The fine Selmer group and height pairings

Chris Wuthrich

Trinity College

A dissertation submitted for the degree of Doctor of Philosophy at the University of Cambridge

May 2004

Abstract

This thesis is concerned with a particular question in the arithmetic of elliptic curves related to Iwasawa theory. Let E/K be an elliptic curve over a number field and let p be any odd prime. The p-primary Selmer group $\mathcal{S}(E/K)$ is then defined to be a certain subgroup of the first Galois cohomology group $H^1(K, E(p))$ with values in the p-primary torsion group of E. From Kummer theory, we know that it contains the image of the Mordell-Weil group $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. If certain standard conjectures are valid then the image has finite index in $\mathcal{S}(E/K)$. The Iwasawa-theory of the Selmer group $\mathcal{S}(E/_\infty K)$ over a $\mathbb{Z}_p$-extension $_\infty K$ of K is well understood if the reduction of E at p is good and ordinary. Via its Euler characteristic formula, it provides some information on the growth of the rank of the Mordell-Weil group in the $\mathbb{Z}_p$-extension.

We propose here the study of a certain subgroup $\mathcal{R}(E/K)$ of the Selmer group, called the fine Selmer group, which is obtained by imposing stronger conditions at the places above p. On this subgroup, one can construct a p-adic height pairing that can be computed using p-adic sigma function. Assuming the non-degeneracy of this pairing, we deduce a formula for the Euler characteristic of $\mathcal{R}(E/_\infty K)$ and many interesting results on the behaviour of the fine Selmer group in $\mathbb{Z}_p$-extensions. One of the advantages of the fine version of the Selmer group is that we do not have to make any assumptions on the type of reduction. Many numerical examples are included.

Declaration

This dissertation is not substantially the same as any I have submitted for a degree or a diploma or any other qualification at any other university. It is the result of my own work and includes nothing which is the outcome of work done in collaboration.

Contents

List of Tables

Introduction

Some miracles never cease to amaze me. One of them is certainly Weil's idea that the number of points defined over any finite field on an algebraic variety can be calculated once it is known for a few small extensions of its field of definition. The idea behind it is the zeta-function of the variety, which turns out to be a rational function. Tate considered a finer question in his Bourbaki talk [Tat66] on the conjecture of Birch and Swinnerton-Dyer. In order to motivate and illustrate the idea of Iwasawa theory in the arithmetic of elliptic curves over number fields we are going to describe quickly how Tate was able to prove a large part of the geometric analogue of the famous conjecture.

Let K be a function field of a curve over a finite field with q elements and let E/K be an elliptic curve. Geometrically this yields an elliptic surface $\mathcal{E}$ defined over the finite field. Suppose that p is a prime number different from the characteristic of K. Denote by $P_2(T)$ the characteristic polynomial of the action of the Frobenius endomorphism on the group $H^2_{\text{ét}}(\bar{\mathcal{E}}, \mathbb{Q}_p)$. This polynomial is one of the factors appearing in the zeta-function of $\mathcal{E}$. Tate starts by reformulating the conjecture of Birch and Swinnerton-Dyer in terms of the polynomial $P_2(T)$ and the geometric invariants of $\mathcal{E}$. A part of the reformulated statement is that, the Brauer group $\operatorname{Br}\mathcal{E} = H^2_{\text{ét}}(\mathcal{E}, \mathbb{G}_m)$, which is the analogue of the Tate-Shafarevich group, is finite. Assuming that the p-primary part of $\operatorname{Br}\mathcal{E}$ is finite, Tate is able to show that the order of vanishing of $P_2(T)$ at $T = q^{-1}$ is equal to the rank of the Néron-Severi group $\operatorname{NS}(\mathcal{E})$ and the leading coefficient is equal to

$$\pm q^{\text{some power}} \cdot \frac{\det(D_i.D_j) \cdot \#\operatorname{Br}\mathcal{E}}{(\operatorname{NS}(\mathcal{E})_{\text{tors}})^2}$$

where the first factor in the numerator is the determinant of the intersection form on the Néron-Severi group. For the proof of this formula one can restrict one's attention to the p-primary parts. Tate then analyses the kernels and cokernels of

the maps in the following diagram (5.12 in [Tat66]).

$$\begin{array}{ccccc} \mathrm{NS}(\mathcal{E})\otimes\mathbb{Z}_p & \xrightarrow{h} & \mathrm{Hom}(\mathrm{NS}(\mathcal{E}),\mathbb{Z}_p) & \cong & \mathrm{Hom}(\mathrm{NS}(\mathcal{E})\otimes\mathbb{Q}_p/\mathbb{Z}_p,\mathbb{Q}_p/\mathbb{Z}_p) \\ \downarrow b & & & & \uparrow \\ H^2_{\text{ét}}(\bar{\mathcal{E}},T_p\mu)^\Gamma & \longrightarrow & H^2_{\text{ét}}(\bar{\mathcal{E}},T_p\mu)_\Gamma & \xrightarrow{\cong} & \mathrm{Hom}(H^2_{\text{ét}}(\bar{\mathcal{E}},\mu(p))^\Gamma,\mathbb{Q}_p/\mathbb{Z}_p) \end{array}$$

Here $\mu(p)$ are the p-power roots of unity and Γ is the absolute Galois group of the finite field of constants of K. The map h is the non-degenerate intersection pairing on $\mathrm{NS}(\mathcal{E})$, while the vertical maps come from the Hochschild-Serre spectral sequence and the natural map from $\mathrm{NS}(\mathcal{E})$ into the second étale cohomology. On the bottom, we have the natural map induced by the identity, followed by the isomorphism defined via Poincaré duality.

Since the work of Iwasawa on the growth of the class group of a number field in a $\mathbb{Z}_p$-extension, we know how to use similar ideas when working over number fields. Now, let E be an elliptic curve over a number field K and let p be an odd prime number. Let Γ be the Galois group of a $\mathbb{Z}_p$-extension ${}_\infty K$ of K. Suppose that the Tate-Shafarevich group $Ш(E/K)$ is finite. Rather than studying the number of points on a variety, we want to look at the growth of the Mordell-Weil group. In Iwasawa theory one is able to define in certain circumstances a power series with coefficients in $\mathbb{Z}_p$ which encodes this information similar to how the zeta-function does for varieties over finite fields.

In the now classical approach one finds an arithmetic analogue to the geometric situation; the Néron-Severi group is replaced by the Mordell-Weil group $E(K)$, and the Selmer group $\mathcal{S}(E/K)$ (see section I.1 for the detailed definitions) takes the place of the second étale cohomology group. Poincaré duality can be substituted by global duality as explained in Tate's article. Schneider [Sch85] and Perrin-Riou [PR82] were the first to find a pairing, called the p-adic height pairing, that would replace the geometric intersection form but only under the restriction that the reduction of E at all places above p is good and ordinary. Also the map b will have finite kernel and cokernel only if one assumes this additional hypothesis; this is called the control theorem of Mazur. Let Reg be the p-adic regulator defined to be the determinant of the p-adic height pairing. It is conjectured, but unknown execpt for very special cases, that the pairing is non-degenerate if the $\mathbb{Z}_p$-extension is cyclotomic.

The beautiful result that can be deduced following the ideas of Tate is that the characteristic power series $f_\mathcal{S} \in \mathbb{Z}_p[\![T]\!]$ of the dual of the Selmer group $\mathcal{S}(E/_\infty K)$ over ${}_\infty K$ has a zero of order at least the rank r of $E(K)$. If the p-adic height is non-degenerate and the Tate-Shafarevich group is known to be finite then the order of vanishing is equal to r and that the first coefficient (up to a unit in $\mathbb{Z}_p^\times$) of $f_\mathcal{S}$ is given

by

$$\frac{\mathrm{Reg}}{p^r} \cdot \frac{\prod_{v|p} N_v^2 \cdot \prod_v c_v \cdot \#Ш(E/K)(p)}{(\#E(K)_{\mathrm{tors}})^2}. \tag{1}$$

The notation N_v stands for the number of points in the reduction of the curve E at a place v above p and $\prod c_v$ is the product of the Tamagawa numbers. Hence the first coefficient and so an important part of the information on the growth of the Mordell-Weil group can be computed with only the invariants from E over K. It is truly miraculous to me, even after three years of Ph.D. on the subject, that one can deduce very often the full structure of $\mathcal{S}(E/_\infty K)$, at least up to something finite. For the classical results on the Selmer group, we refer the reader to [CoSu00], [cetraro99], [Gre99] and [PR92].

Although, just as for Tate's theorem, the finiteness of $Ш(E/K)$ can not be deduced in this way but has to be assumed. Unlike for the geometric case, the characteristic power series can not be linked so easily to the L-function; in fact the "main conjecture" states that f_s is equal to the p-adic L-function.

The fine Selmer group

In this thesis, we consider a subgroup of the Selmer group $\mathcal{S}(E/K)$ and of the Mordell-Weil group $E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Following the terminology in [CoSu], we call[1] it the fine Selmer group $\mathcal{R}(E/K)$ and the fine Mordell-Weil group $\mathcal{M}(E/K)$, respectively. They are defined by imposing more restrictive conditions on the elements of $\mathcal{S}(E/K)$ at all places above p. In particular $\mathcal{M}(E/K)$ is the kernel of the localisation map from $E(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ to the product of $E(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ for all places v dividing p. It is a rather small subgroup. For elliptic curves over $\mathbb{Q}$, the fine Mordell-Weil group is non-trivial only if the rank of $E(\mathbb{Q})$ is strictly larger than one. We propose the fine Mordell-Weil group as another analogue of the Néron-Severi group and the fine Selmer group $\mathcal{R}(E/K)$ might replace the étale cohomology groups mentioned above. It is striking that the analogy works much better and we can drop all conditions on the reduction of E at the places above p. E.g. it is known that the Néron-Severi group $\mathrm{NS}(\bar{\mathcal{E}})$ is still a finitely generated group, while it is known that the Mordell-Weil group $E(_\infty K)$ can very well have infinitely many generator if for instance the reduction at p is supersingular, unlike for the fine Mordell-Weil group $\mathcal{M}(E/_\infty K)$ where we expect that it is still cofinitely generated according to the widely believed weak Leopoldt conjecture VI.9. This goes even further. We also know from étale cohomology that the group $H^2_{\text{ét}}(\mathcal{E}, \mathbb{Z}_p)$ is of finite $\mathbb{Z}_p$-rank. In our case it is a conjecture of Coates and

[1] other names found in the literature include "strict" or "restricted Selmer group" or even "a certain subgroup"

Sujatha [CoSu] that $\mathcal{R}(E/_\infty K)$ is cofinitely generated, at least if $_\infty K$ is the cyclotomic $\mathbb{Z}_p$-extension of K. See conjecture VI.12.

We shall give now an overview of the structure of this thesis. A first result is the control theorem I.15 for the fine Selmer group which provides us with a pseudo-isomorphism b from $\mathcal{R}(E/K)$ to $\mathcal{R}(E/_\infty K)^\Gamma$. In section I.5, a p-adic height pairing is constructed on the fine Selmer group via extensions of the Tate-module T_pE by $T_p\mu$. It is a generalisation of the canonical p-adic height as constructed in [PR92] and it was previously used in [PR95] and [PR93b]. Its non-degeneracy is conjectured if the $\mathbb{Z}_p$-extension is cyclotomic. Next we show in proposition I.23 that there is a diagram completely analogous to the diagram in Tate's article.

Several consequences can be deduced under the hypothesis that the pairing is non-degenerate. First of all, in section I.7, the dual of $\mathcal{R}(E/_\infty K)$ is shown to be a torsion module over the Iwasawa algebra $\Lambda(\Gamma) = \Lambda$ and its characteristic series $f_\mathcal{R}$ has a zero of order equal to the rank of $\mathcal{R}(E/K)$. We proceed in theorem I.33 to compute the first coefficient of $f_\mathcal{R}$, the so-called Euler characteristic of the dual of $\mathcal{R}(E/_\infty K)$. This formula will be simplified substantially in theorem II.4 under the assumption that the fine Tate-Shafarevich group, the fine analogue of $Ш(E/K)$, is finite. The fine Tate-Shafarevich group, denoted by $\text{Ж}(E/K)$, is a subgroup of $Ш(E/K)$ and the difference is discussed in the second chapter, where some numerical computations and examples are also presented.

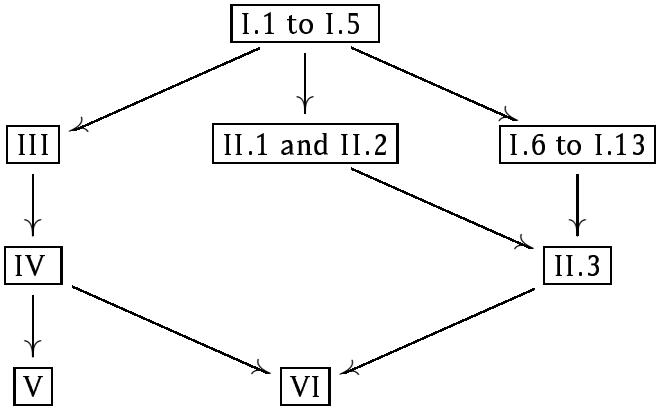
In order to compute explicitely the Euler characteristic of the fine Selmer group, we need to link the algebraically defined height to an analytic height using sigma functions. In chapters III and IV we derive the analytic formula for the p-adic height pairing on the fine Mordell-Weil group; first for a general abelian variety and then for an elliptic curve. We then show that it is the limit of naïve p-adic heights in theorem IV.8, involving only the logarithms of numerators of the x-coordinate on E in a Weierstrass equation.

In chapter V, we look at the variation of the p-adic height on the fine Selmer as a point varies in a family of elliptic curves. It turns out that the variation is p-adically analytic; see theorem V.7. This can be used to prove the non-degeneracy of the p-adic height on the fine Selmer group on many curves at once.

The final chapter is devoted to explanations and presentations of the numerical computations. In the detailed description of some examples of elliptic curves E defined over $\mathbb{Q}$, we show how the formula for the Euler characteristic can be used to determine the characteristic power series for many primes p. In fact, it is often the case that one can prove that $f_\mathcal{R}$ is a unit, and hence $\mathcal{R}(E/K)$ has finite index in $\mathcal{R}(E/_\infty K)$. According to the conjecture VI.15, this should actually be true for all but a

finite number of primes. But $f_{\mathcal{R}}$ is not always a unit; in proposition VI.8 we present an example in which $f_{\mathcal{R}}$ is divisible by the distinguished polynomial $3 + 3T + T^2$. Before the table with the complete numerical results, we present in section VI.4 some conjectures and conclusions.

Leitfaden



Acknowledgement

I would like to express my warmest thanks to my supervisor, John Coates, for his expert guidance in the course of my studies. Out of the many people whom I am indebted to for their help and support, their coffee-breaks and Grasdachschmalspur-philosophiestunden, their hospitality in Genève, Paris and London, I would like to mention specially Paola Argentin, Lucie Campos, Hannu Härkönnen, Sylvia Guibert, Dinesh Markose, Tony Scholl, Gianluigi Sechi, Mike Shuter and Christopher Voll.

Finally, I acknowledge the financial support of the British Council and Trinity College.

Chapter I

Iwasawa theory of the fine Selmer group

> I owe the discovery of Uqbar to the conjunction of a mirror and an encyclopedia.
> Tlön, Uqbar, Orbis Tertius; Jorge Luis Borges.

I.1 Definition and notations

I.1.1 Notations

Let us fix first of all some notation and the general setting we are working in. During the whole chapter, A will be an abelian variety defined over a fixed number field K, with its origin O. Everything we consider is always relative to a prime number p which we will assume to be odd; but no condition on the type of reduction of A at p is made. The dual variety is written $\check{A}$. The ring of integers of K is $\mathcal{O}$ and $\mathcal{O}_\Sigma$ the ring of Σ-integers.

As usual in this situation, a set Σ of places of K is chosen. It must contain all places where A has bad reduction, all places at infinity, as well as all places above p. The symbol $\oplus$ will frequently denote the sum over all places v in Σ. Many things will depend on the choice of this set, but the end results, of course, should be independent. The set of places above p is denoted by $\Sigma(p)$ and the remaining places in Σ by $\Sigma(\nmid p)$. When talking about an extension L of K, we keep the notation Σ for the places in L lying above K.

For the notation of Galois cohomology, we use the following symbols. Let L be any extension of K. The Galois group of the maximal extension of L that is unramified at all places outside Σ is written $G_\Sigma(L)$. If M is a $G_\Sigma(L)$-module, we write $H^i_\Sigma(L,M)$ for the i^{th} restricted Galois cohomology group $H^i(G_\Sigma(L),M)$. If $L=K$, the abbreviation $H^i_\Sigma(M)=H^i_\Sigma(K,M)$ is used. If w is a place of L, then L_w is the completion of L at w; if L is an infinite extension of K, it is understood to be the union of completions of all finite subextension of L. For the local fields, $H^i(L_w,M)$ is the cohomology

with respect to the absolute Galois group of L_w. Suppose v is a place in K, the abbreviation

$$H^i(L_v, M) = \bigoplus_{w|v} H^i(L_w, M)$$

is used whenever M is a module over the absolute Galois group of K_v. All notations for Galois cohomology are as close as possible to the ones used in [NeScWi00]. We will also use the same conventions on the sign of connecting maps.

Often, we will work with a fixed $\mathbb{Z}_p$-extension (see I.2.2). It will be denoted by ${}_\infty K : K$ and its Galois group by Γ. The field ${}_n K$ is the subextension of degree p^n over K. The Galois groups $\mathrm{Gal}({}_\infty K : {}_n K)$ and $\mathrm{Gal}({}_n K : K)$ are denoted by ${}_n\Gamma$ and ${}_n G$, respectively. We try to be consistent and to write all indices indicating the layer in the $\mathbb{Z}_p$-extension on the left. In this way we should be able to avoid things like $\mathbb{Q}_{5,3}$.

Finally, the Pontryagin dual of M is denoted[1] by $\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$. A map between two $\mathbb{Z}_p$-modules, or between duals of $\mathbb{Z}_p$-modules, is called a pseudo-isomorphism if both, kernel and cokernel, are finite. Given an abelian group, a group scheme or a $G_\Sigma(K)$-module M, we use $M[m]$ to denote the m-torsion and M/m for the quotient M/mM; e.g. $K^\times/m$ is the quotient of $K^\times$ by $(K^\times)^m$. The following limits are used frequently: The p-primary torsion part[2] $M(p) = \varinjlim M[p^k]$, the Tate-module, $T_p M = \varprojlim M[p^k]$, the p-adic completion, $M^\star = \varprojlim M/p^k M$ and finally the limit $M \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim M/p^k M$. The notation $\mathbb{G}_m$ is reserved for the multiplicative group and $\mu[m]$ for the m^{th} roots of unity.

I.1.2 The fine Selmer group

Let k be a positive integer. Kummer theory for the abelian variety A provides us with an injection of $A(K)/p^k A(K)$ into the first cohomology group $H^1_\Sigma(A[p^k])$. The classical Selmer group S^k is then defined to be the subgroup of cocycles whose restrictions to $H^1(K_v, A[p^k])$ are contained in the image of the local Kummer map for all places v in Σ. So it is the following kernel

$$0 \longrightarrow S^k \longrightarrow H^1_\Sigma(A[p^k]) \longrightarrow \bigoplus_{v\in\Sigma} H^1(K_v, A)[p^k].$$

In this way, $A(K)/p^k A(K)$ maps into S^k and the latter can be calculated (at least in principle) in order to find an upper bound on the rank of the Mordell-Weil group $A(K)$.

[1] Except for the formal group $\widehat{E}$ of an elliptic curve.

[2] This should not lead to confusions because we never use twists.

We will consider in this thesis a smaller group, the *fine Selmer group*. At the finite level, it is defined as the following kernel

$$0 \longrightarrow R^k \longrightarrow S^k \longrightarrow \bigoplus_{v|p} H^1(K_v, A[p^k]).$$

If we emphasise the dependence on A or K, we will write $R^k(A/K)$. The notation $\check{R}^k$ stands for the fine Selmer group $R^k(\check{A}/K)$ for the dual abelian variety.

Most of the time, we actually consider the limit versions. First, take the limit $\mathbb{S} = \varinjlim S^k$ of the classical Selmer group S^k with respect to the maps induced by the inclusions $A[p^k] \hookrightarrow A[p^{k+1}]$. The fine discrete Selmer group is the group $\mathcal{R} = \varinjlim R^k$. It can be defined directly as the kernel of

$$0 \longrightarrow \mathcal{R} \longrightarrow H^1_\Sigma(A(p)) \longrightarrow \bigoplus_{v\in\Sigma} H^1(K_v, A(p)).$$

The reason why we were allowed to replace the sum to be over all places in Σ rather than over only the places above p is the following. We have to show that the kernel of $H^1(K_v, A(p)) \longrightarrow H^1(K_v, A)(p)$ is trivial. This kernel is equal to $A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ by Kummer theory. The claim follows now from the fact that $A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is trivial if v does not divide p because $A(K_v)$ contains a subgroup of finite index that is isomorphic to a product of $\mathcal{O}_v$.

The compact fine Selmer group is defined to be the projective limit $\mathfrak{R} = \varprojlim R^k$ where the limit follows the multiplication by p from $A[p^{k+1}]$ to $A[p^k]$. Here we can define an even smaller group by

$$0 \longrightarrow \mathfrak{R}_\Sigma \longrightarrow H^1_\Sigma(T_pA) \longrightarrow \bigoplus_{v\in\Sigma} H^1(K_v, T_pA).$$

It turns out that

Lemma I.1. *$\mathfrak{R}_\Sigma$ has finite index in $\mathfrak{R}$.*

Proof. Indeed, there is a sequence

$$0 \longrightarrow \mathfrak{R}_\Sigma \longrightarrow \mathfrak{R} \longrightarrow \bigoplus_{v\in\Sigma(\nmid p)} H^1(K_v, T_pA).$$

Note that the group $T_pH^1(K_v, A)$ is dual to the group $\check{A}(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ under local Tate duality (see [Tat58] and [NeScWi00, Theorem 7.2.6]). If v does not lie above p this group is trivial and so we conclude that the local term on the right of the sequence is equal to p-adic completion $A(K_v)^\star$. This is a finite group by the same argument as before, namely that there is a subgroup isomorphic to a product of $\mathcal{O}_v$. □

When these groups are considered over an extension L of K, they are always defined as a direct limit ranging over all finite subextensions, e.g.

$$0 \longrightarrow \text{Ш}_\Sigma(A/L) \longrightarrow H^1_\Sigma(L, T_pA) \longrightarrow \bigoplus_{v\in\Sigma} H^1(L_v, T_pA)$$

with the convention on the notation previously made.

I.2 Tools

Before we can start to work we need to put the tools in place that we are going to use later. So this section is simply a collection of facts that will be useful. It contains hardly any proofs but references to the relevant literature.

I.2.1 Global duality

As explained in Tate's article [Tat66], the arithmetic analogue of the Poincaré duality in étale cohomology is the "global duality". It was first discovered by Cassels in the special case of an elliptic curve (see [Cas64]) and it was announced in full generality by Tate in [Tat63]. A full proof is presented in the book [NeScWi00, VIII.6]. A good explanation for the case of an elliptic curve is given in [Fis03].

The starting point is the

Proposition I.2. *Let M be a finite p-torsion $G_\Sigma(K)$-module. Let $M' = \mathrm{Hom}(M, \mu(p))$ be the Cartier dual. Then the kernels of the localisation maps*

$$H^1_\Sigma(M) \longrightarrow \oplus H^1(K_v, M)$$
$$H^2_\Sigma(M') \longrightarrow \oplus H^2(K_v, M')$$

are dual to each other.

Remember that $\oplus$ denotes the sum over all places v in Σ. The construction of the duality and the proof of the proposition can be found in [NeScWi00, Theorem 8.6.8]. The explicit description of the isomorphism will be used in I.6.2 and is the starting point for many pairings such as Flach's generalisation [Fla90].

We deduce for our case the following first corollary.

Corollary I.3. *The compact group $\check{\text{Ш}}_\Sigma = \text{Ш}_\Sigma(\check{A}/K)$ is dual to $H^2_\Sigma(A(p))$, i.e. there is an isomorphism*

$$f : \check{\text{Ш}}_\Sigma \xrightarrow{\cong} \widehat{H^2_\Sigma(A(p))} \tag{I.1}$$

and the discrete fine Selmer group fits into the exact sequence

$$0 \longrightarrow A(K)(p) \longrightarrow \oplus A(K_v)(p) \longrightarrow \widehat{H^2_\Sigma(T_p\check{A})} \longrightarrow \mathcal{R} \longrightarrow 0 \tag{I.2}$$

Proof. Note that $A[p^k]' = \check{A}[p^k]$ via the Weil-pairing. The surjectivity in (I.1) follows from the fact that the local cohomology groups $H^2(K_v, A(p))$ vanish since they are dual to $T_pA(K_v) = 0$ by local Tate duality. The first part of the second sequence will be a consequence of the more general duality of Poitou-Tate (I.4). □

Another part of the global duality is the following sequence found by Cassels.

Proposition I.4. *There is an exact sequence of discrete p-torsion groups of finite corank*

$$0 \longrightarrow \mathcal{R} \longrightarrow H^1_\Sigma(A(p)) \longrightarrow \oplus H^1(K_v, A(p)) \longrightarrow \widehat{H^1_\Sigma(T_p\check{A})} \longrightarrow \widehat{\Re_\Sigma} \longrightarrow 0. \quad \text{(I.3)}$$

Proof. This is easily deduced from the explicit sequence of Cassels in his original article [Cas64] or from the formulation in [Rub00, Therem I.7.3]. Otherwise one can view it as a special case of (I.4). □

The general formulation of Tate is the statement that, for any finite p-primary $G_\Sigma(K)$-module, the following 9-term sequence is exact.

$$\begin{aligned} 0 \longrightarrow H^0_\Sigma(M) \longrightarrow \oplus H^0(K_v, M) \longrightarrow \widehat{H^2_\Sigma(M')} \longrightarrow \\ \longrightarrow H^1_\Sigma(M) \longrightarrow \oplus H^1(K_v, M) \longrightarrow \widehat{H^1_\Sigma(M')} \longrightarrow \\ \longrightarrow H^2_\Sigma(M) \longrightarrow \oplus H^2(K_v, M) \longrightarrow \widehat{H^0_\Sigma(M')} \longrightarrow 0 \end{aligned} \quad \text{(I.4)}$$

In particular, when applied to the module $\mu[p^k]$, we get a sequence (see [NeScWi00, page 539])

$$H^1_\Sigma(\mu[p^k]) \longrightarrow \oplus H^1(K_v, \mu[p^k]) \longrightarrow \widehat{H^1_\Sigma(\mathbb{Z}/p^k)} \longrightarrow \mathrm{Cl}(\mathcal{O}_\Sigma)/p^k \longrightarrow 0 \quad \text{(I.5)}$$

where $\mathrm{Cl}(\mathcal{O}_\Sigma)$ is the class group of the Σ-integers $\mathcal{O}_\Sigma$ in K. We may pass to the limit sequences

$$\begin{aligned} H^1_\Sigma(\mu(p)) \longrightarrow \oplus H^1(K_v, \mu(p)) \xrightarrow{g} \widehat{H^1_\Sigma(\mathbb{Z}_p)} \longrightarrow 0 \\ H^1_\Sigma(T_p\mu) \longrightarrow \oplus H^1(K_v, T_p\mu) \xrightarrow{g} G_\Sigma(K)^{p\text{-ab}} \longrightarrow \mathrm{Cl}(\mathcal{O}_\Sigma)(p) \longrightarrow 0 \end{aligned} \quad \text{(I.6)}$$

Here $G_\Sigma(K)^{p\text{-ab}}$ is the Galois group of the maximal abelian p-extension of K that is unramified outside Σ. If the Leopoldt conjecture holds for the field K, then the kernel of the first sequence above is finite, while the kernel of the second, equal to $H^2_\Sigma(\mathbb{Q}_p/\mathbb{Z}_p)$, is zero. This is part of theorem X.3.6 in [NeScWi00].

I.2.2 $\mathbb{Z}_p$-extensions

Let λ be a non-trivial continuous homomorphism from the absolute Galois group $\mathrm{Gal}(\overline{K} : K)$ to $\mathbb{Z}_p$. Its kernel has a fixed field ${}_\infty K$ such that λ induces a map from $\Gamma = \mathrm{Gal}({}_\infty K : K)$ to $\mathbb{Z}_p$ which is an isomorphism onto its image. So ${}_\infty K$ is a $\mathbb{Z}_p$-extension of K.

Composed with the Artin reciprocity map, we obtain a continuous map from the idèle group $\mathbb{I}_K$ of the field K to $\mathbb{Z}_p$. This gives a continuous map λ_υ from $K_\upsilon^\times$ to $\mathbb{Z}_p$ for every place υ in K. If the place υ is at infinity, the map λ_υ has to be trivial because $\mathbb{Z}_p$ has no 2-torsion and is totally disconnected. If the place υ does not divide p, then the group of units $\mathcal{O}_\upsilon^\times$ must lie in the kernel because it has a subgroup of finite index isomorphic to $\mathcal{O}_\upsilon$. We see that λ and the $\mathbb{Z}_p$-extension are unramified outside the places above p. In particular λ factors through $G_\Sigma(K)$ and so it belongs to $H^1_\Sigma(\mathbb{Z}_p) = \mathrm{Hom}(G_\Sigma(K), \mathbb{Z}_p)$.

Furthermore the product-formula must hold, so $\sum \lambda_\upsilon(x) = 0$ if x belongs to $K^\times$ and the sum runs over all places in K.

If the Leopoldt conjecture is known to hold for the field K, then the space $H^1_\Sigma(\mathbb{Z}_p)$ parametrising all λ has rank $r_2 + 1$, where r_2 stands for the number of complex places of K (see [NeScWi00, Proposition X.3.20]).

The most important example is the *cyclotomic* $\mathbb{Z}_p$-extension. Define the cyclotomic character ${}_{\mathrm{cyc}}\chi(\sigma) \in \mathbb{Z}_p^\times$ by $\sigma(\zeta) = \zeta^{{}_{\mathrm{cyc}}\chi(\sigma)}$ for σ in the Galois group $\mathrm{Gal}(\overline{K} : K)$ and ζ in $\mu(p)$. Then ${}_{\mathrm{cyc}}\lambda = \log_p \circ {}_{\mathrm{cyc}}\chi$ is a non-trivial homomorphism as required. Here $\log_p$ is the p-adic logarithm of Iwasawa.

By the explicit description of the Artin reciprocity map for cyclotomic extensions, we find the following formulae. If υ is at infinity, then ${}_{\mathrm{cyc}}\lambda_\upsilon = 0$. Denote by q_υ the number of elements in the residue field $\mathbb{F}_\upsilon$ at a finite place υ. If υ is above $\ell \neq p$, then

$$
\begin{aligned}
{}_{\mathrm{cyc}}\lambda_\upsilon(x) &= \log_p(q_\upsilon) \cdot \mathrm{ord}_\upsilon(x) = -\log_p |N_{K_\upsilon:\mathbb{Q}_\ell}(x)|_\ell \quad \text{and otherwise} \\
{}_{\mathrm{cyc}}\lambda_\upsilon(x) &= -\log_p(N_{K_\upsilon:\mathbb{Q}_p}(x)).
\end{aligned}
$$

As a consequence, we see that

$$
\sum_{\upsilon \nmid p} {}_{\mathrm{cyc}}\lambda_\upsilon(x) = -\sum_{\upsilon | p} {}_{\mathrm{cyc}}\lambda_\upsilon(x) = \log_p(N_{K:\mathbb{Q}}(x)) \quad \text{if } x \in K^\times. \tag{I.7}
$$

I.2.3 Galois cohomology over $\mathbb{Z}_p$-extensions

Let ${}_\infty K : K$ be a $\mathbb{Z}_p$-extension of Galois-group Γ. Let M be a finite p-torsion G_Σ-module. The most important fact about Γ is that it is a group of cohomological

dimension 1. Once again we introduce an abbreviation in notations, namely the often occurring Galois-cohomology groups $H^i(G_\Sigma({}_\infty K), M) = H^i_\Sigma({}_\infty K, M)$ will also be denoted by ${}_\infty H^i_\Sigma(M)$.

Hochschild-Serre

The spectral sequence of Hochschild-Serre (see [NeScWi00, Theorem II.1.5]) degenerates and gives

Lemma I.5. *For all $i \geqslant 1$, there is an exact sequence*

$$0 \longrightarrow H^1(\Gamma, {}_\infty H^{i-1}_\Sigma(M)) \longrightarrow H^i_\Sigma(M) \xrightarrow{\text{res}} {}_\infty H^i_\Sigma(M)^\Gamma \longrightarrow 0. \tag{I.8}$$

In particular, taking limits, we find the useful sequence

$$0 \longrightarrow H^1(\Gamma, {}_\infty H^1_\Sigma(A(p))) \longrightarrow H^2_\Sigma(A(p)) \xrightarrow{\text{res}} {}_\infty H^2_\Sigma(A(p))^\Gamma \longrightarrow 0 \tag{I.9}$$

An explicit description of the injection will be given later in I.6.1.

Tate's spectral sequence

Let me introduce yet another shorthand, namely for the projective limits of global cohomology groups as we walk up the tower to ${}_\infty K$:

$${}_\infty \mathfrak{H}^i_\Sigma(M) = \varprojlim H^i_\Sigma({}_n K, M)$$

where the projective limit is taken with respect to the corestriction maps. They are sometimes denoted by H_{Iw}.

Lemma I.6. *Let M be a finite $G_\Sigma(K)$-module. We have the following sequences and isomorphisms*

$$\begin{array}{ccccccccc}
 & & & & H^1(\Gamma, {}_\infty\mathfrak{H}^2_\Sigma(M)) & \xrightarrow[\cong]{\text{cor}} & H^2_\Sigma(M) & & \\
0 & \longrightarrow & H^1(\Gamma, {}_\infty\mathfrak{H}^1_\Sigma(M)) & \xrightarrow{\text{cor}} & H^1_\Sigma(M) & \longrightarrow & {}_\infty\mathfrak{H}^2_\Sigma(M)^\Gamma & \longrightarrow & 0 \\
0 & \longrightarrow & H^1(\Gamma, {}_\infty\mathfrak{H}^0_\Sigma(M)) & \xrightarrow{\text{cor}} & H^0_\Sigma(M) & \longrightarrow & {}_\infty\mathfrak{H}^1_\Sigma(M)^\Gamma & \longrightarrow & 0 \\
 & & & & & & {}_\infty\mathfrak{H}^0_\Sigma(M)^\Gamma & \xrightarrow[\cong]{} & 0
\end{array}$$

Proof. According to [NeScWi00, Theorem 2.1.11] there is a spectral sequence due to Tate. We spell it out for $G = G_\Sigma(K)$, $H = G_\Sigma({}_\infty K)$ and $A = M$:

$$E_2^{p,q} = H^p\Big(\Gamma, \big(\varprojlim H^{2-q}_\Sigma({}_n K, M)\big)^\wedge\Big) \Longrightarrow H^{2-p-q}_\Sigma(K, M)^\wedge$$

Since Γ has cohomological dimension 1, this collapses and we can extract short exact sequences

$$0 \longrightarrow H^1\left(\Gamma, {}_\infty\mathfrak{H}^{i+1}_\Sigma(M)^\wedge\right) \longrightarrow H^i_\Sigma(M)^\wedge \longrightarrow H^0\left(\Gamma, {}_\infty\mathfrak{H}^i_\Sigma(M)^\wedge\right) \longrightarrow 0. \qquad \text{(I.10)}$$

The fact that the edge morphism is the corestriction map is proven in [NeScWi00, theorem 2.1.12]. □

Corollary I.7. *In particular, we have the following exact sequence*

$$0 \longrightarrow H^1(\Gamma, {}_\infty\mathfrak{H}^1_\Sigma(T_pA)) \xrightarrow{\text{cor}} H^1_\Sigma(T_pA) \longrightarrow {}_\infty\mathfrak{H}^2_\Sigma(T_pA)^\Gamma \longrightarrow 0. \qquad \text{(I.11)}$$

Proof. We will take the inductive limit over k of the sequence (I.10) for $M = A[p^k]$ and $i = 1$. In the first and last term, we end up with things like

$$\varinjlim_k \left(\varprojlim_n H^i_\Sigma({}_nK, A[p^k]) \right).$$

in the second argument of the Γ-cohomology groups. We can swap these projective limits and, using Tate's argument, we can insert the projective limit over k in the cohomology group. □

Over local fields

Suppose ${}_\infty K_w : K_v$ is a $\mathbb{Z}_p$-extension with Galois group Γ_w. The above exact sequences (I.9) and (I.11) have local analogues, but because of local Tate duality, they are actually dual to each other:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(\Gamma_w, H^0({}_\infty K_w, A(p))) & \longrightarrow & H^1(K_v, A(p)) & \longleftarrow & H^1({}_\infty K_w, A(p))^{\Gamma_w} & \longrightarrow & 0 \\ & & \updownarrow & & \updownarrow & & \updownarrow & & \\ 0 & \longleftarrow & \varprojlim H^2({}_nK_w, T_p\check{A})^{\Gamma_w} & \longleftarrow & H^1(K_v, T_p\check{A}) & \longleftarrow & H^1(\Gamma_w, \varprojlim H^1({}_nK_w, T_p\check{A})) & \longleftarrow & 0 \end{array} \qquad \text{(I.12)}$$

Global duality

For fine Selmer groups over ${}_\infty K$, we will use the above abbreviation, namely ${}_\infty\mathcal{R}$ for $\mathcal{R}(A/{}_\infty K)$. By taking limits on the global duality over the finite layers ${}_nK$, one gets the following three statements.

$$\varprojlim \mathfrak{R}_\Sigma(\check{A}/{}_nK) \qquad \text{is dual to} \qquad {}_\infty H^2_\Sigma(A(p)) \qquad \text{(I.13)}$$

There are exact sequences (the symbol $\oplus$ continues to stand for the direct sum over all places above Σ)

$$0 \longrightarrow A({}_\infty K)(p) \longrightarrow \oplus A({}_\infty K_v)(p) \longrightarrow \widehat{{}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})} \longrightarrow {}_\infty\mathcal{R} \longrightarrow 0 \qquad \text{(I.14)}$$

$$\begin{array}{ccccccc} 0 & \longrightarrow & {}_\infty\mathcal{R} & \longrightarrow & {}_\infty H^1_\Sigma(A(p)) & \twoheadrightarrow & \\ & & & & & & \oplus H^1({}_\infty K_v, A(p)) \\ 0 & \leftarrow & {}_\infty H^2_\Sigma(A(p)) & \leftarrow & {}_\infty\widehat{\mathfrak{H}^1_\Sigma(T_p\check{A})} & \leftarrow & \end{array} \qquad (I.15)$$

I.2.4 A homological lemma

The lemma that is proved here is probably standard and need not be explained. Nevertheless I could not find any reference to it in basic textbooks on homological algebra such as [Wei94]. The moment has also come to introduce the notation $\circ\!\!\rightarrow$. It will always mean a map in a cochain complex, while $\longrightarrow$ will be used only if the complex is *exact at the source of the arrow*.

Lemma I.8. *Let $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ be a left exact functor between two abelian categories with enough injectives. Write $G = R^1F$ for its first right derived functor and assume that all higher derived functors vanish. Then, given an exact sequence*

$$0 \longrightarrow X^1 \longrightarrow X^2 \longrightarrow \cdots \longrightarrow X^n \longrightarrow 0$$

in $\mathcal{C}$, there are two cochain complexes in $\mathcal{D}$

$$0 \longrightarrow F\,X^1 \longrightarrow F\,X^2 \longrightarrow F\,X^3 \circ\!\!\rightarrow \cdots \circ\!\!\rightarrow F\,X^n \circ\!\!\rightarrow 0$$

$$0 \longrightarrow G\,X^1 \circ\!\!\rightarrow G\,X^2 \circ\!\!\rightarrow \cdots \circ\!\!\rightarrow G\,X^{n-1} \longrightarrow G\,X^n \longrightarrow 0.$$

Moreover we have canonical isomorphisms $H^{i-1}(G\,X^\bullet) = H^{i+1}(F\,X^\bullet)$ for all i.

Proof. First we split up the exact sequence in short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X^1 & \longrightarrow & X^2 & \longrightarrow & Z^3 & \longrightarrow & 0 \\ 0 & \longrightarrow & Z^3 & \longrightarrow & X^3 & \longrightarrow & Z^4 & \longrightarrow & 0 \\ & & & & \vdots & & & & \\ 0 & \longrightarrow & Z^{n-1} & \longrightarrow & X^{n-1} & \longrightarrow & X^n & \longrightarrow & 0 \end{array}$$

And now we can read the cochain complexes out of a big diagram in figure I.1 on the following page. For the statement on the cohomology groups, note first that the kernel of the map $F\,X^{i+1} \circ\!\!\rightarrow F\,X^{i+2}$ equals $F\,Z^i$, so the group $H^{i+1}(F\,X^\bullet)$ is isomorphic to the image of $F\,Z^i \longrightarrow G\,Z^{i-1}$. On the other side, the image of $G\,X^{i-2} \circ\!\!\rightarrow G\,X^{i-1}$ is the same as the image of $G\,Z^{i-2} \longrightarrow G\,X^{i-1}$ and so the cohomology group $H^{i-1}(G\,X^\bullet)$ is the kernel of $G\,Z^{i-1} \longrightarrow G\,X^i$.

Alternatively, one can use the hyper-cohomology spectral sequence degenerating at the second page, with trivial limit because the starting complex $X^\bullet$ is exact. □

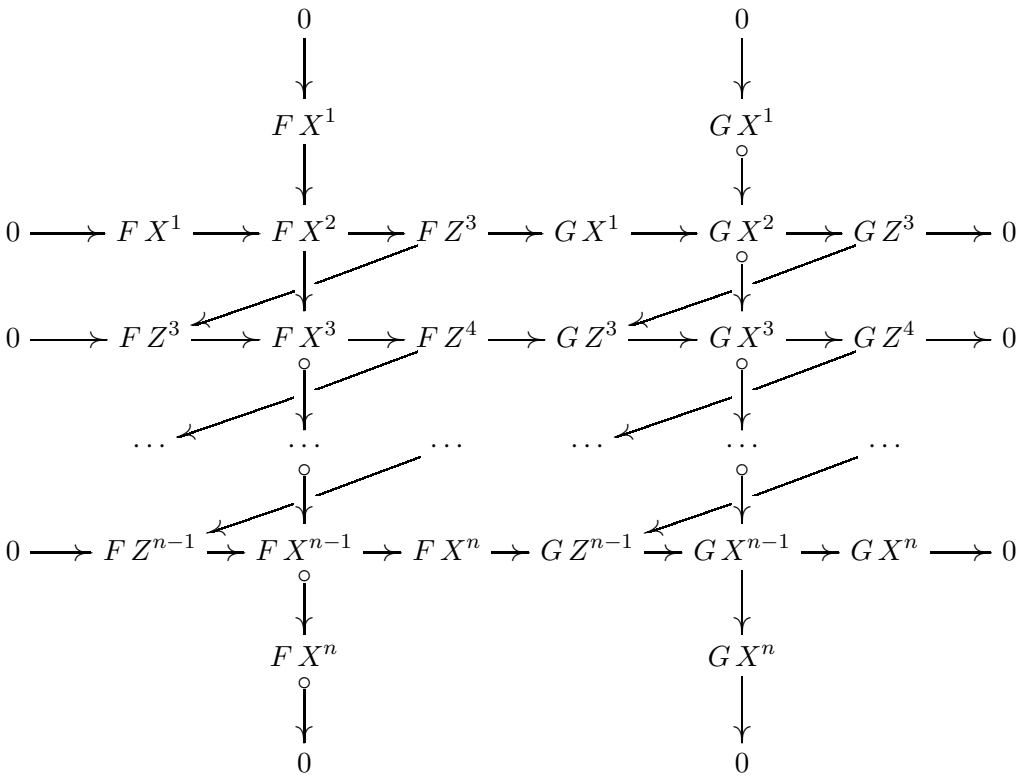


Figure I.1: The complexes appear in a diagram

The main purpose of this lemma are the two corollaries deduced from it. Once we apply it to the functor T_p and then to the functor $H^0(\Gamma, \cdot)$.

Corollary I.9. *Let* $0 \longrightarrow X^1 \longrightarrow \cdots \longrightarrow X^n \longrightarrow 0$ *be an exact sequence of cofinitely generated, abelian* p*-primary groups. Then*

$$0 \longrightarrow T_pX^1 \longrightarrow T_pX^2 \longrightarrow T_pX^3 \circ\!\!\longrightarrow \cdots \circ\!\!\longrightarrow T_pX^n \circ\!\!\longrightarrow 0$$
$$0 \longrightarrow (X^1)^\star \circ\!\!\longrightarrow (X^2)^\star \circ\!\!\longrightarrow \cdots \circ\!\!\longrightarrow (X^{n-1})^\star \longrightarrow (X^n)^\star \longrightarrow 0$$

are complexes. The first one is a complex of finitely generated $\mathbb{Z}_p$*-free modules and has finite cohomology. The second complex is finite.*

Proof. Note first that the first derived functor of $X \longmapsto X[p^k]$ is $X \longmapsto X/p^kX$. Since all $X[p^k]$ are finite groups, the functor $\varprojlim$ is exact (see [Wei94, Exercise 3.5.2]). Now the statement that $H^{i+1}(T_pX^\bullet) = H^{i-1}((X^\bullet)^\star)$ and the finiteness of $(X^i)^\star$, which equals the quotient of X^i by its maximal divisible group, proves the corollary. □

Corollary I.10. *Let* Γ *be a pro-*p*-group of cohomological dimension 1 and let*

$$0 \longrightarrow X^1 \longrightarrow \cdots \longrightarrow X^n \longrightarrow 0$$

be an exact sequence of Γ-module, then we have two cochain complexes

$$0 \longrightarrow (X^1)^\Gamma \longrightarrow (X^2)^\Gamma \to (X^3)^\Gamma \circ\!\!\longrightarrow \cdots \circ\!\!\longrightarrow (X^n)^\Gamma \circ\!\!\longrightarrow 0$$
$$0 \longrightarrow H^1(\Gamma, X^1) \circ\!\!\longrightarrow \cdots \circ\!\!\longrightarrow H^1(\Gamma, X^{n-1}) \to H^1(\Gamma, X^n) \longrightarrow 0$$

I.3 The structure of the fine Selmer group

We start by analysing the compact fine Selmer group $\mathfrak{R}$ and its subgroup $\mathfrak{R}_\Sigma$. The main results of this section are the fact that they are $\mathbb{Z}_p$-free and that there is a construction of a Cassels-Tate pairing on $\mathcal{R}^\star$.

I.3.1 Construction of a diagram

Consider the multiplication by p^k on $A(p)$ and $T_p\check{A}$ as k varies. This can be summed up in the following diagrams.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A[p^k] & \longrightarrow & A(p) & \xrightarrow{[p^k]} & A(p) & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle [p]} & & \uparrow{\scriptstyle [p]} & & \| & & \\
0 & \longrightarrow & A[p^{k+1}] & \longrightarrow & A(p) & \xrightarrow{[p^{k+1}]} & A(p) & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccccc}
0 & \longleftarrow & \check{A}[p^k] & \longleftarrow & T_p\check{A} & \xleftarrow{[p^k]} & T_p\check{A} & \longleftarrow & 0 \\
 & & \downarrow{\scriptstyle \cap} & & \downarrow{\scriptstyle [p]} & & \| & & \\
0 & \longleftarrow & \check{A}[p^{k+1}] & \longleftarrow & T_p\check{A} & \xleftarrow{[p^{k+1}]} & T_p\check{A} & \longleftarrow & 0
\end{array}$$

In the usual manner, we deduce short exact sequences of cohomology groups over a field F containing K.

$$0 \longrightarrow A(F)(p)/p^k \longrightarrow H^1(F, A[p^k]) \longrightarrow H^1(F, A(p))[p^k] \longrightarrow 0$$
$$0 \longleftarrow H^2(F, T_p\check{A})[p^k] \longleftarrow H^1(F, \check{A}[p^k]) \longleftarrow H^1(F, T_p\check{A})/p^k \longleftarrow 0$$

If F is a local field K_υ, then the two exact sequences are dual to each other via Tate duality. Using the multiplication by $[p]$ as in the diagrams above, we can pass to the limits.

$$\begin{array}{l}
0 \longrightarrow A(F)(p) \longrightarrow H^1(F, T_pA) \longrightarrow T_pH^1(F, A(p)) \longrightarrow 0 \\
0 \longleftarrow H^2(F, T_p\check{A})(p) \longleftarrow H^1(F, \check{A}(p)) \longleftarrow H^1(F, T_p\check{A}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longleftarrow 0
\end{array} \tag{I.16}$$

The corollary I.9 applied to the sequence (I.2), we get a complex of finite groups

$$0 \circ\!\!\longrightarrow A(K)(p)^\star \circ\!\!\longrightarrow \oplus A(K_\upsilon)(p)^\star \circ\!\!\longrightarrow \widehat{H^2_\Sigma(T_p\check{A})}^\star \longrightarrow \mathcal{R}^\star \longrightarrow 0.$$

We can rewrite this as

$$0 \longrightarrow A(K)(p) \longrightarrow \oplus A(K_\upsilon)(p) \hookrightarrow H^2_\Sigma(T_p\check{A})(p)^\wedge \longrightarrow \mathcal{R}^\star \longrightarrow 0 \tag{I.17}$$

and we see that the complex is exact everywhere but at the second non-zero term. This follows from the corollary I.9 and the injectivity of the global p-torsion into the local p-torsion.

Again by the same corollary I.9, but applied to the sequence (I.3), we get a complex

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_p\mathcal{R} & \longrightarrow & T_pH^1_\Sigma(A(p)) & \twoheadrightarrow & \\ & & & & & & \oplus T_pH^1(K_\upsilon, A(p)) \\ 0 & \hookleftarrow & T_p\left(\widehat{\check{\mathfrak{R}}_\Sigma}\right) & \hookleftarrow & T_p\left(\widehat{H^1_\Sigma(T_p\check{A})}\right) & \hookleftarrow & \end{array} \tag{I.18}$$

Note also that $T_p(\widehat{X}) = \mathrm{Hom}(X, \mathbb{Z}_p)$ for the last two terms.

Now we can build a huge diagram. We align the short exact sequences found in (I.16) vertically. In the middle appears Cassels sequence (I.3), while the top is a part of the complex (I.17) and the bottom is a part of (I.18). We define therefore three complexes in an short exact sequence by the following nine terms and zero outside. We fix the middle (local) column to be the 0-th term of the cochain complexes.

$$\begin{array}{ccccccc} 0 & & 0 & & 0 & & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ Y^\bullet_{\mathsf{top}} & & A(K)(p) & \hookrightarrow & \oplus A(K_\upsilon)(p) & \hookrightarrow & H^2_\Sigma(T_p\check{A})(p)^\wedge \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ Y^\bullet_{\mathsf{mi}} & & H^1_\Sigma(T_pA) & \hookrightarrow & \oplus H^1(K_\upsilon, T_pA) & \hookrightarrow & H^1_\Sigma(\check{A}(p))^\wedge \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ Y^\bullet_{\mathsf{bo}} & & T_pH^1_\Sigma(A(p)) & \hookrightarrow & \oplus T_p\, H^1(K_\upsilon, A(p)) & \hookrightarrow & \mathrm{Hom}(H^1_\Sigma(T_p\check{A}), \mathbb{Z}_p) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & & 0 & & 0 & & 0 \end{array} \tag{I.19}$$

Although each vertical sequence is split (the top complex is made out of finite groups and the bottom contains only $\mathbb{Z}_p$-free modules), there is, in general, no splitting that makes the diagram commutative.

I.3.2 The compact fine Selmer group is $\mathbb{Z}_p$-free

We define I_Σ to be the finite group $H^0(Y^\bullet_{\mathsf{top}})$. Now we apply the long exact sequence for short exact sequences of cochain complexes as in [Wei94, Theorem 1.3.1]. This

splits into two parts because $H^0(Y^\bullet_{\mathsf{mi}}) = 0$ by (I.3). The first part is

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^{-1}(Y^\bullet_{\mathsf{top}}) & \longrightarrow & H^{-1}(Y^\bullet_{\mathsf{mi}}) & \longrightarrow & H^{-1}(Y^\bullet_{\mathsf{bo}}) & \longrightarrow & H^0(Y^\bullet_{\mathsf{top}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ & & 0 & \longrightarrow & \mathfrak{R}_\Sigma & \longrightarrow & T_p\mathcal{R} & \longrightarrow & I_\Sigma & \longrightarrow & 0 \end{array} \tag{I.20}$$

The third equality comes from the exactness of the first two terms in (I.18).

Instead of summing over all places in Σ, one could look at the first two rows of the above huge diagram (I.19) even if the middle term consists of the sum over all places above p only. It is easy to check that everything just works the same and we end up with a sequence

$$0 \longrightarrow \mathfrak{R} \longrightarrow T_p\mathcal{R} \longrightarrow I_0 \longrightarrow 0 \tag{I.21}$$

where I_0 is a finite group inside the cokernel of the map from $A(K)(p)$ to $\bigoplus A(K_v)(p)$, where this time, the sum is over all places above p. This proves

Proposition I.11. *The groups $\mathfrak{R}_\Sigma(A/K)$ and $\mathfrak{R}(A/K)$ are free $\mathbb{Z}_p$-module. The canonical embedding $\mathfrak{R}(A/K)$ into $T_p\mathcal{R}(A/K)$ has finite cokernel of order $\#I_0$ bounded by*

$$\#I_0 \leqslant \frac{\prod_{v|p} \#A(K_v)(p)}{\#A(K)(p)}$$

We add here the definition of the map a that we will use later.

$$\begin{array}{ccc} a\colon \operatorname{Hom}(\mathcal{R}, \mathbb{Q}_p/\mathbb{Z}_p) & \twoheadrightarrow & \operatorname{Hom}(\mathcal{R}_{\mathsf{div}}, \mathbb{Q}_p/\mathbb{Z}_p) \\ & & \| \\ & & \operatorname{Hom}_{\mathbb{Z}_p}(T_p\mathcal{R}, \mathbb{Z}_p) \rightarrowtail \operatorname{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma, \mathbb{Z}_p) \end{array} \tag{I.22}$$

It has kernel of order $\#\mathcal{R}^\star$ and the cokernel has order $\#I_\Sigma = [\mathfrak{R} : \mathfrak{R}_\Sigma] \cdot \#I_0$.

I.3.3 The Cassels-Tate pairing

Now, we look at the second part of the long exact sequence coming from the short exact sequence of complexes (I.19).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(Y^\bullet_{\mathsf{bo}}) & \longrightarrow & H^1(Y^\bullet_{\mathsf{bo}}) & \longrightarrow & H^1(Y^\bullet_{\mathsf{mi}}) & \longrightarrow & H^1(Y^\bullet_{\mathsf{bo}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \ker(ct) & \longrightarrow & \mathcal{R}^\star & \xrightarrow{ct} & \widehat{\mathcal{R}} & \longrightarrow & H^1(Y^\bullet_{\mathsf{bo}}) & \longrightarrow & 0 \end{array}$$

Since $\mathcal{R}^\star$ is finite, the image of the middle map must lie in $\widehat{\mathcal{R}^\star}$ and so there is a sequence

$$0 \longrightarrow \ker(ct) \longrightarrow \mathcal{R}^\star \xrightarrow{ct} \widehat{\mathcal{R}^\star} \longrightarrow \operatorname{coker}(ct) \longrightarrow 0.$$

From the diagram (I.19) we immediately see that this map here is the same as the one in proposition I.2. So it must be the restriction of the Cassels-Tate pairing to the fine Selmer group. Using the relation between the cohomologies of the two complexes again, we can describe the kernel as

$$0 \longrightarrow \ker(ct) \longrightarrow \mathcal{R}^\star \longrightarrow H^1_\Sigma(A(p))^\star$$

In other words, the kernel consists of elements in $\mathcal{R}$ that become divisible in the group $H^1_\Sigma(A(p))$. This pairing is nothing new, it is in fact a special case of the non-degenerate pairing of Flach [Fla90], namely

$$\mathcal{R}(\check{A}/K)^\star \times H^1_\Sigma(A(p))^\star \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

If the abelian variety is principally polarised, the pairing is alternating.

I.4 The control theorem

I believe the first "control theorem" was discovered in [Maz72] for the classical Selmer group if the reduction is good and ordinary. Ever since, there is hardly an Iwasawa–theoretic article on abelian varieties that does not contain the statement of the control theorem or even a proof of it. It is without any doubt a very crucial step for analysing the growth of the Selmer group in $\mathbb{Z}_p$-extensions.

We will consider everything related to a fixed $\mathbb{Z}_p$-extension ${}_\infty K : K$ with Galois group Γ.

I.4.1 Preliminary lemmata on the torsion

Define the following two groups

$$T_{\text{gl}} = H^1(\Gamma, A({}_\infty K)(p))$$
$$T_{\text{loc}} = \bigoplus_{v\in\Sigma} H^1(\Gamma, H^0({}_\infty K_v, A(p)))$$

which fit into the short exact sequence coming from the inf-res-sequence (or the Hochschild-Serre spectral sequence (I.8)):

$$\begin{aligned} 0 \longrightarrow T_{\text{gl}} \longrightarrow H^1_\Sigma(A(p)) &\xrightarrow{\text{res}} {}_\infty H^1_\Sigma(A(p))^\Gamma \longrightarrow 0 \\ 0 \longrightarrow T_{\text{loc}} \longrightarrow \oplus H^1(K_v, A(p)) &\xrightarrow{\text{res}} \oplus H^0(\Gamma, H^1({}_\infty K_v, A(p))) \longrightarrow 0 \end{aligned} \tag{I.23}$$

Our aim is to prove that both, T_{gl} and T_{loc}, are finite groups. There is one case that is slightly easier to treat; even if it can be deduced from what follows, we prove the finiteness first in this case.

Lemma I.12. *Suppose that the $\mathbb{Z}_p$-extension ${}_\infty K$ is the cyclotomic extension of K and that A has potential good reduction at all places above p, then the above groups are finite of order*

$$\#T_{gl} = \#A(K)(p) \qquad \text{and} \qquad \#T_{loc} = \prod_{v|p} \#A(K_v)(p) \cdot \prod_{v\nmid p} c_v^{(p)},$$

where $c_v^{(p)}$ is the highest power of p dividing the Tamagawa number c_v of A.

Proof. Choose a topological generator γ in Γ. Write $M = A({}_\infty K)(p)$. Imai's result [CoSu00, remark on page 91] or [Ima75] shows that M is finite under the hypotheses made in the statement. Now,

$$0 \longrightarrow M^\Gamma \longrightarrow M \xrightarrow{(\gamma-1)} M \longrightarrow M_\Gamma \longrightarrow 0$$

shows that $\#H^0(\Gamma, M) = \#M_\Gamma = \#H^1(\Gamma, M)$. The same reasoning applies to the group $M = H^0(\Gamma, A({}_\infty K_v)(p))$, if v divides p. The case $v \nmid p$ will be treated in lemma I.14. □

Without the assumption made in the previous lemma, it is still possible to bound the order of the two groups. First the global case:

Lemma I.13. *The group T_{gl} is a finite group of order bounded by $\#A(K)(p)$.*

Proof. Let D be the maximal divisible subgroup of $M = A({}_\infty K)(p)$. Hence M/D is finite. Consider the Γ-cohomology of the exact sequence

$$0 \longrightarrow T_pD \longrightarrow V_pD \longrightarrow D \longrightarrow 0,$$

where $V_pD = T_pD \otimes \mathbb{Q}_p$. Since $H^1(\Gamma, V_pD) = 0$, the group $H^1(\Gamma, T_pD)$ is finite, for D^Γ is a subgroup of $M^\Gamma = A(K)(p)$. By Tate's argument [NeScWi00, Corollary II.2.3.5], we have

$$H^2(\Gamma, T_pD) = \varprojlim H^2(\Gamma, D[p^k]) = 0.$$

Therefore $H^1(\Gamma, D) = 0$ and, similarly, $H^2(\Gamma, D) = 0$. Consider now the long exact sequence

$$0 \longrightarrow D^\Gamma \longrightarrow A(K)(p) \longrightarrow (M/D)^\Gamma \longrightarrow 0 \longrightarrow H^1(\Gamma, M) \longrightarrow H^1(\Gamma, M/D) \longrightarrow 0.$$

It shows that

$$\#T_{\text{gl}} = \#H^1(\Gamma, M) = \#H^1(\Gamma, M/D) = \#H^0(\Gamma, M/D) = \#A(K)(p)/\#D^\Gamma,$$

by the argument already used in the proof of the previous lemma for the finite group M/D. □

In other words, our group T_{gl} counts the p-power torsion points that will not become divisible in $A({}_\infty K)$.

Lemma I.14. *Let υ be a finite place of K. The group $T_\upsilon = H^1(\Gamma, H^0({}_\infty K_\upsilon, A(p)))$ is a finite group of order bounded by $\#A(K_\upsilon)(p)$. If υ does not divide p, T_υ has order equal to the highest power of p dividing the Tamagawa number c_υ. In particular, $T_{loc} = \oplus_{\upsilon\in\Sigma} T_\upsilon$ is a finite group.*

Proof. First Shapiro's lemma [NeScWi00, Proposition 1.6.3] gives us isomorphisms

$$H^i(\Gamma, H^j({}_\infty K_\upsilon, A(p))) \longrightarrow H^i(\Gamma_w, H^j({}_\infty K_w, A(p)))$$

for any chosen place w above υ. If $\upsilon \mid p$ splits completely, then Γ_w is trivial, otherwise it is isomorphic to $\mathbb{Z}_p$ and the bound on the order of T_υ follows as in the previous lemma.

Suppose $\upsilon \nmid p$. Either we use lemma 3.4 in [CoSu00] or we proceed as follows.

Write $\widetilde{\mathscr{A}^\circ}/\mathbb{F}_\upsilon$ for the special fibre of the Néron model $\mathscr{A}$ of A and Φ/K_υ for its group of components. Since $\upsilon \nmid p$, the kernel of the specialisation from the connected component $\mathscr{A}^\circ(K_\upsilon)$ to $\widetilde{\mathscr{A}^\circ}(\mathbb{F}_\upsilon)$ has no p-torsion (see [HiSi00, Proposition C.2.5]). Hence we have

$$0 \longrightarrow \widetilde{\mathscr{A}^\circ}(\mathbb{F}_\upsilon)(p) \longrightarrow A(K_\upsilon)(p) \longrightarrow \Phi(K_\upsilon)(p) \longrightarrow 0.$$

Since Néron models are stable under étale base changes (see [BoLüRa90] or [Sil94, Proposition 5.2]), the group of components of A over ${}_nK_w$ is still the same, because ${}_nK_w : K_\upsilon$ is unramified. Write ${}_nG$ for the Galois group of the non-ramified extension ${}_nK_w : K_\upsilon$. Applying $H^1({}_nG, \cdot)$ to the sequence above, but over ${}_nK_w$, gives

$$0 = H^1({}_n\mathbb{F}_\upsilon/\mathbb{F}_\upsilon, \widetilde{\mathscr{A}^\circ}({}_n\mathbb{F}_\upsilon)(p)) \longrightarrow H^1({}_nG, A(K_\upsilon)(p)) \longrightarrow H^1({}_nG, \Phi({}_nK_w)(p)) \longrightarrow 0$$

where the first equality comes from Lang's theorem [Lan56]. Hence, in the limit we obtain

$$\#T_\upsilon = \#H^1(\Gamma, \Phi({}_\infty K_w)(p)) = \#\Phi(K_\upsilon)(p) = c_\upsilon^{(p)}.$$

□

I.4.2 Building another huge diagram

Let us fix a topological generator γ of Γ, in order to have an isomorphism from $H^1(\Gamma, M)$ to M_Γ. We build up a short exact sequence of cochain complexes in a similar

manner to (I.19). Apply corollary I.10 to the global duality over ${}_\infty K$ as in (I.15) to get a complex

$$\begin{array}{ccccccccc} 0 & \longrightarrow & {}_\infty\mathcal{R}^\Gamma & \longrightarrow & {}_\infty H^1_\Sigma(A(p))^\Gamma & \twoheadrightarrow & \oplus H^1({}_\infty K_v, A(p))^\Gamma \\ 0 & \hookleftarrow & {}_\infty H^2_\Sigma(A(p))^\Gamma & \hookleftarrow & {}_\infty\widehat{\mathfrak{H}^1_\Sigma(T_p\check{A})}^\Gamma & \hookleftarrow & \end{array} \tag{I.24}$$

We use corollary I.10 a second time for the global duality as in (I.14).

$$0 \longrightarrow (A({}_\infty K)(p))_\Gamma \hookrightarrow (\oplus A({}_\infty K)(p))_\Gamma \hookrightarrow {}_\infty\widehat{\mathfrak{H}^2_\Sigma(T_p\check{A})}_\Gamma \longrightarrow {}_\infty\mathcal{R}_\Gamma \longrightarrow (0$$

By definition, the first two terms are the groups T_{loc} and T_{gl}. So the complex becomes

$$0 \longrightarrow T_{\mathsf{gl}} \hookrightarrow T_{\mathsf{loc}} \hookrightarrow ({}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma)^\wedge \longrightarrow {}_\infty\mathcal{R}_\Gamma \longrightarrow 0 \tag{I.25}$$

Once again, we form a short exact sequence of complexes by glueing together three exact sequences, namely (I.23) and the dual of (I.11).

$$\begin{array}{ccccccc} 0 & & 0 & & 0 & & 0 \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ Z^\bullet_{\mathsf{top}} & & {}_\infty H^1_\Sigma(A(p))^\Gamma & \hookrightarrow & \oplus H^1({}_\infty K_v, A(p))^\Gamma & \hookrightarrow & ({}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})_\Gamma)^\wedge \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ Z^\bullet_{\mathsf{mi}} & & H^1_\Sigma(A(p)) & \hookrightarrow & \oplus H^1(K_v, A(p)) & \hookrightarrow & H^1_\Sigma(T_p\check{A})^\wedge \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ Z^\bullet_{\mathsf{bo}} & & T_{\mathsf{gl}} & \hookrightarrow & T_{\mathsf{loc}} & \hookrightarrow & ({}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma)^\wedge \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ 0 & & 0 & & 0 & & 0 \end{array} \tag{I.26}$$

The middle complex is part of Cassels sequence (I.3) and so $H^0(Z^\bullet_{\mathsf{mi}}) = 0$.

I.4.3 The control theorem

The first part of the long exact sequence is

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^{-1}(Z^\bullet_{\mathsf{bo}}) & \longrightarrow & H^{-1}(Z^\bullet_{\mathsf{mi}}) & \longrightarrow & H^{-1}(Z^\bullet_{\mathsf{top}}) & \longrightarrow & H^0(Z^\bullet_{\mathsf{bo}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \ker(b) & \longrightarrow & \mathcal{R} & \xrightarrow{b} & {}_\infty\mathcal{R}^\Gamma & \longrightarrow & \operatorname{coker}(b) & \longrightarrow & 0 \end{array} \tag{I.27}$$

From the finiteness results in lemma I.13 and lemma I.14 we conclude

Control Theorem I.15.
The map $b\colon \mathcal{R}(A/K) \longrightarrow \mathcal{R}(A/{}_\infty K)^\Gamma$ induced by the restriction is a pseudo-isomorphism. The kernel has less elements than $A(K)(p)$ while the size of the cokernel is bounded by $\prod_{v|p} \#A(K_v)(p) \cdot \prod_{v\nmid p} c_v^{(p)}$.

Although it is less important we add a second version of the control theorem, but without proof.

Proposition I.16. *The restriction induces a pseudo-isomorphism from* $\mathfrak{R}_\Sigma(A/K)$ *to* $\mathfrak{R}_\Sigma(A/{}_nK)^{\mathrm{Gal}({}_nK:K)}$.

I.5 The height pairing

We come to the construction of the p-adic height on the fine Selmer group. It is a simplification of the construction by Perrin-Riou in 1.2 of [PR92] (for the ordinary case), 2.3.2 in [PR93b] (for an elliptic curve over $\mathbb{Q}$) and 3.1.2 in [PR95]. The difference is that we are only interested in constructing the pairing on the fine Selmer group while she is constructing pairings on the Selmer groups. Her pairing depends on the choice of a complement N to the space of invariant differentials in the space of differential of the second kind modulo exact differentials. Perrin-Riou notes that the restriction to the fine Selmer group is independent of the choice of N and she makes the conjecture that the pairing affiliated with the cyclotomic extension is non-degenerate on the fine Selmer group (see [PR93b, Conjecture 3.3.7 B i] and [PR03a, Conjecture 2.5]).

Our pairing will first be constructed for the finite fine Selmer group R^k. Afterwards we can pass to the limit to obtain simultaneously a pairing on $\check{\mathfrak{R}}_\Sigma \times \mathcal{R}$ with values in $\mathbb{Q}_p/\mathbb{Z}_p$ and a $\mathbb{Z}_p$-valued pairing $\check{\mathfrak{R}}_\Sigma \times \mathfrak{R}_\Sigma$ which are compatible.

Although we are not explaining this here further, it would be possible to construct the finite height on $\check{R}^k \times R^k$ with values in $\mathbb{Z}/p^k$ using only finite levels ${}_nK : K$ of a $\mathbb{Z}_p$-extension if $n \geqslant k$.

I.5.1 Extensions

The p-adic height pairing on the fine Selmer group will be defined using extensions of $A[p^k]$ by $\mu[p^k]$; in other words, we use Ext-pairings. But instead of the abstract definition (see paragraph 0 of [Mil86]), we do everything explicitely for we will need it anyway when proving that the pairing defined over K equals another pairing obtained from Iwasawa theory.

The symbol $\oplus$ will still mean the sum over all places v in Σ. All $G_\Sigma(K)$-modules will be written additively. This applies also to $\mu[p^k]$ and $T_p\mu$.

Let k be a positive integer. Let ξ be a 1-cocycle representing a class in $R^k_\Sigma(\check{A}/K)$, so it belongs to $H^1_\Sigma(\check{A}[p^k])$ and has trivial restriction to $H^1(K_v, \check{A}[p^k])$ at all places v

in Σ.

Let W_ξ^k be a $G_\Sigma(K)$-module that is isomorphic to $\mu[p^k] \oplus A[p^k]$ as an abelian group and $\sigma \in G_\Sigma(K)$ acts on it by

$$(\zeta, Q)^\sigma = (\zeta^\sigma + \langle \xi_\sigma, Q^\sigma \rangle, Q^\sigma) \qquad \text{for all } \zeta \in \mu[p^k] \text{ and } Q \in A[p^k].$$

Here $\langle \cdot, \cdot \rangle$ denotes the Weil-pairing $\check{A}[p^k] \times A[p^k] \longrightarrow \mu[p^k]$. In particular, we have an exact sequence of $G_\Sigma(K)$-modules:

$$0 \longrightarrow \mu[p^k] \longrightarrow W_\xi^k \longrightarrow A[p^k] \longrightarrow 0. \tag{I.28}$$

Now we come to a few boring lemmata which will give an explicit construction of the height pairing, later.

Lemma I.17. *The sequence* (I.28) *is split exact as a sequence of G_υ-modules for any place υ in Σ.*

Proof. Since $\mathrm{res}_\upsilon(\xi)$ is trivial in $H^1(K_\upsilon, \check{A}[p^k])$ by definition of $R_\Sigma^k(\check{A}/K)$, there is a p^k-torsion point ξ'_υ in $\check{A}(\overline{K_\upsilon})[p^k]$ such that ${\xi'_\upsilon}^\sigma - \xi'_\upsilon = \xi_\sigma$. Now the map $s(P) = (\langle -\xi'_\upsilon, Q \rangle, Q)$ is a section of (I.28). Indeed, it is a G_υ-morphism, because

$$s(Q)^\sigma = (\langle -{\xi'_\upsilon}^\sigma, Q^\sigma \rangle + \langle \xi_\sigma, Q^\sigma \rangle, Q^\sigma) = (\langle -\xi'_\upsilon, Q^\sigma \rangle, Q^\sigma) = s(Q^\sigma).$$

□

Lemma I.18. *The connecting homomorphisms in the long exact sequence*

$$\cdots A(K)[p^k] \xrightarrow{\delta} H_\Sigma^1(\mu[p^k]) \longrightarrow H_\Sigma^1(W_\xi^k) \longrightarrow H_\Sigma^1(A[p^k]) \xrightarrow{\delta} H_\Sigma^2(\mu[p^k]) \cdots \tag{I.29}$$

are obtained as cup-pairings with ξ.

Proof. This is the "compatibility of Ext- and cup-pairings" with its beautiful proof on page 12 in [Mil86]. We only show it for the two maps in (I.29). First, let Q be an element of $A(K)[p^k]$. Then $\delta(Q) = \xi \cup Q$ because

$$(\delta(Q)_\sigma, O) = (0, Q)^\sigma - (0, Q) = (\langle \xi_\sigma, Q \rangle, O)$$

holds for any $\sigma \in G_\Sigma(K)$. Now, let ζ represent an element in $H_\Sigma^1(A[p^k])$. By definition we can compute, for any σ and τ in $G_\Sigma(K)$,

$$((\delta\zeta)_{\sigma,\tau}, O) = d(0, \zeta)_{\sigma,\tau} = -(0, \zeta_{\sigma\tau}) + (0, \zeta_\sigma) + (0, \zeta_\tau)^\sigma = (\langle \xi_\sigma, \zeta_\tau^\sigma \rangle, O).$$

Hence $\delta(\zeta) = \xi \cup \zeta$. □

Lemma I.19. *We have the following diagram*

$$\begin{array}{ccccccccc} A(K)[p^k] & \longrightarrow & H^1_\Sigma(\mu[p^k]) & \longrightarrow & H^1_\Sigma(W^k_\xi) & \longrightarrow & H^1_\Sigma(A[p^k]) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus H^1(K_\upsilon, \mu[p^k]) & \to & \oplus H^1(K_\upsilon, W^k_\xi) & \to & \oplus H^1(K_\upsilon, A[p^k]) & \longrightarrow & 0 \end{array} \tag{I.30}$$

Proof. Everything is obvious from lemma I.17, except the upper right zero. We would expect instead the commutative diagram

$$\begin{array}{ccc} H^1_\Sigma(A[p^k]) & \longrightarrow & H^2_\Sigma(\mu[p^k]) \\ \downarrow & & \downarrow \\ \oplus H^1(K_\upsilon, A[p^k]) & \to & \oplus H^2(K_\upsilon, \mu[p^k]) \end{array}$$

but since the arrow on the bottom is trivial and the arrow on the right is injective by global class field theory, the top arrow is trivial as well. □

Let η be an element of $R^k_\Sigma(A/K)$. By the previous lemma, there is a 1-cochain ω with values in $\mu[p^k]$ such that $d\omega = \xi \cup \eta$. For every υ in Σ, choose a p^k-torsion point η'_υ such that $\mathrm{res}_\upsilon(\eta) = d\eta'_\upsilon$.

Lemma I.20. *The snake map in diagram* (I.30) *maps η to an element of $H^1(K_\upsilon, \mu[p^k])$ that can be represented by the 1-cocycle*

$$\omega_\upsilon = -\mathrm{res}_\upsilon(\omega) - (\mathrm{res}_\upsilon(\xi) \cup \eta'_\upsilon).$$

Proof. First we prove that ω_υ is a 1-cocycle:

$$\begin{aligned} -d\omega_\upsilon &= \mathrm{res}_\upsilon(d\omega) + (\mathrm{res}_\upsilon(d\xi) \cup \eta'_\upsilon) - (\mathrm{res}_\upsilon(\xi) \cup d\eta'_\upsilon) \\ &= \mathrm{res}_\upsilon(\xi \cup \eta) - (\mathrm{res}_\upsilon(\xi) \cup \mathrm{res}_\upsilon(\eta)) = 0. \end{aligned}$$

Now choose a p^k-torsion point ξ'_υ as in the proof of lemma I.17, i.e. such that $d\xi'_\upsilon = \mathrm{res}_\upsilon(\xi)$. Then $d(\xi'_\upsilon \cup \eta'_\upsilon) = (\mathrm{res}_\upsilon(\xi) \cup \eta'_\upsilon) + (\xi'_\upsilon \cup \mathrm{res}_\upsilon(\eta))$ shows us that the class of ω_υ can also be represented by $\omega'_\upsilon = -\mathrm{res}_\upsilon(\omega) + (\xi'_\upsilon \cup \mathrm{res}_\upsilon(\eta))$.

The map $\sigma \mapsto (-\omega_\sigma, \eta_\sigma)$ is a cocycle, since

$$\begin{aligned} d(-\omega, \eta)_{\sigma,\tau} &= -(-\omega_{\sigma\tau}, \eta_{\sigma\tau}) + (-\omega_\sigma, \eta_\sigma) + (-\omega_\tau, \eta_\tau)^\sigma \\ &= (\omega_{\sigma\tau} - \omega_\sigma - \omega^\sigma_\tau + \langle \xi_\sigma, \eta^\sigma_\tau \rangle, O) = (-\langle \xi_\sigma, \eta^\sigma_\tau \rangle + \langle \xi_\sigma, \eta^\sigma_\tau \rangle, O) = 0 \end{aligned}$$

and it is therefore a lifting of η to $H^1_\Sigma(W^k_\xi)$. The restriction of this 1-cocycle to $H^1(K_\upsilon, W^k_\xi)$ differs from the image of the image of ω'_υ by

$$(\omega'_\upsilon, O) - \mathrm{res}_\upsilon(-\omega, \eta) = (\xi'_\upsilon \cup \mathrm{res}_\upsilon(\eta), -\mathrm{res}_\upsilon(\eta)).$$

In the proof of lemma I.17, we showed that this is $-s(\mathrm{res}_\upsilon(\eta))$ which is, by assumption on η, a coboundary. □

I.5.2 Definition of the height

It is exactly the snake-map in diagram (I.30) that gives us the desired height pairing at finite level. This is, for every $\xi \in R^k_\Sigma(\check{A}/K)$, a map

$$H_\xi \colon R^k_\Sigma(A/K) \longrightarrow \widehat{H^1_\Sigma(\mathbb{Z}/p^k)}.$$

because, in fact, the cokernel of the first vertical arrow in diagram (I.30) lies in the dual of $H^1_\Sigma(\mathbb{Z}/p^k)$ by the exact sequence of Poitou-Tate (I.5). Differently formulated, this is a pairing

$$\begin{aligned} R^k_\Sigma(\check{A}/K) \times R^k_\Sigma(A/K) &\longrightarrow \mathbb{Z}/p^k\mathbb{Z} \\ (\xi, \eta) &\longmapsto \langle \xi, \eta \rangle_\lambda = H_\xi(\eta)(\lambda) \end{aligned}$$

for every λ in $H^1_\Sigma(\mathbb{Z}/p^k) = \mathrm{Hom}(G_\Sigma(K), \mathbb{Z}/p^k\mathbb{Z})$.

Explicitly, if we choose a 1-cochain ω_v with values in $\mu[p^k]$ as in lemma I.20, then we can calculate the map g in (I.6) as

$$\langle \xi, \eta \rangle_\lambda = g\left(\sum \omega_v\right)(\lambda) = \sum_{v \in \Sigma} \mathrm{inv}_v(\omega_v \cup \lambda).$$

Here the cup-product is

$$H^1(K_v, \mu[p^k]) \cup H^1(K_v, \mathbb{Z}/p^k) \longrightarrow H^2(K_v, \mu[p^k]) \xrightarrow{\mathrm{inv}_v} \mathbb{Z}/p^k\mathbb{Z}.$$

From the description of ω_v in lemma I.20, it is immediate that the pairing is bilinear.

I.5.3 The p-divisible height pairing

Let ξ be in $\mathfrak{R}_\Sigma(\check{A}/K)$. This is a sequence of elements in $R^k_\Sigma(\check{A}/K)$ giving each an extensions W^k_ξ. They are compatible in the sense that we can define $W_\xi = \varinjlim W^k_\xi$ as an extension of $A(p)$ by $\mu(p)$. By taking inductive limits on the diagram (I.30), the following diagram is obtained.

$$\begin{array}{ccccccccc} & & & & & & \mathcal{R} & & \\ & & & & & & \downarrow & & \\ A(K)(p) & \longrightarrow & H^1_\Sigma(\mu(p)) & \longrightarrow & H^1_\Sigma(W_\xi) & \longrightarrow & H^1_\Sigma(A(p)) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus H^1(K_v, \mu(p)) & \longrightarrow & \oplus H^1(K_v, W_\xi) & \longrightarrow & \oplus H^1(K_v, A(p)) & \longrightarrow & 0 \\ & & \downarrow g & & & & & & \\ H_\xi & \longrightarrow & H^1_\Sigma(\mathbb{Z}_p)^\wedge & & & & & & \end{array} \tag{I.31}$$

This is the *p-divisible pairing associated to λ*; for every λ in $H^1_\Sigma(\mathbb{Z}_p)$, that is a homomorphism from $G_\Sigma(K)$ to $\mathbb{Z}_p$, we obtain a pairing

$$\begin{aligned} \mathfrak{R}_\Sigma(\check{A}/K) \times \mathcal{R}(A/K) &\longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \\ (\xi, \eta) &\longmapsto \langle \xi, \eta \rangle_\lambda \end{aligned}$$

I.5.4 The p-adic height pairing

Let ξ be in $\mathfrak{R}_\Sigma(\check{A}/K)$. The W_ξ^k in the sequence of extensions are also compatible with respect to the $[p]$-maps, hence there is a $G_\Sigma(K)$-module T_ξ which is an extension of T_pA by $T_p\mu$. Again, we get a diagram with a snake map:

$$\begin{array}{ccccccccc}
 & & & & & & \mathfrak{R}_\Sigma & \longrightarrow & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & H^1_\Sigma(T_p\mu) & \longrightarrow & H^1_\Sigma(T_\xi) & \longrightarrow & H^1_\Sigma(T_pA) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \oplus H^1(K_\upsilon, T_p\mu) & \twoheadrightarrow & \oplus H^1(K_\upsilon, T_\xi) & \twoheadrightarrow & \oplus H^1(K_\upsilon, T_pA) & \longrightarrow & 0 \\
 & & \downarrow g & & & & & & \\
 & \xrightarrow{H_\xi} & G_\Sigma(K)^{p\text{-ab}} & & & & & & \\
 & & \downarrow & & & & & & \\
 & & \mathrm{Cl}(\mathcal{O}_\Sigma)(p) & & & & & &
\end{array} \tag{I.32}$$

Here we have a map $H_\xi\colon \mathfrak{R}_\Sigma(A/K) \longrightarrow G_\Sigma(K)^{p\text{-ab}}$ which actually takes values in $G_\Sigma(H)^{p\text{-ab}}$ where H is the p-Hilbert class field of K. Given a λ in $H^1_\Sigma(\mathbb{Z}_p)$ as before, we can construct the *p-adic pairing associated to λ* as follows

$$\begin{array}{rcl}
\mathfrak{R}_\Sigma(\check{A}/K) \times \mathfrak{R}_\Sigma(A/K) & \longrightarrow & \mathbb{Z}_p \\
(\xi, \eta) & \longmapsto & \langle \xi, \eta \rangle_\lambda = \lambda(H_\xi(\eta))
\end{array}$$

which can be written explicitly as

$$\langle \xi, \eta \rangle_\lambda = \lambda \circ g\left(\prod \omega_\upsilon\right) = \sum_{\upsilon \in \Sigma} \lambda_\upsilon(\alpha_\upsilon) = \sum_{\upsilon \in \Sigma} \mathrm{inv}_\upsilon(\omega_\upsilon \cup \lambda)$$

with $\alpha_\upsilon \in (K_\upsilon^\times)^\star$ corresponding to $\omega_\upsilon \in H^1(K_\upsilon, T_p\mu)$ via the Kummer map. Here the map λ_υ is the composition of λ with Artin's reciprocity map as explained in I.2.2.

By the fact that the group $\mathfrak{R}_\Sigma$ has finite index in $\mathfrak{R}$, we can extend the $\mathbb{Z}_p$-valued pairing to a pairing between $\mathfrak{R}(\check{A}/K)$ and $\mathfrak{R}(A/K)$ with values in $\mathbb{Q}_p$ with small denominators.

The *p-adic regulator* associated to λ is the value in $\mathbb{Q}_p$ of the determinant of this pairing. It is well-defined up to a unit in $\mathbb{Z}_p^\times$. We say that the p-adic height associated to λ is non-degenerate on the fine Selmer group if the regulator is not zero. Of course, we should mention here the very important conjecture due to Perrin-Riou mentioned in the beginning of this section.

Conjecture I.21. *If λ defines the cyclotomic $\mathbb{Z}_p$-extension, then the pairing $\langle \cdot, \cdot \rangle_{cyc}$ is non-degenerate on the fine Selmer groups $\mathfrak{R}(\check{A}/K) \times \mathfrak{R}(A/K)$.*

Moreover the pairing can be extended. In fact, the local conditions on the cocycle ξ are not needed. Hence there is a natural pairing

$$H^1_\Sigma(K, T_p\check{A}) \times \mathfrak{R}_\Sigma(A/K) \longrightarrow \mathbb{Z}_p. \tag{I.33}$$

Lemma I.22. *The map* $a\colon \mathrm{Hom}(\mathcal{R}(A/K), \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{R}_\Sigma(A/K), \mathbb{Z}_p)$ *in* (I.22) *maps the* p*-divisible pairing* $\langle \xi, \cdot \rangle_\lambda$ *to the corresponding* p*-adic pairing for all* $\lambda \in H^1_\Sigma(K, \mathbb{Z}_p)$ *and* $\xi \in \mathfrak{R}_\Sigma(\check{A}/K)$.

This is clear from the way we passed simultaneously to the limits. In the case that the abelian variety A is principally polarised, then the induced bilinear form on $\mathfrak{R}_\Sigma(A/K)$ with values in $\mathbb{Z}_p$ is symmetric. This can be verified directly on the cocycles. For elliptic curves, it will be apparent anyway from the formula using sigma functions.

I.6 Iwasawa theoretic height

In the article [Sch85], Schneider defines an analytic and an algebraic height for the classical Selmer group of an abelian varieties with ordinary reduction at all places above p. The algebraic height uses Iwasawa theory and is closely modelled on the use of the intersection form on the Néron-Severi group in the function field case (see [Tat66]). We follow here the description of Perrin-Riou in [PR92] (and the easier explanation in [PR93a]).

We fix a $\mathbb{Z}_p$-extension ${}_\infty K$ via a non-trivial character $\lambda \in H^1_\Sigma(\mathbb{Z}_p)$ and we choose a generator γ in the Galois group Γ.

I.6.1 The map e

There is a map coming from the Hochschild-Serre spectral sequence, see (I.34). An explicit construction, depending on the choice of γ, is given here:

$$e\colon {}_\infty H^1_\Sigma(A(p))_\Gamma \longrightarrow H^2_\Sigma(A(p)). \tag{I.34}$$

Suppose η is a 1-cocycle with values in $A(p)$ representing an element in the source of e. It can be written as a sequence of cocycles $({}_n\eta)$ representing elements of $H^1_\Sigma({}_nK, A(p))$ with ${}_{n+m}\mathrm{res}({}_n\eta) = {}_{n+m}\eta$ for n large enough. (Here and it what follows, the notation ${}_n\mathrm{res}$ and ${}_n\mathrm{cor}$ denote the restriction and corestriction to $H^i_\Sigma({}_nK, \cdot)$.)

Next, λ gives rise to an element l in ${}_\infty\mathfrak{H}^1_\Sigma(\mathbb{Z}_p)$, that is a sequence ${}_nl \in H^1_\Sigma({}_nK, \mathbb{Z}_p)$ defined by that ${}_nl = p^{-n} \cdot {}_n\mathrm{res}(\lambda)$. Indeed,

$${}_n\mathrm{cor}({}_{n+m}l) = p^{-n-m} \cdot {}_n\mathrm{cor} \circ {}_{n+m}\mathrm{res}(\lambda) = p^{-n-m} \cdot p^m \cdot {}_n\mathrm{res}(\lambda) = {}_nl.$$

Let us look at ${}_n\eta \cup {}_nl \in H^2_\Sigma({}_nK, A(p))$. The following calculation

$$\begin{aligned} {}_0\mathrm{cor}({}_{n+m}\eta \cup {}_{n+m}l) &= {}_0\mathrm{cor} \circ {}_n\mathrm{cor}\,({}_{n+m}\mathrm{res}({}_n\eta) \cup {}_{n+m}l) = {}_0\mathrm{cor}\,({}_n\eta \cup {}_n\mathrm{cor}({}_{n+m}l)) \\ &= {}_0\mathrm{cor}\,({}_n\eta \cup {}_nl) \end{aligned}$$

shows that its corestriction to K does not depend on n for sufficiently large n and that so it does not depend on the chosen limit sequence for η. We define $e(\eta) = \lambda(\gamma)^{-1} \cdot {}_0\mathrm{cor}\,({}_n\eta \cup {}_nl)$.

In particular, if η is the restriction of an element in $H^1_\Sigma(A(p))$ it can be written simply as $\lambda(\gamma)^{-1} \cdot (\eta \cup \lambda)$.

This is the map "$\alpha_{S,\gamma}$" in [PR92, paragraph 4.4.7]. It is injective and the cokernel is ${}_\infty H^2_\Sigma(A(p))^\Gamma$. The factor $\lambda(\gamma)^{-1}$ is introduced here, so that e becomes injective and does not depend on λ but only on ${}_\infty K$. Note that since γ is a generator of Γ, the cocycle $\lambda(\gamma)^{-1} \cdot {}_nl$ still has integral values and is actually surjective onto $\mathbb{Z}_p$.

I.6.2 The map f

The first global duality statement in corollary I.3 gave us an isomorphism

$$f\colon \mathfrak{R}_\Sigma(\check{A}/K) \longrightarrow H^2_\Sigma(A(p))^\wedge. \tag{I.35}$$

According to [NeScWi00, page 423], we can explicitly calculate it the following way. Let ξ represent an element in $\check{\mathfrak{R}}_\Sigma$ and let ζ represent something in $H^2_\Sigma(A(p))$. Since $\xi \cup \zeta$ belongs to $H^3_\Sigma(T_p\mu) = 0$, there is a cochain ψ with values in $T_p\mu$ such that $d\psi = \xi \cup \zeta$. For every place υ in Σ, we choose a cochain ξ'_υ with values in $T_p\check{A}$ and a cochain ζ'_υ with values in $A(p)$ such that $d\xi'_\upsilon = \mathrm{res}_\upsilon(\xi)$ and $d\zeta'_\upsilon = \mathrm{res}_\upsilon(\zeta)$. Then the cochains

$$-\mathrm{res}_\upsilon(\psi) + (\xi'_\upsilon \cup \mathrm{res}_\upsilon(\zeta)) \quad \text{and} \quad -\mathrm{res}_\upsilon(\psi) - (\mathrm{res}_\upsilon(\xi) \cup \zeta'_\upsilon)$$

are both cocycles and represent the same element in $H^1(K_\upsilon, T_p\mu)$. The map f is defined by

$$f(\xi)(\zeta) = -\sum_{\upsilon \in \Sigma} \mathrm{inv}_\upsilon \left(\mathrm{res}_\upsilon(\psi) + (\mathrm{res}_\upsilon(\xi) \cup \zeta'_\upsilon)\right).$$

I.6.3 The other maps

Moreover, we have the following maps

$$\begin{aligned} b&\colon \mathcal{R} \longrightarrow {}_\infty\mathcal{R}^\Gamma \\ c&\colon {}_\infty\mathcal{R}^\Gamma \longrightarrow {}_\infty\mathcal{R}_\Gamma \\ d&\colon {}_\infty\mathcal{R}_\Gamma \longrightarrow {}_\infty H^1_\Sigma(A(p))_\Gamma \end{aligned}$$

The map b comes from the control theorem I.15, the map c is induced by the identity and the map d is induced from the inclusion.

If η represents an element of $\mathcal{R}$, then ${}_\infty\mathrm{res}(\eta)$ represents $d \circ c \circ b(\eta)$.

I.6.4 The decomposition of the height

We prove now that the composition of the described maps gives a multiple of the height map. We arrange things in a big diagram that resembles the diagram (5.12) in Tate's article [Tat66]. We could equally well draw a picture like in proposition 6.2 in [Sch85].

Proposition I.23. *With the above notations the p-divisible pairing satisfies*

$$\lambda(\gamma)^{-1} \cdot \langle \xi, \eta \rangle_\lambda = f(\xi)(e \circ d \circ c \circ b(\eta))$$

for all $\xi \in \mathfrak{R}_\Sigma(\check{A}/K)$ and $\eta \in \mathcal{R}(A/K)$. Similarly, the p-adic pairing

$$h_\lambda \colon \mathfrak{R}_\Sigma(\check{A}/K) \longrightarrow \mathrm{Hom}(\mathfrak{R}_\Sigma(A/K), \mathbb{Z}_p)$$

can be calculated as the composition of maps in the commutative diagram

$$\begin{array}{ccccc} \mathcal{R}(A/K) & \xleftarrow{\hat{a}} & \mathrm{Hom}(\mathfrak{R}_\Sigma(A/K), \mathbb{Z}_p)^\wedge & \xrightarrow{\frac{1}{\lambda(\gamma)} \cdot \hat{h}_\lambda} & \mathfrak{R}_\Sigma(\check{A}/K)^\wedge \\ \downarrow{\scriptstyle b} & & & & \uparrow{\scriptstyle \hat{f}} \\ \mathcal{R}(A/{}_\infty K)^\Gamma & \xrightarrow{c} & \mathcal{R}(A/{}_\infty K)_\Gamma & \xrightarrow{d} & {}_\infty H^1_\Sigma(A(p))_\Gamma \xrightarrow{e} H^2_\Sigma(A(p)) \end{array} \tag{I.36}$$

Proof. As explained above in the descriptions of the maps b, c, d and e, the cocycle $\lambda(\gamma)^{-1} \cdot (\eta \cup \lambda)$ represents $\zeta = e \circ d \circ c \circ b(\eta)$. We can specify the choice of ψ in the description of f as $\lambda(\gamma)^{-1} \cdot (\omega \cup \lambda)$ using lemma I.20. Similarly ζ'_υ can be chosen to be $\lambda(\gamma)^{-1} \cdot (\eta'_\upsilon \cup \mathrm{res}_\upsilon(\lambda))$. Then

$$\begin{aligned} f(\xi)(\zeta) &= -\sum_{\upsilon \in \Sigma} \mathrm{inv}_\upsilon \left(\lambda(\gamma)^{-1} \cdot \mathrm{res}_\upsilon(\omega \cup \lambda) + \lambda(\gamma)^{-1} \cdot (\mathrm{res}_\upsilon(\xi) \cup \eta'_\upsilon \cup \lambda) \right) \\ &= \lambda(\gamma)^{-1} \cdot \sum_{\upsilon \in \Sigma} \mathrm{inv}_\upsilon(\omega_\upsilon \cup \lambda) = \lambda(\gamma)^{-1} \cdot \langle \xi, \eta \rangle_\lambda, \end{aligned}$$

using the definition $-\omega_\upsilon = \mathrm{res}_\upsilon(\omega) + \mathrm{res}_\upsilon(\xi) \cup \eta'_\upsilon$ in lemma I.20. This proves the statement for the p-divisible pairing and the compatibility in I.22 finishes the proof. □

I.7 The weak Leopoldt conjecture

We start to deduce results from our p-adic height pairing. From now on, all results will depend on the non-degeneracy of the pairing. The first result, proposition I.26, is a widely believed conjecture, called the weak Leopoldt conjecture. That it can be deduced and numerically verified from the non-degeneracy of the height on the fine Selmer group was also noted by Perrin-Riou in corollaire 3.4.3 in [PR95]. For the general formulation of the weak Leopoldt conjecture due to Greenberg and Schneider, we refer to [PR92, Conjecture 3.2.2] and appendix B in [PR95]. See also section VI.4 for more heuristic information on the conjecture.

Lemma I.24. *If the p-adic height pairing between $\check{\mathfrak{R}}_\Sigma$ and $\mathfrak{R}_\Sigma$ with values in $\mathbb{Z}_p$ is non-degenerate, then ${}_\infty H^2_\Sigma(A(p))^\Gamma = 0$.*

Proof. The map $\lambda(\gamma)^{-1} \cdot \hat{h} = \hat{f} \circ e \circ d \circ c \circ b \circ \hat{a}$ is a pseudo-isomorphism under the hypothesis. Since f is an isomorphism, the cokernel of e is a quotient of the cokernel of the pseudo-isomorphism $\hat{h}$. Hence the cokernel of the map e is finite and this is precisely the dual of the group we would like to see disappear by the remark at the end of the definition of e. But on the other hand, this dual is a subgroup of a free $\mathbb{Z}_p$-module $\check{\mathfrak{R}}_\Sigma$ by proposition I.11, hence zero. □

An old trick in Iwasawa theory is the following

Lemma I.25. *Let M be a discrete p-divisible abelian Γ-module of finite corank with $M^\Gamma = 0$. Then $M = 0$.*

Proof. Let $\alpha \in M$. Since M is the union of $M^{{}_n\Gamma}$ as ${}_n\Gamma$ runs through the open subgroups of Γ, we find a p-primary $N = M^{{}_n\Gamma}$ to which α belongs with an action of $G = \Gamma/{}_n\Gamma \cong \mathbb{Z}/p^n\mathbb{Z}$ such that $N^G = 0$. Let X be the set of elements of exact order p in N. As N is of finite type, X contains $p^k - 1$ elements for some $k \geqslant 0$. Next, X is the reunion of orbits which must have a cardinality dividing $\#G = p^n$ and $1 = p^0$ is excluded because $N^G = 0$. Whence $X = \emptyset$, $N = 0$ and $\alpha = 0$. □

We know that the Γ-module ${}_\infty H^2_\Sigma(A(p))$ is divisible, since $G_\Sigma({}_\infty K)$ is of cohomological dimension 2. The two lemmata together give

Proposition I.26. *If the p-adic height pairing is non-degenerate on the fine Selmer group, then $H^2(G_\Sigma({}_\infty K), A(p)) = 0$.*

As a consequence we can simplify the last term in the global duality over ${}_\infty K$.

Corollary I.27. *If the p-adic height pairing is non-degenerate on the fine Selmer group, then*

$$0 \longrightarrow {}_\infty\mathcal{R} \longrightarrow {}_\infty H^1_\Sigma(A(p)) \longrightarrow \oplus H^1({}_\infty K_v, A(p)) \longrightarrow \widehat{{}_\infty\text{Ш}^1_\Sigma(T_p\check{A})} \longrightarrow 0. \qquad \text{(I.37)}$$

I.8 The fine Selmer group as a Λ-module

The Iwasawa-algebra associated to the $\mathbb{Z}_p$-extension ${}_\infty K$ is denoted by $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$. Our choice of a topological generator γ provides us with an isomorphism between Λ and $\mathbb{Z}_p[\![T]\!]$, where T is a indeterminate corresponding to $\gamma - 1$. For all matters on Λ-modules, the reader is referred to [NeScWi00, Chapter V].

In this section, the structure of $\widehat{{}_\infty\mathcal{R}}$ as a Λ-module is considered. After a lemma on the characteristic power-series of a Λ-module, two results on this module are deduced. The first is the analogue of a conjecture of Mazur for the classical Selmer group.

As in Tate's article [Tat66], we define

$$z(f) = \frac{|\#\operatorname{coker}(f)|_p}{|\#\ker(f)|_p} = \frac{\#\ker(f)}{\#\operatorname{coker}(f)} \qquad \text{(I.38)}$$

for any pseudo-isomorphism f between $\mathbb{Z}_p$-modules. Here is a reformulation of his lemma z.4.

Lemma I.28. *Let X be a finitely generated Λ-module.*

i). The Λ-rank of X equals

$$\operatorname{rank}_\Lambda(X) = \operatorname{rank}_{\mathbb{Z}_p}(X_\Gamma) - \operatorname{rank}_{\mathbb{Z}_p}(X^\Gamma).$$

ii). If X is Λ-torsion, then the order of vanishing of the characteristic power series f_X at $T = 0$ is greater or equal to $\operatorname{rank}_{\mathbb{Z}_p}(X^\Gamma)$.

iii). The map $g\colon X^\Gamma \longrightarrow X_\Gamma$ induced by the identity, is a pseudo-isomorphism if and only if X is Λ-torsion and the cokernel of g is finite. In this case the characteristic power series looks like

$$f_X(T) = z(g)^{-1} \cdot T^{\operatorname{rank}_{\mathbb{Z}_p}(X^\Gamma)} + \cdots \pmod{\mathbb{Z}_p^\times}.$$

Proof. First note that

$$0 \longrightarrow X^\Gamma \longrightarrow X \xrightarrow{T} X \longrightarrow X_\Gamma \longrightarrow 0.$$

If $X = \Lambda$, then $X^\Gamma = 0$ and $X_\Gamma = \mathbb{Z}_p$, so $\operatorname{rank}_{\mathbb{Z}_p}(X_\Gamma) - \operatorname{rank}_{\mathbb{Z}_p}(X^\Gamma) = 1$. Next if $X = \Lambda/(p^\mu) \cong \mathbb{Z}/p^\mu\mathbb{Z}[\![T]\!]$ for some integer $\mu > 0$, then $X^\Gamma = 0$ and $X_\Gamma = \mathbb{Z}/p^\mu\mathbb{Z}$. So in this case g is a pseudo-isomorphism and $z(g) = p^{-\mu}$. If $X = \Lambda/(f) = \mathbb{Z}_p[T]/(f)$ for some polynomial f not divisible by T, then $X^\Gamma = 0$ and $X_\Gamma = \Lambda/(T, f) = \mathbb{Z}_p/(f(0))$. Hence g is a pseudo-isomorphism and $z(g) = p^{-\operatorname{ord}_p(f(0))}$. If X is finite then $z(g) = 1$ by the argument used in the proof of lemma I.12.

Now if $X = \Lambda/(T^n)$ for $n \geqslant 1$, then both X^Γ and X_Γ are isomorphic to $\mathbb{Z}_p$ and the map g is the zero map if $n > 1$ and the identity if $n = 1$.

The lemma follows from the structure theorem for finitely generated Λ-modules (see [NeScWi00, Theorem V.3.8]). □

The following is the analogue of a conjecture of Mazur for the classical Selmer group. In the ordinary case, it follows from the non-degeneracy of the height pairing. In our case it is even easier because it is actually equivalent to the weak Leopoldt conjecture. See [PR95, Proposition 1.3.2].

Proposition I.29. *If the p-adic height on the fine Selmer group is non-degenerate, then the dual of $\mathcal{R}(A/_\infty K)$ is Λ-torsion.*

Proof. We follow the proof of lemma 3.1 in [CoSu]. In the sequence (I.14), we saw that the dual of ${}_\infty\mathcal{R}$ is contained in ${}_\infty\text{Ш}^2_\Sigma(T_p\check{A})$. It is therefore enough to show that the latter is Λ-torsion.

To achieve this, we will use a spectral sequence due to Jannsen (see [Jan94]):

$$E_2^{p,q} = \operatorname{Ext}^p_\Lambda\left({}_\infty H^q_\Sigma(\check{A}(p))^\wedge, \Lambda\right) \Longrightarrow {}_\infty\text{Ш}^{p+q}_\Sigma(T_p\check{A})$$

Thanks to proposition I.26, we have that ${}_\infty H^2_\Sigma(\check{A}(p)) = 0$, so corollary 2 of [Jan94] gives an exact sequence

$$\operatorname{Ext}^2_\Lambda(\check{A}({}_\infty K)(p)^\wedge, \Lambda) \longrightarrow {}_\infty\text{Ш}^2_\Sigma(T_p\check{A}) \longrightarrow \operatorname{Ext}^1_\Lambda({}_\infty H^1_\Sigma(\check{A}(p))^\wedge, \Lambda) \tag{I.39}$$

Now by proposition 5.5.3 in [NeScWi00], we have that the first term is finite and the last term is Λ-torsion. □

A little bit more is contained in the following statement that the non-degeneracy of the height pairing implies the "semi-simplicity at $T = 0$". In case the height is degenerate, one still expects the fine Selmer group to be Λ-torsion, but it might not be a semi-simple module anymore. This question will be treated in I.11.

Proposition I.30. *If the p-adic height on the fine Selmer is non-degenerate, then the map $c\colon {}_\infty\mathcal{R}^\Gamma \longrightarrow {}_\infty\mathcal{R}_\Gamma$ is a pseudo-isomorphism.*

Proof. From the assumption that $\hat{h}$ is a pseudo-isomorphism, and the knowledge that both $\hat{a}$ and b are pseudo-isomorphisms, we can conclude that the kernel of c is finite. Hence the cokernel of $\hat{c}$ is finite. Now, part iii) of lemma I.28 proves the proposition. □

I.9 The Euler characteristic

For a Λ-torsion module X such that the map g in lemma I.28 is a pseudo-isomorphism, the value of $z(g)^{-1} = z(\hat{g})$ is often referred to as the Euler-characteristic. It is the first coefficient of the characteristic power-series. In the classical case, the calculations are due to Schneider [Sch85] and Perrin-Riou [PR82] where the result equals the expected leading term of the p-adic L-function as explained in (1) in the introduction.

We proceed now to the calculation of the Euler characteristic of the dual of ${}_\infty\mathcal{R}$. In the whole section it is assumed that the p-adic height pairing for a fixed λ is non-degenerate on the fine Selmer group.

So all maps but d in the decomposition diagram (I.36) are known to be pseudo-isomorphisms: a by proposition I.11, b by proposition I.15, c by proposition I.30 and e by lemma I.24. Therefore $d\colon \mathcal{R}(A/{}_\infty K)_\Gamma \longrightarrow H^1_\Sigma({}_\infty K, A(p))_\Gamma$ is a pseudo-isomorphism as well. Since the target is known, by lemma I.24, to be isomorphic to the divisible group $H^2_\Sigma(A(p))$, the cokernel of d must be trivial.

Lemma I.31. *The map* $\oplus H^1({}_\infty K_v, A(p))^\Gamma \longrightarrow \widehat{{}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})}^\Gamma$ *is surjective.*

Proof. The weak Leopoldt conjecture, proven in proposition I.26, implies that the map $\oplus H^1({}_\infty K_v, A(p)) \longrightarrow \widehat{{}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})}$ in (I.15) is surjective. Let ${}_\infty C$ be the kernel of this map or equally the cokernel of the inclusion of ${}_\infty\mathcal{R}$ in ${}_\infty H^1_\Sigma(A(p))$. We get the following exact sequence

$$\begin{aligned} 0 \longrightarrow {}_\infty\mathcal{R}^\Gamma \longrightarrow {}_\infty H^1_\Sigma(A(p))^\Gamma \longrightarrow {}_\infty C^\Gamma \longrightarrow \\ \longrightarrow {}_\infty\mathcal{R}_\Gamma \xrightarrow{d} {}_\infty H^1_\Sigma(A(p))_\Gamma \longrightarrow {}_\infty C_\Gamma \longrightarrow 0 \end{aligned} \tag{I.40}$$

From the above remark that d is surjective, we can conclude that ${}_\infty C_\Gamma = 0$ and so

$$0 \longrightarrow {}_\infty C^\Gamma \longrightarrow \oplus H^1({}_\infty K_v, A(p))^\Gamma \longrightarrow \widehat{{}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})}^\Gamma \longrightarrow {}_\infty C_\Gamma = 0 \tag{I.41}$$

concludes the proof. □

We return now to the short exact sequence of complexes (I.26). The second part of the long exact sequence is

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(Z^\bullet_{\mathrm{top}}) & \to & H^1(Z^\bullet_{\mathrm{bo}}) & \to & H^1(Z^\bullet_{\mathrm{mi}}) & \to & H^1(Z^\bullet_{\mathrm{top}}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \ker(d) & \longrightarrow & {}_\infty\mathcal{R}_\Gamma & \longrightarrow & \widehat{\mathfrak{R}_\Sigma} & \longrightarrow & 0 & & \end{array}$$

The last equality comes from the previous lemma; while the first one can be derived from the proof of the previous lemma: By definition $H^0(Z^\bullet_{\mathrm{top}})$ is the cokernel of ${}_\infty H^1_\Sigma(A(p))^\Gamma \longrightarrow {}_\infty C^\Gamma$ because the latter is the kernel of the following map in the complex as seen in (I.41). By (I.40), this cokernel is $\ker(d)$.

We write out the dual of the right hand side of (I.26).

$$\begin{array}{ccccccccccc} & & & & & & 0 & & 0 & & \\ & & & & & & \downarrow & & \downarrow & & \\ & & & & & & \oplus H^1({}_\infty K_v, T_p\check{A})_\Gamma & \leftarrow & {}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})_\Gamma & \leftarrow & 0 \\ & & & & & & \mathrm{cor}\downarrow & & \mathrm{cor}\downarrow & & \downarrow \\ & & & & & & \oplus H^1(K_v, T_p\check{A}) & \leftarrow & H^1_\Sigma(T_p\check{A}) & \leftarrow & \check{\mathfrak{R}}_\Sigma & \leftarrow & 0 \\ & & & & & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \leftarrow & \widehat{T_{\mathrm{gl}}} & \leftarrow & \widehat{T_{\mathrm{loc}}} & \leftarrow & {}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma & \leftarrow & \widehat{{}_\infty\mathcal{R}_\Gamma} & \leftarrow & 0 \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \ker(d) & & \end{array} \qquad \text{(I.42)}$$

We can conclude from lemma I.14 and from the finiteness of $\ker(d)$ that there is an injection of $\check{\mathfrak{R}}_\Sigma$ into the cokernel of corestriction ${}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma$ with image of finite index. Denote be J_Σ the finite cokernel. Now there is also a map from $\check{\mathfrak{R}}$ to ${}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma$ whose restriction to $\check{\mathfrak{R}}_\Sigma$ is the injection; this map is defined as the composition of the inclusion $\check{\mathfrak{R}}$ into $H^1_\Sigma(T_p\check{A})$ followed by the quotient by the image from ${}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})_\Gamma$.

Proposition I.32. *Suppose the p-adic height associated to λ on the fine Selmer group is non-degenerate. Then there is an injection $\mathfrak{R}(\check{A}/K)$ into the cokernel ${}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma$ of the corestriction from ${}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})_\Gamma$ to $H^1_\Sigma(K, T_p\check{A})$ with finite cokernel, say J_0.*

Proof. The map must have finite kernel because $\check{\mathfrak{R}}_\Sigma$ has finite index in $\check{\mathfrak{R}}$. But $\check{\mathfrak{R}}$ is $\mathbb{Z}_p$-free by I.11. □

We conclude that $\#J_\Sigma = [\check{\mathfrak{R}} : \check{\mathfrak{R}}_\Sigma] \cdot \#J_0$. This is so far all we can say about this index. It turns out in the end that we can often prove via the Euler characteristic that the cokernel J_0 is actually trivial. Numerical calculations are done in the last chapter VI. See also I.12 for further information on this proposition.

Theorem I.33.
Suppose the p-adic height associated to λ on the fine Selmer group is non-degenerate. If we denote by r the corank of $\mathcal{R}(A/K)$, then the characteristic power series of the dual of $\mathcal{R}(A/_\infty K)$ is of the form

$$f_{\mathcal{R}}(T) = \frac{\mathrm{Reg}_\lambda(\mathfrak{R}(\check{A}/K), \mathfrak{R}(A/K))}{\lambda(\gamma)^r} \cdot \frac{\#T_{loc} \cdot \#\mathcal{R}(A/K)^\star}{\#T_{gl} \cdot \#J_0 \cdot \#I_0} \cdot T^r + \cdots$$

where Reg_λ is the p-adic regulator associated to λ.

Proof. First, the lower row in the diagram (I.42) yields

$$\begin{aligned}
\#J_\Sigma &= \#ker(d) \cdot \#\,\mathrm{im}({}_\infty\mathfrak{H}^2_\Sigma(T_p\check{A})^\Gamma \longrightarrow \widehat{T_{\mathsf{loc}}}) \\
&= \#ker(d) \cdot \frac{\#T_{\mathsf{loc}}}{\#H^0(Z^\bullet_{\mathsf{bo}})} \cdot \frac{\#H^{-1}(Z^\bullet_{\mathsf{bo}})}{\#T_{\mathsf{gl}}} \\
&= \#ker(d) \cdot \frac{\#T_{\mathsf{loc}}}{\#T_{\mathsf{gl}}} \cdot \frac{\ker(b)}{\mathrm{coker}(b)} \\
&= z(d) \cdot \frac{\#T_{\mathsf{loc}}}{\#T_{\mathsf{gl}}} \cdot z(b).
\end{aligned}$$

By lemma I.28, we know that the first coefficient is $z(\hat{c})^{-1} = z(c)$ and that the order of vanishing of f is equal to r, because of proposition I.30. Thanks to the decomposition in proposition I.23 this equals

$$\begin{aligned}
z(c) &= z(\lambda(\gamma)^{-1}\,\hat{h}) \cdot z(\hat{f})^{-1} \cdot z(e)^{-1} \cdot z(d)^{-1} \cdot z(b)^{-1} \cdot z(\hat{a})^{-1} \\
&= \lambda(\gamma)^{-r} \cdot \mathrm{Reg}_\lambda(\check{\mathfrak{R}}_\Sigma, \mathfrak{R}_\Sigma) \cdot 1 \cdot \frac{\#T_{\mathsf{loc}}}{\#T_{\mathsf{gl}} \cdot \#J_\Sigma} \cdot \frac{\#\mathcal{R}^\star}{\#I_\Sigma} \\
&= \frac{\mathrm{Reg}_\lambda(\check{\mathfrak{R}}, \mathfrak{R}) \cdot [\mathfrak{R} : \mathfrak{R}_\Sigma] \cdot [\check{\mathfrak{R}} : \check{\mathfrak{R}}_\Sigma]}{\lambda(\gamma)^r} \cdot \frac{\#T_{\mathsf{loc}}}{\#T_{\mathsf{gl}} \cdot [\mathfrak{R} : \mathfrak{R}_\Sigma] \cdot \#J_0} \cdot \frac{\#\mathcal{R}^\star}{[\check{\mathfrak{R}} : \check{\mathfrak{R}}_\Sigma] \cdot \#I_0}.
\end{aligned}$$

□

I.9.1 Comments

The formula in theorem I.33 will be substantially simplified in II.3 under the assumption that the Tate-Shafarevich group of A is finite.

Let me make some remarks on the Euler-characteristic. The first factor is normalised so that it does not depend on the character λ anymore, but only on the $\mathbb{Z}_p$-extension it cuts out. The bounds on T_{gl} and T_{loc} are such that they vanish for a lot of cases. We believe that the index I_0 and the order of $\mathcal{R}^\star$ are very often trivial. For the cyclotomic extension, the first factor, the normalised regulator, turns out to be a unit in many case. As a consequence, the Euler-characteristic itself is quite frequently a unit.

I.10 Further consequences

Some additional consequences can be derived from the assumption that the height is non-degenerate on the fine Selmer group. These are all more or less classical results, all follow actually from the weak Leopoldt conjecture rather than the non-degeneracy of the p-adic height. For the case when the fine Selmer group of an elliptic curve over $\mathbb{Q}$ vanishes the results and the proofs turn out to be (almost) the same as in [CoMc94]. This is also part of the article [PR93b].

Once again, the starting point are two versions of global duality, namely

$$\begin{array}{ccccccc}
0 & \longrightarrow & \check{\mathfrak{R}}_\Sigma & \longrightarrow & \check{\mathfrak{R}} & \searrow & \\
 & & & & & & \bigoplus_{v\in\Sigma(\nmid p)} H^1(\widehat{K_v, A}(p)) \\
0 & \longleftarrow & \widehat{\mathcal{S}'} & \longleftarrow & \widehat{H^1_\Sigma(A(p))} & \nwarrow & \\
0 & \longrightarrow & \check{\mathfrak{R}} & \longrightarrow & H^1_\Sigma(T_p\check{A}) & \searrow & \\
 & & & & & & \bigoplus_{v|p} H^1(\widehat{K_v, A}(p)) \\
0 & \longleftarrow & \widehat{\mathcal{R}} & \longleftarrow & \widehat{\mathcal{S}'} & \nwarrow &
\end{array}$$

Here we defined actually a new group $\mathcal{S}'(A/K)$ as the kernel of the map from $H^1_\Sigma(A(p))$ to the local conditions $H^1(K_v, A)(p)$, but only for places v above p. Now, the corresponding sequences over ${}_\infty K$ will contain the projective limit $\varprojlim \mathfrak{R}(\check{A}/{}_n K)$ that we will denote temporarily by ${}_\infty Y$.

$$\begin{array}{ccccccccccc}
 & & 0 & \longrightarrow & {}_\infty Y & \longrightarrow & \bigoplus_{v\in\Sigma(\nmid p)} H^1(\widehat{{}_\infty K_v, A}(p)) & \longrightarrow & {}_\infty\widehat{H^1_\Sigma(A(p))} & \longrightarrow & {}_\infty\widehat{\mathcal{S}'} \longrightarrow 0 \\
0 & \longrightarrow & {}_\infty Y & \longrightarrow & {}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A}) & \longrightarrow & \bigoplus_{v|p} H^1(\widehat{{}_\infty K_v, A}(p)) & \longrightarrow & {}_\infty\widehat{\mathcal{S}'} & \longrightarrow & {}_\infty\widehat{\mathcal{R}} \longrightarrow 0
\end{array} \tag{I.43}$$

The vanishing of the very first term is due to proposition I.26 and (I.13).

I.10.1 Local calculations

First, we note that the group $H^1({}_\infty K_v, A(p))_\Gamma$ is trivial. Indeed, by the sequence coming from the Hochschild-Serre spectral sequence (I.9), we know that it is a subgroup of $H^2(K_v, A(p))$ which is dual to $T_p\check{A}(K_v) = 0$.

The exact sequence (see (I.23))

$$0 \longrightarrow T_v \longrightarrow H^1(K_v, A(p)) \longrightarrow H^1({}_\infty K_v, A(p))^\Gamma \longrightarrow 0$$

shows that, if v does not divide p, then $H^1({}_\infty K_v, A(p))^\Gamma$ is finite and hence the local term in the top row of (I.43) is Λ-torsion. Therefore ${}_\infty Y$ is Λ-torsion.

Now, if v divides p, then the above sequence proves that $H^1({}_\infty K_v, A(p))^\Gamma$ has $\mathbb{Z}_p$-corank equal to $2 \cdot n_v \cdot d$, where $n_v = [K_v : \mathbb{Q}_p]$ and $d = \dim A$. Together with the

remark on the vanishing of $H^1({}_\infty K_\upsilon, A(p))_\Gamma$, this proves that the middle term in the lower sequence of (I.43) has Λ-rank equal to $2 \cdot n \cdot d$ with $n = [K : \mathbb{Q}]$. See [PR92, Proposition 2.1.3].

I.10.2 Global calculations

Proposition I.34. *Assume that the p-adic height on the fine Selmer group associated to ${}_\infty K$ is non-degenerate. Then the Λ-modules $\mathcal{S}'(\widehat{A/{}_\infty K})$, ${}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})$ and ${}_\infty\widehat{H^1_\Sigma(A(p))}$ all have Λ-rank equal to $[K : \mathbb{Q}] \cdot \dim A$. Moreover the dual of ${}_\infty H^1_\Sigma(A(p))$ cannot have any non-trivial finite Λ-submodule.*

Proof. To calculate the Λ-rank of ${}_\infty\widehat{H^1_\Sigma(A(p))}$, we use first the formula in part i) of lemma I.28, then the sequences (I.8) together with lemma I.24 and then finally the global Euler-characteristic calculation by Tate [NeScWi00, Theorem VIII.6.14].

$$\begin{aligned}
\operatorname{rank}_\Lambda {}_\infty\widehat{H^1_\Sigma(A(p))} &= \operatorname{corank}_{\mathbb{Z}_p}\left({}_\infty H^1_\Sigma(A(p))^\Gamma\right) - \operatorname{corank}_{\mathbb{Z}_p}\left({}_\infty H^1_\Sigma(A(p))_\Gamma\right) \\
&= \operatorname{corank}_{\mathbb{Z}_p}\left({}_\infty H^1_\Sigma(A(p))\right) - \operatorname{corank}_{\mathbb{Z}_p}\left({}_\infty H^2_\Sigma(A(p))\right) \\
&= \sum_{\upsilon|\infty} \operatorname{corank}_{\mathbb{Z}_p} A(K_\upsilon)(p) \\
&= r_1 \cdot d + r_2 \cdot 2 \cdot d = n \cdot d
\end{aligned}$$

The last part is due to the fact that the corank of $A(\mathbb{R})(p)$ for an abelian variety defined over $\mathbb{R}$ is equal to its dimension d and the corank of $A(\mathbb{C})(p)$ is twice the dimension. Putting this information and the local calculation in the two sequences (I.43) proves the first part. The fact that the dual of ${}_\infty H^1_\Sigma(A(p))$ has no non-trivial finite Λ-submodules can be shown by proving that ${}_\infty H^1_\Sigma(A(p))_\Gamma$ is $\mathbb{Z}_p$-cofree, see [NeScWi00, Proposition V.9.13]. But if the weak Leopoldt conjecture is valid, this group is isomorphic to the dual of $\check{\mathfrak{R}}_\Sigma$. □

Proposition I.35. *The projective limit $\varprojlim \mathfrak{R}(A/{}_n K)$ is trivial if the height pairing on the fine Selmer group is non-degenerate.*

Proof. Since $H^1({}_\infty K_\upsilon, A(p))_\Gamma$ vanishes, we know that ${}_\infty Y^\Gamma = 0$ from the first sequence in (I.43). Denote the cokernel of the inclusion of ${}_\infty Y$ in ${}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A})$ by ${}_\infty D$. Since ${}_\infty D$ embeds into the local sum in the second sequence in (I.43), it is true that ${}_\infty D^\Gamma = 0$.

Look at the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & {}_\infty Y_\Gamma & \longrightarrow & {}_\infty\text{Ш}^1_\Sigma(T_p\check{A})_\Gamma & \longrightarrow & {}_\infty D_\Gamma & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \check{\text{Ш}} & \longrightarrow & H^1_\Sigma(T_p\check{A}) & \longrightarrow & \bigoplus_{v|p} \widehat{H^1(K_v, A(p))} & \longrightarrow & \cdots \end{array}$$

So there is an injection from the finite group ${}_\infty Y_\Gamma$ down to the $\mathbb{Z}_p$-free $\check{\text{Ш}}$. Therefore ${}_\infty Y_\Gamma$ is trivial. From the structure theorem for finitely generated Λ-modules, we conclude that ${}_\infty Y$ is finite. This is only possible if it is trivial, since it is the projective limit of $\mathbb{Z}_p$-free groups. □

This last proposition is the generalisation of theorem 4 in [CoMc94]. We are going to extend now their theorem 3.

Proposition I.36. *If the height on the fine Selmer group is non-degenerate and if the $\mathfrak{R}_\Sigma(\check{A}/K)$ is equal to $\mathfrak{R}(\check{A}/K)$ then there are no non-trivial finite Λ-submodules in the dual of $\mathcal{S}'(A/{}_\infty K)$.*

Proof. The previous proposition implies that there is an exact sequence

$$0 \longrightarrow {}_\infty\mathcal{S}' \longrightarrow {}_\infty H^1_\Sigma(A(p)) \longrightarrow \bigoplus_{v\in\Sigma(\nmid p)} H^1({}_\infty K_v, A(p)) \longrightarrow 0$$

Denote the last group by ${}_\infty W$. We saw that ${}_\infty W_\Gamma$ is trivial and ${}_\infty W^\Gamma$ is finite. Let us look at the following diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & {}_\infty\mathcal{S}'^\Gamma & \longrightarrow & {}_\infty H^1_\Sigma(A(p))^\Gamma & \longrightarrow & {}_\infty W^\Gamma & \longrightarrow & {}_\infty\mathcal{S}'_\Gamma & \longrightarrow & {}_\infty H^1_\Sigma(A(p))_\Gamma & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & & & \cong\uparrow & & \\ 0 & \longrightarrow & \mathcal{S}' & \longrightarrow & H^1_\Sigma(A(p)) & \longrightarrow & W & \longrightarrow & \widehat{\text{Ш}} & \longrightarrow & \widehat{\text{Ш}_\Sigma} & \longrightarrow & 0 \end{array}$$

where W is the direct sum of the groups $H^1(K_v, A(p))$ for all places in $\Sigma(\nmid p)$. We would like to show that ${}_\infty\mathcal{S}'_\Gamma$ is cofree. Under our assumption the map from $H^1_\Sigma(A(p))$ to W is surjective and so the map from ${}_\infty W^\Gamma$ to ${}_\infty\mathcal{S}'_\Gamma$ is trivial. We conclude that the group in question is isomorphic to the dual of the $\mathbb{Z}_p$-free $\check{\text{Ш}}_\Sigma$. □

The conclusion of the proposition is still valid if we only assume that the reduction map from the elements in $\check{\text{Ш}}$ with good reduction at all places in $\Sigma(\nmid p)$ to $\tilde{A}_{\text{ns}}(\mathbb{F}_v)(p)$ is trivial for all these places. If Σ is chosen to be very large, then this will not be possible and we are unable to draw the conclusion in the proposition.

I.11 Degenerate pairings

Although it in conjectured that the height pairing on the fine Selmer group affiliated with the cyclotomic $\mathbb{Z}_p$-extension is non-degenerate, it is not true for arbitrary $\mathbb{Z}_p$-extensions.

I.11.1 An anti-cyclotomic example

Let $E/\mathbb{Q}$ be an elliptic curve and p an odd prime at which E has good ordinary reduction. Let K be an imaginary quadratic field in which all primes dividing the conductor and p split. Hence the root number of E/K is -1. The (non-generic) case that E has complex multiplication by an order in K has to be excluded. Following the example in 4.2. of [MaRu03], we suppose the Mordell-Weil $E(\mathbb{Q})$ group to have rank 2 and that the p-primary part of the Tate-Shafarevich group $Ш(E/K)(p)$ over K is finite. A theorem of Nekovář [Nek01] guarantees that the rank of $E(K)$ is odd. Hence we may further assume that the rank of $E(K)$ is 3. As a concrete example we could take

$$y^2 = x^3 + x^2 - 13\,x + 18$$

of conductor 655, $p = 3$ and $K = \mathbb{Q}(\sqrt{-56})$.

Let ${}_\infty K$ be the unique $\mathbb{Z}_p$-extension of K which is Galois over $\mathbb{Q}$ and the complex conjugation acts as -1 on Γ. It is called the anti-cyclotomic $\mathbb{Z}_p$-extension.

A theorem of Vatsal and Cornut shows that the Λ-rank of the dual of the classical Selmer group ${}_\infty \mathcal{S}$ over ${}_\infty K$ is 1. This has another consequence, due to Bertolini [Ber01, Theorem 5.4], namely that the dual of ${}_\infty \mathcal{R}$ is Λ-torsion, so the weak Leopoldt conjecture holds.

The fine Selmer group $\mathfrak{R}(E/K)$ has rank 1 because $E(K)$ has rank 3 and the local group $\bigoplus_{v|p} E(K_v)^\star$ has rank 2. The localisation map has image of rank 2 because not all points of $E(K)$ are defined over $\mathbb{Q}$. $\mathfrak{R}(E/K)$ is therefore contained in $E(\mathbb{Q})^\star$ and contains $\mathfrak{R}(E/\mathbb{Q})$ with finite index.

The p-adic height associated to the anti-cyclotomic extension must satisfy that

$$\langle \bar{P}, \bar{Q} \rangle_{\text{anti-cyc}} = -\langle P, Q \rangle_{\text{anti-cyc}}$$

if $\bar{P}$ denotes the complex conjugate of a point P in $E(K)$. Therefore it vanishes on $\mathfrak{R}(E/\mathbb{Q})$ and hence on $\mathfrak{R}(E/K)$. This is the basic example of a degenerate p-adic height for the fine Selmer group.

I.11.2 Derived heights

The degeneracy of the canonical p-adic height on the classical Selmer group (in the ordinary case) is due to the fact that the dual of the Selmer group over ${}_\infty K$ is not Λ-torsion. It contains namely the Heegner module, a certain cyclic Λ-submodule generated by Heegner points, giving rise to universal norms in $E(K)$. A conjecture of Mazur states for this case that these universal norms lie in $E(\mathbb{Q})$. For some numerical examples this is verified in 4.4 in [MaRu03].

For the fine Selmer group the situation is different; the universal norms must lie outside the fine Selmer group, because the weak Leopoldt conjecture holds.

There have been recently several new ways of looking at p-adic height pairings on the classical Selmer group in the case the reduction is good ordinary at all places above p. It seems that the only obstacle to extend these definitions to the supersingular case is that the control theorem does not hold.

For the fine Selmer group there is a control theorem I.15 for all odd primes p. These fancier versions of the height pairing should therefore give similar constructions for the fine Selmer groups.

Derived p-adic heights were first introduced by Bertolini and Darmon in [BeDa94] and [BeDa95]. Their construction can probably be reused for the fine Selmer group. They only construct the derived heights for the case when the map in the control theorem is an isomorphism.

In the recent preprint of Howard [How03], another construction of the derived heights is given. The first part of his paper is in complete generality and we can apply it to our setting by specifying the "Selmer structure" to be the one that defines the fine Selmer group.

The following explanation is a sketch of his arguments applied to the fine Selmer group. Suppose that the weak Leopoldt conjecture holds for simplicity and suppose that the p-primary torsion groups $A({}_\infty K_\upsilon)(p)$ are finite for all places υ above p.

Let I be the augmentation ideal in $\mathbb{Z}/p^k[\![\Gamma]\!]$ and let γ be a generator of Γ. Howard's theorem 1.11 tells us that there is a canonical pairing h between $H^1_\Sigma({}_\infty K, \check{A}[p^k])$ and $R^k_\Sigma(A/{}_\infty K)$ with values in I/I^2. It is basically Flach's generalised Cassels-Tate pairing. He then proceeds to construct the derived height. If M is a $\mathbb{Z}/p^k[\![\Gamma]\!]$-module, let $M^{(n)}$ denote the image of the map

$$M^{{}_n\Gamma}/M^{(n+1)^\Gamma} \longrightarrow M^\Gamma$$

induced by multiplication by $(\gamma-1)^{n-1}$. Here ${}_n\Gamma$ denotes the Galois group of ${}_\infty K : {}_n K$. If ξ belongs to $H^1_\Sigma({}_\infty K, \check{A}[p^k])^{(n)}$, there is an element ξ' in $H^1_\Sigma({}_\infty K, \check{A}[p^k])^{n^\Gamma}$ such that

$(\gamma-1)^{n-1}\cdot\xi'=\xi$. For any element η in $R^k_\Sigma(A/_\infty K)^{(n)}$, define an element $h^{(n)}(\xi,\eta)=(\gamma-1)^{n-1}\cdot h(\xi',\eta)$ in I^n/I^{n+1}. This is called the n-th derived pairing

$$h^{(n)}\colon H^1_\Sigma({}_\infty K,\check{A}[p^k])^{(n)}\times R^k_\Sigma(A/_\infty K)^{(n)}\longrightarrow I^n/I^{n+1},$$

it is independent of the generator γ and the chosen element ξ'. Howard's lemma 2.3 shows that the right kernel of the pairing is exactly $R^k_\Sigma(A/_\infty K)^{(n+1)}$.

Next we will take projective limits over k with respect to the multiplication by p. So we are working over the ring Λ. Note that there is a natural map

$$\varprojlim_k H^1_\Sigma({}_\infty K,\check{A}[p^k])\twoheadrightarrow \varprojlim_k H^1_\Sigma({}_\infty K,\check{A}(p))[p^k]$$

with finite kernel. Similar the projective limit $Y=\varprojlim R^k_\Sigma(A/_\infty K)$ is pseudo-isomorphic to $T_p({}_\infty\mathcal{R})$.

By our assumption that the weak Leopoldt conjecture holds, we may write the Λ-torsion module $\widehat{{}_\infty\mathcal{R}}$, up to pseudo-isomorphism, as

$$\frac{\Lambda}{(f)}\oplus\left(\frac{\Lambda}{(T)}\right)^{e_1}\oplus\left(\frac{\Lambda}{(T^2)}\right)^{e_2}\oplus\cdots\oplus\left(\frac{\Lambda}{(T^N)}\right)^{e_N}$$

for some integers $e_n\geqslant 0$ and some element f in Λ which is not divisible by T. The Λ-module Y must have the same Λ-structure except that the f might be different. In particular, we see that

$$\operatorname{rank}_{\mathbb{Z}_p}Y^{(n)}=\operatorname{rank}_{\mathbb{Z}_p}\left(Y^{(n-1)^\Gamma}\right)-\operatorname{rank}_{\mathbb{Z}_p}\left(Y^{n^\Gamma}\right)=e_{n+1}+e_{n+2}+\cdots+e_N$$

and so $e_n=\operatorname{rank}Y^{(n-1)}-\operatorname{rank}Y^{(n)}$.

Moreover, we have that the part fixed by ${}_n\Gamma$ of Y is equal to

$$Y^{n^\Gamma}=(\varprojlim_k R^k_\Sigma(A/_\infty K))^{n^\Gamma}=\varprojlim_k R^k_\Sigma(A/_\infty K)^{n^\Gamma}\xleftarrow{}\varprojlim_k R^k_\Sigma(A/_n K)=\mathfrak{R}_\Sigma(A/_n K)$$

where the map is a pseudo-isomorphism as can be seen from the control theorem I.16. From $(Y\otimes\mathbb{Q}_p)^\Gamma\xleftarrow{\cong}\mathfrak{R}_\Sigma(A/K)\otimes\mathbb{Q}_p$ we may therefore induce filtrations

$$\begin{aligned}\cdots\subset\mathfrak{R}^{(n)}_\Sigma\subset\cdots\subset\mathfrak{R}^{(2)}_\Sigma\subset\mathfrak{R}^{(1)}_\Sigma&=\mathfrak{R}_\Sigma(A/K)\otimes\mathbb{Q}_p\\ \cdots\subset V^{(n)}\subset\cdots\subset V^{(2)}\subset V^{(1)}&=H^1_\Sigma(K,T_p\check{A})\otimes\mathbb{Q}_p\end{aligned}$$

of vector spaces and a sequence of pairings

$$V^{(n)}\times\mathfrak{R}^{(n)}_\Sigma\longrightarrow I^n/I^{n+1}\otimes\mathbb{Q}_p$$

such that the right kernel is exactly $\mathfrak{R}^{(n+1)}_\Sigma$. Note that we have

$$e_n=\dim\mathfrak{R}^{(n-1)}_\Sigma-\dim\mathfrak{R}^{(n)}_\Sigma.$$

Of course, the pairing on $\mathfrak{R}_\Sigma^{(1)}$ should be nothing else but the p-adic height pairing, divided by $\lambda(\gamma)$.

If the pairing on $\check{\mathfrak{R}}_\Sigma \times \mathfrak{R}_\Sigma$ is non-degenerate, then the right kernel $\mathfrak{R}_\Sigma^{(2)}$ is trivial and so e_1 is equal to the rank of $\mathfrak{R}_\Sigma(A/K)$ and all other e_i are zero. This implies that the order of vanishing of $f_\mathfrak{R}$ is equal to the rank of $\mathfrak{R}_\Sigma(A/K)$. It should be possible to compute the Euler characteristic via a generalised version of the regulator containing information from all derived pairings.

Let us turn back to the example of the degenerated p-adic height on the fine Selmer group for the anti-cyclotomic extension. We expect that the extended pairing $H^1_\Sigma(T_pE) \times \mathfrak{R}_\Sigma \longrightarrow \mathbb{Z}_p$ has a trivial right kernel $\mathfrak{R}_\Sigma^{(2)}$ since a point P on the negative eigenspace $E(K)^-$ should have a non-zero height with a point in $\mathfrak{R}_\Sigma(E/\mathbb{Q})$. At least in the ordinary case this is contained in the conjectures of Mazur and is verified for some cases in [MaRu03]. We could conclude from the above approach that the order of vanishing of $f_\mathfrak{R}$ is still equal to the rank of $\mathfrak{R}_\Sigma(E/K)$, that is 1, even though the pairing on $\mathfrak{R}_\Sigma(E/K) \times \mathfrak{R}_\Sigma(E/K)$ is trivial. In which case, we see that the degeneracy of the height in diagram (I.36) is not because the map c is not a pseudo-isomorphism, but rather that the map d fails to be a pseudo-isomorphism.

Nevertheless, we are expecting that the order of vanishing of $f_\mathfrak{R}$ might be strictly larger than the rank of the fine Selmer group for some $\mathbb{Z}_p$-extensions, namely for "pathological" cases like the ones discovered by Brattström in [Bra85].

It might be that there is a fine analogue of the pairing constructed in Perrin-Riou's article [PR03b] in the ordinary case. It is a pairing between $\widehat{{}_\infty\mathfrak{S}}$ and the corresponding group for the dual $\check{A}$ with values in the quotient of the fraction field of Λ by Λ. It contains the p-adic height pairing on the classical Selmer group as well as a generalised version of the Cassels-Tate pairing. If the Leopoldt conjecture holds, it would have to be constructed starting from the map

$$\widehat{{}_\infty\mathfrak{R}} \longrightarrow \mathrm{Ext}^1_\Lambda({}_\infty H^1_\Sigma(\check{A}(p))^\wedge, \Lambda)$$

induced from Jannsen's spectral sequence (I.39).

The generalisations that are discussed here should also fit into the description of Mazur in [MaRu02]. Therefore it might be that there is a "natural" description of the p-adic height on the fine Selmer group via the Selmer complexes of Nekovář [Nek03].

I.12 Orthogonality

As mentioned at the end of the construction of the height pairing on $\check{\mathfrak{R}}_\Sigma \times \mathfrak{R}_\Sigma$, there is an extension that gives a pairing on $H^1_\Sigma(T_p\check{A}) \times \mathfrak{R}_\Sigma$ with values in $\mathbb{Z}_p$. The proposition I.32 can be strengthened to the following statement (see [PR95, 3.1.4])

Proposition I.37. *The image of the corestriction from ${}_\infty\text{Ш}^1_\Sigma(T_p\check{A})$ in $H^1_\Sigma(T_p\check{A})$ is orthogonal to $\mathfrak{R}_\Sigma(A/K)$ under the extended pairing $H^1_\Sigma(T_p\check{A}) \times \mathfrak{R}_\Sigma(A/K) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p$.*

Proof. Let ξ be an element in the image of the corestriction. For every n there is a cocycle ${}_n\xi$ in $H^1_\Sigma({}_nK, T_p\check{A})$ whose corestriction is ξ. By the usual formula for corestrictions of cup-product, we see that the pairing of ξ and an arbitrary element η of $\mathfrak{R}_\Sigma$ is equal to the corestriction of the pairing of ${}_n\xi$ and the restriction of η to $H^1_\Sigma({}_nK, T_pA)$. But the corestrictions are in the kernel of the maps λ_υ for all places $\upsilon \in \Sigma$ by definition. □

This is related, though not exactly the same, as the main result of [Pla91].

I.12.1 Kato's Euler system

Suppose that $A = E$ is an elliptic curve defined over $\mathbb{Q}$ having good[3] reduction at p. It is known to be modular. In [Kat00], Kato has constructed an Euler system for T_pE via Siegel-units on modular curves. Ever since the work of Kolyvagin, we know that Euler systems provide a link between the analytic and the arithmetic side and give then many amazing consequences. Kato proves in theorem 12.4 that the weak Leopoldt conjecture holds, that the Λ-submodule generated by Kato's zeta elements, let us call it ${}_\infty Z$, in ${}_\infty\text{Ш}^1_\Sigma(T_pE)$ has rank 1 and that the Λ-module ${}_\infty\text{Ш}^1_\Sigma(T_pE)$ itself is torsion-free and, if the $G_\Sigma(\mathbb{Q})$-module $E[p]$ is irreducible, it is even Λ-free.

He also shows half of the main conjecture, namely that the characteristic power series of ${}_\infty Z$ is divisible by the characteristic power series of the dual of ${}_\infty\mathcal{R}$, at least up to a power of p. If the reduction at p is ordinary, there are further results for the classical Selmer group in his theorem 17.4. The dual of the Selmer group ${}_\infty\mathcal{S}$ is Λ-torsion (Mazur's conjecture) and the quotient of $H^1({}_\infty\mathbb{Q}_p, T_pE)$ by the image of ${}_\infty Z$ must have a characteristic power series dividing the series of $\widehat{{}_\infty\text{Ш}}$, at least up to some power of p. Via the Coleman map of Perrin-Riou the localisation of the Euler system is linked to the p-adic L-series of Mazur and Swinnerton-Dyer. See [Rub00, 3.5.15].

[3] I don't think this is necessary, but my limited understanding of Kato's work tells me that I should be careful.

The above proposition explains that the corestriction of the Euler system is orthogonal to $\mathfrak{R}_\Sigma$ in $H^1(\mathbb{Q}, T_pE)$.

I.13 A higher pairing

So far, the pairing constructed starting from the extension associated to an element ξ in $H^1_\Sigma(T_p\check{A})$ were at the level of H^1. The question arises of whether there is hope of getting a new interesting pairing when looking at the same snake map but for H^2. This section is mainly to prove that the pairing obtained in this way is nothing interesting or, to say, nothing new.

Let ξ be an element in $\check{\mathfrak{R}}$ and consider the extension

$$0 \longrightarrow T_p\mu \longrightarrow T_\xi \longrightarrow T_pA \longrightarrow 0. \tag{I.44}$$

Arguments as in the construction of the height pairing show us that there is a diagram of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^2_\Sigma(T_p\mu) & \longrightarrow & H^2_\Sigma(T_\xi) & \longrightarrow & H^2_\Sigma(T_pA) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \oplus H^2(K_v, T_p\mu) & \longrightarrow & \oplus H^2(K_v, T_\xi) & \longrightarrow & \oplus H^2(K_v, T_pA) & \longrightarrow & 0 \end{array}$$

The first vertical arrow is an injection by global class field theory and it cokernel is isomorphic to $\mathbb{Z}_p$ via the invariant map. The snake map is

$$K_\xi : \widehat{\mathcal{R}(\check{A}/K)} \longrightarrow \mathbb{Z}_p$$

or formulated differently it is an element of $\mathrm{Hom}_{\mathbb{Z}_p}\left(\widehat{\mathcal{R}(\check{A}/K)}, \mathbb{Z}_p\right)$ and this group equals $T_p\check{\mathcal{R}}$.

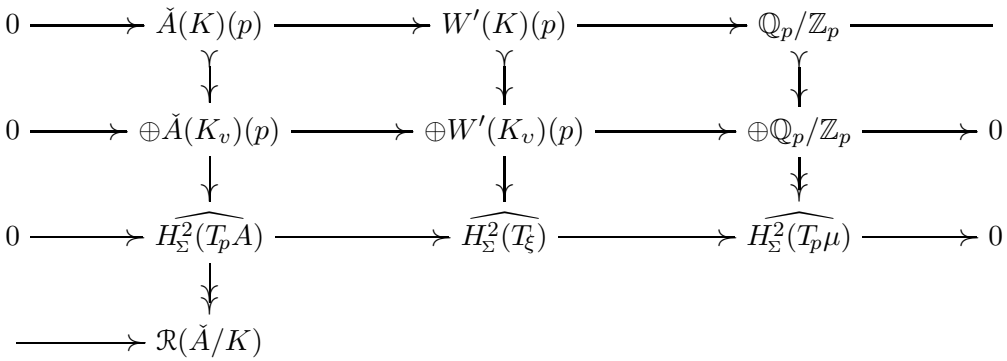
Lemma I.38. *The map K_ξ corresponds to the image of ξ via the embedding of $\mathfrak{R}(\check{A}/K)$ into $T_p\mathcal{R}(\check{A}/K)$.*

Here only a sketch of the proof is given. The Cartier dual of the (I.44) is an extension

$$0 \longrightarrow \check{A}(p) \longrightarrow W'_\xi(p) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$

and by the compatibility of Ext- and cup-pairings, the map from $\mathbb{Q}_p/\mathbb{Z}_p$ to $H^1(F, \check{A}(p))$ is the map sending a to $\xi \otimes a$ in $T_p\mathcal{R}(\check{A}/K) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathcal{R}(\check{A}/K)_{\mathrm{div}}$. The dual of the

above diagram looks as follows (if we use Poitou-Tate in every vertical line)



This shows that the dual of K_ξ has the same description as the map before.

Chapter II

The fine Tate-Shafarevich group

> It is noted that the literature of Uqbar was one of fantasy and that its epics and legends never referred to reality, but to the two imaginary regions of Mlejnas and Tlön...
> Tlön, Uqbar, Orbis Tertius; Jorge Luis Borges.

II.1 Definition and comparison

During this and the next section, we will allow for once the prime p to be equal to 2. For the classical Selmer group, there is a short exact sequence

$$0 \longrightarrow A(K)/p^k A(K) \longrightarrow S^k \longrightarrow Ш[p^k] \longrightarrow 0$$

where $Ш(A/K)$ is defined to be the kernel of localisation from $H^1_\Sigma(K, A)$ to the sum of $H^1(K_\upsilon, A)$, the sum running over all places in Σ. (see [Mil86, Proposition I.6.6]). It is conjectured that $Ш$ is finite.

The fine Selmer group can also be split up in the same fashion. First at finite level, the intersection of R^k with $A(K)/p^k A(K)$ inside S^k will be called the *fine Mordell-Weil group* M^k. It is therefore the kernel of localisation from $A(K)/p^k$ to the sum of the $A(K_\upsilon)/p^k$ for all places υ above p. Similar for the group M^k_Σ.

On the side of $Ш$, we define the cokernel of the embedding M^k into R^k as the *fine Tate-Shafarevich*, denoted by another beautiful Cyrillic letter Ж^k.

Now to the limits. The fine Mordell-Weil group $\mathcal{M}(A/K)$ is defined to be the intersection of $A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ and $\mathcal{R}(A/K)$ inside $H^1_\Sigma(A(p))$. It is therefore the kernel

$$0 \longrightarrow \mathcal{M} \longrightarrow A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \bigoplus_{\upsilon|p} A(K_\upsilon) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

The compact versions are defined in the same way as the following kernels

$$0 \longrightarrow \mathfrak{M} \longrightarrow A(K)^\star \longrightarrow \bigoplus_{v|p} A(K_v)^\star$$
$$0 \longrightarrow \mathfrak{M}_\Sigma \longrightarrow A(K)^\star \longrightarrow \bigoplus_{v\in\Sigma} A(K_v)^\star$$

On the darker side of things, we have the direct limit $\varinjlim Ш^k$ which will be written as $Ш(p)$.

$$0 \longrightarrow \mathcal{M} \longrightarrow \mathcal{R} \longrightarrow Ш(p) \longrightarrow 0$$
$$0 \longrightarrow \mathfrak{M} \longrightarrow \mathfrak{R} \longrightarrow \varprojlim Ш^k \longrightarrow 0$$

Note that the second line is exact because we took projective limits of finite groups. Furthermore we define $Ш$ to be the product $\prod_p Ш(p)$ where p runs through all primes p, including 2. The first little, almost obvious result is

Lemma II.1. *The fine Tate-Shafarevich group $Ш^k$ is contained in $Ш[p^k]$. For the limits, there are inclusions $Ш(p) \subset Ш(p)$ and $\varprojlim Ш^k \subset T_pШ \subset T_pШ$. Moreover the inclusion $\varprojlim Ш^k \subset T_pШ$ has finite index.*

Proof. It can be read off the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/p^k & \longrightarrow & S^k & \longrightarrow & Ш[p^k] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & \bigoplus_{v|p} A(K_v)/p^k & = & \bigoplus_{v|p} A(K_v)/p^k & & & & \end{array}$$

that there is a injection from $Ш^k$ into $Ш[p^k]$ with quotient in the cokernel C^k of the first vertical arrow. Some more work is needed for the last statement of the lemma. If k is large enough so that $A(K_v)[p^k] = A(K_v)(p)$ for all places v above p, then there is a diagram (the sums are over all places above p)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)[p^k] & \longrightarrow & A(K)/p^k & \longrightarrow & (A(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p)[p^k] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus A(K_v)[p^k] & \longrightarrow & \bigoplus A(K_v)/p^k & \longrightarrow & \bigoplus (A(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p)[p^k] & \longrightarrow & 0 \end{array} \tag{II.1}$$

The injectivity of the maps from the p^k-torsion follows from the assumption on k, because none of these torsion points can be divisible by p^k. The diagram provides us with an exact sequence

$$0 \longrightarrow M^k \longrightarrow \mathcal{M}[p^k] \longrightarrow T^k \longrightarrow C^k \longrightarrow C[p^k]$$

where C is the cokernel of the localisation from $A(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ to the corresponding local terms and T^k is the quotient of the local p^k-torsion by the global p^k torsion. Of course, T^k is bounded by T, the quotient of $\bigoplus A(K_v)(p)$ by $A(K)(p)$. The first part of this proof shows that

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ш^k & \longrightarrow & Ш[p^k] & \longrightarrow & C^k \\ & & \downarrow & & \| & & \downarrow \\ 0 & \longrightarrow & Ш[p^k] & \longrightarrow & Ш[p^k] & \longrightarrow & C[p^k] \end{array}$$

and so the quotient of $Ш[p^k]$ by $Ш^k$ is contained in the bounded group T^k. □

It looks now as if the finiteness of the fine Tate-Shafarevich is not any easier to prove than the finiteness of the classical Tate-Shafarevich. In the case of an elliptic curve of positive rank over $\mathbb{Q}$, the cokernel C is finite and so the rank of $T_p Ш$ is equal to the rank of $T_p Ш$. For curves of rank 0 over $\mathbb{Q}$, the rank can differ by at most 1. Needless to say that we expect $Ш$ to be finite in all cases.

Lemma II.2. *If $A = E$ is an elliptic curve defined over $\mathbb{Q}$ of positive rank, then $Ш(E/\mathbb{Q}) = Ш(E/\mathbb{Q})$*

Proof. In the limit we have the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1_\Sigma(E(p)) & \longrightarrow & H^1_\Sigma(E)(p) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & \oplus H^1(\mathbb{Q}_v, E(p)) & \longrightarrow & \oplus H^1(\mathbb{Q}_v, E)(p) & \longrightarrow & 0 \end{array}$$

with the sum over all places in Σ. The first vertical arrow is surjective under our assumption on the rank of $E(\mathbb{Q})$, hence the sequence of kernels reads as

$$0 \longrightarrow Ш(E/\mathbb{Q}) \longrightarrow \mathcal{R}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})(p) \longrightarrow 0.$$

□

The conclusion of the lemma is very specific to this particular case; in general we expect exactly the opposite, namely that $Ш(A/K)$ is very small compared to $Ш(A/K)$. Specially when looking at the behaviour in $\mathbb{Z}_p$-extensions, it is often known that $Ш(A/_nK)(p)$ is bounded even if $Ш(A/_nK)(p)$ is known to grow quite fast as we will see in the numerical examples in chapter VI.

For the sake of completeness, we will add here the following lemma. A proof can be found in corollary 9.6 of [Mil86] or originally in [Cas62].

Lemma II.3. *If $A = E$ is an elliptic curve, then $R^1_\Sigma(E/K)$ is trivial.*

This relies on the fact that the group $E[p]$ does not have more than p^2 elements. It implies that $Ш^1_\Sigma(E/K)$ is trivial.

II.2 Numerical examples

We wish to illustrate the definition of the fine Tate-Shafarevich group with some examples. Let $E/\mathbb{Q}$ be an elliptic curve. Of course, non-trivial Tate-Shafarevich groups are rare. We will look at examples for $p = 2$. This is exactly the case we excluded in everything we have done so far. But the reason, we could not work with $p = 2$ is mainly because the Iwasawa-theory is more complicated in this case. But the properties of the fine Tate-Shafarevich $Ш$ should not be something special for this prime.

II.2.1 An example

Let E be the curve given by the equation

$$E: \qquad y^2 + xy = x^3 - 120050\,x - 16020000$$

of conductor 210. In the tables of Cremona it is called 210E5 and it is the curve of smallest conductor with rational 2-torsion and non-trivial $Ш[2]$.

The torsion of $E(\mathbb{Q})$ is generated by $T_1 = (400, -200)$ and $T_2 = (-\frac{801}{4}, -\frac{801}{8})$, both having order 2. A 3-descent, using the program of Stoll [ScSt04], shows that the 3-primary Selmer group is trivial and hence the curve has rank zero. Now, the complete two-descent as explained in [Sil86, Proposition X.1.4] shows that the 2-Selmer group S^1 (from now on $p = 2$) has dimension 4 over $\mathbb{F}_2$. So $Ш[2]$ contains 4 elements.

The set Σ contains $\{2, 3, 5, 7\}$ and two chosen representatives of generators in $Ш[2]$ are given by $(1, -15)$ and $(1, 5)$ in $\mathbb{Q}(\Sigma, 2) \times \mathbb{Q}(\Sigma, 2)$. Clearly the first element is trivial in the localisation[1] $\mathbb{Q}_2^\times/2 \times \mathbb{Q}_2^\times/2$, while the second element is not. Hence $Ш^1$ is isomorphic to $\mathbb{Z}/2$.

Let us have a closer look at the local group $E(\mathbb{Q}_2)$. The reduction at 2 is split multiplicative of type I_2 and so the group of components $\Phi(\mathbb{Q}_2)$ has two elements. In fact, the point T_1 has bad reduction and so it represents the non-trivial element in $\Phi(\mathbb{Q}_2)$. Since T_1 is a 2-torsion point, we see that the map δ in the following exact sequence is trivial for all $k \geqslant 1$.

$$\begin{aligned} 0 \longrightarrow \widehat{E}(2\mathbb{Z}_2)[2^k] \longrightarrow E(\mathbb{Q}_2)[2^k] \longrightarrow \Phi(\mathbb{Q}_2) \longrightarrow \\ \xrightarrow{\delta} \widehat{E}(2\mathbb{Z}_2)/2^k \longrightarrow E(\mathbb{Q}_2)/2^k \longrightarrow \Phi(\mathbb{Q}_2) \longrightarrow 0. \end{aligned}$$

[1] Remember that our convention $\mathbb{Q}_2^\times/2$ stands for the non-zero 2-adic numbers modulo its squares.

Note that here $\widehat{E}(2\mathbb{Z}_2)$, the kernel of reduction $E^\circ(\mathbb{Q}_2) \longrightarrow \tilde{E}_{\mathsf{ns}}(\mathbb{F}_2)$, is equal to $E^\circ(\mathbb{Q}_2)$ because $\tilde{E}_{\mathsf{ns}}(\mathbb{F}_2)$ is the trivial group. Next the second layer of the formal group $\widehat{E}(2^2\mathbb{Z}_2)$ is isomorphic to $\mathbb{Z}_2$ via the elliptic logarithm. So it has no torsion. The exact sequence

$$\begin{aligned} 0 \longrightarrow \widehat{E}(2\mathbb{Z}_2)[2^k] \longrightarrow \mathbb{Z}/2 \longrightarrow \\ \xrightarrow{\delta'} \widehat{E}(2^2\mathbb{Z}_2)/2^k \longrightarrow \widehat{E}(2\mathbb{Z}_2)/2^k \longrightarrow \mathbb{Z}/2 \longrightarrow 0 \end{aligned}$$

follows from the fact that the quotient of $\widehat{E}(2\mathbb{Z}_2)$ by $\widehat{E}(2^2\mathbb{Z}_2)$ is isomorphic to $\mathbb{Z}/2$. The point T_2 belongs to the first layer of the formal group, but not to the second. Hence the map δ' is trivial as well. We can conclude that

$$\begin{aligned} E(\mathbb{Q}_2)(2) &= \mathbb{Z}/2 \times \mathbb{Z}/2 = E(\mathbb{Q})[2] \\ E(\mathbb{Q}_2)/2^k &= \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^k \end{aligned}$$

for all $k \geqslant 1$.

The localisation of the element $(1, -15)$ is coming from a local point

$$\left(\frac{1 + 2^3 + \mathbf{O}(2)^4}{2^6}, \frac{1 + 2 + 2^2 + 2^3 + \mathbf{O}(2)^4}{2^9}\right)$$

which is trivial in $E(\mathbb{Q}_2)/2$. On the other hand the element $(1, 5)$ is the image of the point

$$\left(\frac{1 + 2^2 + \mathbf{O}(2)^4}{2^2}, \frac{1 + 2^2 + 2^3 + \mathbf{O}(2)^4}{2^6}\right)$$

under the local Kummer map. This is a non-trivial element of $E_2(\mathbb{Q}_2)/2$.

So far we have shown that $Ш^1$ is half of $Ш[2]$. Wishing to enlarge k, we have to make the assumption that $Ш(2) = Ш[2]$. This can be expected because the analytic order of $Ш$ is indeed 4. Since the 2-torsion part of $E(\mathbb{Q}_2)/2^k$ has only dimension 3, it is immediate that the localisation map from S^k, still equal to $(\mathbb{Z}/2)^4$, is not injective. Hence $Ш^k$ contains at least one non-trivial element. On the other hand, we see that the trivial element $(1, 5)$ above does not map into the torsion part of $E(\mathbb{Q}_2)$. Hence it will not map to the trivial element in $E(\mathbb{Q}_2)/2^k$ either. We conclude that

$$Ш^k = Ш = \mathbb{Z}/2 \quad \text{if} \quad Ш(2) = \mathbb{Z}/2 \times \mathbb{Z}/2.$$

II.2.2 Tables

We present three tables. The first table II.1 contains a list of 100 curves all of rank 0 with $E(\mathbb{Q}) = \mathbb{Z}/2 \times \mathbb{Z}/2$ and $Ш[2] = \mathbb{Z}/2 \times \mathbb{Z}/2$. We list the dimension of the fine Selmer group R^1, the fine Mordell-Weil group M^1 and the fine Tate-Shafarevich group $Ш^1$.

Moreover the conductor N, the number of non-singular points N_2 in the reduction at $p = 2$ and the local Tamagawa number c_2 are given for each curve.

The next table II.2 contains the same information, but for curves whose Tate-Shafarevich group is expected to have order 4^2. Here still all curves have rank 0, the torsion group has 3 non-trivial 2-torsion points and $Ш[2]$ has 4 elements. It would be interesting to do a second descent for the these curves.

The last of these tables II.3 contains curves with $E(\mathbb{Q}) = \mathbb{Z}/4 \times \mathbb{Z}/2$ and $Ш[2] = \mathbb{Z}/2 \times \mathbb{Z}/2$ of rank 0.

Table II.1: Fine Tate-Shafarevich groups for curves with four 2-torsion points and a Tate-Shafarevich group of order 4

N	Curve	R^1	M^1	$Ж^1$	N_2	c_2
210	[1, 0, 0, -120050, -16020000]	1	0	1	1	2
582	[1, 0, 0, -194, -1056]	1	0	1	1	2
930	[1, 0, 0, -19220, -1027200]	1	1	0	1	4
1025	[1, -1, 0, -667, 2616]	1	0	1	2	1
1088	[0, 0, 0, -364, -2640]	1	0	1	2	4
1158	[1, 0, 0, -772, -8320]	1	0	1	1	4
1287	[1, -1, 0, -3861, -91368]	2	0	2	2	1
1320	[0, 1, 0, -4840, -131200]	1	0	1	2	2
1521	[1, -1, 0, -6876, 190867]	1	0	1	2	1
1640	[0, 0, 0, -547, -4914]	1	0	1	2	2
1734	[1, 1, 1, -32952, -1912599]	2	1	1	1	4
1752	[0, 1, 0, -1752, -28800]	1	0	1	2	2
2050	[1, -1, 0, -546667, -155435259]	1	0	1	3	2
2175	[1, 1, 0, -10875, -441000]	1	0	1	2	1
2178	[1, -1, 1, -23981, -1418799]	1	0	1	1	2
2184	[0, -1, 0, -176904, -28579716]	1	0	1	2	2
2190	[1, 0, 0, -5062611, -4384495215]	1	0	1	1	4
2205	[1, -1, 0, -59544, -5574717]	1	0	1	2	1
2280	[0, 1, 0, -43320, -3484800]	1	0	1	2	2
2331	[1, -1, 0, -2331, -42728]	1	0	1	2	1
2352	[0, 1, 0, -38432, -2908620]	1	1	0	2	4
2379	[1, 0, 1, -65, -169]	1	0	1	2	1
2394	[1, -1, 1, -10274, -389347]	1	0	1	1	2
2535	[1, 0, 1, -87884, -9194443]	1	0	1	2	1

N	Curve	R^1	M^1	$Ж^1$	N_2	c_2
2670	[1, 1, 1, -13350, -599265]	1	0	1	1	2
2691	[1, -1, 0, -8073, -277160]	1	0	1	2	1
2691	[1, -1, 0, -2833623, -1835242920]	2	0	2	2	1
2725	[1, -1, 1, -7230, 223772]	1	0	1	4	1
2730	[1, 1, 1, -688720, -98092255]	1	1	0	1	4
2736	[0, 0, 0, -787971, -269220350]	1	0	1	2	4
2873	[1, -1, 0, -961, -11088]	1	0	1	2	1
2880	[0, 0, 0, -77772, -8343664]	1	0	1	2	4
3025	[1, -1, 0, -12667, -324384]	1	0	1	2	1
3038	[1, -1, 1, -1014, -12127]	2	0	2	1	2
3042	[1, -1, 0, -1976571, -1059322523]	1	0	1	3	2
3094	[1, -1, 1, -14439, -664177]	1	0	1	1	4
3136	[0, 0, 0, -3724, -82320]	1	0	1	2	4
3168	[0, 0, 0, -176421, -28519940]	1	0	1	2	2
3230	[1, -1, 1, -7923, -268753]	1	0	1	1	2
3234	[1, 1, 1, -123334, -16685089]	1	0	1	1	2
3264	[0, -1, 0, -7297, -195455]	1	0	1	2	4
3264	[0, -1, 0, -110977, -14192255]	1	0	1	2	4
3366	[1, -1, 1, -892319, -324184377]	1	0	1	1	6
3366	[1, -1, 1, -282596, -50200329]	1	0	1	1	4
3462	[1, 0, 0, -6924, -222336]	1	1	0	1	4
3615	[1, 0, 0, -1205, -16200]	2	1	1	4	1
3744	[0, 0, 0, -2109, -37100]	1	0	1	2	2
3770	[1, -1, 0, -160975, 15880761]	1	0	1	3	2
4046	[1, -1, 1, -11181, -225199]	2	0	2	1	2
4056	[0, 1, 0, -8844, -316224]	1	0	1	2	2
4182	[1, 1, 1, -10607, 413201]	2	0	2	1	2
4235	[1, -1, 0, -77644, -8307117]	2	0	2	2	1
4263	[1, 0, 0, -626662, -190991725]	2	1	1	4	1
4350	[1, 0, 0, -6688, -165508]	1	0	1	1	2
4386	[1, 1, 1, -39474, -3035109]	1	0	1	1	2
4400	[0, 0, 0, -126175, -17189250]	1	0	1	2	2
4410	[1, -1, 0, -52942059, -148255335887]	1	0	1	3	2

N	Curve	R^1	M^1	Ж^1	N_2	c_2
4416	[0, 1, 0, -737, -7905]	1	0	1	2	4
4614	[1, 0, 0, -12304, -526336]	1	0	1	1	8
4624	[0, 0, 0, -26299, 1621290]	2	1	1	2	4
4704	[0, 1, 0, -702, -6840]	1	0	1	2	2
4800	[0, 1, 0, -20033, -1091937]	1	0	1	2	4
4830	[1, 0, 0, -5340, -145908]	1	0	1	1	2
4830	[1, 0, 0, -13997340, -20157724800]	1	0	1	1	4
4901	[1, -1, 1, -2229, -6652]	1	0	1	4	1
5225	[1, -1, 1, -24560355, -46841973478]	1	0	1	4	1
5334	[1, 0, 0, -5419344, -4856334336]	1	1	0	1	8
5415	[1, 0, 1, -1813, -29437]	2	0	2	2	1
5439	[1, 0, 1, -1055, -3139]	1	0	1	2	1
5439	[1, 0, 0, -12692, -551265]	2	1	1	4	1
5472	[0, 0, 0, -1029, -12580]	1	0	1	2	2
5694	[1, 0, 0, -449, -891]	1	0	1	1	2
5795	[1, -1, 1, -1932, -32194]	1	0	1	4	1
5808	[0, 1, 0, -42632, -3391500]	1	0	1	2	4
5985	[1, -1, 0, -43740270, 110500349575]	1	0	1	2	1
5986	[1, -1, 1, -84, 83]	2	0	2	1	2
6123	[1, 0, 1, -475, -3919]	1	0	1	2	1
6192	[0, 0, 0, -49539, -4243070]	1	0	1	2	4
6200	[0, 0, 0, -129175, -17865750]	1	0	1	2	2
6286	[1, -1, 1, -4191, -103369]	2	1	1	1	4
6320	[0, 0, 0, -2107, -37206]	1	1	0	2	4
6336	[0, 0, 0, -12684, -548080]	1	0	1	2	4
6410	[1, -1, 1, -8547, -301981]	1	0	1	1	6
6498	[1, -1, 1, -17778596, -28848405049]	1	0	1	1	10
6510	[1, 1, 1, -784690, -245901445]	1	0	1	1	2
6510	[1, 0, 0, -91270, -3587200]	1	0	1	1	2
6552	[0, 0, 0, -1592139, 773244470]	1	0	1	2	2
6600	[0, -1, 0, -100508, 5997012]	1	0	1	2	2
6675	[1, 1, 0, -3750, -86625]	1	0	1	2	1
6762	[1, 1, 1, -547772, 155767961]	2	0	2	1	2

N	Curve	R^1	M^1	$Ш^1$	N_2	c_2
6918	[1, 0, 0, -27672, -1774080]	1	0	1	1	6
6936	[0, -1, 0, -20904, 125244]	2	0	2	2	2
7077	[1, 0, 0, -2359, -44296]	2	0	2	4	1
7176	[0, 1, 0, -49349352, 133418712960]	1	0	1	2	2
7215	[1, 0, 1, -98894, -11966749]	1	0	1	2	1
7230	[1, 1, 1, -940, -6295]	1	0	1	1	2
7434	[1, -1, 0, -38537856, 92092628992]	1	0	1	3	2
7455	[1, 0, 0, -529305, -148264200]	2	0	2	4	1
7470	[1, -1, 1, -8582, -155919]	1	0	1	1	2
7600	[0, 0, 0, -3175, -68250]	1	0	1	2	2

Table II.2: Fine Tate-Shafarevich groups for curves with four 2-torsion points and a Tate-Shafarevich group of order 16

N	Curve	R^1	M^1	$Ш^1$	N_2	c_2
1230	[1, 1, 1, -896670, -327184905]	1	0	1	1	2
1734	[1, 1, 1, -501132, -136748439]	2	0	2	1	2
2535	[1, 0, 1, -1373129, -619428769]	1	0	1	2	1
6486	[1, 0, 0, -101614, -12475936]	1	0	1	1	2
7766	[1, -1, 1, -2589, -50047]	1	0	1	1	2
10025	[1, -1, 0, -83542, -9273009]	1	0	1	2	1
10065	[1, 0, 0, -4465505, -3632440200]	2	0	2	4	1
11760	[0, 1, 0, -94119216, -351482801580]	1	1	0	2	4
12696	[0, 1, 0, -97512, -11681280]	1	0	1	2	2
12870	[1, -1, 0, -12282194745, -523913041814675]	1	0	1	3	2
13120	[0, 0, 0, -1399468, -637222608]	1	0	1	2	4
15558	[1, 0, 0, -140022, -20178720]	1	0	1	1	2
15870	[1, 0, 0, -3745331, -2537009955]	1	0	1	1	2
16448	[0, 0, 0, -87724, -10000080]	1	0	1	2	4
16856	[0, 0, 0, -1927219, -1029751170]	1	0	1	2	2
17157	[1, 0, 0, -288357699, -1884737960136]	2	1	1	4	1
19215	[1, -1, 1, -1144643603, -14905451732038]	1	0	1	4	1

Table II.3: Fine Tate-Shafarevich groups for curves with 8 torsion points and a Tate-Shafarevich group of order 4

N	Curve	R^1	M^1	$Ш^1$	N_2	c_2
1230	[1, 1, 1, -56170, -5105305]	1	0	1	1	4
6486	[1, 0, 0, -6394, -192556]	1	0	1	1	4
7440	[0, -1, 0, -307520, 65740800]	1	0	1	2	4
8103	[1, 0, 0, -37074, -2722941]	1	0	1	4	1
10065	[1, 0, 0, -279380, -56652225]	1	0	1	4	1
15792	[0, -1, 0, -1780224, -892394496]	1	0	1	2	4
17157	[1, 0, 0, -18024654, -29442272301]	1	0	1	4	1

II.3 Revising the Euler-characteristic

From now on, we will assume that $Ш(A/K)$ is finite.

The first immediate consequence is that $\mathfrak{M}$ equals to $\mathfrak{R}$ and that $T_p\mathcal{M}$ is equal to $T_p\mathcal{R}$. Furthermore there is an exact sequence

$$0 \longrightarrow \mathcal{M}^\star \longrightarrow \mathcal{R}^\star \longrightarrow Ш(p) \longrightarrow 0 \tag{II.2}$$

in which we would like to know more about the first term. From the definition of $\mathcal{M}$ and the cokernel C in the proof of the above lemma, we deduce a cochain complex

$$0 \longrightarrow T_p\mathcal{M} \longrightarrow T_p(A(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{c} \bigoplus_{v|p} T_p(A(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \circ\!\!\longrightarrow T_pC \longrightarrow 0.$$

The only place where the sequence is not exact is at the local term where the cohomology equals $\mathcal{M}^\star$. This is a consequence of the homological lemma I.9 and the fact that the groups $A(F)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ are $\mathbb{Z}_p$-cofree, for both $F = K$ and $F = K_v$. This provides us with an exact sequence $0 \longrightarrow \mathcal{M}^\star \longrightarrow \operatorname{coker}(c) \longrightarrow T_pC \longrightarrow 0$ and so the torsion part of $\operatorname{coker}(c)$ equals $\mathcal{M}^\star$. The limit of the diagram (II.1) provides us with an exact sequence

$$0 \longrightarrow \mathfrak{M} \longrightarrow T_p\mathcal{M} \longrightarrow T \longrightarrow D \longrightarrow \operatorname{coker}(c) \longrightarrow 0$$

where D is the cokernel of localisation from $A(K)^\star$ to the corresponding local group at all places above p. Remembering the definition of I_0 in I.11 and using the assumption of the finiteness of the fine Tate-Shafarevich, we can shorten this to

$$0 \longrightarrow I_0 \longrightarrow T \longrightarrow D(p) \longrightarrow \mathcal{M}^\star \longrightarrow 0 \tag{II.3}$$

Fortunately, the Euler-characteristic formula in theorem I.33 can now be simplified.

Theorem II.4.

Let A/K be an abelian variety over a number field with potentially good reduction

at an odd prime p, whose fine Tate-Shafarevich group $Ш(A/K)(p)$ is finite and such that the p-adic height pairing on the fine Selmer group for the cyclotomic extension ${}_\infty K$ is non-degenerate.

Then the Euler characteristic of the dual of the fine Selmer group $\mathcal{R}(A/{}_\infty K)$ over ${}_\infty K$ is equal to

$$\chi(\mathcal{R}) = \chi(\Gamma, \widehat{{}_\infty\mathcal{R}}) = \frac{\mathrm{Reg}(\mathfrak{M}(A/K), \mathfrak{M}(\check{A}/K))}{p^r} \cdot \frac{\#D(p) \cdot \prod_{v\nmid p} c_v \cdot \#Ш(p)}{\#J_0}$$

where r is the $\mathbb{Z}_p$-rank of $\mathfrak{M}(A/K)$ and J_0 is the cokernel of the injection from $\mathfrak{M}(\check{A}/K)$ into the cokernel of corestriction from ${}_\infty\mathfrak{H}^1_\Sigma(T_p\check{A}) \longrightarrow H^1_\Sigma(T_p\check{A})$. Finally D is the cokernel of localisation $A(K)^\star \longrightarrow \oplus_{v|p} A(K_v)^\star$.

Proof. The exact sequences (II.2) and (II.3) show that

$$\#\mathcal{R}^\star = \#\mathcal{M}^\star \cdot \#Ш(p) = \frac{\#D(p) \cdot \#I_0 \cdot \#A(K)(p)}{\prod_{v|p} \#A(K_v)(p)} \cdot \#Ш(p).$$

The theorem follows now from the formula in theorem I.33 and lemma I.12. □

In the case that the reduction is multiplicative at p, the expression on the right multiplied with $A(K)(p)$ is still an upper bound for the Euler characteristic. For the special case of rank 0, the above expression and assumptions can be simplified to

Corollary II.5. *Let A/K be an abelian variety with finite Mordell-Weil group $A(K)$, potentially good reduction at p and finite Tate-Shafarevich $Ш(A/K)$, then*

$$\chi(\mathcal{R}) = \frac{\prod_{v|p} \#A(K_v)(p) \cdot \prod_{v\nmid p} c_v^{(p)} \cdot \#Ш(p)}{\#A(K)(p) \cdot \#J_0}$$

It is interesting to have a look at the special case when the abelian variety A is an elliptic curve E over $\mathbb{Q}$ of rank 1 and p is a good prime greater than 3. From lemma II.2, we conclude that the Euler characteristic of $\widehat{{}_\infty\mathcal{R}}$ is equal to

$$\chi(\mathcal{R}) = \frac{\#D \cdot \prod c_v^{(p)} \cdot \#Ш(p)}{\#J_0 \cdot \#E(\mathbb{Q})(p)} \tag{II.4}$$

According to lemma 9 in [CoMc94] the index $D(p) = D$ can be expressed in terms of the logarithm of the generator P of the infinite part of $E(\mathbb{Q})$. Or we can express their results in terms of the index D. The order of the torsion part of the Γ-invariant part of the dual of ${}_\infty\mathcal{S}'$, which was defined in (I.43), equals

$$\#\left((\widehat{{}_\infty\mathcal{S}'})_\Gamma\right)_{\mathrm{tors}} = \frac{\#D \cdot \prod c_v^{(p)} \cdot \#Ш(p)}{(\#E(\mathbb{Q})(p))^2} = \frac{\#J_0 \cdot \chi(\mathcal{R})}{\#E(\mathbb{Q})(p)}.$$

In particular, $\#J_0 \cdot \chi(\mathcal{R})$ is divisible by $\#E(\mathbb{Q})(p)$. See the table VI.2 for numerical examples.

Chapter III

Torsors and theta functions

> The drop of water still clung to his cheek; the shadow of the bee did not shift in the courtyard; the smoke from the cigarette he had thrown down did not blow away. [...] He worked the third act over twice. He eliminated some rather too-obvious symbols: the repeated striking of the hour, the music. There were no circumstances to constrain him.
> The Secret Miracle, Jorge Luis Borges.

III.1 Torsors

We come to the geometric part. It was probably Bloch in [Blo80] who was first to find a link between the theory of extensions and height pairings. Schneider and Oesterlé modelled their p-adic version on Bloch's description of the real-valued heights. Later, Mazur and Tate [MaTa83] put it in the context of bi-extensions and explained better the canonical p-adic height that exists in the ordinary case.

We will restrict ourselves to single extensions here. We refer to [Ser84, VII.16], [Oes82], [Lan83, 11.6] or [Col98, I.6.3] for a detailed description.

Let A be an abelian variety over a field F which is either the number field K or any of its completions K_v. Let $m = p^k$ for some $k \geqslant 1$. Given a point P in the dual $\check{A}(F)$, we can choose a divisor Δ representing the divisor class P, defined over F, whose support, written $|\Delta|$, is disjoint from $A[m]$. Cutting out the zero-section of the line bundle associated to the divisor Δ gives an extension of commutative F-group schemes

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{j} X_\Delta \xrightarrow{\pi} A \longrightarrow 0. \tag{III.1}$$

As an extension it does not depend on the choice of the divisor Δ, but only on the class P. Since Δ is algebraically equivalent to zero, there exists a function F_Δ on

$A \times A$ defined over F with $F_\Delta(\{O\} \times A) = 1$ and whose divisor is

$$\operatorname{div}(F_\Delta) = \operatorname{sum}^*(\Delta) - p_1^*(\Delta) - p_2^*(\Delta)$$

where $\operatorname{sum}\colon A \times A \longrightarrow A$ is the summation-map and p_1 and p_2 are the projections on the factors. According to section 3 in [Oes82], there exists a birational map $\psi\colon \mathbb{G}_m \times A \dashrightarrow X_\Delta$, defined over F, such that the addition on X_Δ can be written as

$$\psi(x_1, Q_1) + \psi(x_2, Q_2) = \psi(x_1 \cdot x_2 \cdot F_\Delta(Q_1, Q_2)\,,\, Q_1 + Q_2) \tag{III.2}$$

for all x_1, $x_2 \in \overline{F}^\times$ and Q_1, $Q_2 \in A(\overline{F}) \setminus |\Delta|$. Moreover, the map ψ is regular above $U = A \setminus |\Delta|$.

Thanks to the fact that $H^1(F, \mathbb{G}_m) = 0$, a short exact sequence

$$0 \longrightarrow F^\times \longrightarrow X_\Delta(F) \longrightarrow A(F) \longrightarrow 0 \tag{III.3}$$

of abelian groups can be deduced from (III.1). Taking m-torsion of it yields an extension of finite F-group schemes

$$0 \longrightarrow \mu[m] \longrightarrow X_\Delta[m] \longrightarrow A[m] \longrightarrow 0. \tag{III.4}$$

Proposition III.1. *The extension $X_\Delta[m]$ in (III.4) is isomorphic to the extension W_ξ^k constructed in the beginning of section I.5 for $\xi = \kappa(P)$.*

Proof. The proof presented here is analytic, the main reference is [Mum70], especially the theorem on page 20. Let V be a complex vector space and U a lattice in V such that the abelian variety A is isomorphic to U/V. By the description of the dual abelian variety over $\mathbb{C}$, there is, associated to each element P in $\check{A}$, a homomorphism α_P from U to the unit circle in $\mathbb{C}$. Moreover the space $X_P(\mathbb{C})$ can be represented as the space $\mathbb{C}^\times \times V$ quotient by the action of U given by $u \cdot (z, v) = (\alpha_P(u) \cdot z, u + v)$ for all $u \in U$, $z \in \mathbb{C}$ and $v \in V$. Let $\tilde{P}$ be a chosen element of $\check{A}$ such that $m\tilde{P} = P$. By the description of the dual, we see that $\alpha_{\tilde{P}}(u) = \alpha_P(u)^m$ for all $u \in U$.

A point in $X_P(\mathbb{C})[m]$ can be represented by (z, v) such that $(z^m, m \cdot v) = (\alpha_P(u), u)$ for some $u \in U$. Hence there is an m^{th} root of unity ζ such that $z = \zeta \cdot \alpha_{\tilde{P}}(u)$ and v maps to a m-torsion point Q in $A(\mathbb{C})$. Therefore we can send $(z, v) \in X_P[m]$ to (ζ, Q) in W_ξ^k. This is clearly an isomorphism of groups.

An element σ of the Galois group of F sends (z, v) to $(\zeta^\sigma \cdot \alpha_{\tilde{P}^\sigma}(u^\sigma), u^\sigma)$. Now the quotient of $\alpha_{\tilde{P}^\sigma}(u^\sigma)$ by $\alpha_{\tilde{P}}(u^\sigma)$ is equal to $\alpha_{\kappa(P)_\sigma}(u^\sigma)$. The following lemma found on page 184 in [Mum70] shows then that the action on $X_P[m]$ is the same as on W_ξ^k. This will end the proof of the proposition ∎

Lemma III.2. *Let u be an element of U and T be an m-torsion point on $\check{A}(\mathbb{C})$. Then $\alpha_T(u)$ equals the Weil pairing of T with the point on A represented by $\frac{1}{m}u$.*

Proof. Let Δ be a divisor representing T. Since $mT = O$, there are two functions f_T on A of divisor $n\Delta$ and g_T of divisor $[n]^*\Delta$. Hence g_T^n is a multiple of $f_T \circ [n]$ and the Weil pairing of T and a m-torsion point Q of A is the value of the constant function

$$\langle T, Q\rangle_{\text{Weil}} = \frac{g_T(y+Q)}{g_T(y)}.$$

The following maps

$$\mathscr{O}_A(\Delta) \xrightarrow{[n]^*} \mathscr{O}_A([n]^*\Delta) \xleftarrow[\cong]{\cdot g_T} \mathscr{O}_A$$

make the sections of the line bundle associated to Δ over an open W in A correspond to functions h on W such that

$$h(y+Q)\cdot g_T(y+Q) = h(y)\cdot g_T(y) \quad \text{for all } Q \in A[m] \text{ and } y \in W. \tag{III.5}$$

Consider the quotient of $\mathbb{C}\times V$ by the action of U given by $u\cdot(z,v) = (\langle T, Q\rangle_{\text{Weil}}\cdot z, \frac{u}{m}+v)$ with Q being the image of $\frac{u}{m}$ in $A[m]$. The sections of this line bundle are represented by functions h such that $u\cdot(h(y),y) = (h(y+Q), y+Q)$; in other words exactly by the condition (III.5). Hence removing the zero section, this quotient space is nothing else than X_T. We can conclude that $\alpha_T(u) = \langle T, Q\rangle_{\text{Weil}}$ as claimed. □

III.1.1 Completed torsors

We extend here the definitions that we have encountered so far in the chapter to points P in $\check{A}(F)^\star$.

Lemma III.3. *Given a point P in $\check{A}(F)^\star$, we can associate to it an exact sequences*

$$0 \longrightarrow (F^\times)^\star \longrightarrow X_P^\star(F) \longrightarrow A(F)^\star \longrightarrow 0.$$

I guess one should be more precise and say that we actually construct a homomorphism from $\check{A}(F)^\star$ to $\mathrm{Ext}^1_{\mathbb{Z}_p}(A(F)^\star, (F^\times)^\star)$.

Proof. The point P is represented by a sequence of points P_k in $\check{A}(F)$ such that P_{k+n} differs from P_k by $p^k Q$ for some point Q in $\check{A}(F)$. Write X_{k+n} and X_k for the extensions associated to P_{n+k} and P_k respectively. The multiplication by p^k in Ext can be written as

$$X_{p^kQ}(F) = \frac{X_Q(F)\times F^\times}{\{(-j(b), b^{p^k}) \mid b \in F^\times\}},$$

a fact that can be proven either using Baer sums or the fonctoriality of Ext as in a) on page 164 of [Ser84]. The injection of $F^\times$ here sends c to $(j_Q(c), c)$. So the space $X_{k+n}(F)$ associated to P_{k+n} can be represented by elements (x, z, a) with $x \in X_k(F)$, $z \in X_Q(F)$ and a in $F^\times$ such that $\pi(x) = \pi(z)$, subject to the relations $(-j(c), j(c), c) = 0$ and $(j(c), -j(b), b^{p^k}) = 0$ for all b and c in $F^\times$. Hence in $X_{n+k}(F)/p^k$, the expressions $(0, 0, c)$ are trivial. We conclude that there is an inverse to the natural map from $X_{k+n}(F)/p^k$ to $X_k(F)/p^k$, namely the map sending $x \in X_k(F)/p^k$ to $(x, z, 1)$ in $X_{n+k}(F)/p^k$ where z is any lift of $\pi(x)$ to $X_Q(F)$. In other words, the sequence

$$A(F)[p^k] \longrightarrow F^\times/p^k \longrightarrow X_k(F)/p^k \longrightarrow A(F)/p^k \longrightarrow 0 \qquad \text{(III.6)}$$

is isomorphic to the same sequence but with X_k replaced by X_{n+k}.

This proves that via the maps

$$X_{k+n}(F)/p^{n+k} \xleftarrow{[p^n]} X_{k+n}(F)/p^k \xleftarrow{\cong} X_k(F)/p^k$$

we can build the limit $X_P^\star(F) = \varprojlim X_k(F)/p^k$ as k tends to infinity. The limit of the exact sequence III.6 yields the sequence we wish to construct because, under our hypothesis on the field F, the group $A(F)/p^k$ is finite and $T_pA(F)$ is trivial. □

III.2 The pairing on the fine Mordell-Weil group

The reason $\mathbb{G}_m$-torsors were introduced in the last section is that our aim here is to link the cohomological definition of the height pairing on the fine Selmer group to an analytic pairing using theta functions.

Let A be an abelian variety over a number field K and let λ be as usual a map from $G_\Sigma(K)$ to $\mathbb{Z}_p$. The fine Mordell-Weil group $\mathfrak{M}_\Sigma$ was defined to be the following kernel

$$0 \longrightarrow \mathfrak{M}_\Sigma \longrightarrow A(K)^\star \longrightarrow \bigoplus_{v\in\Sigma} A(K_v)^\star$$

Let P be an element of $\check{A}(K)^\star$. It gives rise to a sequence as in lemma III.3

$$0 \longrightarrow (K^\times)^\star \longrightarrow X_P^\star(K) \longrightarrow A(K)^\star \longrightarrow 0$$

and similar for local fields.

Consider the maps λ_v from $(K_v^\times)^\star$ to $\mathbb{Z}_p$. If v does not divide p, then $A(K_v)^\star$ is finite, and hence we are allowed to extend the map λ_v to a map $\tilde{\lambda}_v$ on $X_P^\star(K_v)$ with

values in $\mathbb{Q}_p$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (K_v^\times)^\star & \xrightarrow{j} & X_P^\star(K_v) & \longrightarrow & A(K_v)^\star & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda_v} & & \vdots{\scriptstyle \tilde{\lambda}_v} & & & & \\ & & \mathbb{Z}_p & \hookrightarrow & \mathbb{Q}_p & & & & \end{array}$$

For places above p, we do not need to extend the map λ_v and hence we define $\tilde{\lambda}_v$ only on the image of j.

Proposition III.4. *Let P be an element of $\check{A}(K)^\star$ and Q be an element of $\mathfrak{M}(A/K)$. Choose any lift x of $Q \in A(K)^\star$ to $X_P(K)^\star$. Then*

$$\langle P, Q\rangle_\lambda = \langle \kappa(P), \kappa(Q)\rangle_\lambda = \sum_{all} \tilde{\lambda}_v(x).$$

allows one to evaluate the pairing from $H^1_\Sigma(K, T_p\check{A}) \times \mathfrak{R}(A/K)$ with values in $\mathbb{Q}_p$ on the image of the Kummer map κ.

Proof. (Un)-fortunately, we need to do a little detour via Néron-models. Let $\mathscr{A}^\circ$ be the connected component of the Néron-model of A over $\mathcal{O}$. The theory of extensions developed before should be possible just the same for Néron-models (see [Sch82, Section 3]). We represent the point $P \in \check{A}(K)^\star$ by a sequence of points P_k in $A(K)$. For the point P_k, there is an extension of $\mathcal{O}$-group schemes

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathscr{X}_k \longrightarrow \mathscr{A}^\circ \longrightarrow 0.$$

In particular, this provides us with a sequence

$$0 \longrightarrow \mathcal{O}_\Sigma^\times \longrightarrow \mathscr{X}_k(\mathcal{O}_\Sigma) \longrightarrow \mathscr{A}^\circ(\mathcal{O}_\Sigma) \longrightarrow H^1(\mathcal{O}_\Sigma, \mathbb{G}_m) = \mathrm{Cl}(\mathcal{O}_\Sigma).$$

Define the subgroup $I_k(\mathcal{O}_\Sigma)$ as the image of the map into $\mathscr{A}^\circ(\mathcal{O}_\Sigma)$; it is a subgroup of $A^\circ(K)$ of finite index bounded by the class number of $\mathcal{O}_\Sigma$ for all k. We can multiply the point Q with the class number and the product of the Tamagawa numbers to guarantee that Q lies in $I_k(\mathcal{O}_\Sigma)$ for all k. Thus we may assume that Q lies in the image of the completed $\mathscr{X}_P^\star(\mathcal{O}_\Sigma) = \varprojlim \mathscr{X}_k(\mathcal{O}_\Sigma)/p^k$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathcal{O}_\Sigma^\times)^\star & \longrightarrow & \mathscr{X}_P^\star(\mathcal{O}_\Sigma) & \longrightarrow & \mathscr{A}^\circ(\mathcal{O}_\Sigma)^\star & \longrightarrow & \mathrm{Cl}(\mathcal{O}_\Sigma)(p) \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{v\in\Sigma}(K_v^\times)^\star & \longrightarrow & \bigoplus_{v\in\Sigma} X_P^\star(K_v) & \longrightarrow & \bigoplus_{v\in\Sigma} A(K_v)^\star & \longrightarrow & 0 \end{array}$$

Choose a lift y of Q to $\mathscr{X}_P^\star(\mathcal{O}_\Sigma)$. Comparing this diagram to the definition of the height in (I.32) via the Kummer maps shows that $\langle \kappa(P), \kappa(Q)\rangle_\lambda$ is equal to the sum

of $\tilde{\lambda}_v(y)$ for v in Σ. Here we used the fact that the element y has to belong to the image of j for all places in Σ because Q lies in $\mathfrak{M}_\Sigma(A/K)$.

Let v be a place outside Σ. There is a natural map from the top line of the above diagram to the exact sequence

$$0 \longrightarrow (\mathcal{O}_v^\times)^\star \longrightarrow \mathscr{X}_P^\star(\mathcal{O}_v) \longrightarrow \mathscr{A}^\circ(\mathcal{O}_v)^\star \longrightarrow 0$$

in which all terms are finite. Hence there is a multiple of y that has trivial image in $\mathscr{X}_P^\star(\mathcal{O}_v) \longrightarrow X_P^\star(K_v)$ and so $\tilde{\lambda}_v(y) = 0$. Therefore we have shown the formula with x replaced by y. But the difference of x and y in $X_P^\star(K)$ is the image of an element z from $K^\times$ and, by the product formula, the sum of $\lambda_v(z)$ over all places is zero. □

III.2.1 The class group pairing

We quickly add here a description of the map $A^\circ(K) \longrightarrow \mathrm{Cl}(\mathcal{O}_\Sigma)$ which actually gives a pairing $\check{A}(K) \times A^\circ(K)$ with values in the finite group $\mathrm{Cl}(\mathcal{O}_\Sigma)$. Let Δ be a divisor representing a point $P \in \check{A}(K)$ on the Néron-model $\mathscr{A}$. Write f for the map $\mathscr{A}^\circ \longrightarrow \mathrm{Spec}(\mathcal{O}_\Sigma)$. The section Q in $\mathscr{A}^\circ(\mathcal{O}_\Sigma)$ intersects the divisor Δ in $\Delta.Q$. The divisor class of $f^*(\Delta.Q)$ in $\mathrm{Pic}(\mathrm{Spec}\,\mathcal{O}_\Sigma) = \mathrm{Cl}(\mathcal{O}_\Sigma)$ depends only on the class P of Δ.

This pairing appears in the article [MaTa83] of Mazur and Tate. In the function field case, it is the canonical height pairing described by Manin, see [Sil94, Theorem III.9.3] for the case of an elliptic surface. In the case of an elliptic curve, it will be calculated in IV.1.2.

III.3 Theta functions

Now, we are able to express the pairing using p-adic theta function as introduced by Barsotti, Néron [Nér82], Cristante and Norman [Nor85] (to cite a few).

For any choice of theta functions for the places above p, we construct here a pairing on $\check{A}(K) \times A(K)$ with values in $\mathbb{Q}_p$. In the end, it turns out that, when restricted to the fine Selmer group, all pairings coincide and agree with the p-adic height.

For an elliptic curve we will eventually write down theta functions explicitly and prove what is done in this section in more concrete terms.

Here is théorème 5 in [Oes82].

Proposition III.5. *There exists a continuous morphism $\tilde{\lambda}_v$ extending λ_v to $X_\Delta(K_v)$ with values in $\mathbb{Q}_p$. If v does not divide p, then the map λ_v is unique. For places v above p, the map is unique up to addition by a homomorphism of the form $e \circ \pi$ for a continuous morphism e from $A(K_v)$ to $\mathbb{Q}_p$.*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_v^\times & \longrightarrow & X_\Delta(K_v) & \longrightarrow & A(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda_v} & & \vdots{\scriptstyle \tilde{\lambda}_v} & & & & \\ & & \mathbb{Z}_p & \hookrightarrow & \mathbb{Q}_p & & & & \end{array}$$

Proof. (We follow the proof of Oesterlé.) The uniqueness is clear because there can not be any continuous morphism $A(K_v)$ to $\mathbb{Q}_p$ if v does not divide p.

The associated sequence of Lie algebras over K_v, say

$$0 \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{x} \longrightarrow \mathfrak{n} \longrightarrow 0,$$

as a sequence of vector spaces over K_v is split. Let r' be linear section $\mathfrak{x} \longrightarrow \mathfrak{g}$. Since all Lie algebras are commutative, the map r' is a morphism of Lie algebras. Hence there exists an open V in $X_\Delta(K_v)$ and a morphism r of Lie groups from V to $K_v^\times$ whose tangent map is r'. Now r is a section of j restricted to the image of r. We can extend the definition of r to $j(K_v^\times) + V$. Note that the index of $j(K_v^\times) + V$ in $X_\Delta(K_v)$ is finite, since its image in $A(K_v)$ is an open subgroup of the compact group $A(K_v)$. Therefore we can extend the map $\lambda_v \circ r$ to $X_\Delta(K_v)$. □

Note that in the case that the place is not above p, then this actually says that the valuation $\mathrm{ord}_v \colon K_v^\times \longrightarrow \mathbb{Z}$ can be extended to a homomorphism from $X_\Delta(K_v)$ to $\mathbb{Q}$.

Meanwhile, if the v divides p, the continuous map e from $A(K_v)$ to $\mathbb{Q}_p$ must be of the form $g \circ \mathscr{L}$ with g is $\mathbb{Q}_p$-linear map from the Lie algebra $\mathfrak{n}$ to $\mathbb{Q}_p$ and $\mathscr{L}$ is the logarithm from the formal group into the Lie algebra.

Let Δ be a divisor on $A(K)$, algebraically equivalent to zero, defined over K. By definition of the extension (III.1) of A by $\mathbb{G}_m$ associated to divisor Δ, there exists a rational section s_Δ of π from $A \setminus |\Delta|$ to X defined over K, unique up to multiplication by a scalar in $K^\times$.

Choose now a zero-cycle $\mathfrak{a}$ of degree zero on $A(K)$ whose sum is Q. For every finite place v, define a symbol

$$(\Delta, \mathfrak{a})_v = \tilde{\lambda}_v \circ s_\Delta(\mathfrak{a}) = \sum_{i=1}^N n_i \cdot \tilde{\lambda}_v \circ s_\Delta(Q_i), \qquad \text{if } \mathfrak{a} = \sum_{i=1}^N n_i\,(Q_i).$$

Since $\mathfrak{a}$ has degree 0, the expression does not depend on the scalar factor of s_Δ. It satisfies the properties of the Néron symbols. See section 8 of Néron's seminar talk [Nér82], for the details, or section 4 of [Sch82] and his reference to [Blo80]. See also theorem 11.6.2 in [Lan83].

The above construction of $\tilde{\lambda}_v$ can also be viewed as a section from the Lie algebra $\mathfrak{n}$ of A to the Lie algebra $\mathfrak{x}$ of X_Δ. The associated map from an open subgroup U

of $A(K_v)$ to $X_\Delta(K_v)$ can be written in terms of the birational map ψ in (III.2) as a solution $\theta_{\Delta,v}$ to the equation

$$F_\Delta(x,y) = \frac{\theta_{\Delta,v}(x+y)}{\theta_{\Delta,v}(x)\cdot\theta_{\Delta,v}(y)}$$

where F_Δ is still the rational function on $A\times A$ with divisor $\mathrm{sum}^*(\Delta) - p_1^*(\Delta) - p_2^*(\Delta)$. According to Néron in [Nér82, section 3], there exists analytic functions satisfying this equation and they only differ by an exponential factor of a function of the form $g\circ\mathscr{L}$ as above. To be precise, we should mention here that the analytic function is only defined in a neighbourhood U of O in $A(K_v)$. If we would like to extend it, we have to pass to a finite covering space.

This means that the map $s_v(Q) = \psi(\theta_{\Delta,v}(Q), Q)$ is a section of π.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_v^\times & \longrightarrow & X_P(K_v) & \xrightarrow{\pi} & A(K_v) & \longrightarrow & 0 \\ & & & & & \nwarrow^{s_v} & \uparrow & & \\ & & & & & & A(K_v)\setminus|\Delta| & & \end{array}$$

Since the symbol $(\Delta,\mathfrak{a})_v$ doesn't depend on the scalar factor of the section, we find that

$$(\Delta,\mathfrak{a})_v = \tilde{\lambda}_v\circ s_v(\mathfrak{a})$$

Via ψ there is also an obvious choice of the section r in the proof of proposition III.5, namely the projection on the first factor. Hence $\tilde{\lambda}_v\circ s_v = \lambda_v\circ\theta_{\Delta,v}$. Again, only for places v above p a different choice of the theta function will affect the result by adding a linear form of logarithms on A.

Therefore, depending on our choice of a theta function $\theta_{\Delta,v}$ for the places above p, there is a pairing on $\check{A}(K)\times A(K)$ with values in $\mathbb{Q}_p$ given as

$$\langle P,Q\rangle_{\lambda,\theta} = \sum_{\text{all}} \lambda_v\circ\theta_{\Delta,v}(\mathfrak{a}).$$

if P is the class of Δ and $\mathfrak{a}$ has sum equal to Q.

The term $\lambda_v\circ\theta_{\Delta,v}(\mathfrak{a})$ should be considered as the v-adic distance of $\mathfrak{a}$ from the divisor Δ. This leads to the notion of Weil's height functions and Néron's divisors. See [Lan83, Chapter 10]. Moreover for places outside p, the Néron-symbol $(\Delta,\mathfrak{a})_v$ can be described as the intersection pairing on the Néron model at the special fibre $\widetilde{\mathscr{A}_{\mathbb{F}_v}}$; at least if both are supported in the connected component.

III.3.1 Remarks

These single extensions are only one side of a splitting of bi-extensions. The point of view of bi-extensions is carried out in [MaTa83].

If the abelian variety A has ordinary reduction at all places v above p, there exists a canonical function $\theta_{\Delta,v}$ which gives rise to the canonical height pairing on the classical Selmer group. For this we refer to [MaTa91] and [Col98, Proposition II.6.1] (in the case of elliptic curves) and [Nor85, section 4].

In a more general situation, one can construct p-adic height pairings associated to "splittings of certain Hodge filtrations".

III.3.2 On the fine Mordell-Weil group

From proposition III.4 we deduce now the following

Proposition III.6. *Let P be a point in $\mathfrak{M}_\Sigma(\check{A}/K)$ and Q in $\mathfrak{M}_\Sigma(A/K)$, represented as sequences of points P_k and Q_k in $\check{A}(K)$ and $A(K)$ respectively. Choose theta functions $\theta_{\Delta_k,v}$ for all places v above p associated to the divisors Δ_k in the class of P_k. The height pairing affiliated with λ can be calculated as*

$$\langle P, Q\rangle_\lambda = \lim_{k\to\infty} \sum_{all} \lambda_v \circ \theta_{\Delta_k,v}(\mathfrak{a}_k)$$

where $\mathfrak{a}_k$ is a zero-cycle of degree zero whose sum equals Q_k and whose support is disjoint from the support of Δ_k.

A different choice of the theta functions does not change the result. This is due to that fact that the sequence Q_k approaches O at all places above p and hence the kernel of the logarithm. Once again the restriction on $P \in \check{A}(K)^\star$ to lie in the fine Mordell-Weil group did not actually matter in the construction of the height via theta functions. This corresponds to the extensions of the pairing described in (I.33).

III.3.3 The function field case

We can completely describe the p-adic pairing on an abelian variety over a global function field K in the case that the characteristic of the residue fields is different from p and zero. There are no places above p, and so the fine Selmer group coincides with the classical Selmer group. The pairing, restricted to global points $\check{A}^\circ(K) \otimes A^\circ(K) \longrightarrow \mathbb{Z}_p$ can now be expressed as the p-adic logarithm of the intersection pairing on the Néron model as described in the introduction. Since the intersection pairing is non-degenerated on the Néron-Severi group of the Néron-model viewed as a variety over the field of constants in K, we see that the p-adic height pairing is non-degenerated. We refer to Tate's article [Tat66].

In the case when the characteristic is equal to p, the above questions do not make much sense; as the fine group will be too small. We have to impose that the abelian

variety has ordinary reduction, so that we can use the canonical height pairing as in [Pap00].

Chapter IV

Elliptic curves

In the dream of the man who was dreaming,
the dreamt man awoke.
The circular Ruins; Jorge Luis Borges.

In this chapter, we aim to deduce an analytic formula for the p-adic height on the fine Selmer group of an elliptic curve and to link it to a naïve p-adic height. But first, we have to have a good understanding of the "denominator" of a point on an elliptic curve.

IV.1 Cancellations and the Class Group Pairing

The formulations in this section are kept as general as possible, for we intend to use the results later in the study of families of elliptic curves.

IV.1.1 Cancellation

Let R be a unique factorisation domain. We will study the points of an elliptic curve E over the fraction field F of R, given by a Weierstrass equation

$$y^2 + a_1\,xy + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6 \qquad \text{(Weq)}$$

with coefficients a_i in the ring R. A non-zero point P can always be written in the form

$$P = (x(P), y(P)) = \left(\tfrac{a(P)}{e(P)^2}\,,\,\tfrac{b(P)}{e(P)^3}\right), \qquad \text{(IV.1)}$$

where $a(P)$, $b(P)$ and $e(P)$ are elements of R such that $e(P)$ is relatively prime to both $a(P)$ and $b(P)$. Of course, these expressions are only well-defined up to the multiplication by units in $R^\times$.

The symbol t will always stand for the uniformizer $-\frac{x}{y}$ at the origin O of E in $F(E)$. Let $m > 0$ be an integer. The m-th division polynomial f_m (with respect

to the chosen Weierstrass equation) is defined to be the function in $F(E)$ having divisor $[m]^\star(O) - m^2 \cdot (O)$ and normalised to have $m \cdot t^{1-m^2}$ as the leading term at the origin O. A detailed description of these functions can be found in the first appendix of [MaTa91]. It will be used repeatedly that the square of f_m can be written as a polynomial in the function x of the form

$$f_m^2 = m^2\, x^{m^2-1} + \text{ lower order terms in } x \tag{IV.2}$$

whose coefficients turn out to be polynomials in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$, in particular they are in R. Similarly, the functions $g_m = x \cdot f_m^2 - f_{m+1} \cdot f_{m-1}$, defined for all integers $m > 1$, are polynomials of degree m^2 in x with integral coefficients. These polynomials appear in the formula describing multiplication by m:

$$\frac{a(mP)}{e(mP)^2} = x(mP) = \frac{g_m(P)}{f_m(P)^2} = \frac{g_m(P) \cdot e(P)^{2m^2}}{(f_m(P) \cdot e(P)^{m^2})^2}, \tag{IV.3}$$

valid for $m > 1$ and points $P \in E(F)$ that are not m-torsion. The expression on the right is written as a fraction of elements in R, since the power of $e(P)$ is sufficient to eliminate all the denominator. More precisely

$$f_m(P)^2 \cdot e(P)^{2m^2} = m^2\, a(P)^{m^2-1}\, e(P)^2 + \text{ higher order terms in } e(P) \tag{IV.4}$$

is a polynomial in $R[a(P), e(P)]$. But there is no reason to believe that this expression on the right of (IV.3) is a reduced fraction. By definition of $e(mP)$, the largest common factor of the numerator and the denominator in this fraction will be the square of the following element of R which will be called the *cancellation* of P when multiplied with m :

$$\delta_m(P) = \frac{f_m(P) \cdot e(P)^{m^2}}{e(mP)}. \tag{IV.5}$$

This is well-defined up to a unit in $R^\times$ whenever $m > 1$ and $P \in E(F)$ is not a m-torsion point, but depends on the equation (Weq).

Lemma IV.1. *Under a change of equation of the form*

$$x = u^2 \cdot x' + r_1, \qquad y = u^3 \cdot y' + u^2 r_2 \cdot x' + r_3, \tag{IV.6}$$

with u being a unit in $R^\times$ and the r_i in R, the cancellation $\delta_m(P)$ can only change by a unit.

The main result on cancellations is the following non-cancellation proposition. It can be deduced from the explicit formula for the local non-archimedian real-valued height functions (Theorem VI.4.1 in [Sil94]). We give a short independent proof here.

Proposition IV.2. *Let E be an elliptic curve given by an equation* (Weq) *over a ring R which is complete with respect to a discrete valuation v with residue field $\mathbb{F}_v$. If a point $P \in E(F)$ reduces to a non-singular point in the reduction $\tilde{E}(\mathbb{F}_v)$ then the cancellation $\delta_m(P)$ is a unit for all $m \neq 0$, provided $mP \neq O$.*

Proof. We split the proof into three cases. First suppose that $e(mP)$ and $e(P)$ are both units. Then the reduction $\tilde{P}$ of P and the reduction $m\tilde{P}$ of mP are two non-zero points in the group $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_v)$ of non-singular points on the reduction $\tilde{E}$. The multiplication formula (IV.3) is also valid in this group and so the denominator must be invertible in $\mathbb{F}_v$. This is what we want to prove, since the valuation of $f_m(P) \cdot e(P)^{m^2}$ is zero.

Next, we prove the statement when $e(mP)$ and $e(P)$ have the same valuation $k > 0$. Here our two points P and mP lie in the same layer $\hat{E}(\mathfrak{m}^k)$ of the formal group[1] $\hat{E}$ where $\mathfrak{m}$ is the maximal ideal in R. (We refer to chapter IV of [Sil86] for everything we need about formal groups.) Since there is a canonical isomorphism of groups

$$\frac{\hat{E}(\mathfrak{m}^k)}{\hat{E}(\mathfrak{m}^{k+1})} \cong \frac{\mathfrak{m}^k}{\mathfrak{m}^{k+1}},$$

we see that m must have valuation 0 as an element in R, otherwise mP would belong to $\widehat{E}(\mathfrak{m}^{k+1})$. The valuation of the expression in (IV.4) is $2k$ since $a(P)$ is a unit when $e(P)$ is not, so both terms in the definition (IV.5) of $\delta_m(P)$ have valuation k.

Finally, we look at the case when $e(mP)$ has a strictly bigger valuation than $e(P)$. If so, mP lies in a layer closer to O, and therefore the points $(m-1)P$ and $(m+1)P$ must lie in the same layer as P. Using what we just proved about such multiples, we see that the expressions

$$f_{m+1}(P) \cdot e((m+1)P)^{(m+1)^2} \qquad \text{and} \qquad f_{m-1}(P) \cdot e((m-1)P)^{(m-1)^2}$$

must have the same valuation as $e(P)$. Consider the numerator of the multiplication formula (IV.3):

$$\begin{aligned} g_m(P)\, e(P)^{2m^2} &= (f_m(P)^2\, x(P) - f_{m+1}(P)\, f_{m-1}(P)) \cdot e(P)^{2m^2} \\ &= f_m(P)^2\, e(P)^{2m^2} \cdot a(P)\, e(P)^{-2} \\ &\quad - f_{m+1}(P)\, e(P)^{(m+1)^2} \cdot f_{m-1}(P)\, e(P)^{(m-1)^2} \cdot e(P)^{-2}. \end{aligned}$$

The previous argument shows that the second term is a unit. Meanwhile, because the cancellation $\delta_m(P)^2$ is an integral element, the first term must have valuation at

[1] This is not the Pontryagin dual of E

least as big as the valuation of $e(mP)^2 \cdot e(P)^{-2}$, which is strictly positive in our case. So we see that the square of the cancellation

$$\delta_m(P)^2 = \frac{(f_m(P) \cdot e(P)^{m^2})^2}{e(mP)^2} = \frac{g_m(P) \cdot e(P)^{2m^2}}{a(mP)}$$

is a unit. This concludes the proof. □

Conversely one can prove that the cancellation is not a unit when P reduces to the singular point. The valuation of $\delta_2(P)$ is smaller than half the valuation of the discriminant Δ, but in most cases it is 1 or 2. This leads to a numerical interpretation of the term ($j_v(X, \mathfrak{a})$ in théorème III.4.1 in [Nér65]) that has to be added in the formula for the Néron-Tate height as an intersection pairing on the Néron model.

IV.1.2 The Class Group Pairing

Now, let R be a Noetherian Krull domain with class group $\mathrm{Cl}(R)$, written additively. Let F be the fraction field of R. Let E be an elliptic curve over F given by an equation (Weq) with coefficients in the ring R. The subgroup $E^\circ(F)$ of $E(F)$ of points with non-singular reduction at all primes of height 1 is of finite index by Tate's algorithm [Tat75]. For a non-zero point P in $E^\circ(F)$ and a prime $\mathfrak{p}$ of height 1, the localisation $R_\mathfrak{p}$ of R at $\mathfrak{p}$ is a principal ideal domain, and so we can define an element $e_\mathfrak{p}(P) \in R_\mathfrak{p}$. As a consequence of proposition IV.2 for the completion of $R_\mathfrak{p}$, we get a formula as in exercise 6.4 in [Sil94].

Corollary IV.3. *Let $m > 1$ and let P be a point in $E^\circ(F)$ that is not m-torsion, then, for all $\mathfrak{p}$,*

$$e_\mathfrak{p}(m \cdot P) = e_\mathfrak{p}(P)^{m^2} \cdot f_m(P), \quad \text{up to a unit in } P_\mathfrak{p}^\times.$$

According to remark 3.5.3 in [MaTa83], there is a pairing on $E(F)$ with values in the class group. We have come across this pairing already in III.2.1, but we give an explicit description of this here. If F is a function field of a curve this is just the canonical height on the minimal model considered by Manin. Define a map

$$\begin{aligned} q\colon E^\circ(F) &\to \mathrm{Cl}(R) \\ P &\mapsto \text{ the class of } \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(e_\mathfrak{p}(P)) \cdot \mathfrak{p} \end{aligned}$$

where the sum runs over all primes $\mathfrak{p}$ of height 1. The previous corollary allows us to calculate $q(mP)$ for an integer m: it is the class of

$$\sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(e_\mathfrak{p}(mP)) \cdot \mathfrak{p} = m^2 \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(e_\mathfrak{p}(P)) \cdot \mathfrak{p} + \sum_\mathfrak{p} \mathrm{ord}_\mathfrak{p}(f_m(P)) \cdot \mathfrak{p}.$$

But the second term is just the principal divisor $(f_m(P))$, so we conclude that $q(mP)$ is equal to $m^2 \cdot q(P)$. One can show furthermore that the parallelogram law holds for q and so it induces a bilinear form on $E^\circ(F)$ with values in $\mathrm{Cl}(R)$. But we are only interested in the following consequence:

Proposition IV.4. *Suppose that the class group $\mathrm{Cl}(R)$ is finite. There exists a subgroup of finite index $E^\bullet(F)$ of points P in $E^\circ(F)$ such that $q(P) = 0$, so there are elements $a(P)$, $b(P)$ and $e(P)$ in R, defined up to multiplication by $R^\times$, such that the ideal $(e(P))$ is not contained in any prime ideal of height 1 containing $(a(P))$ or $(b(P))$ and*

$$P = \left(\frac{a(P)}{e(P)^2}, \frac{b(P)}{e(P)^3}\right).$$

For a ring R of dimension 1 such as the number ring $\mathcal{O}$, this just means that the integral elements $e(P)$ and $a(P)$ are prime to each other.

Combining this with the corollary IV.3, we get the

Corollary IV.5. *In this subgroup $E^\bullet(F)$, we have the formula*

$$e(m \cdot P) = e(P)^{m^2} \cdot f_m(P), \quad \text{up to a unit in } R^\times. \tag{IV.7}$$

IV.2 Sigma functions

In this section, we wish to construct explicitely the theta function in the case of an elliptic curve E via the sigma functions. As explained in section III.3, the height on the fine Selmer group can be calculated using any theta function. Here the construction of Bernardi [Ber81] is used, rather than the canonical sigma function of Mazur and Tate in [MaTa91] which exists only if the reduction at places above p is ordinary. There is also a construction of a "canonical" sigma function for elliptic curves by Néron [Nér82, 8. Remark 2], but it was shown by Perrin-Riou in [PR84, page 240] that it actually agrees with the sigma function constructed by Bernardi.

We keep our Weierstrass equation (Weq) for E with coefficients a_i in the ring R. The expression t will still denote the uniformizer $-\frac{x}{y}$ at O. The invariant differential is $\omega = \frac{dx}{2y + a_1 x + a_3}$.

IV.2.1 Bernardi's sigma function

Using the formal group (see [Sil86, IV.1]), we can write

$$\begin{aligned} z = \mathscr{L}(t) &= t + \tfrac{1}{2}a_1\,t^2 + \tfrac{1}{3}(a_1^2 + a_2)\,t^3 + \tfrac{1}{4}(a_1^3 + 2\,a_1\,a_2 + 2\,a_3)\,t^4 + \cdots \\ \wp(t) = x(t) + \tfrac{1}{12}(a_1^2 + 4\,a_2) &= \frac{1}{t^2} - \frac{a_1}{t} + \tfrac{1}{12}(a_1^2 - 8\,a_2) - a_3\,t - (a_4 + a_1\,a_3)\,t^2 + \cdots \\ &= \frac{1}{z^2} + \tfrac{1}{240}(a_1^4 + 8\,a_1^2\,a_2 + 16\,a_2^2 - 24\,a_1\;a_3 - 48\,a_4)\,z^2 + \cdots \end{aligned}$$

for the formal logarithm and the Weierstrass $\wp$-function which are formal series in $F[\![t]\!]$ and $\frac{1}{12}R[\![t]\!]$ respectively. We define the σ-function of Bernardi by the following expression

$$\sigma(z) = z \cdot \exp\left(\iint (\tfrac{1}{z^2} - \wp(z))\,dz\,dz\right),$$

where of course the integration of the series has to be understood as the formal integration. So it is a formal solution to the differential equation

$$\frac{d}{\omega}\left(\frac{d\log\sigma}{\omega}\right) = -\wp. \tag{IV.8}$$

It can be expressed as a power series in z or t:

$$\begin{aligned} \sigma(z) &= z + \tfrac{1}{2880}(-a_1^4 - 8\,a_1^2\,a_2 - 16\,a_2^2 + 24\,a_1\,a_3 + 48\,a_4)\,z^5 + \cdots \\ \sigma(t) &= t + \tfrac{1}{2}a_1\,t^2 + \tfrac{1}{3}(a_1^2 + a_2)\,t^3 + \tfrac{1}{4}(a_1^3 + 2\,a_1\,a_2 + 2\,a_3)\,t^4 + \cdots \quad \in F[\![t]\!] \end{aligned}$$

Specify now that F is a non-archimedian completion K_v of a number field K. The power series $\sigma(t) \in K_v[\![t]\!]$ is a rational function on the formal group $\widehat{E}$ in the sense of [MaTa91, 2.1]. It is normalised and the divisor associated to it is (O). This means nothing else than that in the Weierstrass preparation theorem the decomposition of σ is $t \cdot u$ with $u \in 1 + t \cdot K_v[\![t]\!]$ having neither poles nor zeros. The translation of σ by a divisor Δ of degree zero on $\widehat{E}$ is defined to be

$$\sigma_\Delta(t(P)) = \prod_{i=1}^{N} \sigma(t(P - P_i))^{n_i} \qquad \text{if } \Delta = \sum_{i=1}^{N} n_i \cdot (P_i).$$

Then σ_Δ has divisor Δ on $\widehat{E}$.

The solution σ of the differential equation (IV.8) is not unique, all other solutions are of the form

$$\sigma^\alpha(t) = \sigma(t) \cdot \exp\bigl(\alpha_1 + \alpha_2\,\mathscr{L}(t) + \alpha_3\,\mathscr{L}(t)^2\bigr).$$

If we impose that $\sigma(O) = 0$ and $\frac{d\sigma}{dt}(O) = 1$ then we are limited to the functions

$$\sigma^\alpha(t) = \sigma(t) \cdot \exp\bigl(\alpha \cdot \mathscr{L}(t)^2\bigr).$$

for some $\alpha \in K_v$ (compare with [PR84, page 237]). Such functions are called *sigma functions*. They are all odd in the sense that $\sigma([-1]^* t) = -\sigma(t)$.

For a point Q on $E(K_v)$ with $t(Q)$ of valuation strictly greater than $\mathrm{ord}_v(\ell)/(\ell-1)$, where ℓ is the characteristic[2] of the residue field $\mathbb{F}_v$, the series for $\sigma(Q) = \sigma(t(Q))$ converges (see [Ber81]). In other words, there is an open subgroup U around O on which σ gives an analytic function with a single simple zero at O. If the divisor Δ is supported with in U, then σ_Δ is analytic on U.

From the properties of the complex sigma function, we derive the formal identities in $K(\!(s,t)\!)$

$$\frac{\sigma(t+s)\cdot\sigma(t-s)}{\sigma(t)^2\cdot\sigma(s)^2} = -\wp(t)+\wp(s)$$
$$\sigma([m]t) = f_m(t)\cdot\sigma(t)^{m^2}$$

with the division polynomial f_m. Indeed, these relations are exactly the reason that the local factor at ∞ for the canonical real-valued height is a quasi-quadratic function satisfying the quasi-parallelogram law (see [Sil94, chapter VI]).

The second equation can also be used to extend the definition of the σ-function to the whole of $E(K)$, since the open subgroup U has finite index in the compact group $E(K_v)$. At least up to a root of unity it is well-defined. As we will take the p-adic logarithm of it, this factor disappears again.

Lemma IV.6. *Let Δ be a divisor of degree zero on E, defined over K_v, whose support is contained in U. The analytic function*

$$G(P,Q) = \frac{\sigma_\Delta(P+Q)}{\sigma_\Delta(P)\cdot\sigma_\Delta(Q)}$$

on $U\times U$ is the restriction of a rational function F_Δ defined over K_v on $E\times E$ of divisor $\mathrm{sum}^*(\Delta) - p_1^*(\Delta) - p_2^*(\Delta)$.

Proof. Write $\Delta = \sum n_i P_i$. First, we note that the following function is the restriction of a rational function

$$\prod(-\wp(X-P_i)+\wp(Y))^{n_i} = \prod\Big(\frac{\sigma(X-P_i+Y)\cdot\sigma(X-P_i-Y)}{\sigma(X-P_i)^2\cdot\sigma(Y)^2}\Big)^{n_i}$$
$$= \frac{\sigma_\Delta(X+Y)\cdot\sigma_\Delta(X-Y)}{\sigma_\Delta(X)^2\cdot\sigma(Y)^{(2\sum n_i)}}.$$

The term in $\sigma(Y)$ vanishes because Δ is assumed to have degree 0. Putting $X=Y$, we find that the quotient $\sigma_\Delta([2]X)/\sigma_\Delta(X)^2$ is the restriction of a rational function. If[3]

[2] we do allow $\ell = p$.

[3] for $\ell = 2$ this proves still that the square of the above function is rational, or we could have restricted to $2U$.

$\ell \neq 2$, then $[2]$ is an isomorphism on U and hence we can find X and Y such that

$$P = X + Y \qquad 2\,X = P + Q$$
$$Q = X - Y \qquad 2\,Y = P - Q$$

We conclude that

$$\frac{\sigma_\Delta(X+Y)\,\sigma_\Delta(X-Y)}{\sigma_\Delta(X)^2} \cdot \frac{\sigma_\Delta(X)^2}{\sigma_\Delta([2]X)} = \frac{\sigma_\Delta(P)\cdot\sigma_\Delta(Q)}{\sigma_\Delta(P+Q)}$$

is the restriction of a rational function. It is clear that this has divisor as claimed. □

Of course, the choice of the sigma function is not important for this lemma, a different choice changes the function G by a constant. This is the proof the function σ_Δ is a theta function $\theta_{\Delta,\upsilon}$ as defined in section III.3.

Instead of working with theta functions, we could have adopted the point of view of Colmez in [Col98] who constructs p-adic heights using Green's functions.

IV.3 The p-adic height pairing

Let E be an elliptic curve over a number field K given by a (Weq) over the ring of integers $\mathcal{O}$ of K. We do not require that the equation is minimal with respect to some places and the height pairing is independent of the chosen model. In this section we will find an explicit formula for the p-adic height pairing on the fine Mordell-Weil group affiliated with a character $\lambda\colon G_\Sigma(K) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p$ given as a collection of maps $\lambda_\upsilon\colon K_\upsilon^\times \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p$.

The proposition IV.4 guarantees us the existence of a subgroup $E^\bullet(K)$ in $E(K)$ of finite index such that the denominator $e(P)$ of a point $P \in E^\bullet(K)$ is a well defined element of $\mathcal{O}$.

Let P and Q be two points in $E(K)$. As a divisor Δ for P we choose $(O)-(-P)$ and as the zero-cycle $\mathfrak{a}$ for Q, we take $(Q+T)-(T)$ where T is any point in $E(K)$ close to O. Let υ be any finite place in K and let σ_υ be a υ-adic sigma function. The obvious choice being the sigma function of Bernardi constructed in the previous section. The local symbol is given by

$$(\Delta,\mathfrak{a})_\upsilon = \lambda_\upsilon(\sigma_{\upsilon,\Delta}(\mathfrak{a})) = \lambda_\upsilon\left(\frac{\sigma_\upsilon(Q+T)}{\sigma_\upsilon(Q+T+P)}\cdot\frac{\sigma_\upsilon(P+T)}{\sigma_\upsilon(T)}\right).$$

As a function in T, the right hand side has divisor $(-P-Q)+(O)-(-P)-(-Q)$, so there exists a function[4] $f(T)$ with this divisor defined over the global field K. We

[4] actually a fraction of two linear terms

normalise it so that $\frac{df}{\omega}(O) = 1$. Thus

$$(\Delta, \mathfrak{a})_v = \lambda_v \left(\frac{\sigma_v(P) \cdot \sigma_v(Q)}{\sigma_v(P+Q)} \cdot f(T) \right).$$

The factor can be found by looking at the derivative at O. We draw the conclusion that the pairing for this choice of σ_v is

$$\begin{aligned} \langle P, Q \rangle_{\lambda,\sigma} &= \sum_{\text{all } v} \lambda_v \left(\frac{\sigma_v(P) \cdot \sigma_v(Q)}{\sigma_v(P+Q)} \cdot f(T) \right) \\ &= \sum_{\text{all } v} \lambda_v \left(\frac{\sigma_v(P) \cdot \sigma_v(Q)}{\sigma_v(P+Q)} \right) \end{aligned}$$

The last equality follows from the fact that $f(T)$ is defined over K and so the sum of $\lambda_v(f(T))$ is zero.

If the place v is not above p, then the only thing that matters in the above expression is the valuation of the fraction of the sigma functions. Note that since we normalised the sigma-function, so that $\frac{d\sigma_v}{\omega}(O) = 1$, the valuation of $\sigma_v(P)$ equals the valuation of $e(P)$ if P belongs to the subgroup on which the series σ_v converges. But if P is outside this group, but still belonging to $E^\bullet(K)$, the formula $\sigma_v(P)^{m^2} \cdot f_m(P) = \sigma_v(m\,P)$ that was used to extend the sigma function and the corresponding formula (IV.7) show that the equality between the valuations will still hold.

Therefore, the height pairing associated to these sigma functions σ_v can be further simplified to

$$\langle P, Q \rangle_{\lambda,\sigma} = \sum_{v \nmid p} \lambda_v \left(\frac{e(P) \cdot e(Q)}{e(P+Q)} \right) + \sum_{v \mid p} \lambda_v \left(\frac{\sigma_v(P) \cdot \sigma_v(Q)}{\sigma_v(P+Q)} \right).$$

In particular for the cyclotomic $\mathbb{Z}_p$-extension defined in I.2.2, the pairing takes the form

$$\langle P, Q \rangle_{\text{cyc},\sigma} = \sum_{v \mid p} \log_p \circ N_{K_v:\mathbb{Q}_p} \left(\frac{e(P)}{\sigma_v(P)} \cdot \frac{e(Q)}{\sigma_v(Q)} \cdot \frac{\sigma_v(P+Q)}{e(P+Q)} \right). \tag{IV.9}$$

Both formulae are only valid, if σ_v converges for P and Q for all $v \mid p$ and both, P and Q belong to $E^\bullet(K)$.

Let now P and Q be two elements of $\mathfrak{M}(E/K)$ given by sequences P_k and Q_k of points in $E(K)$. Suppose we can choose them in such a way that they all belong to the subgroup of finite index for which the above formula holds. Then the above formula gives the p-adic height $\langle P, Q \rangle_\lambda$.

$$\langle P, Q \rangle_\lambda = \lim_{k \to \infty} \langle P_k, Q_k \rangle_{\lambda,\sigma}$$

This is independent of the chosen sigma function because a change of the sigma functions by a factor $\exp(\alpha \cdot \mathscr{L}(t)^2)$ changes the v-part of the pairing of P_k with Q_k by

$$N_{K_v:\mathbb{Q}_p}\left(\frac{\exp(\alpha \cdot \mathscr{L}(P_k+Q_k)^2)}{\exp(\alpha \cdot \mathscr{L}(P_k)^2)\cdot \exp(\alpha \cdot \mathscr{L}(Q_k)^2)}\right) = N_{K_v:\mathbb{Q}_p} \circ \exp(2\alpha \cdot \mathscr{L}(P_k)\cdot \mathscr{L}(Q_k)).$$

Note once again that it suffices that Q_k tends v-adically to O for all places v above p and that P can be any point of $E(K)^\star$. This is the extension of the pairing to $E(K)^\star \times \mathfrak{M}$.

Instead of talking about the bilinear form, we could also restrict the attention to the induced quadratic map defined as

$$h_\lambda(P) = \frac{1}{2}\cdot \langle P, P\rangle_\lambda$$

for all P in $\mathfrak{M}(E/K)$. We can recover the bilinear form $\langle\cdot,\cdot\rangle_\lambda$ from h_λ via the formula $\langle P, Q\rangle_\lambda = h_\lambda(P+Q) - h_\lambda(P) - h_\lambda(Q)$. Let us put the results of this section so far into a

Theorem IV.7.

Let E be an elliptic curve over a number field K and let P be a point in the intersection of $\mathfrak{M}(E/K)$ and $E^\bullet(K)^\star$. Write P as a sequence of points $P_k \in E^\bullet(K)$. Then the cyclotomic p-adic height of P can be computed using the formula

$$h_{cyc}(P) = \lim_{k\to\infty} \sum_{v|p} \log_p \circ N_{K_v:\mathbb{Q}_p}\left(\frac{\sigma_v(P_k)}{e(P_k)}\right).$$

This is up to the sign an expression similar to the local decomposition of the canonical real-valued height of Néron and Tate. Since we will only be interested in the valuation of the regulator, the sign does not matter at all. Note also that the coefficients of σ_v are in fact in K for all v. If we take an embedding of K into the algebraic closure $\overline{\mathbb{Q}_p}$, we can write the formula as the logarithm of the sum of conjugates.

We can get rid of the transcendental function σ by expressing it as a limit of naïve heights, involving only the limit of p-adic logarithm of the numerator. The pairing on the fine Selmer group looks "less transcendental" than the canonical pairing on the Selmer group in the ordinary case. One could hope that it is easier to prove that the fine pairing is non-degenerate.

The first limit formula for p-adic heights appeared in Perrin-Riou's articles [PR84] and [PR83]. Almost in the form we present here, it is stated in [BerPR93] where Bernardi and Perrin-Riou used the formula to do calculations of the height pairing associated to the sigma function of Bernardi.

Theorem IV.8.
Let E be an elliptic curve over a number field K. Let P and Q be points in $\mathfrak{M}(E/K)$. that can be written as a sequence of points P_k and Q_k in $E^\bullet(K)$. Then the cyclotomic p-adic height pairing of P and Q is equal to

$$\langle P, Q\rangle_{\text{cyc}} = \frac{1}{2} \cdot \lim_{k\to\infty} \log_p \circ N_{K:\mathbb{Q}} \left(\frac{a(P_k) \cdot a(Q_k)}{a(P_k + Q_k)} \right)$$

where a denotes the numerator as defined in proposition IV.4.

Proof. If a point $P \in E^\bullet(K)$ lies in the domain of convergence of σ_v, we have that

$$\frac{\sigma_v(P)}{t(P)} = 1 + \tfrac{1}{2}\, a_1\, t(P) + \mathbf{O}(t(P))^2 \equiv 1 \pmod{\mathfrak{m}_v^{\operatorname{ord}_v(t(P))}},$$

at least if the valuation of $t(P)$ is sufficiently large so that the denominators do not interfere. Since the valuation of P_k and Q_k are growing with k, the limit of the pairing associated to the sigma function of Bernardi can be simplified to

$$\langle P, Q\rangle_{\text{cyc}} = \lim_{k\to\infty} \log_p \circ N_{K:\mathbb{Q}} \left(\frac{e(P_k)}{t(P_k)} \cdot \frac{e(Q_k)}{t(Q_k)} \cdot \frac{t(P_k + Q_k)}{e(P_k + Q_k)} \right).$$

The Weierstrass equation for a point P with high valuation at a place v gives

$$\begin{aligned} b(P)^2 &\equiv b(P)^2 + a_1\, b(P)\, a(P)\, e(P) + a_3\, b(P)\, e(P)^3 \\ &\equiv a(P)^3 + a_2\, a(P)^2\, e(P)^2 + a_4\, a(P)\, e(P)^4 + a_6\, e(P)^6 \\ &\equiv a(P)^3 \pmod{\mathfrak{m}_v^{\operatorname{ord}_v(t(R))}} \end{aligned}$$

and so

$$\frac{e(P)^2}{t(P)^2} = \frac{b(P)^2}{a(P)^2} \equiv a(P).$$

This proves the theorem. □

Instead of the numerator of the x-coordinate, we could have taken the numerator b of the y-coordinate and change the $\frac{1}{2}$ to a $\frac{1}{3}$ in the theorem.

Chapter V

Variation in families

> The universe (which others call the Library) is composed of an indefinite and perhaps, infinite number of hexagonal galleries, with vast air shafts between, surrounded by very low railings. From any of the hexagon one can see, interminably, the upper and lower floors.
> The Library of Babel; Jorge Luis Borges.

We wish to analyse the variation of the p-adic height of a section in an elliptic surface. For the real-valued height this was initiated by Silverman and Tate, see the chapter III.11 in [Sil94] for details. In the article [Wut04], the variation of the canonical p-adic height on an elliptic surface over the affine line was studied. It was shown that under certain restrictions on the section the height varied continuously.

We transpose these results to the heights studied in this thesis. We also remove the not so important restriction of the base curve being the affine line. Most of the results from [Wut04] carry over to our situation here. For the same important reason as explained for the canonical height, the technical restrictions on the section can not be removed.

Since the fine Selmer group itself is "varying" from fibre to fibre, we shall start by analysing the variation of the height obtained from the sigma function of Bernardi. After that, we will restrict to sections in the fine Mordell-Weil group and prove results about the variation of the height on the fine Selmer group.

V.1 Families

Let K be an number field with $\mathcal{O}$ its ring of integers. Let C be a smooth, projective and geometrically connected curve defined over K and $\mathcal{E}_K \longrightarrow C$ an elliptic surface fibred over C. Also a regular model $\mathcal{C}$ of C over $\mathcal{O}$ can be chosen, see [Liu02, chapter

10]. We will see later that there is no minimal regular model of $\mathcal{E}_K$ over $\mathcal{C}$ with the nice properties we would expect from such a "Néron-model" over a base of dimension 2.

We cover C by a finite number of affine opens U/K such that $\mathrm{Pic}(U) = 0$. Choose regular integral models $\mathcal{U}$ over $\mathcal{O}$ for U of the form

$$\mathcal{U} = \mathrm{Spec}\, R = \mathrm{Spec}(\mathcal{O}[T_1, T_2, \dots T_m]/(f_1, \dots f_n))$$

We see that $\mathrm{Pic}\,\mathcal{U} = \mathrm{Cl}\,\mathcal{O}$. Furthermore, we may refine the cover until we have on every $\mathcal{U}$ a section of the relative differential and hence by [Del75], there is an integral model $\mathcal{E}_\mathcal{U} \longrightarrow \mathcal{U}$ of the surface $\mathcal{E}_K$ given by a Weierstrass equation (Weq) with coefficients a_i in R. The scheme $\mathcal{E}$ obtained by glueing the $\mathcal{E}_\mathcal{U}$ will be referred to as a *family* and the cover $\mathcal{U}$ with the demanded properties will be called a *tight* cover.

There is a group of sections $\mathcal{E}_K(K)$, which can be viewed as the points of the generic fibre, i.e. the solutions of the Weierstrass equations defined over the function field $K(C)$ of C. For short, we write $\mathcal{E}(K)$ for this group and we will call its non-zero elements *sections* of $\mathcal{E}$; they are not sections over $\mathcal{O}$ of the scheme $\mathcal{E}$. Denote by $\mathcal{E}^\circ(K)$ its subgroup of finite index containing the sections that do not meet any singularity of a fibre of $\mathcal{E}_K \longrightarrow C$ as in lemma III.9.4 in [Sil94].

For a closed point τ in C, the fibre above τ will be denoted by $\mathcal{E}_\tau$ and, given a section $P \in \mathcal{E}(K)$, the point P_τ in $\mathcal{E}_\tau(K)$ is where P meets the fibre $\mathcal{E}_\tau$. For a finite place υ of $\mathcal{O}$, $\tilde{\mathcal{E}}_\upsilon$ stands for the reduction of $\mathcal{E}$ at υ, which, on $\mathcal{U}$, is the reduced Weierstrass equation over $\mathbb{F}_\upsilon[T_1, T_2 \dots T_m]/(\bar{f}_j)$. The reductions of the fibre $\mathcal{E}_\tau$ are denoted by $\tilde{\mathcal{E}}_{\tau,\upsilon}$.

V.1.1 Local properties

We start by analysing the properties of the denominator of a section P in $\mathcal{E}^\circ(K)$ for a fixed finite place υ in $\mathcal{O}$. As usual $\mathcal{O}_\upsilon$ denotes the ring of integers of the completion K_υ of the number field K with maximal ideal $\mathfrak{m}_\upsilon$.

All our considerations will be of geometrically local nature and we concentrate therefore on the Weierstrass equation of $\mathcal{E}_\mathcal{U}$ over the ring R. Let $R_\upsilon = \mathcal{O}_\upsilon \otimes_\mathcal{O} R$ be the ring of functions of $\mathcal{U}_\upsilon = \mathcal{U} \times \mathcal{O}_\upsilon$. Note that R_υ is a principal ideal domain under our hypothesis on the class group of R.

We can define, for each section in $\mathcal{E}^\circ(K_\upsilon)$, an element $e_\upsilon(P)$ in R_υ well-defined up to a unit in $R_\upsilon^\times$ as in section IV.1.

Let τ be a point[1] in $\mathcal{U}_\upsilon(\mathcal{O}_\upsilon)$. On the one hand, the coordinates of the point $P_\tau \in$

[1] we are not going to distinguish in notation the generic point on $U(K_\upsilon)$ from the section $\mathcal{U}(\mathcal{O}_\upsilon)$

$\mathcal{E}_\tau(K_\upsilon)$ can be written according to (IV.1) as reduced fractions of elements in $\mathcal{O}_\upsilon$, say

$$P_\tau = \left(\frac{a_\upsilon(P_\tau)}{e_\upsilon(P_\tau)^2} \, , \, \frac{b_\upsilon(P_\tau)}{e_\upsilon(P_\tau)^3} \right),$$

at least if $P_\tau \neq O_\tau$.

On the other hand, when evaluating $e_\upsilon(P) \in R_\upsilon$ at τ, written $e_\upsilon(P)(\tau)$, we will also obtain fractions of elements in $\mathcal{O}_\upsilon$, namely

$$P_\tau = \left(\frac{a_\upsilon(P)(\tau)}{e_\upsilon(P)(\tau)^2} \, , \, \frac{b_\upsilon(P)(\tau)}{e_\upsilon(P)(\tau)^3} \right). \tag{V.1}$$

Once again, we have two fractions that we can compare: we might have some cancellation in the expression (V.1), which allows us to define, for every $\tau \in \mathcal{U}_\upsilon(\mathcal{O}_\upsilon)$ and section $P \in \mathcal{E}^\circ(K_\upsilon)$ with $P_\tau \neq O_\tau$, an element $\gamma_\upsilon(P,\tau)$ in $\mathcal{O}_\upsilon$ by

$$e_\upsilon(P_\tau) \cdot \gamma_\upsilon(P,\tau) = e_\upsilon(P)(\tau), \tag{V.2}$$

which is defined up to a unit in $\mathcal{O}_\upsilon^\times$.

Lemma V.1. *Let $P \in \mathcal{E}^\circ(K_\upsilon)$ be a section in a family $\mathcal{E}$. The map $\tau \mapsto \mathrm{ord}_\upsilon(\gamma_\upsilon(P,\tau))$ from $\mathcal{U}(\mathcal{O}_\upsilon)$ to the integers is bounded and υ-adically continuous.*

Proof. The ring R_υ has dimension 2 and so the intersection of the zero-loci of the relatively prime elements $a_\upsilon(P)$ and $e_\upsilon(P)$ in R_υ is of dimension 0. The intersection number at the maximal ideal $(\mathfrak{m}_\upsilon, \tau)$ in R_υ of $a_\upsilon(P)$ and $e_\upsilon(P)$ is a bound for the valuation of $\gamma_\upsilon(P,\tau)$. □

When a section $P \in \mathcal{E}(K_\upsilon)$ has non-singular reduction for all fibres $\tau \in \mathcal{U}(\mathcal{O}_\upsilon)$, i.e. $P_\tau \in \mathcal{E}_\tau^\circ(K_\upsilon)$ for all τ, we say that the section has *good reduction* (with respect to the cover $\mathcal{U}$).

On an elliptic curve over a local field F, every point can be multiplied by a sufficiently big integer to guarantee that it has good reduction, due to the fact that the subgroup $E^\circ(F)$ is of finite index. Unfortunately, it is not true for families as the following example for $R_\upsilon = \mathbb{Z}_2[T]$ shows:

$$\mathcal{E}: \quad y^2 + x\,y = x^3 - T^3 + 2\,T^2.$$

$\mathcal{E}$ has a section $P = (T,T)$ and $2P = (T^2 - \frac{5}{3}\,T - \frac{2}{9}, -T^3 + 2\,T^2 + \frac{4}{27})$ is in the subgroup $\mathcal{E}^\circ(\mathbb{Q}_2)$. The family has multiplicative reduction at $\tau = 0$ with singularity $(0,0)$, the multiples of the section $2P$ meet the fibre $\mathcal{E}_0$ at

$$\begin{array}{lll} (2P)_0 = (-\frac{2}{9}, \frac{2^2}{27}) & (4P)_0 = (\frac{2^2}{9}, -\frac{2^4}{27}) & (6P)_0 = (-\frac{2^3}{9^2}, \frac{2^6}{9^3}) \\ (8P)_0 = (\frac{2^4}{15^2}, -\frac{2^8}{15^3}) & (10P)_0 = (-\frac{2^5}{33^2}, \frac{2^{10}}{33^3}) & \cdots \end{array}$$

So there is no hope that any multiple of P will have non-singular reduction. Actually the Tamagawa number of the fibre at $\tau = 2^n$ is $2n+1$. In terms of Néron-models, this reflects the fact that the Néron flt-model of $\mathbb{G}_m$ over a discrete valuation ring has an infinite cyclic group of connected components (see Example 10.1.5 in [BoLüRa90]). For an additive fibre, this "group of connected components" would have to be an infinite torsion $K_v/\mathcal{O}_v$, but here not even the Néron flt-model exists.

The following proposition tells us that the above phenomenon is the only obstacle for finding a multiple of a section with good reduction.

Lemma V.2. *Let P be a section of $\mathcal{E}$ defined over K_v.*

i). Suppose $\mathcal{E}_K$ has no bad fibre of multiplicative type. Then there exists a refined tight cover such that a multiple of the section P has good reduction.

ii). If $\mathcal{E}_K$ has fibres of multiplicative type and P belongs to $\mathcal{E}^\circ(K_v)$ then there is such a cover if the reduction of P_τ is non-singular on a whole v-adic neighbourhood of each multiplicative fibre.

Proof. We may suppose that the section P belongs to $\mathcal{E}^\circ(K_v)$. We may refine the cover $\mathcal{U}$ in such a way that every point of $C(K_v)$ appears as the generic point of an element of $\mathcal{U}(\mathcal{O}_v)$ for some $\mathcal{U}$. The cover will still be finite because $C(K_v)$ is compact and the $\mathcal{U}(\mathcal{O}_v)$ are open in the v-adic topology.

First, we treat the case when there is no singular fibre in $\mathcal{U}(\mathcal{O}_v)$. We claim that the index of $\mathcal{E}^\circ_\tau(K_v)$ in $\mathcal{E}_\tau(K_v)$ is bounded for all τ in $\mathcal{U}(\mathcal{O}_v)$. In order to prove this claim, we first have to note that the valuation of the discriminant Δ is bounded because it cannot have a zero on $\mathcal{U}(\mathcal{O}_v)$. For a given τ, we can change the given Weierstrass equation $\mathcal{E}_\tau$ over $\mathcal{O}$ to a minimal form by replacing x by $u^2\,x' + r$ and y by $u^3\,y' + u^2\,s\,y + t$ as in proposition VII.1.3 in [Sil86]. The valuation of u is bounded by $\frac{1}{12}\operatorname{ord}_v(\Delta)$; hence it is bounded on $\mathcal{U}(\mathcal{O}_v)$. The index in the minimal Weierstrass equation is the Tamagawa number and hence it is bounded by the maximum of 4 and the valuation of the discriminant. If u is not a unit, then the index on $\mathcal{E}_\tau$ is the product of the index on the minimal equation, the number of points in the reduction of the minimal equation and $(\#\mathbb{F}_v)^{\operatorname{ord}_v(u)-1}$. This proves the claim.

Next we suppose that there is an additive fibre at τ_0 in $\mathcal{U}(\mathcal{O}_v)$. We may refine the cover, so that the reduction on $\mathcal{U}(\mathcal{O}_v)$ is constant and, hence, additive on the whole v-adic neighbourhood $U_0 = \mathcal{U}(\mathcal{O}_v)$ in $C(K_v)$ of τ_0. We may assume that $(0,0)$ is the singularity on $\mathcal{E}_{\tau_0}$ and that the valuation of $\operatorname{ord}_v(x(P_\tau))$ is bounded because P can not pass through the singularity since it belongs to $\mathcal{E}^\circ(K_v)$. Write $X(P_\tau)$ for the x-coordinate of P_τ in a minimal equation, i.e. $X(P_\tau) = u^{-2} \cdot x(P_\tau)$. If we multiply the

section by 4, we are guaranteed that the point P_τ, for every τ, when transferred to the minimal equation, has non-singular reduction. A point on $\mathcal{E}_\tau$ has non-singular reduction if and only if it has non-singular reduction in the minimal equation and the valuation of its x-coordinate is smaller than $-2\,\mathrm{ord}_v(u)$. Since the valuation of $x(P_\tau)$ is bounded, we may multiply P sufficiently often with the number of elements of the residue field $\mathbb{F}_v$ until this holds for P_τ for all τ. □

Another example is the family over $\mathbb{Z}_2[T]$ given by

$$\mathcal{E}: \qquad y^2 - 2xy + Ty = x^3 - (2+T)x^2 + 2Tx$$

with two independent sections $P = (2,0)$ and $Q = (1,1)$. There is a fibre of multiplicative type at $T = 0$ with its singularity at $(0,0)$. Neither P nor Q meet the singularity, but P has bad reduction. Nevertheless $2P$ has x-coordinate $\frac{T^3-2T^2-8T+16}{(T-4)^2}$ and hits the bad fibre at the same point as Q does. In fact, if τ is divisible by 8, the cancellation $\gamma_2(2P,\tau)$ equals 4 and $e_2(2P_\tau)$ and $a(2P_\tau)$ are units. Hence the reduction of $2P$ is good in this neighbourhood. Here the reduction of $\mathcal{E}_\tau$ for $\tau = 2^n$ is additive of type I^*_{2n-1} with $c_2 = 4$.

V.1.2 Global properties

Let $P \in \mathcal{E}^\circ(K)$ be a section. Since the class number of K is finite and constant for all R in the cover, the proposition IV.4 provides us with a subgroup of finite index $\mathcal{E}^\bullet(K)$ of $\mathcal{E}^\circ(K)$ such that P admits on every $\mathcal{U}$ a global denominator $e(P)$ in R, equal to $e_v(P)$ for all v and well-defined up to an element in $R^\times$.

Lemma V.3. *Let P be section of $\mathcal{E}^\bullet(K)$. Then $\tau \longmapsto \mathrm{ord}_v(\gamma_v(P,\tau))$ is the trivial map for all but a finite number of places.*

Proof. Again R has dimension 2 and the zero-loci of $e(P)$ and $a(P)$ have to intersect in a subscheme of dimension 0 of $\mathcal{U}$. □

Lemma V.4. *Let P be a section of a family $\mathcal{E}$. Suppose that P belongs to $\mathcal{E}^\bullet(K)$. Then for all but a finite number of places v, the section P has good reduction at v*

Proof. Let us exclude all places v for which $\gamma_v(P,\tau)$ is not a unit. For the remaining places v, the conditions for P_τ to have singular reduction at v can be reformulated

by saying that the elements

$$2\,b(P) + a_1\,a(P)\,e(P)^2 + a_3\,e(P)^3 \qquad \text{and}$$
$$3\,a(P)^2 + 2\,a_2\,a(P)e(P)^2 + a_4\,e(P)^4 - a_1\,b(P)\,e(P)$$

of R lie in the maximal ideal $(\mathfrak{m}_v, \tau)$. If they both vanish along a subscheme of $\mathcal{U}$ of dimension 1, then it has to be a component of the zero locus of the discriminant Δ. This would imply that the section P encounters the singularity of a bad fibre on C which is in contradiction to the hypothesis that P belongs to $\mathcal{E}^\circ(K)$. □

We say that a section P in $\mathcal{E}^\bullet(K)$ has *good reduction everywhere* if it has good reduction for all finite places v, that is to say that P_τ belongs to $\mathcal{E}^\circ_\tau(K)$ for all τ.

Proposition V.5. *Let $\mathcal{E}$ be a family and let P be a section. If $\mathcal{E}_K$ has no fibre of multiplicative type then we find a tight cover and a multiple of P with everywhere good reduction.*

If $\mathcal{E}_K$ has multiplicative fibres we might still be lucky and there exists such a multiple, but otherwise we would have to exclude a set of arbitrary small density of $C(K)$.

Proof. We know that we can multiply P into $\mathcal{E}^\bullet(K)$. By the previous lemma, we may concentrate on a finite number of places v. For each of them we can refine the cover sufficiently to be able to apply the local lemma V.2. □

Lemma V.6. *Let P be a section of a family $\mathcal{E}$ that belongs to $\mathcal{E}^\bullet(K)$ and which has good reduction everywhere. Then P_τ belongs to $\mathcal{E}^\bullet_\tau(K)$ for all $\tau \in \mathcal{U}(\mathcal{O})$. There exists an element $\gamma(P,\tau)$ in $\mathcal{O}$, defined up to $\mathcal{O}^\times$, such that $e(P_\tau)\cdot\gamma(P,\tau) = e(P)(\tau)$.*

This together with lemma V.3 implies in particular that we may refine the tight cover in order to assure that $\gamma(P,\tau)$ is a constant on every $\mathcal{U}$, for, up to $R^\times$, the expression $\gamma(P,\tau)$ only takes finitely many values on each $\mathcal{U}$.

Proof. For the first part, note that $q(P) = q(P_\tau)$ under the isomorphism from $\mathrm{Cl}(R)$ to $\mathrm{Cl}(\mathcal{O})$. The existence of $\gamma(P,\tau)$ follows now exactly like in (V.2). □

V.2 Heights in Families

In this section, the variation of the p-adic height associated to the choice of a sigma function σ_v of Bernardi for every place above p is considered as we follow a section

in a family. For simplicity of notation, the formulae are only written for the cyclotomic $\mathbb{Z}_p$-extension rather than for a general λ. Write $h_\sigma(P)$ for the cyclotomic height associated to the sigma function of Bernardi as in (IV.9).

Fix an embedding of $\bar{K}$ into the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$.

Theorem V.7.
Let p be an odd prime and let $\mathcal{E}$ be a family of elliptic curves over a number ring $\mathcal{O}$. Suppose $P \in \mathcal{E}(K)$ is a section that has a multiple with good reduction everywhere. Then the map $\tau \mapsto h_\sigma(P_\tau)$ from $C(K)$ to $\mathbb{Q}_p$ extends to a piecewise rigid analytic function on $C(\mathbb{C}_p)$.

Proof. Choose a tight cover on C. Let Q be a section in $\mathcal{E}^\bullet(K)$ with everywhere good reduction and suppose that the cover is sufficiently fine so that $\gamma(Q,\tau) = \gamma$ is constant on each $\mathcal{U}$. See lemma V.6. Let Q be the multiple of P with good reduction everywhere. Furthermore we want that Q lies in $\mathcal{E}^\bullet(K)$ and that Q_τ belongs to the layer of the formal group $\hat{\mathcal{E}}_\tau(\mathfrak{m}_\upsilon)$ such that $\sigma_\upsilon(Q_\tau)$ converges for all $\tau \in \mathcal{U}(\mathcal{O})$ and all places υ above p. This can always be achieved by multiplying with a sufficiently large integer as $\mathcal{E}^\bullet(K)$ is of finite index and there are only finitely many different reductions at a place υ for different $\tau \in \mathcal{U}(\mathcal{O})$. Now we can calculate the p-adic height of Q_τ according to (IV.9), at least if $Q_\tau \neq O_\tau$:

$$\begin{aligned} h_\sigma(Q_\tau) &= \log_p\Big(\prod_{\upsilon|p} N_{K_\upsilon:\mathbb{Q}_p}\Big(\frac{\sigma_\upsilon(Q_\tau)}{e(Q_\tau)}\Big)\Big) \\ &= \log_p\Big(\prod_{\upsilon|p} N_{K_\upsilon:\mathbb{Q}_p}\Big(\frac{\sigma_\upsilon(Q_\tau)}{e(Q)(\tau)}\Big)\Big) + \log_p \circ N_{K:\mathbb{Q}}(\gamma), \end{aligned} \tag{V.3}$$

and since $h_\sigma(P_\tau)$ is a scalar multiple of $h_\sigma(Q_\tau)$ it suffices to prove the theorem for Q.

Let now υ be a place above p and let U^{an} be the rigid analytic space associated to U over K_υ as in [Sch98]. The rigid analytic functions on $U_0 = \mathcal{U}(\mathcal{O}_\upsilon)$ form the ring R^{an} defined to be the quotient of the Tate-algebra $K_\upsilon\langle T_1, \dots T_m\rangle$ of convergent power series by the ideal generated by the equations f_j of $\mathcal{U}$.

We know that $e(Q)$ is an element of R with no poles on U_0, so in particular it lives in R^{an}. Next we look at

$$t(Q) = -\frac{x(Q)}{y(Q)} = -\frac{a(Q)\cdot e(Q)}{b(Q)} \in K(T).$$

Since Q is in the formal group at υ for all τ in U_0, $t(Q)$ cannot have poles either and so it belongs to R^{an}.

The sigma function of Bernardi was constructed as a power series in t whose coefficients are polynomials in $a_i \in R$ of the (Weq) with rational coefficients. Hence

it is a power series in $R[\![t]\!]$. Substituting t by $t(Q)$ we get a power series $\sigma_v(Q)$ in R^{an} whose zeros are exactly the zeros of $e(Q)$. More precisely, we know that $\frac{\sigma_v(Q)}{e(Q)\cdot\gamma}$ is a unit for all τ in U_0 and so the quotient $\frac{\sigma_v(Q)}{e(Q)}$ is an element of R^{an} without poles or zeros. This shows that on $U_0 \times \mathbb{C}_p$ the function $\log N_{K_v:\mathbb{Q}_p} \frac{\sigma_v(Q)}{e(Q)}$ is an element of $R^{\mathrm{an}} \otimes \mathbb{C}_p$, and so $h(Q_\tau)$ is a finite sum of analytic functions. □

Corollary V.8. *The map $\tau \longmapsto h(P_\tau)$ has either only finitely many zeros in $C(\mathbb{C}_p)$ or it is constant zero on a p-adic open.*

Suppose $\mathcal{E}_K$ is non-split and that it is defined over $\mathbb{Q}$. If the section is non-torsion, we can almost exclude the second case: The j-invariant is non-constant and hence has a zero τ on C. With some luck this zero is a rational point of $C(\mathbb{Q})$ and hence we have a fibre $\mathcal{E}_\tau$ with complex multiplication. By a result of Bertrand [Ber82, Corrolaire 2], the value of the sigma function of Bernardi evaluated on a non-torsion point is a transcendental p-adic number. So unless we are unlucky and the section hits the fibre $\mathcal{E}_\tau$ at a torsion point, we would know that the value of $h_\sigma(P_\tau)$ is non-zero and hence it would be non-zero in a p-adic open of τ.

It is certainly necessary to illustrate the theorem V.7 with a concrete example. Let

$$\mathcal{E}: \qquad y^2 = x^3 + S\,x^2 - (1+S)\,x + 1$$

be a family over $\mathbb{Z}[S]$. As an elliptic surface $\mathcal{E}_{\mathbb{Q}} \longrightarrow \mathbb{P}^1_{\mathbb{Q}}$, it has a bad fibre at $S = \infty$ and at the irreducible divisor $(S^4 + 2\,S^3 - 5\,S^2 - 6\,S - 27)$. It has two independent sections $P = (0,1)$ and $Q = (1,1)$ such that $2P$ and $2Q$ belong to $\mathcal{E}^\bullet(\mathbb{Q})$. Now we will substitute $S = 1 + 36 \cdot T$ to concentrate on a smaller open. Here the reduction at 3 is constant good anomalous for all $\tau \in \mathbb{Z}$. It is not difficult to show that $6P$ has good reduction everywhere for $\tau \in \mathbb{Z}$. We have

$$e(6P) = 324 \cdot T^2 \cdot (12754584\,T^6 + 1889568\,T^5 + 52488\,T^4 - 8748\,T^3 - 486\,T^2 + 1).$$

The resultant of $e(6P)$ and $a(6P)$ is a power of two, but $a(6P)$ is odd for all $\tau \in \mathbb{Z}$. Hence $\gamma(6P,\tau) = 1$ for all $\tau \in \mathbb{Z}$. We see that $(6P)_\tau$ lies in the formal group at 3 for all $\tau \in \mathbb{Z}$.

The sigma function of Bernardi is equal to

$$\sigma_3 = t + \frac{1+36\,T}{3} \cdot t^3 + \frac{47952\,T^2 + 180\,T - 101}{180} \cdot t^5 + \frac{80294976\,T^3 - 5520960\,T^2 - 831816\,T - 12319}{11340} \cdot t^7 + \mathbf{O}(t)^8$$

and evaluates on $6P$ to

$$\sigma_3(6P)(\tau) = (2 \cdot 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + 2 \cdot 3^8 + 2 \cdot 3^9) \cdot \tau^2 + (3^8) \cdot \tau^4 + \mathbf{O}(3)^{10}$$

for all $\tau \in \mathbb{Z}_3$. We can compute the 3-adic height associated to the sigma function of Bernardi

$$h_\sigma(6P_\tau) = 2 \cdot 3^2 \cdot \tau^2 + (3^4 + 3^5) \cdot \tau^3 + 3^5 \cdot \tau^4 + \mathbf{O}(3)^6.$$

In particular this has a unique zero for $\tau = 0$. This is no surprise because $P_{\tau=0} = (1, 0)$ is actually a 3-torsion point on $\mathcal{E}_{\tau=0}$.

With the two section, we can hope to construct a section in $\mathcal{E}(\mathbb{Q}) \otimes \mathbb{Z}_p$ in the kernel of reduction at $p = 3$. In fact the logarithms for $\tau \in \mathbb{Z}$ are

$$z_1 = \mathscr{L}_3(6P_\tau) = 3^4 \cdot \tau^2 \cdot \left((2 + 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4) + 3^4 \cdot \tau^2 + \mathbf{O}(3)^5\right)$$
$$z_2 = \mathscr{L}_3(6Q_\tau) = 3^2 \cdot \left((2 + 2 \cdot 3^3) + (2 \cdot 3^1 + 3^3) \cdot \tau + (2 \cdot 3^2 + 2 \cdot 3^3) \cdot \tau^2 + \mathbf{O}(3)^4\right)$$

and hence z_2 has valuation 2 for all $\tau \in \mathbb{Z}_3$, while z_1 has valuation at least 4. We can conclude that $M = P - \frac{z_1}{z_2} \cdot Q$ belongs to $\mathcal{E}(\mathbb{Q}) \otimes \mathbb{Z}_p$ and for all τ in $\mathbb{Z}$, the element M_τ must belong to $\mathfrak{M}(\mathcal{E}_\tau/\mathbb{Q})$. In particular we can compute the 3-adic height of M_τ for all τ in $\mathbb{Z}$

$$h(M_\tau) = (3^4 + 2 \cdot 3^5) \cdot \tau^2 + 3^5 \cdot \tau^3 + 3^6 \cdot \tau^4 + \mathbf{O}(3)^7.$$

Once again, we can deduce that the height is non-zero for all $\tau \neq 0$. In fact $M_{\tau=0} = O$. We conclude that the 3-adic height on $\mathfrak{M}(\mathcal{E}_\tau/\mathbb{Q})$ is non-degenerate for all $\tau \in \mathbb{Z}$ for which the rank of $\mathcal{E}_\tau(\mathbb{Q})$ is 2.

The rank of the elliptic surface is 2, probably generated by P and Q. For each τ in $\mathbb{Z}$, except a finite number (like $\tau = 0$) the rank of the fibre $\mathcal{E}_\tau(\mathbb{Q})$ is at least 2, by Silverman's specialisation theorem. It is expected that the average of the rank is about $2 + \frac{1}{2}$.

Theorem V.9.
Let $\mathcal{E}$ be a family over a number ring $\mathcal{O}$. Suppose $\{P^{(1)}, \dots P^{(r)}\}$ is a set of sections of $\mathcal{E}$, all having a multiple with everywhere good reduction. Let $\mathfrak{N}$ be the kernel of reduction from $\mathbb{Z}_p P^{(1)} \oplus \cdots \oplus \mathbb{Z}_p P^{(r)}$ to $\oplus_{v|p} \mathcal{E}(K_v)^\star$ for all places v above p. Then the regulator of $\mathfrak{N}_\tau$ is a piecewise rigid analytic function on $C(\mathbb{C}_p)$.

Proof. The v-adic logarithm map $\mathscr{L}_v$ is a power series in $R[\![t]\!]$ and hence $\mathscr{L}_v(P_\tau)$ is rigid analytic on the U_0 of the proof of the previous theorem. We can refine the cover in order to find analytic expressions $\alpha_i^{(j)}(\tau)$ such that

$$M_\tau^{(j)} = \alpha_1^{(j)}(\tau) \cdot P_\tau^{(i)} + \cdots + \alpha_r^{(j)}(\tau) \cdot P_\tau^{(r)}$$

belongs to $\mathfrak{N}_\tau$ for all τ in U_0 and they form a $\mathbb{Z}_p$-basis of $\mathfrak{N}_\tau$ on U_0. The result follows now from the previous theorem. □

Chapter VI

Numerical Computations

> The Aleph's diameter must have been about two or three centimetres, but Cosmic Space was in it, without diminution of size. Each object (the mirror's glass, for instance) was infinite objects, for I clearly saw it from all points in the universe.
> The Aleph; Jorge Luis Borges.

This chapter contains the explanation and results of the numerical calculations done on the fine Mordell-Weil group. Throughout the whole chapter $E/\mathbb{Q}$ is an elliptic curve and p an odd prime. We assume that the fine Tate-Shafarevich group $Ш(E/\mathbb{Q})(p)$ is finite. It is actually conjecturally trivial for all examples considered.

VI.1 The algorithms

VI.1.1 The height pairing

Suppose that the rank r of the Mordell-Weil group $E(\mathbb{Q})$ is strictly larger than 1.

There are essentially two ways of computing the p-adic height on the fine Mordell-Weil group. In the article of Bernardi and Perrin-Riou [BerPR93], they perform calculations of the regulator on the fine Mordell-Weil group for supersingular reduction using the limit formula

$$h(P) = \lim_{k\to\infty} \frac{-1}{2\cdot p^{2k}} \log_p\Big(a(p^k\, P)\Big)$$

where a denotes still the numerator. I suppose that the same method was used in [PR03a].

The main computational problem with this formula is that we need to multiply the point P with p^k which, if p is large, can be very long and complicated. Instead, it is

easier to actually calculate the sigma function of Bernardi directly, using the built-in Weierstrass $\wp$-function in `pari` [pari].

Lemma VI.1. *Define B to be the intersection of $E(\mathbb{Q})$ with $\widehat{E}(p\mathbb{Z}_p)$. The fine Mordell-Weil group $\mathfrak{M}$ is isomorphic to the kernel of the localisation map from $B \otimes \mathbb{Z}_p$ to $\widehat{E}(p\mathbb{Z}_p)$.*

Proof. If we denote as usual by $\Phi(\mathbb{Q}_p)$ the group of components and by $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ the non-singular points in the reduction, we have two exact sequences

$$\begin{aligned} 0 \longrightarrow \widehat{E}(p\mathbb{Z}_p) \longrightarrow E^\circ(\mathbb{Q}_p)^\star \longrightarrow \tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)(p) \longrightarrow 0 \\ 0 \longrightarrow E^\circ(\mathbb{Q}_p)^\star \longrightarrow E(\mathbb{Q}_p)^\star \longrightarrow \Phi(\mathbb{Q}_p)(p) \longrightarrow 0 \end{aligned} \tag{VI.1}$$

Hence the subgroup B has index prime to p in the kernel of the map from $E(\mathbb{Q})$ to $E(\mathbb{Q}_p)^\star$. □

Let Q_1, Q_2,... Q_r be a basis of B. Denote by $\mathscr{L}_p$ the p-adic elliptic logarithm converging on the whole of the formal group and giving us an isomorphism with $p\mathbb{Z}_p$. We conclude that

$$\mathfrak{M} = \{x_1 Q_1 + \cdots + x_r Q_r \mid x_i \in \mathbb{Z}_p \quad \text{such that} \quad x_1 \mathscr{L}_p(Q_1) + \cdots + x_r \mathscr{L}_p(Q_r) = 0\}$$

The first step is therefore to compute a $\mathbb{Z}$-basis of B. If we start with a basis $\{P_i\}$ of $E(\mathbb{Q})$ modulo torsion with relatively small real-valued height, we can find $\mathbb{Z}$-linear combinations of the P_i that lie in B. Once we have found sufficiently many to generate B, a reduction using the LLL-algorithm, permits us to find a basis of B with relatively small real-valued height. In this way, the computation that follow are faster.

Now it is easy to compute the matrix of the bilinear form on $B \otimes \mathbb{Z}_p$ with respect to the sigma function of Bernardi. But it is important to make sure that the points in the basis are multiplied so that they have good reduction at all places. Once a $\mathbb{Z}_p$-basis of $\mathfrak{M}$ (in the presentation above) is found using $\mathscr{L}_p$, the determinant of the pairing restricted to $\mathfrak{M}$ can be computed. Its valuation is independent of all choices, it is the well-defined valuation of the (cyclotomic) regulator on $\mathfrak{M}$.

VI.1.2 The index of $\mathfrak{M}_\Sigma$ in $\mathfrak{M}$

Although it is not needed directly anymore in the final formula of the Euler characteristic, it can still be interesting to compute the index of $\mathfrak{M}_\Sigma$ in $\mathfrak{M}$; under our

assumptions this is the same as the index of $\mathfrak{R}_\Sigma$ in $\mathfrak{R}$. The easiest choice for Σ is as the union of the bad places, $\{\infty\}$ and $\{p\}$. By definition

$$0 \longrightarrow \mathfrak{M}_\Sigma \longrightarrow \mathfrak{M} \longrightarrow \bigoplus_{v\in\Sigma(\nmid p)} E(\mathbb{Q}_v)^\star$$

The target of the localisation map has order

$$c = \prod_{\text{bad } v\neq p} c_v^{(p)} \cdot N_v^{(p)}$$

where c_v is the Tamagawa number at v and N_v is the number of non-singular points in the reduction. This product c, which is a power of p, is quite often equal to 1.

Otherwise, find a basis M_i of $\mathfrak{M}$ expressed as $\mathbb{Z}_p$-combinations of the basis $\{Q_j\}$ of B, say $M_i = \sum m_{i,j}\cdot Q_j$. Choose integers $m'_{i,j}$ that are congruent to $m_{i,j}$ modulo c. Then the points $M'_i = \sum m'_{i,j}\cdot Q_j$ in $E(\mathbb{Q})$ represent a $\mathbb{Z}/c$-basis of $\mathfrak{M}/c$. The index of $\mathfrak{M}_\Sigma$ in $\mathfrak{M}$ is the order of the image generated by points M'_i in the above localisations.

VI.1.3 Local torsion points

Sometimes we wish to compute the number of torsion points in $E(\mathbb{Q}_p)(p)$. Write the symbol $\otimes$ for the tensor product with $\mathbb{Q}_p/\mathbb{Z}_p$. The exact sequences

$$0 \longrightarrow E^\circ(\mathbb{Q}_p)(p) \longrightarrow E(\mathbb{Q}_p)(p) \longrightarrow \Phi(\mathbb{Q}_p)(p) \xrightarrow{\delta} E^\circ(\mathbb{Q}_p)\otimes \longrightarrow E(\mathbb{Q}_p)\otimes \longrightarrow 0$$
$$0 \longrightarrow E^\circ(\mathbb{Q}_p)(p) \longrightarrow \tilde{E}_{\text{ns}}(\mathbb{F}_p)(p) \xrightarrow{\delta'} \widehat{E}(p\mathbb{Z}_p)\otimes \longrightarrow E^\circ(\mathbb{Q}_p)\otimes \longrightarrow 0$$

allow us to compute the local torsion without using the division polynomial. In order to decide if, in case N_p is divisible by p, the map δ' is trivial one takes any point Q in $E^\circ(\mathbb{Q}_p)$ not in the formal group and checks if the point pQ lies in the second layer of the formal group or only in the first layer. Similarly one can check if δ is trivial in the unlucky case that p divides c_p. An example of such a calculation is given in II.2.1.

VI.1.4 The index I_0 of $\mathfrak{M}$ in $T_p\mathcal{M}$

Also this quantity does not appear in the Euler characteristic formula anymore, but we could still be interested in the order of I_0. But in fact we have here a little

Lemma VI.2. *If E has good reduction at p, or more generally if p does not divide c_p, then the natural embedding from $\mathfrak{M}$ to $T_p\mathcal{M}$ is an isomorphism.*

Proof. In proposition I.11 the bound on I_0 shows that if $E(\mathbb{Q}_p)(p)$ is trivial, then so is I_0. Hence we may assume that $E(\mathbb{Q}_p)(p)$ is equal to $\tilde{E}_{\text{ns}}(\mathbb{F}_p)(p) = \mathbb{Z}/p$, because p does

not divide c_p. (Compare with the sequences in the paragraph on the computation of the local torsion.) Consider the following diagram

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \mathfrak{M} & \longrightarrow & T_p\mathcal{M} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(\mathbb{Q})(p) & \longrightarrow & E(\mathbb{Q})^\star & \longrightarrow & T_p\Big(E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p\Big) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(\mathbb{Q}_p)(p) & \longrightarrow & E(\mathbb{Q}_p)^\star & \longrightarrow & T_p\Big(E(\mathbb{Q}_p)\otimes\mathbb{Q}_p/\mathbb{Z}_p\Big) & \longrightarrow & 0
\end{array}$$

Since the p-primary part of $\Phi(\mathbb{Q}_p)$ is trivial, there is an isomorphism in (VI.1) between $E(\mathbb{Q}_p)^\star$ and $E^\circ(\mathbb{Q}_p)^\star$. Also we see that $T_p(E(\mathbb{Q}_p)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$ is equal to $T_p(\widehat{E}(p\mathbb{Z}_p)\otimes\mathbb{Q}_p/\mathbb{Z}_p)=\widehat{E}(p\mathbb{Z}_p)$. Hence the exact sequence

$$0 \longleftarrow \tilde{E}_{\mathsf{ns}}(\mathbb{F}_p)(p) \longleftarrow E(\mathbb{Q}_p)^\star \longleftarrow \widehat{E}(p\mathbb{Z}_p) \longleftarrow 0$$

splits the bottom sequence in the diagram above. □

VI.1.5 The group $D(p)$

The group D is defined to be the cokernel of the localisation map from $E(\mathbb{Q})^\star$ to $E(\mathbb{Q}_p)^\star$. If the rank of the curve is 0, then $D(p)$ is simply the quotient of $E(\mathbb{Q}_p)(p)$ by $E(\mathbb{Q})(p)$. Suppose therefore that the rank is at least 1. Then $D=D(p)$ is finite. After the calculation of the image of $E(\mathbb{Q})$ in $\Phi(\mathbb{Q}_p)(p)$ and $\tilde{E}_{\mathsf{ns}}(\mathbb{F}_p)(p)$, we have also to look at the image of the basis of B within $\widehat{E}(p\mathbb{Z}_p)$. For instance, if the reduction is good and is not anomalous, then $d=\#D(p)$ is such that all Q_i maps into $\widehat{E}(p^{d+1}\mathbb{Z}_p)$ and at least one of them does not lie in $\widehat{E}(p^{d+2}\mathbb{Z}_p)$. The larger the rank is the less frequent there are curves and primes for which D is non-trivial.

VI.2 Examples

VI.2.1 The curves of conductor 11

It is quite traditional, if I may say so, to consider the three curve of conductor 11 as the first and standard example for Iwasawa theory of elliptic curves. Our considerations are based on the detailed description in [CoSu00] chapter 4.4 and in Greenberg's part of [cetraro99] on page 106 and on the pages 120–125. They are the following curves

$$\begin{aligned}
E_1\colon &\qquad y^2+y=x^3-x^2-10\,x-20\\
E_2\colon &\qquad y^2+y=x^3-x^2-7820\,x-263580\\
E_3\colon &\qquad y^2+y=x^3-x^2
\end{aligned}$$

labelled $11A1$, $11A2$ and $11A3$ in Cremona's tables [Cre97]. We include here a lemma that should have shown a long time ago:

Lemma VI.3. *The Tate-Shafarevich groups $Ш(E_i/\mathbb{Q})$ of E_i are trivial for all $i = 1, 2$ and 3.*

Proof. Because of the invariance of the Birch and Swinnerton-Dyer formula under isogeny, it is enough to prove it for $E = E_1$. A 2-descent, using Cremona's `mwrank`, and a 3-descent, using Stoll's `magma` script [ScSt04], prove the statement for the 2-primary and the 3-primary part of $Ш(E/\mathbb{Q})$. For $p = 5$ the triviality of $Ш(E/\mathbb{Q})(p)$ is proven by Fisher in [Fis01]. Now let $K = \mathbb{Q}(\sqrt{-7})$ and write $\alpha = \frac{-1+\sqrt{-7}}{2}$. We profit from the `pari` program of Green [Gre] to compute the Heegner point

$$y_K = (1 + \alpha, 4 \cdot \alpha)$$

associated to the maximal order in K. It has good reduction at all places and the real-valued height of y_K proves that it is not of finite order. Hence $E(K)$ has rank 1 by Kolyvagin's result, stated in [Gro91]. Next, we check that the point y_K is actually a generator of $E(K)$ modulo its torsion part $E(K)_{\text{tors}} = \mathbb{Z}/5 \cdot (5, 5)$. Hence $Ш(E/K)$ has trivial p-part for all odd p such that $\rho\colon \mathrm{Gal}(\mathbb{Q}(E[p]):\mathbb{Q}) \longrightarrow \mathrm{Gl}_2(\mathbb{F}_p)$ is surjective, i.e all but $p = 5$ according to 5.5.2 in [Ser72]. A little descent argument shows that the p-primary part of $Ш(E/\mathbb{Q})$ injects into $Ш(E/K)$ for all primes but $p = 2$. □

Proposition VI.4. *The fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ of E_i over $_\infty\mathbb{Q}$ is finite for all odd primes and $i = 1, 2$ or 3.*

Proof. For all odd primes $p \neq 5$ with good and ordinary reduction, the classical Selmer group is trivial over $_\infty\mathbb{Q}$ (see example after lemma 5.3 in [cetraro99] or theorem 4.6 in [CoSu00]), hence so is $_\infty\mathcal{R}$. For all primes with good, but supersingular reduction, we know from corollary II.5 that

$$\#J_0 \cdot \chi(\mathcal{R}) = \frac{\#E(\mathbb{Q}_p)(p) \cdot \prod_{v \neq p} c_v^{(p)}}{\#E(\mathbb{Q})(p)}.$$

Because neither c_v nor N_p can be divisible by p in this case, the right hand side is trivial and hence the Euler characteristic as well as the mysterious index J_0 are both trivial. This implies that $f_\mathcal{R}$ is a unit and hence, that $_\infty\mathcal{R}$ is finite.

So we are left with two primes, 5 and 11. The curves all have bad reduction at 11 of multiplicative type, so there is no 11-torsion point on $E_i(\mathbb{Q}_{11})$. The product

of the Tamagawa factors is either 5 or 1, so the bound (in the case of multiplicative reduction) gives once again that the Euler characteristic vanishes for $p = 11$.

Finally we come to $p = 5$. For E_3, the classical Selmer group is trivial over ${}_\infty\mathbb{Q}$, so it has to be the same for ${}_\infty\mathcal{R}$. The curve E_2 has no 5-torsion over $\mathbb{Q}_5$ and the product of the Tamagawa number is 1, so the above bound shows that the Euler characteristic is trivial. The curve E_1 is more problematic, as here the above bound is 5, because there are 5 torsion points over $\mathbb{Q}_5$ and $\mathbb{Q}$ and the Tamagawa number c_{11} equals 5. In fact the classical Selmer group is dual to the Λ-module $\Lambda/(5) = \mathbb{Z}/5[\![T]\!]$. (See [cetraro99] on page 121.) Since the characteristic series of ${}_\infty\mathcal{R}$ has to divide the one of the classical Selmer group, it is either 5 or 1. In the first case, the μ-invariant of the dual of ${}_\infty\mathcal{R}$ would be non-zero and this contradicts corollary 3.5 in [CoSu]. Therefore ${}_\infty\mathcal{R}$ is trivial and J_0 has 5 elements. A summary of the calculations for $p = 5$ is given in the following table. □

Curve	N_5	$\prod c_v$	$E(\mathbb{Q}_5)(5)$	$\#E(\mathbb{Q})$	$\chi(\mathcal{S})$	$\chi(\mathcal{R})$	$\#J_0$
E_1	5	5	5	5	5	1	5
E_2	5	1	1	1	5^2	1	1
E_3	5	1	5	5	1	1	1

VI.2.2 The curves of conductor 294

Another example is given by the two curves

$$E_1: \qquad y^2 + xy = x^3 - x - 1$$
$$E_2: \qquad y^2 + xy = x^3 - 141x + 657$$

both of conductor 294 with label $B1$ and $B2$ in Cremona's tables. The work done for the classical Selmer group, as in [CoSu00, 4.10], proves already that the fine Selmer group ${}_\infty\mathcal{S}$ is trivial for all primes but 3, assuming the Tate-Shafarevich group is trivial as expected. The bound from the Euler characteristic shows that it is also finite for $p = 3$. Note that for E_2 and $p = 7$, we must have that $\#J_0 = 7^2$.

VI.2.3 The curve of conductor 37

The curve of smallest conductor with rank 1 is given by

$$E: \qquad y^2 + y = x^3 - x. \tag{VI.2}$$

It is of conductor 37. There are no global torsion points, but the point $P = (0, 0)$ generates the Mordell-Weil group $E(\mathbb{Q}) = \mathbb{Z}P$. The only bad place 37 has reduction of type I_1, so the product of the Tamagawa numbers is 1. It is not hard to show that

Lemma VI.5. *$Ш(E/\mathbb{Q})$ is trivial.*

Proof. (One should consult Zagier's extensive discussion of this curve in [Zag85].) Let K be the field $\mathbb{Q}(\sqrt{-7})$. The Heegner point y_K equals $(0,0)$ which is the generator $E(\mathbb{Q})$ and of $E(K)$. Hence by Kolyvagin's result (theorem 1.3 in [Gro91]) the p-primary part of $Ш(E/K)$ is trivial for all primes $p \neq 2$. We used here Serre's description in 5.5.6 of [Ser72] that the Galois group of the extension obtained by adjoining the p-torsion points is isomorphic to $\mathrm{Gl}_2(\mathbb{F}_p)$ for all primes. This implies the result for $p \neq 2$. For the remaining prime $p = 2$, the program `mwrank` shows that $Ш(E/\mathbb{Q})[2] = 0$. □

For the prime $p = 37$, the bound gives that the Euler characteristic of $\widehat{{}_\infty\mathcal{R}}$ is trivial and so ${}_\infty\mathcal{R}$ must have corank 1 and the fine Tate-Shafarevich $Ш(E/{}_\infty\mathbb{Q})$ is finite.

Let now p be an odd prime different from 37. Then

$$\#J_0 \cdot \chi(\mathcal{R}) = \#D(p) = \#D$$

where D is the cokernel of the localisation $E(\mathbb{Q})^\star$ to $E(\mathbb{Q}_p)^\star$. Since the generator P is integral, the reduction from $E(\mathbb{Q})^\star$ to $\tilde{E}(\mathbb{F}_p)(p)$ is always surjective. Let Q be the first multiple of P that belongs to the formal group $\widehat{E}(p\mathbb{Z}_p)$. So in fact, $\#D$ equals the 1 if the point Q does not belong to the second layer $\widehat{E}(p^2\mathbb{Z}_p)$. Otherwise it equals $\#D = \mathrm{ord}_p(e(Q)) - 1$.

For primes smaller than 1000 it happens only for $p = 179$ and $p = 593$ that D is not trivial. For both these exceptional cases the order of D equals p. Hence for all other primes, the Euler characteristic of $\widehat{{}_\infty\mathcal{R}}$ is trivial.

We shall concentrate now on the case $p = 179$ (the case $p = 593$ can be treated in exactly the same way). The first point to lie in the formal group is $Q = 81\,P$. It has denominator $e(Q)$ exactly divisible by 179^2. Hence $\#J_0 \cdot \chi(\mathcal{R}) = p$.

The question arises if it is the Euler characteristic that is non-trivial or J_0. Since E has good and ordinary reduction at p, we can calculate the Euler characteristic formula of the classical Selmer group $\widehat{{}_\infty\mathcal{S}}$ using the canonical p-adic height of P stated in (1) in the introduction. (See for instance [PR93a].) We find

$$\hat{h}_{179}(P) = 2 \cdot 179 + 159 \cdot 179^2 + \mathbf{O}(179)^3$$

for the canonical 179-adic height of P. This can be used to show that the Euler characteristic $\chi(\mathcal{S})$ of the dual of ${}_\infty\mathcal{S}$ is trivial. This proves that the Euler characteristic of $\widehat{{}_\infty\mathcal{R}}$ must be trivial, too. Hence J_0 has p elements. Now we have a look at the diagram (I.42). It shows that the group J_0 maps to the dual of T_{loc}. We know here

by the bound in lemma I.12 that the group T_{loc} is trivial, since the number of points in the reduction $N_{179} = 162$ is not divisible by p. Therefore the group J_0 equals the kernel $\ker(d)$. Therefore we have found an example where the map d is not an isomorphism. Neither is the map from ${}_\infty\mathcal{R}_\Gamma$ to the dual of $\check{\mathfrak{R}}_\Sigma = 0$. By the control theorem I.15, the group $\mathcal{R}(E/\mathbb{Q}) = D = \mathbb{Z}/p$ injects into ${}_\infty\mathcal{R}^\Gamma \cong \mathbb{Z}/p$ and ${}_\infty\mathcal{R}_\Gamma = \mathbb{Z}/p$.

Proposition VI.6. *Let E be the curve* (VI.2) *of conductor* 37. *For any odd prime $p < 1000$ the fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ and $Ш(E/_\infty\mathbb{Q})$ are finite. The group J_0 is trivial except for the cases $p = 179$ and $p = 593$ when it has order p.*

VI.2.4 The curve of conductor 389

The curve

$$E: \qquad y^2 + y = x^3 + x^2 - 2x$$

has conductor 389 and rank 2. The Mordell-Weil group is generated by $P_1 = (0,0)$ and $P_2 = (1,0)$. The only bad reduction is at 389 with $c_{389} = 1$. Since there are two generators here, the image of the map $E(\mathbb{Q})^\star$ into $E(\mathbb{Q}_p)^\star$ is large and we do not expect that the index D is ever non-trivial for this curve. In fact for primes up to 1000 we could not find any. The Tate-Shafarevich should be trivial; we are going to assume this. Hence in the formula of the Euler characteristic in theorem II.4, the only term that could give a non-trivial bound is the regulator. The only primes below 1000 such that the regulator has valuation larger than 1 are $p = 41$ and $p = 167$. In both cases the valuation is 2. For these good ordinary and non-anomalous primes we can compute the canonical p-adic height on the classical Selmer group: $20 \cdot 41^2 + \mathbf{O}(41)^3$ and $153 \cdot 167^2 + \mathbf{O}(167)^3$ respectively. Hence the fine Selmer group must have trivial Euler-characteristic as well.

Proposition VI.7. *Let E be the curve* (VI.2.4) *of conductor* 389. *Suppose that $Ш(E/\mathbb{Q})$ is trivial. For any odd prime $p < 1000$ the fine Selmer group $\mathcal{R}(E/_\infty\mathbb{Q})$ has corank 1 and $Ш(E/_\infty\mathbb{Q})$ is finite. The J_0 is trivial except if $p = 41$ or $p = 167$ when it has order p.*

VI.2.5 Another example

Until now all the example show how to conclude for all considered primes p that the Euler characteristic of the fine Selmer group is trivial. Here now an example in

which we are unable to decide if it so. Let

$$E: \qquad y^2 + x\,y = x^2 - x^2 - 4\,x + 4$$

be the elliptic curve named $446D$ in the tables of Cremona and let $p = 5$. The curve has good anomalous reduction at p, the Tamagawa numbers are $c_{223} = 1$ and $c_2 = 2$. The localisation map is surjective and so D is trivial. We suppose that the Tate-Shafarevich group has trivial 5-primary part. There are no 5-torsion points on the curve defined over $\mathbb{Q}$. The regulator of the fine Selmer group has valuation 2 and so we know that $\#J_0 \cdot \chi(\mathcal{R})$ has valuation 1. As before, we look at the canonical regulator on the classical Selmer group, it equals $2 \cdot 5 + \mathbf{O}(5)^2$ and so the Euler characteristic of the classical Selmer group has valuation 1. Unfortunately this does not allow us to decide if J_0 or $\chi(\mathcal{R})$ is trivial. Maybe a 2-descent over ${}_1\mathbb{Q}$ could help.

VI.3 A non-trivial Euler characteristic

So far, we did not encounter an example of a non-trivial Euler characteristic for the fine Selmer group. It would be tempting to make a conjecture that not only the μ-invariant is trivial (conjecture A of Coates and Sujatha in [CoSu]) but that also the λ-invariant is trivial, i.e. the Euler characteristic is trivial.

After some search, we finally found a non-trivial Euler characteristic. But it is the only example that we found so far.

Let E be the elliptic curve

$$y^2 = x^3 + x^2 - 18\,x + 25$$

of conductor 5692. No torsion points are rational over $\mathbb{Q}$ and the Mordell-Weil group has rank 2 generated by the points $P_1 = (0, 5)$ and $P_2 = (1, 3)$. The reduction at 2 is of type IV with 3 components and for 1423 the reduction is of type I_1. At $p = 3$ the reduction is good ordinary and anomalous with $N_3 = 6$. The regulator on the fine Selmer group is extremely large; it has valuation 5. We find that $\#J_0 \cdot \chi(\mathcal{R})$ has valuation 6. There is no hope that we can bound the Euler characteristic via the calculations of the classical Selmer group either, for its canonical regulator is $2 \cdot 3^3 + 2 \cdot 3^5 + \mathbf{O}(3)^6$ and its Euler characteristic $\chi(\mathcal{S})$ is equal to 3^3. The analytic order of $Ш(E/\mathbb{Q})$ is 1, but we have been unable to prove that its 3-primary part is indeed trivial.

Proposition VI.8. *If the 3-primary part of $Ш(E/\mathbb{Q})$ is trivial, then the characteristic power series of the dual of $\mathcal{R}(E/_\infty\mathbb{Q})$ for $p = 3$ is divisible by $\omega_1 = T \cdot (3 + 3T + T^2)$.*

Proof. Let $K = {}_1\mathbb{Q}$ be the first layer of the cyclotomic $\mathbb{Z}_3$-extension. It can be generated by an element α with minimal polynomial $\alpha^3 - 3\cdot\alpha + 1 = 0$. The ring of integers $\mathcal{O} = \mathbb{Z}[\alpha]$ has class number 1. With some luck, we were able to find six independent points in $E(K)$, namely

$$\begin{aligned}
P_3 &= \quad (-\alpha^2 - 2\cdot\alpha + 2, -3\cdot\alpha^2 - 3\cdot\alpha + 4),\\
P_4 &= \quad (-\alpha^2 - 2\cdot\alpha + 3, -2\cdot\alpha^2 - 2\cdot\alpha),\\
P_5 &= (-2\cdot\alpha^2 - 3\cdot\alpha + 4, -\alpha^2 + 2,),\\
P_6 &= (-2\cdot\alpha^2 - 2\cdot\alpha + 6, -2\cdot\alpha^2 + 2\cdot\alpha + 9).
\end{aligned}$$

The real-valued height regulator of these points together with P_1 and P_2 is equal to 62.0642480 and so the rank of $E(K)$ is at least 6. The characteristic series of the classical Selmer group must therefore be divisible by $T^2\cdot(3+3T+T^2)^2$. The points P_1, P_2 and P_3 generate in the localisation $E(K_\mathfrak{p})^\star$ at the unique prime $\mathfrak{p} = (\alpha+1)$ above 3 a subgroup of rank 3. Therefore the fine Selmer group $\mathcal{R}(E/K)$ has rank at least 3 and the proposition follows. □

We are unable at present to determine completely the characteristic series. The `pari` script of Simon [Sim02] calculates the rank of $E(K)$ via 2-descent to be 6. Also the Dokchitser brothers have computed the complex L-series for me. $L(E/K,s)$ vanishes of order 6 at $s=1$ and the first coefficient is equal to 1122.8376. So the polynomial $(3+3T+T^2)$ divides $f_\mathcal{S}$ only twice and $f_\mathcal{R}$ only once. According to conjecture 1.11 in [cetraro99] on page 58, the μ-invariant of the Selmer group should be trivial. This would mean that there is another distinguished polynomial in the series $f_\mathcal{S}$.

VI.3.1 Further descent calculations

Encouraged by the above example, we tried to compute some more 2-descents over the first layer of the cyclotomic $\mathbb{Z}_3$-extension K. In the tables VI.5, we will come across a certain number of examples for which the bounds on the Euler characteristic $\chi(\mathcal{R})$ do not permit us to conclude that it is trivial. In these cases it might be interesting to see if the rank grows at the first step of the $\mathbb{Z}_3$-extension like in the previous example. In all the examples we used the nice program of Simon [Sim02]. As in the tables at the end, $\flat$ means that the reduction at $p=3$ is bad, $\natural$ stands for supersingular reduction and when the reduction is anomalous the sign $\blacklozenge$ will indicate it.

In some examples the order of the Selmer group was determined but no points were found. Together with the information that the rank of $E(K)$ must have the

same parity as the rank of $E(\mathbb{Q})$, we are able to give a choice between two values. There were three curve where we were unable to determine the 2-Selmer group. For any other example the rank of the Mordell-Weil group grows by at most 2 and hence the rank of the fine Mordell-Weil group does not grow. We add also the value of the Euler characteristic of the Selmer group $\chi(\mathcal{S})$ to the table. There are four curves for which we can conclude that the characteristic power series $f_{\mathcal{S}}$ of the Selmer group is the product of $\frac{\omega_1}{T}$ and T^r, where r is the rank of $E(\mathbb{Q})$. In these cases we deduce that the fine Selmer group has trivial Euler characteristic. In the list we added a "ω_1" to it.

Table VI.1: Descent calculations over ${}_1\mathbb{Q}$

N	curve	$\operatorname{rank} E(\mathbb{Q})$	$\operatorname{rank} E(K)$		$\chi(\mathcal{S})$
53A	[1,-1,1,0,0]	1	1	♮	
91B	[0,1,1,-7,5]	1	3	♪	2
92B	[0,0,0,-1,1]	1	1	♮	
123B	[0,-1,1,1,-1]	1	1	♭	
142A	[1,-1,1,-12,15]	1	1	♮	
153B	[0,0,1,6,27]	1	1	♭	
156A	[0,-1,0,-5,6]	1	1 or 3	♭	
171B	[0,0,1,6,0]	1	1	♭	
189A	[0,0,1,-3,0]	1	1	♭	
189B	[0,0,1,-24,45]	1	1	♭	
207A	[1,-1,1,-5,20]	1	1	♭	
215A	[0,0,1,-8,-12]	1	1	♮	
219B	[0,1,1,3,2]	1	1	♭	
220A	[0,1,0,-45,100]	1	3	♪	2
225E	[0,0,1,-75,256]	1	1	♭	
226A	[1,0,0,-5,1]	1	3	♪	1 ω_1
446D	[1, -1, 0, -4, 4]	2	2	♮	
794A	[1,0,1,-3,2]	2	2 or 4	♪	2
817A	[0,1,1,1,6]	2	2 or 4	♪	1
944E	[0,0,0,-19,34]	2	2	♮	
1028A	[0,1,0,-10,9]	2	4	♪	1 ω_1
1034A	[1,0,1,-12,14]	2	4	♪	1 ω_1
1132A	[0,1,0,-5,4]	2	4	♪	1 ω_1
1143C	[0,0,1,-3,90]	2	¿	♭	

N	curve	$\operatorname{rank} E(\mathbb{Q})$	$\operatorname{rank} E(K)$		$\chi(Ш)$
1171A	[1,-1,1,-3,0]	2	2	♮	
1446A	[1,1,0,-4,4]	2	2	♭	
1480A	[0,0,0,-28,52]	2	2	♮	
1613A	[0,1,1,-3,0]	2	4	♪	3
1701J	[0,0,1,-27,56]	2	2	♭	
1712D	[0,-1,0,0,16]	2	4		$1\ \omega_1$
1746B	[1,-1,0,-24,44]	2	¿	♭	
1907A	[1,-1,1,-46,130]	2	2	♮	
1917C	[1,-1,1,-41,110]	2	2	♭	
1933A	[1,0,0,1,-2]	2	¿	♪	1
5077A	[0,0,1,-7,6]	3	3	♮	
13766A	[1,0,1,-23,42]	3	3 or 5	♪	1
18562C	[1,0,1,-20,30]	3	3 or 5	♪	1

VI.4 Conjectures

It was already explained earlier in I.7 that there is a widely believed conjecture called the weak Leopoldt conjecture. It is a consequence of the non-degeneracy of the height pairing on the fine Selmer group. As described in I.11, it should hold even if the height is degenerate.

Conjecture VI.9. *Let A/K be an abelian variety and ${}_\infty K$ an arbitrary $\mathbb{Z}_p$-extension of K. It should be true that the dual of the fine Selmer group $\mathcal{R}(A/{}_\infty K)$ is Λ-torsion.*

If $A = E$ is an elliptic curve, K is an abelian extension of $\mathbb{Q}$ and the extension is the cyclotomic extension, the conjecture is verified thanks to the work of Kato [Kat00]. If K is an imaginary quadratic extension of $\mathbb{Q}$ and ${}_\infty K$ is the anti-cyclotomic extension, then it is a consequence of the work of Bertolini-Darmon, Cornut-Vatsal,...

VI.4.1 The growth of the fine Mordell-Weil group

The conjecture implies that the fine Mordell-Weil group $\mathcal{M}(A/{}_\infty K)$ is finitely generated, so we should consider the growth of the rank of the Mordell-Weil group.

Let E/K be an elliptic curve. Assume first that the base-field is simply $\mathbb{Q}$. In this case, the rank of the fine Mordell-Weil group $\mathcal{M}(E/\mathbb{Q})$ is simply $r-1$ if the rank r of the Mordell-Weil group is positive and zero otherwise. This is because the target $E(\mathbb{Q}_p)^\star$ is of $\mathbb{Z}_p$-rank 1 and a multiple of a point of infinite order of $E(\mathbb{Q})$ maps into

the formal group, and hence to a non-zero point in $E(\mathbb{Q}_p)^\star$.

Is there an easy generalisation of this ? Something like the classical Leopoldt conjecture for the p-adically completed group of units in an number field ?

The fine Mordell-Weil group was defined to be

$$0 \longrightarrow \mathfrak{M}(E/K) \longrightarrow E(K) \otimes \mathbb{Z}_p \longrightarrow \oplus_{v|p} E(K_v)^\star.$$

The target of the localisation map has $\mathbb{Z}_p$-rank equal to the degree of the extension $[K : \mathbb{Q}]$. Hence we have the obvious, but very weak inequalities $\operatorname{rank} \mathfrak{M}(E/K) \geqslant 0$ and

$$\max\{\operatorname{rank} E(K) - 1, 0\} \geqslant \operatorname{rank} \mathfrak{M}(E/K) \geqslant \operatorname{rank} E(K) - [K : \mathbb{Q}].$$

See [Jon95, Proposition 7.1].

In $\mathbb{Z}_p$-extensions we can say something more. Assume that the Tate-Shafarevich groups $Ш(E/_nK)$ are all finite and assume first that the dual of ${}_\infty\mathcal{S}$ is Λ-torsion and "semi-simple at all roots of unities". If E has good and ordinary reduction at p, we could ask for the canonical p-adic height on $E({}_nK)$ to be non-degenerate for all n. Then of course, both, $E({}_\infty K)$ and $\mathfrak{M}({}_\infty K)$, are of finite rank.

The rank of $\mathfrak{M}(E/_nK)$ is the rank of $\widehat{{}_\infty\mathcal{R}}/(\omega_n)$ with $\omega_n = (1+T)^{p^n} - 1$. Similar the rank of the whole Mordell-Weil group is the rank of $\widehat{{}_\infty\mathcal{S}}/(\omega_n)$. Write the characteristic series of $\widehat{{}_\infty\mathcal{S}}$ as

$$f_{\mathcal{S}} = h \cdot T^{r_0} \cdot \left(\frac{\omega_1}{T}\right)^{r_1} \cdot \left(\frac{\omega_2}{\omega_1}\right)^{r_2} \cdots$$

for some element $h \in \Lambda$ prime to any of the following factors. The rank of $E(K)$ is r_0 and the rank of $E({}_nK)$ is equal to the sum of the rank of $E({}_{(n-1)}K)$ and $(p^n - p^{n-1}) \cdot r_n$. If the rank jumps up by more than $(p^n - p^{n-1}) \cdot d$ with $d = [K : \mathbb{Q}]$, which is the difference in the rank of the target of the localisation map, then the rank of $\mathfrak{M}$ has to jump up as well by at least $(p^n - p^{n-1}) \cdot (r_n - d)$. Hence we conclude that the characteristic series of the dual of ${}_\infty\mathcal{R}$ has to be divisible by

$$T^{\max\{0,r_0-d\}} \cdot \left(\frac{\omega_1}{T}\right)^{\max\{0,r_1-d\}} \cdot \left(\frac{\omega_2}{\omega_1}\right)^{\max\{0,r_2-d\}} \cdots$$

If the ground field K is $\mathbb{Q}$, then we see that if the rank of the Mordell-Weil group jumps up by some amount, there is a new point P in $E({}_n\mathbb{Q})$ which is not defined over ${}_{(n-1)}\mathbb{Q}$. In the localisation $E({}_n\mathbb{Q}_p)^\star$ at the unique prime above p, the point P can not belong to the image of the localisation from $E({}_{(n-1)}\mathbb{Q})^\star$. Therefore the rank of the fine Mordell-Weil group jumps up if and only if the rank of the Mordell-Weil grows by more than $p^n - p^{n-1}$. Hence we have shown the

Proposition VI.10. *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Suppose that the p-adic height pairing on $E({}_n\mathbb{Q})$ is non-degenerate for all n and that*

the Tate-Shafarevich group $Ш(E/_n\mathbb{Q})(p)$ is finite for all n. Then the characteristic power series of the dual of the fine Selmer group ${}_\infty\mathcal{R}$ is of the form

$$f_{\mathcal{R}} = h' \cdot T^{\max\{0,r_0-1\}} \cdot \left(\frac{\omega_1}{T}\right)^{\max\{0,r_1-1\}} \cdot \left(\frac{\omega_2}{\omega_1}\right)^{\max\{0,r_2-1\}} \cdots$$

for some $h' \in \Lambda$ prime to the following factors. Here the r_i are the powers with which these factors appear in the characteristic series of the dual of the classical Selmer group ${}_\infty\mathcal{S}$.

In other words the quotient of the two characteristic series is exactly once divisible by the polynomials $\frac{\omega_n}{\omega_{n-1}}$ that appear in the series for the Selmer group ${}_\infty\mathcal{S}$.

Next, we wish to consider the case when the Selmer group is not Λ-torsion; the Tate-Shafarevich is still assumed to be finite for all n. We know that the rank of the Mordell-Weil group grows at worst like $\operatorname{rank}_\Lambda(\widehat{{}_\infty\mathcal{S}}) \cdot p^n + \mathbf{O}(1)$. If the $\mathbb{Z}_p$-extension is cyclotomic, it is conjectured (see conjecture 1.8 in [cetraro99] on page 57) that the Mordell-Weil group is finitely generated over ${}_\infty K$ even if the Selmer group is not Λ-torsion (as it can happen for supersingular primes). As noted before, the target of the localisation map grows like $[K:\mathbb{Q}] \cdot p^n$. Hence if the Λ-rank of the dual of ${}_\infty\mathcal{S}$ is less than the degree of K, we would expect once again that the rank of the fine Selmer group is bounded.

The only situation in which something more is known about the growth of the Mordell-Weil group $E({}_nK)$ is the anti-cyclotomic $\mathbb{Z}_p$-extension ${}_\infty K$ above an imaginary number field K. Again, we suppose that E does not have an order of K as its endomorphism ring. Due to the work of Bertolini-Darmon, Cornut-Vatsal,... it is proven that the Λ-rank of ${}_\infty\mathcal{S}$ is 1 and the rank of the Mordell-Weil group grows like $p^n + \mathbf{O}(1)$. See [Ber01, Theorem 5.3]. But the same theorem also states that the rank of the image in the localisation has the same speed of growing, or in other words that the fine Mordell-Weil group $\mathfrak{M}(E/_nK)$ has bounded rank. Actually we even know that the weak Leopoldt conjecture holds.

Somewhat cheeky maybe is the following more general question based on the explanations above.

Question VI.11. *Is it true that the rank of the fine Mordell-Weil group of an elliptic curve only grows in a Galois extension $L:K$ of number fields if the rank of the Mordell-Weil group increases by more than the growth $[L:\mathbb{Q}] - [K:\mathbb{Q}]$ of the degree ?*

VI.4.2 The growth of the fine Tate-Shafarevich group

We assume that the weak Leopoldt conjecture holds and that the $\mathbb{Z}_p$-extension is cyclotomic. Concerning the Iwasawa-invariants of the dual of ${}_\infty\mathcal{R}$ there is a first conjecture due to Coates and Sujatha [CoSu]

Conjecture VI.12. *Let E/K be an elliptic curve, then the μ-invariant of the dual of the fine Selmer group $\mathcal{R}(E/_\infty K)$ should be zero for the cyclotomic $\mathbb{Z}_p$-extension.*

Based on the theorem of Ferrero and Washington, they prove it when the field K is abelian over $\mathbb{Q}$ and there is a p-torsion point defined over K. In the complete calculations presented in the tables in section VI.5, we could not find a counter-example to the conjecture and this provides therefore quite good numerical evidence in support of this conjecture. The conjecture is equivalent to the statement that ${}_\infty\mathcal{R}$ is $\mathbb{Z}_p$-cofree.

Another reason to believe in this conjecture is the analogy with the function field case as explained in the introduction.

We may ask further questions about the structure of ${}_\infty\mathcal{R}$. The very few examples of non-trivial Euler characteristic suggest that one could ask the following question

Question VI.13. *Is it possible that the fine Tate-Shafarevich $Ш(E/_\infty K)(p)$ is infinite over the cyclotomic $\mathbb{Z}_p$-extension for some E and p ?*

Of course, a negative answer includes already the conjecture that the fine Tate-Shafarevich group $Ш(E/_n K)(p)$ is finite for all n. If the base field is $\mathbb{Q}$, then the question can be reformulated by asking if the power series h' in proposition VI.10 is ever a non-unit. Indeed, write $\lambda(Ш)$ for the sum of the degrees of the irreducible distinguished factors of h'. Assuming the finiteness of $Ш(E/_n K)(p)$ and that the characteristic series of the dual of ${}_\infty\mathcal{R}$ equals the expression in that proposition. If p^{e_n} is the order of $Ш(E/_n K)$, then

$$e_n = \mu(\widehat{{}_\infty\mathcal{R}}) \cdot p^n + \lambda(Ш) \cdot n + \mathbf{O}(1).$$

This can be shown using [NeScWi00, Proposition III.5.13]. We have not come across a single example where we could prove that $Ш(E/_\infty\mathbb{Q})$ is infinite. Note that the injection of $Ш(E/_n\mathbb{Q})(p)$ into $Ш(E/_n\mathbb{Q})(p)$ has cokernel in the cokernel of localisation $E({}_n\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E({}_n\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p$; hence in a group of corank $p^n + \mathbf{O}(1)$. So there is still a lot of space for the classical Tate-Shafarevich to grow exponentially.

VI.4.3 Distributions

Let $E/\mathbb{Q}$ be an elliptic curve. We wish to generalise the proposition 5.1 in [cetraro99] on page 105, saying that, for a curve of rank zero, there is a set of primes p of density 1 among all primes where E has good ordinary reduction such that ${}_\infty\mathcal{S} = 0$, i.e. that the rank of the Selmer group does not increase. For the classical Selmer group generalising conjectures and numerical evidence for them were announced in [Wut04]. We shall consider the situation for the growth of the fine Selmer group here.

Proposition VI.14. *For an elliptic curve $E/\mathbb{Q}$ of rank 0 with finite $Ш(E/\mathbb{Q})$, there is a set of primes of density 1 such that $\mathcal{R}(E/_\infty\mathbb{Q})$ is finite.*

Proof. The Euler characteristic formula in corollary II.5 shows that the proof of proposition 5.1 in [cetraro99] can be applied without change. □

Now suppose that the rank is 1. The formula (II.4) could almost be used to prove the same result, if we only knew that the index D is trivial for a set of primes p of density 1. To my knowledge, there are no results in this direction.

For curves of rank larger than 1, there is another factor that will play an important role in the question if the bound on the Euler characteristic is trivial, namely the regulator. The results in chapter V suggest that the regulator is a unit for a set of density 1 among all primes. But remember that there is a second bound coming from the growth of the classical Selmer group which is conjectured to have the same property to be trivial for a set of density 1 among all good ordinary primes (see conjecture 2 in [Wut04]). We therefore dare to make the following

Conjecture VI.15. *Let $E/\mathbb{Q}$ be an elliptic curve. There should be only a finite number of primes p for which the corank $\mathcal{R}(E/_\infty\mathbb{Q})$ is larger than the corank of $\mathcal{R}(E/\mathbb{Q})$.*

It implies that the $Ш(E/_\infty\mathbb{Q})(p)$ is finite for almost all primes if one believes the fine Tate-Shafarevich groups over $\mathbb{Q}$ to be finite. The numerical evidence in the tables VI.5 is very much in support of this conjecture. Of course, for this conjecture to make sense, we have to assume that the conjecture on the μ-invariant hold for almost all primes.

VI.5 Tables

Some notations for the following tables. The symbol $\flat$ will stand for a prime with bad reduction, $\sharp$ for anomalous reduction and $\natural$ for supersingular reduction. The tables contain curves of low conductor found in the tables of Cremona [Cre97]. The conductor N, the coefficients of the global minimal Weierstrass equation $[a_1, a_2, a_3, a_4, a_6]$ are given for each curve as well as the regulator of the fine Mordell-Weil group (Reg.), the product of the Tamagawa numbers (Tam.), the index $D(p)$ from the formula in theorem II.4 and global torsion points $E(\mathbb{Q})(p)$ (Tors.). The expression $J_0\chi = \#J_0 \cdot \chi(\mathcal{R})$ is the product of the Euler characteristic of the dual of the fine Selmer group ${}_\infty\mathcal{R}$ and the unknown index J_0 (or the bound of this product if the reduction is multiplicative). If the curve has good ordinary reduction, we can add to our list the value of the Euler characteristic of the dual of the classical Selmer group ($\chi(\mathcal{S})$). This is also a bound for the Euler characteristic $\chi(\mathcal{R})$ of the dual of the fine Selmer group.

Rather than giving the values, we only list the p-adic valuation of all expressions since this is all that we are interested in anyway. The list only contains the cases when the bound $\#J_0 \cdot \chi(\mathcal{R})$ is not trivial. Hence

> If a curve E an odd prime $p < 300$ is not mentioned in these lists, then the Euler-characteristic $\chi(\mathcal{R})$ of ${}_\infty\mathcal{R}$ and the index J_0 are trivial. Hence ${}_\infty\mathcal{R}$ has the same rank $r-1$ as $\mathcal{R}$ and the fine Tate-Shafarevich $\text{Ш}(E/{}_\infty\mathbb{Q})$ is finite if $\text{Ш}(E/\mathbb{Q})$ is.

Furthermore, the second bound coming from the classical Selmer group permits us to prove in some cases when the reduction is ordinary that the Euler characteristic of the fine Mordell-Weil group is trivial. We also eliminate the five cases that were computed via 2-descent over the first layer of the $\mathbb{Z}_3$-extension in the table VI.1. Hence we are left with only a few cases where we do not know if it is trivial or not, they are denoted with the symbol "**?**" in the beginning. Calculations have been done for all odd primes smaller than 300. If the row for a curve is empty, then there is not any exceptional case at all for $p < 300$.

VI.5.1 Rank 1

The list here contains the first hundred curves of rank 1. Of course, the regulator of the fine Mordell-Weil group is trivial here, since $\mathfrak{M} = 0$. As explained in the end of section II.3, the value of the Euler characteristic is linked to the expression calculated in [CoMc94]. It is therefore no surprise that we get almost the same

table. In fact the only differences are that their table lists much larger primes, but they do not include bad primes. Also, the p-adic height of the generator was not included in their table.

Table VI.2: Euler characteristics for curves of rank 1

	N	Curve	p	$J_0\chi$	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
	37A	[0, 0, 1, -1, 0]	179	1	0	1	0	0
	43A	[0, 1, 1, 0, 0]	13	2	0	2	0	0
?	53A	[1, -1, 1, 0, 0]	♮3	1	0	1	0	
			31	1	0	1	0	0
	57A	[0,-1,1,-2,2]						
	58A	[1,-1,0,-1,1]						
	61A	[1, 0, 0, -2, 1]	5	1	0	1	0	0
			17	1	0	1	0	0
	65A	[1, 0, 0, -1, 0]	7	1	0	1	0	0
?	77A	[0, 0, 1, 2, 0]	♭ 7	1	0	1	0	
?			♭ 11	1	0	1	0	
	79A	[1,1,1,-2,0]						
	82A	[1, 0, 1, -2, 0]	7	1	0	1	0	0
?			♮191	2	0	2	0	
	83A	[1, 1, 1, 1, 0]	7	1	0	1	0	0
	88A	[0, 0, 0, -4, 4]	293	1	0	1	0	0
	89A	[1, 1, 1, -1, 0]	11	1	0	1	0	0
			13	1	0	1	0	0
	91A	[0, 0, 1, 1, 0]	43	1	0	1	0	0
?	91B	[0, 1, 1, -7, 5]	♪3	2	0	2	1	2
?	92B	[0, 0, 0, -1, 1]	♮3	1	1	0	0	
			139	1	0	1	0	0
?	99A	[1, -1, 1, -2, 0]	♭ 11	1	0	1	0	
			19	1	0	1	0	0
	101A	[0,1,1,-1,-1]						
	102A	[1, 1, 0, -2, 0]	73	1	0	1	0	0
	106A	[1,1,0,-7,5]						
	112A	[0, 1, 0, 0, 4]	113	1	0	1	0	0
	117A	[1,-1,1,4,6]						

	N	Curve	p	$J_0\chi$	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
	118A	[1, 1, 0, 1, 1]	61	1	0	1	0	0
?	121B	[0, -1, 1, -7, 10]	♮17	1	0	1	0	
	122A	[1, 0, 1, 2, 0]	47	1	0	1	0	0
			59	1	0	1	0	0
	123A	[0, 1, 1, -10, 10]	♪5	2	1	1	1	0
?	123B	[0, -1, 1, 1, -1]	♭ 3	1	0	1	0	
	124A	[0, 1, 0, -2, 1]	♪3	2	1	1	1	0
	128A	[0, 1, 0, 1, 1]	29	1	0	1	0	0
	129A	[0, -1, 1, -19, 39]	7	1	0	1	0	0
	130A	[1, 0, 1, -33, 68]	♪3	2	1	1	1	0
			103	1	0	1	0	0
?	131A	[0, -1, 1, 1, 0]	♪59	1	0	1	0	1
	135A	[0,0,1,-3,4]						
	136A	[0, 1, 0, -4, 0]	29	1	0	1	0	0
	138A	[1,1,0,-1,1]						
	141A	[0, 1, 1, -12, 2]	7	1	1	0	0	0
			11	1	0	1	0	0
	141D	[0, -1, 1, -1, 0]	53	1	0	1	0	0
?	142A	[1, -1, 1, -12, 15]	♮3	2	2	0	0	
	142B	[1, 1, 0, -1, -1]	3	1	0	1	0	0
			11	1	0	1	0	0
?			♪31	1	0	1	0	1
	143A	[0, -1, 1, -1, -2]	47	1	0	1	0	0
?	145A	[1, -1, 1, -3, 2]	7	1	0	1	0	1
	148A	[0, -1, 0, -5, 1]	3	1	1	0	0	0
	152A	[0, 1, 0, -1, 3]	7	1	0	1	0	0
	153A	[0, 0, 1, -3, 2]	37	1	0	1	0	0
?	153B	[0, 0, 1, 6, 27]	♭ 3	2	0	2	0	
?	154A	[1, -1, 0, -29, 69]	♪5	1	0	1	0	2
?	155A	[0, -1, 1, 10, 6]	♭ 5	2	1	1	1	
	155C	[0, -1, 1, -1, 1]	3	1	0	1	0	0
?	156A	[0, -1, 0, -5, 6]	♭ 3	1	1	0	0	
			11	1	0	1	0	0

	N	Curve	p	$J_0\chi$	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
	158A	[1,-1,1,-9,9]						
	158B	[1, 1, 0, -3, 1]	67	1	0	1	0	0
	160A	[0,1,0,-6,4]						
	162A	[1,-1,0,-6,8]						
	163A	[0, 0, 1, -2, 1]	73	1	0	1	0	0
	166A	[1, 1, 0, -6, 4]	131	1	0	1	0	0
	170A	[1,0,1,-8,6]						
?	171B	[0, 0, 1, 6, 0]	♭ 3	1	0	1	0	
			5	1	0	1	0	0
			239	1	0	1	0	0
	172A	[0, 1, 0, -13, 15]	♪3	2	1	1	1	0
?			7	1	0	1	0	1
?	175A	[0, -1, 1, 2, -2]	♭ 5	1	0	1	0	
			31	1	0	1	0	0
			103	1	0	1	0	0
			127	2	0	2	0	0
			269	1	0	1	0	0
	175B	[0, -1, 1, -33, 93]	149	1	0	1	0	0
	176C	[0, -1, 0, 3, 1]	3	1	0	1	0	0
?	184A	[0, -1, 0, 0, 1]	♪5	2	0	2	0	1
			17	1	0	1	0	0
	184B	[0, -1, 0, -4, 5]	17	1	0	1	0	0
			67	1	0	1	0	0
	185A	[0,1,1,-156,700]						
?	185B	[0, -1, 1, -5, 6]	♭ 5	1	0	1	0	
			7	1	0	1	0	0
			11	1	0	1	0	0
			227	1	0	1	0	0
	185B	[0,-1,1,-5,6]						
	185C	[1, 0, 1, -4, -3]	13	1	0	1	0	0
?	189A	[0, 0, 1, -3, 0]	♭ 3	1	1	1	0	
?	189B	[0, 0, 1, -24, 45]	♭ 3	1	0	1	1	
			5	1	0	1	0	0

	N	Curve	p	$J_0\chi$	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
	190A	[1, -1, 1, -48, 147]	11	1	1	0	0	0
?	190B	[1, 1, 0, 2, 2]	♮11	1	0	1	0	
	192A	[0,-1,0,-4,-2]						
	196A	[0, -1, 0, -2, 1]	3	1	1	0	0	0
			5	1	0	1	0	0
?			♪73	1	0	1	0	1
	197A	[0, 0, 1, -5, 4]	13	1	0	1	0	0
	198A	[1,-1,0,-18,4]						
	200B	[0,1,0,-3,-2]						
	201A	[0, -1, 1, 2, 0]	17	1	0	1	0	0
	201B	[1, 0, 0, -1, 2]	7	1	0	1	0	0
	201C	[1,1,0,-794,8289]						
	203B	[1,1,1,0,-2]						
	205A	[1, -1, 1, -22, 44]	17	1	0	1	0	0
?	207A	[1, -1, 1, -5, 20]	♭3	2	0	2	0	
	208A	[0, -1, 0, 8, -16]	3	1	0	1	0	0
?			♮41	1	0	1	0	
?	208B	[0, -1, 0, -16, 32]	7	2	0	2	0	1
	209A	[0, 1, 1, -27, 55]	♪3	2	1	1	1	0
			37	1	0	1	0	0
	210D	[1,1,0,-3,-3]						
	212A	[0, -1, 0, -4, 8]	3	1	1	0	0	0
			5	1	0	1	0	0
	214A	[1, 0, 0, -12, 16]	7	1	1	0	0	0
?	214B	[1, 0, 1, 1, 0]	♮71	1	0	1	0	
	214C	[1,0,1,-193,1012]						
?	215A	[0, 0, 1, -8, -12]	♮3	1	0	1	0	
	216A	[0, 0, 0, -12, 20]	43	1	0	1	0	0
?			♮101	1	0	1	0	
	218A	[1, 0, 0, -2, 4]	♪3	2	1	1	1	0
	219A	[0, -1, 1, -6, 8]	5	1	0	1	0	0
?	219B	[0, 1, 1, 3, 2]	♭3	2	1	1	1	
			19	1	0	1	0	0

	N	Curve	p	$J_0\chi$	Tam.	$D(p)$	Tors.	$\chi(\text{Ш})$
?	219C	[1, 1, 0, -82, -305]	♪5	1	0	1	0	1
			97	1	0	1	0	0
?	220A	[0, 1, 0, -45, 100]	♪3	3	2	1	1	2
	224A	[0,1,0,2,0]						
?	225A	[0, 0, 1, 0, 1]	♮131	1	0	1	0	
?	225E	[0, 0, 1, -75, 256]	♭ 3	1	1	0	0	
			197	1	0	1	0	0
	226A	[1, 0, 0, -5, 1]	♪3	1	1	0	0	1
?			♪5	1	0	1	0	1

VI.5.2 Rank 2

For curves of rank 2, we have chosen the first hundred curves in Cremona's tables. There are three cases when the calculations of the canonical regulator for the classical Selmer group were too complicated to be done; the symbol "¿" is showing where this happened. Some of the computations here involved quite large numbers. The numerator of a certain point on the curve of conductor 1143 had more than $300'000$ digits.

Table VI.3: Euler characteristics for curves of rank 2

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\text{Ш})$
	389A	[0, 1, 1, -2, 0]	41	1	1	0	0	0	0
			167	1	1	0	0	0	0
	433A	[1, 0, 0, 0, 1]	♪3	1	1	0	0	0	0
			17	1	1	0	0	0	0
			23	1	1	0	0	0	0
			281	1	1	0	0	0	0
?	446D	[1, -1, 0, -4, 4]	♮3	1	1	0	0	0	
?			♪5	1	1	0	0	0	1
?	563A	[1, 1, 1, -15, 16]	♪5	1	1	0	0	0	1
			7	1	1	0	0	0	0
			193	1	1	0	0	0	0
	571B	[0, 1, 1, -4, 2]	5	1	1	0	0	0	0
			13	1	1	0	0	0	0
?	643A	[1, 0, 0, -4, 3]	♮43	2	2	0	0	0	
			59	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
?	655A	[0, 0, 1, -13, 18]	♭5	1	1	0	0	0	
?			7	1	1	0	0	0	1
			13	1	1	0	0	0	0
	664A	[0, 0, 0, -7, 10]							
	681C	[0, -1, 1, 0, 2]	59	1	1	0	0	0	0
	707A	[0, 1, 1, -12, 12]	♪3	1	1	0	0	0	0
?			♭7	2	2	0	0	0	
			79	1	1	0	0	0	0
?	709A	[0, -1, 1, -2, 0]	5	1	1	0	0	0	1
?			7	1	1	0	0	0	2
			19	1	1	0	0	0	0
	718B	[1, 0, 1, -5, 0]	5	1	1	0	0	0	0
			181	1	1	0	0	0	0
?	794A	[1, 0, 1, -3, 2]	♪3	3	3	0	0	0	2
			♪5	2	2	0	0	0	0
			37	1	1	0	0	0	0
?	817A	[0, 1, 1, 1, 6]	♪3	1	1	0	0	0	1
	916C	[0, 0, 0, -4, 1]	281	1	1	0	0	0	0
?	944E	[0, 0, 0, -19, 34]	♮3	1	1	0	0	0	
			31	1	1	0	0	0	0
			67	1	1	0	0	0	0
	997B	[0, -1, 1, -5, -3]	167	1	1	0	0	0	0
	997C	[0, -1, 1, -24, 54]	3	3	3	0	0	0	0
			5	2	2	0	0	0	0
	1001C	[0, 0, 1, -199, 1092]							
	1028A	[0, 1, 0, -10, 9]	♪3	2	1	1	0	0	1
			31	1	1	0	0	0	0
			53	2	2	0	0	0	0
	1034A	[1, 0, 1, -12, 14]	♪3	1	1	0	0	0	1
	1058C	[1, 0, 1, 0, 2]	♪3	1	1	0	0	0	0
	1070A	[1, -1, 0, -10, 16]	67	1	1	0	0	0	0
	1073A	[0, -1, 1, -45, 132]	83	1	1	0	0	0	0
	1077A	[1, 1, 1, -27, 42]	11	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
			23	1	1	0	0	0	0
	1088J	[0, 1, 0, -25, 39]	♪3	1	1	0	0	0	0
?			♪5	2	2	0	0	0	2
	1094A	[1, 0, 1, -7, 6]	♪3	2	2	0	0	0	0
	1102A	[1, 1, 0, -29, 61]							
	1126A	[1, -1, 0, 2, 4]	7	1	1	0	0	0	0
	1132A	[0, 1, 0, -5, 4]	♪3	2	1	1	0	0	1
?			♪5	1	1	0	0	0	1
			7	2	2	0	0	0	0
	1137A	[1, 1, 1, -2, 2]	17	2	2	0	0	0	0
			23	1	1	0	0	0	0
?	1141A	[1, 0, 0, -27, 94]	5	2	1	1	0	0	3
			11	1	1	0	0	0	0
			101	1	1	0	0	0	0
?	1143C	[0, 0, 1, -39, 90]	♭3	3	3	0	0	0	
			5	1	1	0	0	0	0
			13	1	1	0	0	0	0
			41	1	1	0	0	0	0
?			227	1	1	0	0	0	2
	1147A	[0, -1, 1, -9, 9]	3	1	1	0	0	0	0
			43	1	1	0	0	0	0
?	1171A	[1, -1, 1, -3, 0]	♮3	3	3	0	0	0	
?			♪103	1	1	0	0	0	¿
	1246C	[1, -1, 0, -1, 13]	17	1	1	0	0	0	0
	1309B	[0, -1, 1, -22, 52]	3	1	1	0	0	0	0
			13	1	1	0	0	0	0
			83	1	1	0	0	0	0
			179	1	1	0	0	0	0
	1324A	[0, 1, 0, 3, 4]							
	1325E	[0, 1, 1, -8, -6]							
	1431A	[1, -1, 1, -29, -26]	5	1	1	0	0	0	0
	1436A	[0, 1, 0, -12, 4]							
	1443C	[1, 1, 1, -9, 6]	5	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
?	1446A	[1, 1, 0, -4, 4]	♭3	1	1	0	0	0	
			109	1	1	0	0	0	0
	1466B	[1, -1, 1, -42, 105]	11	1	1	0	0	0	0
	1477A	[1, 0, 0, -6, 7]	5	2	2	0	0	0	0
?	1480A	[0, 0, 0, -28, 52]	♮3	1	1	0	0	0	
	1483A	[0, 1, 1, 2, 2]							
	1525C	[1, 0, 0, -8, 7]							
	1531A	[0, 0, 1, -14, 20]	11	1	1	0	0	0	0
	1534B	[1, -1, 0, 5, 37]							
	1570B	[1, 0, 1, -4, 6]	17	1	1	0	0	0	0
	1576A	[0, 1, 0, -9, -5]	53	1	1	0	0	0	0
			67	1	0	0	1	0	0
	1591A	[0, 0, 1, -71, 552]	29	1	1	0	0	0	0
	1594A	[1, -1, 1, -27, 75]							
	1608A	[0, -1, 0, -25, 61]	73	1	1	0	0	0	0
	1611D	[0, 0, 1, -9, 20]							
?	1613A	[0, 1, 1, -3, 0]	♪3	2	2	0	0	0	3
			13	1	1	0	0	0	0
			17	1	1	0	0	0	0
?	1615A	[1, 0, 0, -215, 1192]	♭17	1	1	0	0	0	
	1621A	[1, -1, 1, -4, 4]							
?	1627A	[1, 1, 1, -3, -2]	♮5	1	1	0	0	0	
	1639B	[1, -1, 1, -6, 6]	5	1	1	0	0	0	0
?			♮61	1	1	0	0	0	
	1641B	[0, -1, 1, -4, 6]							
	1642A	[1, 1, 0, -1, 5]	5	1	1	0	0	0	0
?			♮17	1	1	0	0	0	
	1653A	[0, -1, 1, -27, 182]	239	1	1	0	0	0	0
?	1662A	[1, 1, 0, -27, 45]	♭3	2	2	0	0	0	
			♪5	1	1	0	0	0	0
			11	1	1	0	0	0	0
			37	1	1	0	0	0	0
	1664N	[0, 0, 0, -4, 16]	5	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
			11	1	1	0	0	0	0
?	1674D	[1, -1, 0, -9, 9]	♭3	3	3	1	0	0	
			17	1	1	0	0	0	0
			277	1	1	0	0	0	0
?	1688A	[0, 1, 0, -12, 16]	5	1	1	0	0	0	1
	1696D	[0, 0, 0, -76, 256]	5	1	1	0	0	0	0
	1696E	[0, -1, 0, 15, 1]	47	1	1	0	0	0	0
			101	1	1	0	0	0	0
?	1701J	[0, 0, 1, -27, 56]	♭3	2	1	1	1	0	
			♪5	1	1	0	0	0	0
	1712D	[0, -1, 0, 0, 16]	3	1	1	0	0	0	1
			11	1	1	0	0	0	0
			13	1	1	0	0	0	0
			229	1	1	0	0	0	0
			233	1	1	0	0	0	0
	1717B	[0, -1, 1, -4, 4]	5	1	1	0	0	0	0
	1732A	[0, 1, 0, -44, 100]	11	1	1	0	0	0	0
			73	1	0	0	1	0	0
	1738A	[1, 1, 0, -14, 4]	13	1	1	0	0	0	0
	1745D	[0, -1, 1, -6, 6]							
?	1746B	[1, -1, 0, -24, 44]	♭3	1	1	0	0	0	
	1748A	[0, -1, 0, -90, 361]	7	1	1	0	0	0	0
			43	1	1	0	0	0	0
	1752E	[0, -1, 0, -20, 36]	11	1	1	0	0	0	0
	1793B	[0, 1, 1, 6, 6]	199	1	1	0	0	0	0
	1832B	[0, -1, 0, -27, 64]	29	1	1	0	0	0	0
	1856D	[0, -1, 0, -17, 49]	17	1	1	0	0	0	0
?			♪43	1	1	0	0	0	¿
	1862A	[1, 0, 1, -75, 242]	♪3	3	2	1	0	1	0
	1873A	[1, -1, 1, -1, 2]	5	2	2	0	0	0	0
			107	1	1	0	0	0	0
	1887A	[1, 1, 1, -17, 20]	13	1	1	0	0	0	0
			19	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	Tam.	$D(p)$	Tors.	$\chi(\mathcal{S})$
			131	1	1	0	0	0	0
			197	1	1	0	0	0	0
	1888A	[0, -1, 0, -2, 4]							
?	1907A	[1, -1, 1, -46, 130]	♮3	1	1	0	0	0	
			7	2	2	0	0	0	0
?			♮17	1	1	0	0	0	
			31	1	1	0	0	0	0
	1909A	[0, 0, 1, -4, 2]	7	1	1	0	0	0	0
			11	1	1	0	0	0	0
?	1913A	[1, 1, 0, -202, 1025]	7	1	1	0	0	0	1
?	1917C	[1, -1, 1, -41, 110]	♭ 3	2	2	1	0	0	
	1918C	[1, 0, 1, -22, -24]	♪3	1	1	0	0	0	0
			73	1	1	0	0	0	0
?			♭ 137	1	1	0	0	0	
	1922B	[1, 1, 0, -4, -4]	3	2	2	0	0	0	0
			191	1	1	0	0	0	0
?	1933A	[1, 0, 0, 1, -2]	♪3	1	1	0	0	0	1
?			5	1	1	0	0	0	1
			103	1	1	0	0	0	0
	1952B	[0, 1, 0, -17, 31]							
?	1957A	[1, 1, 0, -522, 4315]	♭ 19	1	1	0	0	0	
			43	1	1	0	0	0	0
?			♪163	1	1	0	0	0	¿
	1957B	[1, 1, 1, -8, -12]							
	1964A	[0, 0, 0, -16, 25]	17	2	2	0	0	0	0
	2006D	[1, 1, 0, -88, 284]	89	1	1	0	0	0	0
?	2007A	[1, -1, 1, -14, 42]	♮11	1	1	0	0	0	

VI.5.3 Rank 3

Finally the list the few curves of rank 3 that are in Cremona's lists.

Table VI.4: Euler characteristics for curves of rank 3

	N	Curve	p	$J_0\chi$	Reg	$D(p)$	Tam.	Tors.	$\chi(\mathcal{S})$
?	5077A	[0, 0, 1, -7, 6]	♮3	2	2	0	0	0	
			♪5	1	1	0	0	0	0
	11197A	[1, -1, 1, -6, 0]	53	1	1	0	0	0	0

	N	Curve	p	$J_0\chi$	Reg	$D(p)$	Tam.	Tors.	$\chi(\mathcal{S})$
	11642A	[1,-1,0,-16,28]							
?	12279A	[0, -1, 1, -10, 12]	♪5	1	1	0	0	0	1
			29	1	1	0	0	0	0
?	13766A	[1, 0, 1, -23, 42]	♪3	1	1	0	0	0	1
			♪5	3	3	0	0	0	0
	16811A	[0,0,1,-1,6]							
	18097B	[1, 1, 1, -10, 6]	67	1	1	0	0	0	0
?	18562C	[1, 0, 1, -20, 30]	♪3	2	2	0	0	0	1
			127	1	1	0	0	0	0
?	18745A	[0, 1, 1, -146, 636]	♪3	1	1	0	0	0	1

Bibliography

[Ber81] Dominique Bernardi, *Hauteur p-adique sur les courbes elliptiques*, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser, 1981, pp. 1–14.

[BerPR93] Dominique Bernardi and Bernadette Perrin-Riou, *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 3, 227–232.

[BeDa94] Massimo Bertolini and Henri Darmon, *Derived heights and generalized Mazur-Tate regulators*, Duke Math. J. **76** (1994), no. 1, 75–111.

[BeDa95] Massimo Bertolini and Henri Darmon, *Derived p-adic heights*, Amer. J. Math. **117** (1995), no. 6, 1517–1554.

[Ber01] Massimo Bertolini, *Iwasawa theory for elliptic curves over imaginary quadratic fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 1–25, 21st Journées Arithmétiques (Rome, 2001).

[Ber82] Daniel Bertrand, *Valuers de fonctions thêta et hauteur p-adiques*, Seminar on Number Theory, Paris 1980-81, Progr. Math., vol. 22, Birkhäuser, 1982, pp. 1–11.

[Blo80] Spencer Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **58** (1980), no. 1, 65–76.

[BoLüRa90] Siegfried Bosch, Werner Lütkebohmert and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer, 1990.

[Bra85] Gudrun Brattström, *The invariants of the Tate-Shafarevich group in a $\mathbf{Z}_p$-extension can be infinite*, Duke Math. J. **52** (1985), no. 1, 149–156.

[Cas62] John W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[Cas64] John W. S. Cassels, *Arithmetic on curves of genus* 1. *VII. The dual exact sequence*, J. Reine Angew. Math. **216** (1964), 150–158.

[cetraro99] John Coates, Ralph Greenberg, Kenneth A. Ribet and Karl Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer, 1999, Lectures from the 3rd C.I.M.E. in Cetraro, 1997.

[CoMc94] John Coates and Gary McConnell, *Iwasawa theory of modular elliptic curves of analytic rank at most* 1, J. London Math. Soc. (2) **50** (1994), no. 2, 243–264.

[CoSu] John Coates and Ramdorai Sujatha, *Fine Selmer groups of elliptic curves over* p*-adic Lie extensions*, to be published.

[CoSu00] John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa Publishing House, 2000.

[Col98] Pierre Colmez, *Intégration sur les variétés* p*-adiques*, Astérisque (1998), no. 248.

[Cre97] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[Del75] Pierre Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Antwerp, 1972), Springer, 1975, pp. 53–73. Lecture Notes in Math., Vol. 476.

[Fis01] Tom Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbf{Q}$, J. Eur. Math. Soc. (JEMS) **3** (2001), no. 2, 169–201.

[Fis03] Tom Fisher, *The Cassels-Tate pairing and the Platonic solids*, J. Number Theory **98** (2003), no. 1, 105–155.

[Fla90] Matthias Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127.

[Gre] Peter Green, *Heegner points package*, availabe at `http://www.math.mcgill.ca/darmon/programs/heegner/heegner.html`.

[Gre99] Ralph Greenberg, *Introduction to Iwasawa Theory of Elliptic Curves*, Lectures given at the IAS/Park CityMathematics Institute; available at http://www.math.washington.edu/~greenber/Park.ps, 1999.

[Gro91] Benedict H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, 1991, pp. 235–256.

[HiSi00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry, An introduction*, Graduate Texts in Mathematics, vol. 201, Springer, 2000.

[How03] Benjamin Howard, *Derived p-adic heights and p-adic L-function*, to appear in Amer. J. Math.; available at http://abel.math.harvard.edu/~howard/height.pdf, 2003.

[Ima75] Hideo Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions*, Proc. Japan Acad. **51** (1975), 12–16.

[Jan94] Uwe Jannsen, *A spectral sequence for Iwasawa adjoints*, 1994, unpublished, available at http://www.mathematik.uni-regensburg.de/Jannsen/~Preprints.

[Jon95] John W. Jones, *Plater's p-adic orthogonality relation for abelian varieties*, Houston J. Math. **21** (1995), no. 2, 261–282.

[Kat00] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular curves*, Preprint Series, Graduate School of Mathematical Sciences, The University of Tokyo, 2000.

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[Lan83] Serge Lang, *Fundamentals of Diophantine geometry*, Springer, 1983.

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, 2002.

[MaRu02] Barry Mazur and Karl Rubin, *Pairings occurring in the arithmetic of elliptic curves*, Proceedings of the conference on arithmetic algebraic geometry, Barcelona, 2002; available at http://abel.math.harvard.edu/~mazur/preprints/barcelona.pdf, 2003.

[MaRu03] Barry Mazur and Karl Rubin, *Studying the growth of Mordell-Weil*, Doc. Math., Extra Volume: Kazuya Kato's Fiftieth Birthday, (2003), 585–607.

[MaTa83] Barry Mazur and John Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, 1983, pp. 195–237.

[MaTa91] Barry Mazur and John Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[Mil86] John S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., 1986, available at `http://www.jmilne.org/math/Preprints/ADT.pdf`.

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, 1970.

[Nek01] Jan Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

[Nek03] Jan Nekovář, *Selmer complexes*, 2003, available at `http://www.math.jussieu.fr/~nekovar/pu/`.

[Nér65] André Néron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2) **82** (1965), 249–331.

[Nér82] André Néron, *Fonctions thêta p-adiques et hauteurs p-adiques*, Seminar on Number Theory, Paris 1980-81, Progr. Math., vol. 22, Birkhäuser, 1982, pp. 149–174.

[NeScWi00] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000.

[Nor85] Peter Norman, *p-adic theta functions*, Amer. J. Math. **107** (1985), no. 3, 617–661.

[Oes82] Joseph Oesterlé, *Construction de hauteurs archimédiennes et p-adiques suivant la methode de Bloch*, Seminar on Number Theory, Paris 1980-81, Progr. Math., vol. 22, Birkhäuser, 1982, pp. 175–192.

[Pap00] Matthew A. Papanikolas, *Canonical heights on elliptic curves in characteristic p*, Compositio Math. **122** (2000), no. 3, 299–313.

[pari] C. Batut, D. Bernardi, H. Cohen, M. Olivier and K. Belabas, `pari-gp`, available at `http://pari.math.u-bordeaux.fr/`, 1999.

[Pla91] Andrew Plater, *An orthogonality relation on the points of an elliptic curve*, J. London Math. Soc. (2) **44** (1991), no. 2, 227–249.

[PR82] Bernadette Perrin-Riou, *Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe*, Invent. Math. **70** (1982), no. 3, 369–398.

[PR83] Bernadette Perrin-Riou, *Sur les hauteurs p-adiques*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 6, 291–294.

[PR84] Bernadette Perrin-Riou, *Hauteurs p-adiques*, Seminar on number theory, Paris 1982–83, Progr. Math., vol. 51, Birkhäuser, 1984, pp. 233–257.

[PR92] Bernadette Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.

[PR93a] Bernadette Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes)*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser, 1993, pp. 203–220.

[PR93b] Bernadette Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[PR95] Bernadette Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229.

[PR03a] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186.

[PR03b] Bernadette Perrin-Riou, *Groupes de Selmer et Accouplements; Cas Particulier des Courbes Elliptiques*, Doc. Math., Extra Volume: Kazuya Kato's Fiftieth Birthday, (2003), 725–760.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Sch82] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409.

[Sch85] Peter Schneider, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374.

[Sch98] Peter Schneider, *Basic notions of rigid analytic geometry*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, 1998, pp. 369–378.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ser84] Jean-Pierre Serre, *Groupes algébriques et corps de classes*, Hermann, 1984.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer, 199?, Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.

[Sim02] Denis Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17, `pari` program available at `http://www.math.unicaen.fr/~simon/`.

[ScSt04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231, `magma` program available at `www.math.uni-duesseldorf.de/~stoll/`.

[Tat58] John Tate, *WC-groups over p-adic fields*, Séminaire Bourbaki, Vol. 4, Soc. Math. France, 1995, pp. Exp. No. 156, 265–277.

[Tat63] John Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, 1963, pp. 288–295.

[Tat66] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, 1995, pp. Exp. No. 306, 415–440.

[Tat75] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Antwerp, 1972), Springer, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, 1994.

[Wut04] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, to be published in J. London Math. Soc., 2004.

[Zag85] Don Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Workshop Bonn 1984, Lecture Notes in Math., vol. 1111, Springer, 1985, pp. 225–248.