Iwasawa Theory for Elliptic Curves

by

Archiebold C. Karumbidza

Thesis submitted in partial fulfillment
of the requirements for the award of Masters of Science degree in Mathematics
at the University of Stellenbosch, South Africa

Supervisor: Dr Arnold Keet

April 2006

DECLARATION

I, the undersigned, hereby declare that the work contained in this thesis is my own and has not previously, in its entirety or in part, been submitted at any university for a degree.

Signature

Date 09/03/2006

ABSTRACT

Iwasawa Theory for Elliptic Curves

In this thesis we consider modules over the Iwasawa algebra, these naturally arise in the classical theory of class groups over cyclotomic fields as exposed by Kenkichi Iwasawa. We classify these modules up to psuedo-isomorphism. We apply this classification to estimate the growth of the p-part of the ideal class groups along a $\mathbb{Z}_p$-extension. Class groups can be interpreted as "generalized Selmer groups", these include the traditional Selmer groups attached to elliptic curves. We are thus naturally led to consider the growth of Selmer groups of elliptic curves along a $\mathbb{Z}_p$-extension. Under the hypothesis of good ordinary reduction these Selmer groups have a particulary simple and elegant description, we use this description to prove the so called "Control Theorem" of B. Mazur. As a consequence we are able to investigate the growth behavior of Selmer and Tate-Shafarevich groups along a $\mathbb{Z}_p$-extension. The original motivations for considering the Selmer groups of elliptic curves along a $\mathbb{Z}_p$-extension are however quite different from what has been suggested above. The Mordell-Weil theorem says the abelian group of rational points on an elliptic curve over $\mathbb{Q}$ is finitely generated. It is natural to wonder if the Mordell-Weil theorem still holds over infinite extensions of $\mathbb{Q}$ which are at least Galois. There is a simple criterion due to B. Mazur for the Mordell-Weil theorem to still hold, the hypotheses of this criterion, however, are hard to verify in any particular case. Consequences of the "Control Theorem" allow us to verify this hypothesis over a $\mathbb{Z}_p$-extension, thus the Mordell-Weil Theorem holds for a $\mathbb{Z}_p$-extension

OPSOMMING

Iwasawa Teorie vir Elliptiese Kurwes

In hierdie tesis oorweeg ons modules oor die Iwasawa algebra, hierdie kom natuurlik voor in die klassieke teorie van klas groepe oor sikliese liggame soos blootgestel deur Kenkichi Iwasawa. Ons beskryf hierdie modules tot pseudo-isomorfisme. Ons pas hierdie beskrywing toe om die groei van die p-deel van die ideaal klas groep in 'n $\mathbb{Z}_p$-uitbreiding te benader. Klas groepe kan as veralgemeende Selmer groepe beskou word, hierdie sluit in die tradisionele Selmer groepe verbind aan elliptiese kurwes. Dit is dus vanselfsprekend om die groei van Selmer groepe can elliptiese kurwes in 'n $\mathbb{Z}_p$-uitbreiding te oorweeg. Onder die hipotese van goeie gewone reduksie het hierdie Selmer groepe 'n besondere eenvoudige en elegante beskrywing, ons gebruik hierdie beskrywing om die sogenoemede "Beheer Stelling" van B. Mazur te bewys. As 'n afleiding is dit moontlik om die groei houding can Selmer en Tate-Shafarevich groepe in 'n $\mathbb{Z}_p$-uitbreiding te ondersoek. Die oorspronklike motivering vir die oorweging van Selmer groepe van elliptiese kurwes in 'n $\mathbb{Z}_p$-uitbreiding is egter heelwat anders as wat hierbo aangedui is. Die Mordell-Weil stelling sê dat die Abelian groep van rasionale punte op 'n elliptiese kurwe oor $\mathbb{Q}$ eindig voortgebring is. Dit is algemeen om te wonder of die Mordell-Weil stelllig steeds hou oor oneindige uitbreidings van $\mathbb{Q}$ wat ten minste Galois is. Daar is 'n eenvoudige voorwaarde deur B. Mazur waaronder die Mordell-Weil stelling steeds staan, die hipotese van hierdie voorwaarde is egter moeilik om te kontroleer in enige spesiale voorbeeld. Gevolge van die "Beheer Stelling" laat ons toe om die hipotese te kontroleer oor 'n $\mathbb{Z}_p$-uitbreiding en dus staan die Mordell-Weil stelling vir 'n $\mathbb{Z}_p$-uitbreiding.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr Keet for his patience and support during the entire duration of this thesis, the successful completion of this thesis is in no small measure entirely due to his dedication and unwavering support. I would also like to extend my gratitude to the number theory group at Stellenbosch University, in particular Dr Florian Breuer, who have freely shared their knowledge and made it a wonderful place to study mathematics. I would also like to acknowledge the financial support that I have received from the Department of Mathematics and the African Institute for Mathematics (AIMS) while pursuing my studies. I am very grateful for this.

TABLE OF CONTENTS

CHAPTER I

Introduction

1.1 Preface

Since the beginning of the 20th century, one of the continuing themes which motivated algebraic number theory has been the analogy between algebraic number fields and algebraic function fields. Starting in the 1950's, Kenkichi Iwasawa in a series of now classical papers, introduced the revolutionary idea that you could study class groups over cyclotomic extensions by looking instead at an associated algebraic module. This Iwasawa module encodes a lot of information about a whole family of class groups along the tower of cyclotomic extensions. Iwasawa in particular proved (among other important results) the following famous result:

Let $K = \mathbb{Q}(\zeta_{p^\infty})$ obtained by adjoining to $\mathbb{Q}$ all the p-th power roots of unity. We also define $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$. Let h_n be the order of the ideal class group of K_n and let p^{e_n} be the highest power of p dividing h_n. Then Iwasawa's result says:

- [21] If $e_1 = 0$ (i.e. if p is a "regular" prime in the sense of Kummer) then one has $e_n = 0$ for all n
- [22] For each prime number p, there exist integers m, l, c with $m \geq 0$, $l \geq 0$ such that:

$$e_n = mp^n + ln + c$$

Iwasawa also formulated a number of conjectures concerning the behaviour of ideal class groups in the tower of subfields of a $\mathbb{Z}_p$-extension .

Iwasawa's results suggested a much deeper aspect of the analogy between algebraic number fields and algebraic function fields. In the theory of algebraic function fields, a famous theorem of Andre Weil states that there is a very precise relationship between the zeta function and the divisor class group of an algebraic function field. It was undoubtedly hard to imagine how to even formulate an analogous result for algebraic number fields, but Iwasawa's ideas provided exactly the right framework to make that possible. Iwasawa's Conjecture asserts that there should be a precise relationship between two analogous objects associated with a large class of algebraic number fields: the "p-adic zeta function" discovered by Kubota and Leopoldt and the "Iwasawa Module" which was constructed from ideal class groups. This conjecture has come to be called "Iwasawa's Main Conjecture".

Iwasawa's ideas, whose power lies in subtly mixing p-adic analytic methods with Galois cohomology, have subsequently been applied to a wider circle of problems in arithmetic algebraic geometry. But the origin and archetypal example of Iwasawa's theory is in the classical theory of cyclotomic fields. To explain Iwasawa's ideas let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and consider the p primary part of the ideal class group of K_n, $X_n = Cl(K_n)(p)$. Instead of looking at individual p-class groups, Iwasawa considers the whole family of p-class groups as $n \to \infty$, by patching them up via projective limits. From this process he obtains $X_\infty = \varprojlim_n Cl(K_n)(p)$ which is naturally an Iwasawa module i.e. a module over the group ring $\mathbb{Z}_p[[\Gamma]]$, where Γ is non-canonically isomorphic to $\mathbb{Z}_p$. Iwasawa develops a classification theory for such modules of finite type, and using this classification, he manages to recover the X_n's as quotients of X_∞. The classification theory allows one to get asymptotic estimates on the orders of these quotients and thus on the class groups. Iwasawa's ideas go further than this, and this is the real gem. The algebra $\mathbb{Z}_p[[\Gamma]]$ has an analytic interpretation as the algebra of $\mathbb{Z}_p$-measures on Γ with values in $\mathbb{Z}_p$ (see [28] chapter 4) and this has been used to extend and indeed explain Kummer's results on the connection between the zeta-function and the Bernoulli numbers.

Inspired by Iwasawa's ideas, in the late 1960's Mazur developed an analogous theory for abelian varieties over a $\mathbb{Z}_p$-extension, including a version of "Iwasawa's Main Conjecture" in that context. Mazur's ideas are contained in his article *Rational points of abelian varieties with values in a tower of number fields* [28]. On the one hand, Mazur constructed an Iwasawa Module from the Selmer group of an abelian variety with good reduction over p, which reflected algebraic properties of the abelian variety. Mazur together with Swinnerton-Dyer discovered that they could also construct a natural p-adic L-function which reflected properties of the classical L-function (defined by Hasse and Weil) for the elliptic curve, and that there was a relation between this analytic object and the Iwasawa Module. Manin, in an article entitled *Cyclotomic fields and modular curves* [26], later managed to recast Mazur's ideas in the language and techniques of Galois cohomology, thus giving a simpler account of the subject. All along, one of the primary motivations was to provide an approach to study the behaviour of the Mordell Weil group of elliptic curves (and more generally abelian varieties) and the conjecture of Birch and Swinnerton-Dyer. In this thesis, we give an account of some of the theory mentioned above and hopefully give a glimpse, albeit limited, of what no doubt is one of the pivotal theories in modern arithmetic geometry, whose ideas and influence lies behind some of the finest achievements of the subject. Namely progress on the Birch Swinnerton-Dyer conjectures and Wiles's work on the modularity of elliptic curves to name a few.

If there are any apologies to make it is the notable absence of the analytic side of Iwasawa theory. An attempt to account for this would have demanded a bigger undertaking, with many premium constraints this has however not been possible. We apologise.

1.2 Organisation

The first chapter reviews some of the background material that goes into this thesis. Where we felt provision of the necessary background would lead us too far astray, we have been content to just state the important results and give ample references to sources which treat the material in detail. This in particular applies to the class field theory, where no background has been provided at all, with the sentiment that any such attempt would be inadequate and in any case many good references exist.

In the second chapter we explain the structure theory of $\mathbb{Z}_p$ or Γ-extensions. We show that these extensions are of a particularly simple type. The only closed subgroups of such an extension are of the form $p^n\mathbb{Z}_p$ for some n, and the $\mathbb{Z}_p$-extension can be given as the union of the fixed fields of these closed subgroups. Ramification in the extension only occurs above the prime p and for a sufficiently large base field moving up the tower the extension is totally ramified. Good references for this material are [44] and [24] .

In the third chapter we classify modules over a commutative, noetherian and integrally closed domain up to pseudo-isomorphism. We show that up to pseudo-isomorphism there is a nice decomposition of these modules akin to that of modules over a principal ideal domain. We then specialise our results to modules over the complete group ring $\mathbb{Z}_p[[\Gamma]]$. These are the Iwasawa modules and they naturally fall into the above category. These modules can be identified (after choosing a topological generator of Γ) with modules over the power series ring $\mathbb{Z}_p[[T]]$, which is a 2-dimensional regular local ring. We present various results on some properties of Iwasawa modules and we also obtain asymptotic estimates for orders of certain natural quotients of Iwasawa modules with an eye towards applications to class groups and Selmer groups. Our treatment here is as found in [28]. For a different treatment, albeit less conceptual, we refer the reader to [44].

In the fourth chapter we explore the pioneering work of Kenkichi Iwasawa on ideal class groups. We show that the p-primary part of the class groups along the tower in a $\mathbb{Z}_p$-extension can be realized as quotients of Iwasawa modules. We have nice asymptotic estimates for the orders of such quotients and hence we obtain the famous results of Iwasawa on the asymptotic orders of class groups in a cyclotomic tower.

In the fifth chapter we treat Mazur's [28] synthesis of the ideas of Iwasawa albeit with a change of language and approach. The approach we take is due to Greenberg [14], [15], [13]. More precisely the famous theorem of Mordell-Weil asserts that the abelian group of K-rational points on an elliptic curve (where K is a number field) is finitely generated. Under certain hypotheses an easy result of Mazur shows that this result still holds for certain infinite Galois extensions L. The hypothesis (namely that the rank of the elliptic curve remains bounded over all the finite sub extensions of L) is in general very hard to verify in any particular case. The main theorem of this section is the so called "Control Theorem" of Mazur; and we shall use this theorem to verify this hypothesis over a $\mathbb{Z}_p$-extension. We show that this hypothesis holds over a $\mathbb{Z}_p$-extension, if the elliptic curve E has good ordinary reduction. We proceed by showing that the Selmer group attached to E has a particularly simple intrinsic description in terms of the Galois cohomology on $E[p^\infty]$. We use this description to prove the "Control Theorem", our results then follow from this. For a different treatment based on norms of formal groups of height 1 we refer the reader to [28] and [26].

In the final chapter we give a survey of other aspects of the theory of Iwasawa Modules that we have not managed to touch on. We will in particular discuss the recent attempts at giving a classification of modules over non-commutative Iwasawa algebras. These arise as modules over the complete group algebra $\mathbb{Z}_p[[G]]$ where G is a p-adic analytic lie group.

CHAPTER II

Background

2.1 Galois Cohomology

In this section we quickly go through some of the cohomological machinery that we shall make frequent use of. The ultimate reference for this subject is Serre [39], this can be used in conjunction with [37] or [6]. Haberland [17] is also an excellent reference.

2.2 Group modules

Consider a group G and an abelian group A equipped with a map

$$G \times A \to A,$$

$$(\sigma, a) \mapsto \sigma a.$$

To say that A is a G-set means that

$$\tau(\sigma a) = (\tau\sigma)a \quad \text{and} \quad 1a = a,$$

for all $\sigma, \tau \in G$ and $a \in A$, where 1 is the identity in G. To say that A is a G-module means that, in addition, we have

$$\sigma(a + b) = \sigma a + \sigma b,$$

for all $\sigma \in G$ and $a, b \in A$. This is all equivalent to giving A the structure of $\mathbb{Z}[G]$-module by way of the map

$$\mathbb{Z}[G] \times A \to A$$

$$(\sum_{g \in G} n_g, a) \to \sum_{g \in G} n_g ga$$

Given a G-module A as above, the subgroup of fixed elements of A is

$$A^G := \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\}.$$

A^G is naturally a $\mathbb{Z}[G]$-submodule of A. We say G acts trivially on A if $\sigma a = a$ for all $a \in A$; thus $A^G = A$ if and only if the action is trivial. We also note that $A^G = \mathrm{Hom}_G(\mathbb{Z}, A)$ thus the fixed module functor is just the Hom functor in disguise. When $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$ are considered as G-modules, this is with the trivial action, unless stated otherwise.

2.3 Cohomology

Definition 2.3.1. Let G be a finite group. By a **G-complex** we mean a pair $\mathcal{C} = \{A_n, \delta\}$ where the A_n's are G-modules and the maps δ's (boundary maps) are homomorphisms between the A_n ,these homomorphisms satisfy $\delta \circ \delta = 0$

Thus a complex may be imagined as in the following diagram

$$\cdots \to A_{n+1} \overset{\delta_{n+1}}{\to} A_n \overset{\delta_n}{\to} A_{n-1} \overset{\delta_{n-1}}{\to} \cdots$$

We say a complex $\mathcal{C} = \{A_n, \delta\}$ is exact if $\ker(\delta_n) = \mathrm{im}(\delta_{n+1})$.

Definition 2.3.2. We say a G-module A is **injective** if and only if the functor $\mathrm{Hom}_G(-, A)$ is exact.

Lemma 2.3.3. Let A be a G-module , then A can be embedded in some injective G-module

Proof. (c.f [35] pg 70) □

Definition 2.3.4. An **injective resolution** of a module A is an exact sequence (complex)

$$0 \to A \to I_0 \xrightarrow{\delta_0} \cdots \to I_n \xrightarrow{\delta_n} I_{n+1} \to \cdots$$

with I_n injective for all n.

Using lemma 2.3.3 it is easy to see that every G-module A has such an injective resolution. Given the injective resolution of A we may apply the fixed module functor to the deleted injective resolution of A and get the following sequence of G-modules which is however no longer exact, but is still a complex.

$$0 \to I_0^G \xrightarrow{\delta_0} \cdots \to I_n^G \xrightarrow{\delta_n} I_{n+1}^G \to \cdots$$

We turn this failure of exactness to advantage by defining

$$Z^n(G, A) = \ker(I_{n-1} \xrightarrow{\delta_n} I_{n-2})$$

$$B^n(G, A) = \operatorname{im}(I_{n-1} \xrightarrow{\delta_n} I_{n-1})$$

and we set $B^0(G, A) = 0$. The elements of $Z^n(G, A)$ and $B^n(G, A)$ are called the n-cycles and the n-coboundaries respectively. Since $\delta \circ \delta = 0$, $B^n(G, A) \subseteq Z^n(G, A)$.

Definition 2.3.5. for $n \geq 0$ we define the **n-th cohomology group** of A as

$$H^n(G, A) = Z^n(G, A)/B^n(G, A)$$

Remark 2.3.6. In defining group cohomology of A we had to choose an injective resolution of A, indeed such a resolution is not unique, thus one may wonder if group cohomology is well defined. It turns out however that the cohomology groups do not depend on the choosen resolution ,therefore are well defined up to isomorphism (c.f [1] pg 54). Since $A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, we have a canonical isomorphism

$$H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

Group cohomology may also be defined abstractly as the right derived functors of the fixed module functor. This is equivalent to our definition but is not very useful for calculations (see [25]).

For computational ease group cohomology is usually defined using the "standard cochain complex" (see [6, pg. 96]). More precisely let A be a G-module. Let P_n, $n \geq 0$ be the free $\mathbb{Z}$-module with basis the $(n+1)$-tuples $(g_0, \ldots, g_n)$, endowed with the action of G such that

$$g(g_0, \ldots, g_n) = (gg_0, \ldots, gg_n)$$

Note that P_n is also free as a $\mathbb{Z}[G]$-module with basis $\{(1, g_1, \ldots, g_n) | g_i \in G\}$. We then define a homomorphism $\delta_n \colon P_n \longrightarrow P_{n-1}$ by the rule

$$\delta_n(g_0, \ldots, g_n) = \Sigma(-1)^i(g_0, \ldots, \hat{g}_i, \ldots, g_n)$$

where the symbol $\hat{g}_i$ means that g_i is omitted. Let $P.$ be the complex

$$\cdots \longrightarrow P_n \xrightarrow{\delta_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0$$

It easy to check that $\delta_{n-1} \circ \delta_n = 0$ thus the sequence above is a complex. Let ε be the map $P_0 \longrightarrow \mathbb{Z}$ that sends each basis element to 1.

Lemma 2.3.7. The complex $P\cdot \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$ is exact. (This complex is the free resolution of $\mathbb{Z}$)

Proof. Choose an element $\sigma \in G$ and define $\kappa_n \colon P_n \longrightarrow P_{n+1}$ by

$$\kappa_n(g_0, \ldots, g_n) = (\sigma, g_0, \ldots, g_n)$$

one easily checks that $\delta_{n+1} \circ \kappa_n + \kappa_{n-1} \circ \delta_n = 1$. Hence if $\delta_n(x) = 0$, then $x = \delta_{n+1}(\kappa_n(x))$ □

Applying the fixed module functor $\mathrm{Hom}_G(-, A)$ to the "deleted complex"

$$\cdots \to P_2 \to P_1 \to P_0 \to 0$$

we obtain a cochain complex of G modules

$$\cdots \leftarrow \mathrm{Hom}_G(P_2, A) \leftarrow \mathrm{Hom}_G(P_1, A) \leftarrow \mathrm{Hom}_G(P_0, A) \leftarrow 0$$

An element of $\mathrm{Hom}_G(P_n, A)$ can be identified with the G equivariant maps $f : G^n \to A$, such an f is G equivariant if and only if

$$f(gg_0, \ldots, gg_n) = g(f(g_0, \ldots, g_n)) \text{ for all } g, g_0, \ldots, g_n \in G$$

Let

$$C^n(G, A) := \mathrm{Maps}_G(G^n, A);$$

thus an element of $C^n(G, A)$ is a G equivariant function f of n variables in G,

$$f(g_1, \ldots, g_n) \in A$$

and is called an homogeneous n-cochain. (If in addition, A and G have a topological structure, then we instead consider continuous cochains.). The δ_n boundary maps induce corresponding boundary maps on $\delta_n : C^n(G, A) \to C^{n+1}(G, A)$ defined by

$$(\delta_n f)(g_0, \ldots, g_{n+1}) = \sum (-1)^i f(g_0, \ldots, \hat{g}_i, \ldots, g_{n+1})$$

Hence we have a complex.

$$\cdots \to 0 \to 0 \to C^0(G, A) \xrightarrow{\delta_0} C^1(G, A) \xrightarrow{\delta_1} C^2(G, A) \xrightarrow{\delta_2} \cdots$$

It is convenient, for many applications to pass to a modified definition of the cohomology groups, which reduces the number of variables in the homogeneous cochain $f(g_0, \ldots, g_i, \ldots, g_{n+1})$ by one. Let $\mathscr{C}^0(G, A) = A$ and for $n \geq 1$, let $\mathscr{C}^n(G, A)$ be the abelian group of all continous functions $y : G^n \to A$. We then have an isomorphism

$$C^0(G, A) \to \mathscr{C}^0(G, A) : f(\sigma) \to f(1).$$

For $n \geq 1$ we also have the isomorphism

$$C^n(G, A) \to \mathscr{C}^n(G, A);$$

$$f(\sigma_0, \cdots, \sigma_n) \to y(\sigma_0, \cdots, \sigma_n) = f(1, \sigma_1\sigma_2, \cdots, \sigma_1 \cdots \sigma_n).$$

The inverse of this map is given by

$$y(\sigma_0, \cdots, \sigma_n) \to f(\sigma_0, \cdots, \sigma_n) = \sigma_0 y(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \cdots, \sigma_{n-1}^{-1}\sigma_n).$$

With these isomorphisms, the boundary maps

$$\delta_{n+1} : C^n(G, A) \to C^{n+1}(G, A)$$

are transformed into the homomorphisms

$$\delta_{n+1} : \mathscr{C}^n(G, A) \to \mathscr{C}^{n+1}(G, A)$$

where the maps δ_{n+1} are given by

$$(\delta_1 y)(\sigma) = \sigma a - a \text{ for } a \in A = \mathscr{C}^0(G, A),$$

$$(\delta_2 y)(\sigma, \tau) = \sigma y(\tau) - y(\sigma\tau) + y(\sigma), \text{ for } y \in \mathscr{C}^1(G, A),$$

$$(\delta_3 y)(\sigma, \tau, \rho) = \sigma y(\tau, \rho) - y(\sigma\tau, \rho) + y(\sigma, \tau\rho) - y(\sigma, \tau), \text{ for } y \in \mathscr{C}^2(G, A),$$

$$\cdots = \cdots$$

$$(\delta_n y)(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1 y(\sigma_2, \ldots, \sigma_{n+1}) + \sum_{j=1}^{n} (-1)^{j+1} y(\sigma_1, \ldots, \sigma_{j-1}, \sigma_j\sigma_{j+1}, \sigma_{j+1}, \ldots, \sigma_{n+1})$$

$$+ (-1)^{n+1} y(\sigma_1, \ldots, \sigma_n) \text{ for } y \in \mathscr{C}^n(G, A),.$$

We define cohomology groups using this complex.

Definition 2.3.8. Let $\varphi : G \longrightarrow A$ be a homomorphism from G to A. We say that φ is a crossed homomorphism if $\varphi(\tau\sigma) = \tau\varphi(\sigma) + \varphi(\tau)$ and φ is called a principal crossed homomorphism if $\varphi(\sigma) = a - \sigma(a)$ for some $a \in A$.

$\varphi : G^2 \longrightarrow A$ is called a factor set if $\varphi(\sigma\tau, \rho) + \varphi(\sigma, \tau) = \varphi(\sigma, \tau\rho) + \sigma\varphi(\tau, \rho)$

Hence we see that (see [32] pg 15)

$$\begin{aligned} H^0(G, A) &= A^G, \\ H^1(G, A) &= \frac{\text{crossed-homomorphisms}}{\text{principal crossed-homomorphisms}} \\ &= \text{Hom}(G, A), \text{ if action is trivial}, \\ H^2(G, A) &= \text{classes of ``factor sets''}. \end{aligned}$$

We present an important consequence of this definition.

Theorem 2.3.9. (Hilbert Satz 90) Let L/K be a Galois extension and G its Galois group, then the multiplicative group $L^\times$ is also a G module and we have

$$H^1(G, L^\times) = 0$$

Proof. Let $\varphi : G \longrightarrow L^\times$ be a crossed homomorphism. For $a \in L^\times$, let

$$b = \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma a$$

Then for $\tau \in G$

$$\tau b = \sum_{\sigma} \tau\varphi(\sigma) \cdot \tau\sigma a = \sum_{\sigma} \varphi(\tau)^{-1}\varphi(\tau\sigma)\tau\sigma a = \varphi(\tau)^{-1} b$$

Suppose $b \neq 0$, then $\varphi(\tau) = b/\tau b$ which shows that φ is a principal crossed homomorphism. We need to prove that there exists an a for which $b \neq 0$. By Dedekind's theorem on the linear independence of characters the map

$$\sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma \colon L^\times \longrightarrow L$$

is non zero, hence such an a exists. □

2.4 Characterization of $H^r(G,-)$

For fixed G and varying A the groups $H^r(G,A)$ have the following fundamental properties:

(i) $H^0(G,A) = A^G$.

(ii) $H^r(G,-)$ is a functor

$$\{G\text{-modules}\} \to \{\text{abelian groups}\}\,.$$

(iii) Each short exact sequence

$$0 \to A' \to A \to A'' \to 0$$

gives rise to connecting homomorphisms (see below)

$$\delta : H^r(G,A'') \to H^{r+1}(G,A')$$

from which we get a long chain complex of cohomology groups, functorial in short exact sequences in the natural sense.

(iv) If A is "induced" or "injective", then $H^r(G,A) = 0$ for all $r \neq 0$.

These properties characterize the sequence of functors H^i equipped with the δ's uniquely, up to unique isomorphism.

For a profinite group G, the cohomology groups $H^n(G,A)$ are built up in a simple way from those of the finite factor groups of G. This amounts to using continuous cochains, where continuous means with respect to the Krull topology on G and the discrete topology on A. More precisely let U, V run through the open normal subgroups of G. If $U \subseteq V$ then the projections

$$G^{n+1} \to (G/U)^{n+1} \to (G/V)^{n+1}$$

induce the homomorphisms

$$C^n(G/V, A^V) \to C^n(G/U, A^U) \to C^n(G, A)$$

which commute with the boundary maps δ hence we obtain homomorphisms

$$H^n(G/V, A^V) \to H^n(G/U, A^U) \to H^n(G, A)$$

Thus the cohomology groups $H^n(G/U, A^U)$ form a directed system and we get a canonical homomorphism

$$\varinjlim_{U} H^n(G/U, A^U) \to H^n(G, A)$$

and it turns out that this actually an isomorphism (see [32] page 22).

2.5 Functor of pairs (G, A)

A *morphism of pairs* $(G, A) \mapsto (G', A')$ is given by a pair of maps ϕ and f,

$$\begin{tikzcd} G & G' \arrow[l, "\phi"'] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} A_\phi \arrow[r, "f"] & A' \end{tikzcd} ,$$

where ϕ is a group homomorphism, f is a homomorphism of G'-modules, and A_ϕ means A with the G' action induced by ϕ. A morphism of pairs induces a map

$$H^r(G, A) \to H^r(G', A')$$

obtained by composing the map $H^r(G, A) \to H^r(G', A_\phi)$ induced by ϕ with the map $H^r(G', A_\phi) \to H^r(G', A')$ induced by f. We thus consider $H^r(G, A)$ as a functor of pairs (G, A).

If G' is a subgroup of G then there are maps

$$\begin{tikzcd} H^r(G, A) \arrow[r, shift left, "\text{restriction}"] & H^r(G', A). \arrow[l, shift left, "\text{corestriction}"] \end{tikzcd}$$

Here the corestriction map (also called the "transfer map") is defined only if the index $[G : G']$ is finite.

2.6 The inflation-restriction sequence

Let

$$(G,A) \to (G',A')$$

be a morphism of pairs , as in (2.4). In particular, we can take G' to be a subgroup H of G. We have three special instances of the above map:

1) restriction $H^r(G,A) \to H^r(H,A)$

2) inflation $H^r(G/H,A^H) \to H^r(G,A)$

(for $H \triangleleft G$, $G \to G/H$, $A^H \subset A$)

3) conjugation $H^r(H,A) \xrightarrow{\tilde{\sigma}} H^r(\sigma H \sigma^{-1},A)$, $\sigma \in G$

(for $\sigma h \sigma^{-1} \mapsto h$ and $a \mapsto \sigma a$)

We state the following theorem without proof

Theorem 2.1. If $\sigma \in H$, then the conjugation map $\tilde{\sigma}$ is the identity.

Proof. ([37] chap vii prop 3) □

Theorem 2.2. If H is a normal subgroup of G, then we have the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H^1(G/H,A^H) \arrow[r, "\mathrm{inf}"] & H^1(G,A) \arrow[r, "\mathrm{res}"] & H^1(H,A)^{G/H} \arrow[dll, rounded corners, "d"] \\
& H^2(G/H,A^H) \arrow[r, "\mathrm{inf}"] & H^2(G,A) &
\end{tikzcd}$$

Proof. We only give an outline of the proof. This comes from the "Hochschild-Serre" spectral sequence (see [35] pg 355)

$$E_2^{rs} = H^r(G/H, H^s(H,A)) \Rightarrow H^{r+s}(G,A)$$

By Theorem 2.1, G acts on $H^r(H,A)$ and H acts trivially, so this spectral sequence makes sense. (The profinite case follows immediately from the finite one by direct limit; see the end of Section 2.4.) The low dimensional corner of the spectral sequence can be pictured as follows.

$$\begin{tikzcd}
E^{02} \arrow[d, dash] \arrow[dr, dash] & & \\
E^{01} \arrow[d, dash] \arrow[dr, dash] & E^{11} \arrow[d, dash] \arrow[dr, dash] & \\
E^{00} \arrow[r, dash] & E^{10} \arrow[r, dash] & E^{20}
\end{tikzcd}$$

Inflation and restriction are "edge homomorphisms" in the spectral sequence. The lower left corner pictured above gives the obvious isomorphism $A^G \xrightarrow{\sim} (A^H)^{G/H}$, The map d is the "transgression" and is induced by $d_2 : E_2^{01} \to E_2^{20}$. □

2.7 Cohomological Dimension

Definition 2.7.1. The **cohomological dimension** $\mathbf{cd}(G)$ of a group G is the smallest integer n such that

$$H^q(G, A) = 0 \text{ for all } q > n$$

and all G-modules A. We set $\mathbf{cd}(G) = \infty$ if no such n exists

We will mostly deal with pro-p groups, that is inverse limits of finite p-groups. The cohomology of such groups is relatively simple, the second cohomology groups upwards vanish, i.e. the cohomological dimension of such groups is one. More is true, if a group G contains a free pro-p group then it necessarily has cohomological dimension one. (see [39])

2.8 Kummer theory

Let K^{sep} be a separable closure of a field K, and put $G_K = \text{Gal}(K^{\text{sep}}/K)$. Let $m \geq 1$ be an integer, μ_m be the group of m-th roots of unity in K^{sep} and assume that the image of m in K is nonzero. Associated to the exact sequence

$$0 \longrightarrow \mu_m \longrightarrow (K^{\text{sep}})^* \xrightarrow{m} (K^{\text{sep}})^* \longrightarrow 0,$$

we have a long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mu_m \cap K \arrow[r] & K^* \arrow[r, "m"] & K^* \arrow[dll, rounded corners] \\
 & H^1(G_K, \mu_m) \arrow[r] & H^1(G_K, (K^{\text{sep}})^*) = 0, &
\end{tikzcd}$$

The last equality is Hilbert Satz 90. Thus $H^1(G_K, \mu_m) \xrightarrow{\sim} K^*/(K^*)^m$.

Now assume that $\mu_m \subset K$. Then

$$H^1(G_K, \mu_m) = \text{Hom}_{\text{cont}}(G_K, \mu_m),$$

$$\Longrightarrow K^*/(K^*)^m \cong \text{Hom}_{\text{cont}}(G_K, \mu_m).$$

Now consider a Galois extension L/K where $G = \text{Gal}(L/K)$ is a finite abelian group killed by m. Since G is a quotient of $G_K = \text{Gal}(K^{\text{sep}}/K)$, we have a diagram

$$\begin{tikzcd}
K^*/(K^*)^m \arrow[r, "\cong"] & \text{Hom}_{\text{cont}}(G_K, \mu_m) \\
B \arrow[u, hook] \arrow[r, "\cong"] & \widehat{G} := \text{Hom}(G, \mu_m), \arrow[u, hook]
\end{tikzcd}$$

where B is the subgroup of $K^*/(K^*)^m$ corresponding to $\widehat{G}$.

CHAPTER III

Gamma Extensions of Number Fields

3.1 Structure of $\mathbb{Z}_p$ (Gamma) Extensions

In this section we present some background results, concerning the structure and ramification of $\mathbb{Z}_p$-extensions. These results will be constantly called upon in subsequent sections.

Definition 3.1.1. (Γ or $\mathbb{Z}_p$-extension) Let K be a finite extension $\mathbb{Q}$. Let K_∞ be a Galois extension of K such that $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the additive group of p-adic integers. We say in this case K_∞/K is a Γ-extension.

To give a Γ-extension is the same as giving a tower of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup_{n=0}^{\infty} K_n$$

such that the $\mathrm{Gal}(K_n/K_0)$ is cyclic of order p^n. We prove this claim in the next proposition. Note that we will also consistently use Γ^{p^n} when referring to the Galois group $\mathrm{Gal}(K_\infty/K_n)$ i.e. $\Gamma^{p^n} = \mathrm{Gal}(K_\infty/K_n)$.

Proposition 3.1.2. Let K_∞/K be an extension of fields, then K_∞/K is a Γ extension if and only if there exists

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup_{n=0}^{\infty} K_n$$

such that the $\mathrm{Gal}(K_n/K_0)$ is cyclic of order p^n.

Proof. Suppose that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ then by infinite Galois theory [30] the intermediate fields of K_∞/K correspond to the closed subgroups of $\mathrm{Gal}(K_\infty/K)$. Let $S \neq 0$ be a closed subgroup of $\mathbb{Z}_p$ and let $x \in S$ be of minimal valuation and that $v_p(x) = n$. Then the smallest closed subgroup of $\mathbb{Z}_p$ containing x is $p^n\mathbb{Z}$ hence $S \supset p^n\mathbb{Z}_p$. Let y be an arbitrary element of S then $y = p^m u$ where u is a unit. Hence $y = (p^{m-n}u)p^n$ and $m - n \geq 0$ by minimality of n. Therefore $y \in p^n\mathbb{Z}_p$ i.e. $S \subset p^n\mathbb{Z}_p$. Thus $S = p^n\mathbb{Z}_p$. Let K_n be the fixed field of S, then we have $\mathrm{Gal}(K_n/K_0) = \mathrm{Gal}(K_\infty/K_0)/\mathrm{Gal}(K_\infty/K_n) = \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Conversely if we have a tower of fields as above then

$$\mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(\bigcup K_n/K) = \varprojlim_n \mathrm{Gal}(K_n/K) = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

Thus K_∞/K is clearly a $\mathbb{Z}_p$-extension.

□

We now explain the ramification theory of the $\mathbb{Z}_p$-extension K_∞/K. We show that ramification in the extension K_∞/K only occurs above the prime p and that if we change the base field (moving up the tower of fields K_n), then for large enough n the extension K_∞/K_n is totally ramified. For archimedean primes v we have that the completion $K_v = \mathbb{C}$ or $\mathbb{R}$ hence $|(K_\infty)_\eta/K_v| \leq 2$ where η is a extension of v to K_∞. The inertia group of v is a closed subgroup of $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, hence must be trivial or infinite . Since $|(K_\infty)_\eta/K_v| \leq 2$ i.e finite, we conclude that no ramification occurs for archimedean primes

Proposition 3.1.3. Let K_∞/K be a $\mathbb{Z}_p$-extension and let v be a prime of K which does not lie above p. Then the extension K_∞/K is unramified at v.

Proof. Let $I_v \subseteq \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ be the inertia group of v. Since I_v is a closed subgroup of $\mathrm{Gal}(K_\infty/K)$, we have either $I_v = \{1\}$ or $I_v = p^n\mathbb{Z}_p$ for some n . If $I_v = \{1\}$ then we are done, so we assume $I_v = p^n\mathbb{Z}_p$. In particular I_v is infinite so v is a non-archimedean prime (since I_v must have order 1 or 2 for the infinite primes). Let $U_v(K)(p)$ be the p-units of K_v. By class field theory (see [31] page 299), I_v is the image of the continuous surjective homomorphism

$$U_v(K)(p) \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}(p) \twoheadrightarrow \mathrm{Gal}(K_\infty/K)$$

But $U_v(K)(p) = \mu(K_v)(p)$ is finite, hence $I_v = \{1\}$. □

Lemma 3.1.4. Let $\mathrm{Gal}(K_\infty/K)$ be a $\mathbb{Z}_p$-extension. At least one prime ramifies in this extension, and there exists $n \geq 0$ such that every prime which ramifies in K_∞/K_n is totally ramified.

Proof. If all primes were unramified in K_∞/K then K_∞ would be contained in the maximal unramified abelian extension of K. The Galois group of the maximal unramified abelian extension of K can (using class field theory) be identified with the ideal class group of K which is finite. Hence we obtain a contradiction since $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Therefore some prime must ramify in K_∞/K. By proposition 3.1.3 we know only finitely many primes ramify in K_∞/K, namely those above p. Let these primes then be $p_1, \ldots p_s$ and let $I_1, \ldots I_s$ be their corresponding inertia groups. Then $\bigcap I_j = p^n\mathbb{Z}_p$ for some n. Now the fixed field of $p^n\mathbb{Z}_p$ is K_n and $\mathrm{Gal}(K_\infty/K_n)$ is contained in each I_j. Therefore all the primes above each p_j are totally ramified in K_∞/K_n, and the proof is complete. □

CHAPTER IV

Iwasawa Modules

4.1 Classification of Iwasawa Modules up to Pseudo-isomorphism

In this section we classify modules over a commutative, noetherian and integrally closed domain up to pseudo-isomorphism. We show that up to pseudo-isomorphism there is a nice decomposition of these modules akin to that of modules over a principal ideal domain. Our primary interest however is in modules over the Iwasawa algebra. In the next section we specialize to these particular modules and show that certain natural quotients of Iwasawa modules have nice asymptotic order behavior.

Let A be a commutative, noetherian and integrally closed domain with quotient field K. For every prime ideal $\mathfrak{p}$ in A, one has a canonical embedding of the localisation $A_\mathfrak{p} \hookrightarrow K$ and $A_\mathfrak{p}$ is integrally closed.

Let $\boldsymbol{P(A)}$ be the set of prime ideals of height $\mathrm{ht}(\mathfrak{p}) = \dim A_\mathfrak{p} = 1$. Since A is integrally closed, the localisation $A_\mathfrak{p}$ is a discrete valuation ring and

$$A = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} A_\mathfrak{p}$$

(see [5] chap VII).

Definition 4.1.1. An A-module M is called *reflexive* if the canonical map

$$\varphi_M \colon M \to M^{**} = \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$$

$$m \longrightarrow \varphi_M(m) \colon \alpha \longrightarrow \alpha(m)$$

of M to its bidual is an isomorphism.

If M be a finitely generated torsion-free A-module we define $V := M \otimes_A K$ and $V^\wedge = \mathrm{Hom}(M, K)$. We naturally have the injections

$$M \hookrightarrow M_\mathfrak{p} \hookrightarrow M_\mathfrak{p} \otimes_{A_\mathfrak{p}} K = M \otimes_A K = V$$

$$M^* \hookrightarrow M_\mathfrak{p}^* \hookrightarrow M_\mathfrak{p}^* \otimes_{A_\mathfrak{p}} K = M^* \otimes_{A_\mathfrak{p}} K = \mathrm{Hom}_K(V, K) = V^\wedge$$

Hence we see that

$$M* \cong \{\lambda \in V^\wedge \mid \lambda(m) \in A \text{ for all } m \in M\}$$

$$M_\mathfrak{p}^* \cong \{\lambda \in V^\wedge \mid \lambda(m) \in A_\mathfrak{p} \text{ for all } m \in M_\mathfrak{p}\}$$

Theorem 4.1.2. Let M be a finitely generated torsion-free A-module then

(i) $M^* = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}^*$.

(ii) $M^{**} = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}$.

(iii) $M = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}$ if and only if M is reflexive.

Proof. (i) Clearly $M^* \subset M_\mathfrak{p}^*$ for all $\mathfrak{p} \in \boldsymbol{P(A)}$, hence $M^* \subset \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}^*$. For the other inclusion let $\lambda \in \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}^*$. Then for every $m \in M$ we get $\lambda(m) \in A_\mathfrak{p}$ for all $\mathfrak{p} \in \boldsymbol{P(A)}$, hence $\lambda(m) \in A$, therefore $\lambda \in M^*$ and this proves our result.

(ii) $M_\mathfrak{p}$ is a finitely generated torsion-free module over the discrete valuation ring $A_\mathfrak{p}$, $\mathfrak{p} \in \boldsymbol{P(A)}$, hence $M_\mathfrak{p}$ is free and $M_\mathfrak{p} \longrightarrow M_\mathfrak{p}^{**}$ is an isomorphism. By (i) we have $(M^*)^* = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} (M^*{}_\mathfrak{p})^*$, therefore $(M^*)^* = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} (M_\mathfrak{p})^{**} = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}$.

(iii) If $M = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}$ then by (ii) $M = M^{**}$ hence M is reflexive. If M is reflexive then by (ii) $M = M^{**} = \bigcap_{\mathfrak{p} \in \boldsymbol{P(A)}} M_\mathfrak{p}$

□

We have the following immediate consequence.

Corollary 4.1.3. If M is a finitely generated torsion-free A-module them M^* is a reflexive module.

For our purposes the important fact is that certain reflexive modules are free.

Definition 4.1.4. A *regular local* ring is a local ring A with maximal ideal $\mathfrak{m}$ so that $\mathfrak{m}$ can be generated with exactly d elements where d is the Krull dimension of the ring A. Equivalently, A is regular if the vector space $\mathfrak{m}/\mathfrak{m}^2$ has dimension d. Let A be a regular local ring, a *regular system of parameters* is a sequence $x_1, \cdots, x_n$ with $x_i \in \mathfrak{m}$ such that $A/(x_1, \cdots, x_n)$ has dimension zero.

Proposition 4.1.5. let A be an 2-dimensional regular local ring, and let (p_1, p_2) be a regular system of parameters generating the maximal ideal of A. For a finitely generated A-module M, the following assertions are equivalent.

(i) M is a reflexive A-module.

(ii) M is a free A module

Proof. [9] [32] The implication (ii) → (i) is easy so we only show the nontrivial implication. We assume (i) is true, in particular M is reflexive, hence torsion-free. Therefore multiplication by p_1 is injective on M. If $\varphi\colon A^r \twoheadrightarrow M$ is a minimal free presentation of M, we obtain the following commutative exact diagram.

$$\begin{tikzcd}
0 \arrow[r] & A^r \arrow[r, "p_1"] \arrow[d, "\varphi"] & A^r \arrow[r] \arrow[d, "\varphi"] & (A/p_1)^r \arrow[r] \arrow[d, "\bar{\varphi}"] & 0 \\
0 \arrow[r] & M \arrow[r, "p_1"] & M \arrow[r] & M/p_1 \arrow[r] & 0
\end{tikzcd}$$

If we now assume that M/p_1 is a free A/p_1-module, then by the snake lemma $\operatorname{corker}(\bar{\varphi}) = 0$ and we also have the exact sequence

$$0 \longrightarrow \ker(\bar{\varphi}) \xrightarrow{p_1} (A/p_1)^r \longrightarrow M/p_1 \longrightarrow 0.$$

Applying $\mathrm{Tor}_n^{A/p_1}(-, A/\mathfrak{m})$ we obtain

$$\mathrm{Tor}_1^A(M/p_1, A/\mathfrak{m}) \longrightarrow \ker(\bar{\varphi}) \otimes A/\mathfrak{m} \xrightarrow{p_1} (A/p_1)^r \otimes A/\mathfrak{m} \longrightarrow M/p_1 \otimes A/\mathfrak{m} \longrightarrow 0$$

Since M/p_1 is a free A/p_1-module the first term vanishes i.e. M/p_1 is flat. The map $\bar{\varphi}$ induces the map $\bar{\varphi} : (A/p_1)^r \otimes A/\mathfrak{m} \to M/p_1 \otimes A/\mathfrak{m}$. We study the kernel of this map i.e. $\ker(\bar{\varphi}) \otimes A/\mathfrak{m}$. Now $(A/p_1)^r \otimes A/\mathfrak{m} \cong ((A/p_1)/\mathfrak{m}(A/p_1))^r$ and $M/p_1 \otimes A/\mathfrak{m} \cong (M/p_1)/\mathfrak{m}(M/p_1)$. $((A/p_1)/\mathfrak{m}(A/p_1))^r$ is a vector space of dimension r over $((A/p_1)/\mathfrak{m}(A/p_1))$ and $(M/p_1)/\mathfrak{m}(M/p_1)$ is also a vector space over $(A/p_1)/\mathfrak{m}(A/p_1)$. By minimality of the presentation, $(M/p_1)/\mathfrak{m}(M/p_1)$ is also of dimension r, thus $\ker(\bar{\varphi}) \otimes A/\mathfrak{m} = 0$ which implies

$$\ker(\bar{\varphi}) \otimes A/\mathfrak{m} = \ker(\bar{\varphi})/\mathfrak{m}\ker(\bar{\varphi}) = 0.$$

Hence by Nakayama's lemma $\ker(\bar{\varphi}) = 0$ i.e. $\bar{\varphi}$ is an isomorphism. By the snake lemma applied to the commutative diagram above, we have that multiplication by p_1 on $\ker(\varphi)$ is an isomorphism. But $p_1 \in \mathfrak{m}$ therefore $p_1\ker(\varphi) \subseteq \mathfrak{m}\ker(\varphi)$ which implies

$$\ker(\varphi) = p_1\ker(\varphi) \subseteq \mathfrak{m}\ker(\varphi).$$

Again by Nakayama's lemma we obtain $\ker(\varphi) = 0$. Therefore φ is an isomorphism and M is a free A-module.

It remains to show that M/p_1 is a free A/p_1-module. A/p_1 is regular of dimension 1 (i.e. a discrete valuation ring), therefore A/p_1 is also an integral domain (see [27] page 106), which implies that the A/p_1-module $\mathrm{Hom}(M^*, A/p_1)$ is torsion-free. Since A is an integral domain, the map

$$M^{**}/p_1 = \mathrm{Hom}_A(M^*, A) \otimes A/p_1 \hookrightarrow \mathrm{Hom}_A(M^*, A/p_1),$$

is injective. Since M is reflexive, $M/p_1 = M^{**}/p_1$ is a torsion-free module over the discrete valuation ring A/p_1. Therefore M/p_1 is a free A/p_1-module. This completes our proof. □

Definition 4.1.6. A finitely generated A-module is called **pseudo-null** if the following equivalent conditions hold.

(i) $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ in A of height $\mathrm{ht}(\mathfrak{p}) \leq 1$.

(ii) If $\mathfrak{p}$ is a prime ideal with $\mathfrak{a} = \mathrm{ann}_A(M) \subseteq \mathfrak{p}$ then $\mathrm{ht}(\mathfrak{p}) \geq 2$

The above equivalence is clear since $M_{\mathfrak{p}} = 0$ if and only if there is an $s \in A \setminus \mathfrak{p}$ such that $sM = 0$, hence $\mathrm{ann}_A(M) \nsubseteq \mathfrak{p}$.

In the case that A is a 2-dimensional, noetherian, integrally closed, local domain with finite residue field the **pseudo-null** modules are just the finite modules. Indeed if M is finite then there exists an $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$, hence $\mathrm{supp}(M) \subseteq \{\mathfrak{m}\}$. Conversely if $\mathrm{supp}(M) = \{\mathfrak{p} \in \mathrm{SpecA} | \mathfrak{a} \subseteq \mathfrak{p}\} \subset \{\mathfrak{m}\}$, then $\mathfrak{m}^r \subset \mathfrak{a}$ for some $r \in \mathbb{N}$ and M is a finitely generated $A/\mathfrak{m}^r$-module. But $A/\mathfrak{m}^r$ is finite hence M is finite as well.

Definition 4.1.7. A homomorphism $f\colon M \to N$ of finitely generated A-modules is called a **pseudo-isomorphism** if $\ker(f)$ and $\mathrm{coker}(f)$ are pseudo-null or equivalently if

$$f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \xrightarrow{\sim} N_{\mathfrak{p}}\,,$$

is an isomorphism for all $\mathfrak{p}$ of height ≤ 1. We write

$$f\colon M \xrightarrow{\approx} N\,.$$

Proposition 4.1.8. Let M be a finitely generated torsion-free A-module. Then there exists an injective pseudo-isomorphism of M into a reflexive A-module M'

Proof. Consider the canonical morphism

$$\varphi_M \colon M \to M^{**}.$$

Localizing at the prime ideal $\mathfrak{p}$ of height 1, we obtain $A_{\mathfrak{p}}$ which is a discrete valuation ring hence $M_{\mathfrak{p}}$ is a free finitely generated $A_{\mathfrak{p}}$-module. Therefore the map $M_{\mathfrak{p}} \to M_{\mathfrak{p}}^{**}$ is an isomorphism for all $\mathfrak{p}$ of height ≤ 1. The map φ_M is thus a pseudo-isomorphism. Since M is finitely generated, M^* is also finitely generated. Hence by corollary 4.1.3 M^{**} is reflexive. Let K be the quotient field of A, then since φ_M is a pseudo-isomorphism, when we localize with the zero ideal (0), we obtain $\ker(\varphi_M)_{(0)} = \ker(\varphi_M) \otimes_A K = 0$. Therefore $\ker(\varphi_M)$ is torsion, and since M is torsion-free we have $\ker(\varphi_M) = 0$. □

Lemma 4.1.9. Let M be a finitely generated torsion A-module and let $\alpha \in A$ be a non zero element such that $\operatorname{supp}(A/\alpha A)$ is disjoint to $\operatorname{supp}(M) \cap \mathbf{P(A)}$. Then multiplication on M by α is a pseudo-isomorphism.

Proof. Let $\alpha \in A$ such that $\operatorname{supp}(A/\alpha A)$ is disjoint to $\operatorname{supp}(M) \cap \ \mathbf{P(A)}$. Consider the multiplication by α map

$$\alpha \colon M \to M.$$

Localizing at $\mathfrak{p} \in \ \mathbf{P(A)}$ we have the map

$$\alpha_{\mathfrak{p}} \colon M_{\mathfrak{p}} \to M_{\mathfrak{p}}.$$

Since $\operatorname{supp}(A/\alpha A)$ is disjoint to $\operatorname{supp}(M) \cap \ \mathbf{P(A)}$, for $\mathfrak{p} \in \operatorname{supp}(M) \cap \mathbf{P(A)}$ we then obtain

$$(A/\alpha A)_{\mathfrak{p}} = A_{\mathfrak{p}}/\alpha A_{\mathfrak{p}} = 0,$$

hence α is a unit in $A_{\mathfrak{p}}$, hence the map $\alpha_{\mathfrak{p}}$ is an isomorphism on localization by height 1 prime ideals, thus α is a pseudo-isomorphism.

□

For a finitely generated A-module M, let $T_A(M)$ be the torsion submodule and $F_A(M)$ be the maximal torsion free quotient of M .

Proposition 4.1.10. If the A-module M is finitely generated, then

(i) there exists a pseudo-isomorphism

$$f\colon M \xrightarrow{\approx} T_A(M) \oplus F_A(M)\ .$$

(ii) there exists a finite family $\{\mathfrak{p}_i\}_{i\in I}$ of prime ideals of height 1 in A, a finite family $\{n_i\}_{i\in I}$ of natural numbers and a pseudo-isomorphism

$$g\colon T_A(M) \xrightarrow{\approx} \bigoplus_{i\in I} A/{\mathfrak{p}_i}^{n_i}\ .$$

The families $\{\mathfrak{p}_i\}$ and $\{n_i\}$ are uniquely determined by $T_A(M)$ up to reordering.

Proof. Let $\{p_1, \ldots, p_h\} = \text{supp}(M) \bigcap \boldsymbol{P(A)}$. If $h = 0$ then $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \boldsymbol{P(A)}$, then $T_A(M)$ is pseudo-null. The following maps

$$f\colon M \xrightarrow{can} F_A(M)\ ,$$

and

$$g\colon T_A(M) \xrightarrow{\approx} 0\ ,$$

satisfy the requirements of the theorem. Now let $h > 0$ and consider $S = \bigcap_{i=1}^{h} A/\mathfrak{p}_i = A \backslash \bigcup_{i=1}^{h} \mathfrak{p}_i$. $S^{-1}A$ is a semi-local Dedekind domain (the only primes are the ones that contain $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$) and therefore a principal ideal domain. $S^{-1}M$ is a module over $S^{-1}A$ and $S^{-1}T_A(M)$ is its torsion submodule. By the well known structure theorem for modules over a principal ideal domain $S^{-1}T_A(M)$ is a direct summand of $S^{-1}M$. Since M is also finitely generated, we have

$$\text{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}T_A(M)) = S^{-1}\text{Hom}_A(M, T_A(M)).$$

Hence there exists a morphism $f_0 \colon M \to T_A(M)$ and $s_0 \in S$ such that

$$\frac{f_0}{s_0} : S^{-1}M \to S^{-1}T_A(M),$$

is the projector of $S^{-1}M$ onto its direct summand $S^{-1}T_A(M)$. Therefore $\frac{f_0}{s_0}$ is the identity on $S^{-1}T_A(M)$ and thus there exists an $s_1 \in S$ such that for $f_1 = s_1 f_0$

$$f_1|_{T_A(M)} = s_1 s_0 id_{T_A(M)}.$$

Now let

$$f = (f_1, \mathrm{can}) \colon M \to T_A(M) \oplus F_A(M)$$

and consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & T_A(M) \arrow[r] \arrow[d, "f_1|_{T_A(M)}"] & M \arrow[r] \arrow[d, "f"] & F_A(M) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & T_A(M) \arrow[r] & T_A(M) \oplus F_A(M) \arrow[r] & F_A(M) \arrow[r] & 0
\end{tikzcd}$$

The snake lemma shows that $\ker(f) = \ker(f_1|_{T_A(M)})$ and $\mathrm{coker}(f) = \mathrm{coker}(f_1|_{T_A(M)})$. But $f_1|_{S^{-1}T_A(M)}$ is a map between two torsion A-modules and it is multiplication by a unit of S, hence by lemma 4.1.9 it is a pseudo-isomorphism. This proves (i).

In order to prove (ii) let

$$E := \bigoplus_{i=1}^{h} \bigoplus_{j=1}^{r_i} A/\mathfrak{p}_i^{n_{ij}}.$$

for natural numbers n_{ij} such that there exists an isomorphism

$$g_0 \colon S^{-1}T_A(M) \xrightarrow{\sim} S^{-1}E.$$

Again $S^{-1}A$ is a semilocal ring with maximal ideals $S^{-1}\mathfrak{p}_i$, $i = 1, \ldots, n$. Consider

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}T_A(M), S^{-1}E) = S^{-1}\mathrm{Hom}_A(T_A(M), E).$$

We obtain a morphism $g \colon T_A(M) \to E$ and an $s \in S$ such that $g = sg_0$. Again by lemma 4.1.9 we see that g is a pseudo-isomorphism . □

Theorem 4.1.11. Let A be a 2-dimensional regular local ring and let M be a finitely generated A-module. Then there exist finitely many height 1 prime ideals $\mathfrak{p}_i$, $i \in I$, a non-negative integer r, natural numbers n_i and a pseudo-isomorphism.

$$f \colon M \xrightarrow{\approx} A^r \oplus \bigoplus_{i \in I} A/\mathfrak{p}_i{}^{n_i} .$$

The prime ideals $\mathfrak{p}_i$ and the numbers r and n_i are uniquely determined by M,

$$r = \dim_K M \otimes_A K \text{ and } \{\mathfrak{p}_i | i \in I\} = \operatorname{supp}(M) \cap \mathbf{P(A)}.$$

Proof. By proposition 4.1.10(i) we have a pseudo-isomorphism

$$f \colon M \xrightarrow{\approx} T_A(M) \oplus F_A(M) .$$

and by proposition 4.1.10(ii) we have a pseudo-isomorphism

$$g \colon T_A(M) \xrightarrow{\approx} \bigoplus_{i \in I} A/\mathfrak{p}_i{}^{n_i} .$$

Now by proposition 4.1.8, $F_A(M)$ is pseudo-isomorphic to a reflexive module M', and since A is 2-dimensional regular local ring we have by proposition 4.1.5 that M' is free. Hence $F_A(M)$ is pseudo-isomorphism to a free module A^r. Putting this together we have proved that there is a pseudo-isomorphism

$$f \colon M \xrightarrow{\approx} A^r \oplus \bigoplus_{i \in I} A/\mathfrak{p}_i{}^{n_i} .$$

□

4.2 Iwasawa Modules

We denote by Γ a group non canonically isomorphic to $\mathbb{Z}_p$. This means we will not specify a particular isomorphism $\phi \colon \Gamma \cong \mathbb{Z}_p$

Definition 4.2.1. The **Iwasawa Algebra** is the complete group ring

$$\Lambda = \varprojlim_{n} \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]] = \mathbb{Z}_p[[\Gamma]].$$

We define an Iwasawa module to be a compact Λ-module.

We will see that by choosing a topological generator γ of Γ, the Iwasawa algebra can be identified with the power series ring $\mathbb{Z}_p[[T]]$. This is a local ring with maximal ideal (p, T). We state the next crucial lemma without proof. (see [5] chap III for a proof).

Lemma 4.2.2. **(Division Lemma)** Let $f = \sum_{n=0}^{\infty} a_n T^n \in \mathbb{Z}_p[[T]]$ and let $s: = \inf\{ n \mid p \nmid a_n\}$ be finite (s is the **reduced degree** of f). Then every $g \in \mathbb{Z}_p[[T]]$ can be written uniquely as

$$g = fq + r$$

with $q \in \mathbb{Z}_p[[T]]$ and a polynomial $r \in \mathbb{Z}_p[T]$ of degree $\leq s - 1$. In particular $\mathbb{Z}_p[[T]]/(f)$ is free $\mathbb{Z}_p$-module of rank s with basis $\{T^i \mod f | i = 0, \ldots, s-1\}$.

Definition 4.2.3. A polynomial $F \in \mathbb{Z}_p[T]$ is called a **Weierstraß polynomial** if it is of the form

$$F = T^s + a_{s-1}T^{s-1} + \ldots + a_1 T + a_0$$

and the coefficients $a_0, \ldots, a_{s-1}$ are divisible by p.

Corollary 4.2.4. Let F be Weierstraß polynomial. Then the injection

$$\mathbb{Z}_p[T] \hookrightarrow \mathbb{Z}_p[[T]],$$

induces an isomorphism

$$\mathbb{Z}_p[T]/F\mathbb{Z}_p[T] \to \mathbb{Z}_p[[T]]/F\mathbb{Z}_p[[T]].$$

Proof. Let $s = \deg(F)$ (the reduced degree of F). By the division lemma (4.2.2) we have a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}_p[T]/(F) \arrow[rr] \arrow[dr, "\sim"] & & \mathbb{Z}_p[[T]]/(F) \arrow[dl, "\sim"'] \\
& \sum_{i=0}^{s-1} T^i \mathbb{Z}_p &
\end{tikzcd}$$

which gives the result. □

Theorem 4.2.5. (**Weierstraß Preparation Theorem**) Let $f \in \mathbb{Z}_p[[T]]$ with finite reduced degree s. Then there exists a unique decomposition

$$f = F \cdot u$$

into a Weierstraß polynomial F of degree s and a unit $u \in \mathbb{Z}_p[[T]]$. Furthermore F is the characteristic polynomial of the endomorphism on the free $\mathbb{Z}_p$-module $\mathbb{Z}_p[[T]]/(f)$ given by multiplication by T.

Proof. By the division lemma 4.2.2. There exists a unique $v \in \mathbb{Z}_p[[T]]$ and unique polynomial $G = \sum_{i=0}^{s-1} a_i T^i$, such that

$$T^s = f \cdot v - G.$$

Since f has reduced degree s and

$$\overline{f} \cdot \overline{v} = T^s + \overline{a}_{s-1} T^{s-1} + \cdots + \overline{a}_0$$

(here $^-$denotes reduction $\mod p$), it follows that $\overline{a}_i = 0$ for all $i = 0, \ldots, s-1$, and $\deg(\overline{v}) = 0$, Therefore $v \in \mathbb{Z}_p[[T]]^\times$ and $F = T^s + G$ is a Weiersraß polynomial. By corollary 4.2.4,

$$\mathbb{Z}_p[[T]]/(f) = \mathbb{Z}_p[[T]]/(F) \cong \mathbb{Z}_p[T]/(F).$$

Hence F is the characteristic polynomial of multiplication by T, this proves the last assertion.

□

Now let $p = \mathrm{char}(\mathbb{Z}_p/p\mathbb{Z}_p)$, also let Γ be a multiplicative group (non-canonically) isomorphic to the additive group $\mathbb{Z}_p$ and let Γ^{p^n} be the unique subgroup of Γ of index p^n.

Proposition 4.2.6. Let γ be a topological generator of $\Gamma \cong \mathbb{Z}_p$. Then the map

$$\mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p[[\Gamma]] = \varprojlim_n \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]]$$

$$T \rightarrow \gamma - 1$$

is an isomorphism of topological $\mathbb{Z}_p$-algebras.

Proof. Consider the Weierstraß polynomials

$$\omega_n = (1+T)^{p^n} - 1 = T^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} T^{p^n-i} \text{ , } n \geq 0.$$

By corollary 4.2.4

$$\mathbb{Z}_p[[T]]/(\omega_n) \cong \mathbb{Z}_p[T]/(\omega_n)$$

Now consider the map

$$\mathbb{Z}_p[T]/(\omega_n) \longrightarrow \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]] \text{ given by}$$

$$T \mod \omega_n \mapsto \gamma - 1 \mod \Gamma^{p^n}.$$

This map is an isomorphism of $\mathbb{Z}_p$-algebras with inverse

$$\gamma \mod \Gamma^{p^n} \mapsto T + 1 \mod \omega_n.$$

Since

$$\omega_{n+1} = \omega_n((T+1)^{p^n(p-1)} + \cdots + (T+1)^{p^n} + 1)$$

we obtain a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}_p[[T]]/(\omega_{n+1}) \arrow[r, "\sim"] \arrow[d] & \mathbb{Z}_p[[\Gamma/\Gamma^{p^{n+1}}]] \arrow[d] \\
\mathbb{Z}_p[[T]]/(\omega_n) \arrow[r, "\sim"] & \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]]
\end{tikzcd}$$

and hence an isomorphism

$$\varprojlim_n \mathbb{Z}_p[[T]]/(\omega_n) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]] = \mathbb{Z}_p[[\Gamma]] \ .$$

Finally the natural homomorphism

$$\mathbb{Z}_p[[T]] \to \varprojlim_n \mathbb{Z}_p[[T]]/(\omega_n),$$

is an isomorphism. Indeed since $\mathbb{Z}_p[[T]]$ is compact and its image is dense, it is therefore surjective. The inclusion $\omega_n \mathbb{Z}_p[[T]] \subseteq (p,T)^{n+1}$ implies that $\bigcap_n \omega_n \mathbb{Z}_p[[T]] \subseteq \bigcap_n (p,T)^{n+1} = \{0\}$ so the kernel is zero. □

In what follows we fix a topological generator γ of Γ and then identify $\mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[T]]$.

Lemma 4.2.7. The prime ideals of height 1 in Λ are

$$(p) \text{ and } (F)$$

where F is an irreducible Weierstraß polynomial over $\mathbb{Z}_p$.

Proof. Since $\mathbb{Z}_p[[T]]$ is a factorial ring, the prime ideals of height 1 are of the form $\mathfrak{p} = (f)$ where f is a irreducible element in Λ. If $(f) \neq (p)$, then the reduced element $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[[T]]$ is not trivial, and by the Weierstraß preparation theorem 4.2.5, $(f) = (F)$ where F is an irreducible Weierstraß polynomial over $\mathbb{Z}_p$. But a polynomial is irreducible over $\mathbb{Z}_p[[T]]$ if and only if it is irreducible over $\mathbb{Z}_p[T]$ (see [5] chap VII). □

We recall the definition of the **Iwasawa Algebra**, it is the complete group ring

$$\Lambda = \varprojlim_{n} \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]] = \mathbb{Z}_p[[\Gamma]],$$

and we define an Iwasawa module to be a compact Λ-module. Applying the Structure Theorem 4.1.11 from the previous section and using propositions 4.2.6 and the comments made after definition 4.1.6 we obtain the following

Theorem 4.2.8. **(Structure theorem for Iwasawa modules**) Let M be a finitely generated Iwasawa module. Then there is a pseudo-isomorphism

$$M \xrightarrow{\approx} \Lambda^r \oplus \bigoplus_{i=1}^{r} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{s} \Lambda/F_j(T)^{n_j}$$

with finite kernel and cokernel. The F_j are irreducible Weierstraß polynomials, and the numbers r, m_i, n_j and the prime ideals $F_j\Lambda$ are uniquely determined by M .

From the decomposition above we make the following definitions

$$\begin{aligned} r(M) &= \mathrm{rank}_\Lambda(M) \text{ the } \boldsymbol{\Lambda}\textbf{-rank} \text{ of M} \\ \mu(M) &= \sum_{i=1}^{r} m_i \text{ the } \textbf{Iwasawa} - \mu \textbf{ invariant } \text{ of M} \\ \lambda(M) &= \sum_{j=1}^{s} n_j deg(F_j) \text{ the } \textbf{Iwasawa} - \lambda \textbf{ invariant } \text{ of M} \\ F_M &= \prod_{j=1}^{s} F_j^{n_j} \text{ the } \textbf{Iwasawa polynomial } \text{ of M} \end{aligned}$$

To determine whether a Λ-module X is finitely generated, the following result is crucial.

Lemma 4.2.9 (Topological Nakayama Lemma). Let Λ be a compact topological ring and let X be a compact Λ-module. Let $\mathfrak{m}$ denote the maximal ideal of Λ then,

(i) If $\mathfrak{m}X = X$ then $X = 0$;

(ii) X is finitely generated over Λ if and only if $X/\mathfrak{m}X$ is a finitely generated $\Lambda/\mathfrak{m}\Lambda$-module. Furthermore if $\{x_1, \ldots, x_n\}$ generates $X/\mathfrak{m}X$ over $\mathbb{Z}$ then they generate X as a Λ-module.

(iii) If X/TX is finite then X is a finitely generated torsion Λ-module.

Proof. (i) Let U be a small neighbourhood of 0 in X. Since $\mathfrak{m}^n \to 0$ in Λ, for each $z \in X$, there exists a neighbourhood U_z of z such that $\mathfrak{m}^n U_z \subset U$. X is a compact Λ-module hence only finitely many U_z cover X, thus $\mathfrak{m}^n X \subset U$ for large n. Since X is compact and $\mathfrak{m}X = X$ we obtain

$$X = \bigcap \mathfrak{m}^n X = 0, \tag{4.1}$$

for the compact Λ-module X.

(ii) We only prove the nontrivial implication.

If $\{x_1, \ldots, x_n\}$ generate $X/\mathfrak{m}X$ as a vector space over $\Lambda/\mathfrak{m}\Lambda$, let

$$Y = \bigoplus_{i=1}^{n} \Lambda x_i \subseteq X.$$

Y is the image of the compact Λ-module Λ^n, under the map

$$\Lambda^n \xrightarrow{\phi} \bigoplus \Lambda x_i.$$

Y is thus a closed subset of X hence X/Y is a compact Λ-module. Since $\{x_1, \ldots, x_n\}$ generates $X/\mathfrak{m}X$ we have

$$Y + \mathfrak{m}X = X,$$

hence that

$$X/Y = (Y + \mathfrak{m}X)/Y = \mathfrak{m}(X/Y).$$

We therefore obtain $\mathfrak{m}^n(X/Y) = X/Y$ for all $n \geq 0$. By (i) we have $X/Y = 0$. Thus $\{x_1, \ldots, x_n\}$ generates X, and X is finitely generated as a Λ-module.

(iii) Since X is finitely generated by the x_i, let m be the exponent of the finite p-group X/TX. We have,

$$p^m x_i = T(\Sigma_{j=1}^n \lambda_{ij} x_j)$$

for some $\lambda_{ij} \in \Lambda$. Therefore $M\underline{x} = \underline{0}$ where M is the matrix $[T\lambda_{ij}] - p^m I$ and $\underline{x} = (x_1, \cdots, x_n)$. From this we obtain (by multiplying by the adjoint of M),

$$\text{Adj}(M)M\underline{x} = \det(M)\underline{x} = \underline{0}.$$

Let $g(T) = \det(M)$, now $g(T)$ is a nonzero element of Λ, since $g(0) = p^{nm}$, hence $g(T)$ annihilates X, since it annihilates the generators of X, which shows that X is a torsion Λ-module.

□

One classical feature of Iwasawa theory is the description of the asymptotic order of certain quotients of Iwasawa modules an n grows large. We present this description below. It will be of utmost importance in the coming chapters.

Definition 4.2.10. For $n \geq 0$ we denote the p^n-th cyclotomic polynomial by

$$\xi_n = \frac{\omega_n}{\omega_{n-1}}$$

where we put $\omega_{-1} = 1$ and $\omega_n = (T+1)^{p^n} - 1$.

We can expand the the expression for ω_n, we obtain

$$\omega_n = (T+1)^{p^n} - 1 = T^{p^n} + \sum_{i=1}^{p^n-1} \binom{p^n}{i} T^{p^n-i} \text{ , } n \geq 0.$$

hence

$$\omega_n = \xi_0 \cdot \xi_1 \cdot \ldots \xi_n \text{ and } \xi_0 = \omega_0 = T \text{ , } \xi_k = \sum_{i=0}^{p-1} (1+T)^{ip^{k-1}} \text{ for } k \geq 1.$$

Lemma 4.2.11. Let M be a finitely generated Λ-torsion module which is free of rank λ as a $\mathbb{Z}_p$-module. Then

$$\xi_n M = \frac{\omega_{n+1}}{\omega_n} M = pM \text{ for } n \geq \frac{\lambda(\lambda-1)}{2}.$$

Proof. The endomorphism on $M \otimes_{\mathbb{Z}_p} \mathbb{F}_p \cong \mathbb{F}_p^\lambda$ given by multiplication by T has the characteristic polynomial T^λ (see theorem 4.2.5). Hence T is nilpotent. If we choose a suitable basis for $M \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ the matrix representing the action of $\gamma = T + 1$ is of the form

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \dots & \dots & \dots & * \\ 0 & 0 & \dots & 1 \end{pmatrix} \in GL(\lambda, \mathbb{F}_p)$$

hence is contained in a p-sylow subgroup of $GL(\lambda, \mathbb{F}_p)$. Now $\#GL(\lambda, \mathbb{F}_p) = p^{\frac{\lambda(\lambda-1)}{2}} \prod_{i=1}^{\lambda}(p^i - 1)$, hence the p-sylow subgroup is of order $p^{\frac{\lambda(\lambda-1)}{2}}$ and is generated by the unipotent matrices. Therefore $\gamma^{p^n} = 1$ on $M \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ for $n \geq \frac{\lambda(\lambda-1)}{2}$. Let $A \in M(\lambda \times \lambda, \mathbb{Z}_p)$ be the matrix corresponding to the action of γ on M with respect to some basis, then

$$\begin{aligned} A^{p^n} &\equiv I \mod p \\ &\equiv I + pB \mod p^2 \text{ for some } B \in M(\lambda \times \lambda, \mathbb{Z}_p) \end{aligned}$$

where I denotes the unit matrix. It follows that

$$\begin{aligned} A^{p^n(p-1)} + \cdots + A^{p^n} + I &\equiv pI + ((p-1) + \cdots 1)pB \mod p^2 \\ &\equiv pI \mod p^2 \text{ for odd } p \end{aligned}$$

so that

$$A^{p^n(p-1)} + \cdots + A^{p^n} + I = pU \text{ with } U \in GL(\lambda, \mathbb{F}_p).$$

Therefore

$$\xi_{n+1} M = (\gamma^{p^n(p-1)} + \cdots + \gamma^{p^n} + 1)M = pM.$$

□

Definition 4.2.12. Let M be a Λ-module. Let M^δ denote the maximal Λ-submodule on which Γ acts discretely : i.e.

$$M^\delta = \bigcup_n M^{\Gamma_n}.$$

Let $M_0 = \mathrm{tor}_{\mathbb{Z}_p} M^\delta$ and if $M^\delta/M_0 \neq 0$ let $d = d(M)$ be the minimum number such that Γ_d acts trivially on M^δ/M_0.

Let $n \geq n_0 \geq d(M)$ and define

$$\begin{aligned}\nu_n &= \frac{\omega_n}{\omega_{n_0}} = \xi_{n_0+1} \cdots \xi_n \\ &= 1 + (1+T)^{p^{n_0}} + \cdots + (1+T)^{p^{n_0}(p^{n-n_0}-1)}.\end{aligned}$$

Lemma 4.2.13. (i) Let M be finitely generated Λ-module then, M_0 is the maximal finite submodule of M.

(ii) Let M be finitely generated torsion Λ-module then, for $n \geq n_0$, $\mathrm{supp}(M/\nu_n M)$ is disjoint to $\mathrm{supp}(M) \cap$ $\mathbf{P(A)}$.

(iii) The map $\nu_n : M/M_0 \to M/M_0$ is injective.

Proof. (i) Since M is a finitely generated Λ-module, so is M^δ. Thus for some $d = d(M) \geq 0$, Γ_d acts trivially on M^δ. M^δ is a thus a Λ-torsion module, since $\omega_d = \gamma^d - 1$ kills M^δ. Now by definition $M_0 = \mathrm{tor}_{\mathbb{Z}_p} M^\delta$, therefore it is clearly the maximal finite submodule of M.

(ii) If M is a finitely generated torsion Λ-module, then by details in (i) above we have $\omega_d M = 0$ for some $d \geq 0$. Hence $\mathrm{supp}(M) \cap$ $\mathbf{P(A)} = \{(\xi_{n_i}) \mid n_i \leq d(M)\}$. Therefore we have a pseudo-isomorphism,

$$M \xrightarrow{\approx} \bigoplus_i \Lambda/(\xi_{n_i}) \text{ where } n_i \leq d(M).$$

For $n \geq n_0$ $\{(\xi_{n_0+1}), \cdots (\xi_n)\}$ is disjoint to $\{(\xi_{n_i}) \mid n_i \leq d(M)\}$. Hence $\mathrm{supp}(M) \cap$ $\mathbf{P(A)}$ is disjoint to $\mathrm{supp}(M/\nu_n M)$.

(iii) We have the short exact sequence

$$0 \to M_0 \to M \to M/M_0 \to 0.$$

This fits into the commutative diagram

(4.2)
$$\begin{tikzcd}
0 \arrow[r] & M_0 \arrow[r] \arrow[d, "\nu_n"] & M \arrow[r] \arrow[d, "\nu_n"] & M/M_0 \arrow[r] \arrow[d, "\nu_n"] & 0 \\
0 \arrow[r] & M_0 \arrow[r] & M \arrow[r] & M/M_0 \arrow[r] & 0
\end{tikzcd}$$

By the snake lemma we have the following exact sequence

$$0 \to \ker(\upsilon_n|_{M_0}) \to \ker(\upsilon_n) \to \ker(\upsilon_n|_{M/M_0}) \to \operatorname{coker}(\upsilon_n|_{M_0}) \to \operatorname{coker}(\upsilon_n) \to \cdots$$

Since for $n \geq n_0$ $\operatorname{supp}(M/\nu_n M)$ is disjoint to $\operatorname{supp}(M) \cap$ $\mathbf{P(A)}$, the multiplication by υ_n map is therefore a pseudo-isomorphism by lemma 4.1.9. Hence $\ker(\upsilon_n)$, $\operatorname{coker}(\upsilon_n)$, $\ker(\upsilon_n|_{M_0})$ and $\operatorname{coker}(\upsilon_n|_{M_0})$ are finite Λ-module, since Λ is a two dimensional regular local ring. From the exact sequence above we see that $\ker(\upsilon_n|_{M/M_0})$ is finite as well and $\ker(\upsilon_n|_{M/M_0}) = B/M_0$, for some Λ-submodule B of M. Since $\ker(\upsilon_n|_{M/M_0})$ is finite and M_0 is finite by (i) above, B is therefore a finite Λ-submodule of M. M_0 is maximally finite in M by (i) above. Hence $B \subseteq M_0$, i.e. $\ker(\upsilon_n|_{M/M_0}) = B/M_0 = 0$. Thus proving the injectivity of the map $\nu_n : M/M_0 \to M/M_0$.

□

Proposition 4.2.14. Let M be a finitely generated Λ-torsion module and let $n_0 \geq d(M)$ be a fixed number. Then

$$\#(M/\frac{\omega_n}{\omega_{n_0}}M) = p^{\mu p^n + \lambda n + \nu}$$

for all n large enough, where $\mu = \mu(M)$, $\lambda = \lambda(M)$ and ν is a constant independent of n.

Proof. Consider the map

$$\nu_n \colon M \to M.$$

By lemma 4.2.13 (ii) and the details in the proof, we have for $n \geq n_0$, that $\ker(v_n|_{M/M_0}) = 0$ and the corkenel of ν_n, $M/\nu_n M$ is finite. By the snake lemma applied to the commutative diagram 4.2, we have the exact sequence

$$0 \to M_0/\nu_n \to M/\nu_n \to (M/M_0)/\nu_n \to 0.$$

Hence

$$\#(M/\nu_n) = \#((M/M_0)/\nu_n) \cdot \#M_0/\nu_n.$$

To calculate $\#((M/M_0)/\nu_n)$, let $N = M/M_0$. By the structure theorem of finitely generated Λ-modules (see theorem 4.2.8) we have an exact sequence

$$0 \to N \to E \to C \to 0$$

where C is finite and E is a Λ-module of the form

$$\bigoplus_{i=1}^{r}(\Lambda/p^{m_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(F_j(T)^{n_j}).$$

Since multiplication by ν_n is injective on E, we have an exact sequence

$$0 \to S_{\nu_n} \to N/\nu_n \to E/\nu_n \to C/\nu_n \to 0,$$

where S_{ν_n} is defined by the following exact sequence

$$0 \to S_{\nu_n} \to C \overset{\nu_n}{\to} C \to C/\nu_n \to 0.$$

Hence

$$\#(N/\nu_n) = \#E/\nu_n \text{ (ignoring the constant factors).}$$

Let $E_i = \Lambda/p^{m_i}$, then clearly $\#(E_i/\omega_n) = p^{m_i p^n}$ and the exact sequence

$$0 \to E_i/\omega_{n_0} \overset{\nu_n}{\to} E_i/\omega_n \to E_i/\nu_n \to 0,$$

shows that

$$\#(E_i/\nu_n) = p^{m_i(p^n - p^{n_0})}$$

We now deal with the other summands of E. If $E_j = \Lambda/F_j(T)^{n_j}$, then for $n \gg 0$ lemma 4.2.11 above coupled with the fact that multiplication by $\xi_{n+1} = \frac{\omega_{n+1}}{\omega_n}$ is injective on E_j, tells us that the the following sequence is exact.

$$0 \longrightarrow E_j/\nu_n \overset{\frac{\omega_n}{\omega_{n_0}}}{\longrightarrow} E_j/\nu_{n+1} \longrightarrow E_j/p \longrightarrow 0$$

Therefore

$$\#(E_j/\nu_{n+1}) = p^{n_j \deg(F_j)} \#(E_j/\nu_n).$$

Hence

$$\#(E_j/\nu_n) = p^{n_j \deg(F_j)(n-n_0)} \#(E_j/\nu_0).$$

Putting all the estimates for the summands of E together we obtain

$$\#(E/\nu_n) = p^{\lambda(N)n + \mu(N)p^n + c},$$

where c is a constant independent of n, and our proof is complete. □

CHAPTER V

Classical Iwasawa Theory

5.1 Class Groups in $\mathbb{Z}_p$ extensions

In this section we study class groups over a $\mathbb{Z}_p$-extension. All the results in this section we owe to Iwasawa, however his original proofs were for the cyclotomic $\mathbb{Z}_p$-extension and rather complicated [21]. Serre in [36], identified the category of Iwasawa modules with the category of modules over the power series ring $\mathbb{Z}_p[[T]]$, of finite type, thus giving easier proofs of Iwasawa's results. We mainly follow his exposition.

Let p be a prime number, which will be fixed in all that follows.

Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ be the field obtained from $\mathbb{Q}$ by adjoining all the p^{n+1}-roots of unity. Then $K_n/\mathbb{Q}$ is an abelian extension and

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times.$$

Let $h_n = \#Cl(K_n)$, the order of the ideal class group of K_n and let

p^{e_n} be the highest power of p dividing h_n.

Iwasawa's classical results are:

Theorem 5.1.1. (see [21])

If $e_1 = 0$ (i.e. $p \nmid h_1$ and p is a "regular" prime in the sense of Kummer) then $e_n = 0$ for all n.

Theorem 5.1.2. (see [22])

For each prime p, there are integers m, l, c with $m \geq 0$ and $l \geq 0$ such that

$$e_n = mp^n + ln + c$$

for n sufficiently large.

We give a proof for an abitrary $\mathbb{Z}_p$-extension K_∞/K. These theorems follow from the structure theory of finitely generated modules over the Iwasawa algebra. Let $K_\infty = \bigcup_{n=0}^{\infty} K_n$. By proposition 3.1.2, we have that $\text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Let $X_n = Cl(K_n)(p)$ (the p-part of the ideal class group of K_n). The norm map between any two successive steps in the tower is surjective on the ideal class groups (see [24] chap III). We then have a surjective sequence

$$X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots$$

i.e. the X_n's form an inverse system under the norm map. Let $X = \varprojlim_n X_n$. Let L_n be the maximal abelian unramified p-extension of K_n i.e. the p-primary part of the Hilbert class field of K_n. Class field theory now gives us an isomorphism $X_n \cong \text{Gal}(L_n/K_n)$ (see [31]) such that the following diagram is commutative

$$\begin{tikzcd}
X_{n+1} \arrow[r, "\cong"] \arrow[d, "\text{norm}"] & \text{Gal}(L_{n+1}/K_{n+1}) \arrow[d, "\text{res}"] \\
X_n \arrow[r, "\cong"] & \text{Gal}(L_n/K_n)
\end{tikzcd}$$

We will now work under the following assumption in all that follows:

Assumption 5.1.3. All primes which ramify in K_∞/K are totally ramified

Remark 5.1.4. If this assumption is not true for the base field K then by lemma 3.1.4 it will be true for all K_n with $n \geq n_0$ for some n_0. Therefore we can replace K by K_{n_0} as the base field in this case.

Since K_∞/K_n is totally ramified above p, and the extension L_n is unramified, our assumption implies that L_n and K_∞ are linearly disjoint over K_n. By Galois theory

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty).$$

Let $L_\infty = \bigcup_{n=0}^{\infty} L_n$. The X_n's form an inverse system under the norm map, hence taking the projective limit we get

$$\begin{aligned} X &= \varprojlim_n X_n = \varprojlim_n \mathrm{Gal}(L_n/K_n) \\ &= \varprojlim_n \mathrm{Gal}(L_nK_\infty/K_\infty) = \varprojlim_n \mathrm{Gal}(\bigcup_n L_nK_\infty/K_\infty) \\ &= \mathrm{Gal}(L_\infty/K_\infty). \end{aligned}$$

The lattice of fields is as follows,

$$\begin{tikzcd}
 & & & L_\infty \\
 & & K_\infty L_{n+1} \arrow[ur] \arrow[dr] & \\
 & K_\infty L_n \arrow[ur] \arrow[ddrr] & & L_{n+1} \\
K_\infty \arrow[ur] \arrow[uuurrr, bend left, "X"] & & & \\
 & K_{n+1} \arrow[ul] \arrow[uurr] & & L_n \\
 & & K_n \arrow[ul] \arrow[ur] & \\
 & & & K \arrow[ul] \arrow[uuulll, bend left, "\Gamma"]
\end{tikzcd}$$

X packages all the information about the X_n in one place, and more importantly, X can be equipped with the structure of a (finitely generated torsion) Λ-module. Then by theorem 4.2.8 X is pseudo-isomorphic to a direct sum of modules of the form $\Lambda/(p^{n_i})$, $\Lambda/(F(T)^{s_i})$. We need a way to recover the class groups X_n from X. We note that each L_n is Galois over K by maximality, hence L_∞ is also Galois over K. We proceed as follows.

Lemma 5.1.5. X is a Λ-module.

Proof. We have the exact sequence.

$$0 \longrightarrow X_n \longrightarrow \mathrm{Gal}(L_n/K) \longrightarrow \Gamma_n \longrightarrow 0. \tag{5.1}$$

Let $\Gamma_n = \Gamma/\Gamma^{p^n}$ and let $\gamma \in \Gamma_n$

Then Γ_n acts on X_n by conjugation i.e.

$$x^{\gamma} = \tilde{\gamma}x(\tilde{\gamma})^{-1}$$

where $x \in X_n$ and $\tilde{\gamma}$ is a lift of γ to $\mathrm{Gal}(L_n/K_n)$. This action is well defined since $\mathrm{Gal}(L_n/K_n)$ is abelian. Since X_n is a pro-p group $\mathbb{Z}_p$ acts on X_n, therefore X_n becomes a $\mathbb{Z}_p[\Gamma_n]$-module. Now

$$\varprojlim_n \mathbb{Z}_p[[\Gamma_n]] = \mathbb{Z}_p[[\Gamma]] = \Lambda \text{ and}$$

$$X = \varprojlim_n X_n.$$

Hence we realize X as a Λ-module. Indeed for any $x \in X$ we can write x as a vector $x = (x_n)$ with $x_n \in X_n$ and for $\gamma \in \Lambda$ we have $\gamma = (\gamma_n)$, with $\gamma_n \in \Gamma_n$. We can then explicitly define the action of Λ on X by,

$$\gamma \cdot x = (\gamma_n) \cdot (x_n) = (\gamma_n \cdot x_n).$$

It is easily checked that $\gamma \cdot x \in X$. □

Before we recover the X_n's from the Λ-module X, we prove some auxiliary lemmas.

Lemma 5.1.6. Let $G = \mathrm{Gal}(K_\infty/K)$ and Let $v_1, \ldots, v_k$ be the valuations of K which ramify in K_∞/K and let $I_i \subset \Gamma = \mathrm{Gal}(K_\infty/K)$ be their inertia groups. Let w_i be an extension of v_i to L_∞, let $S_i \subset \mathrm{Gal}(L_\infty/K)$ be the inertia group of w_i and W_i be the fixed field of S_i. Then G is a semidirect product of S_i by X i.e. $G = X \cdot S_i$ and $X \cap S_i = \{1\}$.

Proof. Since L_∞/K_∞ is unramified we have $S_i \cap X = 0$. Consider the following diagram.

$$\begin{tikzcd}
 & 1 \arrow[d] \arrow[ddl] \arrow[ddr] & & & & L_\infty \arrow[d] \arrow[ddl] \arrow[ddr] & \\
 & S_i \cap X \arrow[dl] \arrow[dr] & & & & W_iK_\infty \arrow[dl] \arrow[dr] & \\
S_i \arrow[dr] & & X \arrow[dl] \arrow[rr, Leftrightarrow, "\text{Galois Correspondence}"] & & W_i \arrow[dr] & & K_\infty \arrow[dl] \\
 & \mathrm{Gal}(L_\infty/K) & & & & K &
\end{tikzcd}$$

We have $S_i = \mathrm{Gal}(L_\infty/W_i)$ and L_∞/W_i is a totally ramified extension for w_i, it follows that $L_\infty/K_\infty W_i$ is also totally ramified since $K_\infty W_i \supset W_i$. Since $L_\infty/K_\infty W_i$ also belongs to the unramified extension L_∞/K_∞, we must have

$$L_\infty = K_\infty W_i.$$

This is illustrated by the diagram above. We have the following lattice diagram.

$$\begin{tikzcd}
 & L_\infty = W_iK_\infty \arrow[dl] \arrow[dr] & \\
W_i \arrow[dr] & & K_\infty \arrow[dl] \\
 & W_i \cap K_\infty \arrow[d] & \\
 & K &
\end{tikzcd}$$

By Galois theory

$$\mathrm{Gal}(K_\infty W_i/W_i) \cong \mathrm{Gal}(L_\infty/W_i) \cong \mathrm{Gal}(K_\infty/W_i \cap K_\infty),$$

(where the map inducing the isomorphism is a restriction from W_iL_∞ to L_∞). Since W_i/K is unramified and K_∞/K is totally ramified , we obtain $W_i \cap K_\infty = K$. Each I_i is a closed subgroup of Γ, therefore $I_i = p^{n_i}\Gamma$ for some $n_i \geq 0$.

Under our assumption (totally ramified) $n_i = 0$ for all i, i.e. $I_i = \Gamma$. Hence the map $S_i = \mathrm{Gal}(L_\infty/W_i) \hookrightarrow \mathrm{Gal}(K_\infty/K)$ is surjective hence bijective. Therefore each S_i is complementary to X in $\mathrm{Gal}(L_\infty/K)$ (i.e. $\mathrm{Gal}(L_\infty/K) = X \cdot S_i$, and $X \cap S_i = \{1\}$). Thus $G = \mathrm{Gal}(L_\infty/W_i)$ is a semidirect product of S_i by X. □

Under our assumption we have the isomorphism $S_i \cong \Gamma$. Let $\gamma \in \Gamma$ be a topological generator of Γ. For each i, let $\sigma_i \in S_i$ map to γ under the above isomorphism. Now $\sigma_i \in G = X \cdot S_i$ (this is possible since $S_i \subset G$), therefore $\sigma_i = a_i s$, where $a_i \in X$ and $s \in S_i$. Since $a_i \in X = \mathrm{Gal}(L_\infty/K_\infty)$, we have $a_i|_{K_\infty} = \mathrm{id}$, hence $\sigma_i|_{K_\infty} = s$. Since $s \in S_1$ and $s|_{K_\infty} = \gamma$ we obtain $s = \sigma_1$. Therefore we have

$$\sigma_i = a_i \sigma_1 \quad , \quad a_i \in X.$$

Lemma 5.1.7. Let $\overline{[G,G]}$ be the closure of the commutator subgroup of G. Then

$$\overline{[G,G]} = (1-\gamma)X.$$

Proof. Γ acts on X, and since the map $S_1 \hookrightarrow \Gamma = G/X$ is onto, we may lift $\sigma \in \Gamma$ to the corresponding element in X, to define an action of S_1 on X. For simplicity we identify Γ with S_1, so that $x^\sigma :\, = \sigma x \sigma^{-1}$. Let $a = \alpha x, b = \beta y$ with $\alpha, \beta \in \Gamma$ and $x, y \in X$ be arbitrary elements of $G = X \cdot I_i$. A typical commutator in G looks as follows

$$\begin{aligned} aba^{-1}b^{-1} &= (\alpha x)(\beta y)(\alpha x)^{-1}(\beta y)^{-1} \\ &= x^\alpha \alpha\beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (y x^{-1})^{\alpha\beta} (y^{-1})^\beta \text{ (since } \Gamma \text{ is abelian)} \\ &= (x^\alpha)^{1-\beta} (y^\beta)^{\alpha-1} \text{ where } \beta - 1, \alpha - 1 \in \Lambda. \end{aligned}$$

Let $\beta = 1$ and $\alpha = \gamma$ in the commutator above, then we see that $y^{\gamma-1} \in \overline{[G,G]}$ therefore $X^{\gamma-1} \subseteq \overline{[G,G]}$. To show the other inclusion we need to show that $aba^{-1}b^{-1} \subseteq$

$X^{\gamma-1}$. It is sufficient to show that $(x^{\alpha})^{1-\beta} \in X^{\gamma-1}$ and $(y^{\beta})^{1-\alpha} \in X^{\gamma-1}$. First we note that for arbitrary β, there exists $c \in \mathbb{Z}_p$ such that $\beta = \gamma^c$ (since γ is the topological generator of Γ), we also have $\gamma - 1 = T$, therefore

$$1 - \beta = 1 - \gamma^c = 1 - (1+T)^c = 1 - \sum_{0}^{\infty} \binom{c}{n} T^n \in T\Lambda.$$

Now $1 - \beta \in T\Lambda$ hence $(x^{\alpha})^{1-\beta} \in X^{\gamma-1}$, similarly $(y^{\beta})^{1-\alpha} \in X^{\gamma-1}$. $X^{\gamma-1} = TX$ is a closed subgroup of G, being the image of the compact set X under the continuous map $\gamma - 1$. Therefore $\overline{[G, G]} \subseteq X^{\gamma-1}$ and our proof is complete. □

We now recover the class groups X_n as certain quotients of X.

Theorem 5.1.8. Let Y_n be the $\mathbb{Z}_p$ submodule defined by the following recipe

(i) Y_0 is generated by the a_i and by $(1-\gamma)X$ i.e.

$$Y_0 = \langle a_2, \ldots, a_k, (1-\gamma)X \rangle$$

(ii) $Y_n = v_n Y_0$ where

$$v_n = 1 + \gamma + \gamma^2 + \ldots + \gamma^{p^n - 1}$$

Then $X_n = X/Y_n$.

Proof. (i) $X_n = \text{Gal}(L_n/K_n)$, where L_n is the maximal abelian unramified p-primary extension of K_n. Therefore L_0 is the maximal abelian unramified p-primary extension of K_0 contained in L_∞. Let K^{ab} be the maximal abelian extension of K contained in L_∞, then

$$\text{Gal}(K^{ab}/K) \cong \text{Gal}(L_\infty/K)/\text{Gal}(L_\infty/K^{ab}),$$

where $\text{Gal}(L_\infty/K^{ab})$ is the commutator subgroup. For each i let again $S_i \subset \text{Gal}(L_\infty/K)$ be the inertia group for the valuation w_i on L_∞ extending the valuation v_i on K_∞. An intermediate field E/K is unramified if and only if each w_i is unramified in E/K (i.e. E is contained in the inertia field of every w_i). Since the w_i are the only primes that ramify, E/K is maximal unramified if and only if it is the fixed field of the smallest subgroup of $\mathrm{Gal}(L_\infty/K)$ that contains all the inertia groups S_i. L_0 is the maximal abelian unramified p-primary extension of K_0 contained in L_∞ hence

$$X_0 = \mathrm{Gal}(L_0/K_0) \cong \mathrm{Gal}(L_\infty/K)/Z_0,$$

where Z_0 is the smallest subgroup of $\mathrm{Gal}(L_\infty/K)$ which contains the commutator subgroup (since the extension is required to be abelian) and also contains all the inertia groups (since it is required to be unramified as well). Therefore by lemma 5.1.7

$$Z_0 = \overline{\langle X^{\gamma-1}, S_1, \dots, S_k \rangle},$$

where $X^{\gamma-1}$ is the commutator subgroup. By the same lemma S_i is generated by $\sigma_i = a_i\sigma_1$ with $a_1 = 1$, therefore

$$Z_0 = \overline{\langle X^{\gamma-1}, S_i, a_2, \dots, a_k \rangle},$$

which implies

$$\begin{aligned} X_0 = \mathrm{Gal}(L_0/K_0) &\cong \mathrm{Gal}(L_\infty/K)/Z_0 \\ &= X \cdot S_1/\overline{\langle X^{\gamma-1}, S_1, a_2, \dots, a_k \rangle} \\ &= X/\overline{\langle X^{\gamma-1}, a_2, \dots, a_k \rangle} \\ &= X/Y_0. \end{aligned}$$

(ii) Suppose $n > 0$, then $X_n = \mathrm{Gal}(L_n/K_n)$ and

$$\mathrm{Gal}(K_\infty/K_n) \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p.$$

The topological generator of $\mathrm{Gal}(K_\infty/K_n)$ is γ^{p^n}. Let $w_{i,n}$ be the valuation extending $v_{i,n}$ in L_∞/K_n, and let the corresponding inertia group be $S_{i,n} = \mathrm{Gal}(L_\infty/W_{i,n})$, where $W_{i,n}$ is the inertia field of $w_{i,n}$ in L_∞/K_n. Let $\sigma_{i,n} \in S_{i,n} = \mathrm{Gal}(L_\infty/W_{i,n})$ with $\sigma_{i,n} \xrightarrow{\text{res}} \gamma^{p^n}$ i.e. $\sigma_{i,n}$ maps to the generator of $\mathrm{Gal}(K_\infty/K_n)$ by the restriction map to K_∞. Since σ_i restricts to γ the restriction map $S_i = \mathrm{Gal}(L_\infty/W_i) \xrightarrow{\text{res}} \mathrm{Gal}(L_\infty/K_n)$ implies that ${\sigma_i}^{p^n}$ maps to γ^{p^n} . We therefore obtain $\sigma_{i,n} = {\sigma_i}^{p^n}$. By the same argument as in lemma 5.1.6 we have a semidirect product decomposition for $\mathrm{Gal}(L_\infty/K_n)$. This time

$$\mathrm{Gal}(L_\infty/K_n) = X \cdot I_{i,n} \text{ since } \sigma_{i,n} \in \mathrm{Gal}(L_\infty/K_n).$$

Therefore $\sigma_{i,n} = a_{i,n}I_{1,n}$ with $a_{i,n} \in X$. Now for any $k \in \mathbb{Z}$

$$\begin{aligned}
{\sigma_i}^{k+1} &= (a_i\sigma_1)^{k+1} \\
&= (a_i\sigma_1)(a_i\sigma_1)(a_i\sigma_1)\cdots(a_i\sigma_1)(k+1 \text{ times }) \\
&= a_i\sigma_1 a_i {\sigma_1}^{-1}\sigma_1^2 a_i {\sigma_1}^{-2}\sigma_1^3 a_i \sigma_1^{-3}\cdots\sigma_1^k a_i {\sigma_1}^{-k}\sigma_1^{k+1}.
\end{aligned}$$

The action of γ is conjugation by σ_1, hence we obtain

$$\begin{aligned}
\sigma_{i,n} &= {\sigma_i}^{p^n} \\
&= a_i(\gamma^1 a_i)(\gamma^2 a_i)(\gamma^3 a_i)\cdots(\gamma^{p^n-1}a_i)\sigma_1^{p^n} \\
&= (1+\gamma^1+\gamma^2+\cdots+\gamma^{p^n-1})a_i\sigma_1^{p^n} \\
&= v_n a_i \sigma_1^{p^n}.
\end{aligned} \tag{5.2}$$

L_n is the maximal abelian unramified p-primary extension of K_n contained in L_∞ hence

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_\infty/K_n)/Z_n,$$

where Z_n is the smallest subgroup of $\mathrm{Gal}(L_\infty/K_n)$ which contains the commutator subgroup (since the extension is required to be abelian), and also contains all the inertia groups (since it is required to be unramified as well). Therefore

$$Z_n = \overline{\langle X^{\gamma^{p^n}-1}, S_{1,n}, \dots, S_{s,n}\rangle},$$

where γ^{p^n} is now the topological generator of $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}_p$. As shown above $S_{i,n}$ is generated by $\sigma_{i,n} = a_{i,n}S_{1,n}$ with $a_{1,n} = 1$. Hence

$$Z_n = \overline{\langle X^{\gamma^{p^n}-1}, I_{1,n}, a_{2,n}, \dots, a_{s,n}\rangle}.$$

We note that

$$X^{\gamma^{p^n}-1} = (\gamma^{p^n}-1)X = (1+\gamma^1+\gamma^2+\cdots+\gamma^{p^n-1})(1-\gamma)X = \upsilon_n(1-\gamma)X$$

We now determine the $a_{i,n}$. This is now easy, $\sigma_{i,n} = a_{i,n}I_{1,n}$ implies $\sigma_{i,n} = a_{i,n}\sigma_1^{p^n}$ (since $I_{1,n}$ is generated by $\sigma_{1,n} = \sigma_1^{p^n}$). Comparing this with equation (5.2) we have

$$a_{i,n} = (1+\gamma^1+\gamma^2+\cdots+\gamma^{p^n-1})a_i = \upsilon_n a_i.$$

Hence

$$\begin{aligned} X_n &= \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_\infty/K)/Z_n \\ &= X \cdot S_{1,n}/\overline{\langle \upsilon_n(1-\gamma)X, S_{1,n}, \upsilon_n a_2, \dots, \upsilon_n a_k\rangle} \\ &= X/\upsilon_n\overline{\langle X^{\gamma^{p^n}-1}, a_2, \dots, a_k\rangle} \\ &= X/\upsilon_n Y_0 = X/Y_n. \end{aligned}$$

This completes our proof.

□

Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension, Hence $K = \mathbb{Q}(\zeta_p)$. Since only one prime p ramifies, $k = 1$ in theorem 5.1.8. This implies $Y_0 = \langle(1-\gamma)X\rangle = \omega_0 X$ and $Y_n = \langle \upsilon_n(1-\gamma)X\rangle = \omega_n X$. Hence

$$X_n = X/\omega_n X = Cl(K_n)(p) \tag{5.3}$$

which is finite. Now if $e_1 = 0$ that is $X_0 = 0$ then $X = \omega_0 X$ and since $\omega_0 \in \mathfrak{m} = (p, T)$ by Nakayama's Lemma 4.2.9, we have $X = 0$ whence $X_n = 0$ for all n that is $e_n = 0$ for all n and we have proved Iwasawa's first result, lemma 5.1.1.

We have worked under the assumption that our $\mathbb{Z}_p$-extension K_∞/K is totally ramified, this is not entirely neccesary. Indeed by lemma 3.1.4 for some $e > n_0$, with $n_0 \gg 0$ the extension K_∞/K_e is totally ramified. Hence we dispence with our assumption and instead work with the $\mathbb{Z}_p$-extension K_∞/K_e for large enough e. A few things change though, since the topological generator of $\mathrm{Gal}(K_\infty/K_e)$ is γ^{p^e} our v_n and Y_0 must change to reflect this.

Definition 5.1.9.

$$v_{n,e} := (1 + \gamma^{p^n} + \gamma^{2p^n} + \cdots + \gamma^{p^e(p^n-1)})$$

$$Y_e = \langle a_2, \ldots, a_k, (1 - \gamma^{p^e})X \rangle$$

With the above definitions for the extension $\mathrm{Gal}(K_\infty/K_e)$ for $n \geq n_0$ we have $X_n = X/v_{n,e}Y_e = X/Y_{n,e}$.

For the applications in mind, it is important that $X = \mathrm{Gal}(L_\infty/K_\infty)$ be a finitely generated Λ-module (it also turns out to be a torsion Λ-module).

Theorem 5.1.10. $X = \mathrm{Gal}(L_\infty/K_\infty)$ is a finitely generated torsion Λ-module

Proof. Since $Y_{n+1,e} \subset Y_{n,e} \subset X$ we have

$$Y_{n,e}/Y_{n+1,e} = Y_{n,e}/v_{n,e}Y_{n,e} \subset X/Y_{n,e} = X_n.$$

Now $v_{n,e} \in \mathfrak{m} = (p, T)$, hence

$$Y_{n,e}/\mathfrak{m}Y_{n,e} \subset Y_{n,e}/v_{n,e}Y_{n,e} \subset X_n.$$

Therefore $\#(Y_{n,e}/\mathfrak{m}Y_{n,e}) \leq \#X_n$. Now $X_n \cong Cl(K_n)(p)$ hence finite. By Nakayama's lemma it follows that $Y_{n,e}$ is finitely generated. Since $X/Y_{0,e} = X_0$ is finite, it follows that X is finitely generated. □

We now prove Iwasawa's second result. For $n \geq e$ we have $X_n = X/v_{n,e}Y_e$, but $v_{n,e} = \frac{\omega_n}{\omega_e}$ where $\omega_n = (1+T)^{p^n} - 1$. Therefore

$$\#X_n = \#(X/Y_e) \cdot \#(Y_e/\frac{\omega_n}{\omega_e}Y_e) = \#Cl(K_e)(p) \cdot \#(Y_e/\frac{\omega_n}{\omega_e}Y_e).$$

Since $\#Cl(K_e)(p)$ is finite and we are interested in an asymptotic result we only compute $\#(Y_e/\frac{\omega_n}{\omega_e}Y_e)$. Now Y_e is a $\mathbb{Z}_p$-submodule of X and X is finitely generated hence Y_e is finitely generated. By theorem 4.2.14 we have

$$\#(Y_e/\frac{\omega_n}{\omega_e}Y_e) = p^{\mu p^n + \lambda n + \nu},$$

for all n large enough, where $\mu = \mu(M)$, $\lambda = \lambda(M)$ (here $M = (Y_e/\frac{\omega_n}{\omega_e}Y_e)$) and ν is a constant independent of n. Therefore

$$\#X_n = p^{\mu p^n + \lambda n + \nu},$$

for n large enough. This completes the proof of theorem 5.1.2.

It is interesting to recast some of our results about the Λ-module X in terms of its dual

$$\widehat{X} = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p).$$

$\widehat{X}$ is a subgroup of $H^1(G_{K_\infty}, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(\mathrm{Gal}(K_\infty^{\mathrm{ab}}/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$ defined by imposing certain local conditions on a cohomology group. Thus $\widehat{X}$ is an instance of what has come to be called a "**Generalized Selmer group**" [12]. In terms of the dual theorem 5.1.10 says that $\widehat{X}$ is a finitely generated cotorsion Λ-module (see section 6.2) and since

(5.4) $$\widehat{X_n} = \mathrm{Hom}(X/v_{n,e}Y_e, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)^{G_n} = \widehat{X}^{G_n}$$

for some subgroup G_n of $\mathrm{Gal}(K_\infty/K_e)$. Iwasawa's result above then reads

$$\#\widehat{X}^{G_n} = p^{\mu p^n + \lambda n + \nu}$$

for large n and is really a result about the size of Selmer groups. We see then that studying class groups is indeed studying Selmer groups, generalized of course. We continue with this theme in the next section where we study Selmer groups attached to elliptic curves. In particular we shall prove a weaker analogue of equation (5.4) called "Mazur's Control Theorem" where the isomorphism is replaced by a pseudo-isomorphism.

CHAPTER VI

Iwasawa Theory for Elliptic Curves

6.1 Mordell-Weil groups

Let E an elliptic curve defined over K where K is a finite extension of $\mathbb{Q}$. We want to understand the structure of the abelian group $E(K)$ (the *Mordell-Weil group*) of K-rational points on E. A classical theorem due to L. Mordell and subsequently generalized by A. Weil states the following .

Theorem 6.1.1 (Mordell-Weil). Let E an elliptic curve defined over K, where K is a finite extension of $\mathbb{Q}$, then $E(K)$ is a finitely generated abelian group.

Proof. (see [40] Chapter VIII, page 189.) We will be content to just note that the main ingredients for the proof are the "weak Mordell-Weil theorem", and a height function, which enables a "descent" strategy going back to Fermat. □

The Mordell-Weil theorem states that the abelian group $E(K)$ of K-rational points on $E(K)$ has the structure

$$E(K) \cong \mathbb{Z}^r \times E_{\text{tors}}(K)$$

where $E_{\text{tors}}(K)$ is the finite torsion subgroup of $E(K)$ and r is a non-negative integer called the *rank* of the elliptic curve. For any given elliptic curve it is easy to determine the torsion subgroup. It comes as a surprise that there is no procedure to determine the rank in general. Efforts to get a grip on this mysterious quantity are behind much recent activity in number theory, centred around the famous Birch Swinnerton-Dyer Conjecture [2].

The Mordell-Weil Theorem may fail to hold if K is an infinite extension of $\mathbb{Q}$. We give an example of this phenomenon. Consider $E(\overline{\mathbb{Q}})$ where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, then

$$E_{\text{tors}}(\overline{\mathbb{Q}}) = \bigcup_n E_{\text{tors}}(\mathbb{C})[n] = \bigcup_n (\mathbb{Z}/n\mathbb{Z})^2 = (\mathbb{Q}/\mathbb{Z})^2$$

is certainly not finite. Now $E(\overline{\mathbb{Q}})$ is a divisible group. Taking the quotient $E(\overline{\mathbb{Q}})/E_{\text{tors}}(\overline{\mathbb{Q}})$ gives a uniquely divisible group. Therefore we can consider $E(\overline{\mathbb{Q}})/E_{\text{tors}}(\overline{\mathbb{Q}})$ as a vector space over $\mathbb{Q}$. The rank of this $\mathbb{Q}$ vector space is infinite. It can be easily shown that this is equivalent to the statement that $\text{rank}_{\mathbb{Z}}(E(L))$ is unbounded as L varies over all finite extensions of $\mathbb{Q}$ (see [14] pg 3) .

From the above example we see that $E(\overline{\mathbb{Q}})$ is not finitely generated.

There are however infinite algebraic extensions K of $\mathbb{Q}$ such that $E(K)$ is finitely generated. For Galois extensions B. Mazur in [28] gives a simple necessary and sufficient condition for this to happen. We state and prove this result.

Theorem 6.1.2. Let K be a Galois extension of $\mathbb{Q}$. Assume that $E_{\text{tors}}(K)$ is finite, then $\text{rank}_{\mathbb{Z}}(E(L))$ is bounded as L varies over all finite extensions of $\mathbb{Q}$ contained in K if and only if $E(K)$ is finitely generated.

Proof. Choose a finite extension L of $\mathbb{Q}$ contained in K such that $\text{rank}_{\mathbb{Z}}(E(L))$ is maximal . Then $E(K)/E(L)$ must be a torsion group. Indeed suppose $x \in E(K)/E(L)$ is a point of infinite order i.e. x is independent of the generators in $E(L)$. We now consider the finite extension $L(x)$ obtained by adjoining x to L, since x is independent of the generators in $E(L)$ we have that $\text{rank}_{\mathbb{Z}}(E(L(x))) > \text{rank}_{\mathbb{Z}}(E(L))$, contradicting the maximality of $\operatorname{rank}_{\mathbb{Z}}(E(L))$ for all finite extensions. Now suppose $P \in E(K)$. Then there exists an integer $m \geq 1$ such that $mP \in E(L)$ since $E(K)/E(L)$ is torsion. Let $\sigma \in \operatorname{Gal}(K/L)$ then we have

$$m(\sigma(P) - P) = \sigma(mP) - mP = O_E$$

therefore $\sigma(P) - P \in E_{\text{tors}}(K)$. Let $t = |E_{\text{tors}}(K)|$ we then have that $t(\sigma(P) - P) = O_E$, i.e. $\sigma(tP) = tP$ for all $\sigma \in \operatorname{Gal}(K/L)$. This implies that $tP \in E(L)$ for all $P \in E(K)$. Hence we can define a homomorphism $\varphi : E(K) \to E(L)$ by $\varphi(P) = tP$. The image of φ is finitely generated since it is a subgroup of $E(L)$. The kernel of φ is just $E_{\text{tors}}(K)$. It then follows that $E(K)$ is finitely generated. Conversely it is clear that if $E(K)$ is finitely generated, then $\operatorname{rank}_{\mathbb{Z}}(E(L))$ is bounded for all finite extension L of $\mathbb{Q}$ contained in K. □

Verifying the hypothesis of the above theorem is hard. Especially the hypothesis about the behaviour of $\operatorname{rank}_{\mathbb{Z}}(E(L))$ as L varies over all finite extensions of $\mathbb{Q}$ contained in K. Indeed the behaviour of $\operatorname{rank}_{\mathbb{Z}}(E(L))$ is the focus of this section. We will work towards verifying this hypothesis for an important class of Galois extensions, namely the $\mathbb{Z}_p$-extensions. The finiteness of $E_{\text{tors}}(K)$ can be verified in many important situations (see [28] page 234). One result which we will prove completely is the following theorem due to B.Mazur [28].

Theorem 6.1.3. Suppose E is an elliptic curve defined over a number field K. Let p be a prime such that E has good reduction at all primes of K lying over p. Assume that both $E(K)$ and $\text{Ш}(K, E)_p$ are finite. Let $K_\infty = \bigcup_n K_n$ be a $\mathbb{Z}_p$-extension of K. Then $\operatorname{rank}_{\mathbb{Z}}(E(K_n))$ is bounded for all $n \geq 0$.

This theorem will be a consequence of Mazur's Control theorem, together with basic results on Iwasawa modules. But instead of studying Mordell-Weil groups directly we study the behaviour of Selmer groups instead.

6.2 Selmer Groups

Let K be a algebraic extension of $\mathbb{Q}$. Suppose that E is an elliptic curve defined over K. One of the principal ways to study the Mordell-Weil group is by Galois cohomology. We embed a quotient of the Mordell-Weil group into the *Selmer group* which is a cohomology subgroup and show that this *Selmer group* is finite. We review the construction of the *Selmer group* below, but first we present a standard result from algebraic geometry.

Lemma 6.2.1. Let C_1, C_2 be projective curves defined over an algebraically closed field K, then any morphism $\varphi : C_1 \to C_2$ is either constant or surjective

Proof. (See [19], Chapter II.6.8). □

Recalling that an elliptic curve is a projective variety of dimension one and that the multiplication by n map is non-constant, we have the following easy consequence of lemma 6.2.1

Corollary 6.2.2. Let E be an elliptic curve defined over an algebraic closure $\overline{K}$ of K and n any integer, then the multiplication by n map

$$n\colon E(\overline{K}) \to E(\overline{K})$$

is a surjective morphism.

By corollary 6.2.2 we obtain the following short exact sequence of continuous G_K-modules, where $G_K = \mathrm{Gal}(\overline{K}/K)$

$$0 \to E(\overline{K})[n] \to E(\overline{K}) \xrightarrow{n} E(\overline{K}) \to 0$$

Taking Galois cohomology we obtain the following long exact sequence .

$$0 \to H^0(G, E[n]) \to H^0(G, E) \to H^0(G, E) \to H^1(G, E[n]) \to H^1(G, E) \to H^1(G, E) \to \cdots$$

From which we extract the following fundamental exact sequence:

$$(6.1) \qquad 0 \to E(K)/nE(K) \to H^1(G_K, E(\overline{K})[n]) \xrightarrow{n} H^1(G_K, E)[n] \to 0$$

If we could prove that $H^1(G_K, E(\overline{K})[n])$ is finite, then this short exact sequence would allow us to conclude that $E(K)/nE(K)$ is finite and we would have thus proved the "weak Mordell-Weil" theorem. Unfortunately it turns out that $H^1(G, E(\overline{K})[n])$ is never finite for a number field K. We can however still study $E(K)/nE(K)$ by looking at its image in a smaller finite subgroup of $H^1(G, E(\overline{K})[n])$ (the *Selmer group*).

The fundamental short exact sequence (6.1) tells us that the image of $E(K)/nE(K)$ is precisely $\ker(n)$. To determine $\ker(n)$ we need to decide which cohomology classes of $H^1(G_K, E(\overline{K})[n])$ map to the trivial class in $H^1(G_K, E)[n]$. The cohomology group $H^1(G_K, E)[n]$ has a geometric interpretation, its cohomology classes are in one to one correspondence with the principal homogeneous spaces of E (see [40] chapter X). Furthermore a cohomology class is trivial in $H^1(G_K, E)[n]$ if and only if the associated principal homogeneous space has a K-rational point. Over a number field K we do not as yet have an effective solution to the problem of deciding whether a principal homogeneous space has a K-rational point. However over a local field this problem has an effective solution, Hensel's lemma allows us to work over the residue field which is finite, this coupled with estimates of the number of points on a variety over a finite field means we have an effective algorithm for finding all the rational points over a local field.

We are thus tempted to reduce the problem to a local situation. This motivates the following considerations. Consider a place ν of K and let K_ν be the completion of K at ν. This gives us an embedding $K \hookrightarrow K_\nu$ which induces the injection $G_{K_v} \hookrightarrow G_K$, we therefore can consider G_{K_v} as a subgroup of G_K. We thus have restriction maps from $H^1(G_K, E)$ to $H^1(G_{K_v}, E)$. Repeating the same arguments as above now over a local field K_v, we obtain the following short exact sequence

$$0 \to E(K_v)/nE(K_v) \to H^1(G_{K_v}, E(\overline{K_v})[n]) \xrightarrow{n} H^1(G_{K_v}, E)[n] \to 0$$

The inclusion maps $G_{K_v} \hookrightarrow G_K$ and $E(K) \hookrightarrow E(K_\nu)$ induce restriction maps on cohomology groups, hence we obtain the following commutative diagram (the vertical arrows being the restriction maps).

$$\begin{tikzcd}
0 \arrow[r] & E(K)/nE(K) \arrow[r, "\delta"] \arrow[d] & H^1(G_K, E(\overline{K})[n]) \arrow[r] \arrow[d] & H^1(G_K, E)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K_v)/nE(K_v) \arrow[r, "\delta_v"] & H^1(G_{Kv}, E(\overline{K}_v)[n]) \arrow[r] & H^1(G_{K_v}, E)[n] \arrow[r] & 0
\end{tikzcd}$$

We wish to replace $H^1(G_K, E(\overline{K})[n])$ by a smaller subset , that still contains $E(K)/nE(K)$, but for which we can prove finiteness. Accordingly we make the following observation. If $\gamma \in H^1(G_K, E(\overline{K})[n])$ comes from an element of $E(K)/nE(K)$ then by commutativity of the diagram above, it's image γ_v in $H^1(G_{K_v}, E[n])$ comes from an element of $E(K_v)/nE(K_v)$. This suggests that we define the *n-Selmer group* as:

$$\mathrm{Sel}_E(K)_n = \ker\left(H^1(G_K, E(K)[n]) \to \prod_v H^1(G_{K_v}, E)[n]\right).$$

Finally, in the same spirit of the definition of the Selmer group, we define the *Tate-Shafarevich group* as:

$$Ш(K, E) = \ker\left(H^1(G_K, E) \to \prod_v H^1(G_{K_v}, E)\right).$$

Lemma 6.2.3. Let

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

be maps between modules A , B , C. Then there exists an exact sequence

$$0 \to \ker(\alpha) \to \ker(\beta \circ \alpha) \to \ker(\beta) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta \circ \alpha) \to \operatorname{coker}(\beta) \to 0$$

Proof. This is an simple application of the snake lemma (see [35] page 174) □

Applying lemma 6.2.3 to

$$H^1(K, E[n]) \to H^1(K, E)[n] \to \prod_v H^1(K_v, E)[n]$$

we obtain that the n-torsion part of the *Tate-Shafarevich* group and the *n-Selmer* group fit into the following fundamental short exact sequence

$$(6.2) \qquad 0 \to E(K)/nE(K) \to \mathrm{Sel}_E(K)_n \to Ш(K, E)[n] \to 0$$

Thus the n-Selmer group is important in trying to understand various arithmetic properties of $E(K)$ since the "weak Mordell-Weil" group injects into it and more importantly the n-Selmer group is finite and effectively computable.

Remark 6.2.4. The Tate-Shafarevich group is precisely the group that measures the failure of the Hasse principle for elliptic curves. Indeed a non-trivial element of $Ш(K, E)$ does not have a K-rational point on its corresponding principal homogeneous space, while it has by definition K_v-rational points for all v of K. It is an open conjecture whether the Tate-Shafarevich the group is finite in general.

We can rewrite the short exact sequence (6.1) as

$$0 \to E(K) \otimes (\mathbb{Z}/n\mathbb{Z}) \to H^1(G_K, E(\overline{K})[n]) \xrightarrow{n} H^1(G_K, E)[n] \to 0$$

Taking direct limits we have

$$(6.3) \qquad 0 \to E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \to H^1(G_K, E(\overline{K})_{\mathrm{tors}}) \xrightarrow{n} H^1(G_K, E) \to 0$$

From this we obtain the following commutative diagram, where the vertical maps are the restriction maps.

(6.4)

$$\begin{tikzcd}
0 \arrow[r] & E(K)\otimes(\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa"] \arrow[d, "a_v"] & H^1(G_K, E(\overline{K})_{\text{tors}}) \arrow[r, "\lambda"] \arrow[d, "b_v"] & H^1(G_K, E) \arrow[r] \arrow[d, "c_v"] & 0 \\
0 \arrow[r] & E(K_v)\otimes(\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa_v"] & H^1(G_{K_v}, E(\overline{K_v})_{\text{tors}}) \arrow[r, "\lambda_v"] & H^1(G_{K_v}, E) \arrow[r] & 0
\end{tikzcd}$$

We will naturally call the maps κ, κ_v the global and local Kummer maps since the horizontal exact rows are an imitation of classical Kummer theory (see section 2.8). From general cohomology (see section 2.3) we can explicitly describe the Kummer maps as follows. Let $\alpha = a \otimes (m/n + \mathbb{Z}) \in E(K_v) \otimes (\mathbb{Q}/\mathbb{Z})$ with $a \in E(K_v)$ and $m/n + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Let $b \in E(\bar{K}_v)$ such that $nb = ma$, then $\kappa(\alpha)$ is the class of the 1-cocycle ϕ_α given by $\phi_\alpha(g) = g(b) - (b)$ for all $g \in G_{K_v}$. Finally we then define the *Selmer group* as

$$\mathrm{Sel}_E(K) = \ker\left(H^1(G_K, E(K)_{\text{tors}}) \to \prod_v H^1(G_{K_v}, E)\right)$$

Now from the commutative diagram (6.4) we see that $[\varphi] \in \mathrm{Sel}_E(K)$ if and only if $\lambda_v \circ b_v([\varphi]) = 0$ for all places v of K. This is equivalent to requiring that $b_v([\varphi]) \in \ker(\lambda_v) = \mathrm{im}(\kappa_v)$ for all places v of K. Therefore $[\varphi] \in \mathrm{Sel}_E(K)$ if and only if

$$[\varphi] \in \ker\left(H^1(G_K, E(K)_{\text{tors}}) \to \prod_v H^1(G_{K_v}, E(\overline{K_v})_{\text{tors}})/\mathrm{im}(\kappa_v)\right).$$

Thus we get an alternative description of the *Selmer group.* i.e.

$$\mathrm{Sel}_E(K) = \ker\left(H^1(G_K, E(K)_{\text{tors}}) \to \prod_v H^1(G_{K_v}, E(\overline{K_v})_{\text{tors}})/\mathrm{im}(\kappa_v)\right)$$

Remark 6.2.5. This description also follows immediately by looking at the bottom horizontal row of the commutative diagram (6.4).

Let p be a prime. The p-primary part of $\mathbb{Q}/\mathbb{Z}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ therefore for any field L the p-primary subgroup of $L \otimes (\mathbb{Q}/\mathbb{Z})$ can be identified with $L \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$.

We will now for any algebraic extension $K/\mathbb{Q}$, let κ, κ_v instead denote the global and local Kummer maps restricted to the p-primary subgroups i.e.:

$$\kappa : E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K, E[p^\infty])$$

$$\kappa_v : E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_v, E[p^\infty])$$

Where K is any algebraic extension of $\mathbb{Q}$. We denote the p-primary subgroup of the *Selmer group* by

$$\mathrm{Sel}_E(K)_p = \mathrm{Ker}\left(H^1(K, E[p^\infty]) \to \prod_v H^1(K_v, E[p^\infty])/\mathrm{im}(\kappa_v) \right)$$

Everything in the definition depends on the G_K- module $E[p^\infty]$, except possibly for $\mathrm{im}(\kappa_v)$. Faltings has proved [10] that E is determined up to K-isogeny by the G_K representation space $V_p(E) = T_p(E) \otimes \mathbb{Q}_p$, where $T_p(E)$ denotes the p-adic Tate module for E. More precisely the G_K-module $E[p^\infty] = V_p(E)/T_p(E)$ determines E up to a K-isogeny of degree prime to p. Now $\mathrm{Sel}_E(K)_p$ is not changed by such K-isogenies and hence we might hope to define it using only the G_K-module $E[p^\infty]$. It clearly suffices to give such a description of the subgroup $\mathrm{im}(\kappa_v)$ of $H^1(K_v, E[p^\infty])$ for all primes v of K. We assume in all that follows that E has good ordinary reduction at all primes of K above p.

Proposition 6.2.6. (i) Let E be an elliptic curve defined over an algebraic extension K_v of $\mathbb{Q}_l$ where $l \neq p$. Then

$$E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

(ii) Let E be an elliptic curve defined over $K_v = \mathbb{C}$ or $K_v = \mathbb{R}$, then

$$E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

(iii) Let E be an elliptic curve defined over an algebraic extension K_v of $\mathbb{Q}_p$. Then

$$E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v : \mathbb{Q}_p]}.$$

Thus $\mathrm{im}(\kappa_v) = 0$ whenever $v \nmid p$ and $\mathrm{im}(\kappa_v) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]}$ when $v \mid p$.

Proof. (i) Suppose that K_v is a finite extension of $\mathbb{Q}_l$. Then a theorem of E. Lutz (see [40] chapter VII prop 6.3) states that

$$E(K_v) = \mathbb{Z}_l^{[K_v:\mathbb{Q}_l]} \times T$$

where T is the finite torsion subgroup of $E(K_v)$. Let $x \otimes y \in \mathbb{Z}_l \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Since $\mathbb{Q}_p/\mathbb{Z}_p$ is a p-group, let p^n be the order of y. As $l \nmid p$, $\mathbb{Z}_l$ is p-divisible hence we can find $w \in \mathbb{Z}_l$ such that $x = p^n w$, thus

$$x \otimes y = p^n w \otimes y = w \otimes p^n y = w \otimes 0 = 0.$$

Therefore $\mathbb{Z}_l \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. For any finite group T we have $T \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Thus

$$E(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Z}_p^{[K_v:\mathbb{Q}_p]} \times T) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$$

Now if K_v is an infinite algebraic extension of $\mathbb{Q}_l$ then we have $K_v = \bigcup L_v$ where L_v runs over all the finite extensions of $\mathbb{Q}_l$ contained in K_v. Since $E(L_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$, it follows that $E(K_v) = 0$.

(ii) If $K_v = \mathbb{R}$ then $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ or $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now $\mathbb{R}/\mathbb{Z}$ is p-divisible, hence either

$$E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = E(\mathbb{R}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{R}/\mathbb{Z} \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0, \text{ or}$$

$$E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = E(\mathbb{R}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = (\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$$

If $K_v = \mathbb{C}$ then $E(K_v) \cong (\mathbb{R}/\mathbb{Z})^2$ hence

$$E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{R}/\mathbb{Z})^2 \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$$

Hence for $l \nmid p$ we have $\mathrm{im}(\kappa_v) = 0$.

(iii) If K_v is a finite extension of $\mathbb{Q}_p$ then by E. Lutz's theorem

$$E(K_v) \cong \mathbb{Z}_p^{[K_v : \mathbb{Q}_p]} \times T$$

where T is the torsion subgroup of $E(K_v)$. Thus we obtain

$$\mathrm{im}(\kappa_v) = E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = (\mathbb{Z}_p^{[K_v : \mathbb{Q}_p]} \times T) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v : \mathbb{Q}_p]}$$

Hence for $v \mid p$ we have $\mathrm{im}(\kappa_v) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v : \mathbb{Q}_p]}$ and our proof is complete. □

Since E has good ordinary reduction above v, the reduced curve $\tilde{E}(\overline{k}_v)$ over the residue field for v has an element of order p. We define the reduction map π by

$$\pi \colon E[p^\infty] \to \tilde{E}[p^\infty]$$
$$P \to \tilde{P}.$$

The kernel of the reduction map is $\mathcal{F}(\overline{\mathfrak{m}})[p^\infty]$, We will also for brevity denote $\mathcal{F}(\overline{\mathfrak{m}})$ by $\mathcal{F}$. Indeed this kernel can be identified with the formal group $\mathcal{F}(\overline{\mathfrak{m}})$ of height 1 ([40] chapter IV) associated to the elliptic curve E, where $\overline{\mathfrak{m}}$ is the maximal ideal of the ring of integers of $\overline{K}_v$. Thus when restricted to the p-primary part of the elliptic curve the kernel will be $\mathcal{F}(\overline{\mathfrak{m}})[p^\infty]$. Note that since for all n

$$E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2 \text{ and } \tilde{E}[p^n] \cong \mathbb{Z}/n\mathbb{Z}$$

we have that

$$\tilde{E}[p^\infty] = \varinjlim_n \tilde{E}[p^n] = \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Q}_p/\mathbb{Z}_p$$
$$E[p^\infty] = \varinjlim_n E[p^n] = \varinjlim_n (\mathbb{Z}/p^n\mathbb{Z})^2 \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2.$$

The group G_{K_v} acts on $E(\overline{K}_v)$ in a natural way and the reduction map is equivariant. Let I_v be the inertia group of v, we have an exact sequence (see [30] page 172).

$$0 \to I_v \to G_{K_v} \xrightarrow{\phi} G_{k_v} \to 0. \tag{6.5}$$

Therefore G_{K_v} acts on $\tilde{E}(\overline{k}_v)$ via the homomorphism ϕ i.e.

$$g \cdot P = \phi(g)P$$

where $P \in \tilde{E}(\overline{k}_v)$ and $g \in G_{K_v}$.

From the reduction map we have the following short exact sequence

$$0 \to \mathcal{F}[p^\infty] \to E[p^\infty] \xrightarrow{\pi} \tilde{E}[p^\infty] \to 0. \tag{6.6}$$

Remark 6.2.7. G_{k_v} acts on $\tilde{E}[p^\infty]$ by a character $\psi : G_{k_v} \to \mathbb{Z}_p{}^\times$ because $\tilde{E}[p^\infty]$ is a 1-dimensional representation. Similarly the action of G_{K_v} on $\mathcal{F}[p^\infty]$ is by a character $\varphi : G_{k_v} \to \mathbb{Z}_p{}^\times$. By the short exact sequence (6.5) $G_{K_v}/I_v \cong G_{k_v}$ so we can regard ψ as a character of G_{K_v} which acts trivially on I_v.

We now consider the map

$$\varepsilon_v \colon H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty])$$

induced from the inclusion $\mathcal{F}[p^\infty] \subset E[p^\infty]$ and give a description of $\mathrm{im}(\kappa_v)$ using this map.

Proposition 6.2.8. Let K_v be a finite extension of $\mathbb{Q}_p$ and suppose E has good ordinary reduction at v. Then $\mathrm{im}(\kappa_v) = \mathrm{im}(\varepsilon_v)_{\mathrm{div}}$, where $\mathrm{im}(\varepsilon_v)_{\mathrm{div}}$ is the maximal divisible subgroup of $\mathrm{im}(\varepsilon_v)$.

Proof. By proposition 6.2.6 we have $\mathrm{im}(\kappa_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v : \mathbb{Q}_p]}$

We will be done if we can show

(i) $\mathrm{im}(\kappa_v) \subset \mathrm{im}(\varepsilon_v)$

(ii) $\mathrm{im}(\varepsilon_v)$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v : \mathbb{Q}_p]} \times T$ where T is a finite group.

For then we would have $\mathrm{im}(\varepsilon_v) = \mathrm{im}(\kappa_v) \times T$ and since $\mathrm{im}(\kappa_v)$ is divisible (because it is the image of a divisible group) we would then obtain

$$\mathrm{im}(\varepsilon_v)_{\mathrm{div}} = \mathrm{im}(\kappa_v)_{\mathrm{div}} = \mathrm{im}(\kappa_v).$$

(i) The exact sequence (6.6) induces the following long exact sequence of cohomology groups

$$\begin{tikzcd}
 & H^0(K_v, E[p^\infty]) \arrow[r] & H^0(K_v, \tilde{E}[p^\infty]) \arrow[dll, rounded corners] \\
H^1(K_v, \mathcal{F}[p^\infty]) \arrow[r, "\varepsilon_v"] & H^1(K_v, E[p^\infty]) \arrow[r, "\pi_v"] & H^1(K_v, \tilde{E}[p^\infty]) \arrow[dll, rounded corners] \\
H^2(K_v, \mathcal{F}[p^\infty]) & &
\end{tikzcd}$$

We see then that $\mathrm{im}(\varepsilon_v) = \ker(\pi_{\mathrm{v}})$, hence the inclusion $\mathrm{im}(\kappa_v) \subset \mathrm{im}(\varepsilon_v)$ would follow if we can show that $\pi_v \circ \kappa_v$ is the zero map. Let $[\varphi] \in \mathrm{im}(\kappa_v)$ be a cohomology class, with φ as a representative 1-cocycle, then there exists $Q \in E(\bar{K}_v)$ such that $\varphi(g) = g(Q) - Q$ for all $g \in G_{K_v}$. The reduction map $E[p^\infty] \to \tilde{E}[p^\infty]$ induces the cocycle $\bar{\varphi}$ where $\tilde{\varphi} = g(\tilde{Q}) - \tilde{Q}$ for all $g \in G_{K_v}$ where $\bar{Q} \in \tilde{E}(\bar{k}_v)$ is the reduction of Q. That is $\pi_v([\varphi]) = [\bar{\varphi}] \in H^1(K_v, \tilde{E}[p^\infty])$. $[\bar{\varphi}]$ is a principal crossed homomorphism, hence is a trivial cohomology class in $H^1(K_v, \tilde{E}(\bar{k}_v))$. But $\tilde{E}(\bar{k}_v)$ is a torsion group therefore its p-primary subgroup $\tilde{E}[p^\infty]$ is a direct summand, therefore we have $\tilde{E}(\bar{k}_v) = \tilde{E}[p^\infty] \times T$ for some prime to p torsion group T. Hence $\pi_v([\varphi]) = [\bar{\varphi}]$ is indeed trivial on $\tilde{E}[p^\infty]$ as well hence $\mathrm{im}(\kappa_v) \subset \mathrm{im}(\varepsilon_v)$ as was to be shown.

(ii) Taking cohomology on the short exact sequence (6.6) we obtain the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{F}[p^\infty]^{G_{K_v}} \arrow[r] & E[p^\infty]^{G_{K_v}} \arrow[r] & \tilde{E}[p^\infty]^{G_{K_v}} \arrow[dll, rounded corners] \\
 & H^1(K_v, \mathcal{F}[p^\infty]) \arrow[r, "\varepsilon_v"] & H^1(K_v, E[p^\infty]). &
\end{tikzcd}$$

Now

$$\tilde{E}[p^\infty]^{G_{K_v}} = \tilde{E}[p^\infty]^{G_{k_v}} = \tilde{E}(k_v)[p^\infty] = \tilde{E}(k_v)_p$$

is a finite group. (Note that the first equality follows from the fact that G_{K_v} acts on $\tilde{E}[p^\infty]$ through G_{k_v}). We would be done if we can show that the $\mathbb{Z}_p$-corank of $H^1(K_v, \mathcal{F}[p^\infty])$ is $[K_v\colon \mathbb{Q}_p]$. Lemma 6.2.9 below will prove this thereby completing our proof.

□

Because of the considerable importance of the next lemma we will give two proofs. The first, which is easier and often more effective, uses in an essential way the duality results of Tate and Poitou on Galois cohomology of local fields. The second will be "Iwasawa Theoretic" in the sense that is exploits the structure theory of Iwasawa modules and indeed the results about Iwasawa modules we shall use are accredited to Kenkichi Iwasawa [22]. For the sake of continuity, we defer the second proof to the end of this section since the argument is somewhat long.

Let A be a discrete G_{K_v}-module with $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as a $\mathbb{Z}_p$-module. We also let $\widehat{A}(1)$ denote the G_{K_v}-module $\mathrm{Hom}(A, \mu_{p^\infty})$. $\widehat{A}(1)$ is called the *Tate twist* of A and when A is a finite module, it clearly has the same order as A.

We shall frequently use the following terminology. Let A be a p-primary abelian group, A can therefore be regarded as a $\mathbb{Z}_p$- module. If we put the discrete topology on A then its *Pontryagin dual* $\widehat{A} = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact $\mathbb{Z}_p$-module. We say that A is *cofinitely generated* as a $\mathbb{Z}_p$-module if $\widehat{A}$ is finitely generated as a $\mathbb{Z}_p$-module. We define $\mathrm{corank}_{\mathbb{Z}_p} A$ to be the rank of $\widehat{A}$ as a $\mathbb{Z}_p$-module.

Lemma 6.2.9. (Corank Lemma)

(i) Let K_v be a finite extension of $\mathbb{Q}_p$. Let A be a discrete G_{K_v}-module with $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as a $\mathbb{Z}_p$-module. Then $H^1(K_v, A)$ is a cofinitely generated $\mathbb{Z}_p$-

module and

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, A) = r[K_v\colon \mathbb{Q}_p] + \mathrm{corank}_{\mathbb{Z}_p} H^0(K_v, A) + \mathrm{rank}_{\mathbb{Z}_p} H^0(K_v, \widehat{A}(1)).$$

(ii) Let K_v be a finite extension of $\mathbb{Q}_l$ where $l \neq p$. Then $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated with corank equal to

$$\mathrm{corank}_{\mathbb{Z}_p} H^0(K_v, A) + \mathrm{rank}_{\mathbb{Z}_p} H^0(K_v, \widehat{A}(1)).$$

We first state the following deep result without proof.

Theorem 6.2.10. (Poitou-Tate) Let A be a finite p-primary G_{K_v}-module, with order $|A| = p^a$. Then

(i) $\prod_{i=0}^{2} |H^i(K_v, A)|^{(-1)^i} = \begin{cases} p^{-a[K_v\colon \mathbb{Q}_p]} & \text{if } v \mid p, \\ 1 & \text{if } v \nmid p. \end{cases}$

(ii) $H^2(K_v, A)$ is the Pontryagin dual of $H^0(K_v, \widehat{A}(1))$ and hence has the same order.

Proof. (see [32] page 324) □

The result above extends to infinite p-primary G_{K_v}-modules as we now show.

Corollary 6.2.11. (Poitou-Tate) Let A be a p-primary G_{K_v}-module. Then

(i) $\sum_{i=0}^{2} (-1)^i \mathrm{corank}_{\mathbb{Z}_p}(H^i(K_v, A)) = \begin{cases} -[K_v\colon \mathbb{Q}_p]\mathrm{corank}_{\mathbb{Z}_p}(A) & \text{if } v \mid p, \\ 0 & \text{if } v \nmid p. \end{cases}$

(ii) $H^2(K_v, A)$ is the Pontryagin dual of $H^0(K_v, \widehat{A}(1))$. Hence

$$\mathrm{corank}_{\mathbb{Z}_p}(H^2(K_v, A)) = \mathrm{rank}_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1))).$$

Proof. (i) Let A be a p-primary G_{K_v}-module. Then $A = \bigcup_n A[p^n]$, where each $A[p^n]$ has order p^{a_n} for some $a_n \geq 0$. Since the simple p-groups are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we have $a_n = \dim_{\mathbb{F}_p} A[p^n]$. For each n, $H^i(K_v, A[p^n])$ is a finite p-group. Therefore

$$\mid H^i(K_v, A[p^n]) \mid = p^{c_n^i}, \text{ with } c_n^i = \dim_{\mathbb{F}_p} H^i(K_v, A[p^n]).$$

By the theorem of Poitou and Tate,

$$\prod_{i=0}^{2} p^{c_n^i(-1)^i} = \begin{cases} p^{-a_n[K_v\colon \mathbb{Q}_p]} & \text{if } v \mid p, \\ 1 & \text{if } v \nmid p. \end{cases}$$

Hence we obtain

$$\sum_{i=0}^{2}(-1)^i \dim_{\mathbb{F}_p}(H^i(K_v, A[p^n]) = \begin{cases} -\dim_{\mathbb{F}_p}(A[p^n])[K_v\colon \mathbb{Q}_p] & \text{if } v \mid p, \\ 0 & \text{if } v \nmid p. \end{cases}$$

We have that $A = \bigcup_n A[p^n] = \varinjlim_{n} A[p^n]$ and $\varinjlim_{n} H^i(K_v, A[p^n]) = H^i(K_v, A)$. Hence $\dim_{\mathbb{F}_p} A[p^n] = \operatorname{corank}_{\mathbb{Z}_p} A$, and $\dim_{\mathbb{F}_p}(H^i(K_v, A[p^n])) = \operatorname{corank}_{\mathbb{Z}_p}(H^i(K_v, A))$. We have have proved the first part of our theorem.

(ii) The proof follows immediately by taking direct limits in theorem 6.2.10(ii).

□

We now finish the proof of proposition 6.2.9 by calculating $\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v, A)$ where $A = \mathcal{F}[p^\infty]$. Now $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ and $\widehat{A}(1) \cong \mathbb{Z}_p$. $H^0(K_v, A)$ is a subgroup of $H^0(K_v, E[p^\infty]) = E(K_v)_p$ which is finite hence $\operatorname{corank}_{\mathbb{Z}_p} H^0(K_v, A) = 0$. By Poitou-Tate duality, $H^2(K_v, A) \cong H^0(K_v, \widehat{A}(1))$ and since $\widehat{A}(1) \cong \mathbb{Z}_p$, G_{K_v} acts on $\widehat{A}(1)$ by a character $\varphi\colon G_{K_v} \to {\mathbb{Z}_p}^\times$, $H^0(K_v, \widehat{A}(1)) = 0$. Therefore $\operatorname{corank}_{\mathbb{Z}_p} H^2(K_v, A) = 0$. Hence by the corank lemma, $\operatorname{rank}_{\mathbb{Z}_p} H^1(K_v, A) = [K\colon \mathbb{Q}_p]$. This proves proposition 6.2.8(ii).

It will be important in the next section to have information about the index $[\operatorname{im}(\kappa_v)\colon \operatorname{im}(\varepsilon_v)]$.

Theorem 6.2.12. Let K_v be a finite extension of $\mathbb{Q}_p$ and let E/K_v be an elliptic curve with good ordinary reduction at v. Then $\mathrm{im}(\kappa_v)$ has finite index in $\mathrm{im}(\varepsilon_v)$, more precisely $|\mathrm{im}(\varepsilon_v)/\mathrm{im}(\kappa_v)| \leq |\tilde{E}(k_v)_p|$ where k_v is the residue field of v. In particular if $p \nmid |\tilde{E}(k_v)|$ then $\mathrm{im}(\kappa_v) = \mathrm{im}(\varepsilon_v)$

Proof. From the proof of lemma 6.2.9, we saw that $H^1(\widehat{K_v, \mathcal{F}}[p^\infty]) = \mathbb{Z}_p^{[K\,:\,\mathbb{Q}_p]} \times T$ hence $H^1(K_v, \mathcal{F}[p^\infty]) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K\,:\,\mathbb{Q}_p]} \times \hat{T}$ where $\hat{T}$ is a finite p-group. Thus $H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}} = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K\,:\,\mathbb{Q}_p]}$ and we obtain $H^1(K_v, \mathcal{F}[p^\infty])/H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}} = \hat{T}$. The multiplication by p^m map thus kills $H^1(K_v, \mathcal{F}[p^\infty])/H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}}$ for some $m \gg 0$. Therefore for such an m we have

$$p^m H^1(K_v, \mathcal{F}[p^\infty]) = H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}}.$$

Let $A = \mathcal{F}[p^\infty]$. Then for m as above consider the exact sequence

$$0 \longrightarrow A[p^m] \longrightarrow A \xrightarrow{p^m} A \longrightarrow 0.$$

Taking cohomology we obtain the long exact sequence

$$\cdots \longrightarrow H^1(K_v, A) \xrightarrow{p^m} H^1(K_v, A) \longrightarrow H^2(K_v, A[p^m]) \longrightarrow \cdots$$

Thus we see that $|H^1(K_v, \mathcal{F}[p^\infty])/H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}}|$, and hence $[\mathrm{im}(\kappa_v) \colon \mathrm{im}(\varepsilon_v)]$, is bounded above by $H^2(K_v, A[p^m])$ for $m \gg 0$. Now $H^2(K_v, A[p^m])$ has the same order as $H^0(K_v, \widehat{A[p^m]}(1))$ by Poitou-Tate duality. The exact sequence (6.6) and the Weil pairing induce the pairing.

$$A[p^m] \times \tilde{E}[p^m] \longrightarrow \mu_{p^m}$$

(recall $A = \mathcal{F}[p^\infty]$). Since Weil pairing is non-degenerate this pairing is non-degenerate. From this pairing we obtain

$$\mathrm{Hom}(A[p^m], \mu_{p^m}) \cong \tilde{E}[p^m]$$

as G_{K_v}-modules, which implies

$$\begin{aligned}\widehat{A[p^m]}(1) &= \mathrm{Hom}(A[p^m], \mu_{p^\infty})\\ &\cong \mathrm{Hom}(A[p^m], \mu_{p^m})\\ &\cong \tilde{E}[p^m]\end{aligned}$$

Thus $H^0(K_v, \widehat{A[p^m]}(1)) = H^0(K_v, \tilde{E}[p^m]) = \tilde{E}(k_v)_{p^m}$ for $m \gg 0$. Therefore $\mathrm{im}(\kappa_v)/\mathrm{im}(\varepsilon_v)$ is cyclic and

$$[\mathrm{im}(\kappa_v) \colon \mathrm{im}(\varepsilon_v)] \leq |\tilde{E}(\kappa_v)_{p^m}| \leq |\tilde{E}(\kappa_v)_p|.$$

The proof is complete. This inequality is actually an equality, but the above result is adequate for our purposes. □

Under certain restrictive hypothesis we can extend proposition 6.2.8 to infinite extensions. We make a few definitions first.

Definition 6.2.13. A **supernatural number** n is a formal product

$$n = \prod_p p^{n(p)}$$

where p runs through the set of prime numbers, and $n(p)$ is a positive integer or ∞.

If m is another supernatural number we say m divides n written $m \mid n$ if $m(p) \leq n(p)$ for all p. We can do algebra with supernatural numbers, with a few rules. We define $\infty + \infty = \infty$, $\infty + a = \infty$ where a is any finite integer (see [34] page 34). Thus we can define the LCM of two supernatural numbers n and m as follows.

$$\mathrm{LCM}(n, m) = \prod_p p^{s(n,m)}$$

where $s(n, m) = \max(n(p), m(p))$. Let G be a profinite group and let $\mathcal{U}$ be the set of all open normal subgroups of G. If H is a closed normal subgroup of G we define the profinite index of H in G as follows

$$[G : H] = \mathrm{LCM}\{[G/U : HU/U] \mid U \in \mathcal{U}\}$$

We then define the **profinite order** $\#G$ of G, as

$$\#G = [G : \{1\}] = \mathrm{LCM}\{G/U \mid U \in \mathcal{U}\}$$

Definition 6.2.14. Let L be an infinite Galois extension of K. We define the **profinite degree** of the extension L/K to be $\#G$ where $G - \mathrm{Gal}(L/K)$

Theorem 6.2.15. Let K_v be an extension of $\mathbb{Q}_p$ with finite residue field. Assume that p^∞ divides the profinite degree of $K_v/\mathbb{Q}_p$. Then $\mathrm{im}(\kappa_v) = \mathrm{im}(\varepsilon_v)$

Remark 6.2.16. The hypotheses in the above theorem are satisfied in particular if K_v is a ramified $\mathbb{Z}_p$ extension of F_v where F_v is a finite extension of $\mathbb{Q}_p$.

Proof. By the same argument as in proposition 6.2.8(i) we have $\mathrm{im}(\kappa_v) \subseteq \mathrm{im}(\varepsilon_v)$. Our strategy then is to show that $\mathrm{im}(\varepsilon_v)$ is divisible and that $\mathrm{im}(\varepsilon_v)/\mathrm{im}(\kappa_v)$ is finite, this will give our result. Now $K_v = \bigcup_n F_v^{(n)}$ where $F_v^{(n)}$ runs over all the finite extensions of $\mathbb{Q}_p$ contained in K_v. We define

$$\varepsilon_v^{(n)} \colon H^1(F_v^{(n)}, \mathcal{F}[p^\infty]) \to H^1(F_v^{(n)}, E[p^\infty])$$

$$\kappa_v^{(n)} \colon E(F_v^{(n)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(F_v^{(n)}, E[p^\infty]).$$

Now

$$H^1(K_v, E[p^\infty]) = \varinjlim_n H^1(F_v^{(n)}, E[p^\infty])$$

(see section 2.4) hence we have $\varepsilon_v = \varinjlim_n(\varepsilon_v^{(n)})$ and $\kappa_v = \varinjlim_n(\kappa_v^{(n)})$ which implies that $\mathrm{im}(\kappa_v)/\mathrm{im}(\varepsilon_v)$ is finite since it is the direct limit of the finite subgroups $\mathrm{im}(\kappa_v^{(n)})/\mathrm{im}(\varepsilon_v^{(n)})$ which by theorem 6.2.12 are uniformly bounded by $|\tilde{E}(k_v)_p|$.

We now show that $\mathrm{im}(\varepsilon_v)$ is divisible. By the map

$$\varepsilon_v \colon H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty]),$$

it is enough to show that $H^1(K_v, \mathcal{F}[p^\infty])$ is divisible. Now our assumption on the profinite degree implies that G_{K_v} contains an infinite pro-p subgroup hence has cohomological dimension 1 (see section 2.7 and [39] chapter 3). So $H^2(K_v, A) = 0$ for any G_{K_v}-module A.

Lct $A = \mathcal{F}[p^\infty]$. From thc short cxact scqucncc

$$0 \longrightarrow A[p] \longrightarrow A \xrightarrow{p} A \longrightarrow 0$$

we obtain thc long exact sequencc

$$\cdots \longrightarrow H^1(K_v, A) \xrightarrow{p} H^1(K_v, A) \longrightarrow H^2(K_v, A[p]) = 0 \longrightarrow \cdots$$

Thus $H^1(K_v, A)$ is p-divisible. But A is a p-primary group hence $H^1(K_v, A)$ is also p-primary. Thus $H^1(K_v, A)$ is in fact divisible, and our result is proved. □

We have gotten a satisfactory intrinsic description of the Selmer group in the case of good ordinary reduction at a prime v of K lying above p. We wonder what happens in the other cases. We first consider the case where E has split multiplicative reduction at a prime v of K lying above p.

If E has split multiplicative reduction at a prime v of K lying above p and K_v is a finite extension of $\mathbb{Q}_p$, then E/K_v is a Tate curve (see [41] page 422). Thus we have the parametrization

$$\overline{K_v}^\times / < q_E > \xrightarrow{\sim} E(\overline{K_v})$$

where $< q_E >$ is the infinite cyclic group of $\overline{K_v}^\times$ generated by the Tate period q_E of E. Now q_E has positive valuation so

$$\mu_{p^\infty} \cap < q_E > = 1. \qquad (6.7)$$

Our parametrization above induces the map

$$\mu_{p^\infty} \longrightarrow E(\overline{K_v}) \cong \overline{K_v}^\times / < q_E > .$$

This coupled with (6.7) gives us the following exact sequence

$$(6.8) \qquad 0 \to \mu_{p^\infty} \to E(\overline{K_v})[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

From (6.8) we obtain the long exact sequence

$$\cdots \to H^0(K_v, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_v, \mu_{p^\infty}) \xrightarrow{\varepsilon_v} H^1(K_v, E[p^\infty]) \to \cdots$$

Classical Kummer theory give us the isomorphism $K_v^\times/nK_v^\times \cong H^1(K_v, \mu_{p^n})$ and on taking projective limits we obtain $K_v^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p = H^1(K_v, \mu_{p^\infty})$. We have $K_v^\times = \pi^{\mathbb{Z}} \times U_{K_v}$ and $U_{K_v} \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[K_v:\,\mathbb{Q}_p]}$ (see [30] page 141) hence

$$K_v^\times \cong \mathbb{Z} \times \mathbb{Z}^{[K_v:\,\mathbb{Q}_p]} \times \texttt{finite group}.$$

Thus we have

$$H^1(K_v, \mu_{p^\infty}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\,\mathbb{Q}_p]+1}.$$

We also have $H^0(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p$, since G_{K_v} acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$. Therefore $\mathrm{im}(\varepsilon_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\,\mathbb{Q}_p]}$. By proposition 6.2.6(iii) we get

$$\mathrm{im}(\kappa_v) = \mathrm{im}(\varepsilon_v)$$

in the case of split multiplicative reduction.

Let E have non-split multiplicative reduction at a prime v of K lying above an odd prime p. Since $\varepsilon_v = \varinjlim_n \varepsilon_v^{(n)}$ and $\kappa_v = \varinjlim_n \kappa_v^{(n)}$ (see proof of theorem 6.2.15) , we are reduced to consider finite extensions K_{v_n} of K_v. If E becomes split over K_{v_n} then we are in the case just considered and we are done. If not then by the "Corank Lemma" we have

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, \mathcal{F}[p^\infty]) = [K_v\colon \mathbb{Q}_p]$$

and since $\mathcal{F}[p^\infty]$ has cohomological dimension 1, $H^1(K_v, \mathcal{F}[p^\infty])$ is divisible. Therefore $H^1(K_v, \mathcal{F}[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\,\mathbb{Q}_p]}$. This and proposition 6.2.6(iii) allows us to conclude that

$$\operatorname{im}(\kappa_v) = \operatorname{im}(\varepsilon_v).$$

Thus in the case of multiplicative reduction we have a somewhat better result than proposition 6.2.8 for the good ordinary reduction case.

We now look at the case that E has good supersingular reduction at a prime v of K lying above p. Now $\tilde{E}[p^\infty] = 0$ therefore we have an isomorphism $\mathcal{F}[p^\infty] \cong E[p^\infty]$ where $\mathcal{F}(\mathfrak{m})$ is this time the formal group of height 2. If K_v is a finite extension of $\mathbb{Q}_p$ and using our definition of the map ε_v above, we see that an isomorphism of the form $\operatorname{im}(\kappa_v) = \operatorname{im}(\varepsilon_v)_{\text{div}}$ as in the case of good ordinary reduction is certainly impossible. Despite this Bloch and Kato [4] have in this case an alternative "good" definition of $\operatorname{im}(\kappa_v)$. This definition allows us to describe $\operatorname{im}(\kappa_v)$ in a way that depends only on the G_{K_v}-module $E[p^\infty]$ and more satisfyingly it coincides with the description of $\operatorname{im}(\kappa_v)$ in the good ordinary reduction case. The description involves the mysterious ring B_{cris} introduced by Fontaine [11]. We can only manage little more than state Bloch-Kato's result. Some preparation first.

Let K_v be a finite extension of $\mathbb{Q}_p$ and let $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(E)$ is the Tate module of E. We define

$$H^1_f(K_v, V_p(E)) = \ker\left(H^1(K_v, V_p(E)) \to H^1(K_v, V_p(E) \otimes_{\mathbb{Q}_p} B_{\text{cris}})\right)$$

(We note that $V_p(E)$ contains $T_p(E)$ as a G_{K_v}-invariant $\mathbb{Z}_p$ lattice and $V_p(E)/T_p(E) \cong E[p^\infty]$). The map $V_p(E) \to E[p^\infty]$ induces the homomorphism $H^1(K_v, V_p(E)) \to H^1(K_v, E[p^\infty])$. Thus we have the commutative diagram

$$\begin{tikzcd}
H^1(K_v, V_p(E)) \arrow[r] & H^1(K_v, E[p^\infty]) \\
H^1_f(K_v, V_p(E)) \arrow[u, hook] \arrow[ur, "\phi"] &
\end{tikzcd}$$

Theorem 6.2.17. (Bloch-Kato) Let $H^1_f(K_v, E[p^\infty])$ denote $\mathrm{im}(\phi)$ in the above commutative diagram then

$$\mathrm{im}(\kappa_v) = H^1_f(K_v, E[p^\infty])$$

Proof. (see [4]) □

If K_v is an infinite extension of $\mathbb{Q}_p$, we say that K_v is *deeply ramified* if $H^1(K_v, \bar{\mathfrak{m}}) = 0$) . For "deeply ramified" extensions Hilbert satz 90 is true for formal groups i.e. $H^1(K_v, \mathcal{F}(\bar{\mathfrak{m}})) = 0$, where $\mathcal{F}(\bar{\mathfrak{m}})$ is the formal group of height 2 and $\bar{\mathfrak{m}}$ denotes the maximal ideal of the ring of integers of $\bar{\mathbb{Q}}_p$. Since $\mathcal{F}(\bar{\mathfrak{m}})$ is divisible we can imitate Kummer theory: we have the exact sequence

$$0 \to \mathcal{F}(\bar{\mathfrak{m}})[p^n] \to \mathcal{F}(\bar{\mathfrak{m}}) \xrightarrow{p^n} \mathcal{F}(\bar{\mathfrak{m}}) \to 0$$

and taking cohomology we have the long exact sequence

$$H^0(K_v, \mathcal{F}(\bar{\mathfrak{m}})) \xrightarrow{p^n} H^0(K_v, \mathcal{F}(\bar{\mathfrak{m}})) \to H^1(K_v, \mathcal{F}(\bar{\mathfrak{m}})[p^n]) \to 0$$

(we used Hilbert satz 90 for formal groups to get the last surjection). Thus we have $\mathcal{F}(\bar{\mathfrak{m}})/p^n\mathcal{F}(\bar{\mathfrak{m}}) \cong H^1(K_v, \mathcal{F}(\bar{\mathfrak{m}})[p^n])$ and taking inverse limits we obtain $\mathcal{F}(\bar{\mathfrak{m}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong H^1(K_v, \mathcal{F}(\bar{\mathfrak{m}})[p^\infty])$. But $E(\overline{K}_v)[p^\infty] \cong \mathcal{F}(\bar{\mathfrak{m}})[p^\infty]$ since $\tilde{E}[p^\infty] = 0$. Therefore

$$\mathrm{im}(\kappa_v) = H^1(K_v, E[p^\infty]).$$

In the next section we will use our descriptions of the Selmer groups to prove the main result of this chapter: "Mazur's control theorem ".

6.3 Control Theorems

In this section we study the Galois theoretic behaviour of Selmer Groups. The main result is the "Control Theorem" of Mazur. We also study consequences of this theorem concerning the behaviour of the Mordell-Weil group and the Tate-Shafarevich group in a $\mathbb{Z}_p$-extension.

Remark 6.3.1. R. Greenberg [16] in recent work has vastly generalized the "Control Theorem" to the case that the Galois group of the extension is a p-adic lie group. We will however merely note that such a generalization exists.

Let K be a finite extension of $\mathbb{Q}$ and E an elliptic curve defined over K.

Theorem 6.3.2. (Control Theorem) Assume that p is a prime and that E has good ordinary reduction at all primes of K lying over p. Assume that $K_\infty = \bigcup_n K_n$ is a $\mathbb{Z}_p$ extension of K. Then the natural maps

$$\mathrm{Sel}_E(K_n)_p \longrightarrow \mathrm{Sel}_E(K_\infty)_p{}^{\mathrm{Gal}(K_\infty/K_n)}$$

have finite kernels and cokernels, and their orders are bounded as $n \longrightarrow \infty$.

Proof. Let K_n denote the unique subfield of K_∞ containing K such that $[K_n : K] = p^n$. In section 6.1 we described the images of the local Kummer homomorphisms. (propositions 6.2.6 and 6.2.8). We base our proof of the Control Theorem on this description. Let E be an elliptic curve defined over K and let F be an algebraic extension of K. For every prime η of F, we let

$$\mathcal{H}_E(F_\eta) = H^1(F_\eta, E[p^\infty])/\mathrm{im}(\kappa_\eta)$$

and we also let $\mathcal{P}_E(F) = \prod_\eta \mathcal{H}_E(F_\eta)$, where η runs over all the primes of F. Thus the p-part of the selmer group can be written as

$$\mathrm{Sel}_E(F)_p = \ker\left(H^1(F, E[p^\infty]) \longrightarrow \mathcal{P}_E(F)\right)$$

where the map is induced by restricting cocycles to decompostion groups. We set

$$\mathcal{G}_E(F) = \mathrm{im}\left(H^1(F, E[p^\infty]) \longrightarrow \mathcal{P}_E(F)\right)$$

and let $F_\infty = \bigcup_n F_n$ be an arbitrary $\mathbb{Z}_p$-extension of F .

Consider the following commutative diagram with exact rows.

(6.1)

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_E(K_n)_p \arrow[r] \arrow[d, "s_n"] & H^1(K_n, E[p^\infty]) \arrow[r] \arrow[d, "h_n"] & \mathcal{G}_E(K_n) \arrow[r] \arrow[d, "g_n"] & 0 \\
0 \arrow[r] & \mathrm{Sel}_E(K_\infty)_p^{\Gamma^{p^n}} \arrow[r] & H^1(K_\infty, E[p^\infty])^{\Gamma^{p^n}} \arrow[r] & \mathcal{G}_E(K_\infty)^{\Gamma^{p^n}} &
\end{tikzcd}$$

Here $\Gamma^{p^n} = \mathrm{Gal}(K_\infty/K_n)$ as usual, and s_n , h_n and g_n are the natural restriction maps. The snake lemma gives us the following exact sequence.

(6.2)

$$0 \to \ker(s_n) \to \ker(h_n) \to \ker(g_n) \to \mathrm{coker}(s_n) \to \mathrm{coker}(h_n) \to \mathrm{coker}(g_n) \to 0.$$

We study $\ker(s_n)$ and $\mathrm{coker}(s_n)$ indirectly by studying $\ker(h_n)$, $\ker(g_n)$, $\mathrm{coker}(h_n)$, $\mathrm{coker}(g_n)$ in the above exact sequence. We do this in the following sequence of lemmas.

Lemma 6.3.3. The kernel of h_n is finite and has bounded order as n varies.

Proof. Let $H = \mathrm{Gal}(\bar{K}/K_\infty)$ and consider the inflation restriction sequence

$$0 \to H^1(G_{K_n}/H, E[p^\infty]^H) \to H^1(K_n, E[p^\infty]) \xrightarrow{h_n} H^1(K_\infty, E[p^\infty])^{\Gamma^{p^n}}.$$

Clearly $\ker(h_n) = H^1(G_{K_n}/H, E[p^\infty]^H)$. Let $B = E[p^\infty]^H$. Then $B = E(F_\infty)_p = E[p^\infty]^H$, the p-primary subgroup of $E(K_\infty)$. Now $G_{K_n}/H = \mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n}$ hence $\ker(h_n) = H^1(\Gamma^{p^n}, B)$. Let γ denote a topological generator of Γ. Since Γ^{p^n} is a topologically cyclic group $H^1(\Gamma^{p^n}, B) = B/(\gamma^{p^n} - 1)B$ (see [32] pg 68). Now considering $\phi = \gamma^{p^n} - 1$ as an endomorphism on B,

$$\ker(\phi) = \{P \in E(F_\infty)_p | (\gamma^{p^n} - 1)P = 0\} = \{P \in E(F_\infty)_p | \gamma^{p^n} P = P\}.$$

Since γ^{p^n} is a topological generator of $\mathrm{Gal}(K_\infty/K_n)$ we see that $P \in \ker(\phi)$ if and only if $P \in E(K_n)_p$. $E(K_n)$ is finitely generated hence it's p-primary part $E(K_n)_p$, is finite thus $\ker(\phi)$ is finite. Now by Lutz's theorem (c.f [40] chapter VII prop 6.3) $B = E(F_\infty)_p = E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p) \times \texttt{(finite group)}$. Therefore B_{div} has finite $\mathbb{Z}_p$-corank and

$$B_{\text{div}} \subseteq B/\ker(\phi) \cong \operatorname{im}(\gamma^{p^n} - 1) = (\gamma^{p^n} - 1)B \subseteq B$$

so

$$B_{\text{div}} \subseteq (\gamma^{p^n} - 1)B \subseteq B.$$

Thus

$$|H^1(\Gamma^{p^n}, B)| = |B/(\gamma^{p^n} - 1)B| \leq |B/B_{\text{div}}|$$

and $[B : B_{\text{div}}]$ is independent of n. □

Lemma 6.3.4. h_n is surjective i.e. $\operatorname{coker}(h_n) = 0$.

Proof. Consider the inflation restriction sequence

$$H^1(K_n, E[p^\infty]) \xrightarrow{h_n} H^1(K_\infty, E[p^\infty])^{\Gamma^{p^n}} \to H^2(\Gamma^{p^n}, B)$$

where $B = E[p^\infty]^{\Gamma^{p^n}} = H^0(\operatorname{Gal}(F_\infty/F_n), E[p^\infty])$. Γ^{p^n} is isomorphic to $\mathbb{Z}_p$ as topological groups hence Γ^{p^n} is a free pro-p group, consequently Γ^{p^n} has cohomological dimension 1 (see section 2.7), thus $H^2(\Gamma^{p^n}, B) = 0$ and h_n is surjective as claimed. □

We now determine $\ker(g_n)$. Let v be any prime of K, and let v_n denote any prime of K_n lying over v. We focus on each factor in $\mathcal{P}_E(K_n)$. Consider

$$r_{v_n} \colon \mathcal{H}_E((K_n)_{v_n}) \to \mathcal{H}_E((K_\infty)_\eta) \tag{6.3}$$

where η is any prime of K_∞ lying above v_n, ($\mathcal{P}_E(K_\infty)$ has a factor for all such η's, but the kernels are the same). If v is archimedean, then v splits completely in K_∞/K , i.e. $(K_\infty)_\eta = K_v$ for all $\eta \mid v$. Thus $\ker(r_{v_n}) = 0$. For nonarchimedean v, we consider separately $v \mid p$ and $v \nmid p$.

Lemma 6.3.5. Suppose v is a nonarchimedean prime of K not dividing p. Then $\ker(r_{v_n})$ is finite and has bounded order as n varies. If E has good reduction at v, then $\ker(r_{v_n}) = 0$ for all n.

Proof. Since $(K_n)_{v_n}$ and $(K_\infty)_\eta$ are algebraic extensions of K_v, by proposition 6.2.6 we have $\mathrm{im}((K_\infty)_\eta) = \mathrm{im}((K_n)_{v_n}) = 0$, hence

$$\mathcal{H}_E((K_n)_{v_n}) = H^1((K_n)_{v_n}, E[p^\infty]) \text{ and}$$

$$\mathcal{H}_E((K_\infty)_\eta) = H^1((K_\infty)_\eta, E[p^\infty]).$$

The inflation-restriction sequence

$$0 \to H^1(\Gamma_{v_n}, E[p^\infty]^{G(K_\infty)_\eta}) \to H^1((K_n)_{v_n}, E[p^\infty]) \xrightarrow{r_{v_n}} H^1((K_\infty)_\eta, E[p^\infty])$$

shows that $\ker(r_{v_n}) = H^1(\Gamma_{v_n}, E[p^\infty]^{G(K_\infty)_\eta})$ where

$$\Gamma_{v_n} = \mathrm{Gal}((F_\infty)_\eta/(K_n)_{v_n}) \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p$$

Let $B_v = H^0(K_\infty)_\eta, E[p^\infty])$. Then

$$\begin{aligned} B_v &= E[p^\infty]^{G(K_\infty)_\eta} \\ &= E((K_\infty)_\eta)_p \\ &= (\mathbb{Q}_p/\mathbb{Z}_p)^e \times \texttt{(finite group)},\ 0 \le e \le 2 \end{aligned}$$

Now $\ker(r_{v_n}) = B_v/(\gamma_{v_n} - 1)B_v$ where γ_{v_n} is a generator of Γ_{v_n}. The map

$$\phi\colon B_v \xrightarrow{\gamma_{v_n}-1} B_v$$

has finite kernel since $E((K_n)_{v_n})$ is finitely generated and hence has finite p-primary subgroup. We thus conclude as in lemma 6.3.3 that $|\ker(r_{v_n})| \le |B_v/(B_v)_{\mathrm{div}}|$ which is independent of n and v_n. If E has good reduction at v then since $v \nmid p$, $K_v(E[p^\infty])/K_v$ is an unramified extension (see [40] chap 7). The formalism of the Weil pairing gives $(K_\infty)_\eta \subset K_v(E[p^\infty])$ and $\Delta = \mathrm{Gal}(K_v(E[p^\infty])/K_v)$ is a finite cyclic group of order prime to p. Now $E[p^\infty]^\Delta$ is divisible hence $B_v = (B_v)_{\mathrm{div}}$ and $\ker(r_{v_n}) = 0$ □

Now assume that $v \mid p$. For each n, let f_{v_n} denote the residue field for $(K_n)_{v_n}$. Either v splits completely in K_∞/K, v is ramified in K_∞/K or v is unramified but finitely decomposed in K_∞/K. In the first two cases the finite field f_{v_n} stabilizes, and so f_η is finite, where f_η is the residue field for any prime η of K_∞ lying over p. Let $\tilde{E}$ denote the reduction of E at v.

Lemma 6.3.6. Suppose that v is a prime of K dividing p. If E has good ordinary reduction at v, then $\ker(r_{v_n})$ is finite and has bounded order as n varies.

Proof. If v splits completely in K_∞/K then $\ker(r_{v_n}) = 0$ for all n. If v is ramified in K_∞/K then by theorem 6.2.15, $\mathrm{im}(\kappa_{v_n}) = \mathrm{im}(\varepsilon_{v_n})$ so we can factor r_{v_n} as follows

$$\begin{tikzcd}
H^1((K_n)_{v_n}, E[p^\infty])/\mathrm{im}(\kappa_{v_n}) \arrow[r, "a_{v_n}"] \arrow[dr, "r_{v_n}"] & H^1((K_n)_{v_n}, E[p^\infty])/\mathrm{im}(\varepsilon_{v_n}) \arrow[d, "b_{v_n}"] \\
 & H^1((K_\infty)_\eta, E[p^\infty])/\mathrm{im}(\varepsilon_\eta)
\end{tikzcd}$$

Since a_{v_n} is surjective

$$|\ker(r_{v_n})| = |\ker(a_{v_n})| \cdot |\ker(b_{v_n})|.$$

But $\ker(a_{v_n}) = \mathrm{im}(\varepsilon_{v_n})/\mathrm{im}(\kappa_{v_n})$, therefore by theorem 6.2.12 we have $|\ker(a_{v_n})| \leq |\tilde{E}(f_\eta)_p|$, so the order is bounded by a finite group. The exact sequence

$$0 \to \mathcal{F}[p^\infty] \to E[p^\infty] \xrightarrow{\pi} \tilde{E}[p^\infty] \to 0$$

on the other hand gives us the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1((K_n)_{v_n}, E[p^\infty])/\mathrm{im}(\varepsilon_{v_n}) \arrow[r, "\pi_{v_n}"] \arrow[d, "b_{v_n}"] & H^1((K_n)_{v_n}, \tilde{E}[p^\infty]) \arrow[d, "c_{v_n}"] \\
0 \arrow[r] & H^1((K_\infty)_\eta, E[p^\infty])/\mathrm{im}(\varepsilon_\eta) \arrow[r, "\pi_\eta"] & H^1((K_\infty)_\eta, \tilde{E}[p^\infty])
\end{tikzcd}$$

The snake lemma gives $|\ker(b_{v_n})| \leq |\ker(c_{v_n})|$. The inflation-restriction sequence

$$0 \to H^1((K_\infty)_\eta/(K_n)_{v_n}, \tilde{E}(f_\eta)_p) \to H^1((K_n)_{v_n}, \tilde{E}[p^\infty]) \xrightarrow{c_{v_n}} H^1((K_\infty)_\eta, \tilde{E}[p^\infty])$$

shows that $\ker(c_{v_n}) = H^1((K_\infty)_\eta/(K_n)_{v_n}, \tilde{E}(f_\eta)_p)$. Since $\mathrm{Gal}((K_\infty)_\eta/(K_n)_{v_n})$ is topologically cyclic with generator say γ_{v_n} we have

$$\ker(c_{v_n}) = \tilde{E}(f_\eta)_p/(\gamma_{v_n} - 1)\tilde{E}(f_\eta)_p.$$

So $|\ker(c_{v_n})| \leq |\tilde{E}(f_\eta)_p|$ and

$$|\ker(r_{v_n})| \leq |\tilde{E}(f_\eta)_p|^2$$

in the case that v is ramified.

If v is unramified but finitely decomposed in K_∞/K, then $(K_\infty)_\eta$ is the unramified $\mathbb{Z}_p$-extension of K_v. f_η is infinite in this case. By the Kummer exact sequence 6.3 (after restricting to the p-part of the sequence and replacing K by $(K_n)_{v_n}$), we have $H^1((K_n)_{v_n}, E[p^\infty])/\operatorname{im}((K_n)_{v_n}) = H^1((K_n)_{v_n}, E(\overline{(K_n)}_{v_n}))$. Similary for $H^1((K_\infty)_\eta, E[p^\infty])/\operatorname{im}((K_\infty)_\eta)$, hence

$$\ker(r_{v_n}) = \ker(H^1((K_n)_{v_n}, E) \to H^1((K_\infty)_\eta, E)).$$

A simple inflation restriction argument, shows that

$$\ker(r_{v_n}) = H^1((K_\infty)_\eta/(K_n)_{v_n}, E((K_\infty)_\eta))$$

Let $L = (K_\infty)_\eta$ and $M = (K_n)_{v_n}$. Let l and m be the residue fields of L and M respectively. We want to show that $\ker(r_{v_n}) = H^1(L/M, E(L)) = 0$. From the reduction map, we have the short exact sequence

$$0 \to \mathcal{F}(\mathfrak{m}) \to E(L) \xrightarrow{\pi} \tilde{E}(l)) \to 0,$$

where $\mathfrak{m}$ is the maximal ideal of L. Taking cohomology we have the long exact sequence

$$\cdots \to H^1(L/M, \mathcal{F}(\mathfrak{m})) \to H^1(L/M, E(L)) \to H^1(L/M, \tilde{E}(l)) \to 0$$

We have to show that both $H^1(L/M, \mathcal{F}(\mathfrak{m}))$ and $H^1(L/M, \tilde{E}(l))$ vanish. The formal group $\mathcal{F}(\mathfrak{m})$ has a filtration ([40] pg 118),

$$\mathcal{F}(\mathfrak{m}) \supset \mathcal{F}(\mathfrak{m}^1) \supset \mathcal{F}(\mathfrak{m}^2) \cdots \mathcal{F}(\mathfrak{m}^n) \cdots$$

and we also have the isomorphism $\mathcal{F}(\mathfrak{m}^i)/\mathcal{F}(\mathfrak{m}^{i+1}) = l$. Since L/M is an finite unramified p-extension we have $\mathrm{Gal}(L/M) = \mathrm{Gal}(l/m)$. Taking cohomology on the exact sequence

$$0 \to \mathcal{F}(\mathfrak{m}^{i+1}) \to \mathcal{F}(\mathfrak{m}^i) \to l \to 0$$

we have the long exact sequence

$$\begin{tikzcd}
\cdots \arrow[r] & H^0(L/M, l) \arrow[r] & H^1(L/M, \mathcal{F}(\mathfrak{m}^{i+1})) \arrow[dl] \\
& H^1(L/M, \mathcal{F}(\mathfrak{m}^i)) \arrow[r] & H^1(l/m, l) = 0
\end{tikzcd}$$

The vanishing of the last cohomology group is theorem ([37],Chap X, prop 1). By the above long exact sequence we would be done if we can show that $H^1(L/M, \mathcal{F}(\mathfrak{m}^i)) = 0$, for large i. The formal logarithm converges for large i hence $\mathcal{F}(\mathfrak{m}^i) = \mathfrak{m}^i$ for $i \gg 0$. We thus obtain $H^1(L/M, \mathcal{F}(\mathfrak{m}^i)) = H^1(L/M, \mathfrak{m}^i)$. Now $H^1(L/M, \mathfrak{m}^i) = 0$ since $\mathfrak{m}^i$ is an induced module.

We now show that $H^1(L/M, \tilde{E}(l)) = 0$. We use similar arguments to the ones above. We have the inflation restriction sequence

$$0 \to H^1(L/M, \tilde{E}(l)) \to H^1(m^{\mathrm{unr}}/m, \tilde{E}(m^{\mathrm{unr}})) \to H^1(m^{\mathrm{unr}}/l, \tilde{E}(m^{\mathrm{unr}}))^{\mathrm{Gal}(m^{\mathrm{unr}}/l)} \to \cdots$$

where m^{unr} is the maximal unramified extension of m. We will be done if we can show that $H^1(m^{\mathrm{unr}}/m, \tilde{E}(m^{\mathrm{unr}})) = 0$. Now $\mathrm{Gal}(m^{\mathrm{unr}}/m) \cong \mathrm{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v)$. By the long exact sequence coming from the short exact sequence

$$0 \to \mathcal{F}(\mathfrak{m}) \to E(m^{\mathrm{unr}}) \to \tilde{E}(\bar{\mathbb{F}}_v) \to 0,$$

where $\mathfrak{m}$ is the maximal ideal of m^{unr}. It suffices to show that $H^1(\text{Gal}(m^{\text{unr}}/m), \mathcal{F}(\mathfrak{m}))$ and $H^1(\mathbb{F}_v, \tilde{E})$ are both zero. Now if $\mathcal{C}$ is any curve over $\mathbb{F}_v$, the Hasse bound shows that $\mathcal{C}(\mathbb{F}_v)$ is non empty and therefore we know that $\tilde{E}$ has no nontrivial principal homogeneous spaces. This is the same as the claim that $H^1(\mathbb{F}_v, \tilde{E}) = 0$. The formal group $\mathcal{F}(\mathfrak{m})$ has a filtration ([40] pg 118),

$$\mathcal{F}(\mathfrak{m}) \supset \mathcal{F}(\mathfrak{m}^1) \supset \mathcal{F}(\mathfrak{m}^2) \cdots \mathcal{F}(\mathfrak{m}^n) \cdots ,$$

and we have an exact sequence

$$0 \to \mathcal{F}(\mathfrak{m}^{i+1}) \to \mathcal{F}(\mathfrak{m}^i) \to \bar{\mathbb{F}}_v \to 0$$

for each $i \geq 1$. The long exact sequence associated to this exact sequence reduces the problem of proving $H^1(\text{Gal}(m^{\text{unr}}/m), \mathcal{F}(\mathfrak{m})) = 0$, to that of proving that $H^1(\text{Gal}(m^{\text{unr}}/m), \mathcal{F}(\mathfrak{m}^i)) = 0$, for some higher $i \geq 1$. If i is sufficiently large, then the formal logarithm converges and this shows that

$$H^1(\text{Gal}(m^{\text{unr}}/m), \mathcal{F}(\mathfrak{m}^i)) = H^1(\text{Gal}(m^{\text{unr}}/m), \mathfrak{m}^i)$$

which is zero since the group $\mathfrak{m}^i$ is an induced module. This completes the proof of lemma 6.3.6 . □

Lemma 6.3.7. The order of $\ker(g_n)$ is bounded as n varies.

Proof. Let v be any prime of K. If v splits completely in K_∞/K then $\ker(r_{v_n}) = 0$ and these primes do not contribute to $\ker(g_n)$. For all the other primes v of K the number of primes lying above v is bounded as $n \to \infty$. If E has good ordinary reduction at v and $v \nmid p$ then $\ker(r_{v_n}) = 0$ and these primes also do not contribute to $\ker(g_n)$. Thus there are only finitely many primes $v \mid p$ that need to be considered and for each such v there are a bounded number of v_n's . For these v_n's lemma 6.3.5 and lemma 6.3.6 imply that $\ker(r_{v_n})$ is bounded as n varies, hence $\ker(g_n) = \prod_{v_n} \ker(r_{v_n})$ is bounded as n varies and our proof is complete.

□

We now finish off the proof of the "Control Theorem". Lemma 6.3.3 implies that $\ker(s_n)$ is finite and has bounded order no matter what type of reduction E has at $v \mid p$. By lemmas 6.3.4 and 6.3.7. Since these fit into the exact sequence 6.2, we see that cokers_n is finite and of bounded order, assuming that E has good ordinary reduction at all $v \mid p$. The proof of the Mazur's "Control Theorem" is now complete. □

We now present some consequences of Mazur's control theorem. We will show that the order of the p-part of the Selmer group is controlled for large n. We will also study the ranks of the Selmer groups asymptotically in a $\mathbb{Z}_p$-extension.

We recall some notation: we denote by Γ a group non canonically isomorphic to the p-adic integers $\mathbb{Z}_p$. We also denote the **Iwasawa Algebra** by Λ i.e.

$$\Lambda := \varprojlim_n \mathbb{Z}_p[[\Gamma/\Gamma^{p^n}]] = \mathbb{Z}_p[[\Gamma]].$$

We also define an Iwasawa module to be a compact Λ-module. By choosing a topological generator γ of Γ, the Iwasawa algebra can be identified with the power series ring $\mathbb{Z}_p[[T]]$ using the map $\gamma \to 1 + T$.

Definition 6.3.8. Let A be discrete Λ-module, we say A is Λ-*cotorsion* if its Pontryagin dual $\hat{A} = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is a Λ-torsion module. A is Λ-*cofinitely* generated if $\hat{A}$ is a finitely generated Λ-module.

Corollary 6.3.9. Let E be an elliptic curve defined over K and let p be a prime such that E has good ordinary reduction at all primes of K lying over p. Suppose also that $\mathrm{Sel}_E(K)_p$ is finite. Then $\mathrm{Sel}_E(K_\infty)_p$ is Λ-cotorsion and $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded as n varies.

Proof. Since $\mathrm{Sel}_E(K)_p$ is finite we have by the control theorem that ${\mathrm{Sel}_E(K_\infty)_p}^{\mathrm{Gal}(K_\infty/K_n)}$ is finite. Let X be the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ i.e.

$$X = \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since X is a p-primary abelian group we can equip X with the structure of a Λ-module. Taking the Pontryagin dual we obtain $\mathrm{Sel}_E(K_\infty)_p \cong \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. $\mathrm{Sel}_E(K_\infty)_p$ thus inherits a natural Λ action given by $(\gamma f)(x) = (\gamma f)(\gamma^{-1}x)$ where $f \in \mathrm{Sel}_E(K_\infty)_p$ and γ is a topological generator of Γ. If f is fixed by Γ then $f(\gamma^{-1}x) = \gamma^{-1}f(x)$ and we see that such an f is a Γ equivariant homomorphism, hence

$${\mathrm{Sel}_E(K_\infty)_p}^\Gamma = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)^\Gamma = \mathrm{Hom}_\Gamma(X, \mathbb{Q}_p/\mathbb{Z}_p)$$

Since f is a Γ equivariant homomorphism, then

$$f((\gamma - 1)x) = f(\gamma x - x) = \gamma \cdot f(x) - f(x) = 0.$$

We see then that f factors through $X/(\gamma - 1)X = X/TX$ (this is the maximal quotient on which Γ acts trivially). Therefore

$${\mathrm{Sel}_E(K_\infty)_p}^\Gamma = \mathrm{Hom}_\Gamma(X, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}(X/TX, \mathbb{Q}_p/\mathbb{Z}_p)$$

Hence $|X/TX| = |{\mathrm{Sel}_E(K_\infty)_p}^\Gamma|$ which is finite by assumption, but $|X/\mathfrak{m}X| = |X/(p,T)X| \leq |X/TX|$. Thus $X/\mathfrak{m}X$ is finite as well. By Nakayama's lemma 4.2.9 we see that X is a finitely generated torsion Λ-module. Its dual $\mathrm{Sel}_E(K_\infty)_p$ is thus Λ-cotorsion. Now

$$X/X_{\mathbb{Z}_p-\mathrm{tors}} \cong \mathbb{Z}_p^\lambda$$

for some $\lambda \geq 0$. Taking duals, $(\mathrm{Sel}_E(K_\infty)_p)_{\text{ div}} = (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$, and by the "Control Theorem" $\mathrm{Sel}_E(K_n)_p$ maps to $\mathrm{Sel}_E(K_\infty)_p{}^{\Gamma_n}$ with finite kernel. Hence

$$(\mathrm{Sel}_E(K_n)_p)_{\text{ div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n}$$

where $t_n \leq \lambda$. By the fundamental exact sequence (6.2)

$$E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\text{rank}(E(K_n))}$$

is a subgroup of $(\mathrm{Sel}_E(K_n)_p)_{\text{ div}}$. Hence

$$\text{rank}(E(K_n)) \leq \lambda$$

for all $n \geq 0$ □

It is possible that the p-primary part of the Selmer group over K_∞ vanishes, hence also rank$(E(K_n))$. We establish in the next corollary under which conditions this might happen.

Definition 6.3.10. Let v be a prime of K where E has good ordinary reduction. If the characteristic of the residue field k_v divides $|\tilde{E}(k_v)|$, then v is called an **anomalous** prime for E.

Corollary 6.3.11. Let E be an elliptic curve defined over K and let p be a prime such that E has good ordinary reduction at all primes of K lying over p. Suppose that $\mathrm{Sel}_E(K)_p = 0$, that no prime of K over p is anomalous for E, and that $E(K_v)_p = 0$ for all primes v of K where E has bad reduction. Then $\mathrm{Sel}_E(K_\infty)_p = 0$

Proof. We claim that the map

$$\mathrm{Sel}_E(K)_p \longrightarrow \mathrm{Sel}_E(K_\infty)_p{}^{\mathrm{Gal}(K_\infty/K)}$$

is surjective. By hypothesis $\mathrm{Sel}_E(K)_p = 0$, hence $\mathrm{Sel}_E(K_\infty)_p{}^\Gamma = 0$, which implies that its dual $X/TX = 0$, where $X = \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. By Nakayama's lemma 4.2.9 we have X = 0, hence

$$\mathrm{Sel}_E(K_\infty)_p = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

We now verify our claim:

Let v be a prime of K such that $v|p$. If v is unramified in K_∞/K then by arguments carried out in lemma 6.3.6 $\ker(r_v) = 0$. If v is ramified in K_∞/K, let f_η be the residue field for a prime η of K_∞ above v. Then f_η/f_v is a finite p-extension. By the reduction map we have the short exact sequence

$$0 \longrightarrow \mathcal{F}[p^\infty] \longrightarrow E(K_\infty)[p^\infty] \xrightarrow{\pi} \tilde{E}(f_\eta)[p^\infty] \longrightarrow 0.$$

Now $\tilde{E}(f_\eta)_p^{\mathrm{Gal}(f_\eta/f_v)} = \tilde{E}(f_v)_p = 0$, by hypothesis and since $\mathrm{Gal}(f_\eta/f_v)$ is a p-group acting on a p-group, it follows that $\tilde{E}(f_\eta)_p = 0$. Hence by the first part of lemma 6.3.6 we have $|\ker(r_v)| \leq |\tilde{E}(f_\eta)_p|^2 = 0$ therefore $\ker(r_v) = 0$. If v is a prime of K where E has bad reduction, then by hypothesis $v \nmid p$. Let η be a prime of K_∞ lying above v. Then $\mathrm{Gal}((K_\infty)_\eta/K_v) = \mathrm{Gal}(f_\eta/f_v)$ is either 0 or is isomorphic to $\mathbb{Z}_p$. We thus have $E((K_\infty)_\eta)_p^{\mathrm{Gal}((K_\infty)_\eta/K_v)} = E(K_v)_p = 0$, hence it follows that $E((K_\infty)_\eta)_p = 0$. We recall that in lemma 6.3.5 we defined $B_v = H^0((K_\infty)_\eta, E[p^\infty])$ this is just $E((K_\infty)_\eta)_p$ and this vanishes by the arguments above. Since in lemma 6.3.5 we proved that

$$\ker(r_v) = H^1(\Gamma_v, B_v) = B_v/(\gamma - 1)B_v,$$

we thus see that $\ker(r_v) = 0$ for all primes v of K lying above p, hence these primes do not contribute to $\ker(g_0)$ in lemma 6.3.7, therefore $\ker(g_0) = 0$. By lemma 6.3.4 we already have $\mathrm{coker}(h_0) = 0$ hence from exact sequence 6.2 we see that $\mathrm{coker}(s_0) = 0$. Therefore the map is surjective as claimed. □

Corollary 6.3.12. Let E be an elliptic curve defined over K and let p be a prime such that E has good ordinary reduction at all primes of K lying over p. Let K_∞/K be a $\mathbb{Z}_p$-extension. Suppose that both $E(K_n)$ and $Ш(K_n, E)_p$ are finite for all n. Then there exists integers $\lambda, \mu \geq 0$ depending only on E and K_∞/K such that

$$|Ш(K_n, E)_p| = p^{\mu p^n + \lambda n + o(1)} \text{ as } n \longrightarrow \infty.$$

Remark 6.3.13. The hypothesis that $E(K_n)$ is finite is not neccesary, it only simplifies our arguments. See theorem 1.10 in [13] for proof a which does not use this hypothesis.

Proof. Let X be the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ i.e.

$$X = \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since X is a p-primary abelian group it has a natural Γ-module structure. Taking the Pontryagin dual we obtain $\mathrm{Sel}_E(K_\infty)_p \cong \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. $\mathrm{Sel}_E(K_\infty)_p$ inherits a natural Λ action given by $(\gamma \cdot f)(x) = (\gamma f)(\gamma^{-1}x)$ where $f \in \mathrm{Sel}_E(K_\infty)_p$ and γ is a topological generator of Γ. If f is fixed by Γ then $f(\gamma^{-1}x) = \gamma^{-1}f(x)$ and we see that such an f is a Γ equivariant homomorphism. Now Γ^{p^n} is a closed subgroup of Γ. Hence Γ^{p^n} acts on $\mathrm{Sel}_E(K_\infty)_p$ through the induced natural action given by $(\gamma^{p^n} \cdot f)(x) = (\gamma^{p^n} f)((\gamma^{p^n})^{-1}x)$. Thus we have $f(((\gamma^{p^n})^{-1} - 1)x) = 0$ i.e.f factors through $((\gamma^{p^n})^{-1} - 1)X$. We thus have

$$\text{(6.4)} \qquad \mathrm{Sel}_E(K_\infty)_p{}^{\Gamma^{p^n}} = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma^{p^n}} = \mathrm{Hom}(X/(\gamma^{p^n} - 1)X, \mathbb{Q}_p/\mathbb{Z}_p).$$

Since $\gamma^{p^n} - 1 = \omega_n = (1+T)^{p^n} - 1$ we have $X/(\gamma^{p^n} - 1)X = X/\omega_n X$. From equation 6.4 we obtain $|\mathrm{Sel}_E(K_\infty)_p{}^{\Gamma^{p^n}}| = |X/\omega_n X|$. We claim that $\mathrm{Sel}_E(K_\infty)_p{}^{\Gamma^{p^n}}$ is finite, hence also $|X/\omega_n X|$ for all n. For $n = 0$ we have that $X/\omega_0 X = X/TX$

is finite, it then follows by Nakayama's lemma 4.2.9, that X is a finitely generated Λ-torsion module. Let ϕ denote the map appearing in the "Control Theorem" so that we have $|\mathrm{Sel}_E(K_n)_p|/\ker(\phi) \cong \mathrm{im}(\phi)$. Hence $|\mathrm{Sel}_E(K_n)_p| = |\ker(\phi)||\mathrm{im}(\phi)|$. By the "Control Theorem", $|\ker(\phi)| = p^{e_n}$ where e_n is bounded as n varies. Since ϕ is not surjective, we also have $|\mathrm{im}(\phi)| \lneqq |\mathrm{Sel}_E(K_\infty)_p{}^{\Gamma^{p^n}}|$. Therefore $|\mathrm{Sel}_E(K_n)_p| \lneqq p^{e_n}|X/\omega_n X|$. However, since X is a finitely generated Λ-torsion module, we have by theorem 4.2.14 that

$$|X/\omega_n X| = p^{\mu p^n + \lambda n + o(1)}$$

for $n \gg 0$. We thus obtain for $n \gg 0$,

$$|\mathrm{Sel}_E(K_n)_p| = p^{e_n} \cdot p^{\mu p^n + \lambda n + o(1)} = p^{\mu p^n + \lambda n + o(1)}.$$

By the fundamental exact sequence 6.2

$$|\mathrm{Sel}_E(K_n)_p| = |E(K_n)/nE(K_n)||Ш(K_n, E)_p|$$

and since by hypothesis, $E(K_n)$ is finite it follows that

$$|Ш(K_n, E)_p| = p^{\mu p^n + \lambda n + o(1)}$$

as $n \longrightarrow \infty$, and our proof is complete save for the claim, which we now prove. From the exact sequence 6.2, we obtain (by taking direct limits) the short exact sequence

$$(6.5) \qquad 0 \longrightarrow E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_E(K_n)_p \longrightarrow Ш(K_n, E)_p \longrightarrow 0$$

Since $E(K_n)$ and $Ш(K_n, E)_p$ are finite for all n by hypothesis, we easily obtain that $\mathrm{Sel}_E(K_n)_p$ is finite for all $n \geq 0$. Hence by the "Control theorem" $\mathrm{Sel}_E(K_\infty)_p{}^{\mathrm{Gal}(K_\infty/K_n)}$ is finite for all n. This verifies our claim.

□

It is possible for the rank of $E(K_n)$ to be unbounded in a $\mathbb{Z}_p$-extension, even if E has good ordinary reduction at the primes lying over p. However the following result shows there is some regularity to this growth.

Corollary 6.3.14. Suppose that E is an elliptic curve defined over K which has good ordinary reduction at all primes of K lying over p. Let K_∞/K be a $\mathbb{Z}_p$-extension and let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ (the Iwasawa algebra). Let $r = \operatorname{corank}_\Lambda(\operatorname{Sel}_E(K_\infty)_p)$. Then

$$\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}_E(K_n)_p) = rp^n + O(1) \text{ as } n \to \infty.$$

If in particular $Ш(K_n, E)_p$ is finite for all n, then as $n \to \infty$

$$\operatorname{rank}(E(K_n)) = rp^n + O(1).$$

Proof. Let $X(K_\infty) = \operatorname{Hom}(\operatorname{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$ and $X(K_n) = \operatorname{Hom}(\operatorname{Sel}_E(K_n)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Taking the dual of X we obtain $\operatorname{Sel}_E(K_\infty)_p = \operatorname{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. It is well known that X is finitely generated Λ-module (cf. [26] Theorem 4.5(a)). By the structure theorem for Iwasawa modules 4.2.8, X is pseudo-isomorphic to $\Lambda \times Y \times Z$, where Y is a free $\mathbb{Z}_p$-module of finite rank and Z is a torsion group of bounded exponent. By the same arguments as in the proof of thereom 6.3.12 Γ acts on $\operatorname{Sel}_E(K_\infty)_p$. With this action we obtain that $X/\omega_n X$ is dual to ${\operatorname{Sel}_E(K_\infty)_p}^{\Gamma^{p^n}}$ (see equation 6.4). Hence

$$\operatorname{rank}(X/\omega_n X) = \operatorname{corank}_{\mathbb{Z}_p}({\operatorname{Sel}_E(K_\infty)_p}^{\Gamma^{p^n}}).$$

Therefore by the "Control Theorem"

$$\operatorname{corank}_{\mathbb{Z}_p}({\operatorname{Sel}_E(K_\infty)_p}^{\Gamma^{p^n}}) = \operatorname{corank}_{\mathbb{Z}_p}(\operatorname{Sel}_E(K_n)_p).$$

Now $\Lambda/\omega_n\Lambda$ has $\mathbb{Z}_p$-rank p^n, $Y/\omega_n Y$ has bounded $\mathbb{Z}_p$-rank and $Z/\omega_n Z$ is finite. Hence

$$\operatorname{rank}_{\mathbb{Z}_p}(X/\omega_n X) = rp^n + O(1) \text{ as } n \to \infty.$$

Thus $\text{corank}_{\mathbb{Z}_p}(\text{Sel}_E(K_n)_p) = rp^n + O(1)$ as $n \to \infty$. If in addition $Ш(K_n, E)_p$ is finite for all n, then by the fundamental exact sequence (6.5) $E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has finite index in $\text{Sel}_E(K_n)_p$. Therefore $E(K_n)$ has the same $\mathbb{Z}_p$-rank as $\text{Sel}_E(K_n)_p$, i.e. $\text{rank}_{\mathbb{Z}_p}(E(K_n)) = rp^n + O(1)$ as $n \to \infty$. □

We now give the promised "Iwasawa Theoretic" proof of the "Corank Lemma". We restate the lemma for convenience.

Lemma 6.3.15. **(Corank Lemma)** Let K_v be a finite extension of $\mathbb{Q}_p$ then $H^1(K_v, A)$ is a cofinitely generated $\mathbb{Z}_p$-module and $\text{corank}_{\mathbb{Z}_p} H^1(K_v, A) = [K_v \colon \mathbb{Q}_p] + \delta$ where $\delta = 1$, if ψ is either the trivial character or the cyclotomic character of G_{K_v} and $\delta = 0$ otherwise.

Proof. If ψ is the trivial character then $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\psi) \cong \mathbb{Q}_p/\mathbb{Z}_p$. Since G_{K_v} acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$

$$H^1(K_v, A) = H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}(G_{K_v}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Hence

$$H^1(K_v, A) = \text{Hom}(\text{Gal}(K_v^{\text{ab}}/K_v), \mathbb{Q}_p/\mathbb{Z}_p). \tag{6.6}$$

By local class field theory we have the Artin map, which is injective and has dense image (cf.[44] pg 342)

$$K_v^\times \to \text{Gal}(L/K_v)$$

where L is a finite extension of K_v. This induces the isomorphism

$$K_v^\times / N_{L/K_v}(K) \cong \text{Gal}(L/K_v).$$

Now $K_v^\times \cong \mathbb{Z} \times \mu_{p-1} \times U^{(1)}$ where $U^{(1)}$ is the group of pricipal units in K_v. Taking the limit with respect to the norm we obtain $\widehat{K_v^\times} \cong \text{Gal}(K_v^{\text{ab}}/K_v)$ where $\widehat{K_v^\times} =$

$\mathbb{Z}_p^{[K_v:\,\mathbb{Q}_p]} \times \hat{\mathbb{Z}} \times (K_v^\times)_{\text{tors}}$, hence $\text{Gal}(K_v^{\text{ab}}/K_v) \cong \mathbb{Z}_p^{[K_v:\,\mathbb{Q}_p]} \times \hat{\mathbb{Z}} \times (K_v^\times)_{\text{tors}}$. By equation 6.6

$$H^1(K_v, A) = (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\,\mathbb{Q}_p]} \times \hat{\mathbb{Z}} \times (K_v^\times)_p,$$

hence $H^1(K_v, A)$ has $\mathbb{Z}_p$ corank $[K_v:\,\mathbb{Q}_p] + 1$.

If ψ is the cyclotomic character then $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\psi) = \mu_{p^\infty}$ as a G_{K_v}-module, hence

$$H^1(K_v, A) = H^1(K_v, \mu_{p^\infty}) = K_v^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p.$$

The last equality is classical Kummer theory. Therefore $H^1(K_v, A)$ clearly has $\mathbb{Z}_p$-corank $[K_v:\,\mathbb{Q}_p] + 1$.

We now suppose that ψ is neither the cyclotomic nor trivial character. If $\text{img}(\psi)$ has finite order then it factors through $\Delta = \text{Gal}(F/K_v)$ where F is a finite extension of K_v. Now $\text{img}(\psi) \cong G_{K_v}/\ker(\psi) \cong \text{Gal}(F/K_v)$. The inflation-restriction sequence

$$\begin{tikzcd}
0 \arrow[r] & H^1(\Delta, A) \arrow[r] & H^1(G_{K_v}, A) \arrow[r] & H^1(\ker(\psi), A)^\Delta \arrow[dll] \\
 & H^2(\Delta, A) \arrow[r] & H^2(G_{K_v}, A).
\end{tikzcd}$$

shows that $\text{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \text{corank}_{\mathbb{Z}_p} H^1(\ker(\psi), A)^\Delta$, since all the other groups are finite and do not contribute to the corank of $H^1(G_{K_v}, A)$. Now $\ker(\psi)$ acts trivially on A, hence $H^1(\ker(\psi), A)^\Delta = \text{Hom}(\ker(\psi), A)^\Delta$. Also $\ker(\psi) = \text{Gal}(\bar{K}_v/F)$ hence $H^1(\ker(\psi), A)^\Delta = \text{Hom}_\Delta(\text{Gal}(F^{\text{ab}}/F), A)$. By local class field theory $\text{Gal}(F^{\text{ab}}/F) \cong \mathbb{Z}_p^{[K_v:\,\mathbb{Q}_p]} \times \hat{\mathbb{Z}} \times (K_v^\times)_{\text{tors}}$, hence $H^1(K_v, A)$ has $\mathbb{Z}_p$-corank $[K_v:\,\mathbb{Q}_p]$.

If $\text{img}(\psi)$ is infinite, let $F_\infty = \bar{K}_v^{\ker(\psi)}$ so that $G = \text{Gal}(F_\infty/K_v)$ acts faithfully on $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\psi)$. Now $G \cong \text{img}(\psi)$, which is a subgroup of $\mathbb{Z}_p^\times$. Hence $G \cong \Delta \times \Gamma$, where Δ is a finite group of order dividing $p-1$ if p is odd, of order 1 or 2 if $p = 2$, and $\Gamma \cong \mathbb{Z}_p$. Let $F_0 = F_\infty^\Gamma$, then

$$\text{Gal}(F_0/K_v) \cong G_{K_v}/\text{Gal}(\bar{K}_v/F_0) = G_{K_v}/\Gamma = \Delta.$$

Since $\Gamma = \mathrm{Gal}(F_\infty/F_0) \cong \mathbb{Z}_p$, F_∞/F_0 is a $\mathbb{Z}_p$-extension, hence $F_\infty = \bigcup_n F_n$ where F_n/F_0 is cyclic of degree p^n. We now calculate some of the cohomology groups in the inflation-restriction sequence

$$(6.7) \qquad 0 \to H^1(G,A) \to H^1(K_v,A) \to H^1(F_\infty,A)^G \to H^2(G,A) \to 0.$$

- $H^2(G,A)$

  If p is odd then $p \nmid |\Delta|$, and since Γ is a free pro-p group, it has cohomological dimension 1. Hence $H^2(G,A) = 0$ (c.f section 2.7).

  If $p = 2$ and $|\Delta| = 1$, then by the same argument, $H^2(G,A) = 0$.

  If $p = 2$ and $|\Delta| = 2$, then $H^2(G,A) = \mathbb{Z}/2\mathbb{Z}$.

- $H^1(G,A)$

  If $|\Delta| = 1$ then $G = \Gamma$, a cyclic group. Hence $H^1(G,A) = A/(\gamma-1)A$, considering $\gamma - 1$ as an endomorphism on A , we see that $\ker(\gamma-1)$ is finite, and $\mathrm{im}(\gamma-1)$ is divisible, hence $H^1(G,A) = 0$.

  If p odd and $|\Delta| > 1$ then by a simple inflation restriction argument $H^1(G,A) =$ 0

  If $p = 2$ and $|\Delta| = 2$, then $|A^\Delta| = 2$ hence $H^1(G,A) = \mathbb{Z}/2\mathbb{Z}$.

Since these groups are finite in all cases they do not contribute to the corank of $H^1(G_{K_v}, (\mathbb{Q}_p/\mathbb{Z}_p)(\psi))$. Hence from the inflation restriction sequence 6.7

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \mathrm{corank}_{\mathbb{Z}_p} H^1(F_\infty, A)^G$$

Since G_{F_∞} acts trivially on $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\psi)$, $H^1(F_\infty,A)^G = \mathrm{Hom}_G(F_\infty, A)$. Let M_∞ denote the maximal abelian pro-p extension of F_∞ (i.e. the compositum of all finite p-extension of F_∞). Let $X = \mathrm{Gal}(M_\infty/F_\infty)$ then

$$H^1(F_\infty, A) = \mathrm{Hom}(F_\infty, A) = \mathrm{Hom}(\mathrm{Gal}(M_\infty/F_\infty), A) = \mathrm{Hom}(X, A)$$

where we require the homomorphisms to be continuous. M_∞ is a Galois extension of K_v and $\mathrm{Gal}(M_\infty/K_v)$ can be regarded as a group extension of the quotient group $G = \mathrm{Gal}(F_\infty/F_v)$, by the closed normal subgroup $X = \mathrm{Gal}(M_\infty/F_\infty)$. Hence G acts on X (by inner automorphisms). Now $H^1(F_\infty, A)^G = \mathrm{Hom}_G(X, A)$ and X is a $\mathbb{Z}_p$-module. G acts $\mathbb{Z}_p$-linearly on X and continuously. Now for any $f \in \mathrm{Hom}_G(X, A)$ the action of G on f is given by:

$$g \cdot f = g \cdot f(g^{-1}x) = \psi(g) \cdot f(g^{-1}x). \tag{6.8}$$

All the elements of $\mathrm{Hom}_G(X, A)$ are fixed by G, hence $f(x) = \psi(g) \cdot f(g^{-1}x)$ which implies $f(g \cdot x) = \psi(g) \cdot f(x)$ and by $\mathbb{Z}_p$-linearity of the action we obtain $f(g \cdot x) = f(\psi(g)x)$ hence $f(g \cdot x - \psi(g)x) = 0$. Therefore f factors through $(g - \psi(g))X$. Hence we obtain that

$$\mathrm{Hom}_G(X, A) = \mathrm{Hom}(X^\psi, A);$$

where $X^\psi = X/(g - \psi(g))X$. Therefore

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Hom}(X^\psi, A) = \mathrm{rank}_{\mathbb{Z}_p} X^\psi.$$

□

Consider the character $\psi\colon G = \Delta \times \Gamma \to \mathbb{Z}_p^\times$.

Let $\psi_\Delta = \psi|_\Delta$ and $\psi_\Gamma = \psi|_\Gamma$. Then $X^\psi = (X^{\psi_\Delta})^{\psi_\Gamma}$ hence $X^\psi = X^{\psi_\Delta}/(\gamma - \psi_\Gamma(\gamma))X^{\psi_\Delta}$. Therefore

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \mathrm{rank}_{\mathbb{Z}_p}(X^{\psi_\Delta}/(\gamma - \psi_\Gamma(\gamma))X^{\psi_\Delta}) \tag{6.9}$$

We determine this rank by considering X^{ψ_Δ} as a Λ-module. X is a compact abelian pro-p group, thus by Pontryagin duality it's dual $\mathrm{Hom}(X, A)$ is a discrete p-primary Γ-module. X therefore can be regarded as Λ-module. Let M_n be the maximal pro-p

extension of F_n, then by local class field theory

$$\operatorname{Gal}(M_n/F_n) \cong \mathbb{Z}_p^{[F_n\colon \mathbb{Q}_p]+1} \times \mu_{F_n},$$

where μ_{F_n} denotes the group of p-power roots of unity in F_n. Now $[F_n\colon \mathbb{Q}_p] = [K_v\colon \mathbb{Q}_p]|\Delta|p^n$ furthermore, we can identify Δ with a subgroup of $\operatorname{Gal}(F_n/K_v)$, so Δ acts on $\operatorname{Gal}(M_n/F_n)$ (by inner automorphisms). Since $p \nmid |\Delta|$, the characters of Δ for odd p, have values in $\mathbb{Z}_p^\times$. Hence the following decomposition of $\operatorname{Gal}(M_n/F_n)$ by the characters of $\hat{\Delta}$.

$$\operatorname{Gal}(M_n/F_n) = \bigoplus_{\chi\in\hat{\Delta}} \operatorname{Gal}(M_n/F_n)^\chi,$$

where

$$\operatorname{Gal}(M_n/F_n)^\chi = \{x \in X|\delta(x) = \chi(\delta)x\} = e_\chi X,$$

is the χ-eigenspace and e_χ is the idempotent for χ in $\mathbb{Z}_p[\Delta]$.

If $p = 2$, we define $\operatorname{Gal}(M_n/F_n)^\chi$ to be the maximal quotient of $\operatorname{Gal}(M_n/F_n)$ on which Δ acts on χ. The reciprocity map is Δ-equivariant hence

$$\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{Gal}(M_n/F_n)^\chi) = \begin{cases} [F_v\colon \mathbb{Q}_p]p^n, & \chi \text{ is nontrival} \\ [F_v\colon \mathbb{Q}_p]\,p^n + 1, & \chi \text{ is trivial} \end{cases}$$

The extra 1, if χ is trivial could be thought of as corresponding to $\operatorname{Gal}(F_\infty/F_n) \cong \mathbb{Z}_p$, since $F_\infty \subset M_n$ and Δ acts trivially on $\operatorname{Gal}(F_\infty/F_n)$. Hence we actually have

$$\operatorname{rank}_{\mathbb{Z}_p}(\operatorname{Gal}(M_n/F_\infty)^\chi) = [F_v\colon \mathbb{Q}_p]p^n,$$

for all $n \geq 0$ and all characters χ of Δ. Now the commutator subgroup $\operatorname{Gal}(M_\infty/F_n)'$ of $\operatorname{Gal}(M_\infty/F_n)$ is $(\gamma^{p^n} - 1)X$, hence

$$\operatorname{Gal}(M_\infty/F_n) = (\gamma^{p^n} - 1)X = \omega_n X.$$

Therefore

$$\operatorname{Gal}(M_n/F_\infty) = X/\omega_n X$$

for all $n \geq 0$ where $\omega_n = (1+T)^{p^n} - 1$. We now prove the following facts about X.

Proposition 6.3.16. (i) X is a finitely generated Λ-module.

(ii) $\text{rank}_\Lambda X = [F_v\colon \mathbb{Q}_p]|\Delta|$

More presicely for each character χ of Δ, $\text{rank}_\Lambda X^\chi = [F_v\colon \mathbb{Q}_p]$

(iii) If F_∞ contains the group μ_{p^∞} of p-power roots of unity then the Λ-torsion submodule $X_{\Lambda\text{-tors}}$ is isomorphic to $T_p(\mu_{p^\infty})$, the Tate module of μ_{p^∞}, otherwise $X_{\Lambda_{\text{tors}}} = 0$.

Proof. (i) Since $\omega_n \in \mathfrak{m} = (p, T)$

$$\#(X/(p,T)X) = \#(X/\omega_n X) < \#(X/TX) = \#(X/\omega_0 X);$$

but $w_0 = T$ and $\#(X/\omega_0 X) = \#\text{Gal}(M_0/F_\infty)$, which is finite. Hence by theorem 4.2.9, X is a finitely generated Λ-module. Therefore

$$\text{rank}_{\mathbb{Z}_p}(X/\omega_n X) = \text{rank}_{\mathbb{Z}_p}(\text{Gal}(M_n/F_\infty)) = \sum_{\chi\in\hat{\Delta}} \text{rank}_{\mathbb{Z}_p}(\text{Gal}(M_n/F_\infty)^\chi) = [F_v\colon \mathbb{Q}_p]|\Delta|p^n$$

which implies

$$\text{rank}_{\mathbb{Z}_p}(X) = [F_v\colon \mathbb{Q}_p]|\Delta|.$$

The isomorphism $X/\omega_n X \cong \text{Gal}(M_n/F_n)$ is equivariant, hence

$$(X/\omega_n X)^\chi = X^\chi/\omega_n X^\chi \cong \text{Gal}(M_n/F_n)^\chi.$$

Hence for each $\chi \in \hat{\Delta}$ and $n \geq 0$,

$$\text{rank}_{\mathbb{Z}_p}(X^\chi/\omega_n X^\chi) = [F_v\colon \mathbb{Q}_p]p^n.$$

hence

$$\text{rank}_{\mathbb{Z}_p}(X^\chi) = [F_v\colon \mathbb{Q}_p]$$

Now G_{F_∞} contains an infinite pro-p subgroup (namely its sylow subgroup), hence has cohomological dimension 1. This implies $\hat{X} = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p) = H^1(K_\infty, A)$ is divisible. It follows that $X = \hat{\hat{X}}$ is torsion free as a $\mathbb{Z}_p$-module. Hence X has no non-zero finite Λ-submodules.

(ii) Let $Y = X_{\Lambda-\mathrm{tors}}$, and let $W = X/Y$. W is the torsion free part of W. We have the following exact sequence.

$$0 \longrightarrow Y/\omega_n Y \longrightarrow X/\omega_n X \longrightarrow W/\omega_n W \longrightarrow 0,$$

for all $n \geq 0$. Now $\mathrm{rank}_{\mathbb{Z}_p}(W) = [F_v \colon \mathbb{Q}_p]|\Delta| = r$ i.e $W \cong \Lambda^r$. Therefore

$$W/\omega_n W = \bigoplus_{i=1}^{r} (\Lambda/\omega_n\Lambda) = \bigoplus_{i=1}^{r} \mathbb{Z}_p[T]/(\omega_n) \tag{6.10}$$

Hence

$$\mathrm{rank}_{\mathbb{Z}_p}(W/\omega_n W) = p^n \times r = [F_v \colon \mathbb{Q}_p]|\Delta|p^n$$

This is same as the $\mathbb{Z}_p$-rank of $X/\omega_n X$ hence $Y/\omega_n Y$ must be a finite group. Since $X/\omega_n X \cong \mathrm{Gal}(M_n/F_\infty) \cong \mathbb{Z}_p^{[F_n \colon \mathbb{Q}_p]+1} \times \mu_{F_n}$, we obtain $(X/\omega_n X)_{\mathrm{tors}} = (Y/\omega_n Y)_{\mathrm{tors}} = Y/\omega_n Y = \mu_{F_n}$.

Now if μ_n has bounded order as $n \longrightarrow \infty$ i.e. $(\mu_{p^\infty} \subsetneq F_\infty)$. Then $Y/\omega_n Y$ also has bounded order as $n \longrightarrow \infty$, hence $Y = \varprojlim_n Y/\omega_n Y$ is finite. Since X does no have any finite submodules, $Y = 0$. This proves the second statement.

(iii) Since $Y = \varprojlim_n Y/\omega_n Y$ and $Y/\omega_n Y$ is cyclic for all n, we see that Y is infinite. Hence $Y \cong \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module. Therefore the $\mathbb{Z}_p$-torsion subgroup of $W/\omega_n W$ has unbounded order as $n \longrightarrow \infty$ (i.e. $\mu_{p^\infty} \subset F_\infty$). $Y/\omega_n Y$ must then have unbounded order as $n \longrightarrow \infty$. Since $Y/\omega_n Y$ is isomorphic to a subgroup of μ_{F_n} it implies

$$Y = \varprojlim_n \mu_{F_n} = T_p(\mu_{p^\infty}).$$

This completes our proof.

□

We can now complete the proof of our lemma. By equation 6.9

$$\text{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \text{rank}_{\mathbb{Z}_p}(X^{\psi_\Delta}/g(T)X^{\psi_\Delta})$$

where $g(T) = T - b$ and $b = \psi_\Gamma(\gamma) - 1 \in p\mathbb{Z}_p$. $g(T)$ is thus a distinguished polynomial of degree 1, and hence by proposition 6.3.16, X^{ψ_Δ} is pseudo-isomorphic to either $\Lambda^{[F_v : \mathbb{Q}_p]}$ or $Y \cdot \Lambda^{[F_v : \mathbb{Q}_p]}$ where $Y = T_p(\mu_{p^\infty})$ in the case that $(\mu_{p^\infty} \subset F_\infty)$ and ψ_Δ is the character giving the action of Δ on μ_{p^∞}. Now $\Lambda/g(T)\Lambda \cong \mathbb{Z}_p^{\deg g(T)}$ thus $\Lambda/g(T)\Lambda$ has $\mathbb{Z}_p$-rank 1 . If $(\mu_{p^\infty} \subsetneq F_\infty)$ it then follows that indeed $\text{corank}_{\mathbb{Z}_p} H^1(K_v, A) = [F_v : \mathbb{Q}_p]$. If $(\mu_{p^\infty} \subsetneq F_\infty)$ then $G = \text{Gal}(F_\infty/K_v)$ acts on $T_p(\mu_{p^\infty})$ by a character χ. We assuming that $\chi \neq \psi$. If $\psi_\Delta \neq \chi_\Delta$, then $Y = 0$. If $\psi_\Delta = \chi_\Delta$ then $Y = T_p(\mu_{p^\infty})$, but $\psi_\Gamma \neq \chi_\Gamma$ and so it follows that $Y/g(T)Y$ is finite. In either case, we find that $X^{\psi_\Delta}/g(T)X^{\psi_\Delta}$ has $\mathbb{Z}_p$-rank $[F_v : \mathbb{Q}_p]$. The proof is now complete

CHAPTER VII

Conclusion

7.1 Non commutative Iwasawa Algebras

The starting point of the Iwasawa theory of (non-commutative) p-adic Lie groups was M. Harris' thesis [18] in 1979. For an elliptic curve E over a number field K without complex multiplication he studied the Selmer group $\mathrm{Sel}_E(K_\infty)$ over the extension $K_\infty = K(E[p^\infty])$ which arises by adjoining the p-division points of E to K. Then, the Galois group $G = \mathrm{Gal}(K_\infty/K)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ - due to a celebrated theorem of Serre [38] and so a (compact) p-adic Lie group. Following Iwasawa's general idea, he studied the Pontryagin dual $\mathrm{Sel}_E(K_\infty)^\vee$ of the Selmer group as a module over the Iwasawa algebra

$$\Lambda(G) = \mathbb{Z}_p[[G]].$$

In this section we survey the current state of the subject and give interesting arithmetic examples of these modules.

Definition 7.1.1. A *topological group* G is a group that is also a topological space, such that the group multiplication $(g,h) \to gh$ and the inverse operation $g \to g^{-1}$ are continuous maps.

Definition 7.1.2. A topological group G is *profinite* if it is the inverse limit $\varprojlim_i G_i$, in the category of topological groups, of an inverse system of finite groups G_i. The group G is a *pro-p* group if all the G_i are finite p-groups.

Definition 7.1.3. A topological group G is finitely generated if there is a finite subset X of G such that G is equal to the closure in G of the subgroup generated by X.

Definition 7.1.4. A topological group G is called a *p-adic Lie group* if G has the structure of an analytic manifold over $\mathbb{Q}_p$ and if the function $G \times G \longrightarrow G$ defined by $(g, s) \longrightarrow gs^{-1}$ is analytic.

p-adic Lie groups have a feature which is not held in common with the better understood Lie Groups over $\mathbb{R}$ and $\mathbb{C}$. We have a completely group theoretic description of them.

Definition 7.1.5. A pro-p group G is called *powerful* if $[G, G] \subseteq G^p$ (the group generated by all the p-th power elements of G), for an odd prime p or $[G, G] \subseteq G^4$ for $p = 2$.

Definition 7.1.6. A pro-p group G is *uniform* if it is

(i) finitely generated

(ii) powerful, and

(iii) satisfies

$[P_i(G) : P_{i+1}(G)] = [P_1(G) : P_2(G)]$,

where $P_1(G) = G$ and $P_{i+1}(G) = P_i(G)^p[P_i(G) : G]$.

where ($[P_i(G) : G]$) is the group generated by all commutators $[x, y]$ with $x \in P_i(G)$, $y \in G$. The descending sequence of groups

$$G = P_1(G) \supseteq P_2(G) \supseteq P_3(G) \cdots$$

is called the central lower p-series of G.

Theorem 7.1.7. (Lazard) A topological group G is a p-adic Lie group if and only if G contains an open subgroup which is a uniform pro-p group.

Proof. See [29]. □

We now give a natural prototype for a p-adic Lie group. Let E be an elliptic curve defined over $\mathbb{Q}$. We denote the p-part of E by E_{p^∞}. Let

$$G = \mathrm{Gal}(\mathbb{Q}(E_{p^\infty})/\mathbb{Q}).$$

By a celebrated theorem of Serre [38], G is isomorphic to an open subgroup of $GL_2(\mathbb{Z}_p)$, and hence is a non-abelian, p-adic, Lie group of dimension four. This group can be considered the natural generalization of the classical Iwasawa algebra where we adjoined the p^n-th roots of unity.

Definition 7.1.8. Let G be a p-adic Lie group. The non-commutative Iwasawa algebra over G is the completed group ring

$$\Lambda(G) = \mathbb{Z}_p[[G]] = \varprojlim_{U} \mathbb{Z}_p[G/U]$$

where U runs through the open normal subgroups of G.

The classical Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$ proved useful in the study of Selmer groups attached to elliptic curves and class groups. We naturally seek in the first instance an analogous structure theory of modules over the non-commutative Iwasawa algebra, with an eye towards applications to arithmetic. More modestly we ask what the definition of *pseudo-null* should be for such modules.

In the commutative case, the dimension of a finitely generated R-module M is defined to be Krull dimension of the support of M in spec R. The module M is then said to be pseudo-null if the codimension of M, with respect to the dimension of R over itself is greater than or equal to 2.

A dimension theory for non-commutative *Auslander regular* modules has been given by Bjork [3]. He shows that a finitely generated non-commutative Auslander regular module M is equipped with a canonical filtration

$$T_0(M) \subseteq T_1(M) \subseteq \cdots T_{d-1}(M) \subseteq T_d(M) = M.$$

Using the filtration he manages to define the dimension of M as the least upper bound of length of this filtration chain. This definition coincides with the Krull dimension in the case M is a commutative regular local ring. Using this dimension theory O. Venjakob [43], has the following obvious candidate definition for pseudo-null in the non-commutative case.

Definition 7.1.9. A finitely generated Λ-module is called *pseudo-null* if and only if its codimension is greater that or equal to 2.

When $G \cong \mathbb{Z}_p^d$ this is the usual classical definition of pseudo-null.

Definition 7.1.10. The *Iwasawa Adjoints* of a Λ-module M are defined by

$$E^i(M) = \mathrm{Ext}^i_\Lambda(M, \Lambda); \text{ for } i \geq 0.$$

Definition 7.1.11. The *grade* of a module $M \neq 0$ is given by

$$j(M) = \min\{i : E^i(M) \neq 0\}$$

where we set $j(\{0\}) = \infty$

Definition 7.1.12. Auslander Condition on Λ : For all Λ-modules M, all integers m and all submodules N of $E^m(M)$, we require that $j(N) \geq m$.

Definition 7.1.13. A Noetherian ring Λ is *Auslander regular* if it has finite global homological dimension and the Auslander condition holds.

In order to apply the above theory to $\Lambda(G)$-modules then we need to show that they are *Auslander regular.* O. Venjakob has shown:

Theorem 7.1.14. If G is a p-adic Lie group without p-torsion, then $\Lambda(G)$ is an Auslander regular ring.

Proof. See [43], theorem 3.26 □

Definition 7.1.15. A p-valuation on a group G is a function

$$\omega : G \longrightarrow (0, \infty]$$

satisfying the following axioms for all $x, y \in G$:

(i) $\omega(1) = \infty$, and $\frac{1}{p-1} \leq \omega(x) \leq \infty$ for $x \neq 1$;

(ii) $\omega(xy^{-1}) \geq \min\{\omega(x), \omega(y)\}$;

(iii) $\omega(x^{-1}y^{-1}xy) \geq \omega(x) + \omega(y)$;

(iv) $\omega(x^p) = \omega(x) + 1$.

We say G is p-valued if G possesses a p-valuation.

Remark 7.1.16. If G is compact and is p-valued then G is complete with respect to the p-valuation ω in the following sense. For each $u \geq 0$, let G_u be the subgroup of G consisting of all g such that $\omega(g) \geq u$. Now G_u is open in G because, choosing $N > u$, G_u contains the subgroup of G generated by the p^n-th powers and it is well known that this latter subgroup is a neighbourhood of the identity in a p-adic Lie group. Hence the family $\{G_u : u > 0\}$ form an open basis at the identity for the topology of G: their intersection is trivial and G is compact so the natural map $G \longrightarrow \varprojlim_{u} G/G_u$ is an isomorphism. The following basic fact is established in [29]: If G is p-valued then G is a pro-p group and has no element of order p.

The structure theory of non-commutative Λ-modules has recently been worked out by several authors. S. Howson (the central torsion part [20]), O. Venjakob (the p-torsion part [42]) and J. Coates-P. Schneider-R-Sujatha (the general case [23])

Theorem 7.1.17. (J. Coates-P. Schneider-R-Sujatha) Let G be a p-valued compact p-adic Lie group, and let M be a finitely generated torsion $\Lambda(G)$-module. Let M_0 be the maximal pseudo-null submodule of M. Then there exists non-zero left ideals $L_1, \cdots, L_n$ and a $\Lambda(G)$-injection

$$\phi : \bigoplus_{i=1}^{n} \Lambda(G)/L_i \longrightarrow M/M_0,$$

with coker(ϕ) pseudo-null.

Proof. (See [23].) □

7.2 Arithmetic Examples

In this section we give two concrete examples of finitely generated $\Lambda(G)$-modules, that arise naturally in arithmetic geometry. We also present a numerical example.

Example 7.2.1. Let $p \geq 5$, and let μ_{p^n} $(1 \leq n \leq \infty)$ denote the group of all p^n-th roots of unity. Let F be any finite extension of $\mathbb{Q}$ containing μ_p, and define

$$F^{cyc} = F(\mu_{p^\infty}) \ , \ \Gamma = \mathrm{Gal}(F^{cyc}/F).$$

Now fix a non zero element α of F, which is not a root of unity, and define

$$K_\infty = F^{cyc}(\alpha^{1/p^n} : n = 1, 2, \cdots), \ G = \mathrm{Gal}(K_\infty/F)$$

Let $H = \text{Gal}(K_\infty/F^{cyc})$, then both H and Γ are isomorphic to $\mathbb{Z}_p$, therefore G is a p-adic Lie group of dimension 2, which is p-valued. Moreover G is not commutative. Perhaps the simplest left $\Lambda(G)$-module is the following :

Let L_∞ denote the maximal unramified abelian extension of K_∞, and let $X = \text{Gal}(L_\infty/K_\infty)$. We have a continuous left action of G on X via inner automorphisms (if $\sigma \in G$, we define $\sigma x = \tilde{\sigma} x \tilde{\sigma}^{-1}$, where $\tilde{\sigma}$ denotes any lifting of σ to the Galois group of L_∞ over F). By a result of Y. Ochi [33], X is a finitely generated torsion $\Lambda(G)$-module. Surprisingly little else is known about this particular example. In particular there is no known example of X which is not pseudo-null as a $\Lambda(G)$-module.

Example 7.2.2. Let F be a finite extension of $\mathbb{Q}$, and E an elliptic curve defined over F with $\text{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$. Let $p \geq 5$, and let E_{p^n} $(1 \leq n \leq \infty)$ denote the group of p^n-division points on E. We define

$$F_\infty = F(E_{p^\infty}),\ G = \text{Gal}(F_\infty/F).$$

The action of G on E_{p^∞} defines an injection of G into $\text{Aut}(E_{p^\infty}) \cong \text{GL}_2(\mathbb{Z}_p)$, and by a theorem of Serre [38], the image of G is open in $\text{GL}_2(\mathbb{Z}_p)$. By the Weil-pairing $F^{cyc} = F(\mu_{p^\infty})$ is contained in F_∞, and we put

$$H = \text{Gal}(F_\infty/F^{cyc}),\ \Gamma = \text{Gal}(F^{cyc}/F).$$

We shall assume from now on that G is pro-p (this can always be achieved, if necessary we replace F by a finite extension, e.g. by $F(E_p)$). Hence Γ is pro-p, and so is isomorphic to $\mathbb{Z}_p$.

For each intermediate field L with $F \subseteq L \subseteq F_\infty$, we define the *Selmer group* of

E over L by:

$$\mathrm{Sel}_E(L) = \ker\left(H^1(G_L, E_{p^\infty}) \longrightarrow \prod_v H^1(G_{L_v}, E(\overline{L_v}))\right),$$

where v runs over all finite places of L, and L_v denotes the union of the completions at v of all finite extensions of F contained in L. We have as usual the exact sequence

$$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_E(L) \to Ш(L, E)[p] \to 0$$

where $Ш(L, E)[p]$ denotes the p-part of the Tate-Shafarevich group of E over L. We write

$$X(E/L) = \mathrm{Hom}(\mathrm{Sel}_E(L), \mathbb{Q}_p/\mathbb{Z}_p)$$

for the compact Pontryagin dual of the discrete p-primary module $\mathrm{Sel}_E(L)$. If L is Galois over F then the Galois group $\mathrm{Gal}(L/F)$ of L over F has a natural action on both $\mathrm{Sel}_E(L)$ and $X(E/L)$, and it is easily seen that $X(E/L)$ is always a finitely generated $\Lambda(\mathrm{Gal}(E/L))$-module.

Primary interest though has always been on the $\Lambda(G)$-modules $X(E/F^{cyc})$ and $X(E/F_\infty)$. If E has good reduction at all primes v of F dividing p, then conjectures of B. Mazur [28] and M. Harris [18] affirm respectively that $X(E/F^{cyc})$ is a $\Lambda(\Gamma)$-torsion module and $X(E/F_\infty)$ is a $\Lambda(G)$-torsion module. In [7] the following examples of Harris's conjecture are proven, to deduce also new examples of Mazur's conjecture.

Theorem 7.2.3. Assume that: (i) $p \geq 5$ (ii) G is pro-p (iii) E has good ordinary reduction at all the places v of F dividing p, and (iv) $X(E/F^{cyc})$ is a finitely generated $\mathbb{Z}_p$-module. Then $X(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module where $H = \mathrm{Gal}(F_\infty/F^{cyc})$. In particular, $X(E/F_\infty)$ is a torsion $\Lambda(G)$-module.

We now give a numerical example of an elliptic curve over its field of p-power division points

Example 7.2.4. Let E be the elliptic curve $X_1(11)$ defined over $\mathbb{Q}$ by the equation

$$E : y^2 + y = x^3 - x^2$$

E has good ordinary reduction at the prime 5. Taking $p = 5$, $F = \mathbb{Q}(\mu_5)$, and noting that the point $(0, 0)$ has order 5 on E, we see that $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of F. Now the image of G in $\mathrm{Aut}(E_{5^\infty})$ can be identified with the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $GL_2(\mathbb{Z}_5)$ with $a \equiv d \equiv 1 \mod 5$ and $c \equiv 0 \mod 5^2$. This group is in turn isomorphic to the group of all matrices in $GL_2(\mathbb{Z}_5)$ which are congruent to the identity modulo 5. Finally it is well known that $\mathrm{Sel}_E(F^{cyc}) = 0$ (see [8] chapter V) . Hence hypothesis (i) ,(ii) ,(iii) and (iv) of theorem 7.2.3 hold for E over F. We conclude that $X(E/F_\infty)$ is a torsion $\Lambda(G)$-module, with the Iwasawa μ invariant equal to zero and with no non-zero pseudo-null submodule.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. Babakhanian. *Cohomological Methods in Group Theory*, volume 11. Dekker, Pure and Applied Mathematics, New York, 1972.

[2] B. J. Birch. Elliptic curves over **Q**: A progress report. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 396–400. Amer. Math. Soc., Providence, R.I., 1971.

[3] J.-E. Bjork. Filtered noetherian rings, in noetherian rings and their applications. *Math Surveys and Monographs*, 24:59–97, 1987.

[4] S. Bloch and K. Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[5] N. Bourbaki. *Commutative algebra.* Hermann, Paris, 1972.

[6] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[7] J.H. Coates and S. Howson. Euler Characteristics and Elliptic Curves II. *to appear in J. Math. Soc. Japan*, 53(1):175–235, 2001.

[8] J.H. Coates and R. Sujatha. *Galois Cohomology of Elliptic Curves.* Lecture Notes at the Tata Institute of Fundamental Research, 2000.

[9] V. Diekert. Eine bemerkung zu freien Moduln über regularen lokalen Ringen. *J. Algebra*, 101(1)::188–189, 1986.

[10] G. Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[11] J-M. Fontaine. Le corps des priodes p-adiques. *in Priodes p-adiques. Astrisque. Soc. Math. de France*, 223, 1994.

[12] R. Greenberg. The structure of Selmer groups. *Proceedings Natl. Acad. of Science*, 94 ,(1-4):11125–11128, 1997.

[13] R. Greenberg. Iwasawa theory for elliptic curves. *Lecture Notes in Maths*, 1716(1-4):51–144, 1999.

[14] R. Greenberg. Introduction to Iwasawa theory. *Arithmetic algebraic geometry (Park City, UT, 1999)*, 9(1-4):407–464, 2001.

[15] R. Greenberg. Iwasawa theory past and present–class field theory–its centenary and prospect. *Adv. Stud. Pure Math.*, 30(1-4):335–385, 2001.

[16] R. Greenberg. Galois theory for the Selmer group of an abelian variety. *Compositio Math.*, 136(3):255–297, 2003.

[17] K. Haberland. *Galois cohomology of algebraic number fields.* VEB Deutscher Verlag der Wissenschaften, Berlin, 1978. With two appendices by Helmut Koch and Thomas Zink.

[18] M. Harris. p-adic Representations Arising from Descent on Abelian Varieties. *Compositio Math.*, 39(2):177–245, 1979.

[19] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[20] S. Howson. Structure of central torsion Iwasawa modules. *Bull. Soc. Math. France*, 130(4):507–535, (2002).

[21] K. Iwasawa. A note on the class numbers of algebraic number fields. *Abh. math Sem Hamburg*, 20:247–258, 1956.

[22] K. Iwasawa. On γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65:183–226, 1959.

[23] P. Schneider J. Coates and R. Sujatha. Modules over Iwasawa algebras. *J. Inst. Math. Jussieu.*, 2(2):73 – 108, 2003.

[24] S. Lang. *Cyclotomic fields.* springer-Verlag, New York, first edition, 1979.

[25] S. Lang. *Algebra.* Addison-Wesley Publishing Co., Reading, Mass., third edition, 1993.

[26] Y. I. Manin. Cyclotomic fields and modular curves. *Russian Math. Surveys*, 26(6):7–78, 1971.

[27] H. Matsumura. *Commutative ring theory.* Cambridge University Press, Cambridge, 1986. Translated from the Japanese by M. Reid.

[28] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[29] Lazard Michel. Groupes analytiques p-adiques. *Inst. Hautes Etudes Sci. Publ.Math*, 26:389–603, 1965.

[30] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, Berlin, 1986.

[31] J. Neukirch. *Class Field Theory.* Springer-Verlag, Berlin, 1986.

[32] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften.* Springer Verlag, 2000.

[33] Y. Ochi. Iwasawa modules via homotopy theory. *PhD thesis, University of Cambridge*, 1999.

[34] L. Ribes and P. Zalesskii, editors. *Profinite groups.* Springer-Verlag,Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge ; 40, Berlin, 2000.

[35] J. Rotman. *An introduction to homological algebra.* (Academic Press, Inc. [Harcourt Brace Jovanovich Publishers], New York-London, 1979. Pure and Applied Mathematics, 85.

[36] J-P. Serre. Classes de corps cyclotomiques. *Seminairé Bourbaki*, 174(1):179–230, 1958.

[37] J-P. Serre. Local class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 128–161. Thompson, Washington, D.C., 1967.

[38] J-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[39] J-P. Serre. *Galois cohomology.* Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author.

[40] J. H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[41] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.

[42] O. Venjakob. Iwasawa theory of p-adic lie extensions. *Dissertation, University of Heidelberg,* (2001).

[43] O. Venjakob. On the structure theory of the Iwasawa algebra of a p-adic lie group. *J. Eur. Math. Soc. (JEMS)*, 4(3):271–311, (2002).

[44] L. Washington. *Introduction to Cyclotomic Fields.* Number 83 in GTM. Springer-Verlag, New York, second edition, 1997.