $\Theta \circ (\mathrm{loc}, \Gamma)(P)$. □

2.4 Application to proving non-density

Recall that, as described in the introduction, the crucial global input in the non-abelian Chabauty method is the non-density of the morphism

$$H^1_{f,\mathcal{L}}(G_T, U_n) \to H^1_f(G_p, U_n)$$

There are at present two contexts in which such non-density can be proved. The first is when U satisfies the dimension estimate

$$\sum_{i=1}^{n} \dim_{\mathbb{Q}_p} H^1_f(G_T, U[i]) < \sum_{i=1}^{n} \dim_{\mathbb{Q}_p} H^1_f(G_p, U[i])$$

The second, developed in [44], is when one can prove non-density of the map on (abelian) Galois cohomology

$$H^1_f(G_T, L_n(z)) \to H^1_f(G_p, L_n(z))$$

(recall that $L_n(z)$ denotes the Lie algebra of $U_n(z)$). This is used in [44] to prove non-density of the localisation map for Selmer varieties of $\mathbb{P}^1 - \{0, 1, \infty\}$ over totally real fields, and uses crucially the non-triviality of the boundary maps from $H^1(G_T, L_{n-1})$ to $H^1(G_T, L[n])$, which may make it of limited applicability for curves over $\mathbb{Q}$.

In this section we describe situations in which linearisation of the Selmer variety can be used to give a new method for proving non-density in certain situations where the dimension estimate is not satisfied.

2.4.1 Genus 2 bielliptic curves

Let X be a genus 2 curve with Jacobian isogenous to $E \times E$ where E is an elliptic curve of Mordell-Weil rank 2. We take p to be a prime for which

$$G_{\mathbb{Q}} \to \mathrm{GL}(E[p])$$

is onto. Write $V_E := T_P E \otimes \mathbb{Q}_p$, so that $V \simeq V_E^{\oplus 2}$. Then $\overline{\wedge^2 V} \simeq \mathrm{Sym}^2 V_E \oplus \mathbb{Q}_p(1)^{\oplus 2}$. Let U be the quotient of U_2 with $[L, L] \simeq \mathrm{Sym}^2 V_E$. As explained above we may replace $E(V, \mathrm{Sym}^2 V_E)$ with the extension

$$0 \to \mathrm{Sym}^2 V_E \to E(V, \mathrm{Sym}^2 V_E) \to H^1_f(G_T, V) \otimes_R V \to 0$$

which is universal for extensions of V by $\mathrm{Sym}^2 V_E$ coming from $H^1_f(G_T, V)$.

The main theorem of this subsection is

Theorem 8. *Suppose E has Mordell-Weil rank 2. Then*

$$\mathrm{loc}_p : H^1_f(G_T, U) \to H^1_f(G_p, U)$$

is not dense

Remark 3. Note that U does not satisfy the dimension hypothesis: by Flach's theorem the dimension of $H^1_f(G_T, U)$ is 4, and by p-adic Hodge theory $H^1_f(G_p, \mathrm{Sym}^2 V_E)$ and $\mathrm{rk}\, E(\mathbb{Q})$ both have dimension 2. Looking tangentially, at a point z we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & H^1_f(G_T, U) & \longrightarrow & H^1_f(G_T, V) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1_f(G_p, \mathrm{Sym}^2 V_E) & \longrightarrow & H^1_f(G_p, L(z)) & \longrightarrow & H^1_f(G_p, V) & \longrightarrow & 0 \end{array}$$

where L is the Lie algebra of U. (technically it appears we are assuming that $H^1_f(G_T, V)$ is the closure of $\mathrm{Jac}(X)(\mathbb{Q})$ in $H^1(G_T, V)$, but this is just notational convenience, as out actual interest is in the variety $H^1_{f,\mathcal{L}}(G_T, U)$, which we have *defined* to consist of elements in whose image in $H^1_f(G_T, V)$ comes from the Jacobian). Hence one approach to proving the non-density stated in the theorem might be to compute the boundary map

$$\ker(H^1_f(G_T, V) \to H^1_f(G_p, V)) \to H^1_f(G_p, \mathrm{Sym}^2 V_E)$$

directly. The approach taken here is more convoluted, but has the advantage of giving explicit equations for $X(\mathbb{Q}_p) \cap H^1_{f,\mathcal{L}}(G_T, U)$, which are used in the last chapter to give computational bounds on the number of points of X as in the theorem

Let

$$f_1, f_2 : X \to E$$

be independent morphisms inducing an isogeny

$$\mathrm{Jac}(X) \to E \times E$$

and hence an isomorphism $V \simeq V_E \oplus V_E$. This induces

$$\mathrm{Mat}_2(\mathbb{Q}_p) \simeq R < \mathrm{End}_{G_T}(V)$$

If we take R to be $\mathrm{Mat}_2(\mathbb{Q}_p)$, then

$$E_R(V, \mathrm{Sym}^2 V_E) \simeq E_{\mathbb{Q}_p}(V_E, \mathrm{Sym}^2 V_E)$$

where the latter is defined to be the subspace of $E(V_E, \mathrm{Sym}^2 V_E)$ corresponding to extensions of V_E by $\mathrm{Sym}^2 V_E$ coming from the natural map

$$\tau_E : V_E \to V_E^* \otimes \mathrm{Sym}^2 V_E.$$

$$v \mapsto (w \mapsto vw).$$

Lemma 20. *The map*

$$\overline{\Psi} : H^1_f(G_T, V) \to H^1_f(G_T, V_E)^{\otimes 2}$$

is given by

$$\overline{\Psi}(c) = (f_{1*}(c + \kappa(2b - D)) \otimes (f_{2*}(c)) - (f_{2*}(c + \kappa(2b - D)) \otimes (f_{1*}(c))$$

where b is the basepoint of X, D is the hyperelliptic rational divisor defined in Lemma 4 and the maps

$$f_{i*} : H^1_f(G_T, V) \to H^1_f(G_T, V_E)$$

are induced from the maps

$$f_i : X \to E.$$

Proof. By Lemma 4, the extension class $[IA(b)]^{(c)}$ is equal to $\tau_*(c + \kappa(2b - D))$, where τ denotes the homomorphism

$$V \to V^* \otimes \mathrm{Sym}^2 V_E$$

$$v \mapsto (w \mapsto \overline{v \wedge w}).$$

Recall that $\mathrm{Sym}^2 V_E$ is identified as a direct summand of $\overline{\wedge^2 V}$ via the isomorphism

$$\wedge^2(V_E \oplus V_E) \simeq \wedge^2 V_E \oplus \wedge^2 V_E \oplus V_E \otimes V_E.$$

Via the isomorphism $V^* \otimes \mathrm{Sym}^2 V_E \simeq (V_E^* \otimes \mathrm{Sym}^2 V_E)^{\oplus 2}$, $\tau(v)$ is then identified with the $(\tau(f_{1*}(v), -f_{2*}(v))$. Hence

$$\overline{\Psi}(c) = c \otimes_R (c + \kappa(2b - D))$$

is identified with

$$(f_{1*}(c), f_{2*}(c)) \otimes_R (f_{1*}(c + \kappa(2b - D)), -f_{2*}(c + \kappa(2b - D))).$$

The result now follows from Lemma 13. □

2.4.2 Constructing other elements of $H^1_f(G_T, E(V_E, \mathrm{Sym}^2 V_E)$

Recall that when U was a $\mathbb{Q}_p(1)$ quotient, Ψ could be modified to give a map Ψ^{Sym} such that $\overline{\Psi}^{\mathrm{Sym}}$ has target $\mathrm{Sym}^2 H^1_f(G_T, V)$. In the case of X and U as above, we may define a modification of Ψ, denoted Ψ^{alt}, such that $\overline{\Psi}^{\mathrm{alt}}$ lands in $\wedge^2 H^1_f(G_T, V)$.

Definition 17. Given two representations E_1, E_2 in extensions

$$0 \to V_E \to E_i \to \mathbb{Q}_p \to 0$$

let $\overline{E_1 E_2}^{(-)}$ be the quotient of $E_1 \otimes E_2$ by $\wedge^2 V_E$. Hence $\overline{E_1 E_2}^{(-)}$ defines an element of $H^1(G_T, E(V_E, \mathrm{Sym}^2 V_E))$ and by projection an element of $H^1_f(G_T, V_E) \otimes H^1_f(G_T, V_E)$.

The reason for the minus sign is as follows:

Lemma 21. *The image of* $\overline{E_1 E_2}^{(-)}$ *in* $H^1_f(G_T, V_E) \otimes H^1_f(G_T, V_E)$ *is*

$$[E_1] \otimes [E_2] + [E_2] \otimes [E_1]$$

This motivates another definition:

Definition 18. Define $H^1_f(G_T, E(V_E, \mathrm{Sym}^2 V_E))^{\mathrm{alt}}$ to be the pull-back of $H^1_f(G_T, E(V_E, \mathrm{Sym}^2 V_E))$ by $\wedge^2 H^1_f(G_T, V_E) \to H^1(G_T, V_E)^{\otimes 2}$:

$$0 \to H^1(G_T, \mathrm{Sym}^2 V_E) \to H^1(G_T, E(V_E, \mathrm{Sym}^2 V_E))^{\mathrm{alt}} \to \wedge^2 H^1_f(G_T, V_E) \to 0$$

For a mixed extension W with image $\sum [W_i] \otimes [Z_i]$ in $H^1_f(G_T, V_E)^{\otimes 2}$, define $[W]^{\mathrm{alt}}$ in $H^1_f(G_T, E(V_E, \mathrm{Sym}^2 V_E))^{\mathrm{alt}}$ to be

$$[W] - \frac{1}{2} \sum [\overline{W_i Z_i}^{(-)}]$$

Hence we have a morphism

$$\Psi^{\mathrm{alt}} : H^1_f(G_T, U) \to H^1_f(G_T, E(V_E, \mathrm{Sym}^2 V_E))^{\mathrm{alt}}$$

$$P \mapsto [A(b)^{(P)}]^{\mathrm{alt}} = [A(b)^{(P)}] - \frac{1}{2}\overline{(f_{1*} \circ \kappa)(2b - D) f_{2*}(c)}^{(-)} + \frac{1}{2}\overline{(f_{2*} \circ \kappa)(2b - D) f_{1*}(c)}^{(-)}$$

whose image in $\wedge^2 H^1_f(G_T, V_E)$ is given by

$$f_{1*}(P) \wedge f_{2*}(P) + \frac{1}{2}(f_{1*} \circ \kappa)(2b - D) \wedge f_{2*})(P) - \frac{1}{2}(f_{2*} \circ \kappa)(2b - D) \wedge f_{1*}(P) \quad (2.17)$$

For the map Θ defined in the next section, we compare Ψ^{alt} with its local analogue:

Definition 19. As with Ψ, we have a local version of Ψ^{alt}, which will be denoted Ψ_p^{alt}. The construction is exactly the same, only with $H_f^1(G_T, .)$ replaced everywhere with $H_f^1(G_p, .)$. Note that since $H_f^1(G_p, \wedge^2 V_E)$ is one-dimensional, $\wedge^2 H_f^1(G_p, V_E) = 0$, and hence Ψ_p^{alt} is a map

$$H_f^1(G_p, U) \to H_f^1(G_p, \operatorname{Sym}^2 V_E)$$

2.4.3 Definition of Θ

To construct the morphism Θ, we first have to choose a splitting s of

$$H_f^1(G_T, E(V_E, \operatorname{Sym}^2 V_E))^{\text{alt}} \to \wedge^2 H_f^1(G_T, V_E) \tag{2.18}$$

Note that since $\wedge^2 H_f^1(G_T, V_E)$ is one dimensional, such a spliting can be achieved by finding a rational point $z \in X(\mathbb{Q})$ such that

$$f_{1*}(j_1(z)) \wedge f_{2*}(j_1(z)) + \frac{1}{2}(f_{1*} \circ \kappa)(2b - D) \wedge f_{2*})(j_1(z)) - \frac{1}{2}(f_{2*} \circ \kappa)(2b - D) \wedge f_{1*}(j_1(z)) \neq 0 \tag{2.19}$$

Definition 20. Define

$$\Gamma : H_f^1(G_T, U) \to \wedge^2 H^1(G_T, V_E) \tag{2.20}$$

$$P \mapsto f_{1*}(P) \wedge f_{2*}(P) + \frac{1}{2}(f_{1*} \circ \kappa)(2b - D) \wedge f_{2*}(j_1(z)) - \frac{1}{2}(f_{2*} \circ \kappa)(2b - D) \wedge f_{1*}(j_1(z))$$

and define

$$\Theta : H_f^1(G_T, p) \times \wedge^2 H_f^1(G_T, V_E) \to H_f^1(G_p, \operatorname{Sym}^2 V_E)$$
$$(P, c) \mapsto \Psi_p^{\text{alt}}(P) - \operatorname{loc} \circ s(c)$$

Lemma 22. *Θ is surjective.*

Proof. $H_f^1(G_p, U)$ admits an action of $H_f^1(G_p, \operatorname{Sym}^2 V_E)$, and Θ is equivariant with respect to this action. □

Theorem 9. *The codimension of the image of*

$$\operatorname{loc} \times \Gamma : H_f^1(G_T, U) \to H_f^1(G_p, U) \times \wedge^2 H_f^1(G_T, V)$$

is at least two. In particular, $\operatorname{loc}(H_f^1(G_T, U))$ *is not Zariski dense in* $H_f^1(G_p, U)$.

Proof. By construction,

$$\Theta \circ (\mathrm{loc} \times \Gamma) \in \mathrm{loc}_p(H^1_f(G_T, \mathrm{Sym}^2 V_E))$$

which is zero by Flach's theorem. Hence by the previous Lemma (and noting that $H^1_f(G_p, \mathrm{Sym}^2 V) \simeq D_{dR}(\mathrm{Sym}^2 V)/F^0$ is two dimensional) the codimension is at least two. □

2.4.4 2nd example

Suppose X is a hyperelliptic curve with Jacobian isogenous to A_1^{n+1}, with A_1 a polarised abelian variety of dimension d. Then, as in section , the depth 2 fundamental group of X contains a $\mathbb{Q}_p(1)^{n(n+3)/2}$. Hence in order to apply the dimension estimate to prove finiteness of $X(\mathbb{Q}_p)_2$ one needs that the Mordell-Weil rank is (roughly) smaller than $n/2+d$. In this section we show that the maps Ψ^{Sym} (applied to various $\mathbb{Q}_p(1)$-quotients of the fundamental group) give a refinement of this.

Theorem 10. *Suppose X is a hyperelliptic curve with Jacobian isogenous to $A_1^{n+1} \times A_2$, with A_1 a polarised abelian variety of Mordell-Weil rank n. Then*

$$\mathrm{loc} : H^1_f(G_T, U) \to H^1_f(G_p, U)$$

is non-dense.

Note that the hypotheses mean we can apply the Manin-Demyanenko theorem to find $X(\mathbb{Q})$ [58]. The goal of this section is to suggest that curves satisfying the Manin-Demyanenko hypotheses may have enough structure in their Selmer varieties to enable one to prove non-density of the localisation map even when the dimension of the global Selmer variety is large. The main reason for restricting to hyperelliptic curves is to allow us to ignore the abelian variety A_2. One obvious limitation of this result is that curves with lots of independent maps to simple abelian varieties are rather rare, and when they do arise in nature (e.g. the towers of modular curves $X_0(p^r)$) there is no reason to expect them to be hyperelliptic. Hence it is natural to wonder whether it is possible to modify these methods so they also apply in this context.

2.4.4.1 A modification of j

Before proving the theorem, it will be convenient to introduce a small modification of the function j for U a $\mathbb{Q}_p(1)$-quotient of U_2. Recall that, by the weight monodromy conjecture for curves, for all v not equal to p

$$H^1(G_v, V) = H^0(G_v, V) = 0$$

Hence the map

$$H^1(G_v, [U,U]) \to H^1(G_v, U)$$

is an isomorphism, so $\prod_{v \in T_0} j_v$ may canonically be viewed as a function with target $\prod_{v \in T_0} H^1(G_v, \mathbb{Q}_v(1))$. For any (c_v) in $\prod_{v \in T_0} H^1(G_v, \mathbb{Q}_v(1))$, there is a unique lift to c in $H^1(G_T, \mathbb{Q}_v(1))$ which is crystalline at v. We use this lift to define a modified version of j which lands in $H^1_f(G_T, U_2)$, rather than merely $H^1_{f,\mathcal{L}}(G_T, U_2)$.

Definition 21. Define

$$j_2^o : X(\mathbb{Q}) \to H^1_f(G_T, U_2)$$

to be the function sending $x \in X(\mathbb{Q})$ to $j_2(x) - c$, where $(j_{2,v}(x))_{v \in T_0} = (c_v)$ above.

2.4.4.2 Proof of Theorem 10

Let $f_i : X \to A_1$ $(i = 0, \ldots, n)$ be n independent morphisms inducing the isogeny

$$\mathrm{Jac}(X) \to A_1^n \times A_2$$

For $0 \leq i \leq n$, let

$$f_{i*} : H^1_f(G_T, V) \to H^1_f(G_T, V_1) \tag{2.21}$$

be the induced pushforward morphism ($V_1 = T_p A_1 \otimes \mathbb{Q}_p$). We also use f_{i*} to denote the pushforward

$$H^1_f(G_T, U) \to H^1_f(G_T, V_1)$$

Since A_1 has rank n, for any z there will be a linear relation between the $(f_{i*} \circ j_1)(z)$ (for $0 \leq i \leq n$). The morphism

$$H^1_f(G_T, U) \to S$$

is supposed to remember the linear relation.

Definition 22. Define $S := (\wedge^n H^1_f(G_T, V_1))^{\oplus(n+1)}$ and

$$G = (G_0, \ldots, G_n) : H^1_f(G_T, V) \to S$$

by

$$G_i(c) = (-1)^i f_{0*}(c) \wedge \ldots \wedge \widehat{f_{i*}(c)} \wedge \ldots \wedge f_{n*}(c)$$

By elementary linear algebra, this satisfies

Lemma 23. *For any c in $H^1_f(G_T, V)$,*

$$\sum_i G_i(c) \otimes f_{i*}(c) = 0$$

in $(\wedge^n H^1_f(G_T, V_1)) \otimes H^1_f(G_T, V_1)$.

We now need to keep track of all the mixed representations with graded pieces $\mathbb{Q}_p, V^{\oplus n}$ and $\mathbb{Q}_p(1)$ we can build out of $A(b)^{(P)}$, for P a U-torsor. Write V as $\oplus_{i=0}^n f_i^* V_1$. Let

$$p : \wedge^2 V_1 \to \mathbb{Q}_p(1)$$

be the surjection induced from the polarisation on A_1. Then the product homomorphism

$$V \otimes V \to \mathbb{Q}_p(1)^{n(n+3)/2}$$

is given by

$$(v_0, \ldots, v_n) \otimes (w_0, \ldots, w_n) \mapsto ((p(v_i \wedge w_i) - p(v_0 \wedge w_0))_{1 \leq i \leq n}, (p(v_i \wedge w_j - w_i \wedge v_j))_{0 \leq i < j \leq n})$$

Note that our computation of the extension $IA(b)$ means that we can henceforth assume A_2 is trivial, as if we take the quotient U as above, then $V_2 = T_p(A_2) \otimes \mathbb{Q}_p$ is a Galois stable central subgroup of U.

Definition 23. For $i < j$ let $U^{(i,j)}$ be the quotient of U with product $V \otimes V \to \mathbb{Q}_p(1)$ given by $p \circ (f_{i*} \otimes f_{j*} - f_{i*} \otimes f_{j*})$ and for $1 \leq i \leq n$ let $U^{(i,i)}$ be the quotient corresponding to $p \circ (f_{i*} \otimes f_{i*} - f_{0*} \otimes f_{0*})$. Let $A^{(i,j)}(b)$ denote the corresponding mixed extension. Define

$$\Psi^{(i,j)} : H^1_f(G_T, U) \to H^1_f(G_T, E(V, \mathbb{Q}_p(1)))$$

$$P \mapsto [A^{(i,j)}(b)^{(P)}]$$

Note that we are imposing the local conditions that P is trivial away from p, so $\Psi^{(i,j)}$ gives a function on rational points by composition with j^o, not j.

Lemma 24. *For $i \neq j$,*

$$\overline{\Psi}^{(i,j)}(P) = (f_{i*}(P)+(f_{i*}\circ\kappa)(2b-D))\otimes f_{j*}(P)+(f_{j*}(P)+(f_{j*}\circ\kappa)(2b-D))\otimes f_{i*}(P)$$

For $1 \leq n$,

$$\overline{\Psi}^{(i,i)}(P) = (f_{i*}(P)+(f_{i*}\circ\kappa)(2b-D))\otimes f_{i*}(P)-(f_{i*}(P)+(f_{0*}\circ\kappa)(2b-D))\otimes f_{0*}(P)$$

Proof. This follows from the fact that the endomorphism

$$\tau^{(i,j)} : V \to V$$

describing the commutator on $U^{(i,j)}$ is given by $f_i^* f_{j*} + f_j^* f_{i*}$ when $i \neq j$ and $f_i^* f_{i*} - f_0^* f_{0*}$ when $i = j$ (via the isomorphism $V^*(1) \simeq V$ induced by p). □

We also define

$$\Psi^{(i,j),\mathrm{Sym}} : H^1_f(G_T, U) \to H^1_f(G_T, E(V, \mathbb{Q}_p(1)))^{\mathrm{Sym}}$$
$$P \mapsto [A^{(i,j)}(b)^{(P)}]^{\mathrm{Sym}}$$

and

$$\overline{\Psi}^{(i,j),\mathrm{Sym}} : H^1_f(G_T, U) \to \mathrm{Sym}^2 H^1_f(G_T, V_1)$$

Hence, rearranging Lemma 24

Lemma 25. *For $i \neq j$,*

$$\begin{aligned}\overline{\Psi}^{(i,j),\mathrm{Sym}}(P) &= 2f_{i*}(P)f_{j*}(P) + (f_{i*}\circ\kappa)(2b-D)f_{j*}(P) + (f_{j*}\circ\kappa)(2b-D)f_{i*}(P) \\ &= 2(f_{i*}(P) + \frac{1}{2}(f_{i*}\circ\kappa)(2b-D))(f_{j*}(P) + \frac{1}{2}(f_{j*}\circ\kappa)(2b-D)) \\ &- \frac{1}{2}(f_{i*}\circ\kappa)(2b-D)(f_{j*}\circ\kappa)(2b-D) + \frac{1}{4}(f_{0*}\circ\kappa)(2b-D)^2\end{aligned}$$

For $1 \leq i \leq n$,

$$\begin{aligned}\overline{\Psi}^{(i,i),\mathrm{Sym}}(P) &= (f_{i*}(P) + (f_{i*}\circ\kappa)(2b-D))f_{i*}(P) - (f_{0*}(P) + (f_{0*}\circ\kappa)(2b-D))f_{0*}(P) \\ &= (f_{i*}(P) + \frac{1}{2}(f_{i*}\circ\kappa)(2b-D))^2 - (f_{0*}(P) + \frac{1}{2}(f_{0*}\circ\kappa)(2b-D))^2 \\ &- \frac{1}{4}(f_{i*}\circ\kappa)(2b-D)^2 + \frac{1}{4}(f_{0*}\circ\kappa)(2b-D)^2\end{aligned} \tag{2.22}$$

Define

$$\Gamma : H^1_f(G,U) \to S$$
$$P \mapsto G(\pi_*(P) + \kappa(b - \frac{D}{2}))$$

Definition 24. Define

$$\Theta_0 : H^1_f(G_p,U) \times S \to \wedge^n H^1_f(G_T,V_1) \otimes H^1_f(G_p,V_1)$$

by

$$\Theta_0(P,(\lambda_i)) = \sum_{i=0}^{n} \lambda_i \otimes (f_{i*}(\pi_*(P) + \kappa(b - \frac{D}{2})))$$

Note that by Lemma 23,

$$\Theta_0 \circ (\mathrm{loc} \times \Gamma) = 0 \tag{2.23}$$

so in particular the localisation map factors through $\ker(\Theta_0)$

$$H^1_f(G_T,U) \to \ker(\Theta_0) \to H^1_f(G_p,U)$$

Hence we want to show that the codimension of $H^1_f(G_T,U)$ in $\ker(\Theta)_0$ is bigger than $n-g$. As before, let s be a splitting of

$$H^1_f(G_T,E(V_1,\mathbb{Q}_p(1)))^{\mathrm{Sym}} \to \mathrm{Sym}^2 H^1_f(G_T,V_1)$$

and let

$$\Psi_p^{(i,j),\mathrm{Sym}} : H^1_f(G_p,U) \to H^1_f(G_p,E_p(V_1,\mathbb{Q}_p(1)))^{\mathrm{Sym}}$$

be the local analogue of $\Psi^{(i,j),\mathrm{Sym}}$.

Theorem 11. *For $1 \leq i \leq n$, the map*

$$\Theta_i : H^1_f(G_p,U) \times S \to \wedge^n H^1_f(G_T,V_1)^{\otimes 2} \otimes H^1_f(G_p,E(V,\mathbb{Q}_p(1)))^{\mathrm{Sym}}$$

sending $(P,(\lambda_0,\ldots,\lambda_n))$ to

$$\lambda_i \otimes \lambda_0 \otimes \Psi^{(i,i)}(P) + \sum_{j\neq i} \lambda_j \otimes \lambda_0 \otimes \Psi^{(i,j)}(P) - \sum_{j\neq 0} \lambda_j \otimes \lambda_0 \otimes \Psi^{(0,j)}(P)$$
$$+\frac{1}{4}\sum_{j=0}^{n} \lambda_j \otimes (\lambda_i \otimes s(f_{j*} \circ \kappa(b - \frac{D}{2})) - \lambda_0 \otimes s(f_{0*} \circ \kappa(b - \frac{D}{2}))$$

sends $\ker(\Theta_0)$ to $H^1_f(G_p,\mathbb{Q}_p(1))$, and sends $(\mathrm{loc} \times \Gamma)(H^1_f(G_T,U))$ to zero.

Proof. Recall that by definition of the λ_i,

$$\sum \lambda_i \otimes (f_{i*}(\pi_*(P) + \kappa(b - \frac{D}{2}))) = 0$$

Hence

$$\begin{aligned} &\lambda_i \otimes \lambda_0 \otimes (f_{i*}(\pi_*(P) + \kappa(b - \frac{D}{2})))(f_{i*}(\pi_*(P) + \kappa(b - \frac{D}{2}))) \\ &- \lambda_i \otimes \lambda_0 \otimes (f_{0*}(\pi_*(P) + \kappa(b - \frac{D}{2})))(f_{0*}(\pi_*(P) + \kappa(b - \frac{D}{2}))) \\ &+ \sum_{j \neq i} \lambda_j \otimes \lambda_0 \otimes (f_{j*}(\pi_*(P) + \kappa(b - \frac{D}{2})))(f_{i*}(\pi_*(P) + \kappa(b - \frac{D}{2}))) \\ &- \sum_{j \neq 0} \lambda_i \otimes \lambda_j \otimes (f_{j*}(\pi_*(P) + \kappa(b - \frac{D}{2})))(f_{0*}(\pi_*(P) + \kappa(b - \frac{D}{2}))) \\ &= 0 \end{aligned} \tag{2.24}$$

Finally note that by Lemma 25, this means that the image of Θ_i in $\wedge^n H^1_f(G_T, V)^{\otimes n} \otimes \operatorname{Sym}^2 H^1_f(G_p, V_1)$ is zero. The same computation guarantees that if $(P, (\lambda_i))$ lies in $(\operatorname{loc} \times \Gamma)(H^1_f(G_T, U))$, then $\Theta_i(P, (\lambda_i))$ defines an element of $H^1_f(G_T, \mathbb{Q}_p(1)) = 0$. ☐

Define

$$\Theta = (\Theta_1, \ldots, \Theta_n) : \ker(\Theta_0) \to \wedge^n H^1_f(G_T, V_1)^{\otimes 2} \otimes H^1_f(G_p, \mathbb{Q}_p(1)) \tag{2.25}$$

Theorem 12. *Θ is surjective, and*

$$\Theta \circ (\operatorname{loc} \times \Gamma) : H^1_f(G_T, U) \to \wedge^n H^1_f(G_T, V_1)^{\otimes 2} \otimes H^1_f(G_p, \mathbb{Q}_p(1))$$

is zero.

Proof. For surjectivity, it again suffices to note that $H^1_f(G_p, [L, L])$ acts on $\ker(\Theta_0)$ and $\wedge^n H^1_f(G_T, V_1)^{\otimes 2} \otimes H^1_f(G_p, \mathbb{Q}_p(1))$ in a natural way. For triviality of the global map, note that by the lemma above, for P in $H^1_f(G_T, U)$

$$\lambda_i \otimes \lambda_0 \otimes \Psi^{(i,i),\mathrm{Sym}}(P) + \sum_{j\neq i} \lambda_j \otimes \lambda_0 \otimes \Psi^{(i,j)}(P)$$
$$- \sum_{j\neq 0} \lambda_j \otimes \lambda_0 \otimes \Psi^{(0,j)}(P)$$
$$+ \frac{1}{4}\sum_{j=0}^{n} \lambda_j \otimes (\lambda_i \otimes s(f_{j*} \circ \kappa(b - \frac{D}{2})) - \lambda_0 \otimes s(f_{0*} \circ \kappa(b - \frac{D}{2}))$$

is zero in $\wedge^n H^1_f(G_T, V_1)^{\otimes 2} \otimes H^1_f(G_T, V_1)$. This implies $\Theta(\mathrm{loc}(P), \Gamma(P))$ is the localisation of a global $\mathbb{Q}_p(1)^{\oplus n}$ class, and is hence zero. □

2.5 $\mathbb{Q}_p(1)$-quotients and p-adic heights

This section is concerned with giving an explicit description of the mixed extensions arising from $\mathbb{Q}_p(1)$-quotients, and their relation to the mixed extensions arising from the theory of motivic height pairings as developed by Nekovar and Scholl [56],[50]. Such relations have been established in the case of fundamental groups of affine elliptic curves in work of Balakrishnan and Besser [6] and Balakrishnan, Dan-Cohen, Kim and Wewers [4] and in the case of affine hyperelliptic curves in work of Balakrishnan, Besser and Muller [5].

2.5.1 Mixed motives related to the height pairing on X

In this subsection we review the motivic construction of mixed extensions associated to height pairings as developed by Nekovar and Scholl, and in the next we prove the relation with fundamental groups. .

Let W_1 and W_2 be elements of $\mathrm{Div}^0(\overline{X})$ with disjoint support. We have an exact sequence

$$0 \to H^0(\overline{X}) \to H^0(|W_2|) \to H^1(\overline{X}; |W_2|) \to H^1(\overline{X}) \to 0$$

and via the isomorphisms

$$H^2_{|W_1|}(\overline{X}; |W_2|) \simeq H^2_{|W_1|}(\overline{X})$$

$$H^2(\overline{X}; W_2) \simeq H^2(\overline{X})$$

we have an exact sequence

$$0 \to H^1(\overline{X}; |W_2|) \to H^1(\overline{X} - |W_1|; |W_2|) \to H^2_{|W_1|}(\overline{X}) \to H^2(\overline{X}) \to 0$$

The 0-divisors W_1 and W_2 defines maps

$$\pi_2 : \text{coker}\left(H^0(\overline{X}) \to H^0(|W_2|)\right) \to \mathbb{Q}_l$$

and

$$\iota_1 : \mathbb{Q}_l(-1) \to \ker\left(H^2_{|W_1|}(\overline{X}) \to H^2(\overline{X})\right)$$

Definition 25. For null homologous cycles W_1 and W_2 on $\overline{X}$ (i.e. zero divisors) we define $H(W_1, W_2) = H(X)(W_1, W_2)$ to be the subquotient of

$$H^1(\overline{X} - |W_1|; |W_2|)$$

obtained by first pulling back by ι_1 to get a new representation H_1

$$\begin{array}{ccc} H_1 & \longrightarrow & \mathbb{Q}_l(-1) \\ \downarrow & & \downarrow \\ H^1(\overline{X} - |W_1|; |W_2|) & \longrightarrow & H_1 \end{array}$$

and then pushing out H_1 by π_2:

$$\begin{array}{ccc} H^0(|W_2|) & \longrightarrow & E_1 \\ \downarrow & & \downarrow \\ \mathbb{Q}_l & \longrightarrow & E_{1,2} \end{array}$$

Note that $[H(W_1, W_2)]$ defines an element of $H^1(G_T, E(V, \mathbb{Q}_p(1))$. Recall

$$[H(W_1, W_2 + W_3)] = [H(W_1, W_2)] + [H(W_1, W_3)] \tag{2.26}$$

and for $f : X' \to X$ a morphism of curves, and divisors D on X and D' on X',

$$[H(X')(D', f^*D)] = [H(X)(f_*D', D)] \tag{2.27}$$

2.5.1.1 Nekovar's height functions and relation to other theories of p-adic heights

Nekovar constructs local heights from mixed extensions as follows: Fix a splitting

$$s : H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})/F^1 H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p}) \to H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})$$

of the Hodge filtration isotropic with respect to Poincaré duality (i.e. for all v, w in $H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})/F^1$, $s(v) \cup s(w) = 0$). Let M be a G_T-representation with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ which is de Rham at p. At $v \neq p$, by the weight monodromy conjecture for curves

$$H^1(G_v, V) = H^0(G_v, V) = 0,$$

hence

$$H^1(G_v, M_1) \simeq H^1(G_v, \mathbb{Q}_p(1))$$

At the prime p, Nekovar defines a function

$$H^1_g()$$

using p-adic Hodge theory and the splitting s. The p-adic logarithm map defines a function

$$H^1(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_v^\times \otimes \mathbb{Q}_p \to \mathbb{Q}_p$$

given by

$$x \mapsto \log_p(v).v(x)$$

at $v \neq p$ and

$$x \mapsto \log_p(x)$$

at $v = p$. Hence, at each prime v we obtain a function λ_v defined on pairs of elements of $\mathrm{Div}^0(X)$ with disjoint support.

Nekovar proves that, for $\mu_i \in \mathbb{Q}_p$, E_i and D_i in $\mathrm{Div}^0(X)$, if $\sum \mu_i(D_i, E_i)$ satisfy

$$\sum \mu_i \kappa(D_i)\kappa(E_i) = 0$$

in $\mathrm{Sym}^2 H^1_f(G_T, V)$, then

$$\sum_{v,i} \mu_i \lambda_v(D_i, E_i) = 0$$

hence $\sum_v \lambda_v$ factors through the map to $\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X)$.

There is an alternative definition of a p-adic height pairing on curves given by Coleman and Gross in [23]. See [14] for the relation between Nekovar's height and the Coleman-Gross p-adic height, [51] Proposition 2.16 or [56] section 4 for the relation between these extensions and local heights at primes away from p, and [6] for the relation to p-adic sigma functions in the case of an elliptic curve In the case of an elliptic curve $E = (E, O)$ the relation with more classical local heights allows us to canonically extend the λ_v to divisors with non-disjoint support, and in this case we define

$$\lambda_v(P) := \lambda_v(P - O, P - O).$$

2.5.2 Height pairings and $\mathbb{Q}_p(1)$-quotients of the fundamental group

We now explain how to relate this to fundamental groups. Via Beilinson's cohomological characterisation of the path-space $A_2(b, z)$, this is reduced to relating subquotients of $H^1(\overline{X} - |Z_1|; |Z_2|)$ to subquotients of $H^2(\overline{X} \times \overline{X}; |Z|)$, where the divisors Z arise from Beilinson's theorem.

Let b and z be distinct. Define $X_1 := \{b\} \times \overline{X}$ and $X_2 := \overline{X} \times \{z\}$ and inclusions

$$i_1 : X_1 \hookrightarrow X \times X$$

$$i_2 : X_2 \hookrightarrow X \times X$$

$$i_3 : \Delta \hookrightarrow X \times X$$

Let

$$\pi_1, \pi_2 : X \times X \to X$$

denote the projection maps. The particular cohomology group we are interested in is $H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta)$, which is a mixed representation with graded pieces $\mathbb{Q}_p$, $H^1(\overline{X})$ and

$$\ker(H^1(\overline{X})^{\otimes 2} \xrightarrow{\cup} H^2(\overline{X}))$$

(dual to $A_2(b, z)$). For any element ξ of $\mathrm{Hom}(\mathbb{Q}_p(-1), H)$ we get, by pulling back, an extension

$$0 \to H^1(\overline{X}; \{z_1\} \cup \{z_2\}) \to E_\xi \to \mathbb{Q}_p(-1) \to 0$$

We can characterise this construction cohomologically.

Let Z_0 be a divisor of $\overline{X} \times \overline{X}$ intersecting X_1, X_2 and Δ properly. Let

$$\mathrm{cl}_{Z_0} : \mathbb{Q}_p(-1) \to H^2_{\acute{e}t}(\overline{X} \times \overline{X})$$

denote the cycle class of Z_0, and let

$$\xi : \mathbb{Q}_p(-1) \to H^2_{\acute{e}t}(\overline{X} \times \overline{X})$$

denote the composite

$$\mathbb{Q}_p(-1) \xrightarrow{\mathrm{cl}_{Z_0}} H^2_{\acute{e}t}(\overline{X} \times \overline{X}) \to H^1_{\acute{e}t}(\overline{X})^{\otimes 2} \xrightarrow{\simeq} H^2(\overline{X} \times \overline{X}; X_1 \cup X_2)$$

where the last map is the isomorphism induced by

$$H^2(\overline{X} \times \overline{X}; X_1 \cup X_2) \to H^2(\overline{X} \times \overline{X})$$

Suppose that ξ lands in the kernel of the cup product. Note that this condition is equivalent to requiring that Z_0 ha trace zero as an endomorphism of H^1.

Theorem 13. *The extension*

$$H^1(X; b \cup z) \to E_{Z_0} \to \mathbb{Q}_p(-1) \to 0$$

obtained from pulling back $A_2(b, z)$ *by* ξ *is isomorphic to* $H_X(z-b, i_3^*Z_0 - i_1^*Z_0 - i_2^*Z_0)$

Proof. For any cycle Z we have a commutative diagram with exact columns and rows

$$\begin{array}{ccccc}
H^1_{i_3^*|Z|}(X; \{b\} \cup \{z\}) & \longrightarrow & H^2_{|Z|}(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2_{|Z|}(\overline{X} \times \overline{X}; X_1 \cup X_2) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(\overline{X}; \{b\} \cup \{z\}) & \longrightarrow & H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2(\overline{X} \times \overline{X}; X_1 \cup X_2) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(\overline{X} - i_3^*|Z|; \{b\} \cup \{z\}) & \longrightarrow & H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2)
\end{array}$$

Let $\pi_2^* i_1^* Z_0$ denote the divisor obtained by fibering the divisor $i_1^* Z_0$ of X with X (so that if $i_1^* Z_0 = \sum n_i x_i$, then $\pi_2^* i_1^* Z_0 = \sum n_i x_i \times \overline{X}$. Similarly define $\pi_1^* i_2^* Z_0$. Define

$$Z := Z_0 - i_1^* Z - i_2^* Z$$

Corresponding to Z we have a homomorphism

$$\widetilde{\mathrm{cl}} : \mathbb{Q}_p(-1) \to H^2_{|Z_0|}(\overline{X} \times \overline{X})$$

intermediate between the homomorphism to $H^2_{|Z|}$ and the cycle class to H^2. By construction the pullback of $\widetilde{\mathrm{cl}}$ to $H^2(X_1 \times X_2)$ is zero, hence $\widetilde{\mathrm{cl}}(\mathbb{Q}_p(1))$ lies in the image of

$$H^2_{|Z_0|}(\overline{X} \times \overline{X}; X_1 \cup X_2) \hookrightarrow H^2_{|Z_0|}(\overline{X} \times \overline{X})$$

so we henceforth think of $\widetilde{\mathrm{cl}}$ as a homomorphism to $H^2_{|Z_0|}(\overline{X} \times \overline{X}; X_1 \cup X_2)$. Note that the image of $\widetilde{\mathrm{cl}}$ in $H^2(\overline{X} \times \overline{X}; X_1 \cup X_2)$ equals ξ, and so in particular the image of ξ in $H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2)$ is zero.

The map

$$H^1(\overline{X}, \mathbb{Q}_p; \{b\} \cup \{z\}) \hookrightarrow H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta)$$

is injective, hence it will be enough to show that the image of the class of Z_0 in $H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2 \cup \Delta)/H^1(\overline{X}; \{b\} \cup \{z\})$ equals that of the class of $i_3^* Z_0 - i_1^* Z_0 - i_2^* Z_0$.

Hence the result follows from general diagram chasing:

Let

$$W := \mathrm{Ker}(H^2(\overline{X} \times \overline{X}; X_1 \cup X_2) \to H^2(\overline{X}; b \cup z))$$

Let

$$\delta : \mathrm{Ker}(\gamma) \to \mathrm{Coker}(\alpha)$$

denote the connecting homomorphism of the six-term exact sequence associated to

$$\begin{array}{ccccccc}
 & H^1(\overline{X}; b \cup z) & \longrightarrow & H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) & \longrightarrow & W & \longrightarrow 0 \\
 & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & \\
0 \to & H^1(\overline{X} - i_3^*|Z|; b \cup z) & \longrightarrow & H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2(\overline{X} \times \overline{X} - |Z|; X_1 \cup X_2) &
\end{array}$$

Let $W' := \mathrm{Ker}(H^2_{|Z|}(\overline{X} \times \overline{X}; X_1 \cup X_2) \to H^2(\overline{X}; b \cup z))$ Then the map

$$W' \xrightarrow{i_3^*} H^2_{i_3^*|Z|}(X; b \cup z)$$

factors as

$$W' \to \mathrm{Ker}(\gamma) \xrightarrow{\delta} \mathrm{Coker}(\alpha) \to H^2_{i_3^*|Z|}(X; b \cup z)$$

This identification completes the proof of the theorem. □

We note a similar affine version of this result. Let $Y = X - x$. Then $A_2(Y)(b, z)$ has graded pieces $\mathbb{Q}_p, V$ and $V^{\otimes 2}$. Hence for *any* correspondence $Z \subset X \times X$ not cohomologous to zero, intersecting $X_1, X_2, \Delta, x \times X, X \times x$ and (b, b) and (z, z) properly, we get a mixed extension E_Z with graded pieces $\mathbb{Q}_p(-1)$, V and $\mathbb{Q}_p$. (from the pulling back $A_2(Y)(b, z)^*$ by Z. In a similar manner to the theorem above, we obtain the following characterisation of E_Z.

Theorem 14. *The mixed extension E_Z is isomorphic to $H_X(z - b, i_3^* Z - i_1^* Z - i_2^* Z + mx)$, where m is the intersection number of Z with $X_1 + X_2 - \Delta$.*

Proof. The argument is as before, with the six term exact sequence used in the previous proof replaced by

$$\begin{array}{ccccccc}
 & H^1(\overline{Y}; b \cup z) & \longrightarrow & H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2(\overline{Y} \times \overline{X} - x; X_1 \cup X_2) & \longrightarrow 0 \\
 & \downarrow \alpha' & & \downarrow \beta' & & \downarrow \gamma' & \\
0 \longrightarrow & H^1(\overline{Y} - i_3^*|Z|; b \cup z) & \longrightarrow & H^2(\overline{Y} \times \overline{Y} - |Z|; X_1 \cup X_2 \cup \Delta) & \longrightarrow & H^2(\overline{Y} \times \overline{Y} - |Z|; X_1 \cup X_2) &
\end{array}$$

and the identification of i_3^* with the connecting morphism replaced by the identification of the connecting morphism of the new six term exact sequence with

$$H^2_{|Z|}(\overline{X} - x \times \overline{X} - x; X_1 \cup X_2) \to H^2_{i_3^*|Z|}(\overline{X} - x - i_3^*|Z|; b \cup z)$$

. □

Note that in the case $Z.(X_1 + X_2 - \Delta) = 0$, we recover the formula for pulling back A_2 of X by a trace zero correspondence. Note also that we recover the formula for the extension class $[IA(b, z)]$ given in [25], where $A(b, z) = E_Z^*$ is the quotient of $A_2(b, z)$ dual to E_Z.

2.5.3 Some examples in genus 1 and 2

This subsection contains two examples that will be used in the last chapter. For x a point on an elliptic or hyperelliptic curve, we denote by x^- its image under the hyperelliptic involution.

Example 1. Let E be an elliptic curve. Let x be a point of E. Let b and z be points not in $E[2]$ or equal to x. Let Z be the cycle $\Delta^- = \{(x, x^-)\}$. Then $i_1^* Z = b^-$, $i_2^* Z = z^-$ and $i_3^* Z = E[2]$. Hence

$$[A(E - O)(b, z)] = H(z - b, E[2] - b^- - z^- - 2x) \tag{2.28}$$

Example 2. Let X be a genus 2 curve of the form

$$y^2 = x^6 + ax^4 + bx^2 + 1$$

Define

$$E_1 : y^2 = x^3 + ax^2 + b + 1$$

$$E_2 : y^2 = x^3 + bx^2 + ax + 1$$

and

$$f_1 : X \to E_1$$

$$(x, y) \mapsto (x^2, y)$$

$$(x, y) \mapsto (x^{-2}, yx^{-3})$$

Define $Z_1 \subset X \times X$ to be the graph of the automorphism

$$g_1 : (x, y) \mapsto (-x, y)$$

and Z_2 to be the graph of

$$g_2 : (x, y) \mapsto (-x, -y)$$

Then $Z_1 - Z_2$ satifies the hypotheses of Theorem 13 , hence we get a $\mathbb{Q}_p(1)$ quotient U of the fundamental group, and corresponding mixed extension $A(b, z)$. Let V_1 and V_2 denote the $\mathbb{Q}_p$-Tate modules of E_1 and E_2, so that

$$V \simeq V_1 \oplus V_2$$

For any point b_1 and z_1 on E_1 $[A(E_1 - O)(b_1, z_1)]$ naturally defines an element of $H^1(G_T, E(V, \mathbb{Q}_p(1)))$, and similarly for E_2. In the case where b is an integral tangential basepoint, it is shown in [4] that these extensions are closely related to local heights. In this section we show that these mixed extensions are also related to mixed extensions on X: for $i = 1, 2$ we denote by κ_i the Kummer map for the elliptic curve E_i.

Proposition 4. Let t_1 and t_2 be integral tangent vectors at the origins of E_1 and E_2 respectively.

$$\begin{aligned}[A(b,z)] = [A(E_1 - O)(t, f_1(z))] &- \frac{1}{2}[A(E_2 - O)(t, f_2(z) + (0,1))] \\ &- \frac{1}{2}[A(E_2 - O)(t, f_2(z) - (0,1))] + \frac{1}{2}[A(E_2 - O)(t, f_2(b) + (0,1))] \\ &+ \frac{1}{2}[A(E_2 - O)(t, f_2(b) - (0,1))] + \overline{\kappa_2(f_2(z))\kappa_2(f_2(b))}\end{aligned}$$

When b is the point ∞^+,

$$\begin{aligned}[A(\infty^+, z)] = [A(E_1 - O)(t, f_1(z))] &- \frac{1}{2}[A(E_2 - O)(t_2, f_2(z) + (0,1))] \\ &- \frac{1}{2}[A(E_2 - O)(t_2, f_2(z) - (0,1))] + \frac{1}{2}[A(E_2 - O)(t, 2(0,1))] \\ &+ \overline{\kappa_2((0,1))\kappa_2(f_2(z))}.\end{aligned}$$

Proof. Let ∞^+ and ∞^- denote the two points of X at infinity. Theorem 13 gives the identity

$$A(b,z) \simeq H(z - b, g_1(z) - g_2(z) + g_1(b) - g_2(b) - (0,1) - (0,-1) + \infty^+ + \infty^-) \quad (2.29)$$

Note that

$$f_1 * (z^-) = g_2(z) + z^-$$

$$f_2 * (z^-) = g_1(z) + z^-$$

$$f_1^* E_1[2] = f_2^*(E[2] - O) = 6D$$

Hence

$[A(b,z)]$
$= [H(z-b, g_1(z) - g_2(z) + g_1(b) - g_2(b) - (0,1) - (0,-1) + \infty^+\infty^-)$
$= [H(X)(z-b, f_1^*(z^-) - f_2^*(z^-) + f_1^*(b^-) - f_2^*(b^-) + D - D - (0,1) - (0,-1) + \infty^+\infty^-)$
$= [H(X)(z-b, f_2^*(f_2(z)^-) + f_2^*(f_2(b)^-) - 3D - f_2^*O + \frac{1}{2}f_2^*((0,1)) + \frac{1}{2}f_2^*((0,-1)))]$
$- [H(X)(z-b, f_1^*(f_1(z)^-) + f_1^*(f_1(b)^-) - 3D)]$
$= [A(E_1 - O)(f_1(b), f_1(z))] - \frac{1}{2}[A(E_2 - (0,1))(f_2(b), f_2(z))] - \frac{1}{2}[A(E_2 - (0,-1), f_2(b), f_2(z))$
$= [A(E_1 - O)(f_1(b), f_1(z))] - \frac{1}{2}[A(E_2 - O)(f_2(b) + (0,1), f_2(z) + (0,1))]$
$- \frac{1}{2}[A(E_2 - O)(f_2(b) - (0,1), f_2(z) - (0,1))]$

Finally, recall the composition of paths formula for Ψ (Lemma 17)

$$[A(x_1,x_3)] = [A(x_1,x_2)] + [A(x_2,x_3)] + \overline{\kappa(x_2 - x_1)\kappa(x_3 - x_1)}]$$

Applying this to $[A(E_2 - O)(f_2(b) + (0,1), f_2(z) + (0,1))]$ and $[A(E_2 - O)(f_2(b) - (0,1), f_2(z) - (0,1))]$ gives

$$\begin{aligned}
&[A(E_2 - O)(f_2(b) + (0,1), f_2(z) + (0,1))] + [A(E_2 - O)(f_2(b) - (0,1), f_2(z) - (0,1))] \\
=&[A(E_2 - O)(t, f_2(z) + (0,1))] + [A(E_2 - O)(t, f_2(z) - (0,1))] \\
&- [A(E_2 - O)(t, f_2(b) + (0,1))] - [A(E_2 - O)(t, f_2(b) - (0,1))]
\end{aligned}$$

□

Chapter 3

Local structure

The previous chapter gives a means to compute equations satisfied by the cohomology varieties $H^1_{f,\mathcal{L}}(G_T, U)$ via embedding into an affine space $H^1_{f,T}(G_T, E(V, [L, L]))$. To utilise this for the explicit nonabelian Chabauty method, we need to be able to compute the local unipotent Kummer maps

$$j_{n,v} : X(\mathbb{Q}_v) \to H^1(G_v, U_n)$$

for primes $v \in T$. In this chapter this computation is discussed in detail (as before, the emphasis will be on U_2 and its quotients). For $v \in T_0$, several new results are obtained. A refinement on the bound in [46] on the size of $j_{n,v}(X(\mathbb{Q}_v))$ is given. This refinement further describes a method for computing $j_{n,v}$, given a regular semistable model. We implement this method to prove that $j_{2,v}$ distinguishes irreducible components of the special fibre of a regular semistable model when the Jacobian of X has good reduction. Further we use it to give an example to show that this need not hold without the assumption on the Jacobian of X.

At the prime p, the focus of this chapter is on explicit formulae for the map $j_{n,p}$. Some foundational material on the unipotent rigid and de Rham fundamental groups is recalled in sections 3 and 4, along with the relation to the étale fundamental group. In section 3 we sketch an algorithm for computing the Hodge filtration, and hence a formula for the local unipotent Albanese map

$$j_n^{\mathrm{cr}} : X(\mathbb{Q}_p) \to U^{dR}/F^0$$

This enable us to give explicit formulae for local analogues of the maps Θ and Ψ at the prime p in section 5. This is used in the next chapter to describe explicit formulae for the maps Θ and the finite sets they produce.

3.1 Local structure at $v \neq p$

We describe the local unipotent Kummer map

$$j_{n,l} : X(\mathbb{Q}_l) \to H^1(G_l, U_n)$$

at a prime $l \neq p$ of bad reduction. By the weight monodromy arguments of chapter 1 this amounts to computing the action of inertia on $A_n(b)$ and $A_n(b, z)$. Our method for computing this map follows the paper of Oda [52]. In loc. cit., Oda uses the deformation theory of curves, together with Abhyankar's Lemma, to replace mixed characteristic with equal characteristic (0,0). The question then becomes of a combinatorial topological nature, similar to the argument of [52] and Oda and collaborators [3]. A contrast between these works and the material of this thesis is that Oda focuses on the computation of the outer action of the Galois group on the fundamental group, which forgets basepoints and simplifies the description of the monodromy action. By contrast, our interest is in the how the monodromy varies with the basepoint. Hence we need to modify arguments slightly to keep track of basepoints, which introduces some cumbersome arguments (even though conceptually they are natural extensions of Oda's work). At the end of the section we give a few examples illustrating how to implement this method in practice for the map

$$j_l : X(\mathbb{Q}_l) \to H^1(G_l, U)$$

where U is a quotient of U_2.

3.1.1 Galois cohomology

To describe $j_{n,v}$, we use the fact that

$$H^1(G_{\mathbb{Q}_l}, U_n) \to H^1(H, U_n)$$

is injective for any finite index subgroup H. We henceforth fix an extension $L_0|\mathbb{Q}_v$ over which X has a minimal regular semistable model

$$\mathcal{X}_{\mathcal{O}_{L_0}} \to \mathrm{Spec}(\mathcal{O}_{L_0})$$

Remark 4. The semistability condition is a natural one to impose as it makes the action of inertia unipotent. The reason for imposing regularity is that we want to be able to characterise the torsor of paths between two points purely in terms of their reduction to the special fibre. When the model is not regular, there may be points of bad reductions $\overline{z}$ in the special fibre such that z_1 and z_2 reduce to z, but the torsor of paths from z_1 to z_2 is nontrivial.

Let $Y_1, \ldots, Y_d$ denote the irreducible components of $\mathcal{X} \times \mathrm{Spec}(k)$ (where k is the residue field of L_0). Let g_i denote the genus of Y_i. Then V, restricted to G_{L_0}, admits a monodromy filtration

$$0 = W_3V \subset W_2V \subset W_1V \subset W_0V = V$$

such that inertia acts trivially on the graded pieces, and G_k acts on V_i/V_{i+1} with weight $-i$. We obtain an induced weight filtration

$$U_n = W_0U_n \supset W_1U_n \supset W_2U_n \supset \ldots \supset W_{2n+1}U_n = 1$$

As the conjugation action of U_n on itself respects the weight filtration, this is a filtration by normal subgroups. If we are interested in the unipotent Kummer map, the information contained in W_3U_n can be ignored:

Lemma 26. *For all n, the map*

$$H^1(G_v, U_n) \to H^1(G_v, U_n/W_3U_n)$$

is an isomorphism

Proof. It is sufficient to prove that $H^1(G_v, W_3U[i])$ and $H^2(G_v, W_3U[i])$ are zero for all i, which follows from the fact that for weight reasons

$$H^0(G_v, U[i]) = H^0(G_v, U[i]^*(1)) = 0$$

□

We henceforth work with a quotient U of U_n for which $W_3 U = 1$.

Let L denote the maximal unramified extension of L_0.

Lemma 27. *The map*

$$H^1(G_{L_0}, U) \to H^1(G_L, U)$$

is injective.

Proof. It is sufficient to prove that for all i,

$$H^1(\mathrm{Gal}(\overline{k}|k), U[i]^{I_v}) = 0$$

which follows from the weight monodromy conjecture for curves. □

3.1.2 Log smooth deformations of $\mathcal{X}$

By the above the study of the unipotent Kummer map for a curve X over $\mathbb{Q}_l$ is reduced to its study over L, where L is the maximal unramified extension of a finite extension L_0 of $\mathbb{Q}_l$ over which X admits a regular semistable model. Let π be a uniformiser of L, and let

$$\mathcal{X} \to \mathrm{Spec}(\mathcal{O}_L)$$

also denote the base change of this model to $\mathcal{O}_L$.

Let R denote the Henselisation of $\mathcal{O}_L[t]$ at the prime ideal (t). We recall the version of Abhyankar's Lemma used by Oda:

Proposition 5. *[37] Let K denote the field of fractions of the strict Henselisation of R at the prime ideal (t). Let*

$$p : R[1/t] \to L$$

denote the specialisation at $t = \pi$, and let

$$i : R[1/t] \to K$$

denote the natural inclusion. Let $\overline{p}$ and $\overline{i}$ denote the induced composite morphisms to algebraic closures

$$L \hookrightarrow \overline{L}$$

and

$$K \hookrightarrow \overline{K}$$

Then

$$p_* : \pi_1^{\acute{e}t}(\mathrm{Spec}(R[1/t], \overline{p})^{(l)} \to \mathrm{Gal}(\overline{L}|L)^{(l)}$$

and

$$i_* : \pi_1^{\acute{e}t}(\mathrm{Spec}(R[1/t], \overline{i})^{(l)} \to \mathrm{Gal}(\overline{K}|K)^{(l)}$$

are isomorphisms (where $^{(l)}$ *denotes the maximal prime to* l *quotient).*

To use this result, we need to construct a regular semistable deformation of $\mathcal{X}$ to R. The construction of such a deformation is standard in the literature on monodromy operators for curves [21] [1]

The existence of such a deformation is proved in two steps, following [21]. First, we need the following result, which is a consequence of [40]:

Theorem 15 (Kato)**.** *There exists a compatible family of deformations*

$$f_n : \mathcal{X}_n \to \mathcal{O}_L[T]/(T)^n$$

of $\mathcal{X} \to \mathcal{O}_L$ *such that for each* n *every singular point of* $\mathcal{X}_n$ *has an étale neighbourhood isomorphic to*

$$\mathcal{O}_L[x, y, T]/(xy - T)$$

Taking the limit over n we obtain

$$\widetilde{f} : \widetilde{\mathcal{X}} \to \mathcal{O}_L[\![T]\!]$$

whose fibre at a $T = \pi$ is isomorphic to $\mathcal{X}$ (shifting co-ordinates by π), and whose singularities are étale locally of the form $xy - T$. We extend the sections b and z to sections

$$\widetilde{b}, \widetilde{z} : \mathrm{Spec}(\mathcal{O}_L[\![T]\!]) \to \widetilde{\mathcal{X}}$$

For the second step, by Artin's approximation theorem [2], $\widetilde{f}$ is the pullback under $R_0 \to \mathcal{O}_L[\![T]\!]$ of some

$$\overline{f} : \overline{\mathcal{X}} \to R_0$$

where R_0 is some finite cover of $\mathcal{O}_L[T]$ unramified along (T), contained inside the Henselisation R.

By Hensel's Lemma, the sections b and z come from sections

$$\overline{b}, \overline{z} : \mathrm{Spec}(R_0) \to \overline{\mathcal{X}}$$

The sections $\overline{b}$ and $\overline{z}$ induce, for any geometric point $s : R_0[1/T] \to \overline{F}$, an action of $\pi_1^{ét}(\mathrm{Spec}(R_0[1/T], s)$ on $\pi_1^{ét}(\overline{\mathcal{X}} \times_s \overline{F}, s \circ \overline{b})$, $\pi_1^{ét}(\overline{\mathcal{X}} \times_s \overline{F}, s \circ \overline{z})$ and $\pi_1^{ét}(\overline{\mathcal{X}} \times_s \overline{F}; s \circ \overline{b}, s \circ \overline{z})$.

By Abhynakar's Lemma, taking the geometric points

$$\overline{p} : R[1/T] \to \overline{L}$$

$$\overline{i} : R[1/T] \to \overline{K}$$

we can identify the $\mathrm{Gal}(\overline{L}|L)$ and $\pi_1^{ét,(l)}(\mathrm{Spec}(R[1/T]), \overline{p})$ actions on

$$\pi_1^{ét,p}(\overline{\mathcal{X}} \times_{\overline{p}} \overline{L}, \overline{p} \circ \overline{b}),$$

and we can also identify the $\mathrm{Gal}(\overline{K}|K)$ and $\pi_1^{ét,(l)}(\mathrm{Spec}(R[1/T]), \overline{i})$ actions on

$$\pi_1^{ét,p}(\overline{\mathcal{X}} \times_{\overline{i}} \overline{K}, \overline{i} \circ \overline{b}).$$

.

Choosing a path from $\overline{p}$ to $\overline{i}$, we get a commutative diagram

$$\begin{array}{ccc}
\mathrm{Gal}(\overline{L}|L)^{(l)} & \longrightarrow & \mathrm{Gal}(\overline{K}|K)^{(l)} \\
\downarrow & & \downarrow \\
\mathrm{Aut}\, \pi_1^{ét,p}(\overline{\mathcal{X}} \times_{\overline{p}} \overline{L}) & \longrightarrow & \mathrm{Aut}\, \pi_1^{ét,p}(\overline{\mathcal{X}} \times_{\overline{i}} \overline{K})
\end{array}$$

Choosing an embedding $j : \overline{L} \hookrightarrow \mathbb{C}$, we get a regular family of semistable algebraic curves over $\mathbb{C}$:

$$\overline{\mathcal{X}} \times_{\mathcal{O}_L} \mathbb{C} \to \mathrm{Spec}(R_0 \otimes_{\mathcal{O}_L} \mathbb{C})$$

and sections

$$\overline{b} \times 1, \overline{z} \times 1 : \mathrm{Spec}(R_0 \otimes_{\mathcal{O}_L} \mathbb{C}) \to \overline{\mathcal{X}} \times_{\mathcal{O}_L} \mathbb{C}$$

The maps $\pi_1^{ét}(\mathrm{Spec}(R \otimes_{\overline{L}} \mathbb{C}[1/T], \overline{s}) \to \pi_1^{ét}(\mathrm{Spec}(R[1/T], s \circ (1 \times j))$, $\pi_1^{ét}(\overline{\mathcal{X}} \times \overline{s}) \to \pi_1^{ét}(\overline{\mathcal{X}} \times \overline{s'})$ and $\mathrm{Gal}(\overline{K} \otimes_{\overline{L}} \mathbb{C} | K \otimes_{\overline{L}} \mathbb{C}) \to \mathrm{Gal}(\overline{K}|K)$ are isomorphisms. We fix a path between

$$R \otimes_{\overline{L}} \mathbb{C}[1/T] \to \overline{K}$$

and a tangential basepoint, t, at $T = 0$ Pick a prime p_0 in $R_0 \otimes_{\mathcal{O}_L} \mathbb{C}$ lying between (t) and the maximal ideal of $R \times_{\overline{L}} \mathbb{C}$ under

$$\mathbb{C}[t] \subset R_0 \otimes_{\mathcal{O}_L} \mathbb{C} \subset R \otimes_{\overline{L}} \mathbb{C}$$

Let $U \ni p_0$ be a contractible neighbourhood of p_0 in the complex analytification of $\mathrm{Spec}(R_0 \otimes_{\mathcal{O}_L} \mathbb{C})$ with a fixed isomorphism of pointed complex analytic spaces

$$(U, p_0) \simeq (D, 0)$$

where D is the open unit disc. Let

$$X^{\mathrm{an}} \subset (\overline{\mathcal{X}} \times_{\mathcal{O}_L} \mathbb{C})^{\mathrm{an}}$$

denote the preimage of D under

$$(\overline{\mathcal{X}} \times_{\mathcal{O}_L} \mathbb{C})^{\mathrm{an}} \to \mathrm{Spec}(R_0 \otimes_{\mathcal{O}_L} \mathbb{C})$$

giving a family

$$f^{\mathrm{an}} : X^{\mathrm{an}} \to D$$

of complex analytic spaces, and sections

$$b^{\mathrm{an}}, z^{\mathrm{an}} : D \to X^{an}$$

Let $B = \mathrm{Spec}(R_0 \otimes_{\mathcal{O}_L} \mathbb{C}) - p_0$. Let t be a tangential basepoint at p_0. Let t^{an} denote the corresponding basepoint of $D - 0$. Choose a path from t to the algebraic closure of the generic point of B.

Applying the Riemann Existence Theorem the topological closure of the natural map from $\pi_1(D - 0, t^{an})$ to $\pi_1(B, t)$ is identified with the inertia group at p_0, which is equal to the image of $\mathrm{Gal}(\overline{K} \otimes_{\overline{L}} \mathbb{C} | K \otimes_{\overline{L}} \mathbb{C})$. Pick a point η in $D - 0$, and a path from t^{an} to η. This then identifies $\pi_1(X_\eta^{\mathrm{an}}; b^{\mathrm{an}}, z^{\mathrm{an}}) \times_{\pi_1(X_\eta^{\mathrm{an}}, b^{\mathrm{an}})} \pi_1^{ét}(\overline{X} \times_{R_0} \overline{K} \otimes_{\overline{L}} \mathbb{C}, b)$ with $\pi_1^{ét}(\overline{X} \times_{R_0} \overline{K} \otimes_{\overline{L}} \mathbb{C}; b, z)$. We get a commutative diagram:

$$\begin{array}{ccc}
 & & \mathrm{Gal}(\overline{K} \otimes_{\overline{L}} \mathbb{C} | K \otimes_{\overline{L}} \mathbb{C}) \\
 & & \downarrow \\
\pi_1^{\mathrm{top}}(D - 0, t^{\mathrm{an}}) & \longrightarrow & \pi_1^{ét}(B, t) \\
\downarrow & & \downarrow \\
\mathrm{Aut}(\pi_1^{\mathrm{top}}(X_\eta; b^{\mathrm{an}}, z^{\mathrm{an}}) & \longrightarrow & \mathrm{Aut}\, \pi_1^{ét}(\overline{X} \times_{R_0} \overline{K} \otimes_{\overline{L}} \mathbb{C}; b, z)
\end{array}$$

which, putting everything together, identifies the $I_v^{(l)}$ action on $\pi_1^{\acute{e}t,p}(X \times \overline{L}; b, z)$ with the $\pi_1(D-0,\eta)$ action on $\pi_1(X_\eta^{\mathrm{an}}; b, z)$.

3.1.2.1 Computing topological monodromy

We now describe how to compute the action of $\pi_1^{\mathrm{top}}(D-0,\eta)$ on $\pi_1^{\mathrm{top}}(X_\eta^{an}; b, z)$, following Oda. Henceforth γ will denote a fixed generator of $\pi_1^{\mathrm{top}}(D-0,\eta)$.

Let $(v_\alpha)_{1\leq\alpha\leq n}$ be the vertex set of the dual graph of the special fibre, and (e_β) the edge set, corresponding to a set of singular points (z_β). At each z_β, fix an open neighbourhood $U_\beta \ni z_\beta$ in X^{an} and isomorphism of complex analytic spaces over D

$$\psi_\beta : U_\beta \xrightarrow{\simeq} M$$

Let where $M = \{(xy = t) | \|x\|^2 + \|y\|^2 < 1\}$. Fix sections

$$s_1, s_2 : D \to M$$

such that the $\pi_1(D-0)$-equivariant torsor of paths from $\eta \circ s_1$ to $\eta \circ s_2$ is nontrivial: Let δ_M be a generator of $\pi_1(M_\eta, \eta \circ s_1)$ and p_M a path in M_η from $\eta \circ s_1$ to $\eta \circ s_2$ such that $\gamma p_M = \delta_M p_M$. The isomorphisms ψ_β give associated paths on U_β, determining an orientation for each edge e_β. Let δ_β be the loop in $\pi_1(U_{\beta,\eta}, \eta \circ s_1 \circ \psi_\beta)$ corresponding to δ_M. This gives a recipe for computing the γ-action on a path as follows: any path p on X^{an} induces a path $e_{i_1}^{k_1} \ldots e_{i_m}^{k_m}$ in the dual graph (where $k_m \in \{\pm 1\}$. Decompose p as $p_1 \ldots p_m$, so that p_j corresponds to $e_{i_j}^{k_j}$. Then

$$\gamma(p) = \delta_{i_1} p_1 \ldots \delta_{i_m} p_m$$

Below we show how to use this in explicit examples.

3.1.2.2 Computing the unipotent Kummer map for Heisenberg quotients

We fix a curve X over a finite extension of $\mathbb{Q}_l$ with semistable reduction, and a basepoint b. Let $U' = U'(b)$ be a quotient of $U_2(b)$ such that $[L', L']$ is self-dual (i.e. $[L', L'] \simeq [L', L']^*(2)$). Γ will henceforth denote either the prime-to-l part of the inertia subgroup of G_{L_0} or $\pi_1(D-0,\eta)$. Let U be a quotient of U' with $W_3 U = 1$. Let A be the quotient of the universal enveloping algebra with graded pieces $\mathbb{Q}$, V

and $[L, L]/W_3[L, L]$. Let I be the augmentation ideal. So A is isomorphic to the quotient of the universal enveloping algebra by the ideal generated by I^3, $\mathrm{Sym}^2 I$ and $W_3 I$.

Let L denote the Lie algebra. The maps

$$L \to A$$

and

$$U \to A^\times$$

gives isomorphisms

$$L \xrightarrow{\simeq} IA$$

$$U \xrightarrow{\simeq} 1 + IA$$

Lemma 28. *Let U be as above. Then a Γ-equivariant U-torsor P is trivial if and only if the exact sequence of Γ-modules*

$$0 \to IA^{(P)} \to A^{(P)} \xrightarrow{\pi} \mathbb{Q}_p \to 0$$

splits

Proof. There is a Γ-equivariant isomorphism

$$\pi^{-1}(1) \simeq P$$

Hence P is trivial if and only if $\pi^{-1}(1)$ has a Γ-fixed point, which happens if and only if the exact sequence splits. □

3.2 Examples

In this section we illustrate some features of the local unipotent Kummer map j at a prime of bad reduction. Unsurprisingly, the structure of j depends on properties of the dual graph of the special fibre of a semistable model. We show that in the case Oda originally considered (where the Jacobian has potentially good reduction but X doesn't) the map j can distinguish irreducible components of a minimal semistable regular model. This need not hold in general, and in the subsequent subsection a totally degenerate genus 2 counterexample is given.

3.2.1 V has potential good reduction

Suppose the action of I_l on V is finite, but X doesn't have potential good reduction. Recall that by the theorem of Serre and Tate [60] this means that the Jacobian of X has potential good reduction, hence we are in the situation considered in [52]. Let $L|\mathbb{Q}_l$ be a finite extension over which V is unramified. Then the dual graph of a stable model of X is a tree.

Lemma 29. *A is unramified.*

Proof. Recall

$$A \simeq IA \oplus \mathbb{Q}_p$$

as a Galois module, so it is enough to show that IA is unramified. This can be seen for weight reasons: V and $[L, L]$ (the graded pieces of IA) are unramified and pure of weights -1 and -2 respectively, so there are no ramified extensions of V by $[L, L]$. □

Hence in order to show that the torsor of paths from a basepoint b to z is nontrivial, it is enough to find a path from b to x which is not fixed by γ.

Theorem 16. *Let X be a smooth proper curve over a local field K as above, with a minimal regular semistable model $\mathcal{X}$. Suppose b and z in $X(K)$ lie on distinct irreducible components of the special fibre of $\mathcal{X}$. Then $j_2(b, z)$ is non-trivial.*

Proof. Let X_η^{an} be the fibre at η of the family of semistable complex analytic spaces X^{an} defined above, and let $b = b^{\mathrm{an}}$ and $z = z^{\mathrm{an}}$ denote the corresponding section. By the above it is enough to show that the action of $\pi_1(D - O)$ on the depth 2 torsor of paths from b^{an} to z^{an} is nontrivial. The idea of the proof is very simple. When the two points are on adjacent irreducible components it is essentially immediate. In general, we pick an irreducible component b' inbetween and show that the torsors from b' to b and b' to z must be distinct. The result then follows by induction on the number of irreducible components between b and z. Below we spell this argument out in detail:

Since the dual graph of the special fibre is a tree, there is a unique minimal path from the irreducible component of b to the irreducible component of z. Decompose this path as $e_{\alpha_1} \ldots e_{\alpha_n}$ where e_{α_i} is a directed edge from $v_{\alpha_{i-1}}$ to v_{α_i}, and for

$i \neq j$ $v_{\alpha_i} \neq v_{\alpha_j}$ by minimality. Let $v_{\beta_1}, \ldots v_{\beta_m}$ be the subsequence of irreducible components of genus bigger than 0. Hence the irreducible components connecting β_i and β_{i+1} are a chain of $\mathbb{P}^1$s. We prove the theorem by induction on m. In fact we prove slightly more. Recall that for each edge e we have a neighbourhood U_e in X such that

$$X - \cup_e U_e \simeq \cup_v C_v^{\times} \times D$$

where $C_v^{\times}$ is the Riemann surface obtained from the irreducible component of the special fibre v by removing small neighbourhoods of the singular points.

Given a nonrepeating path $P = e_1 \ldots e_n$ on the dual graph with vertices $v_0 \ldots v_n$ let X_P be the topological space fibered over D obtained by contracting all $C_v^{\times} \times D$ for v not in P, and contracting all U_e for e not in P. Hence X_P admits a map of spaces over D

$$X \to X_P$$

Since the dual graph is a tree the fundamental group of X_P has $2\sum_i g_i$ generators, where g_i is the genus of v_i.

Any nonrepeating path P on the dual graph can be extended to a larger nonrepeating path whose end vertices have positive genus. To see this, note that by Castenuovo's criterion, if v is an irreducible component of genus zero which only intersects one other component then $\mathcal{X}$ admits a blow-down contracting v, hence by minimality of the model the claim follows.

Given a nonrepeating path P, let P' be a minimal extension to a path whose end vertices have positive genus. Let $v_{n_0}, \ldots, v_{n_m}$ be the subsequence of vertices of P' of positive genus.

We claim that the image of the torsor of paths from b to z in the fundamental group of $X_{P'}$ is nontrivial.

This can be seen by induction on m. First suppose m is zero. Then as in [52] the Dehn twist associated to the path from v_{n_0} to v_{n_m} is nontrivial in $X_{P'}$, and hence so is the action of γ on P in $X_{P'}$.

Now suppose $m > 0$. Then there is a vertex v in P of positive genus. Decompose P as $P_1 P_2$, where P_1 and P_2 both have v as an end vertex. Let P_1' and P_2' be extensions to paths with end vertices of positive genus. If the torsor of paths P were unramified, then the action of γ on P_1 would have to be inverse to the action on P_2. But the image of P_2 in X_{P_1} is trivial, whereas the image of P_1 is ramified, hence the actions cannot be inverse. $\square$

3.2.2 Totally degenerate genus 2 curves

In this section we give an example to show that in general the map j_2 need not distinguish the irreducible components of a minimal regular semistable model.

Theorem 17. *Let X be a genus two curve admitting a stable regular model with special fibre isomorphic to two genus zero curves intersecting transversally at three points z_1, z_2, z_3. For all x, y in $X(K)$, $P(x, y)$ is a trivial G_K-equivariant $U_2(x)$ torsor.*

Example 3. The modular curve $X_0(37)$ has genus two, and by the theorem of Deligne and Rapoport has a model over $\mathbb{Z}_{37}$ as above [28].

Proof. As before we deform $\mathcal{X}$ and replace it with a family of semi-stable (and in this case actually stable) curves

$$X^{\mathrm{an}} \to D$$

and sections

$$x_1^{\mathrm{an}}, x_2^{\mathrm{an}} : D \to X^{\mathrm{an}}$$

Let z_1, z_2 and z_3 denote the three singular points, with corresponding neighbourhoods U_1, U_2 and U_3 in X^{an}. $X^{\mathrm{an}} - (U_1 \cup U_2 \cup U_3)$ is isomorphic to

$$D \times Y$$

where Y is a disjoint union of two copies of $\mathbb{P}^1$ minus three disjoint discs. Let p_1, p_2 and p_3 be three paths from x_1^{an} to x_2^{an}, such that p_i meets U_i and none of the other U_j. Define $c = p_1 p_2^{-1}$ and $d = p_3 p_2^{-1}$ (recall we are composing paths from left to right, so c is a loop with basepoint x_1^{an}. Fix an orientation of X identifying $H^2(X, \mathbb{Q})$ with $\mathbb{Q}$.

Choose loops q_1, q_2, q_3 based at x_1, such that

- q_i loops once around the missing point z_i

- none of the q_i meet the U_j
- Taking $\{c, d, q_1, q_3\}$ as a basis of H_1, the dual basis $\{c^*, d^*, q_1^*, q_3^*\}$ satisfies

$$c^* \cup q_1^* = d^* \cup q_3^* = 1 \tag{3.1}$$

- The loop q_2 satisfies

$$[q_1] + [q_2] + [q_3] = 0$$

  in H_1.

By the description of γ given in the previous section, there are $\epsilon_i \in \{\pm 1\}$ such that, for $1 \leq i \leq 3$,

$$\gamma.p_i = q_i^{\epsilon_i}.p_i$$

Note that since q_1, q_2 and q_3 all lie in W_2, they commute in U.

Let C, D, Q_1 and Q_3 denote the logarithms of c, d, Q_1 and Q_3 in L. Let $A(x_1)$ be the quotient of the enveloping algebra described above. It follows from the definitions above that A is isomorphic to

$$\mathbb{Q} \oplus V \oplus \wedge^2 V / \langle C \wedge Q_1 + D \wedge Q_3, Q_1 \wedge Q_3 \rangle$$

As above, we identify U with $1 + IA \subset A^\times$. So

$$\begin{aligned}
\gamma(C) &= \gamma(1 + C) - 1 \\
&= (1 + \epsilon_1 Q_1)(1 + C)(1 + \epsilon_2(Q_1 + Q_3)) - 1 && (3.2) \\
&= C + (\epsilon_1 + \epsilon_2)Q_1 + \epsilon_2 Q_3 + (\epsilon_2 - \epsilon_1)C \wedge Q_1 + \epsilon_2 C \wedge Q_3 && (3.3)
\end{aligned}$$

and similarly

$$\gamma(D) = D + (\epsilon_3 + \epsilon_2)Q_3 + \epsilon_2 Q_1 + (\epsilon_2 - \epsilon_3)D \wedge Q_3 + \epsilon_2 D \wedge Q_1$$

By Lemma 28, to prove that $[P(x_1, x_2)]$ is trivial it is sufficient to prove that $A^{(P)}$ splits. We may write an element of $A^{(P)}$ as a sum of paths from x_1 to x_2, with a left action of A. $A^{(P)}$ is generated by the path p_2 defined above, which has γ action

$$\gamma p_2 - p_2 = -\epsilon_2(Q_1 + Q_3).p_2$$

To construct a splitting of $A^{(P)}$, it is hence enough to show that $(Q_1 + Q_3).p_2$ lies in $(\gamma - 1)IA$. So we compute the action of γ on elements of IA:

$$\begin{aligned}
&\gamma(C.p_2) - C.p_2 \\
&= ((\epsilon_1 + \epsilon_2)Q_1 + \epsilon_2 Q_3 + (\epsilon_2 - \epsilon_1)C \wedge Q_1 + \epsilon_2 C \wedge Q_3)(1 + \epsilon_2(Q_1 + Q_3))p_2 \\
&= [(\epsilon_1 + \epsilon_2)Q_1 + \epsilon_2 Q_3 - \epsilon_1 C \wedge Q_1]p_2
\end{aligned}$$

Similarly

$$\gamma(D.p_2) - D.p_2 = [(\epsilon_3 + \epsilon_2)Q_3 + \epsilon_2 Q_1 - \epsilon_3 D \wedge Q_3]p_2$$

Hence

$$\begin{aligned}
&\epsilon_3(\gamma - 1)C.p_2 + \epsilon_1(\gamma - 1)D.p_2 \\
&= [(\epsilon_1\epsilon_2 + \epsilon_1\epsilon_3 + \epsilon_2\epsilon_3)(Q_1 + Q_3) - \epsilon_1\epsilon_3(C \wedge Q_1 + D \wedge Q_3)].p_2 \\
&\in \langle (Q_1 + Q_3).p_2 \rangle
\end{aligned}$$

since $C \wedge Q_1 + C \wedge Q_3 = 0$ This completes the proof of the theorem. □

3.3 The de Rham fundamental group

The remainder of this chapter describes the local structure of the unipotent Kummer map, and the local version of Ψ, at the prime p.

By p-adic Hodge theory, this amounts to describing maps

$$j^{\mathrm{cr}} : X(\mathbb{Q}_p) \to U^{dR}/F^0$$

and

$$\Psi^{\mathrm{cr}} : U^{dR}/F^0 \to E_p^{cry}(V, [L, L])/F^0$$

which replace the $G_{\mathbb{Q}_p}$-structure of $P^{\acute{e}t}(b, z)$ with the compatible structure of a Hodge filtration (coming from the theory of the de Rham fundamental group and Frobenius action (coming from the theory of the crystalline fundamental group). The next few sections will be spent preparing the definition of $E_p^{cry}(V, [L, L])/F^0$ and Ψ^{cr}.

In this section we describe the de Rham analogues of U_n^{dR}, P_n^{dR} and A_n^{dR}, as constructed in [26]. In order to describe these objects for a projective curve X, it will be convenient to describe the theory in the more general setting of a a curve Y over a field K of characteristic zero, contained inside a projective curve X with (possibly empty) complement D. Denote by $\mathcal{C}^{dR}(Y)$ the category of unipotent flat connections on Y. An object of $\mathcal{C}^{dR}(Y)$ is then a vector bundle $\mathcal{V}$ on Y, together with

$$\nabla : \mathcal{V} \to \mathcal{V} \otimes \Omega_Y^1$$

satsifying $\nabla(fv) = df \otimes v + f \otimes \nabla(v)$ $f \in \mathcal{O}(U), v \in \mathcal{V}(U)$, $U \subset X$, satisfying the flatness condition $\nabla^2 = 0$, and such that there exist a decreasing filtration

$$\mathcal{V} \supset \mathcal{V}_1 \supset \ldots \supset \mathcal{V}_n = 0$$

by subconnections, such that $\mathcal{V}_i/\mathcal{V}_{i+1}$ is isomorphic to a direct sum of copies of the trivial connection $(\mathcal{O}, d)$. A morphism in $\mathcal{C}^{dR}(Y)$ is a morphism of vector bundles that is horizontal with respect to the connections: that is, a morphism

$$(\mathcal{V}_1, \nabla_1) \to (\mathcal{V}_2, \nabla_2)$$

is a morphism of vector bundles

$$f : \mathcal{V}_1 \to \mathcal{V}_2$$

such that

$$\begin{array}{ccc} \mathcal{V}_1 & \xrightarrow{f} & \mathcal{V}_2 \\ \downarrow \nabla_1 & & \downarrow \nabla_2 \\ \Omega^1 \otimes \mathcal{V}_1 & \xrightarrow{1 \otimes f} & \Omega^1 \otimes \mathcal{V}_2 \end{array}$$

commutes. The reason for allowing the case of an affine curve is that in this case any vector bundle admits a trivialisation, and hence a connection on an n-dimensional vector bundle is (up to isomorphism) given as

$$\mathcal{O}_Y^{\oplus n} \to (\Omega_Y^1)^{\oplus n}$$

We may view the category of connections on X as a subcategory of $\mathcal{C}^{dR}(Y)$. Although the subcategory of vector bundles on X is not full in the category of vector bundles on Y, by Deligne's theorem (see below) the category $\mathcal{C}^{dR}(X)$ is a full subcategory of $\mathcal{C}^{dR}(Y)$.

For any point x on Y we have a fibre functor x^* from $\mathcal{C}^{dR}(Y)$ to the category of K-vector spaces. $\mathcal{C}^{dR}(Y)$ obtains the structure of a neutral Tannakian category, and similarly to before we obtain the following objects:

- finite dimensional n-step unipotent groups $U_n^{dR}(x)$ over K satisfying

$$\pi_1(\mathcal{C}^{dR}(Y), x) = \varprojlim U_n$$

- n-step nilpotent Lie algebras $L_n^{dR}(x)$ over K corresponding to U_n via the exponential map.
- A family of nilpotent K-algebras $A_n^{dR}(x)$ such that $\varprojlim A_n dR(x)$ is isomorphic to the universal enveloping algebra of the pro-nilpotent Lie algebra $\varprojlim L_n(x)$.
- Flat connections $\mathcal{A}_{n,x}^{dR}$, $\mathcal{L}_n^{dR}$ corresponding to $A_n(x)$ and $L_n(x)$ via the equivalence of Tannakian categories between modules for $\varprojlim A_n(x)$ and $\mathcal{C}^{dR}(Y)$.
- A family $P_n^{dR}(b, z) = P_n^{dR}(z)$ of left $U_n^{dR}(b)$-torsors.

Where there is no risk of confusion we shall frequently omit the superscript and write simply $\mathcal{A}_n, A_n(b, z)$ etc. Where this ambiguity about the underlying curve we write the universal connection $\mathcal{A}_n$ as $\mathcal{A}_n(Y)$. In the case where $|D| = d > 0$, we can give an explicit formula for ∇ as follows:

Definition 26. Fix a set $\omega_0 \ldots, \omega_{2g+d-2}$ of global differentials on an affine open Y forming a basis of $H^1_{dR}(Y)$. Let $K\langle T_0, \ldots, T_{2g+d-2}\rangle$ denote the free associative K-algebra generated by $2g+d-1$ variables $T_0, \ldots, T_{2g-1}$ and denote by I the two-sided ideal $(T_0, \ldots, T_{2g+d-2})$. Define the *universal connection* to be the inverse system of connections with trivial bundle $K\langle T_0, \ldots, T_{2g+d-2}\rangle / I^{n+1} \otimes R$, and connection given by

$$\nabla(v \otimes 1) \mapsto -\sum T_i v \otimes \omega_i$$

In [42], Kim shows that $(K\langle T_0, \dots, T_{2g+d-2}\rangle / I^n \otimes \mathcal{O}_Y)_n$ is universal for unipotent connections:

Theorem 18 (Kim,[42])**.** *(i): Let $\mathcal{V} \in \mathcal{C}^{dR}$, $x \in Y(K)$, and $v \in x^*\mathcal{V}$. For all $n \gg 0$, there exists a unique morphism of connections*

$$f : K\langle T_0, \dots, T_{2g+d-2}\rangle / I^n \otimes R \to \mathcal{V}$$

such that

$$x^* f : K\langle T_0, \dots, T_{2g+d-2}\rangle / I^n \to x^* V$$

sends 1 to v.
(ii): There is a canonical isomorphism of connections

$$f : K\langle T_0, \dots, T_{2g+d-2}\rangle / I^{n+1} \otimes \mathcal{O} \simeq \mathcal{A}_n^{dR}$$

We shall henceforth identify the fibres of $\mathcal{A}_n$ with $A_n := K\langle T_0, \dots, T_{2g+d-2}\rangle / I^{n+1}$. As explained in loc. cit., this theorem identifies the category of flat connections on Y with the category of finite $K\langle T_0, \dots, T_{2g+d-2}\rangle$-modules.

Our principal interest is actually in computing the the universal connection for the projective curve X, rather than an affine open. However as in the étale case this will be a quotient of the universal connection of an affine open

Remark 5. In the case when D is empty, one can describe the de Rham enveloping algebra of X as follows. By removing a nonempty divisor D, one may choose differentials of the second kind $\omega_0, \dots, \omega_{2g-1}$ forming a basis of $H^1_{dR}(X)$. As above, use these to define a connection on the trivial (pro-) vector bundle over Y with fibre isomorphic to a free (pro-) associative algebra on 2g generators. The graded pieces of this are isomorphic to $(H^1_{dR}(X)^{\otimes n})^*$. As in the étale case, one quotients by the two-sided ideal generated by an element of I^2. We know that modulo I^3 this element can be taken to be the image of $H^2_{dR}(X)^*$ in $H^1_{dR}(X)^{\otimes 2}$ arising from the map

$$H^2_{dR}(X)^* \to (H^1_{dR}(X)^{\otimes 2})^*$$

dual to the cup product. By Serre's residue formula for the cup product in de Rham cohomology [57], an equivalent description is that one take the maximal quotient of $\mathcal{A}_2(Y)$ which extends to a connection without singularities on X. We write this as

$$\mathcal{A}_2(X)|_Y \simeq K\langle T_0, \ldots, T_{2g-1}\rangle/(I^3, H^2(X)^*)$$

where $H^2(X)^*$ is identified as a linear combination of $T_i \otimes T_j$ by viewing the T_i as the dual basis of the ω_i and $H^2(X)^*$ is viewed as a submodule of $(H^1(X)^*)^{\otimes 2}$ via

$$H^2(X)^* \xrightarrow{\cup^*} (H^1(X)^*)^{\otimes 2}$$

The following notation will be used to describe the universal connection of a projective curve in a relatively concrete fashion.

Definition 27. Let X be a smooth projective curve of genus $g > 1$ over a field K of characteristic zero. Let $\omega_0, \ldots, \omega_{2g-1}$ be a set of differentials of the second kind giving a basis of $H^1_{\mathrm{dR}}(X)$. The ω_i are also taken to be a basis such that $\omega_0, \ldots, \omega_{g-1}$ form a basis of $H^0(X, \Omega^1)$. Let $Y \subset X$ be an open affine such that $\omega_g, \ldots, \omega_{2g-1}$ are without poles on Y. Define $\mathcal{A}_{\log,n}$ to be the bundle $K\langle T_0, \ldots, T_{2g-1}\rangle/I^{n+1} \otimes \mathcal{O}_Y$ with connection

$$\nabla v \otimes f = v \otimes df - \sum T_i v \otimes f\omega_i$$

Definition 28. We refer to the isomorphisms

$$A_{\log,n}(b,z) \simeq K\langle T_0, \ldots, T_{2g-1}\rangle/I^{n+1}$$

as the *affine trivialisation* of $\mathcal{A}_{\log,n}$ at z. Given a choice of differentials $\omega_0, \ldots, \omega_{2g-1}$ of the second kind without poles on $Y \subset X$, giving a basis of $H^1_{dR}(X)$, we will frequently identify basis of the abelianisation of the de Rham fundamental group dual to the ω_i with the free vector space generated by $T_0, \ldots, T_{2g-1}$. When there is no risk of confusion with its étale analogue, we shall write $H^1_{dR}(X)^*$ as V, so that the graded pieces of $A_{\log,n}$ are identified with $V^{\otimes i}$. Similarly, for an open affine Y we write $H^1_{\mathrm{dR}}(Y)^*$ as V_Y.

We now return to considering $\mathcal{A}_n = \mathcal{A}_n(Y)$. Kim's theorem gives an explicit description of the group of endomorphisms of the connections $\mathcal{A}_n^{\mathrm{dR}}$ as follows. Let $\mathrm{End}_{\mathrm{dR}}(\mathcal{A}_n)$ denote the algebra of endomorphisms of $\mathcal{A}_n$ in the category of flat connections. For $b \in X(K)$ let b^* denote the fibre functor at b.

Lemma 30. *For $f \in A_n$ we may construct a endomorphism $\gamma(f)$ of the connection $\mathcal{A}_n$ by sending $g \in H^0(Y, \mathcal{A}_n) \simeq A_n \otimes H^0(Y, \mathcal{O}_Y)$ to $g.f$.*

Proof. Clearly this defines a morphism of vector bundles, hence it suffices to check that the diagram

$$\begin{array}{ccc} \mathcal{A}_n & \xrightarrow{\gamma(f)} & \mathcal{A}_n \\ \downarrow \nabla & & \downarrow \nabla \\ \Omega^1 \otimes \mathcal{A}_n & \xrightarrow{1 \otimes \gamma(f)} & \Omega^1 \otimes \mathcal{A}_n \end{array}$$

commutes. As we are in the affine situation it is sufficient to check this on global sections. Let g be a global section in $\mathcal{A}_n$. Then the diagram commutes as

$$\nabla \circ \gamma(f)(g) = \gamma(f) \circ \nabla(g) = -\sum \omega_i \otimes T_i g f.$$

□

This lemma allows us to obtain the following corollary of Kim's theorem:

Corollary 4. *Let*

$$\Xi : \mathrm{End}_{dR}(\mathcal{A}_n) \to A_n$$

be the map sending an endomorphism α to $b^*(\alpha)(1)$. Then Ξ is a bijection, and hence every endomorphism of $\mathcal{A}_n$ is of the form $\gamma(f)$ for some f in A_n.

Proof. The fact that the map is bijective follows immediately from Kim's theorem, which says that there for any f in A_n there is a unique morphism of connections $\mathcal{A}_n \to \mathcal{A}_n$ sending 1 to f (via the isomorphism $b^*\mathcal{A}_n \simeq A_n$). By the previous Lemma this unique morphism is $\gamma(f)$. □

In the projective case we similarly associate to an element f of $K\langle T_0, \ldots, T_{2g-1}\rangle$ an endomorphism $\gamma(f)$ of the connection with log singularities $\mathcal{A}_{\log,n}$, and obtain an isomorphism

$$\mathrm{End}_{\mathrm{dR}}(\mathcal{A}_{\log,n}) \xrightarrow{\simeq} A_n$$

3.3.1 The Hodge filtration

The connection $\mathcal{A}_n$ is enriched with an additional structure of a *Hodge filtration* by sub-bundles $F^i\mathcal{A}_n$. Pulling these sub-bundles back gives a Hodge filtration on the $A_n(z_0, z)$, which is one half of the filtered ϕ-module structure utilised in previous sections. In all documented examples of explicit nonabelian Chabauty theory the isomorphism $A_n(z_0, z) \simeq \oplus A[i]$ has respected the Hodge filtration ([43],[24]), which reduces the description of the extension of the filtered ϕ-module structure of $A_n(z_0, z)$ to a description of the action of Frobenius. The fact that the vector space isomorphism respects the Hodge filtration for $\mathbb{P}^1 - \{0, 1, \infty\}$ is elementary, and in [43] the fact that it respects the Hodge filtration in the case $Y = E - O$, $n = 2$ is proved analytically using (archimedean) Hodge theory. In general, the trivialisation will *not* respect the Hodge filtration (see subsection 3.3.3 below), and hence in order to describe the localisation of $\Psi(z)$ explicitly a new method to compute the Hodge filtration is needed. In this subsection we recall the characterisation in [38] of the Hodge filtration on the de Rham fundamental group, and use it to produce an algorithmic description of the Hodge filtration. Hadian characterises the Hodge filtration by replacing connections on an affine curve with connections with log singularities on the projective curve, using the following theorem, which is a special case of Deligne's canonical extension theorem [29]:

Theorem 19 (Deligne)**.** *Let K be a field of characteristic zero. Let X be a smooth curve over K, and D a divisor of X. Let $\mathcal{C}^{dR}(X - D)$ denote the Tannakian category of flat connections on $X - D$. Let $\mathcal{C}^{dR}(X(\log[D]))$ denote the Tannakian category of vector bundles on X with connections with log singularities along D. Then the forgetful functor*

$$\mathcal{C}^{dR}(X(\log[D])) \to \mathcal{C}^{dR}(X - D)$$

is an equivalence of categories.

Definition 29. Given a flat connection $\mathcal{V}$ on $X - D$, we will denote by $\mathcal{V}^o$ an extension of this to a bundle with log connection on X.

We now describe the work of Hadian in characterising the Hodge filtration on the universal connection $\mathcal{A}_n$.

Definition 30. By a filtered connection $\mathcal{V} = (\mathcal{V}, \nabla, F^\bullet)$ we shall mean a vector bundle $\mathcal{V}$ together with a flat connection ∇ and a decreasing filtration

$$\mathcal{V} = F^m\mathcal{V} \supset F^{m+1}\mathcal{V} \supset \dots F^n\mathcal{V} = 0$$

(for some $m < n \in \mathbb{Z}$), satisfying the *Griffiths transversality* condition

$$\nabla(F^i\mathcal{V}) \subset \Omega^1 \otimes F^{i-1}\mathcal{V}$$

for all i. We similarly define a filtered connection with log singularities. We sometimes write a filtered connection as $(\mathcal{V}, F^\bullet)$ and sometimes simply as $\mathcal{V}$.

First Hadian proves:

Lemma 31. *Let $\mathcal{E}$ and $\mathcal{F}$ be filtered connections with logarithmic singularities along D. Then the group of isomorphism classes of extensions of $\mathcal{E}$ and $\mathcal{F}$ (in the category of filtered flat connections on X with logarithmic singularities along D) is isomorphic to the first hypercohomology group of the complex*

$$F^0(\mathcal{E}^* \otimes \mathcal{F}) \xrightarrow{\nabla} \Omega^1 \otimes F^{-1}(\mathcal{E}^* \otimes \mathcal{F})$$

where ∇ denotes the associated connection on the internal Hom bundle $\mathcal{E}^* \otimes \mathcal{F}$.

By computing these hypercohomology groups in the case $\mathcal{E} = \mathcal{A}_{n-1}$ and $\mathcal{F} = V_Y^{\otimes n} \otimes \mathcal{O}_X$, Hadian proves the following lemma:

Lemma 32 (Hadian [38], Lemma 2.2.6.)**.** *There exists a filtration $(F^i\mathcal{A}^o)_n$ of vector bundles such that*
(i): for all n the sequence of connections

$$0 \to \mathcal{O}_X \otimes V_Y^{\otimes n} \to \mathcal{A}_n^o \to \mathcal{A}_{n-1}^o \to 0$$

respects the filtrations, where $\mathcal{O}_X \otimes V_Y^{\otimes n}$ is given the filtration induced by the Hodge filtration on $V_Y^{\otimes n}$.
(ii): For all n, the filtration F^i satisfies Griffiths transversality, and hence gives $\mathcal{A}_n$ the structure of a filtered connection. for all i.
(iii): The filtration F^i is unique up to isomorphism of filtered connections.

Remark 6. It is easy to see that the analogous theorem for the bundle $\mathcal{A}_n$ on $X - D$ (when D is nonempty) is false: since the category of unipotent vector bundles on $X - D$ is trivial, there will be many ways to lift the Hodge filtration on the graded pieces and satisfy Griffiths transversality. Hence the content of computing the Hodge filtration on the $\mathcal{A}_n$ is contained in computing its canonical extension to X.

Remark 7. The statement of the Lemma is somewhat weaker than the statement given in [38]. In loc. cit. the author states that the filtration is unique (without allowing for automorphisms). This is deduced by inductively determining the from the computation that the map

$$\mathrm{Ext}^1_{\mathrm{dR}}(\mathcal{A}_{n-1}, V_Y^{\otimes n}) \to \mathrm{Ext}^1_{\mathrm{dR,fil}}((\mathcal{A}_{n-1}, F^\bullet \mathcal{A}_{n-1}), (V_Y^{\otimes n}, F^\bullet V_Y^{\otimes n}))$$

is injective. However, this only implies that there is a unique *extension class* of filtered connections $[(\mathcal{A}_n, F^\bullet)]$ corresponding to the extension class $[\mathcal{A}_n]$.

Corollary 5. *Let W be any filtered quotient of $V_Y^{\otimes n}$, and let $\mathcal{B}$ be the corresponding quotient of the connection $\mathcal{A}_n$. Hence the map*

$$\mathcal{A}_n \to \mathcal{A}_{n-1}$$

factors through

$$\mathcal{A}_n \to \mathcal{B}$$

and $\mathcal{B}$ is an extension

$$0 \to W \otimes \mathcal{O}_Y \to \mathcal{B}$$

Then there is a unique lift of the filtrations on $\mathcal{A}^o_{n-1}$ and $W \otimes \mathcal{O}_X$ to a filtered connection structure on $\mathcal{B}^o$ such that in the fibre at b, 1 lies in $b^* F^0 \mathcal{B}$.

Proof. The category of filtered K-vector spaces is semisimple, so W admits a filtered complement

$$V_Y^{\otimes n} \simeq W \oplus W'$$

Hence

$$\mathrm{Ext}^1_{\mathrm{dR,fil}}(V_Y^{\otimes n} \otimes \mathcal{O}_X, \mathcal{A}_{n-1}) \simeq \mathrm{Ext}^1_{\mathrm{dR,fil}}(W \otimes \mathcal{O}_X, \mathcal{A}_{n-1}) \oplus \mathrm{Ext}^1_{\mathrm{dR,fil}}(W' \otimes \mathcal{O}_X, \mathcal{A}_{n-1})$$

and

$$\mathrm{Ext}^1_{\mathrm{dR}}(V_Y^{\otimes n}\otimes \mathcal{O}_X,\mathcal{A}_{n-1})\simeq \mathrm{Ext}^1_{\mathrm{dR}}(W\otimes \mathcal{O}_X,\mathcal{A}_{n-1})\oplus \mathrm{Ext}^1_{\mathrm{dR}}(W'\otimes \mathcal{O}_X,\mathcal{A}_{n-1}).$$

Therefore uniqueness of the lift of the filtration on $\mathcal{A}_{n-1}$ to $\mathcal{A}_n$ given conditions on $b^*\mathcal{A}_n$ imply uniqueness of the lift of the filtration on $\mathcal{A}_{n-1}$ to $\mathcal{B}$ given conditions on $b^*\mathcal{B}$. □

To compute the Hodge filtration on $\mathcal{A}_n$ in the projective case we may compute the Hodge filtration on the universal connection of an open affine Y, and then take the quotient to get the Hodge filtration on the univeral connection on the projective curve X.

Corollary 6. *Let X be a smooth projective curve with open affine Y, and let $\omega_0,\ldots,\omega_{2g-1}$ be a set of differentials of the second kind forming a basis of $H^1_{dR}(X)$, such that all poles of the ω_i lie in $X-Y$. Let $\mathcal{A}_{\log,n}$ be the corresponding bundle defined above, so that the quotient map*

$$\mathcal{A}_n(Y)\to\mathcal{A}_n(X)$$

factors through $\mathcal{A}_{\log,n}$. Then $\mathcal{A}_{\log,n}$ has a filtered connection structure uniquely determined by the conditions

- *The exact sequence*

  $$0\to V^{\otimes n}\otimes \mathcal{O}_X\to \mathcal{A}^o_{\log,n}\to \mathcal{A}^o_{\log,n-1}\to 0$$

  is an exact sequence of filtered connections, where the filtration on $V^{\otimes n}\otimes\mathcal{O}_X$ is induced by the Hodge filtration on $H^1_{dR}(X)$.

- *with respect to the affine trivialisation*

  $$b^*\mathcal{A}_{\log,n}\simeq K\langle T_0,\ldots,T_{2g-1}\rangle/I^{n+1}$$

  the element $1\in b^*\mathcal{A}_n$ lies in $b^*F^0\mathcal{A}_n$.

Proof. Extend $\omega_0, \dots, \omega_{2g-1}$ to a basis $\omega_0, \dots, \omega_{2g+d-2}$ of $H^1_{\mathrm{dR}}(Y)$ and let

$$\mathcal{A}_n(Y) \simeq K\langle T_0, \dots, T_{2g+d-2}\rangle/(T_0, \dots, T_{2g+d-2})^{n+1} \otimes \mathcal{O}_Y$$

denote the corresponding universal connection on Y. Then $\mathcal{A}_{\log,n}$ is naturally a quotient of $\mathcal{A}_n(Y)$, with the quotient map being induced by the projection

$$\tau : K\langle T_0, \dots, T_{2g+d-2}\rangle \to K\langle T_0, \dots, T_{2g-1}\rangle$$

sending all T_i to zero for $i \geq 2g$. Let

$$\mathcal{B}_n := K\langle T_0, \dots, T_{2g+d-2}\rangle/((T_0, \dots, T_{2g+d-2})^{n+1}, J_n)$$

where J_n is defined to be the kernel of the composite map

$$K\langle T_0, \dots, T_{2g+d-2}\rangle \xrightarrow{\tau} K\langle T_0, \dots, T_{2g-1}\rangle \to K\langle T_0, \dots, T_{2g-1}\rangle/((T_0, \dots, T_{2g-1})^{n+1}, J_n)$$

Then $\mathcal{B}_n$ is naturally a quotient connection of $\mathcal{A}_n(Y)$, and sits in an exact sequence

$$0 \to \ker(\mathcal{A}_{\log,n} \to \mathcal{A}_{\log,n-1}) \to \mathcal{B}_n \to \mathcal{A}_{n-1}(Y) \to 0$$

Another way to characterise $\mathcal{B}_n$ is as

$$\mathcal{B}_n := \ker(\mathcal{A}_{\log,n} \oplus \mathcal{A}_{n-1}(Y) \to \mathcal{A}_{\log,n-1})$$

where the the map is the difference of the two projections

$$\mathcal{A}_{\log,n} \to \mathcal{A}_{\log,n-1}$$

and

$$\mathcal{A}_{n-1}(Y) \to \mathcal{A}_{\log,n-1}(Y).$$

So $\mathcal{B}_n$ is the fibre product of the connections $\mathcal{A}_{\log,n}$ and $\mathcal{A}_{n-1}(Y)$ over $\mathcal{A}_{\log,n-1}$. It follows that any filtrations on $\mathcal{A}_{\log,n}$ and $\mathcal{A}_{n-1}(Y)$ which agree on $\mathcal{A}_{\log,n-1}$ define a filtration on $\mathcal{B}_n$. Hence different lifts of the Hodge filtration from $\mathcal{A}_{\log,n-1}$ to $\mathcal{A}_{\log,n}$ induce different lifts of the Hodge filtration from $\mathcal{A}_{n-1}(Y)$ to $\mathcal{B}_n$. The result now follows from Corollary 5 . □

3.3.2 Describing the Hodge filtration

We now apply the results of Hadian to describe an algorithm for computing the Hodge filtration given the explicit description of the connection ∇ in terms of differentials of the second kind giving a basis of de Rham cohomology. By the previous section the Hodge filtration is uniquely determined by the exact sequence

$$0 \to V^{\otimes n} \otimes \mathcal{O}_X \to \mathcal{A}_{\log,n} \to \mathcal{A}_{\log,n-1} \to 0.$$

The following proposition is essentially an immediate corollary of Hadian's theorem, and will be useful in computing the Hodge filtration.

Proposition 6. *The Hodge filtration on $\mathcal{A}^o_{\log,n}$ is the unique lift of the filtration on $\mathcal{A}^o_{\log,n-1}$ and $V^{\otimes n} \otimes \mathcal{O}_X$ to a filtered connection structure on $\mathcal{A}^o_{\log,n}$ such that*

- *The sequence*

$$0 \to V^{\otimes n} \otimes \mathcal{O}_X \to \mathcal{A}^o_{\log,n} \to \mathcal{A}^o_{\log,n-1} \to 0$$

  is an exact sequence of filtered connections.

- *With respect to the affine trivialisation*

$$\mathcal{A}_{\log,n} \simeq \oplus_{i=0}^n V^{\otimes n} \otimes \mathcal{O}_Y$$

  described above, the element $1 \in A_{\log,n}(b) = b^*\mathcal{A}_{\log,n}$ lies in $F^0 A_{\log,n}(b) := b^* F^0 \mathcal{A}_{\log,n}$.

Proof. We know by Kim's theorem (Theorem 18 above) that via the isomorphism $b^*\mathcal{A}_{\log,n} \simeq K\langle T_0, \ldots, T_{2g-1}\rangle / I^{n+1}$ the element 1 in $K\langle T_0, \ldots, T_{2g-1}\rangle / I^{n+1}$ corresponds to the identity element of the quotient of the enveloping algebra. In particular it lies in $F^0 A_{\log,n}(b)$, so we know that the filtration on $\mathcal{A}_{\log,n}$ satisfies the property in the statement of the Proposition. Now suppose $\widetilde{F}^\bullet$ is any filtration on $(\mathcal{A}_{\log,n}, F^\bullet)$ which lifts the filtrations on $\mathcal{A}_{\log,n-1}$ on $V^{\otimes n} \otimes \mathcal{O}_Y$ with the property that $1 \in A_{\log,n}(b)$ lies in $b^*\widetilde{F}^0\mathcal{A}_{\log,n}$. Then by Hadian's theorem there exists an isomorphism of filtered connections

$$(\mathcal{A}^o_{\log,n}, F^\bullet) \to (\mathcal{A}^o_{\log,n}, \widetilde{F}^\bullet)$$

which is the identity of $V^{\otimes n} \otimes \mathcal{O}_Y$ and the identity on $\mathcal{A}_{\log,n-1}$. On the other hand, by Corollary 4, since any automorphism of the connection $\mathcal{A}_{\log,n}$ must be of the form $\gamma(f)$ for some f in $A_{\log,n}(b)$. Since it is identity on $A_{\log,n-1}(b)$ f must be equal to $1+w$ for some w in I^n/I^{n+1}. Since 1 lies in $b^*F^0\mathcal{A}_{\log,n}$ and in $b^*\widetilde{F}^0\mathcal{A}_{\log,n}$ w must lie in $F^0V^{\otimes n}$. □

We will describe an inductive process for computing the Hodge filtration. We recall a couple of standard facts whose proof we include for completeness.

The first is the standard description for how a connection ∇ changes under gauge transformation:

Lemma 33. *Let $(\mathcal{O}^{\oplus n}, \nabla)$ be a flat connection on a scheme Z. Let $e_i : \mathcal{O} \hookrightarrow \mathcal{O}_n$ $(1 \leq i \leq n)$ be the natural basis of $\mathcal{O}^{\oplus n}$. Suppose that with respect to the the trivialisation (e_i) the connection ∇ is given by*

$$\nabla = d + \Omega$$

for $\Omega \in H^0(Y, \Omega^1) \otimes \mathrm{Mat}_n(K)$. Suppose

$$\Psi : \mathcal{O}^{\oplus n} \to \mathcal{O}^{\oplus n}$$

is an automorphism of the vector bundle $\mathcal{O}^{\oplus n}$. Then with respect to the basis $\Psi^{-1}e_i$, the connection ∇ is given by

$$d + \Psi^{-1}\Omega\Psi + \Psi^{-1}d\Psi.$$

Proof. Describing the connection ∇ with respect to the trivialisation $\Psi^{-1}e_i$ amounts to computing the top horizontal map in the commutative diagram

$$\begin{array}{ccc} \mathcal{O}^{\oplus n} & \longrightarrow & \Omega^1 \otimes \mathcal{O}^{\oplus n} \\ \downarrow \Psi & & \downarrow 1 \otimes \Psi \\ \mathcal{O}^{\oplus n} & \xrightarrow{d+\Omega} & \Omega^1 \otimes \mathcal{O}^{\oplus n}. \end{array}$$

Hence the lemma follows from the fact that $d \circ \Psi(f) = (1 \otimes \Psi)(d(f)) + (d\Psi)(f)$. □

The second fact will be used to guarantee uniqueness of lifts of sub-bundles:

Lemma 34. *Let $\omega_0, \dots, \omega_{2g-1}$ be differentials of the second kind on X, without poles on an affine open Y, forming a basis of $H^1_{dR}(X)$. As before suppose that $\omega_0, \dots, \omega_{g-1}$ are in $H^0(X, \Omega^1)$. For each $x \in X - Y$, let t_x be a parameter, and let $f_{i,x} \in K(\!(t_x)\!)$ (for $g \leq i < 2g$) be such that the specialisation of ω_i to* $\mathrm{Spec}\, K(\!(t_x)\!)$ *equals $df_{i,x}$.*

Suppose there exists a function $g \in H^0(Y, \mathcal{O}_Y)$, and constants $\mu_1, \dots, \mu_r$ in K such that, at all points x in $X - Y$,

$$g - \sum \mu_i f_{i,x} \in K[\![t_x]\!]$$

Then g is constant and for all $g \leq i < 2g$, $\mu_i = 0$.

Proof. The differential

$$dg - \sum_{g \leq i < 2g} \mu_i \omega_i$$

has no poles on X, hence defines an element of $H^0(X, \Omega^1)$, say

$$dg - \sum_{g \leq i < 2g} \mu_i \omega_i = \sum_{0 \leq i < g} \lambda_i \omega_i$$

Since the ω_i form a basis of de Rham cohomology the result follows. □

We now describe an inductive process for computing the Hodge filtration on $A_n(b, z)$. Suppose we have a trivialised vector bundle $\mathcal{V} \simeq \mathcal{O}^{\oplus n}$ on $Y = X - D$ with a connection

$$\nabla : \mathcal{V} \to \mathcal{V} \otimes \Omega^1$$

One then proceeds as follows:

(i): At each $x \in D$, find a parameter t_x and write ω_i as an element of $K(\!(t_x)\!)dt_x$.

(ii): Compute Deligne's canonical extension of $\mathcal{A}_n$ to a bundle $\mathcal{A}_n^o$ with connection (possibly with log singularities) on X: Let i_x be the morphism

$$i_x : \mathrm{Spec}(K(\!(t_x)\!)) \to \mathrm{Spec}(K[\![t_x]\!])$$

and j_x the morphism

$$j_x : \mathrm{Spec}(K(\!(t_x)\!)) \hookrightarrow Y$$

To extend $(\mathcal{A}_n, \nabla)$ to a log connection on X we need to find charts and transition maps for $(\mathcal{A}_n^o, \nabla^o)$ at all x in D. Hence it is sufficient to define, for all x in D,

- A connection $(\mathcal{V}^\infty, \nabla^\infty)$ on $\mathrm{Spec}(K[\![t]\!])$ with log singularities at zero
- A unipotent isomorphism $j^*(\mathcal{V}, \nabla) \simeq i^*(\mathcal{V}^\infty, \nabla^\infty)$ of connections on $\mathrm{Spec}(K(\!(t)\!))$ (in the sense above).

This problem amounts to a question of finding a *gauge transformation* of $(\mathcal{A}_{\log,n}, \nabla)$ which removes all its poles of order larger than 2 at x. This is described explicitly by the Lemma 33 above.

(iii): To produce a Hodge filtration, we seek sub-bundles $F^i\mathcal{A}_{\log,n}$ on $X - D$ and $F^i A_{\log,n}[\![t_x]\!]$ on $\mathrm{Spec}(K[\![t_x]\!])$ each satisfying Griffiths transversality and agreeing with the Hodge filtration on graded pieces, and which agree on the $\mathrm{Spec}(K(\!(t_x)\!))$. These may be inductively computed using Hadian's Lemma, as the explicit description of the extension of $\mathcal{A}_{\log,n}$ to $\mathcal{A}^o_{\log,n}$ renders explicit the condition of the sub-bundles $F^i\mathcal{A}_{\log,n}$ of $\mathcal{A}_{\log,n}$ extending to sub-bundles $F^i\mathcal{A}^o_{\log,n}$ of $\mathcal{A}^o_{\log,n}$.

Example 4. In this example we determine the Hodge filtration on $\mathcal{A}_1$ $(= \mathcal{A}_{\log,1})$. In this case the Griffiths transversality condition is empty. We have to determine an extension of the Hodge filtration on $V \otimes \mathcal{O}_X$ to a filtration on $\mathcal{A}^o_1$, or a equivalently a lift of $\mathcal{A}_0$ to a sub-bundle of $\mathcal{A}^o_1/(F^0V \otimes \mathcal{O}_X)$. By the description of the universal connection given above, the affine trivialisation of $\mathcal{A}^o_1/(F^0V \otimes \mathcal{O}_X)$ extends to a trivialisation of $\mathcal{A}^o_1/F^0$ at infinity, hence the bundle $\mathcal{A}^o_1/(F^0V \otimes \mathcal{O}_X)$ is trivial.

Example 5. In this example we sketch how the process works for the bundles $F^i\mathcal{A}_{\log,2}$. First consider the problem of lifting $F^0\mathcal{A}_1$ to a sub-bundle of $\mathcal{A}_{\log,2}$. Since $F^0V^{\otimes 2} \otimes \mathcal{O}_Y$ will be a sub-bundle of $F^0\mathcal{A}_{\log,2}$ it is enough to consider the problem of lifting $F^0\mathcal{A}_1$ to $\mathcal{A}_{\log,2}/F^0V^{\otimes 2} \otimes \mathcal{O}_Y$. The constraint will come from the fact that this extends to a lift of $F^0\mathcal{A}^o_1$ to $\mathcal{A}^o_{\log,2}/F^0V^{\otimes 2} \otimes \mathcal{O}_X$. At each missing point x let t_x be a parameter. Suppose that the charts defining the bundle $\mathcal{A}_{\log,2}$ are given at x by

$$\psi_x : A_2 \otimes K(\!(t_x)\!) \xrightarrow{\simeq} A_2 \otimes K(\!(t_x)\!)$$

such that

$$\psi_x(1) = 1 + \sum f_i T_i + \sum g_{ij} \overline{T_i \otimes T_j}$$

$$\psi_x(T_k) = T_k + \sum h_{ijk} \overline{T_i \otimes T_j}$$

for some f_i, g_{ij}, h_{ijk} in $K(\!(t_x)\!)$. The f_i have the property that $\omega_i - f_i \in K[\![t_x]\!]dt_x$. The h_{ijk} can be taken to be $\delta_{jk} f_i$. By the previous example, we know that $F^0\mathcal{A}_1$ has a basis of sections $1, T_g, \ldots, T_{2g-1}$. Suppose these lift to sections

$$1 + \sum a_{ij} T_i \otimes T_j, T_k + \sum b_{ijk} T_i \otimes T_j$$

of $F^0\mathcal{A}_{\log,2}$. Let x be a point in $X - Y$. Then with respect to the chart at x, the sections above are given as

$$1 + \sum f_i T_i + \sum (a_{ij} + g_{ij}) T_i \otimes T_j, T_k + \sum (b_{ijk} + h_{ijk}) T_i \otimes T_j$$

We know that the $K(\!(t_x)\!)$-vector space generated by these elements is of the form $M \otimes_{K[\![t_x]\!]} K(\!(t_x)\!)$ for some free $K[\![t_x]\!]$ module M. This must then be generated by the $T_k + \sum (b_{ijk} + h_{ijk}) T_i \otimes T_j$ and by $1 + \sum (a_{ij} + g_{ij} - \sum_k (b_{ijk} + h_{ijk}) f_k) T_i \otimes T_j$. Hence $b_{ijk} + h_{ijk}$ lies in $K[\![t_x]\!]$ for all x. Hence b_{ijk} is constant. The fact that the a_{ij} and the b_{ijk} are uniquely determined is now a trivial application of Lemma 34 : a different choice of global functions a_{ij} and constants b_{ijk} gives the equation

$$a_{ij} - \widetilde{a}_{ij} = \sum (b_{ijk} - \widetilde{b}_{ijk}) f_k$$

By Lemma 34, $b_{ijk} = \widetilde{b}_{ijk}$ and $a_{ij} - \widetilde{a}_{ij}$ is constant. However since in the fibre at b we know 1 lies in $b^* F^0 \mathcal{A}_{\log,2}$, if both lifts define Hodge filtrations on $\mathcal{A}_{\log,2}$ we must have $a_{ij}(b) = \widetilde{a}_{ij}(b) = 0$.

Definition 31. For $0 \leq i, j < 2g$ such that the minimum of i and j is less than j, define $p_{ij} \in H^0(Y, \mathcal{O}_Y)$ by the property that $1 + \sum p_{ij} T_i \otimes T_j$ defines an element of $H^0(Y, F^0\mathcal{A}_{\log,2})$.

3.3.3 Example: Hyperelliptic curves

In this subsection we give an example of the universal connection, and of the above process for the connection $\mathcal{A}_{\log,2}$. The curve we take is a genus 2 curve with Jacobian isogenous to $E \times E$, as considered in the previous chapter. This computation will be used in the next chapter to obtain an explicit formula for $X(\mathbb{Q}_p) \cap H^1_{f,\mathcal{L}}(G_T, U)$. The computation of the Hodge filtration at depth 2 for a general hyperelliptic curve proceeds similarly.

Let X be a hyperelliptic curve of the form

$$y^2 = x^6 + ax^4 + ax^2 + 1$$

To calculate the gauge transformation describing the Hodge filtration, we need to describe X and the ω_i at infinity.

At infinity X is again given by

$$v^2 = u^6 + au^4 + au^2 + 1$$

with the gluing given by

$$u = x^{-1}; v = yx^{-3}$$

We may define ∞^+ to be the point $(u, v) = (0, 1)$ and ∞^- to be the point $(u, v) = (0, -1)$.

(i): We now describe the rational differentials ω_i at $\infty^\pm$.

At ∞^+ : here u is a local parameter, and

$$\begin{aligned}
v^{-1} &\equiv 1 - \frac{1}{2}au^2 - \frac{1}{2}au^4 + \frac{3}{8}a^2u^4 \mod u^6 \\
\omega_0 &\equiv [-\frac{1}{2}u + \frac{1}{4}au^3]du \mod u^5 du, \\
\omega_1 &\equiv [-\frac{1}{2} + \frac{1}{4}au^2]du \mod u^4 du, \\
\omega_2 &\equiv [-u^{-3} + (\frac{1}{2}a - \frac{5}{8}a^2)u]du \mod u^3, \qquad (3.4) \\
\omega_3 &\equiv [-\frac{1}{2}u^{-2} + \frac{1}{4}a]du \mod u^2. \qquad (3.5)
\end{aligned}$$

At ∞^- : the formulae are identical, but with a sign change:

$$\begin{aligned}
v^{-1} &\equiv -1 + \frac{1}{2}au^2 + \frac{1}{2}au^4 - \frac{3}{8}a^2u^4 \mod u^6 \\
\omega_0 &\equiv [\frac{1}{2}u - \frac{1}{4}au^3]du \mod u^5 du, \\
\omega_1 &\equiv [\frac{1}{2} - \frac{1}{4}au^2]du \mod u^4 du, \\
\omega_2 &\equiv [u^{-3} - (\frac{1}{2}a - \frac{5}{8}a^2)u]du \mod u^3, \qquad (3.6) \\
\omega_3 &\equiv [\frac{1}{2}u^{-2} - \frac{1}{4}a]du \mod u^2. \qquad (3.7)
\end{aligned}$$

(ii): We now compute the canonical extension $\mathcal{A}^o_{\log,2}$.

That is, we want to find a gluing morphism

$$\Psi_+ : K\langle T_0,\dots,T_3 \otimes K((u)) \xrightarrow{\simeq} K\langle T_0,\dots,T_3\rangle \otimes K((u))$$

$$\mu+\sum \mu_i T_i+\sum \mu_{ij}T_i\otimes T_j \mapsto \mu_0+\sum(\mu_i+f_i^+\mu_0)T_i+\sum(\mu_{ij}+\mu_0 g_{ij}^+ +\mu_k h_{ijk}^+)T_i\otimes T_j$$

near ∞^+ (and similarly Ψ_- near ∞^-, with power series $f_i^-, g_{ij}^-, h_{ijk}^-$). such that the connection ∇ on $\mathcal{A}_{\log,2}$ extends to a connection with log singularities on the bundle with trivialisations $K\langle T_0,\dots,T_3\rangle/I^3\otimes\mathcal{O}_U$ for $U=Y,\mathrm{Spec}(\widehat{\mathcal{O}}_{\infty^+}),\mathrm{Spec}(\widehat{\mathcal{O}}_{\infty^-})$ and gluing morphisms Ψ_+ and Ψ_-. Recall that we have already computed the f_i :

$$f_0^+=f_1^+=0, f_2^+=\frac{1}{2}u^{-2}, f_3^+=\frac{1}{2}u^{-1}.$$

Given the description of the ω_i at ∞^-, we may take $f_i^-=-df_i^+$. To solve for g_{ij}^+ and h_{ijk}^+ we need to solve the equation

$$\Psi_+^{-1}\Omega\Psi_+ + \Psi_+^{-1}d\Psi_+ \equiv 0 \mod u^{-1}du \tag{3.8}$$

in $\mathrm{End}\, K\langle T_0,\dots,T_3\rangle\otimes K((u))$, and similarly for Ψ_-. We now work this out in detail for Ψ_+. First note that Ψ_+^{-1} sends T_k to $T_k-\sum h_{ijk}^+ T_i\otimes T_j$. Hence (3.8) may be written more explicitly as

$$\begin{aligned}&-\sum\omega_i T_i+\sum_{i,j}(-\omega_i f_j^+ +\sum_k h_{ijk}^+\omega_k)T_i\otimes T_j\\&-\sum_{i,j,k}h_{ijk}^+ df_k^+ T_i\otimes T_j+\sum df_i^+T_i+\sum dg_{ij}^+ T_i\otimes T_j\equiv 0 \mod u^{-1}du\end{aligned}$$

(taking the image of 1) and for $0\le k\le 3$

$$-\sum_i \omega_i T_i\otimes T_k+\sum_{i,j} dh_{ijk}^+ T_i\otimes T_j\equiv 0 \mod u^{-1}du$$

(taking the image of T_k). The latter equation implies that for all i,j,k

$$dh_{ijk}^+\equiv df_i^+\delta_{jk}\equiv 0 \mod u^{-1}du$$

where δ_{jk} denotes the Kronecker delta. We take

$$h_{ijk}^+ = f_i^+\delta_{jk}$$

For the first equation we have already worked out the conditions for the T_i coefficients and hence it suffices to consider $T_i \otimes T_j$ coefficients, which gives

$$-\omega_i f_j^+ + dg_{ij}^+ + \sum_k h_{ijk}^+(\omega_k + df_k^+) \equiv 0 \mod u^{-1}du$$

Using the description of the f_i^+ and ω_j above this can be rewritten as

$$-\omega_i f_j^+ + dg_{ij}^+ + f_i^+(\omega_j - df_j^+) \equiv 0 \mod u^{-1}du$$

Hence

$$(dg_{ij}^+) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{4}u^{-2} \\ 0 & \frac{1}{4}u^{-2} & -\frac{1}{2}u^{-5} & -\frac{1}{2}u^{-4} - \frac{a}{8}u^{-2} \\ 0 & 0 & -\frac{1}{4}u^{-4} + \frac{a}{8}u^{-2} & -\frac{1}{4}u^{-3} \end{pmatrix} du$$

So

$$(g_{ij}^+) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{4}u^{-1} \\ 0 & -\frac{1}{4}u^{-1} & \frac{1}{8}u^{-4} & \frac{1}{6}u^{-3} + \frac{a}{8}u^{-1} \\ 0 & 0 & \frac{1}{12}u^{-3} - \frac{a}{8}u^{-1} & \frac{1}{8}u^{-2} \end{pmatrix}$$

At ∞^- we take

$$g_{ij} = g_{ij}^-$$

(unlike at depth 1 where $df_i^+ = -df_i^-$). Having computed the charts, we now compute the Hodge filtration. First we try to lift $F^0\mathcal{A}_1^o$ to $F^0\mathcal{A}_{\log,2}^o/(F^0V^{\otimes 2})\otimes\mathcal{O}_X$. Unlike with $\mathcal{A}_1$, extending $F^0\mathcal{A}_1$ to a sub-bundle of $\mathcal{A}_{\log,2}/F^0V^{\otimes 2}\otimes\mathcal{O}_Y$ via the affine trivialisation

$$\mathcal{A}_{\log,2} \simeq \mathcal{A}_1 \oplus V^{\otimes 2} \otimes \mathcal{O}_Y$$

will *not* extend to a sub-bundle of X as the functions g_{12}^+ and g_{21}^+ are nonzero. However, the free $\mathcal{O}_Y$ sub-module of $\mathcal{A}_{\log,2}/F^0V^{\otimes 2}\otimes\mathcal{O}_Y$ generated by

$$1 + \frac{1}{4}x(T_1 \otimes T_2 - T_2 \otimes T_1), T_2, T_3$$

does extend to a sub-bundle of $\mathcal{A}_{\log,2}^o/F^0V^{\otimes 2}\otimes\mathcal{O}_X$ (recall $u = x^{-1}$). Since we know that in the fibre at the basepoint b, 1 lies in $F^0A_{\log,2}(b)$, $F^0\mathcal{A}_{\log,2}/(F^0V^{\otimes 2}\otimes\mathcal{O}_Y)$ is generated by

$$1 + \frac{1}{4}(x - x(b))(T_1 \otimes T_2 - T_2 \otimes T_1), T_2, T_3.$$

A priori we can take any lift of the section T_2 and T_3 to sections of $\mathcal{A}_{\log,2}/(F^0V^{\otimes 2}\otimes \mathcal{O}_Y)$. Having lifted F^0 it remains to define $F^{-1}\mathcal{A}_{\log,2}$. By Griffiths tranversality, we know that

$$\nabla(1) = -\sum \omega_i \otimes T_i$$

is an element of $H^0(Y, \Omega^1 \otimes F^{-1}\mathcal{A}_{\log,2})$.

(iii): Finally, we compute the Hodge filtration on $\mathcal{A}_2$. We first compute $F^0\mathcal{A}_2$ and then explain how $F^{-1}\mathcal{A}_{\log,2}$ is determined by Griffiths transversality. By Example 4 we know that the Hodge filtration on $\mathcal{A}_1$ is described by

$$F^0\mathcal{A}_1 = \mathcal{O}_Y.1 \oplus \mathcal{O}_Y.T_2 \oplus \mathcal{O}_Y.T_3$$

As explained in Example 5 it will be enough to compute a lift of $F^0\mathcal{A}_1$ to a rank 3 sub-bundle of $\mathcal{A}_{\log,2}/F^0V^{\otimes 2}\otimes \mathcal{O}_Y$. Suppose the sections $1, T_2$ and T_3 lift to sections $1+\sum a_{ij}T_i \otimes T_j$ and $T_k + \sum b_{ijk}T_i \otimes T_j$ of $F^0\mathcal{A}_{\log,2}/F^0V^{\otimes 2}\otimes \mathcal{O}_Y$ for some $a_{ij}, b_{ijk} \in H^0(Y, \mathcal{O}_Y)$. Then, pulling back to the field of fractions $K(\!(u)\!)$ of the formal completion of the local ring at ∞^+, these sections are given, with respect to the chart at ∞^+ , by

$$1+\sum f_i^+ T_i + \sum (g_{ij}^+ + a_{ij})T_i \otimes T_j,$$

The constraint on the a_{ij} and b_{ijk} is that this $K(\!(u)\!)$ vector space should come from a $K[\![u]\!]$ module - i.e. there should exist a $K[\![u]\!]$ module M such that $M \otimes K(\!(u)\!)$ is the vector space generated by

$$1+\sum f_i^+ T_i + \sum (g_{ij}^+ + a_{ij})T_i \otimes T_j,$$

and the $T_k + \sum (h_{ijk} + b_{ijk})T_i \otimes T_j$. First note that this implies the b_{ijk} are elements of $H^0(Y, \mathcal{O}_Y)$ with no pole at ∞^+ and ∞^-, and hence are constant functions. The remaining condition is that

$$a_{ij} + g_{ij}^+ - f_2^+ b_{ij2} - f_3^+ b_{ij3}$$

at ∞^+ and

$$a_{ij} + g_{ij}^- - f_2^- b_{ij2} - f_3^- b_{ij3}$$

at ∞^-. We claim that all b_{ijk} must be zero. To see this first note that taking all b_{ijk} equal to zero and a_{ij} equal to $\frac{1}{4}(x - x(b))$ when $(i,j) = (1,2)$ or $(2,1)$ and zero otherwise does give a lift of F^0. Then note that this lift satisfies the property that $1 \in A_2 \simeq b^* A_{\log,2}(b)$ lies in $F^0 A_{\log,2}(b)$. Arguing as in example 5 we see that this is the unique lift satisfying this property.

Also as in example 5 Griffiths tranversality now uniquely characterises $F^{-1}\mathcal{A}_{\log,2}$.

3.3.3.1 A quotient of $\mathcal{A}_2(X)$

In chapter 4 we will need to work with a quotient of $\mathcal{A}_2(X)$.

Let E be the elliptic curve

$$y^2 = x^3 + ax^2 + ax + 1$$

Define covers

$$f_1 : X \to E; \quad (x, y) \mapsto (x^2, y)$$
$$f_2 : X \to E; \quad (x, y) \mapsto (x^{-2}, yx^{-3})$$

Then via the maps f_1 and f_2,

$$H^1_{\mathrm{dR}}(X) \simeq H^1_{\mathrm{dR}}(E)^{\oplus 2}.$$

Hence we have a quotient $\mathcal{A}$ which is in an exact sequence

$$0 \to \mathrm{Sym}^2(H^1_{\mathrm{dR}}(E)^*) \otimes \mathcal{O}_X \to \mathcal{A}^o \to \mathcal{A}^o_1 \to 0$$

Above we describe the ω_i giving a basis of $H^1_{\mathrm{dR}}(X)$. We now describe $\mathrm{Sym}^2 H^1_{\mathrm{dR}}(E)$ in terms of the ω_i:

Lemma 35. *The image of* $\mathrm{Sym}^2 H^1_{dR}(E)$ *in* $\wedge^2 H^1_{dR}(X)$ *is spanned by the classes of the differentials*

$$\omega_0 \wedge \omega_1, \omega_2 \wedge \omega_3, \omega_0 \wedge \omega_3 + \omega_1 \wedge \omega_2.$$

Proof. The image of

$$f_1^* : H^1_{dR}(E) \to H^1_{dR}(X)$$

is spanned by the differentials ω_1 and ω_3, and the automorphism

$$g : (x, y) \mapsto (x^{-1}, yx^{-3})$$

sends $x^i\omega$ to $-x^{1-i}\omega$, hence

$$x\omega \mapsto -\omega, x^3\omega \mapsto x^{-2}\omega$$

In $H^1_{\mathrm{dR}}(Y)$ the classes of the differentials $[x^i\omega]$ satisfy the relation

$$(i+3)[x^{5+i}\omega] + a(i+2)[x^{3+i}\omega] + a(i+1)[x^{1+i}\omega] + i[x^{i-1}\omega] = 0.$$

so on the level of cohomology

$$[x^3\omega] \mapsto a[x^2\omega] - 2[x^4\omega]$$

as required. □

Hence the previous section implies the following proposition which will be used in chapter 4:

Proposition 7. $F^0\mathcal{A}$ *is spanned by*

$$1 \pm \frac{1}{2}(x(z) - x(b))(T_1 \wedge T_2 + T_0 \wedge T_3),$$

together with T_i *and* $\overline{T_i \wedge T_j}$ *for* $i, j > 1$.

3.4 The crystalline fundamental group

In this section we review the definition of the category of overconvergent isocrystals on the special fibre $Y_{\mathbb{F}_p}$ of Y at p, as constructed by Berthelot [12]. This was used by Chiarellotto and Le Stum in [19]] to define a rigid fundamental group, which they show is isomorphic to the de Rham fundamental group. Unlike the de Rham fundamental group, it has a natural action of Frobenius, and this gives the spaces $A_n^{dR}(b, z)$ the structure of filtered ϕ-modules (see the next section). Berthelot's notion of the realization of an isocrystal is based around choosing an additional structure on $Y_{\mathbb{F}_p}$:

Definition 32. A *rigid triple* over $\mathbb{Z}_p$ is a triple $T = (X, Y, P)$, where P is a formal scheme over $\mathrm{Spf}(\mathbb{Z}_p)$, X is a closed $\mathbb{F}_p$-subscheme, and $Y \subset X$ is an open $\mathbb{F}_p$-subscheme of X, such that P is smooth in a neighbourhood of Y.

As the present work is concerned with the case where we are given a smooth curve over $\mathbb{Z}_p$, our rigid triples will be chosen to be of the form $(X_{\mathbb{F}_p}, Y_{\mathbb{F}_p}, \mathfrak{X})$ where $X_{\mathbb{F}_p}, Y_{\mathbb{F}_p}$ are the special fibres of smooth curves $\mathcal{X}$, $\mathcal{Y}$ over $\mathbb{Z}_p$ and $\mathfrak{X}$ is the corresponding formal scheme over $\mathrm{Spf}(\mathbb{Z}_p)$. Let $X_{\mathbb{Q}_p}$ and $Y_{\mathbb{Q}_p}$ denote the generic fibres, $\mathfrak{Y}$ the formal scheme corresponding to $\mathcal{Y}$ and $X^{\mathrm{an}}_{\mathbb{Q}_p}$ and $Y^{\mathrm{an}}_{\mathbb{Q}_p}$ the Raynaud generic fibres.

Definition 33. For $\mathcal{X}$ as above, and z a $\mathbb{Q}_p$-point, denote by $\mathrm{sp}(z)$ the specialisation to $X(\mathbb{F}_p)$. For any subscheme $Z \subset X_{\mathbb{F}_p}$, let $]Z[\subset X^{\mathrm{an}}_{\mathbb{Q}_p}$ denote the fibre of Z under the specialisation map. Define the functor $j^\dagger$ from the category of sheaves on $Y^{\mathrm{an}}_{\mathbb{Q}_p}$ to itself sending M to

$$\varinjlim_{U} M(U)$$

where the limit is over all strict neighbourhoods U of $]Y_{\mathbb{F}_p}[$ in X.

Definition 34. An isocrystal on a rigid triple T is a locally free $j^\dagger \mathcal{O}_{P^{\mathrm{an}}_{\mathbb{Q}_p}}$-module M on $Y^{\mathrm{an}}_{\mathbb{Q}_p}$ together with a connection

$$\nabla : M \to M \otimes \Omega^1_{\mathfrak{X}}.$$

An isocrystal $\mathcal{F}$ is said to be *overconvergent* if it comes from a connection on U for some strict neighbourhood $U \subset]Y[$.

The trivial isocrystal is $(j^\dagger \mathcal{O}, d)$. Clearly, this isocrystal is overconvergent. Say an isocrystal $\mathcal{M}$ is *unipotent* if it admits a filtration by sub-isocrystals

$$\mathcal{M} = \mathcal{M}_0 \supset \ldots \supset \mathcal{M}_n = 0$$

with $\mathcal{M}_i/\mathcal{M}_{i+1} \simeq (j^\dagger \mathcal{O}, d)$ for all i. In [19], it is shown that a unipotent isocrystal is automatically overconvergent:

Theorem 20 (Chiarellotto, Le Stum [19])**.** *Let $\mathcal{M}_1$, $\mathcal{M}_2$ be overconvergent isocrystals. Let*

$$0 \to \mathcal{M}_2 \to \mathcal{M}_3 \to \mathcal{M}_1 \to 0$$

be a short exact sequence of isocrystals. Then $\mathcal{M}_3$ is overconvergent.

Definition 35. We denote by $\mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$ the category of unipotent isocrystals on Y. $\mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$ has the structure of a neutral Tannakian category over $\mathbb{Q}_p$. We may similarly define a category $\mathcal{C}^{\mathrm{rig}}(X_{\mathbb{F}_p})$ on the special fibre of X. For a basepoint b in $Y_{\mathbb{F}_p}$, we denote by $U_\infty^{\mathrm{rig}}(b)$ the fundamental group of the this category with basepoint b. As before we have associated objects $U_n^{\mathrm{rig}}(b)$, $P_n^{\mathrm{rig}}(b,z)$, $\mathcal{A}_n^{\mathrm{rig}}$, $A_n^{\mathrm{rig}}(b,z)$ etc. As with the de Rham fundamental group, although our real interest is in the fundamental group of X, it will often be convenient to work with the larger category $\mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$ instead.

Given any non-trivial morphism of curves

$$f : X_1 \to X_2$$

we obtain a functor

$$f^* : \mathcal{C}^{\mathrm{rig}}(X_2) \to \mathcal{C}^{\mathrm{rig}}(X_1)$$

In particular, the absolute Frobenius on $Y_{\mathbb{F}_p}$ hence defines a functor

$$\phi^* : \mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p}) \to \mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$$

and hence an action of Frobenius on $U_n(b), P_n(b,z), A_n(b,z)$. As in the étale case, the action of Frobenius can be defined via

$$A_n(b,z) = P(b,z) \times_{U_n(b)} A_n(b).$$

and on graded pieces of $A_n(b)$ and $U_n(b)$ the action can be identified with the action of ϕ^* on $(H^1_{\mathrm{rig}}(X_{\mathbb{F}_p}, \mathbb{Q}_p)^*)^{\otimes n}$. By using the Riemann hypothesis for the crystalline cohomology of the curve $X_{\mathbb{F}_p}$, Besser showed the following:

Lemma 36 (Besser,[13])**.** *$P_n^{\mathrm{rig}}(x,z)$ has a unique Frobenius invariant point, for any x, z and n.*

3.4.1 Berthelot-Ogus comparison for fundamental groups

Suppose now we have a smooth curve $\mathcal{Y}$ over $\mathbb{Z}_p$ with generic fibre $Y_{\mathbb{Q}_p}$ and special fibre $Y_{\mathbb{F}_p}$ and $\mathfrak{Y}$ the associated formal scheme over $\mathrm{Spf}(\mathbb{Z}_p)$. Let $Y_{\mathbb{Q}_p}^{\mathrm{an}}$ denote the Raynaud generic fibre of $\mathrm{Spf}(\mathbb{Z}_p)$. Recall the *analytification functor*

$$M \mapsto M^{\mathrm{an}}$$

sending vector bundles on $Y_{\mathbb{Q}_p}$ to $Y_{\mathbb{Q}_p}^{\mathrm{an}}$. Composing the analytification functor with $j^\dagger$ defines a functor

$$\mathcal{C}^{dR}(Y_{\mathbb{Q}_p}) \to \mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$$
$$M \mapsto j^\dagger M^{\mathrm{an}}$$

The following theorem shows that up to equivalence these are all possible overconvergent isocrystals:

Theorem 21 ([19], Chiarellotto, Le Stum)**.** *The functor $j^\dagger$ gives an equivalence of categories*

$$\mathcal{C}^{dR}(Y_{\mathbb{Q}_p}) \to \mathcal{C}^{\mathrm{rig}}(Y_{\mathbb{F}_p})$$

For any $\mathbb{Z}_p$ points

$$b, z : \mathrm{Spec}(\mathbb{Z}_p) \to \mathcal{Y}$$

we have an isomorphism

$$P_n^{\mathrm{rig}}(sp(b), sp(z)) \simeq P_n^{dR}(z, b)$$

Via this theorem $P_n^{dR}(b, z)$ is equipped with an action of Frobenius. We similarly obtain Frobenius actions on L_n^{dR} and $A_n^{dR}(b, z)$.

Definition 36. Fix a choice of differentials of the second kind defining a universal connection. Define $p^{\mathrm{cr}}(z) = (p^{\mathrm{cr}})_n \in U_\infty^{dR}(b) \subset A_\infty^{dR}(b)$ to be the unique element such that $p^{\mathrm{cr}}(z).e$ is the Frobenius invariant path in $P_\infty^{dR}(b, z) = (P_n^{dR}(b, z))_n$, where $e \in P_\infty^{dR}(b, z)$ denotes the element corresponding to 1 via the affine trivialisation of the universal connection given by a choice of differentials of the second kind.

Note that although the Frobenius action on $P_n^{dR}(b, z)$ is defined via the reduction of the points b and z mod p, the element $p^{\mathrm{cr}}(z)$ will still be nontrivial even when b and z have the same reduction. In this case, it will be given by the canonical parallel transport between horizontal sections of a unipotent overconvergent connection on an open unit disc.

3.4.2 The crystalline unipotent Kummer map and p-adic comparision theorem

The theory described above associates to each p-adic point z a left $U^{dR}(b)$-torsor $P^{dR}(b,z) \subset A^{dR}(b,z)$, equipped with an action of Frobenius and a Hodge filtration by subvarieties compatible with the corresponding structures on $U^{dR}(b)$. We shall henceforth refer to such a datum as a U-torsor with *compatible filtered ϕ-structure.*

Let T be any U^{dR} torsor with compatible filtered ϕ-structure. Then $T(\mathbb{Q}_p)$ contains a unique element t^{cr} which has trivial ϕ-action and an element t^H which lies in $F^0 T$ (see [42]). Hence we may associate to T an element $u \in U$ such that $ut^{\mathrm{cr}} = t^H$. Since $F^0 T$ is an $F^0 U$-torsor, the element u is non-canonical, but the class $\overline{u}$ in U/F^0 is indepedendent of any choices.

Lemma 37 (Kim,[42])**.** *The map*

$$P \mapsto uF^0 U(\mathbb{Q}_p) \tag{3.9}$$

defined an isomorphism between the set of isomorphism classes of U-torsors with compatible filtered ϕ-structure and U/F^0.

Definition 37. Define

$$j_n^{\mathrm{cr}} : X(\mathbb{Q}_p) \to U/F^0 \tag{3.10}$$

to be the map sending z to the class of the U-torsor $P(b,z)$.

It follows from the definition of p^{cr} that it is related to j_n^{cr} as follows:

Lemma 38. *Let $\omega_1, \ldots, \omega_{2g}$ be a set of differentials of the second kind without poles on $Y \subset X$. The morphism j_n^{cr} is given explicitly on $]Y_{\mathbb{F}_p}[$ by*

$$z \mapsto p^{\mathrm{cr}}(z) p^H(z)$$

where $p^H \in U_n^{dR}(b)/F^0$ is the unique class such that, identifying fibres via the affine trivialisation, the image of p^H in $P_n^{dR}(b,z) \subset A_n^{dR}(b,z)$ lies in F^0

Proof. By Kim [42], j_n^{cr} is given by taking the unique frobenius invariant element p of $P_n^{\mathrm{dR}}(b,z)$ and finding an element u of $U_n(b)$, and an element q of $F^0 P_n(b,z)$ such that

$$p = uq$$

(one then taken $j_n^{\mathrm{cr}}(z) = uF^0U_n(b)$). We know that with respect to the affine trivialisation $p = p^{\mathrm{cr}}$, completing the proof. $\square$

Recall that at depth 2, p^H was given by the functions p_{ij}^H defined in the previous chapter.

The map j_n^{cr} gives an analytic interpretation of $j_{n,p}^{\acute{e}t}$, via p-adic Hodge theory. Recall Fontaine's functor D_{cr} is a functor from the category of continuous p-adic Galois representations to the category of filtered ϕ-modules. As explained in [42], Fontaine's functor defines a map

$$H^1_f(G_p, U) \to D_{dR}(U)/F^0$$

from isomorphism classes of crystalline G_p-equivariant U-torsors to $D_{cr}(U)$ torsors with compatible ϕ-actions and Hodge filtrations.

Namely, the data of a unipotent group U is equivalent to that of the Hopf algebra $\mathcal{O}_U$, and a torsor T for an algebraic group U is determined by its co-ordinate ring $\mathcal{O}_T$ together with a co-action map

$$\mathcal{O}_T \to \mathcal{O}_T \otimes \mathcal{O}_U$$

In the étale case, these co-ordinate rings are ind-objects in the category of continuous $\mathbb{Q}_p$-representations of $G_{\mathbb{Q}_p}$, hence applying D_{cr} to $\mathcal{O}_U$ gives a filtered Hopf algebra with a Frobenius action, and this determines a unipotent group $D_{cr}(U)$ with Frobenius and Hodge filtration. Similarly, applying D_{cr} to $\mathcal{O}_T$ gives a $D_{cr}(U)$-torsor T, with compatible filtered ϕ-structure.

By nonabelian p-adic Hodge theory [53] $A_n^{dR}(x,y)$ is related to $A_n^{\acute{e}t}(x,y)$ by Fontaine's crystalline periods functor:

Theorem 22 (Olsson). *There is an isomorphism*

$$D_{cr}(A_n^{\acute{e}t}(x,y))) \simeq A_n^{dR}(x,y)$$

respecting the action of Frobenius and the Hodge filtration, such that the commutative diagram

$$\begin{array}{ccc} D_{cr}(A_n^{\acute{e}t}(x)) \otimes D_{cr}(A_n^{\acute{e}t}(x,y)) & \longrightarrow & D_{cr}(A_n^{\acute{e}t}(x,y)) \\ \downarrow \simeq & & \downarrow \simeq \\ A_n^{dR}(x) \otimes A_n^{dR}(x,y) & \longrightarrow & A_n^{dR}(x,y) \end{array}$$

respects the Hodge filtration and action of Frobenius.

This implies that the $U^{dR}(b)$-torsor with compatible filtered ϕ-structure obtained by applying Fontaine's functor to $P_n^{ét}(x,z)$ is exactly the $P_n^{dR}(b,z)$.

It is shown in [42] that the function

$$Y(\mathbb{Q}_p) \to U^{dR}$$

$$z \mapsto p^{\mathrm{cr}}(z)$$

has Zariski dense image, as mentioned in chapter 1. Since $x \mapsto xp^H(z)$ is invertible and algebraic, this implies that j_n^{cr} has Zariski dense image.

3.4.3 Splitting U/F^0

In this section we explain how the choice of differentials of the second kind inducing a basis of de Rham cohomology gives a splitting of $U \to U/F^0$

Lemma 39. *Let*

$$L \simeq L/F^0 \oplus F^0 L$$

be a splitting of the Hodge filtration on L. Then there exists a splitting

$$\mathrm{spl} : U/F^0 \to U$$

of the quotient by F^0 map, such that $\log(\mathrm{spl}(U/F^0)) = L/F^0$

Proof. This can be seen by induction on the degree nilpotency of U. If U is abelian then there is nothing to prove. Now consider a general U, and suppose the result is known for U/Z, where Z is a subgroup lying in the center of U. Then note that the exponential and logarithm maps are equivariant with respect to the action of Z (where we consider Z as acting on L via

$$(z,x) \mapsto \log(z) + x$$

for $z \in Z$, $x \in L$). Hence there is a unique splitting of $U \to U/F^0$ which agrees with the splitting of the Hodge filtration on L and Z. □

3.4.4 Example

Suppose $U = U_2$. Then

$$p^{\mathrm{cr}}(z) = 1 + \sum_{i=0}^{2g-1} \int_b^z \omega_i T_i + \sum_{i=0}^{2g-1} \int_b^z \omega_i \omega_j \overline{T_i \otimes T_j}$$

$$p^H(z) = 1 + \sum p_{ij}^H(z) \overline{T_i \otimes T_j}$$

Hence

Lemma 40. *With respect to the splitting $U/F^0 \to U$ defined above, j^{cr} is given by*

$$z \mapsto 1 + \sum_{i=0}^{g-1} \int_b^z \omega_i T_i + \sum_{0 \leq i < j < g} \int (\omega_i \omega_j - \omega_j \omega_i) \overline{T_i \wedge T_j}$$
$$+2 \sum_{0 \leq i < g \leq j < 2g} \int \omega_i \omega_j \overline{T_i \wedge T_j} - \sum p_{ij}^H(z) \overline{T_i \otimes T_j}$$

Proof. This follows from the previous section, together with the standard iterated integral identity

$$\int_b^z \omega_i \omega_i + \int_b^z \omega_j \omega_i = (\int_b^z \omega_i)(\int_n^z \omega_j)$$

(see e.g. [18]). □

3.5 Filtered F-isocrystals

We now want to mimic the approach of chapter 1 in a local context - that is, we replace the nonabelian torsors $P(b, z)$ with abelian extensions $A(b, z)$, to define a map

$$\mathbb{Q}_p[U^{dR}/F^0] \to E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}])/F^0$$

from compatible U^{dR}-torsors to extensions of a filtered ϕ-module which is universal for extensions of V^{dR} by $[L^{dR}, L^{dR}]$.

Let

$$\phi : \mathcal{Y} \to \mathcal{X}$$

be a lift of the absolute Frobenius on $Y_{\mathbb{F}_p}$. By [54] such a lift always exists if Y is affine. The triple $(\mathcal{Y}, \mathcal{X}, \phi)$ is referred to in [8] as a *syntomic datum.*

Definition 38. A *Frobenius structure*, or *F-structure*, on an overconvergent isocrystal $\mathcal{M}$ is an isomorphism

$$\Phi : \phi^*(\mathcal{M}, \nabla) \xrightarrow{\simeq} (\mathcal{M}, \nabla)$$

of overconvergent isocrystals. We denote by $\mathcal{C}^{F-\mathrm{rig}}(X_{\mathbb{F}_p})$ the $\mathbb{Q}_p$-linear abelian category of F-isocrystals.

We also define an F-isocrystal on $\mathrm{Spec}(\mathbb{Z}_p)$ to be an overconvergent isocrystal on $\mathrm{Spec}(\mathbb{Z}_p)$ with an isomorphism with its Frobenius pull-back. Hence an F-isocrystal is simply a $\mathbb{Q}_p$-vector space equipped with an endomorphism, denoted ϕ^*.

For F-isocrystals M and N, we denote by $\mathrm{Ext}^i_{F-\mathrm{rig}}(M, N)$ the $\mathbb{Q}_p$-vector space of homotopy classes of i-fold extensions of F-isocrystals.

Definition 39. Given a syntomic datum as above, a *filtered F-isocrystal* is a 4-tuple $(M, \nabla, F^\bullet, \Phi)$ where M is a finite dimensional vector bundle on $X_{\mathbb{Q}_p}$, ∇ is a flat connection on M, $F^\bullet$ is a filtration on M satisfying Griffiths transversality with respect to ∇, and Φ is a Frobenius structure on $j^\dagger(M^{an}, \nabla)$. For a filtered F-isocrystal M, we denote by $H^i_{\mathrm{syn}}(X, M)$ the $\mathbb{Q}_p$-vector space of homotopy classes of i-fold extensions of filtered F-isocrystals.

By the above, $(\mathcal{A}_n^{dR}, \nabla, F^\bullet, \Phi)$ is an example of a filtered F-isocrystal.

Definition 40. We may similarly define the notion of an F-isocrystal on $\mathrm{Spec}(\mathbb{Z}_p)$: namely, a filtered F-isocrystal on $\mathrm{Spec}(\mathbb{Z}_p)$ is defined to be a filtered $\mathbb{Q}_p$-vector space $(V^{dR}, F^\bullet)$, a $\mathbb{Q}_p$-vector space with an endomorphism $(V^{\mathrm{cr}}, \phi^*)$, and an isomorphism of $\mathbb{Q}_p$-vector spaces

$$V^{dR} \simeq V^{\mathrm{cr}}$$

We shall often regard a filtered F-isocrystal on $\mathrm{Spec}(\mathbb{Z}_p)$ as a vector space with endomorphism and filtration, and refer to it as a *filtered ϕ-module*. The filtration $F^\bullet$ will often be referred to as the Hodge filtration, and ϕ as Frobenius. The category of filtered ϕ-modules will be denoted $\mathcal{C}^{\mathrm{fil},\phi}$.

Definition 41. Given an $\mathbb{F}_p$-point $\overline{z}$, let $z_0 \in X(\mathbb{Z}_p)$ denote the *Teichmuller lift* corresponding to the Frobenius lift ϕ - hence z_0 is the unique fixed point of $\phi|_{]\overline{z}[}$.

For an F-isocrystal $\mathcal{M}$ the pull-back $\overline{z}^*\mathcal{M}$ may be defined as the fibre of the bundle $\mathcal{M}$ at the point z_0. Since z_0 is ϕ-stable, the fibre $z_0^*\mathcal{M}$ admits an action of ϕ via the F-structure on $\mathcal{M}$, giving a functor

$$\overline{z}^* : \mathcal{C}^{F-\mathrm{rig}}(Y_{\mathbb{F}_p}) \to \mathcal{C}^{\mathrm{fil},\phi}$$

Hence associated to any $\mathbb{Z}_p$ point z, we have the following data

- A filtered $\mathbb{Q}_p$-vector space $z_{\mathbb{Q}_p}^* A_n^{dR}$
- A $\mathbb{Q}_p$-vector space $z_{\mathbb{F}_p}^* A_n^{\mathrm{rig}}$
- An endomorphism $\phi^* : z_{\mathbb{F}_p}^* A_n^{\mathrm{rig}} \to z_{\mathbb{F}_p}^* A_n^{\mathrm{rig}}$
- An isomorphism $z_{\mathbb{F}_p}^* A_n^{\mathrm{rig}} \xrightarrow{\simeq} z_{\mathbb{Q}_p}^* A_n^{dR}$ coming from parallel transport on the residue disc $]z[$

Note that the affine trivialisation

$$\overline{A}_2^{dR}(x,y) \simeq \mathbb{Q}_p \oplus V^{dR} \oplus \overline{\wedge^2 V^{dR}}$$

will in general not respect the Hodge filtration or the action of Frobenius, even at $y = x$. Recall the description of extensions of filtered ϕ-modules (see e.g. [50], Proposition 1.21):

Lemma 41. *Let*

$$0 \to Z \to E \to \mathbb{Q}_p \to 0 \tag{3.11}$$

be a morphism of filtered ϕ-modules. Suppose $Z^{\phi=1} = 0$. Let s^ϕ be a ϕ-equivariant splitting of $E \to \mathbb{Q}_p$, and s^H a splitting respecting the Hodge filtration. The map

$$[E] \mapsto s^\phi - s^H \mod F^0 Z$$

$$\mathrm{Ext}^1_{\mathrm{fil},\phi}(\mathbb{Q}_p, Z) \to Z/F^0$$

is a vector space isomorphism.

Concretely, we may describe the action of ϕ as follows:

Lemma 42. *Let z_0 be a Teichmuller point on the residue disc $]z[$. View $z_0^*\mathcal{A}_n$ as a ϕ-module via the pull-back of the F-structure on $\mathcal{A}_n$. Then the filtered ϕ-module associated to $A_n(x,z)$ is the filtered vector space $A_n^{dR}(x,z)$, the ϕ-module $z_0^*\mathcal{A}_n$, and the isomorphism*

$$(A_n^{dR}(x,z) =)z^* j^\dagger \mathcal{A}_n \simeq z_0^* j^\dagger \mathcal{A}_n$$

defined by parallel transport on a residue disc.

Proof. The filtered ϕ-module structure on $A_n^{\mathrm{dR}}(x,z)$ is defined to be the pull-back of the filtered F-isocrystal $\mathcal{A}_n^{\mathrm{dR}}$ by

$$z : \mathrm{Spec}(\mathbb{Z}_p) \to \mathcal{A}_n.$$

The statement of the Lemma is then exactly the definition of the pull back of a filtered F-isocrystal by a $\mathbb{Z}_p$-point given in [10], Definition 4.5. □

At the point $x = z$, the filtered ϕ module $A_n^{dR}(x)$ admits a canonical splitting

$$A_n^{dR}(x) \simeq \mathbb{Q}_p \oplus IA_n^{dR}(x)$$

coming from the unit map $\mathbb{Q}_p \to A_n(x)$.

3.5.1 Characterising the Frobenius pull-back

In this subsection we note the following Lemma:

Lemma 43. *The Frobenius pull-back*

$$\phi^* \mathcal{A}_n^{\mathrm{rig}} \xrightarrow{\simeq} \mathcal{A}_n^{\mathrm{rig}}$$

is uniquely characterised by the fact that, pulling back by

$$\overline{z} : \mathrm{Spec}(\mathbb{F}_p) \to \mathcal{X}_{\mathbb{F}_p},$$

the isomorphism is identified with the ϕ-equivariant parallel-transport isomorphism

$$A_n^{dR}(z) \xrightarrow{\simeq} A_n^{dR}(z, z_0)$$

Proof. Since the de Rham fundamental group is isomorphic to the crystalline fundamental group, the group of endomorphisms of the universal isocrystal $\mathcal{A}_n^{\mathrm{rig}}$ □

3.5.2 Extensions of F-isocrystals

Fix a basepoint b. Recall the unipotent isocrystal $\mathcal{A}_n$ (relative to the $\mathbb{F}_p$-point $\mathrm{sp}(b)$) defined in section 2.4.

The theorem of Chiarellotto and Le Stum on the equivalence between the categories of unipotent isocrystals and unipotent flat connections implies:

Corollary 7. *For any n-unipotent isocrystal $\mathcal{F}$ and any $v \in z^*\mathcal{F}$ there exists a unique morphism of isocrystals*

$$\mathcal{A}_n \to z^*\mathcal{F}$$

such that the pull-back

$$z^*\mathcal{A}_n \to \mathcal{F}$$

sends 1 *in $z^*\mathcal{A}_n \simeq A_n$ to v*

Recall [11](Corollary A.14) (more details may be found for example in [9])

Theorem 23. *The sequence*

$$0 \to H^1_{\mathrm{syn}}(\mathbb{Z}_p, H^m_{\mathrm{rig}}(\mathcal{X}, \mathcal{M}) \to H^{m+1}_{\mathrm{syn}}(\mathcal{X}, \mathcal{M}) \to H^0_{\mathrm{syn}}(\mathbb{Z}_p, H^{m+1}_{\mathrm{rig}}(\mathcal{X}, \mathcal{M})) \to 0$$

is exact

In the case $m = 0$ we obtain an exact sequence

$$0 \to \mathrm{Ext}^1_{\mathrm{fil}-\phi}(\mathbb{Q}_p, H^0_{dR}(M)) \to \mathrm{Ext}^1_{F-\mathrm{rig}}(\mathcal{O}, M) \to \mathrm{Hom}_{\mathrm{fil}-\phi}(\mathbb{Q}_p, H^1_{dR}(M)) \to 0$$

where Ext^i_{F-rig} denotes the ith Ext group in the abelian category of F-isocrystals on $\mathcal{X}$.

Corollary 8. *Let $(\mathcal{A}^{\mathrm{rig}}_n, \nabla_n)$ be the isocrystals from definition 35, and let b be a Teichmuller point of X. There is a unique F-structure on the family of isocrystals $(\mathcal{A}^{dR}_n, \nabla_n)_n$ is uniquely determined by by the conditions*

- *The exact sequence*

$$0 \to I/I^2 \otimes \mathcal{O} \to \mathcal{A}^{\mathrm{rig}}_1 \to \mathcal{O} \to 0 \tag{3.12}$$

  where $\mathcal{O}$ has the trivial F-structure and the F-structure on $I/I^2 \otimes \mathcal{O}$ is induced from the Frobenius action on $I/I^2 \simeq H^1_{\mathrm{rig}}(X_{\mathbb{F}_p}, \mathbb{Q}_p)^*$.

- *For $n > 1$, the exact sequence*

$$0 \to I^n/I^{n+1} \otimes \mathcal{O} \to \mathcal{A}_n^{\mathrm{rig}} \to \mathcal{A}_{n-1}^{\mathrm{rig}} \to 0 \tag{3.13}$$

  where the F-structure on $I^n/I^{n+1} \otimes \mathcal{O}$ is induced from the Frobenius action on I^n/I^{n+1} viewed as a quotient of $H^1_{\mathrm{rig}}(X_{\mathbb{F}_p}, \mathbb{Q}_p)^{*\otimes n}$.

- *$(\mathcal{A}_n^{dR}, \nabla_n, F^\bullet, \Phi)$ has the structure of a filtered F-isocrystal.*

- *The filtered ϕ-module obtained from taking the fibre of the filtered F-isocrystal $(\mathcal{A}_n^{dR}, \nabla_n, F^\bullet, \Phi)$ at the point b admits a splitting of*

$$b^*\mathcal{A}_n^{dR} \to b^*\mathcal{A}_0^{dR} = \mathbb{Q}_p$$

Proof. We prove this by induction on n. For $n = 0$ there is nothing to prove. For $n > 0$ the exact sequence above implies that the set of F-structures on $\mathcal{A}_n^{\mathrm{rig}}$ lifting the F-structure on $\mathcal{A}_{n-1}^{\mathrm{rig}}$ and $I^n/I^{n+1} \otimes \mathcal{O}$ is a (non-empty) torsor for

$$H^1_{\mathrm{fil}-\phi}(\mathbb{Q}_p, (I^n/I^{n+1})^* \otimes H^0_{dR}(\mathcal{A}_{n-1}^{dR})) \simeq H^1_{\mathrm{fil}-\phi}(\mathbb{Q}_p, (I^n/I^{n+1})^* \otimes (I^{n-1}/I^n))$$

(by Theorem 23). The pull-back morphism

$$b^* : \mathrm{Ext}^1_{F-\mathrm{rig}}(\mathcal{O}, (I^n/I^{n+1})^* \otimes \mathcal{A}_{n-1}^{dR}) \to \mathrm{Ext}^1_{\mathrm{fil}\,\phi}(\mathbb{Q}_p, (I^n/I^{n+1})^* \otimes b^*\mathcal{A}_{n-1}^{dR})$$

commutes with the action of $H^1_{\mathrm{fil}-\phi}(\mathbb{Q}_p, (I^n/I^{n+1})^* \otimes (I^{n-1}/I^n))$, and hence there is a unique choice of lift for which the induced $\mathrm{Ext}^1_{\mathrm{fil},\phi}(\mathbb{Q}_p, (I^n/I^{n+1}))$ class of $b^*\mathcal{A}_n^{\mathrm{rig}}$ is trivial. □

3.5.3 Iterated integrals

Definition 42. We now return to the case where Y is affine, so that $A_\infty(b)$ is free on its generators $T_0, \dots, T_{2g+d-2}$. We define the *iterated Coleman integral* of 1-forms $\omega_{n_1} \dots \omega_{n_k}$ from z to w to be the $T_{n_1} \dots T_{n_k}$ coefficient of the image of $1 \in z^*\mathcal{A}_n^{dR}$ under the unique Frobenius-equivariant isomorphism ([13])

$$z^*\mathcal{A}_n \xrightarrow{\simeq} x^*\mathcal{A}_n$$

Note that $\int_w^z \omega_1 \dots \omega_n$ is independent of the choice of Frobenius lift, as it is defined in terms of the action of Frobenius on the category of isocrystals. Note further that if one takes a smaller open $Y' \subset Y$, one gets the same definition of $\int_w^z \omega_{n_1} \dots \omega_{n_k}$, hence for X projective we may define iterated Coleman integrals by choosing an affine open on which all the differentials are defined.

Remark 8. We briefly recall the intuition behind the notation: recall when $\mathrm{sp}(z) = \mathrm{sp}(w)$ the Frobenius equivariant isomorphism from $A(w)$ to $A(z)$ is given by parallel transport of horizontal sections. Write a horizontal section of $\mathcal{A}_n$ as

$$s = \sum_w a_w w(T_0, \dots, T_{2g+d-2})$$

where the sum is over all words of length at most n. Then by definition of the connection, (see Definition 26), s satisfies

$$ds_{T_i w} = s_w \omega_i$$

Example 6. Abelian Coleman integrals have a well-known interpretation as representing the extension classes of $D_{cr}(A_1^{\text{ét}}(x, z))$. Namely, since the affine trivialisation of $A_1(x)$ will respect the Frobenius filtration, the ϕ equivariant-splitting of $A_1(x, z) \to \mathbb{Q}_p$ can be given by

$$\mathbb{Q}_p \hookrightarrow A_1(x) \to A_1(x, z)$$

where the first map is the inclusion of filtered ϕ-modules and the second is the Frobenius-equivariant isomorphism. Hence with respect to the affine trivialisation the Frobenius-equivariant splitting of $A_1(x, z) \to \mathbb{Q}_p$ is given by

$$1 \mapsto 1 + \sum_{i=0}^{2g-1} \int_x^z \omega_i T_i$$

Since the affine trivialisation respects the Hodge filtration on A_1, the corresponding extension class is exactly given $\sum \int_x^z \omega_i T_i$.

In general, one cannot express a Frobenius equivariant isomorphism

$$\mathbb{Q}_p \oplus V \oplus [L, L] \xrightarrow{\simeq} A(b, z)$$

purely in terms of iterated Coleman integrals from b to z, as the extension

$$0 \to [L, L] \to IA(b) \to V \to 0$$

can be nontrivial. For this reason we introduce the following notation:

Definition 43. Define

$$G(b) = G : V \to \overline{\wedge^2 V}$$

to be the unique homomorphism such that $\begin{pmatrix} \mathbf{1}_V & \\ G & \mathbf{1}_{\overline{\wedge^2 V}} \end{pmatrix}$ defines a Frobenius equivariant isomorphism

$$V \oplus \overline{\wedge^2 V} \xrightarrow{\simeq} I\overline{A}_2(b)$$

Lemma 44. *The Frobenius equivariant section of*

$$A_2(b,z) \to \mathbb{Q}_p$$

is given by

$$1 \mapsto 1 + \sum \int_b^z \omega_i T_i + \sum_{i,j} \int_b^z (\omega_i \omega_j - \omega_j \omega_i) \overline{T_i \wedge T_j}$$

Proof. We have a Frobenius equivariant commutative diagram

$$\begin{array}{ccc} A_2(b) & \longrightarrow & A_2(b,z) \\ \downarrow & & \downarrow \\ \mathbb{Q}_p & = & \mathbb{Q}_p \end{array}$$

where the vertical maps are the projections coming from quotienting modulo I and the top horizontal map is given by iterated Coleman integrals as in definition . However the left vertical map admits a Frobenius equivariant splitting via the affine trivialisation, hence by composition we get the Frobenius equivariant splitting of $A_2(b,z)$ required. □

One situation in which the function G can be made more explicit is when X is a hyperelliptic curve.

Lemma 45. *Let X be a hyperelliptic curve, and as usual for a point $z = (x,y)$ on X let z^- denote the point $(x,-y)$. Then*

$$G(b) = \sum_{i=1}^{2g} \int_{b^-}^{b} \omega_i T_i$$

Proof. For $\mathbb{Q}_p$ points z_1 and z_2 and a global differential ω, denote $\int_{z_1}^{z_2}\omega$ by $\int^{z_2-z_1}\omega$, and hence define $\int^{\sum \mu_i z_i}\omega$ for an arbitrary $\mathbb{Q}$-divisor $\sum \mu_i z_i$ of degree zero by linearity.

Arguing as in Lemma 4,

$$G(b) = \sum_{i=0}^{g-1} \int^{2b-D} \omega_i T_i$$

Finally note that

$$\int^{2b-D} \omega_i = -\int^{2b^- -D} \omega_i$$

since D is fixed by the hyperelliptic involution, so

$$\int^{2b-D} \omega_i = \int_{b^-}^{b} \omega_i$$

□

3.5.4 Universal extensions of filtered ϕ-modules

This subsection gives the crystalline analogue of the map Ψ defined in the previous chapter.

Given a left U-torsor P with compatible filtered ϕ-structure, and a filtered ϕ-module W with a compatible action of U, define the twist of W by P to be the filtered ϕ-module

$$W \times_U P = W \times U / \sim$$

where as before $\sim$ is the equivalence relation

$$(v,p) \sim (vu, u^{-1}p)$$

for all $v \in V, u \in U, p \in P$. The ϕ-actions and Hodge filtrations on W and P induce a ϕ-action and Hodge filtration on $W \times P$, and compatibility with the U-action imply this gives a well-defined filtered ϕ-module structure on the quotient.

It remains to construct a space which is a target for all twists of $A(b)$ by U-torsors with compatible filtered ϕ-structure. As in the Galois case, we may define a universal extension of V by $[L,L]$, denoted $E_p^{\mathrm{cr}}(V,[L,L])$. Note that given a filtered ϕ-module W, when thinking of W/F^0 as a filtered ϕ-module we give it the trivial Hodge filtration and Frobenius action (so it is isomorphic to $\mathbb{Q}_p^{\oplus n}$ for some n). The following lemma describing the universal extension of V by $[L, L]$ is proved exactly as for the Galois analogue of chapter 2.

Lemma 46. *There is a filtered ϕ-module $E_p^{\mathrm{cr}}(V, \overline{\wedge^2 V})$, and an exact sequence of filtered ϕ-modules*

$$0 \to [L, L] \to E_p^{\mathrm{cr}}(V, [L, L]) \to (\mathrm{Hom}(V, [L, L])/F^0) \otimes V \to 0$$

satisfying the following universal property for extensions for filtered ϕ-modules: for any short exact sequence of filtered ϕ-modules

$$0 \to [L, L] \to W \to V \to 0$$

there is a unique commutative diagram of filtered ϕ-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & [L,L] & \longrightarrow & W & \longrightarrow & V & \longrightarrow & 0 \\ & & \Vert & & \downarrow & & \downarrow {\scriptstyle 1_V \otimes [W]} & & \\ 0 & \longrightarrow & [L,L] & \longrightarrow & E_p^{\mathrm{cr}}(V, [L,L]) & \longrightarrow & V & \longrightarrow & 0 \end{array}$$

We similarly define $E_{p,R}^{\mathrm{cr}}(V, [L, L])$ for $\mathbb{Q}_p$-algebras R acting on V. For X a hyperelliptic curve this may be replaced by the filtered ϕ-module $E_{\tau,R}^{\mathrm{cr}}(V, [L, L])$ which is is universal for extensions of V by $[L, L]$ coming from V/F^0. Recall (see e.g. [15]) that for any crystalline $G_{\mathbb{Q}_p}$-representation W such that $D_{\mathrm{cr}}(W)^{\phi=1} = 0$, the natural map

$$H_f^1(G_p, W) \to \mathrm{Ext}^1_{\mathrm{fil},\phi}(\mathbb{Q}_p, D_{\mathrm{cr}}(W))$$

induced by Fontaine's functor is an isomorphism. Since V has weight -1 and $[L, L]$ has weight -2, we obtain isomorphisms

$$D_{cr}(E_p(V^{\acute{e}t}, [L^{\acute{e}t}, L^{\acute{e}t}])) \simeq E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}]) \tag{3.14}$$

$$H_f^1(G_p, E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}])) \simeq E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}])/F^0$$

Definition 44. Define

$$\Psi^{\mathrm{cr}} : U/F^0 \to E_p^{\mathrm{cr}}(V, [L, L])/F^0$$

$$[P] \mapsto [P \times_U A(b)]$$

and similarly define Ψ_R^{cr}, $\Psi_R^{\mathrm{cr,Sym}}$ and so forth.

To obtain explicit equations for global cohomology classes inside $E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}])/F^0$ we need to write down a basis of $E_p^{\mathrm{cr}}(V^{dR}, [L^{dR}, L^{dR}])$.

Lemma 47. *Choose a splitting*

$$t : V^* \otimes [L, L]/F^0 \to V^* \otimes [L, L]$$

of the Hodge filtration of $V^* \otimes [L, L]$. Then $E_p^{\mathrm{cr}}(V, [L, L])$ admits a splitting of the Hodge filtration

$$t^H : (V^* \otimes [L, L]/F^0) \otimes V \oplus [L, L] \xrightarrow{\simeq} E_p^{\mathrm{cr}}(V, [L, L])$$

and a splitting of the ϕ-action

$$t^\phi : (V^* \otimes [L, L]/F^0) \otimes V \oplus [L, L] \xrightarrow{\simeq} E_p^{\mathrm{cr}}(V, [L, L])$$

such that

$$(t^H)^{-1} \circ t^\phi - 1 : (V^* \otimes [L, L]/F^0) \otimes V \to [L, L]$$

is given by

$$v \otimes w \mapsto t(v)(w)$$

Proof. Let M be the extension of V by $[L, L]$ defined by the property that it has Frobenius and Hodge splittings t^H and t^ϕ as above. It will be enough to show that M satisfies the universal properties required. Given an extension W of V by $[L, L]$ there is a unique choice of Frobenius equivariant splitting

$$s^\phi : V \oplus [L, L] \xrightarrow{\simeq} M,$$

by the Weil conjectures. Then there is a unique choice of Hodge splitting of

$$s^H V \oplus [L, L] \xrightarrow{\simeq} M$$

such that

$$s^{\phi} - s^{H} : V \to [L, L]$$

lies in the image of t. Hence

$$s^{\phi} - s^{H} = t([W])$$

since their image in $V^* \otimes [L, L]/F^0$ agree. We define

$$W \to M$$

to be the map sending $s^H(v, w)$ to $t^H([W] \otimes v, w)$. To check that this is ϕ-equivariant we need to check where $s^{\phi}(v, 0)$ is sent. By definition

$$s^{\phi}(v) = s^H(v) + t([W])(v) = s^H(v, t([W])(v)),$$

hence this is sent to $t^H([W] \otimes v, t([W]))$, which, by definition of M, equals $t^H([W] \otimes v, 0)$. Uniqueness follows. $\square$

A choice of differential forms $\omega_1, \ldots, \omega_{2g}$ generating $H^1_{dR}(X)$ gives a basis of $E_p^{\mathrm{cr}}(V, \overline{\wedge^2 V})$ as follows:

Definition 45. Let

$$s : V/F^0 \to V$$

be the splitting of the Hodge filtration induced by the basis ω_i. This induces a splitting of the Hodge filtration of $V^* \otimes \overline{\wedge^2 V}$, and hence the function G decomposes as $G_1 + G_2$, where

$$G_1 = G_1(b) \in (V^* \otimes \overline{\wedge^2 V})/F^0$$

and

$$G_2 = G_2(b) \in F^0(V^* \otimes \overline{\wedge^2 V}).$$

giving the following explicit description of Ψ^{cr}:

Lemma 48. *1. The map*

$$\Psi^{\mathrm{cr}} : U/F^0 \to E_p^{\mathrm{cr}}(V, [L, L])/F^0$$

sends

$$1 + v + u$$

to

$$(G_1(v) + \tau(v_1)) \otimes v_1 + G_2(v)(v) + \tau(v_2)(v) + u$$

2.

$$\Psi^{\mathrm{cr}}(z) = (G_1 + \sum_{i=0}^{g-1} \omega_i \tau(T_i)) \otimes \sum_{i=0}^{g-1} \omega_i T_i$$

$$\sum_{0\le i<j<g} \int_b^z (\omega_i\omega_j - \omega_j\omega_i)\overline{T_i \wedge T_i}$$

$$+ \sum_{0\le i<g\le j<2g} [\int_b^z (\omega_i\omega_j - \omega_j\omega_i) + (\int_b^z \omega_i)(\int_b^z \omega_j) - p^H_{ij}(z)]\overline{T_i \wedge T_j}$$

$$+ \sum_{0\le i<g} (\int_b^z \omega_i) G(T_i)$$

Proof. Let W be a mixed filtered ϕ-module in an exact sequence

$$0 \to [L, L] \to W \to V \to 0$$

equipped with a splitting of the Hodge filtration

$$t^H : V \oplus [L, L] \xrightarrow{\simeq} W$$

and a splitting of the ϕ-action

$$t^\phi : V \oplus [L, L] \xrightarrow{\simeq} W$$

Define $t \in \mathrm{Hom}(V, [L, L])$ by

$$t^\phi \circ (t^H)^{-1} = 1 + t$$

Let $t = t_1 + t_2$ be the decomposition induced by the splitting

$$\mathrm{Hom}(V, [L, L]) \simeq \mathrm{Hom}(V, [L, L])/F^0 \oplus F^0\,\mathrm{Hom}(V, [L, L])$$

Then the map

$$W \to E^{\mathrm{cr}}_p(V, [L, L])$$

for $v \in V$ and $u \in [L, L]$, is given by

$$t^H(v + u) \mapsto t_1 \otimes v \oplus t_2(v) + u$$

By definition of G,

$$\mathbb{Q}_p \oplus V \oplus [L, L] \mapsto A(b)$$

$$(\lambda, v, u) \mapsto (\lambda, v, G(v))$$

is ϕ-equivariant (as usual, we are writing $A(b)$ as a direct sum via the affine trivialisation). By definition of Coleman integration,

$$A(b) \mapsto A(b, z)$$

$$(\lambda, v, u) \mapsto (\lambda, v + \lambda \sum_{i=0}^{2g-1} \int_b^z \omega_i T_i, v + \overline{(\sum_i (\int_b^z \omega_i) T_i) \wedge v} + \sum_{i,j} \int_b^z \omega_i \omega_j \overline{T_i \wedge T_j}) \tag{3.15}$$

The Lemma then follows from composing these two maps. □

3.5.5 Global formulae

In this subsection we record what this tells us about formulae for rational points. We return to the global setting: X is defined over $\mathbb{Q}$, p is a prime of good reduction and U denotes a $G_{\mathbb{Q}}$-stable quotient of U_2 (for possibly varying basepoints). T_0 is the set of primes of bad reduction, and for $v \in T_0$, and b, z in $X(\mathbb{Q}_v)$, let $[j(b,z)]$ denote the $H^1(G_v, [L,L])$ class corresponding to $j(b,z)$ via the isomorphism

$$H^1(G_v, [L,L]) \simeq H^1(G_v, U)$$

Proposition 8. *Suppose* $\sum \lambda_i(z_i)$ *in* $\mathbb{Q}_p[X(\mathbb{Q})]$ *satisfies*

$$\sum \lambda_i(z_i - b) = 0$$

in $\mathrm{Jac}(X)$ *and*

$$\sum \lambda_i(z_i - b)^2 = 0$$

in $\mathrm{Sym}^2 \mathrm{Jac}(X)$. *Suppose that for all* v *in* T_0,

$$\sum \lambda_i [j(b, z_i)] = 0 \tag{3.16}$$

in $H^1(G_v, [L,L])$. *Then*

$$(G_1 + \sum_{i=0}^{g-1} \omega_i \tau(T_i)) \otimes \sum_{i=0}^{g-1} \omega_i T_i$$

$$\sum_{0 \leq i < j < g} \int_b^z (\omega_i \omega_j - \omega_j \omega_i) \overline{T_i \wedge T_i}$$

$$+ \sum_{0 \leq i < g \leq j < 2g} [\int_b^z (\omega_i \omega_j - \omega_j \omega_i) + (\int_b^z \omega_i)(\int_b^z \omega_j) - p_{ij}^H(z)] \overline{T_i \wedge T_j}$$

$$+ \sum_{0 \leq i < g} (\int_b^z \omega_i) G(T_i)$$

is in the image of $H^1_f(G_T, [L,L])$.

Proof. The conditions on the image of $\sum \lambda_i(z_i)$ in $\mathrm{Jac}(X)$ and $\mathrm{Sym}^2 \mathrm{Jac}(X)$ ensure that $\overline{\Psi}(\sum \lambda_i z_i) = 0$, by Lemma 15. Hence $\sum \lambda_i \Psi(z_i)$ defines an element of $H^1(G_T, [L,L])$ which is crystalline at p, and by (3.18) is unramified away from p, hence defining an element of $H^1_f(G_T, \overline{\wedge^2 V})$. Finally, by Lemma 48 its image in $D_{dR}(\overline{\wedge^2 V})/F^0$ is given by the formula above. □

For hyperelliptic curves, we may use the description of G given in Lemma 45 to give a more explicit formula:

Proposition 9. *Let* X *be a hyperelliptic curve of genus* g. *Suppose*

$$\sum \lambda_k(z_k, b_k)$$

in $\mathbb{Q}_p[X(\mathbb{Q}) \times X(\mathbb{Q})]$ *satisfies*

$$\sum \lambda_k(z_k - b_k) \otimes (z_k + b_k - D) = 0 \tag{3.17}$$

in $\mathrm{Jac}(X) \otimes \mathrm{Jac}(X) \otimes \mathbb{Q}_p$, *and, for all* $v \in T_0$,

$$\sum \lambda_i [j(b_k, z_k)] = 0 \tag{3.18}$$

in $H^1(G_v, [L,L])$. *Then*

$$\sum_{i<j, i<g} \int_{b_k}^{z_k} (\omega_i \omega_j - \omega_i \omega_j) +$$

$$\sum_{i<g\leq j} \left[(\int_{b_k}^{z_k} (\omega_i \omega_j - \omega_i \omega_j) + (\int_{b_k^-}^{z_k} \omega_i)(\int_{b_k}^{z_k} \omega_j) - p_{ij}^H \overline{T_i \wedge T_j} \right]$$

$$\in [L,L]/F^0$$

lies in the image of $H^1_f(G_T, [L, L])$.

Proof. Again $\sum \lambda_i [A(b_i, z_i)]$ lies in $H^1(G_T, [L, L])$, this time by Lemma 4 and Lemma 15. Equation 3.17 ensures that it lies in $H^1_f(G_T, [L, L])$. The formula for its image in $[L, L]/F^0$ follows from Lemma 48, together with the expression for G given in Lemma 45. □

Chapter 4

Examples

In this chapter we give some examples where the theory of Selmer varieties can be implemented to find finite sets containing $X(\mathbb{Q})$. This is joint work with Jennifer Balakrishnan.

4.1 Bielliptic curves of Mordell-Weil rank 2

In this section we return to the situation of example 2 from the first chapter: recall X is a bielliptic curve

$$y^2 = x^6 + ax^4 + bx^2 + 1$$

with morphisms f_1 and f_2 down to elliptic curves E_1 and E_2. V_1 and V_2 are the $\mathbb{Q}_p$-Tate modules of E_1 and E_2, and κ_i denotes the Kummer map from $E_i(\mathbb{Q})$ to $H^1_f(G_T, V_i)$.

We aim to give a description of the set of rational points $X(\mathbb{Q})$ in the case where E_1 and E_2 both have rank 1. The problem of explicitly describing the rational points of such curves has also been studied (by different methods) by Flynn and Wetherell in [16], [33], [63], and effective methods have been obtained in many cases. Their approach is to try to find a cover of X whose Prym variety satisfies the hypotheses of Chabauty's theorem.

We give a formula for the set of rational points of X in terms of local heights on the elliptic curves E_1 and E_2. In our conventions of local heights we follow [4]. This means that our λ_v is equal to twice the $\widehat{\lambda}_v$ of [61], which differs from $\widehat{\lambda}'_v$ by $\frac{1}{12}v(\Delta)$. At a prime of good reduction, λ_v is just $\min\{0, v(x)\} \log_p(v)\}$.

Suppose E_1 and E_2 both have Mordell Weil rank 1, and let $z_1 \in E_1(\mathbb{Q})$ and $z_2 \in E_2(\mathbb{Q})$ be Mordell-Weil generators. Let $\lambda_{E_1,v}$ and $\lambda_{E_2,v}$ denote the local p-adic heights of E_1 and E_2 at the prime v, and denote by $h_{E_1} := \sum_v \lambda_{E_1,v}$ and $h_{E_2} := \sum_v \lambda_{E_2,v}$ the global heights. For computational reasons it is simpler to rewrite the double integrals purely in terms of p-adic heights on E_1 and E_2.

Theorem 24. *Define*

$$\begin{aligned} \rho :& X(\mathbb{Q}_p) \to \mathbb{Q}_p \\ & z \mapsto 2\lambda_{p,E_1}(f_1(z)) - 2\frac{\log_{E_1}(f_1(z))^2}{\log_{E_1}(z_1)^2} h_{E_1}(z_1) \\ & - \lambda_{p,E_2}(f_2(z) - (0,1)) - \lambda_{p,E_2}(f_2(z) + (0,1)) \\ & + \frac{\log_{E_2}(f_2(z) - (0,1))^2 + \log_{E_2}(f_2(z) + (0,1))^2}{\log_{E_2}(z_2)^2} h_{E_2}(z_2) \end{aligned}$$

Then $X(\mathbb{Q}_p)_2$ is finite, and is contained in the finite set of z in $X(\mathbb{Q}_p)$ such that

$$\rho(z) = \sum_{v \in T_0} \beta_v$$

where β_v ranges over the finite set of possible values of

$$2\lambda_{E_1,v}(x(f_1(z))) - \lambda_{E_2,v}(x(f_2(z)) + (0,1)) - \lambda_{E_2,v}(x(f_2(z)) - (0,1))$$

for z in $X(\mathbb{Q})_v$.

Proof. The result is a special case of part (ii) of Lemma 19: we work with the $\mathbb{Q}_p(1)$-quotient of the fundamental group introduced in section 2.4.1. and take basepoint $b = \infty^+$, and $R = \mathrm{Mat}_2(\mathbb{Q}_p)$. Then via the isomorphism $V \simeq V_1 \oplus V_2$,

$$\kappa(z - b) = (\kappa_1(f_1(z)), \kappa_2(f_2(z)) - \kappa_2((0,1)))$$

and

$$\overline{\Psi}_R(z)^{\mathrm{Sym}} = \kappa_1(f_1(z))^2 + \kappa_2(f_2(z) + (0,1))\kappa(f_2(z) - (0,1))$$

The points P_1 and P_2 form a basis of $H^1_f(G_T, V)$, and a section s is given by sending $(\mu_1\kappa_1(P_1), \mu_2\kappa_2(P_2))$ to

$$\mu_1^2[A(E_1 - O)(t_1, P_1)] - \mu_2(\mu_2 + 2\frac{\log_{E_2}((0,1))}{\log_{E_2}(P_2)})[A(E_2 - O)(t_2, P_2)]$$

Hence for any rational point z, we obtain the two linear relations

$$\log_{E_1}(f_1(z)) = \mu_1 \log_{E_1}(P_1)$$
$$\log_{E_2}(f_2(z)) = \mu_2 \log_{E_2}(P_2)$$

and a quadratic relation

$$[A(X)(b,z)] - 2\mu_1^2[A(E-O)(t,f_1(z))] - 2(\mu_2^2 - \frac{\log_{E_2}((0,1))}{\log_{E_2}(P_2)})[A(E-O)(t,f_2(z))] \in H^1(G_T, \mathbb{Q}_p(1))$$

Finally, $[A(X)(b,z)]$ is related to local heights as follows: recall the formula for $[A(X)(b,z)]$ given in chapter 1, Theorem :

$$\begin{aligned}[A(b,z)] = {} & [A(E_1-O)(t,f_1(z))] - \frac{1}{2}[A(E_2-O)(t,f_2(z)+(0,1))] \\ & - \frac{1}{2}[A(E_2-O)(t,f_2(z)-(0,1))] + \frac{1}{2}[A(E_2-O)(t,f_2(b)+(0,1))] \\ & + \frac{1}{2}[A(E_2-O)(t,f_2(b)-(0,1))] + \overline{\kappa_2(f_2(z))\kappa_2(f_2(b))}\end{aligned}$$

By [6] in the case $v = p$ and [4] for $v \neq p$, for an elliptic curve E and integral tangential basepoint t,

$$\mathrm{loc}_v([A(E-O)(t,P)]) = \lambda_{E,v}(P)$$

completing the proof. □

The possible values of β_v can be calculated using Silverman's algorithmic formula for local heights on elliptic curves [61], on in some cases by finding a nice model of E_1 and E_2.

4.1.1 First example

Let X denote the genus 2 curve given by

$$y^2 = x^6 - 4x^4 + 3x^2 + 1$$

Let E_1, E_2, f_1, and f_2 be as before. E_1 and E_2 both have Mordell-Weil rank 1. Since E_1 and E_2 have integral j-invariants, X has potential good reduction away from 2, and hence the quantity

$$2\lambda_{E_1,v}(x(f_1(z))) - \lambda_{E_2,v}(x(f_2(z)) + (0,1)) - \lambda_{E_2,v}(x(f_2(z)) - (0,1))$$

is identically zero for $v \neq 2, p$, $z \in X(\mathbb{Q}_v)$. Hence

$$\beta = 2\lambda_{E_1,2}(x(f_1(z))) - \lambda_{E_2,2}(x(f_2(z)) + (0,1)) - \lambda_{E_2,2}(x(f_2(z)) - (0,1)).$$

Computing heights on smooth models of E_1 and E_2 over finite extensions of $\mathbb{Q}_l$ shows

Proposition 10. *The possible values of β are*

$$\beta = \begin{cases} \log(2) & \text{if } v(x(z)) > 0, \\ -\frac{1}{3}\log(2) & \text{if } v(x(z)) = 0, \\ 2\log(2) & \text{if } v(x(z)) < 0, \end{cases}$$

Proof. Define β_1 and β_2 in $\mathbb{Q}$ by

$$2\lambda_{E_1,2}(x(f_1(z))) = \beta_1 \log(2)$$
$$\lambda_{E_2,2}(x(f_2(z)) + (0,1)) + \lambda_{E_2,2}(x(f_2(z)) - (0,1)) = \beta_2 \log(2).$$

As E_1 and E_2 have potential good reduction, the local heights may be computed by finding smooth models over a finite extension L of $\mathbb{Q}_2$, and using the formula

$$\lambda_{E_i,v}(P) = \min v(x(P)) \tag{4.1}$$

for the height of a point z in E_i at a prime v of L of good reduction, where x is the x-coordinate of a smooth $\mathcal{O}_L$-model of E_i.

Starting with the model $Y^2 = X^3 - 4X^2 + 3X + 1$, put

$$Y = 2u_1 + 2^{2/3}w_1 + 1,$$
$$X = 2^{2/3}w_1 + 1.$$

This defines a smooth model, which we denote by $\mathcal{E}_1$:

$$u_1^2 + 2^{2/3}u_1w_1 + u_1 = w_1^3 - 2^{1/3}w_1^2 - 2^{2/3}w_1$$

which now has good reduction.

4.1.1.1 An integral model for E_2

Given the $\mathbb{Q}_2$-model $Y^2 = X^3 + 3X^2 - 4X + 1$, we put

$$Y = 2u_2 + 2^{2/3}\alpha w_2 + \beta,$$
$$X = 2^{2/3}w_2 + \gamma,$$

where

$$\alpha = (1 + 2^{1/2})^{1/2}$$
$$\beta = (7 - 2^{3/2})^{1/2}$$
$$\gamma = 2^{1/2},$$

giving a smooth model $\mathcal{E}_2$:

$$u_2^2 + (7-2^{3/2})^{1/2}u_2^{2/3}(1+2^{1/2})u_2w_2 = w_2^3 + 2^{1/3}(1+2^{1/2})w_2^2 + 2^{-1/3}(1+3.2^{1/2}-(3+5.2^{1/2})^{1/2})w_2$$

which is integral because $v(1 + 3.2^{1/2} - (3 + 5.2^{1/2})^{1/2}) \geq 1/2$.

Let Δ_i denote the minimal discriminant of the curve E_i at 2 *over* $\mathbb{Q}_2$. Then

$$\lambda_{E_i,2}(P) = \min\{v(w_i(P)), 0\} - \frac{1}{6}v(\Delta_i)$$

Note that $v(\Delta_1) = v(\Delta_2) = 4$.

4.1.1.2 Possible values of β

$\beta_1 = \max\{\frac{2}{3} - v_2(x(f_1(z)) + 1), 0\} - \frac{2}{3}$.
If $v(x(f_1(z))) > 0$, then $\beta_1 = 0$.
If $x(f_1(z)) \in \mathbb{Z}_2^\times$ then $2|(x(f_1(z)) + 1)$, hence $\beta + 1 = -2/3$.
If $v(x) = -n < 0$, then $\beta_1 = 2n$.

$$\begin{aligned}\beta_2 \log(2) &= \lambda_{E_2}(f_2(z) + (0,1)) + \lambda_{E_2}(f_2(z) - (0,1)) \\ &= \lambda_{E_2}\left(\frac{-4x(f_2(z)) + 2 - 2y(f_2(z))}{x(f_2(z))^2}\right) + \lambda_{E_2}\left(\frac{-4x(f_2(z)) + 2 + 2y(f_2(z))}{x(f_2(z))^2}\right) \\ &= \max\left\{\frac{1}{6} - v_2\left(1 + 2^{1/2}\left(\frac{-2x(f_2(z)) + 1 - y(f_2(z))}{x(f_2(z))^2}\right)\right), 0\right\} - \frac{2}{3} \\ &\quad + \max\left\{\frac{1}{6} - v_2\left(1 + 2^{1/2}\left(\frac{-2x(f_2(z)) + 1 + y(f_2(z))}{x(f_2(z))^2}\right)\right), 0\right\} - \frac{2}{3}.\end{aligned}$$

Case 1: $v(x(f_2(z)) \leq 0$. Then $\beta_2 = -1$.
Case 2: $v(x(f_2(z)) > 0$. Let $x(f_2(z)) = 2^n u$, where necessarily $n \geq 2$. Then

$$y(f_2(z)) \equiv \pm(1 + (-2^{3n-1}u^3 + 3.2^{2n-1}u^2 - 2^{n+1}u)) \mod 2^{4n-2}$$

Hence

$$\begin{aligned}
&\lambda_{E_2}(f_2(z) + (0,1)) + \lambda_{E_2}(f_2(z) - (0,1)) \\
&= \max\left\{\frac{1}{6} - v_2\left(1 + 2^{1/2}\left(\frac{-2^{n+1}u + 1 - 1 + 2^{n+1}u - 3.2^{2n-1}u^2}{2^{2n}u^2}\right)\right), 0\right\} - \frac{2}{3} \\
&\quad + \max\left\{\frac{1}{6} - v_2\left(1 + 2^{1/2}\left(\frac{-2^{n+1}u + 1 + 1 - 2^{n+1}u + 3.2^{2n-1}u^2}{2^{2n}u^2}\right)\right), 0\right\} - \frac{2}{3} \\
&= 2n - 2.
\end{aligned}$$

This completes the proof of the proposition. □

4.1.1.3 Local heights at p

Searching for solutions in $X(\mathbb{Q}_p)$ to $\rho(z) = \beta$ for the three possible values above, one finds:

$]z[$	$x(z) \in \mathbb{Z}_p$	$z \in X(\mathbb{Q})$	$\rho(z)$
$(0, \pm 1)$	$O(5^7)$	$(0, \pm 1)$	$\log(2)$
	$3 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + O(5^7)$	$(\frac{5}{2}, \pm\frac{83}{8})$	$2\log(2)$
	$2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + O(5^7)$	$(-\frac{5}{2}, \pm\frac{83}{8})$	$2\log(2)$
$(1, \pm 1)$	$1 + O(5^8)$	$(1, \pm 1)$	$-\frac{1}{3}\log(2)$
	$1 + 4 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + 2 \cdot 5^6 + O(5^7)$		$-\frac{1}{3}\log(2)$
$(4, \pm 1)$	$4 + 4 \cdot 5 + 2 \cdot 5^4 + 5^5 + 2 \cdot 5^6 + O(5^7)$		$-\frac{1}{3}\log(2)$
	$4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 4 \cdot 5^6 + O(5^7)$	$(-1, \pm 1)$	$-\frac{1}{3}\log(2)$

4.1.2 Second example

Now take X to be be the bielliptic curve

$$X : y^2 = x^6 - 2x^4 - x^2 + 1$$

, and E_1 and E_2 to be

$$\begin{aligned}
E_1 &= x^3 - 2x^2 - x + 1 \\
E_2 &= x^3 - x^2 - 2x + 1
\end{aligned}$$

Again, E_1 and E_2 both have Mordell-Weil rank 1 and integral j-invariant. Moreover, E_1, E_2 both have good ordinary reduction at $p = 3$.

Let

$$\rho(z) = 2\lambda_{p,E_1}(f_1(z)) - 2\frac{\log_{E_1}(f_1(z))^2}{\log_{E_1}(z_1)^2}h_{E_1}(z_1) - \lambda_{p,E_2}(f_2(z) - (0,1)) - \lambda_{p,E_2}(f_2(z) + (0,1))$$
$$+ \frac{\log_{E_2}(f_2(z) - (0,1))^2 + \log_{E_2}(f_2(z) + (0,1))^2}{\log_{E_2}(z_2)^2}h_{E_2}(z_2) = \beta$$

Again, one may compute the possible values of β by hand. First note that $X(\mathbb{Q}_2)$ has no $\mathbb{Q}_2$ points whose x-co-ordinate has valuation zero (e.g. by checking mod 8).

Proposition 11. *For all z in $X(\mathbb{Q}_2)$,*

$$2\lambda_2(f_2(z)) - \lambda_2(f_1(z) + (0,1)) - \lambda_2(f_1(z) - (0,1)) = \begin{cases} \frac{8}{3}\log(2) & v(x(z)) < 0 \\ \frac{4}{3}\log(2) & v(x(z)) > 0 \end{cases}$$

Proof. We compute local heights on E_1 using [61]. First, note that the equation given above for E_1 isn't minimal at 2. A minimal equation is given by

$$y^2 = v^3 + v^2 - 2v - 1$$

(so $x = v+1$). E_1 has type II reduction, which means that the singular point mod 2 doesn't lift to a $\mathbb{Q}_2$ point. Hence

$$\lambda_2(f_1(z)) = 2\max\{0, -v(x(z))\}\log(2)$$

Now consider E_2. Here the original equation given for E_2 is minimal, and it has type IV reduction. The unique point of bad reduction is $(0,1)$. Again by Silverman [61], the formula for the local height at points (x_0, y_0) of bad reduction is given by

$$\lambda_2((x_0, y_0)) = -\frac{2}{3}(1 + v(y_0))$$

The x-co-ordinate of $(x,y) \pm (0,1)$ is given by $\frac{-2x+2\pm 2y}{x^2}$. Hence the possible contributions from

$$-\lambda_2(f_2(z) + (0,1)) - \lambda_2(f_2(z) - (0,1))$$

are

- $v(x(z)) > 0$: Then $v(x(f_2(z))) < 0$, and

$$v(y(f_2(z))) = \frac{3}{2}v(x(f_2(z)))$$

  So $v\left(\frac{-2x(f_2(z))+2\pm 2y(f_2(z))}{x(f_2(z))}\right) > 0$, i.e.

$$\lambda_2(f_2(z) + (0,1)) + \lambda_2(f_2(z) - (0,1)) = -\frac{4}{3}\log(2)$$

- $v(x(z)) < 0$: Then $v(x_0) \geq 2$, where $x_0 := x(f_2(z))$.

$$y(f_2(z)) \equiv \pm \left(1 + \frac{1}{2}(x_0^3 - x_0^2 - 2x_0) - \frac{1}{8}(x_0^3 - x_0^2 - 2x_0)^2\right) \mod 2x_0^2$$
$$\equiv \pm \left(1 - x_0 - x_0^2\right) \mod 2x_0^2$$

Hence one of $-2x_0 - 2 \pm 2y(f_2(z))$ has valuation 2, and the other has valuation $1 + 2v(x_0)$. Hence

$$\lambda_2(f_2(z)+(0,1)) + \lambda_2(f_2(z)-(0,1)) = -\frac{2}{3}\log(2) + \max\{0, 1 - v(x(z))\}\log(2)$$

Hence

$$2\lambda_2(f_2(z)) - \lambda_2(f_1(z) + (0,1)) - \lambda_2(f_1(z) - (0,1)) = \begin{cases} \frac{8}{3}\log(2) & v(x(z)) < 0 \\ \frac{4}{3}\log(2) & v(x(z)) > 0 \end{cases}$$

□

This gives the following set of solutions:

$]z[$	$x(z) \in \mathbb{Z}_p$	$z \in X(\mathbb{Q})$	$\rho(z)$
$(0, \pm 1)$	$2 \cdot 3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 + 3^7 + O(3^8)$	$(\frac{3}{2}, \pm\frac{1}{8})$	$\frac{8}{3}\log(2)$
	$3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 + 3^7 + O(3^8)$	$(-\frac{3}{2}, \frac{1}{8})$	$\frac{8}{3}\log(2)$
	$O(3^8)$	$(0, \pm 1)$	$\frac{4}{3}\log(2)$
$\infty^{\pm}$	$3^{-1} + 1 + 3^3 + 2 \cdot 3^4 + 2 \cdot 3^7 + O(3^8)$		0
	$2 \cdot 3^{-1} + 1 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 2 \cdot 3^5 + 2 \cdot 3^6 + O(3^8)$		0
	$\infty^{\pm}$	$\infty^{\pm}$	$-\frac{4}{3}\log(2)$

This gives that

$$X(\mathbb{Q}) = \left\{(0, \pm 1), \left(\frac{3}{2}, \pm\frac{1}{8}\right), \left(-\frac{3}{2}, \pm\frac{1}{8}\right), \infty^{\pm}\right\}.$$

4.1.3 An elementary approach

In this subsection we note that it is possible to give an elementary approach to proving Theorem 24. Namely, we give an elementary proof of the following proposition:

Proposition 12. *For almost all primes l,*

$$2\lambda_l(f_1(z)) - \lambda_l(f_2(z) - (0,1)) - \lambda_l(f_2(z) + (0,1)) \tag{4.2}$$

is zero, and for all $l \neq p$ it can only take finitely many values.

Following the argument of [5], this then gives a finite set of polynomial relations satisfied by the local heights on E_i and elliptic logarithms. Proof of finiteness is then reduced to showing directly that the Coleman functions involved in the equation of Theorem 24 are algebraically independent.

The proof of the proposition will follow straightforwardly from standard facts about local heights [62].

Theorem 25. *Let $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ be a Weierstrass equation with $\mathbb{Z}_l$-coefficients.*
(i): At all points z of good reduction with respect to this model,

$$\lambda_v(z) = \min\{v_l(x(z)), 0\} \log_p(l)$$

(ii): For any z not in $E[2]$,

$$\lambda_v([2]z) = 4\lambda(z) + 2v_l(2y(z) + a_1x(z) + a_3) \log_p(l)$$

Proof of Proposition 12. First suppose that l is an odd prime of good reduction for the models $y^2 = x^3+bx^2+ax+1$ and $y^2 = x^3+ax^2+bx+1$. Let z be a rational point of X, and let $w = (x_0, y_0) := f_2(z)$ be its image in E_2. We want to estimate the height of the points $w_1 = z - (0, 1)$ and $w_2 = z - (0, -1)$. Let $w_1 = (x_1, y_1)$ and $w_2 = (x_2, y_2)$. Then by a simple application of the addition formula we see $x_1 = \frac{bx_0+2-2y_0}{x_0^2}$ and $x_2 = \frac{bx_0+2+2y_0}{x_0^2}$. If $x_0 \in \mathbb{Z}_l^\times$ then $\min(v_l(x_1), 0) = 0$. If x_0 has negative valuation then it is easy to see $v_l(x_1)$ and $v_l(x_2)$ are positive. Finally, if $l|x_0$, then either $y_0 \equiv 1$ or $y_0 \equiv -1 \mod l$. In the first case, $v_l(x_2) = -2v_l(x_0)$. For x_1, note that

$$\begin{aligned} y_0 &\equiv 1 + \frac{1}{2}(bx_0 + ax_0^2) - \frac{1}{8}(bx_0 + ax_0^2)^2 \mod (x_0)^3 \\ &\equiv 1 + \frac{1}{2}bx_0 - \frac{1}{8}(b^2 - 4a)x_0^2, \end{aligned}$$

and hence $v_l(x_2) = 0$, since $b^2 - 4a$ is in $\mathbb{Z}_l^\times$. The second case is identical, swapping x_1 and x_2.

Hence in all cases

$$2 \max\{v_l(x_0), 0\} + \min\{v_l(x_1), 0\} + \min\{v_l(x_2)\} = 0$$

It follows that at all primes l at which $y^2 = x^3 + ax^2 + bx + 1$ defines a smooth $\mathbb{Z}_l$-model, (4.2) is identically zero, since

$$\max\{v_l(x_0), 0\} = -\min\{v_l(x(f_1(z), 0\}.$$

Now suppose that the Weierstrass equations $y^2 = x^3 + bx^2 + ax + 1$ and $y^2 = x^3 + ax^2 + bx + 1$ do not define smooth $\mathbb{Z}_l$-models. After passing to a finite extension $K|\mathbb{Q}_l$ we find a new Weierstrass equation over $\mathcal{O}_K$ with only finitely many points of bad reduction, such that the origin is a point of good reduction. Hence using part (ii) of the theorem stated above $\lambda_l(z) - \frac{1}{2}v_l(x_F(z))\log_p(l)$ can only take finitely many values, where $x_F(z)$ denotes the x-coordinate of z with respect to the new Weierstrass equation F. However, whenver elliptic curves E_1 and E_2 defined by Weierstrass equations $F_1(x_1, y_1) = 0$ and $F_2(x_2, y_2) = 0$ are isomorphic, there is an isomorphism of the form

$$x_2 = \alpha x_1 + \beta,$$
$$y_2 = \gamma y_1 + \delta x_1 + \epsilon$$

(see [48], Corollary 7.4.33), hence $\lambda_v(z) - \frac{1}{2}v_l(x_F(z))\log_p(l)$ can only take finitely many values.

□

4.2 Some bielliptic genus 2 curves of Mordell-Weil rank 4

Consider the following curves over $\mathbb{Q}(T)$:

$$\mathcal{X} : y^2 = x^6 + Tx^4 + Tx^2 + 1$$

$$\mathcal{E} : y^2 = x^3 + Tx^2 + Tx + 1$$

$$f_1, f_2 : \mathcal{X} \to \mathcal{E}$$

$$(x, y) \mapsto (x^2, y)$$

$$(x, y) \mapsto (x^{-2}, yx^{-3})$$

The following results are quoted from [47]:

- The fibres $X = X_a$ and $E = E_a$ at $T = a$ has good reduction away from $T = -1, 3$
- The point $(0, 1)$ is of infinite order on $\mathcal{E}$
- For a of height larger than 18, $(0, 1)$ has infinite order in E_a

The article [47] considers the case where a is chosen such that E has rank 1 and $(0, 1)$ is a Mordell-Weil generator. In this case Demyanenko's theorem gives an effective bound on the number of rational points, and the authors extend this to give a uniform bound for all such a.

We are interested in the situation where a is such that E has rank 2. Recall there is an isomorphism

$$V \simeq V_E^{\oplus 2}$$

Take U to be the quotient of U_2 with $[U, U] \simeq \mathrm{Sym}^2 V_E$, with basepoint $b = (0, 1)$. By Theorem 8 the localisation map for $H^1_f(G_T, U)$ is non-dense. The results of the previous chapters may be used to find an explicit formula for $X(\mathbb{Q}) \cap H^1_f(G_T, U)$, via the maps Ψ_R and Ψ_R^{cr}, where R is taken to be $\mathrm{Mat}_2(\mathbb{Q}_p)$.

4.2.1 Ψ_R and Ψ_R^{cr}

Let $\omega_E = dx/2y$ denote the canonical differential on E. Recall from section 3.3.3 we have a basis of $H^1_{dR}(X)$ given by the differentials of the second kind

$$\omega_0 = \omega, \quad \omega_1 = x\omega, \quad \omega_2 = \left(2x^4 - ax^2\right)\omega, \quad \omega_3 = x^3\omega.$$

ω_1 and ω_3 are obtained from pulling back differentials of E via f_1, and ω_0 and ω_2 are obtained from pulling back via f_2. At the level of cohomology, the automorphism

$$(x, y) \mapsto (x^{-1}, yx^{-3})$$

swaps $[\omega_0]$ and $[\omega_1]$ and swaps $[\omega_2]$ and $[\omega_3]$. Hence $\overline{\Psi}_R^{\mathrm{cr}}$ is given by

$$\begin{aligned} z \mapsto & (\int_b^z \omega_0)(\int_{b^-}^z \omega_1) - (\int_b^z \omega_1)(\int_{b^-}^z \omega_0) \\ &= (\int_b^z \omega_0)(\int_{b^-}^b \omega_1) - (\int_b^z \omega_1)(\int_{b^-}^b \omega_0) \\ &= (\int_b^z \omega_0)(\int_{b^-}^b \omega_1) \end{aligned}$$

- the last equality follows from

$$\int_{b^-}^b \omega_0 = \frac{1}{2}\int_{f_2(b)}^{f_2(b)} \omega_E = 0$$

Let $T_{E,0}$ and $T_{E,1}$ be a basis of V_E^{dR} dual to the basis ω_E and $x\omega_E$ on $H^1_{dR}(E)$. Then, using the description of the Hodge filtration given in Lemma 7, the map

$$\Psi_R^{\mathrm{cr,alt}} : X(\mathbb{Q}_p) \to \mathrm{Sym}^2 V_E^{dR}/F^0$$

is given by

$$z \mapsto (F_1(z) - \frac{1}{2}(\int_b^z \omega_0)(\int_{b^-}^b \omega_1))T_{E,0}^2 + F_2(z)T_{E,0}T_{E,1}$$

where

$$F_1(z) = \int_b^z (\omega_0\omega_1 - \omega_1\omega_0)$$

$$F_2(z) = 2\int_b^z (-\omega_0\omega_3 + a\omega_1\omega_2 + 2\omega_1\omega_4) + \frac{1}{2}(x(b) - x(z))$$
$$- (\int_b^z \omega_0)(\int_{b^-}^b \omega_3) + a(\int_b^z \omega_1)(\int_{b^-}^b \omega_2) + 2(\int_b^z \omega_1)(\int_{b^-}^b \omega_3)$$

(see section 3.5.5).

4.2.2 Computing Ψ_R^{alt} and Θ

We take P_1, P_2 to be points in $E(\mathbb{Q})$ generating $E(\mathbb{Q}) \otimes \mathbb{Q}$, such that $P_1 - (0,1)$ is torsion.

Define

$$\lambda_i : X(\mathbb{Q}) \to \mathbb{Q}_p$$

$(1 \leq i \leq 4)$ by

$$\log_E(f_1(z)) = \lambda_1(z)\log_E(P_1) + \lambda_2(z)\log_E(P_2) \tag{4.3}$$

$$\log_E(f_2(z)) = \lambda_3(z)\log_E(P_1) + \lambda_4(z)\log_E(P_2) \tag{4.4}$$

For example, $\lambda_i(z_0)$ is 1 when $i = 1$ and zero otherwise. We can give an explicit formula for a finite set containing $X(\mathbb{Q})$ in terms of the functions F_3, F_4 and $\int_b^z \omega_1$.

Theorem 26. *Suppose $w \in X(\mathbb{Q})$ is such that $\lambda_1(w)\lambda_4(w) - \lambda_2(w)\lambda_3(w) \neq 0$. Then $X(\mathbb{Q})$ is contained inside the set of z in $X(\mathbb{Q})_p$ satisfying*

$$F_2(w)(F_1(z) - \frac{1}{2}(\int_b^z \omega_0)(\int_{b^-}^b \omega_1)) = F_2(z)(F_1(z) - \frac{1}{2}(\int_b^w \omega_0)(\int_{b^-}^b \omega_1))$$

Proof. by section 2.4 the map

$$\overline{\Psi}^{\text{alt}} : X(\mathbb{Q}) \to \wedge^2 E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p$$

is given by

$$z \mapsto 2\lambda_1\lambda_4 - 2\lambda_2\lambda_3$$

By section 2.4 whenever $\mu_1 z_1 + \mu_2 z_2$ satisfies

$$z \mapsto \mu_i(\lambda_1(z_i)\lambda_4(z_i) - \lambda_2(z_i)\lambda_3(z_i) = 0$$

we have

$$\sum \mu_i F_2(z_i) = 0$$

and

$$\sum \mu_i (F_1(z) - \frac{1}{2}(\int_b^z \omega_0)(\int_{b^-}^b \omega_1)) = 0$$

□

4.2.3 Example

Let X denote the genus 2 curve

$$y^2 = x^6 + 31x^4 + 31x^2 + 1$$

. The elliptic curve $y^2 = x^3+31x^2+31x+1$ has Mordell-Weil rank 2. By elementary computation, the size of $X(\mathbb{Q})$ is at least 16:

$$X(\mathbb{Q}) \supset \{(0,\pm 1), (\pm 1, \pm 8), (\pm 7, \pm 440), (\pm\frac{1}{7}, \pm\frac{440}{343}), \infty^{\pm}\}$$

For the section s we find that $w = (-7, 440)$ has $\lambda_1\lambda_4 - \lambda_2\lambda_3 = 4$ $\lambda_3 = 1$ and $\lambda_4 = 3$. Hence by Theorem 26, for all z in $X(\mathbb{Q})$,

$$F_2(w)(F_1(z) - \frac{1}{2}(\int_b^z \omega_0)(\int_{b^-}^b \omega_1)) = F_2(z)(F_1(z) - \frac{1}{2}(\int_b^w \omega_0)(\int_{b^-}^b \omega_1))$$

The solutions to this equation are tabulated below:

$]z[$	$x(z) \in \mathbb{Z}_p$	$z \in X(\mathbb{Q})$
$(0,\pm 1)$	$O(3^8)$	$(0,\pm 1)$
	$2\cdot 3 + 2\cdot 3^3 + 2\cdot 3^5 + 3^7 + O(3^8)$	
	$3 + 2\cdot 3^2 + 2\cdot 3^4 + 2\cdot 3^6 + 3^7 + O(3^8)$	
$(1,\pm 2)$	$1 + O(3^8)$	$(1,\pm 8)$
	$1 + 2\cdot 3 + O(3^8)$	$(7,\pm 440)$
	$1 + 3 + 2\cdot 3^3 + 3^4 + 2\cdot 3^5 + 3^7 + O(3^8)$	$(\frac{1}{7}, \pm\frac{440}{343})$
$(2,\pm 2)$	$2 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + O(3^8)$	$(-7,\pm 440)$
	$2 + 3 + 2\cdot 3^2 + 3^4 + 2\cdot 3^6 + 3^7 + O(3^8)$	$(-\frac{1}{7}, \pm\frac{440}{343})$
	$2 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + 2\cdot 3^7 + O(3^8)$	$(-1,\pm 8)$
$\infty^{\pm}$	$2\cdot 3^{-1} + 1 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 3^7 + O(3^8)$	
	$3^{-1} + 1 + 2\cdot 3^5 + 2\cdot 3^6 + 3^7 + O(3^8)$	
	$\infty^{\pm}$	$\infty^{\pm}$

Hence some of the solutions appear not to come from rational points. It would be of interest to see if one can further refine the set of solutions by using the the $\mathbb{Q}_p(1)^{\oplus 2}$ quotient of U_2.

Bibliography

[1] F. Andreatta, A. Iovita, and M. Kim. A p-adic non-abelian criterion for good reduction of curves. 2013.

[2] M. Artin. Algebraic approximation of structures over complete local rings. *Publications Mathématiques de l'IHES*, 36(1):23–58, 1969.

[3] M. Asada, M. Matsumoto, and T. Oda. Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve. *Journal of Pure and Applied Algebra*, 103(3):235–283, 1995.

[4] J. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves. *arXiv preprint arXiv:1209.0640*, 2012.

[5] J S Balakrishnan, A Besser, and J S Müller. p-adic height pairings and integral points on hyperelliptic curves. *arXiv preprint arXiv:1302.2944*, 2013.

[6] J.S. Balakrishnan and A. Besser. Coleman-Gross height pairings and the p-adic sigma function. *J. Reine Angew. Math.*, 2013. to appear.

[7] J.S. Balakrishnan, K.S. Kedlaya, and M. Kim. Appendix and erratum to "Massey products for elliptic curves of rank 1". *J. Amer. Math. Soc.*, 24(1):281–291, 2011.

[8] K Bannai. Rigid syntomic cohomology and p-adic polylogarithms. *Journal fur die Reine und Angewandte Mathematik*, 529:205–237, 2000.

[9] K Bannai. Syntomic cohomology as a p-adic absolute hodge cohomology. *Mathematische Zeitschrift*, 242(3):443–480, 2002.

[10] K Bannai. Specialization of the p-adic polylogarithm to p-th power roots of unity. *Doc. Math.*, Extra Vol.:73–97, (2003).

[11] K Bannai and G Kings. p-adic elliptic polylogarithm, p-adic Eisenstein series and Katz measure. *American journal of mathematics*, 132(6):1609–1654, 2010.

[12] P Berthelot. *Cohomologie rigide et cohomologie rigide à supports propres.* Université de Rennes 1. Institut de Recherche Mathématique de Rennes [IRMAR], 1996.

[13] A. Besser. Coleman integration using the Tannakian formalism. *Math. Ann.*, 322(1):19–48, 2002.

[14] A. Besser. The p-adic height pairings of Coleman-Gross and of Nekovář. In *Number Theory*, volume 36 of *CRM Proceedings & Lecture Notes*, pages 13–25. American Mathematical Society, 2004.

[15] S. Bloch and K. Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[16] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2. Cambridge University Press, Cambridge, 1996.

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

[18] K. T. Chen. Algebras of iterated path integrals and fundamental groups. *Trans. Amer. Math. Soc.*, 156:359–379, 1971.

[19] B Chiarellotto and B Le Stum. F-isocristaux unipotents. *Compositio Mathematica*, 116(01):81–110, 1999.

[20] J. Coates and M Kim. Selmer varieties for curves with cm jacobians. *Kyoto Journal of Mathematics*, 50(4):827–852, 2010.

[21] R Coleman and A Iovita. Hidden structures on semistable curves.

[22] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[23] R. F. Coleman and B. H. Gross. p-adic heights on curves. In *Algebraic Number Theory – in honor of K. Iwasawa*, volume 17 of *Advanced Studies in Pure Mathematics*, pages 73–81, 1989.

[24] I Dan-Cohen and S Wewers. Explicit Chabauty–Kim theory for the thrice punctured line in depth 2. *Proceedings of the London Mathematical Society*, 110(1):133–171, 2015.

[25] H Darmon, V Rotger, and I Sols. Iterated integrals, diagonal cycles, and rational points on elliptic curves.

[26] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbb{Q}$, number 16 in Publ. MRSI, pages 79–297, 1989.

[27] P Deligne and AB Goncharov. Groupes fondamentaux motiviques de tate mixte. Technical report, math/0302267, 2003.

[28] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, Berlin, 1973. Springer.

[29] Pierre Deligne. Équations différentielles à points singuliers réguliers. *Lecture Notes in Math.*, 163, 1970.

[30] R. Kiehl E. Freitag. *Etale Cohomology and the Weil Conjectures*, volume 13. Springer, 1988.

[31] J S Ellenberg. Upper bounds for the growth of mordell-weil ranks in pro-p towers of jacobians. *arXiv preprint arXiv:1001.4266*, 2010.

[32] M Flach. A finiteness theorem for the symmetric square of an elliptic curve. *Inventiones mathematicae*, 109(1):307–327, 1992.

[33] E V Flynn and J L Wetherell. Finding rational points on bielliptic genus 2 curves. *manuscripta mathematica*, 100(4):519–533, 1999.

[34] E V Flynn and J L Wetherell. Covering collections and a challenge problem of serre. *Acta Arith.*, 98:2, 2001.

[35] J-M Fontaine and Bernadette Perrin-Riou. Autour des conjectures de bloch et kato. i, cohomologie galoisienne. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 313(5):189–196, 1991.

[36] AB Goncharov. Mixed elliptic motives. galois representations in arithmetic algebraic geometry (durham, 1996), 147–221. *London Math. Soc. Lecture Note Ser*, 254.

[37] A. Grothendieck. *Groupes de monodromie en géométrie algébrique. I.* Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288.

[38] M Hadian. Motivic fundamental groups and integral points. *Duke Mathematical Journal*, 160(3):503–565, 2011.

[39] U Jannsen. On the l-adic cohomology of varieties over number fields and its galois cohomology. In *Galois Groups over* $\mathbb{Q}$, pages 315–360. Springer, 1989.

[40] K Kato. Logarithmic structures of fontaine-illusie. *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 191–224, 1989.

[41] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[42] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[43] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23:725–747, 2010.

[44] M Kim. Tangential localization for selmer varieties. *Duke Mathematical Journal*, 161(2):173–199, 2012.

[45] M Kim. Diophantine geometry and non-abelian reciprocity laws i. *arXiv preprint arXiv:1312.7019*, 2013.

[46] M Kim and A Tamagawa. The l-component of the unipotent albanese map. *Mathematische Annalen*, 340(1):223–235, 2008.

[47] L Kulesz, G Matera, and É Schost. Uniform bounds on the number of rational points of a family of curves of genus 2. *Journal of Number Theory*, 108(2):241–267, 2004.

[48] Q Liu and R Erné. *Algebraic geometry and arithmetic curves*, volume 6. Oxford university press Oxford, 2002.

[49] D. Mumford. *Abelian varieties.* Published for the Tata Institute of Fundamental Research, Bombay, 1970. Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[50] J. Nekovář. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, pages 127–202. Birkhäuser Boston, Boston, MA, 1993.

[51] J Nekovár. On the p-adic height of heegner cycles. *Mathematische Annalen*, 302:609–686, 1995.

[52] T Oda. A note on ramification of the galois representation on the fundamental group of an algebraic curve, ii. *Journal of Number Theory*, 53(2):342–355, 1995.

[53] M C Olsson. *Towards non-abelian p-adic Hodge theory in the good reduction case.* American Mathematical Soc., 2011.

[54] M. van der Put. The cohomology of Monsky and Washnitzer. *Mémoires de la Société Mathématique de France Sér. 2*, 23:33–59, 1986.

[55] D Quillen. Rational homotopy theory. *Annals of Mathematics*, pages 205–295, 1969.

[56] A J Scholl. Height pairings and special values of L-functions. In *U. Jannsen, SL Kleiman, J.–P. Serre, "Motives", Proceedings of the Research Conference on Motives held July*, pages 571–598, 1991.

[57] J-P. Serre. *Algebraic groups and class fields.* Springer-Verlag, New York, 1988. Translated from the French.

[58] J-P Serre. Lectures on the Mordell-Weil theorem. *Aspects of Mathematics*, 1989.

[59] J-P Serre. *Galois cohomology.* Springer, 2002.

[60] J-P. Serre and J. T. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[61] J H Silverman. Computing heights on elliptic curves. *Mathematics of computation*, 51(183):339–358, 1988.

[62] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.

[63] J. L. Wetherell. Bounding the number of rational points on certain curves of high rank. *UC Berkeley Ph.D. thesis*, 1997.