Classifying Lambda-Modules up to Isomorphism and Applications to Iwasawa Theory

by

Chase Franks

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved April 2011 by the
Graduate Supervisory Committee:

Nancy Childress, Chair
Hélène Barcelo
Andrew Bremner
John Jones
Jack Spielberg

ARIZONA STATE UNIVERSITY

May 2011

ABSTRACT

In Iwasawa theory, one studies how an arithmetic or geometric object grows as its field of definition varies over certain sequences of number fields. For example, let $F/\mathbb{Q}$ be a finite extension of fields, and let $E : y^2 = x^3 + Ax + B$ with $A, B \in F$ be an elliptic curve. If $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots F_\infty = \bigcup_{i=0}^{\infty} F_i$, one may be interested in properties like the ranks and torsion subgroups of the increasing family of curves $E(F_0) \subseteq E(F_1) \subseteq \cdots \subseteq E(F_\infty)$. The main technique for studying this sequence of curves when $\mathrm{Gal}(F_\infty/F)$ has a p-adic analytic structure is to use the action of $\mathrm{Gal}(F_n/F)$ on $E(F_n)$ and the Galois cohomology groups attached to E, i.e. the Selmer and Tate-Shafarevich groups. As n varies, these Galois actions fit into a coherent family, and taking a direct limit one obtains a short exact sequence of modules

$$0 \longrightarrow E(F_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Sel}_E(F_\infty)_p \longrightarrow Ш_E(F_\infty)_p \longrightarrow 0$$

over the profinite group algebra $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$. When $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, this ring is isomorphic to $\Lambda = \mathbb{Z}_p[[T]]$, and the Λ-module structure of $\mathrm{Sel}_E(F_\infty)_p$ and $Ш_E(F_\infty)_p$ encode all the information about the curves $E(F_n)$ as n varies.

In this dissertation, it will be shown how one can classify certain finitely generated Λ-modules with fixed characteristic polynomial $f(T) \in \mathbb{Z}_p[T]$ up to isomorphism. The results yield explicit generators for each module up to isomorphism. As an application, it is shown how to identify the isomorphism class of $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ in this explicit form, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and E is an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p, and possessing the property that $E(\mathbb{Q})$ has no p-torsion.

To my wife Nina,

I dedicate all my results.

ACKNOWLEDGEMENTS

I would like to thank my kind and patient advisor Nancy Childress for introducing me to Iwasawa theory and the non-archimedean world, and allowing me to find my own voice as a researcher. I would also like to thank Andrew Bremner for teaching me the subject of elliptic curves and Diophantine equations, and John Jones for his fascinating course in modular forms. It was Hiroki Sumida (Hiroshima) who informed me of the unpublished calculation done by Hachimori, and suggested that I pursue the classification problem which led to this dissertation. Valuable feedback and encouragement was given by Mirela Çiperiani, Chris Wuthrich, William Stein, and Romyar Sharifi. I especially thank my colleague Ahmed Matar for our countless discussions and his sound advice. Lastly, I thank Arizona State University for supporting me as a teaching assistant, and giving me many opportunities to grow as a teacher of mathematics.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

Let $F/\mathbb{Q}_p$ be a finite extension, and let $\mathcal{O}$ be the ring of integers in F. Let $\pi \in \mathcal{O}$ be a uniformizing parameter, so that the maximal ideal of $\mathcal{O}$ is (π). Let Λ denote the power series ring $\mathcal{O}[[T]]$ over $\mathcal{O}$. This dissertation studies finitely generated torsion Λ-modules which possess no nonzero finite Λ-submodules. To be more precise, for a finitely generated torsion Λ-module M, one first has the well-known

Theorem 1.0.1 (Structure Theorem). There exists a Λ-homomorphism

$$M \longrightarrow \bigoplus_{i=1}^{n} \Lambda/(f_i(T)^{e_i})$$

with finite kernel and cokernel. Each $f_i(T)$ is either the uniformizer π or an irreducible distinguished polynomial $f_i(T) \in \mathcal{O}[T]$. The $f_i(T)$ and the $e_i \in \mathbb{N} \setminus \{0\}$ are uniquely determined by M.

$P(T) = a_0 + a_1 T + \cdots + T^m \in \mathcal{O}[T]$ is distinguished when $a_0, a_1, \ldots, a_{m-1}$ are in (π). The characteristic polynomial of M is

$$\mathrm{char}_\Lambda(M) = \prod_{i=1}^{n} f_i(T)^{e_i}$$

which can be written as $\pi^\mu f(T)$ with $f(T)$ distinguished. Let $\deg f = \lambda$. Let $\mathcal{M}_f$ denote the set of isomorphism classes of Λ-modules M such that $\mathrm{char}_\Lambda(M) = f(T)$ and M has no nontrivial Λ-submodules. In [13] the problem of determining $\mathcal{M}_f$ was introduced, and it was shown that $\mathcal{M}_f$ is finite when the f_i are distinct, $e_i \leq 1$, and $\mu = 0$. The assumption that M has no finite Λ-submodules implies that the map in the Structure theorem is injective with finite cokernel. Hence M can be regarded as a Λ-submodule of $E_f = \oplus \Lambda/(f_i)$ with finite quotient E_f/M. This dissertation gives a method for determining $\mathcal{M}_f$ under these assumptions.

When each $f_i(T) = T - \alpha_i$, then $E_f = \bigoplus_i^n \Lambda/(T - \alpha_i)$ can be identified with the free $\mathcal{O}$-module of rank n where T acts on the ith factor as multiplication by α_i. The submodules M of E_f with finite quotient E_f/M must have maximal $\mathcal{O}$-rank n. The strategy for determining $\mathcal{M}_f$ will be as follows. Theorem 2.0.4 will show that up to isomorphism, any submodule $M \subseteq E_f$ has generators over $\mathcal{O}$ of a certain upper triangular form

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ & \pi^i & * & * & \cdots & * \\ & & \pi^j & * & \cdots & * \\ & & & \ddots & & \\ & & & & & \\ & & & & & \pi^k \end{pmatrix},$$

i.e. M is generated over $\mathcal{O}$ by the rows of G. The valuations along the diagonal can be bounded, and using elementary row operations, the integral entries * can be reduced modulo the power of π directly below. There are then a finite number of matrices $G_1, G_2, \ldots, G_r$ to consider, and representatives for the classes in $\mathcal{M}_f$ can be found among the modules M_t, where M_t is generated over $\mathcal{O}$ by the rows of G_t. In practice, r can be quite large, and one seeks to find a distinct set of representatives. The main task is to decide when $M_s \cong M_t$.

1.1 The Ring Λ

In this section, some relevant facts about the ring Λ which will be useful later on will be discussed. A good reference for Λ-modules and Iwasawa theory is [16]. The first fact is that Λ enjoys a division algorithm much like for rings of polynomials over a field.

Theorem 1.1.1. Let $P(T)$ be a distinguished polynomial of degree r, and $f(T) \in \Lambda$. Then there exist $q(T) \in \Lambda$ and $r(T) \in \mathcal{O}[T]$ such that $f(T) =$

$P(T)q(T) + r(T)$. The polynomial $r(T)$ is unique of degree less than or equal to $r - 1$.

Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$. Let $\mu = \mu(f) = \min\{\text{ord}_\pi(a_i)\}_{i=0}^{\infty}$, so that $f(T) = \pi^\mu \sum_{i=1}^{\infty} b_i T^i$ with at least one of the b_i a unit. Define $\lambda(f) = \min\{i | b_0, b_1, \ldots, b_{i-1} \in (\pi), b_i \notin (\pi)\}$.

Theorem 1.1.2 (Weierstrauss Preparation). Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$. Then $f(T)$ factors uniquely as $\pi^\mu P(T)U(T)$ with $U(T)$ a unit and $P(T)$ a distinguished polynomial of degree $\lambda(f)$.

From this theorem, it follows that Λ is a unique factorization domain. The irreducible elements are π, and distinguished irreducible polynomials $P(T)$. Therefore the ideals $(0), (\pi)$ and $(P(T))$ are prime. The ideal $\mathfrak{m} = (T, \pi)$ is clearly maximal since $\Lambda/\mathfrak{m} \cong \mathcal{O}/(\pi) \cong \mathbb{F}_q$ for some finite field $\mathbb{F}_q$ with $q = p^f$ elements. It turns out that these are the only prime ideals, and Λ is a regular local ring of dimension 2 with unique maximal ideal $\mathfrak{m}$ (see [16]).

The following result from [13] makes an explicit Weierstrauss Preparation factorization possible on any computer that can perform polynomial factorization modulo powers of π.

Theorem 1.1.3 (Proposition 3). Let $f_i(T) = P_i(T)U_i(T)$ for $i = 1, 2$ be Weierstrauss factorizations, where the P_i are distinguished polynomials, and the U_i are unit power series. Let $\mathfrak{m} = (\pi, T)$ be the unique maximal ideal of Λ. If $\lambda(f_1) = \lambda = \lambda(f_2)$, $f_i(T) \in \mathfrak{m}^l$ for $l \geq 1$, and $f_1(T) \equiv f_2(T) \mod \mathfrak{m}^{\lambda k+1}$, then

$$P_1(T) \equiv P_2(T) \mod \mathfrak{m}^{k+l}.$$

Since $\pi^n, T^n \in \mathfrak{m}^n$, to (partially) reduce modulo $\mathfrak{m}^n$ one can reduce coefficient-wise by π^n and then truncate the result by T^n. As an example to

see how this result is used, the program SAGE [10] returns the following for the 3-adic L-series, $L_3(E,T)$ of the elliptic curve $E = 50a1$ from Cremona's tables:

$$L = 3+3^2+2\cdot 3^4+2\cdot 3^5+2\cdot 3^6+3^7+O(3^9)+(3+2\cdot 3^2+3^5+O(3^6))\cdot T+(2+3^2+2\cdot 3^3+2\cdot 3^4+O(3^6))\cdot T^2+(3^3+2\cdot 3^4+O(3^5))\cdot T^3+(2\cdot 3^2+3^5+O(3^6))\cdot T^4+(2+3+2\cdot 3^2+3^3+3^4+2\cdot 3^5+O(3^6))\cdot T^5+(1+3+3^2+3^3+3^4+O(3^5))\cdot T^6+(1+3+2\cdot 3^3+3^4+2\cdot 3^5+O(3^6))\cdot T^7+(2\cdot 3+2\cdot 3^2+3^3+3^4+2\cdot 3^5+O(3^6))\cdot T^8+(3+3^3+O(3^4))\cdot T^9$$

Hence $L_3(E,T) \cong L \bmod \mathfrak{m}^4$, and both are in $\mathfrak{m}$. One can see that $\lambda = 2$, hence $l = 1, k = 1$ in the above theorem. Lifting L to a polynomial and factoring gives

$$(1+3^2+O(3^4))\cdot((1+O(3^4))\cdot T+(1+O(3^4)))\cdot((1+O(3^4))\cdot T^2+(1+3+3^3+O(3^4))\cdot T+(1+2\cdot 3+2\cdot 3^3+O(3^4)))\cdot((1+O(3^4))\cdot T^2+(2+3^2+3^3+O(3^4))\cdot T+(2+3^2+3^3+O(3^4)))\cdot((1+O(3^4))\cdot T^2+(2\cdot 3+O(3^4))\cdot T+(2\cdot 3+O(3^4)))\cdot((3+O(3^4))\cdot T^2+(3+3^2+O(3^4))\cdot T+(1+3+3^3+O(3^4)))$$

and since anything with a unit constant term is a unit, one can read off the distinguished polynomial part as the second to last factor $P(T) = T^2+6T+6$, known to accuracy $\mathfrak{m}^{k+l} = \mathfrak{m}^2$. To increase this accuracy, one increases the accuracy of the approximation to $L_3(E,T)$.

Chapter 2

GENERATORS

In this section, it is shown that each class in $\mathcal{M}_f$ has a representative equal to a module generated over $\mathcal{O}$ by the rows of a matrix of type G. The following lemma will be useful.

Lemma 2.0.1. Let $M \subseteq \mathcal{O}^n$ be an $\mathcal{O}$-submodule of rank n. Then M can be generated by the rows of a matrix having the form

$$\begin{pmatrix} \pi^{a_1} & x_{1,2} & x_{1,3} & \cdots & x_{1,n} \\ & \pi^{a_2} & x_{2,3} & \cdots & x_{2,n} \\ & & \ddots & & \vdots \\ & & & & \pi^{a_n} \end{pmatrix},$$

where $a_i \in \mathbb{N}$ and $x_{i,j} \in \mathcal{O}$.

Proof. The proof will be by induction on n. Since any rank 1 submodule of $\mathcal{O}$ is an ideal (π^a), the result is true for $n = 1$. Suppose that the result is true for $n-1$. Let $\mathrm{proj}_i : \mathcal{O}^n \longrightarrow \mathcal{O}$ denote projection onto the ith factor. The image $\mathrm{proj}_1(M)$ must be a nonzero ideal in $\mathcal{O}$ since otherwise $M \subseteq \ker(\mathrm{proj}_1) \cong \mathcal{O}^{n-1}$ and M would then have rank $n-1$ or less. Hence $\mathrm{proj}_1(M) = (\pi^{a_1})$ and there is an element $(\pi^{a_1}, x_{1,2}, x_{1,3}, \ldots, x_{1,n}) \in M$. Let $(y_1, y_2, \ldots, y_n) \in M$. Then $y_1 = \alpha\pi^{a_1}$ for some $\alpha \in \mathcal{O}$, so that $(y_1, y_2, \ldots, y_n) - \alpha(\pi^{a_1}, x_{1,2}, x_{1,3}, \ldots, x_{1,n}) = (0, z_2, \ldots, z_n) \in \ker(\mathrm{proj}_1) \cap M$. Since $\mathrm{proj}_1(M)$ has rank 1, $\ker(\mathrm{proj}_1) \cap M$ has rank $n-1$, and by the inductive hypothesis it is generated by

$$(0, \pi^{a_2}, x_{2,3}, \ldots, x_{2,n}), \ldots, (0, 0, \ldots, \pi^{a_n})$$

having the required form. The result follows. □

The next lemma shows that dividing the columns of a matrix by elements of $\mathcal{O}$ preserves the Λ-isomorphism class of the Λ-module generated by

its rows inside of E_f. The proof given below is slightly different than the one in [14].

Lemma 2.0.2. [Lemma 1 in [14]] For any nonzero $x_1, x_2, \ldots, x_n \in \mathcal{O}$, the map $\phi : E_f \longrightarrow E_f$ given by $(e_1, e_2, \ldots, e_n) \mapsto (x_1 e_1, x_2 e_2, \ldots, x_n e_n)$ is an injective homomorphism of Λ-modules, and hence induces a Λ-isomorphism $M \longrightarrow \phi(M)$ for any Λ-submodule $M \subset E_f$.

Proof. Since T acts diagonally on E_f, it is clear that the action of T commutes with ϕ, hence ϕ is a Λ-homomorphism. Suppose $\phi(e_1, e_2, \ldots, e_n) = (x_1 e_1, x_2 e_2, \ldots, x_n e_n) = (0, 0, \ldots, 0)$ in E_f. Then $x_1 e_1 = g(T)(T - \alpha_1)$ for some power series $g(T) \in \Lambda$. Since α_1 is a root of a distinguished polynomial, $|\alpha_1| < 1$, and hence $g(\alpha_1)$ is defined and converges to an element in $\mathcal{O}$. Then $x_1 e_1 = g(\alpha_1)(\alpha_1 - \alpha_1) = 0$, and since $\mathcal{O}$ is a domain, this implies that $e_1 = 0$. Similarly, $e_2 = e_3 = \cdots = e_n = 0$. □

Let M have the $\mathcal{O}$-basis given by the rows of the matrix from lemma 2.0.1. The lemma just proved allows one to divide a column of M by an element of $\mathcal{O}$, and even though the submodule of E_f generated by the rows of the resulting matrix is different, the isomorphism class is the same. One may also multiply rows by units, or add an integral multiple of one row to another since these operations just change the basis used to describe M as an $\mathcal{O}$-module. The generators for $\lambda = 2$ and 3 are produced below, and then an inductive proof is given for all λ.

For $\lambda = 2$, let $M \subseteq E_f$ be generated over $\mathcal{O}$ by the rows of

$$B = \begin{pmatrix} \pi^{a_1} & x_{1,2} \\ 0 & \pi^{a_2} \end{pmatrix}$$

with $a_1, a_2, \in \mathbb{N}$ and $x_{1,2} \in \mathcal{O}$. One can reduce $x_{1,2}$ modulo π^{a_2} by using row operations, and if $x_{1,2} = 0$, then one may replace row 1 with the sum of rows

1 and 2 to make $x_{1,2} \neq 0$. One may therefore assume that $\mathrm{ord}_\pi(x_{1,2}) \leq a_2$. By Lemma 2.0.2, one can divide column 1 by π^{a_1}, and column 2 by $x_{1,2}$ to produce the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & u\pi^i \end{pmatrix},$$

where $u\pi^k = \pi^{a_2}/x_{1,2}$. Dividing row 2 by u produces

$$G = \begin{pmatrix} 1 & 1 \\ 0 & \pi^i \end{pmatrix}.$$

The case $\lambda = 3$ will illustrate the inductive step in the proof of theorem 2.0.4 below. Let

$$B = \begin{pmatrix} \pi^{a_1} & x_{1,2} & x_{1,3} \\ & \pi^{a_2} & x_{2,3} \\ & & \pi^{a_3} \end{pmatrix}.$$

By the case $\lambda = 2$ one can use row and column operations to produce a matrix in the form

$$\begin{pmatrix} 1 & 1 \\ & \pi^{i_1} \end{pmatrix}$$

as the principle 2 by 2 submatrix of B, so that without loss of generality one may assume that

$$B = \begin{pmatrix} 1 & 1 & x_{1,3} \\ & \pi^{i_1} & x_{2,3} \\ & & \pi^{a_3} \end{pmatrix}.$$

By using row operations one may assume that both $\mathrm{ord}_\pi(x_{1,3})$ and $\mathrm{ord}_\pi(x_{2,3})$ are less than or equal to a_3. Now after these initial reductions, one has two cases: $\mathrm{ord}_\pi(x_{1,3}) \leq \mathrm{ord}_\pi(x_{2,3})$ or $\mathrm{ord}_\pi(x_{2,3}) < \mathrm{ord}_\pi(x_{1,3})$. If $\mathrm{ord}_\pi(x_{1,3}) \leq$

$\mathrm{ord}_\pi(x_{2,3}) \leq a_3$ then one can divide column 3 by $x_{1,3}$, producing

$$\begin{pmatrix} 1 & 1 & 1 \\ & \pi^{i_1} & b \\ & & v\pi^{i_2} \end{pmatrix}$$

where v is a π-adic unit. Dividing row 3 by v gives generators of the required form. Now assume that $\mathrm{ord}_\pi(x_{2,3}) < \mathrm{ord}_\pi(x_{1,3}) \leq a_3$. Then dividing column 3 by $x_{2,3}$ gives the form

$$\begin{pmatrix} 1 & 1 & c \\ & \pi^{i_1} & 1 \\ & & w\pi^{i_2} \end{pmatrix}$$

where w is a π-adic unit and $c \in (\pi)$. If $\alpha \in \mathcal{O}$, applying the row operation $R_1 = R_1 + (\alpha - c)R_2$ transforms the top row into

$$(1, 1 + (\alpha - c)\pi^{i_1}, \alpha).$$

Modulo π this row becomes $(1, 1 + \alpha\pi^{i_1}, \alpha)$, so that the entries along the top row can be made into units if one can find α with both α and $1 + \alpha$ units in $\mathcal{O}$. This is possible as long as $\mathcal{O}/(\pi) \ncong \mathbb{F}_2$ since one can then choose any element $\alpha_0 \neq 0, -1$ in the finite field $\mathcal{O}/(\pi)$ and lift it to $\alpha \in \mathcal{O}$. Hence, the units $1 + (\alpha - c)\pi^{i_1}$ and α can be divided from the columns and multiplied from the rows to produce the desired form.

For $\mathcal{O}$ the residue characteristic is the characteristic of its residue field $\mathcal{O}/(\pi)$. If the residue characteristic is p, one has $\mathcal{O}/(\pi) \cong \mathbb{F}_q$, where $q = p^f$. Note that the proof for $\lambda = 2$ holds when $\mathcal{O}$ has any residue characteristic, and for $\lambda = 3$ it was necessary that $q \neq 2$.

Theorem 2.0.4. Let $\mathcal{O}$ have residue field $\mathcal{O}/(\pi) \cong \mathbb{F}_q$ with $q = p^f$. Assume that $\lambda \leq q$. Then $\mathcal{M}_f$ has representatives M, where M can be generated as

an $\mathcal{O}$-module inside of E_f by the rows of a matrix in the form

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ & \pi^{i_1} & b_{2,3} & b_{2,4} & \cdots & b_{2,n} \\ & & \pi^{i_2} & b_{3,4} & \cdots & b_{3,n} \\ & & & \ddots & & \\ & & & & & \pi^{i_{n-1}} \end{pmatrix},$$

with $i_k \in \mathbb{N}$ and the $b_{i,j} \in \mathcal{O}$.

Proof. The proof is by induction along principle submatrices, the base case having already been established for $\lambda = 2$. Suppose one has obtained a principle submatrix consisting of the first $k+1$ by $k+1$ entries in the form

$$B_k = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & x_1 \\ & \pi^{i_1} & b_{2,3} & \cdots & b_{2,k} & x_2 \\ & & \ddots & & \vdots & \\ & & & & \pi^{i_{k-1}} & x_{k+1} \\ & & & & & \pi^{a_k} \end{pmatrix},$$

where $k+1 \leq \lambda$. By using row reduction if necessary, one may assume that the entries in the rightmost column have valuation less than or equal to a_k and are all nonzero. If x_1 has smallest valuation among the entries in the rightmost column, then dividing the column by x_1 yields

$$\begin{pmatrix} 1 \\ b_2 \\ \vdots \\ b_{k+1} \\ v\pi^{i_k} \end{pmatrix},$$

and dividing the $k+1$st row by v transforms B into the desired form. Otherwise, among the entries $x_2, x_3, x_4, \ldots, \pi^{a_k}$, one may choose x_j to have smallest

valuation. Dividing the column by x_j yields

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{j-1} \\ 1 \\ b_{j+1} \\ \vdots \\ w\pi^{i_k} \end{pmatrix}.$$

If c_1 is already a unit, then one may divide this column by c_1, and multiply the $k+1$st row by c_1/w to yield a column in the desired form. In any event, one can divide row $k+1$ by w, so one may assume that $c_1 \in (\pi)$ and $w = 1$. Now consider the polynomial $g(x)$ where

$$x(x+1)\prod_{t=j+1}^{k}(b_{j,t}x+1) \equiv g(x) \in \mathbb{F}_q[x].$$

Note that $g(x)$ has degree $k-j+2 < \lambda \leq q$, so there is some $\alpha \in \mathcal{O}$ such that

$$\alpha(\alpha+1)\prod_{t=j+1}^{k}(b_{j,t}\alpha+1) \not\equiv 0 \bmod (\pi).$$

Applying the row operation $R_1 = R_1 + (\alpha - c_1)R_j$ to the matrix transforms the top row into the form

$$(1,\ldots,1,1+(\alpha-c_1)\pi^{i_{j-1}},1+(\alpha-c_1)b_{j,j+1},\ldots,1+(\alpha-c_1)b_{j,k},\alpha).$$

Reducing modulo π, this row becomes

$$(1,\ldots,1,1+\alpha\pi^{i_{j-1}},1+\alpha b_{j,j+1},\ldots,1+\alpha b_{j,k},\alpha)$$

since $c_1 \in (\pi)$. Since none of these entries are 0 modulo π by the choice of α, the entries in row 1 are all units. Dividing each unit from the column and then multiplying it from the row below produces a matrix B_{k+1} in the desired form. Hence by induction the result holds. $\square$

There are some interesting consequences of the existence of these upper triangular generators. The first of these is given in the next theorem.

Theorem 2.1.1. The tuple $(i_1, i_2, \ldots, i_{n-1})$ is a Λ-module invariant.

For two matrices $A, B \in \mathrm{Mat}_{n\times n}(F)$, write $A \sim_{\mathcal{O}} B$ if $A = XBX^{-1}$ for some X in $\mathrm{GL}_n(\mathcal{O})$, in which case one says that A and B are integrally similar. It is easy to check that integral similarity defines an equivalence relation.

Lemma 2.1.1. Let M_1 and M_2 be Λ-submodules of E_f with maximal $\mathcal{O}$-rank n, and let $[T]_1, [T]_2$ be the matrix representations of the action of T with respect to any $\mathcal{O}$-bases chosen for M_1 and M_2. Then $M_1 \cong M_2$ as Λ-modules if and only if $[T]_1 \sim_{\mathcal{O}} [T]_2$.

Proof. Let $\phi : M_1 \longrightarrow M_2$ be a Λ-isomorphism. Since ϕ is an isomorphism of $\mathcal{O}$-modules of rank n, ϕ has a matrix representation $[\phi] \in \mathrm{GL}_n(\mathcal{O})$ with respect to the given $\mathcal{O}$-bases. Since ϕ is Λ-linear, one has $\phi \circ T = T \circ \phi$. Then $[\phi][T]_1 = [T]_2[\phi]$ which is equivalent to $[\phi][T]_1[\phi]^{-1} = [T]_2$. Hence $[T]_1 \sim_{\mathcal{O}} [T]_2$.

Conversely, any $X \in \mathrm{GL}_n(\mathcal{O})$ such that $X[T]_1X^{-1} = [T]_2$ induces an isomorphism of $\mathcal{O}$-modules which commutes with the action of T. This clearly implies that the isomorphism induced by X commutes with polynomials in $\mathcal{O}[T]$, so the isomorphism of $\mathcal{O}$-modules induced by X is $\mathcal{O}[T]$-linear. Any such isomorphism automatically extends to be Λ-linear.

To see this, recall that Λ has the (π, T)-adic topology induced by its maximal ideal $\mathfrak{m} = (\pi, T)$. One requires the action $\Lambda \times M \longrightarrow M$ to be continuous for any Λ-module M, where M has some topology. Also, ϕ :

$M_1 \longrightarrow M_2$ is required to be continuous. Now suppose $\phi : M_1 \longrightarrow M_2$ is a continuous map of topological $\mathcal{O}$-modules with $\phi \circ T = T \circ \phi$. Then ϕ commutes with any polynomial in $\mathcal{O}[T]$. Let $g(T) \in \Lambda$ and choose a sequence of polynomials $(g_n(T))$ such that $g_n(T) \to g(T)$ as $n \to \infty$, where the limit is taken in the (π, T)-adic sense (since $\pi^n, T^n \in (\pi, T)^n$, one can take the $g_n(T)$ to have coefficients that converge π-adically to the coefficients of $g(T)$ along higher and higher powers of T). Then for any $\alpha \in M_1$

$$\begin{aligned}
\phi(g(T)\alpha) &= \phi((\lim g_n(T))\alpha) \\
&= \phi(\lim g_n(T)\alpha) \\
&= \lim \phi(g_n(T)\alpha) \\
&= \lim g_n(T)\phi(\alpha) \\
&= (\lim g_n(T))\phi(\alpha) \\
&= g(T)\phi(\alpha).
\end{aligned}$$

Hence ϕ is Λ-linear and is therefore a Λ-isomorphism from M_1 to M_2.

□

Now let $[T]$ be the matrix representation of the action of T on M where M has generators given by the rows of G. Let $D(\alpha_1, \ldots, \alpha_n)$ be the n by n diagonal matrix with the roots of f, $\alpha_1, \ldots, \alpha_n$, along the diagonal. Then one has $[T] = GD(\alpha_1, \ldots, \alpha_n)G^{-1}$. Suppose $M_1, M_2 \subseteq E_f$ with generators given by the matrices G_1, G_2 respectively, in the form given in theorem 2.0.4, and let $X = [\varphi] \in GL_n(\mathcal{O})$ be the matrix representation of a Λ-isomorphism

$\varphi : M_1 \to M_2$ in the given bases. Letting $D = D(\alpha_1, \ldots, \alpha_n)$, one has

$$\begin{aligned} & X[T]_1 = [T]_2 X \\ \Leftrightarrow & XG_1 D G_1^{-1} = G_2 D G_2^{-1} X \\ \Leftrightarrow & (G_2^{-1} X G_1) D (G_1^{-1} X^{-1} G_2) = D \end{aligned}$$

The last equality is equivalent to saying that the matrix $G_2^{-1} X G_1$ is in the stabilizer of $GL_n(F)$ acting on itself via conjugation. The following result is easy to prove.

Lemma 2.1.2. Let K be a field. If A stabilizes a diagonal matrix D in $\mathrm{GL}_n(K)$ with distinct entries along the diagonal, then A must be diagonal.

Hence $G_2^{-1} X G_1 = A$ for some diagonal matrix A, say $A = D(d_1, \ldots, d_n)$ and one has

$$X = G_2 D(d_1, \ldots, d_n) G_1^{-1},$$

so that X is upper triangular. Let the powers of π along the diagonal of G_2 be $1, \pi^{i_1}, \ldots, \pi^{i_{n-1}}$, and similarly, let $1, \pi^{j_1}, \ldots, \pi^{j_{n-1}}$ be along the diagonal of G_1. Since $X \in \mathrm{GL}_n(\mathcal{O})$, must be upper triangular with integral entries, it must have the form

$$X = \begin{pmatrix} u_1 & x_{1,2} & \cdots & x_{1,n-1} & x_{1,n} \\ & u_2 & \ldots & x_{2,n-1} & x_{2,n} \\ & & \ddots & \vdots & \vdots \\ & & & u_{n-1} & x_{n-1,n} \\ & & & & u_n \end{pmatrix}$$

with units $u_i \in \mathcal{O}^\times$ and integral entries $x_{i,j}$, and one can solve for the diagonal entries $d_1, \ldots, d_n$ as $D(d_1, \ldots, d_n) = G_2^{-1} X G_1$. This gives

$$d_1 = u_1, d_2 = u_2 \pi^{\Delta_1}, d_3 = u_3 \pi^{\Delta_2}, \ldots, d_n = u_n \pi^{\Delta_{n-1}},$$

where $\Delta_k = j_k - i_k$ for $k = 1, \ldots, n-1$. Everything is in place to prove theorem 2.1.1.

Proof. Consider the equation $XG_1 = G_2D(d_1, d_2, \ldots, d_n)$. The left-hand side is integral, and since the top row of the right-hand side is $d_1, d_2, \ldots, d_n$, one has $0 \leq \Delta_k = j_k - i_k$ for $k = 1, \ldots, n-1$. Assume $\Delta_k > 0$ for some k, so that $0 \leq i_k < j_k$. Then π divides d_{k+1} so that π divides every entry in the $k+1$st column of $G_2D(d_1, \ldots, d_n)$. Therefore π must divide the $k+1$st column of XG_1. Since X and G_1 are both upper triangular, the nonzero entries of the $k+1$st column of their product is the product of the $k+1$ by $k+1$ principle sub-matrix of X with the nonzero part of the $k+1$st column of G_1, say

$$\begin{pmatrix} u_1 & x_{1,2} & \cdots & x_{1,k+1} \\ & u_2 & \cdots & x_{2,k+1} \\ & & \ddots & \\ & & & u_{k+1} \end{pmatrix} \begin{pmatrix} 1 \\ b_2 \\ \vdots \\ b_k \\ \pi^{j_k} \end{pmatrix}.$$

Now one works from the bottom up to yield the contradiction $\pi \mid u_1$. Since π divides $b_k u_k + x_{k,k+1}\pi^{j_k}$, one has $\pi | b_k$ since $j_k > 0$ and u_k is a unit. Similarly, since π divides

$$u_{k-1}b_{k-1} + x_{k-1,k}b_k + x_{k-1,k+1}\pi^{j_k}$$

and $\pi | b_k$, π must divide b_{k-1} since u_{k-1} is a unit. Continuing in this manner, one has that π divides $b_2, b_3, \ldots, b_k$. Since π divides the topmost entry

$$u_1 + x_{1,2}b_2 + \cdots + x_{1,k}b_k + x_{1,k+1}\pi^{j_k},$$

and π divides the b's, this yields $\pi | u_1$. □

The results obtained so far give a specific form that any Λ-isomorphism $\varphi : M_1 \to M_2$ must take. Namely,

$$X = [\varphi] = G_2D(u_1, \ldots, u_n)G_1^{-1}$$

for some units $u_i \in \mathcal{O}^\times$. Let $\mathrm{Isom}_\Lambda(M_1, M_2)$ be the collection of Λ-isomorphisms from M_1 to M_2, and $\mathrm{Aut}_\Lambda(M) = \mathrm{Isom}_\Lambda(M, M)$, a group under function composition. One has

Theorem 2.1.2. For M_1 and M_2 generated by G_1 and G_2 respectively, define the map of sets

$$\varphi_{1,2} : (\mathcal{O}^\times)^n \to \mathrm{GL}_n(F)$$

by $\varphi_{1,2}(u) = G_2 D(u) G_1^{-1}$. Then $M_1 \cong M_2$ if and only if $\mathrm{im}\varphi_{1,2} \cap K \neq \emptyset$, where $K = \mathrm{GL}_n(\mathcal{O})$. If $X = \varphi_{1,2}(u) \in K$, then X is the matrix representation of a Λ-isomorphism in the given $\mathcal{O}$-bases. All Λ-isomorphisms are obtained this way.

Denote the n-dimensional integral torus over $\mathcal{O}$ by

$$\mathbb{G}_m^n(\mathcal{O}) = (\mathcal{O}^\times)^n.$$

For a Λ-module $M \subseteq E_f$ generated over $\mathcal{O}$ by the rows of G, the map $\varphi_M : \mathbb{G}_m^n(\mathcal{O}) \to \mathrm{GL}_n(F)$ given by

$$u = (u_1, \ldots, u_n) \mapsto GD(u)G^{-1}$$

is easily seen to be an injective group homomorphism, and one has

$$\mathrm{Aut}_\Lambda(M) \cong \varphi_M^{-1}(K)$$

where $K = \mathrm{GL}_n(\mathcal{O})$, the maximal compact subgroup of $GL_n(F)$. Therefore $\mathrm{Aut}_\Lambda(M)$ is realized as a subgroup of $\mathbb{G}_m^n(\mathcal{O})$. A consequence of this is

Theorem 2.1.3. $\mathrm{Aut}_\Lambda(M)$ is an abelian group.

If $M_1 \cong M_2$ as Λ-modules, then one canonically has $\mathrm{Aut}_\Lambda(M_1) \cong \mathrm{Aut}_\Lambda(M_2)$. Regarding the automorphism group as a subgroup of $\mathbb{G}_m^n(\mathcal{O})$, one obtains the stronger result

Theorem 2.1.4. If $M_1 \cong M_2$ as Λ-modules, then $\mathrm{Aut}_\Lambda(M_1)$ and $\mathrm{Aut}_\Lambda(M_2)$ coincide as subgroups of $\mathbb{G}_m^n(\mathcal{O})$.

Proof. Let $\varphi_{1,2}(u) = G_2 D(u) G_1^{-1} \in \mathrm{GL}_n(\mathcal{O})$ and suppose $v \in \mathrm{Aut}_\Lambda(M_1)$ so that $\varphi_{M_1}(v) = G_1 D(v) G_1^{-1} \in GL_n(\mathcal{O})$. Then

$$\begin{aligned}
\varphi_{1,2}(u)\varphi_{M_1}(v)\varphi_{1,2}(u)^{-1} &= G_2 D(u) G_1^{-1} (G_1 D(v) G_1^{-1}) G_1 D(u^{-1}) G_2^{-1} \\
&= G_2 D(v) G_2^{-1} \\
&\in \mathrm{GL}_n(\mathcal{O}).
\end{aligned}$$

which shows $\mathrm{Aut}_\Lambda(M_1) \subseteq \mathrm{Aut}_\Lambda(M_2)$. By symmetry one has $\mathrm{Aut}_\Lambda(M_2) \subseteq \mathrm{Aut}_\Lambda(M_1)$. □

It is unknown whether or not two Λ-modules with the same automorphism group in $\mathbb{G}_m^n(\mathcal{O})$ are forced to be isomorphic. However, for non-isomorphic Λ-modules, one can construct examples where the automorphism groups intersect nontrivially.

Chapter 3

Λ-MODULES WITH $\lambda = 2$

The Λ-modules with $\lambda = 2$ and $\mu = 0$ were classified in [13] and [8]. These results will be used later in Chapter 5 for the applications to elliptic curves.

Let $F/\mathbb{Q}_p$ be a finite extension, and let $\mathcal{O}$ be the ring of integers of F with uniformizer π. Let $f(T) \in \mathcal{O}[T]$ be a distinguished polynomial of degree $\lambda = 2$. As before $\mathcal{M}_f$ denotes the set of isomorphism classes of Λ-modules M satisfying:

- $\mathrm{char}_\Lambda(M) = f(T)$, and
- M has no nontrivial finite Λ-submodules

There are two cases to consider. First, suppose that $f(T)$ is reducible over $\mathcal{O}$, in which case $f(T) = (T - \alpha_1)(T - \alpha_2)$. The conditions above imply that M may be regarded as a submodule of $E_f = \Lambda/(T - \alpha_1) \oplus \Lambda/(T - \alpha_2)$ with finite quotient $C = E_f/M$. Write elements of M as $(x, y) \in \mathcal{O}^2$, where T acts as $T(x, y) = (\alpha_1 x, \alpha_2 y)$. The following result is proved in [13].

Theorem 3.0.5. Assume the roots α_1 and α_2 are distinct, and set $e = \mathrm{ord}_\pi(\alpha_2 - \alpha_1)$. Then $|\mathcal{M}_f| = e + 1$, and the modules

$$N_i = \langle (1, 1), (0, \pi^i) \rangle_\mathcal{O}$$

for $0 \leq i \leq e$ are a complete set of representives for the isomorphism classes in $\mathcal{M}_f$.

The notation $\langle g_1, g_2 \rangle_\mathcal{O}$ means the submodule of E_f generated over $\mathcal{O}$ by g_1, g_2.

Proof. Let N_i be generated over $\mathcal{O}$ by the rows of $G = \begin{pmatrix} 1 & 1 \\ & \pi^i \end{pmatrix}$. By theorem 2.1.1, the powers of π along the diagonal are a Λ-module invariant of M, hence the N_i represent distinct classes in $\mathcal{M}_f$. Since every class in $\mathcal{M}_f$ can be represented by N_i by theorem 2.0.4, this shows that the modules N_i are a a distinct set of representatives. To bound i, one uses module closure. Since $T(1,1) = (\alpha, \beta)$ must be in N_i, one must have $(\alpha, \beta) = x(1,1) + y(0, \pi^i)$ for $x, y \in \mathcal{O}$. This forces $x = \alpha$, and $y = (\beta - \alpha)/\pi^i$, hence $i \leq e$. □

Now consider the case where $f(T) = T^2 + bT + c \in \mathbb{Z}_p[T]$ is distinguished and irreducible, with distinct roots α, β lying in a quadratic extension of $F/\mathbb{Q}_p$. Let $M \subseteq \Lambda/(T^2 + aT + b)$ be a Λ-submodule with maximal $\mathcal{O}$-rank 2. Using the Division algorithm in Λ, elements of M can be represented in the form $xT + y$ for some $x, y \in \mathbb{Z}_p$. The following result is proved in [8].

Theorem 3.0.6. Let p be an odd prime. The Λ-modules $N_k = \langle T + \frac{b}{2}, p^k \rangle_{\mathbb{Z}_p}$ for $0 \leq k \leq \frac{\mathrm{ord}_p(b^2 - 4c)}{2}$ form a complete set of representatives for the isomorphism classes in $\mathcal{M}_f$.

This result actually applies when $\mathbb{Z}_p$ is replaced by the ring of integers in any finite extension of $\mathbb{Q}_p$, but the result is stated here for $\mathbb{Z}_p$ because it is sufficient for our applications in Chapter 6. The proof of this result is given below. Koike's idea is to extend scalars to the the ring of integers of F, where $f(T)$ splits. One can then apply Theorem 3.0.5. The proof is included here for the sake of completeness, and to illustrate the relationship between $\mathcal{M}_f$ for reducible and irreducible $f(T)$.

Proof. First, observe that lemma 2.0.1 implies that any submodule $N \subseteq \Lambda/(f(T))$ with $\mathrm{rank}_{\mathbb{Z}_p} N = 2$ has the form $\langle \pi^{a_1} T + x_{1,2}, \pi^{a_2} \rangle_{\mathbb{Z}_p}$. It is easy

to see that module closure implies $a_1 \leq \mathrm{ord}_p(x_{1,2})$ and $a_1 \leq a_2$, and since multiplication by π^{a_1} is a Λ-isomorphism, one may assume without loss of generality that $N = \langle T - a, \pi^k \rangle_{\mathbb{Z}_p}$ for some $a \in \mathbb{Z}_p$.

Let $F/\mathbb{Q}_p$ be the splitting field for $f(T)$, with ring of integers denoted by $\mathcal{O}$. Let π be a uniformizer for $\mathcal{O}$, so that (π) is the unique maximal ideal of $\mathcal{O}$. Let $\Lambda_{\mathcal{O}} = \mathcal{O}[[T]]$. Since $\mathcal{O} \cong \mathbb{Z}_p^2$ as a $\mathbb{Z}_p$-algebra, one has $\Lambda_{\mathcal{O}} \cong \Lambda^2$ as a Λ-module. Hence if M is a Λ-module, extending the scalars to $\Lambda_{\mathcal{O}}$ gives $M \otimes_\Lambda \Lambda_{\mathcal{O}} \cong M \oplus M$. The functor $M \mapsto M \otimes_\Lambda \Lambda_{\mathcal{O}}$ is therefore faithfully flat from the category of Λ–modules to the category of $\Lambda_{\mathcal{O}}$-modules, and therefore $M_1 \cong M_2$ over Λ if and only if $M_1 \otimes \Lambda_{\mathcal{O}} \cong M_2 \otimes \Lambda_{\mathcal{O}}$ over $\Lambda_{\mathcal{O}}$. Let $\mathcal{M}_f^{\mathcal{O}}$ denote the isomorphism classes of $\Lambda_{\mathcal{O}}$-modules with characteristic polynomial $f(T)$ and having no nontrivial finite $\Lambda_{\mathcal{O}}$-submodules. The functor $\_ \otimes \Lambda_{\mathcal{O}}$ therefore induces an injection

$$\mathcal{M}_f \longrightarrow \mathcal{M}_f^{\mathcal{O}}.$$

The result for the reducible case gives the $e+1$ representives: $\langle (1,1), (0,\pi^i) \rangle_{\mathcal{O}}$ for the classes in $\mathcal{M}_f^{\mathcal{O}}$, where $e = \mathrm{ord}_\pi(\beta - \alpha)$.

Now consider the image of $\_ \otimes \Lambda_{\mathcal{O}}$. Applying $\_ \otimes \Lambda_{\mathcal{O}}$ to the exact sequence

$$0 \longrightarrow N_k \longrightarrow \Lambda/(f(T)) \longrightarrow C \longrightarrow 0$$

gives

$$0 \longrightarrow N_k \otimes \Lambda_{\mathcal{O}} \longrightarrow \Lambda_{\mathcal{O}}/(f(T)) \longrightarrow C \otimes \Lambda_{\mathcal{O}} \longrightarrow 0,$$

and one has $N_k \otimes \Lambda_{\mathcal{O}} \cong \langle T + b/2, p^k \rangle_{\mathcal{O}}$. Under the canonical pseudo-isomorphism $\Lambda_{\mathcal{O}}/(f(T)) \to \Lambda_{\mathcal{O}}/(T-\alpha) \oplus \Lambda_{\mathcal{O}}/(T-\beta)$, the generators $T + b/2, p^k$ become

$$T + b/2 \mapsto ((\alpha - \beta)/2, (\beta - \alpha)/2)$$
$$p^k \mapsto (p^k, p^k)$$

Therefore $N_k \otimes \Lambda_{\mathcal{O}}$ is identified with the submodule of $\Lambda_{\mathcal{O}}/(T-\alpha) \oplus \Lambda_{\mathcal{O}}/(T-\beta)$ generated over $\mathcal{O}$ by the rows of the matrix

$$B = \begin{pmatrix} \frac{\alpha-\beta}{2} & \frac{\beta-\alpha}{2} \\ p^k & p^k \end{pmatrix}.$$

Suppose that $F/\mathbb{Q}_p$ is unramified. Using the row and column operations allowed in the proof of Theorem 2.0.4, one can bring B to the form

$$\begin{pmatrix} 1 & 1 \\ & \pi^{e-k} \end{pmatrix}.$$

It only remains to see that as k ranges over $0, 1, \ldots, \mathrm{ord}_p(b^2-4c)/2$, the exponent $e-k$ ranges over $0, 1, \ldots, e$, so that $\mathcal{M}_f$ maps surjectively, hence bijectively, to $\mathcal{M}_f^{\mathcal{O}}$. But

$$\begin{aligned} \mathrm{ord}_p(b^2-4c) &= \mathrm{ord}_\pi(b^2-4c) \\ &= \mathrm{ord}_\pi((\beta-\alpha)^2) \\ &= 2e. \end{aligned}$$

and the result follows in this case.

Otherwise $F/\mathbb{Q}_p$ is totally ramified, so that $p = u\pi^2$ for some $u \in \mathcal{O}^\times$. The matrix B becomes

$$\begin{pmatrix} \pi^e & -\pi^e \\ \pi^{2k} & \pi^{2k} \end{pmatrix}$$

after dividing the units from the rows. If $2k \leq e$, one exchanges row 1 and 2 of B and performs the same row and column operations used above to produce the matrix

$$\begin{pmatrix} 1 & 1 \\ & \pi^{e-2k} \end{pmatrix},$$

while if $e < 2k$, similar row and column operations yield

$$\begin{pmatrix} 1 & 1 \\ & \pi^{2k-e} \end{pmatrix}.$$

Note that since one knows before hand that $N_k \otimes \Lambda_{\mathcal{O}}$ is a $\Lambda_{\mathcal{O}}$-module, one must have $2k - e \leq e$, which implies $k \leq e$. Therefore, as k ranges over $0, 1, 2, \cdots, e$, the modules N_k are identified into classes as $N_k \cong N_{e-k}$, so the N_k represent $\lfloor e/2 \rfloor = \lfloor \mathrm{ord}_p(b^2 - 4c)/2 \rfloor$ distinct classes. If one has a different $T - a$ as the first generator instead of $T + b/2$, it is can be shown by a similar argument (see [8]) that the resulting classes are identified in the same way. Therefore the N_k as k ranges over $0, 1, 2, \ldots, \lfloor \mathrm{ord}_p(b^2 - 4c)/2 \rfloor$ form a set of distinct and exhaustive representatives for the classes in $\mathcal{M}_f$. $\square$

Chapter 4

Λ-MODULES WITH $\lambda = 3$

Let $f(T) = (T-\alpha_1)(T-\alpha_2)(T-\alpha_3) \in \mathcal{O}[T]$, with roots $\alpha_i \in (\pi)$ such that $\alpha_i \neq \alpha_j$ for $i \neq j$. As before $\mathcal{M}_f$ denote the set of Λ-isomorphism classes of modules M such that $\mathrm{char}_\Lambda M = f(T)$, and such that M has no nontrivial finite Λ-submodules. By theorem 2.0.4, each isomorphism class in $\mathcal{M}_f$ can be represented by a module M generated over $\mathcal{O}$ by the rows of a matrix

$$G = \begin{pmatrix} 1 & 1 & 1 \\ & \pi^i & a \\ & & \pi^j \end{pmatrix}$$

when $3 \leq q = |\mathcal{O}/(\pi)|$. As in [14], $[i,j,a]$ denotes the Λ-isomorphism class corresponding to G. In this chapter, it will be shown that there are only a finite number of possible G. The proof of this is essentially to use Λ-module closure to bound the i,j, and once this is accomplished, using row operations one may reduce a mod π^j so that the parameter a may be taken in the finite ring $\mathcal{O}/(\pi^j)$. Then, an if and only if condition is given for when two classes $[i,j,a_t]$ for $t = 1,2$ are equal.

4.1 Bounding the Generators

Bounding the parameters i,j suffices to illustrate a special case of the fundamental finiteness result from [13]:

Theorem 4.1.1. [Sumida's theorem] If $f(T) \in \Lambda \setminus (\pi)$, then $\mathcal{M}_f$ is finite if and only if $f(T)$ is square-free, i.e. $f(T)$ cannot be written as $g(T)^2 h(T)$ for power series $g(T) \in \Lambda \setminus \Lambda^\times, h(T) \in \Lambda$.

First consider the elementary Λ-module $E_{\mathrm{ann}} = \Lambda/(f(T))$. Since $(f(T)) \subseteq (T-\alpha_i)$, one has natural surjections $E_{\mathrm{ann}} \longrightarrow \Lambda/(T-\alpha_i)$ given by $g(T)$ mod $(f(T)) \mapsto g(T)$ mod $(T-\alpha_i)$, and their sum induces a map $\psi : E_{\mathrm{ann}} \longrightarrow E_f$

given by $\psi(g(T)) = (g(\alpha_1), g(\alpha_2), g(\alpha_3))$. By lemma 13.8 in [16], this map is injective with finite cokernel, so by theorem 2.0.4 one can find an isomorphic copy of $\psi(E_{\text{ann}})$ in E_f with generators given by G. To see this explicitly, using the Division Algorithm in Λ, E_{ann} has an $\mathcal{O}$-basis given by $\{1, T, T^2\}$ which maps to the $\mathcal{O}$-basis

$$(1,1,1), (\alpha_1, \alpha_2, \alpha_3), (\alpha_1^2, \alpha_2^2, \alpha_3^2)$$

for the image $\psi(E_{\text{ann}})$. One can apply row operations to the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix}$$

to rewrite the generators of $\psi(E_{\text{ann}})$ in upper triangular form. Since this is a common exercise in linear algebra, the details will not be shown, but simply write the result as

$$\begin{pmatrix} 1 & 1 & 1 \\ & \alpha_2 - \alpha_1 & \alpha_3 - \alpha_1 \\ & & (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \end{pmatrix}.$$

Write $\alpha_2 - \alpha_1 = u\pi^l$, $\alpha_3 - \alpha_1 = v\pi^m$, and $\alpha_3 - \alpha_2 = w\pi^n$ for units u, v, w. Dividing row 2 of the above matrix by u and row 3 by vw gives the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ & \pi^l & u_f\pi^m \\ & & \pi^{m+n} \end{pmatrix}$$

with $u_f = \frac{v}{u}$, a unit determined by f. Therefore E_{ann} falls into the class $[l, m+n, u_f p^m]$. It is easy to see that any M with generators equal to the rows of the matrix G must contain E_{ann}. Since $(1,1,1) \in M$, and since $TM \subseteq M$, one must have $T(1,1,1) = (\alpha_1, \alpha_2, \alpha_3) \in M$ and $T^2(1,1,1) = (\alpha_1^2, \alpha_2^2, \alpha_3^2) \in M$.

Hence M contains a copy of E_{ann}. Hence the rows of the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ & \pi^l & u_f\pi^m \\ & & \pi^{m+n} \end{pmatrix}$$

must be in M, and one must be able to write each row as an $\mathcal{O}$-linear combination of the generators of M. This automatically gives $0 \leq i \leq l$, and $0 \leq j \leq m+n$ so the parameters i, j, a are bounded. One must also have $(0, \pi^l, u_f\pi^m) \in M$ so that

$$x(0, \pi^i, a) + y(0, 0, \pi^j) = (0, \pi^l, u_f\pi^m),$$

which after solving for x and re-substituting implies $\pi^{l-i}a \equiv u_f\pi^m \bmod \pi^j$. As long as these conditions are met, the module closure relation $T(1,1,1) \in M$ is satisfied. The only other nontrivial closure condition needed is $T(0, \pi^i, a) \in M$. Hence for some $x, y \in \mathcal{O}$,

$$\begin{aligned} T(0, \pi^i, a) &= (0, \alpha_2\pi^i, \alpha_3 a) \\ &= x(0, \pi^i, a) + y(0, 0, \pi^j) \end{aligned}$$

so that $x = \alpha_2$ and one must be able to write $\alpha_2 a + y\pi^j = \alpha_3 a$. This is possible if and only if $j \leq n + \text{ord}_\pi(a)$. If the convention is made that the roots of $f(T)$ are labeled to make $l \leq m$, then for $j \leq l - i$, the above congruence imposes no restriction on a, while for $j > l - i$ one must have $a \equiv u_f\pi^{m-l+i} \bmod \pi^{j-l+i}$. In this case $\text{ord}_\pi(a)$ is forced to be $m - l + i$, so the inequality $j \leq n + \text{ord}_\pi(a)$ implies $j \leq n + m - l + i$.

To summarize what has been shown so far, for the prime powers of π^i, π^j in the matrix G, one must have $0 \leq i \leq l$ and $0 \leq j \leq m+n$. In addition, for a fixed j, one can take $a \in \mathcal{O}/(\pi^j)$. If $i + j \leq l$, then one can

take any $a \bmod \pi^j$. Otherwise, if $l < i + j$, then the congruence uniquely determines a modulo π^{i+j-l}. Lastly, $j \leq n + m - l + i$. These conditions are implied by module closure $TM \subset M$. Conversely, any M generated over $\mathcal{O}$ by the rows of G with i, j, a satisfying these conditions is closed under the action of T and is therefore a Λ-module.

Module Closure Relations:

MC1 $(i, j) \in [0..l] \times [0..n + m]$ with $j \leq n + m - l + i$

MC2 If $i + j \leq l$, any $a \in \mathcal{O}/(\pi^j)$ is allowed.

MC3 If $l < i + j$, then $a \equiv \pi^{m-(l-i)} u_f \bmod \pi^{i+j-l}$.

These conditions are illustrated in figure 4.1 below.

4.2 Λ-Isomorphism and Integral Similarity

Now consider the problem of determining when two Λ-modules generated over $\mathcal{O}$ by the rows of G in E_f are isomorphic. If M is generated over $\mathcal{O}$ by the matrix G, then it has already been shown in section 2.1 that the powers of π along the diagonal of G are an invariant of M. In the notation from [14], the question is: for a_1, a_2 in $\mathcal{O}/(\pi^j)$, when is $[i, j, a_1] = [i, j, a_2]$? Let $G(i, j, a)$ be the matrix

$$G(i, j, a) = \begin{pmatrix} 1 & 1 & 1 \\ & \pi^i & a \\ & & \pi^j \end{pmatrix},$$

and let M_1, M_2 be generated over $\mathcal{O}$ by the rows of $G(i, j, a_1)$ and $G(i, j, a_2)$ respectively. In section 2.1, it was already shown that any Λ-isomorphism $\phi : M_1 \longrightarrow M_2$ must have a matrix representation of the form

$$X = [\varphi] = G_2 D(u_1, u_2, u_3) G_1^{-1}$$

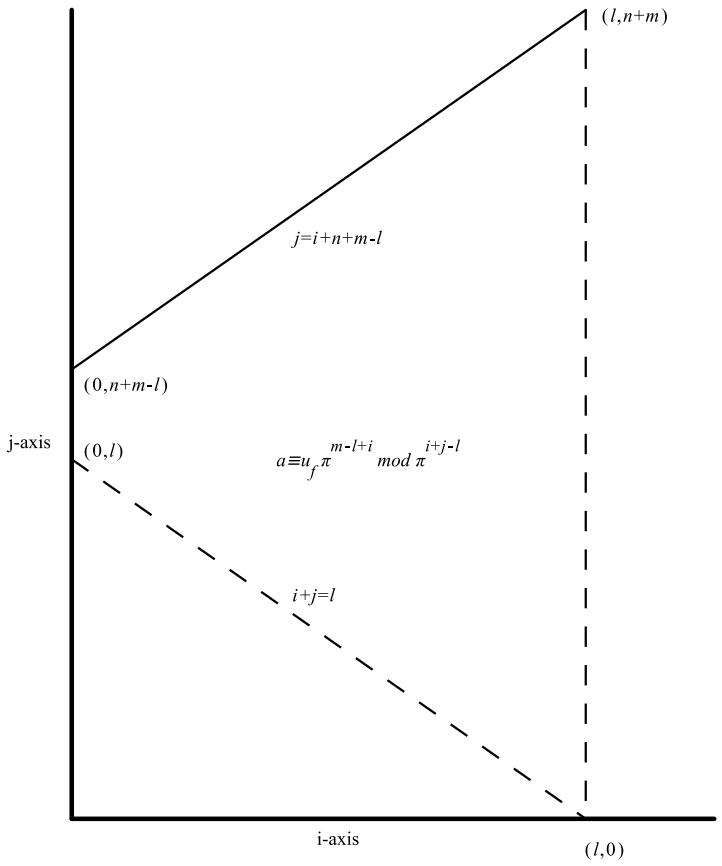

Figure 4.1: Parameter Domain For Module Closure

with respect to the given $\mathcal{O}$-bases, where $u_1, u_2, u_3 \in \mathcal{O}^\times$. Let

$$X = \begin{pmatrix} u_1 & x & y \\ & u_2 & z \\ & & u_3 \end{pmatrix},$$

and note that the only condition that prevents X from being in $\mathrm{GL}_3(\mathcal{O})$ is the integrality of x, y, z. Write the last equation as $XG_1 = G_2 D(u_1, u_2, u_3)$. Equating the off-diagonal entries of the left and right-hand sides gives the

system

$$u_1 + x\pi^i = u_2 \tag{4.1a}$$

$$u_1 + xa_1 + y\pi^j = u_3 \tag{4.1b}$$

$$u_2 a_1 + z\pi^j = a_2 u_3, \tag{4.1c}$$

and viewing the last equation as a congruence modulo π^j, one sees that $[i, j, a_1] = [i, j, a_2]$ implies $\mathrm{ord}_\pi(a_1) = \mathrm{ord}_\pi(a_2)$. Viewing (4.1a)-(4.1c) as a system in the unknowns u_1, u_2, u_3, and x, y, z, one can solve for the u_i in terms of x, y, and z. The system 4.1 in matrix form is

$$\begin{pmatrix} 1 & -1 & 0 & \pi^i & 0 & 0 \\ 1 & 0 & -1 & a_1 & \pi^j & 0 \\ 0 & a_1 & -a_2 & 0 & 0 & \pi^j \end{pmatrix},$$

and viewing this as a system of equations over F, one can bring this matrix into the form $(I_{3\times 3}|B(a_1, a_2))$ with

$$B(a_1, a_2) = \frac{1}{a_1 - a_2} \begin{pmatrix} a_1(\pi^i - a_2) & -a_2\pi^j & \pi^j \\ a_2(\pi^i - a_1) & -a_2\pi^j & \pi^j \\ a_1(\pi^i - a_1) & -a_1\pi^j & \pi^j \end{pmatrix}.$$

Note that $a_1 - a_2 \neq 0$ since one may assume without loss of generality that $a_1 \not\equiv a_2 \bmod \pi^j$. Therefore one has $[i, j, a_1] = [i, j, a_2]$ if and only if there exist $x, y, z \in \mathcal{O}$ with

$$B(a_1, a_2) \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in (\mathcal{O}^\times)^3.$$

To test this condition, one can ignore the last two columns in $B(a_1, a_2)$ since one can assume $k' = \mathrm{ord}_\pi(a_1 - a_2) < j$ (a is taken modπ^j). For example, the first entry of a linear combination of the columns of $B(a_1, a_2)$ is

$$x\frac{a_1(\pi^i - a_2)}{a_1 - a_2} - y\frac{a_2\pi^j}{a_1 - a_2} + z\frac{\pi^j}{a_1 - a_2},$$

and since the last two terms are always divisible by π, the sum will be a unit if and only if $xa_1(\pi^i - a_2)/(a_1 - a_2)$ is a unit for some $x \in \mathcal{O}$. This is possible if and only if $\mathrm{ord}_\pi(a_1) + \mathrm{ord}_\pi(\pi^i - a_2) \leq \mathrm{ord}_\pi(a_1 - a_2)$. The same argument applies to the other two rows of $B(a_1, a_2)$. One now has the following useful criterion for when two isomorphism classes $[i, j, a_1]$ and $[i, j, a_2]$ are the same.

Theorem 4.2.1. For $a_1, a_2 \in \mathcal{O}/(\pi^j)$, $[i, j, a_1] = [i, j, a_2]$ if and only if $\mathrm{ord}_\pi(a_1) = \mathrm{ord}_\pi(a_2), \mathrm{ord}_\pi(\pi^i - a_1) = \mathrm{ord}_\pi(\pi^i - a_2)$ and $\mathrm{ord}_\pi(a_1) + \mathrm{ord}_\pi(\pi^i - a_2) \leq \mathrm{ord}_\pi(a_1 - a_2)$. Letting $k = \mathrm{ord}_\pi(a_s)$, $a_s = v_s\pi^k$ for $v_s \in \mathcal{O}^\times, s = 1, 2$, and $k' = \mathrm{ord}_\pi(a_1 - a_2)$, this condition is equivalent to:

1. If $k < i$, then $2k \leq k'$.
2. If $k = i$, then $\mathrm{ord}_\pi(1 - v_1) = \mathrm{ord}_\pi(1 - v_2)$ and $2k + \mathrm{ord}_\pi(1 - v_s) \leq k'$.
3. If $i < k$, then $k + i \leq k'$.

Proof. First suppose that $k < i$. By the Isosceles Triangle Property, $\mathrm{ord}_\pi(\pi^i - a_2) = k$, and similarly all entries in the first column of $(a_1 - a_2)B(a_1, a_2)$ have valuation $2k$, so the condition becomes $2k \leq k'$. If $i < k$, the Isosceles Triangle Property gives $\mathrm{ord}_\pi(\pi^i - a_2) = i$, and a similar argument gives $k + i \leq k'$. If $k = i$, then $\mathrm{ord}_\pi(\pi^i - a_2) = \mathrm{ord}_\pi(\pi^k(1 - u_2)) = k + \mathrm{ord}_\pi(1 - u_2)$ and similarly $\mathrm{ord}_\pi(\pi^i - a_1) = k + \mathrm{ord}_\pi(1 - u_1)$. Now the condition is that there exists an $x \in \mathcal{O}$ so that

$$\mathrm{ord}_\pi(xa_1(\pi^i - a_2)) = \mathrm{ord}_\pi(x) + 2k + \mathrm{ord}_\pi(1 - v_2) = k'$$
$$\mathrm{ord}_\pi(xa_2(\pi^i - a_1)) = \mathrm{ord}_\pi(x) + 2k + \mathrm{ord}_\pi(1 - v_1) = k'$$
$$\mathrm{ord}_\pi(xa_1(\pi^i - a_1)) = \mathrm{ord}_\pi(x) + 2k + \mathrm{ord}_\pi(1 - v_1) = k'.$$

Therefore, one must have $\mathrm{ord}_\pi(1 - v_1) = \mathrm{ord}_p(1 - v_2)$ and $2k + \mathrm{ord}_\pi(1 - v_s) = k' - \mathrm{ord}_\pi(x) \leq k'$. Conversely, if these inequalities are met in each case, then

x can be chosen to be the unique power of π which multiplies the first column of $B(a_1, a_2)$ into $(\mathcal{O}^\times)^3$. $\square$

Although the proof and the discussion preceeding it were somewhat ad hoc since there were exactly the same number of units u_1, u_2, u_3 as off-diagonal entries of the matrix X, the quantities $i, j, \mathrm{ord}_\pi(a)$ were discovered to be invariants of the $\mathcal{O}$-submodule generated by the rows of $G(i, j, a)$. One can use localization to explain these invariants, and the quantity $\mathrm{ord}_\pi(\pi^i - a)$ appearing in theorem 4.2.1. For example, localizing M at $f_3(T) = (T - \alpha_3)$, gives the Λ_{f_3}-submodule $M_{f_3} = \langle (1/1, 1/1, 1/1), (0, \pi^i/1, a/1), (0, 0, \pi^j/1) \rangle_{\mathcal{O}}$ of $(E_f)_{f_3}$. Here the fact that localization distributes over direct sums is being used to form the fractions over each component. Since f_3 is a unit in Λ_{f_3},

$$M_{f_3} = f_3 M_{f_3} = \left\langle \left(\frac{\alpha_1 - \alpha_3}{1}, \frac{\alpha_2 - \alpha_3}{1}, 0 \right), \left(0, \frac{\pi^i(\alpha_2 - \alpha_3)}{1}, 0 \right), (0, 0, 0) \right\rangle_{\mathcal{O}},$$

where the last coordinates have been made 0 by multiplying by f_3. Assembling these into a matrix and dividing columns 1 and 2 by $\alpha_1 - \alpha_3$ and $\alpha_2 - \alpha_3$ implies

$$M_{f_3} \cong \langle (1/1, 1/1, 0), (0, \pi^i/1, 0) \rangle_{\mathcal{O}}$$

by theorem 2.0.2. For the case $\lambda = 2$ it was already shown that the power of π occuring along the diagonal of G is an invariant. Repeating this argument at $f_2(T) = T - \alpha_2$ and suppressing the second coordinate, M_{f_2} is generated by $(1, 1), (0, a), (0, \pi^j)$ which falls into the class $\langle (1, 1), (0, \pi^{\min\{j, \mathrm{ord}_\pi(a)\}}) \rangle_{\mathcal{O}}$ which gives the degree 2 invariant $\min\{j, \mathrm{ord}_\pi(a)\}$. At $f_1(T) = T - \alpha_1$, $M_{f_1} \cong \langle (1, 1), (\pi^i, a), (0, \pi^j) \rangle_{\mathcal{O}} = \langle (1, 1), (0, a - \pi^i), (0, \pi^j) \rangle_{\mathcal{O}}$ which similarly gives the degree 2 invariant $\min\{j, \mathrm{ord}_\pi(\pi^i - a)\}$. These local invariants are being added on the left side of the inequality in theorem 4.2.1.

Two examples will now be given to see how theorem 4.2.1 allows one to calculate $\mathcal{M}_f$. These two examples have been calculated previously by Sumida

and Hachimori, respectively. Our method differs considerably from that in [14] since all possibilities for l, m, n are being handled at once.

4.3 Examples

Example: $(l, m, n) = (1, 1, 1)$

The module closure conditions imply $(i, j) \in [0..1] \times [0..2]$ with $j \leq i+1$. Hence $(i, j) = (0, 0), (0, 1), (1, 0), (1, 1), (1, 2)$. For $j = 0$, there is only the class given by $a = 0$, so one has the classes $E_f = [0, 0, 0]$ and $[1, 0, 0]$. For $(0, 1)$, one must have $a \in \mathcal{O}/(\pi)$, and the invariant $\mathrm{ord}_\pi(a)$ can be 0 or ∞. If a is a unit, then $k = 0 = i$ and by theorem 4.2.1 $a = 1$ is in a class by itself. Otherwise $a \neq 1$, and $\mathrm{ord}_\pi(1 - a) = 0$. Substituting into the case $k = i$ of theorem 4.2.1 gives $0 \leq k'$ which is always true. This gives the classes $[0, 1, 1]$ and $[0, 1, 2]$. For $\mathrm{ord}_\pi(a) = \infty$ there is only the class $[0, 1, 0]$. For $(i, j) = (1, 1)$, one is above the line $i + j = l$, so the congruence in the module closure relation MC3 must be taken into account. Hence $a \equiv \pi u_f \equiv 0 \bmod \pi$ yielding the class $[1, 1, 0]$. Similarly for the remaining case $(i, j) = (1, 2)$, one has $a \equiv \pi u_f \bmod \pi^2$ giving the class $E_{\mathrm{ann}} = [1, 2, \pi u_f]$. These are precisely the 7 classes found by Sumida in [14] for this case.

Example: $(l, m, n) = (2, 2, 2)$

The parameter domain is $[0..2] \times [0..4]$ with $j \leq i + 2$. This gives the 12 possibilities for i, j shown in figure 4.2:

As in the previous example, for $j = 0$ one has the three classes $[0, 0, 0], [1, 0, 0]$, and $[2, 0, 0]$. The same calculations as in the previous example also give the three classes $[0, 1, 0], [0, 1, 1]$, and $[0, 1, 2]$ for $(i, j) = (0, 1)$. For $i = 2$, MC3 implies $a \equiv \pi^2 u_f \bmod \pi^j$ giving the four classes $[2, j, \pi^2 u_f]$ for $j = 1, 2, 3, 4$.

For $(i, j) = (0, 2)$ the possibilities for $\mathrm{ord}_\pi(a)$ are 0,1, and ∞. If a is a unit, then one is in case $i = k = 0$ of theorem 4.2.1, and the condition is that

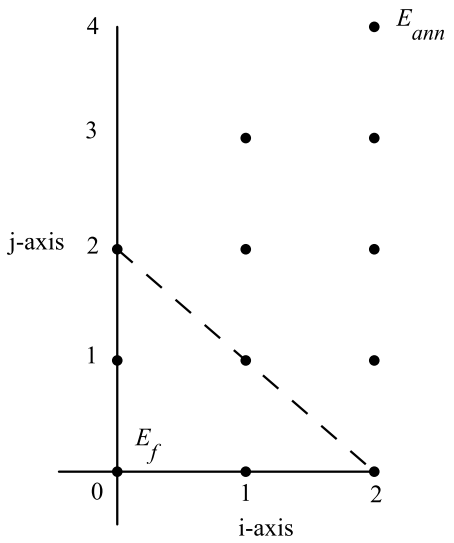

Figure 4.2: Parameter Domain For $(l, m, n) = (2, 2, 2)$

$\text{ord}_\pi(1 - v_s) \leq k'$, i.e. one can identify two classes corresponding to a_1, a_2 if they agree up to at least as many π-adic digits as their depth in the 1-unit filtration of $\mathcal{O}^\times$. If $\text{ord}_\pi(1-v_s) = 0$, then one can identify all such a to the class corresponding to 2 since one only needs $0 \leq k'$. If $\text{ord}_\pi(1 - v_s) = 1$, then one can identify all such a_1, a_2 with $1 \leq k'$. But for any two units at level 1 in the 1-unit filtration, say $a_1 = 1 + \alpha_1\pi, a_2 = 1 + \beta_1\pi$ with $\alpha_1, \beta_1 \neq 0$, they already agree in the first digit so they all identify to $1 + \pi$. At level 2, $a \equiv 1 \bmod \pi^2$. This gives the classes $[0, 2, 2], [0, 2, 1+\pi], [0, 2, 1]$. If $\text{ord}_\pi(a) = 1$, then one is in case $i < k$ of theorem 4.2.1 and require $2 \leq k'$, therefore one can only identify two classes if $a_1 \equiv a_2 \bmod \pi^2$. This gives the class $[0, 2, \pi]$. Lastly there is the class $[0, 2, 0]$ for a total of 5 classes in this case.

For $(i, j) = (1, 1)$, $\text{ord}_\pi(a) = 0, \infty$. If a is a unit modπ, then one can identify two units if and only if $0 \leq k'$, so all units identify to the class given

by $a = 1$. Hence there are two classes for this case given by $[1, 1, 1], [1, 1, 0]$.

For $(i, j) = (1, 2)$ above the line $i + j = 2$, module closure condition 3 requires $a \equiv \pi u_f \equiv 0 \bmod \pi$. Hence $k = 1 = i$, and the condition in theorem 4.2.1 gives $2 \leq 2 + \mathrm{ord}_\pi(1 - v_s) \leq k'$ so one can identify a_1 and a_2 if and only if $a_1 \equiv a_2 \bmod \pi^2$. Since there are $|\mathcal{O}/(\pi)|$ integers $\bmod \pi^2$ satisfying $a \equiv 0 \bmod \pi$, one has $q = p^f$ distinct classes $[1, 2, \alpha\pi]$ for $\alpha \in \mathbb{F}_q$.

For $(i, j) = (1, 3)$ above the line $i+j = 2$, MC3 forces $a \equiv \pi u_f \mod \pi^2$. Then a has a π-adic expansion

$$a = \alpha_1 \pi + \alpha_2 \pi^2$$

with $\alpha_1 \equiv u_f \bmod \pi$, and $\alpha_2 \in \mathbb{F}_q$. The condition for identifying two classes becomes $2+\mathrm{ord}_\pi(1-v_s) \leq k'$. If $a_2 = \beta_1\pi+\beta_2\pi^2$ is a similar π-adic expansion, then $v_1 = \alpha_1 + \alpha_2\pi$ and $v_2 = \beta_1 + \beta_2\pi$ with $\beta_1 \equiv \alpha_1 \equiv u_f \bmod \pi$. Since $u_f \not\equiv 1 \bmod \pi$, one has $\mathrm{ord}_\pi(1 - v_s) = 0$ for $s = 1, 2$. Therefore one can identify two classes if $2 \leq k'$. Since the first two π-adic digits are already equal, this condition is always true and the possible a collapse to one class

given by $[1, 3, u_f\pi]$. Hence, there are a total of $q + 18$ classes given by:

$$[0, 0, 0],$$

$$[0, 1, 0], [0, 1, 1], [0, 1, 2],$$

$$[0, 2, 0], [0, 2, 1], [0, 2, 2], [0, 2, 1 + \pi], [0, 2, \pi],$$

$$[1, 0, 0],$$

$$[1, 1, 0], [1, 1, 1],$$

$$[1, 2, \alpha\pi] \text{ for } \alpha \in \mathbb{F}_q,$$

$$[1, 3, u_f\pi],$$

$$[2, 0, 0],$$

$$[2, j, \pi^2 u_f] \text{ for } j = 1, 2, 3, 4,$$

where $q = p^f$ for f the residue field degree of $F/\mathbb{Q}_p$.

The elementary types:

Let P be a partition of $\{1, 2, 3\}$, and consider the elementary Λ-modules

$$E = \bigoplus_{B \in P} \Lambda / \prod_{i \in B} (T - \alpha_i).$$

There are 5 partitions of $\{1, 2, 3\}$ corresponding to the elementary types

$$\Lambda/(T - \alpha_1) \oplus \Lambda/(T - \alpha_2)(T - \alpha_3)$$

$$\Lambda/(T - \alpha_3) \oplus \Lambda/(T - \alpha_1)(T - \alpha_2)$$

$$\Lambda/(T - \alpha_2) \oplus \Lambda/(T - \alpha_1)(T - \alpha_3)$$

$$E_{\text{ann}} = \Lambda/f$$

$$E_f = \Lambda/(T - \alpha_1) \oplus \Lambda/(T - \alpha_2) \oplus \Lambda/(T - \alpha_3).$$

In the notation $[i, j, a]$ these are given as $[0, n, 1]$, $[l, 0, 0]$, $[0, m, 0]$, $[0, 0, 0]$, and $[l, m + n, u_f \pi^m]$, respectively.

Chapter 5

Λ-MODULES WITH $\lambda = 4$

As before, $\mathcal{O}$ denotes the ring of integers in a finite extension $F/\mathbb{Q}_p$, and let π be a generator of the maximal ideal of $\mathcal{O}$. Let $f(T) = \prod_{i=1}^{4}(T - \alpha_i)$. As before, $\mathcal{M}_f$ denotes the set of isomorphism classes of $\Lambda = \mathcal{O}[[T]]$-submodules $M \subseteq E_f = \bigoplus_{i=1}^{4} \Lambda/(T - \alpha_i)$, with finite quotient E_f/M. By theorem 2.0.4, up to isomorphism, M is generated over $\mathcal{O}$ by the rows of some

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ & \pi^i & a & b \\ & & \pi^j & c \\ & & & \pi^k \end{pmatrix}$$

when $4 \leq q$. Denote the isomorphism class of M by $[i, j, k, a, b, c]$, where $a \in \mathcal{O}/(\pi^j)$ and $b, c \in \mathcal{O}/(\pi^k)$. The tuple (i, j, k) is a Λ-module invariant of M by theorem 2.1.1. As before, module closure $TM \subseteq M$ bounds the parameters, and one has reduced $\mathcal{M}_f$ to a finite list $\{[i, j, k, a, b, c]\}$. For each tuple (i, j, k) in the list, the task is then to decide when two classes, $[i, j, k, a_t, b_t, c_t]$ for $t = 1, 2$ are the same.

In general the technique in chapter 4 which produced theorem 4.2.1 does not work well for $\lambda > 3$. The system of equations resulting from the matrix equation

$$XG_1 = G_2D$$

was simple enough that one could solve for the unit entries u along the diagonal in in terms of the off-diagonal entries of X. For larger λ, the equations become much too cumbersome to solve. In this section, an algorithm will be given, based on the approach at the end of section 2.1, to decide when two classes are the same. For Λ-modules M_1, M_2, a map $\varphi_{1,2} : (\mathcal{O}^\times)^4 \to GL_n(F)$ was

defined, and it was shown that $M_1 \cong M_2$ if and only if $\mathrm{im}\varphi_{1,2} \cap K \neq \emptyset$, where $K = \mathrm{GL}_n(\mathcal{O})$. This enables one to search for an isomorphism by finding a $u \in (\mathcal{O}^\times)^n$ with $\varphi_{1,2}(u) \in K$. One problem with this is that $(\mathcal{O}^\times)^n$ is infinite, so the first task is to show that one only needs to search over $\overline{u} \in ((\mathcal{O}/(\pi^m))^\times)^n$ for some m. This is still in general a large set. The idea for further reducing the size is to "divide" out the nontrivial automorphisms of M_1 and M_2 from $(\mathcal{O}^\times)^n$. At the same time, one can use theorem 2.1.4 to decide that $M_1 \ncong M_2$.

5.1 Generators

The first goal is to translate the module closure condition into restrictions on the parameters i, j, k, a, b, c. The module $E_{\mathrm{ann}} = \Lambda/(f(T))$ will again play a fundamental role, and should be viewed as a lower bound in the lattice of Λ-submodules of E_f up to isomorphism. First, consider the canonical map $\psi : E_{\mathrm{ann}} \to E_f$ given by

$$\psi(g(T) \bmod (f(T))) = (g(\alpha_1), g(\alpha_2), g(\alpha_3), g(\alpha_4)).$$

Lemma 13.8 in [16] implies that ψ is injective with finite co-kernel. The Division Algorithm for Λ implies that E_{ann} has an $\mathcal{O}$-basis $\{1, T, T^2, T^3\}$ which maps to the $\mathcal{O}$-basis $\{(1,1,1,1), (\alpha_1, \alpha_2, \alpha_3, \alpha_4), (\alpha_1^2, \alpha_2^2, \alpha_3^2, \alpha_4^2), (\alpha_1^3, \alpha_2^3, \alpha_3^3, \alpha_4^3)\}$ for the image $\psi(E_{\mathrm{ann}})$. Assemble this basis into the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 \end{pmatrix},$$

and use row operations to produce the upper triangular form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ & \alpha_1 - \alpha_2 & \alpha_1 - \alpha_3 & \alpha_1 - \alpha_4 \\ & & (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) & (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_4) \\ & & & (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4) \end{pmatrix}.$$

Note that these row operations preserve the image (not just the isomorphism class) of E_{ann} inside of E_f. Since theorem 2.0.4 shows that any submodule $M \subseteq E_f$ up to isomorphism contains $(1,1,1,1)$, module closure implies that M must contain the T-cyclic basis generated by $(1,1,1,1)$, which is the basis for $\psi(E_{\text{ann}})$ given by the rows of the Vandermonde matrix above. Hence $\psi(E_{\text{ann}}) \subseteq M \subseteq E_f$.

To bound the i,j,k, write $\alpha_m - \alpha_n = u_{m,n}\pi^{v_{m,n}}$ for $1 \leq m < n \leq 4$, where each $u_{m,n} \in \mathcal{O}^\times$. Since $\psi(E_{\text{ann}}) \subseteq M$ for any Λ-submodule of E_f up to isomorphism, one must be able to express the rows of the above matrix as an $\mathcal{O}$-linear combination of the generators given by the rows of G. This immediately gives $0 \leq i \leq v_{1,2}, 0 \leq j \leq v_{1,3}+v_{2,3}$, and $0 \leq k \leq v_{1,4}+v_{2,4}+v_{3,4}$, hence the parameters $a \in \mathcal{O}/(\pi^j)$, $b,c \in \mathcal{O}/(\pi^k)$ are bounded. Therefore, $\mathcal{M}_f$ is finite. As before, not all choices of i,j,k,a,b,c will yield an $\mathcal{O}$-module closed under the action of T.

To derive conditions for module closure, one can express the action of T as a matrix with respect to the free $\mathcal{O}$-module basis $g_1 = (1,1,1,1), g_2 = (0,\pi^i,a,b), g_3 = (0,0,\pi^j,c), g_4 = (0,0,0,\pi^k)$. Letting $M = \langle g_1,g_2,g_3,g_4\rangle_{\mathcal{O}}$, one has $TM \subseteq M$ if and only if the matrix representation of T has all entries in $\mathcal{O}$. Then for

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 \\ & \pi^i & a & b \\ & & \pi^j & c \\ & & & \pi^k \end{pmatrix},$$

the entries of

$$\begin{pmatrix} \alpha_1 & x_{1,2} & x_{1,3} & x_{1,4} \\ & \alpha_2 & x_{2,3} & x_{2,4} \\ & & \alpha_3 & x_{3,4} \\ & & & \alpha_4 \end{pmatrix} = GD(\alpha_1, \alpha_2, \alpha_3, \alpha_4)G^{-1}$$

must be in $\mathcal{O}$. One can easily calculate the right-hand side formally in $\mathrm{GL}_4(F)$, and the integrality conditions are summarized below.

Lemma 5.1.1. Let $u_f = \frac{u_{1,3}}{u_{1,2}}, v_f = \frac{u_{1,4}}{u_{1,2}}$, and $w_f = \frac{u_{2,4}}{u_{2,3}}$. Then $TM \subseteq M$ if and only if $0 \leq i \leq v_{1,2}$, $0 \leq j \leq v_{1,3} + v_{2,3}$, and $0 \leq k \leq v_{1,4} + v_{2,4} + v_{3,4}$, and the quantities

1. $x_{1,3} = u_f \pi^{v_{1,3}-j} - a\pi^{v_{1,2}-(i+j)}$
2. $x_{2,3} = a\pi^{v_{2,3}-j}$
3. $x_{1,4} = v_f \pi^{v_{1,4}-k} - b\pi^{v_{1,2}-(i+k)} - u_f c\pi^{v_{1,3}-(j+k)} + ac\pi^{v_{1,2}-(i+j+k)}$
4. $x_{2,4} = w_f b\pi^{v_{2,4}-k} - ac\pi^{v_{2,3}-(j+k)}$
5. $x_{3,4} = c\pi^{v_{3,4}-k}$

are in $\mathcal{O}$.

5.2 Λ-Isomorphism

For a fixed (i, j, k), one only needs to sort the classes $[i, j, k, a, b, c]$ for the allowable $a \in \mathcal{O}/(\pi^j)$ and $b, c \in \mathcal{O}/(\pi^k)$ which satisfy the module closure conditions in lemma 5.1.1. When there is a fixed (i, j, k) in mind, one can suppress i, j and k from the notation and write $[a, b, c]$ for the isomorphism

class $[i,j,k,a,b,c] \in \mathcal{M}_f$. Let

$$G(i,j,k,a,b,c) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ & \pi^i & a & b \\ & & \pi^j & c \\ & & & \pi^k \end{pmatrix}.$$

Set $G_t = G(i,j,k,a_t,b_t,c_t)$, and let M_t be generated over $\mathcal{O}$ by the rows of G_t inside E_f for $t = 1,2$.

Consider the function

$$(\mathcal{O}^\times)^4 \xrightarrow{\varphi_{1,2}} \mathrm{GL}_4(F)$$

given by

$$u \mapsto X = G_2 D(u) G_1^{-1}.$$

By theorem 2.1.2, one has a Λ-isomorphism $M_1 \to M_2$ whose matrix representation with respect to the given generators is $X = \varphi_{1,2}(u_1,u_2,u_3,u_4)$, if and only if $\mathrm{im}\varphi_{1,2} \cap \mathrm{GL}_4(\mathcal{O}) \neq \emptyset$. For this to be a useful criterion, one has to reduce this to checking whether $\varphi_{1,2}(S) \cap \mathrm{GL}_4(\mathcal{O}) \neq \emptyset$ for some finite subset $S \subset (\mathcal{O}^\times)^4$. The next result shows that this can be accomplished with S equal to the canonical lift of $((\mathcal{O}/(\pi^{i+j+k}))^\times)^4$ to $(\mathcal{O}^\times)^4$.

Theorem 5.2.1. Let $u, v \in (\mathcal{O}^\times)^4$, and suppose that $v \equiv u \bmod \pi^{i+j+k}$ and $\varphi_{1,2}(v) \in \mathrm{GL}_4(\mathcal{O})$. Then $\varphi_{1,2}(u) \in \mathrm{GL}_4(\mathcal{O})$.

Proof. Write $u = v + x\pi^{i+j+k}$ for some $x \in \mathcal{O}^4$, and observe that $\varphi_{1,2}$ (extended to F^4) is a linear map of vector spaces $F^4 \to \mathrm{Mat}_{4\times 4}(F)$. Hence $\varphi_{1,2}$ has a matrix representation, say A, and by explicit computation one can observe that the entries of this matrix are linear combinations of integral elements (the $a, b, c's$) with powers of π in the denominator. The largest power of π in the denominator is π^{i+j+k}, hence $\pi^{i+j+k}A$ has integral entries. Therefore

$\varphi_{1,2}(u) = \varphi_{1,2}(v + x\pi^{i+j+k}) = A(v + x\pi^{i+j+k}) = Av + \pi^{i+j+k}Ax$, and since Av and $\pi^{i+j+k}Ax$ have integral entries, so does $\varphi_{1,2}(u)$. Since $\varphi_{1,2}(u)$ (or anything in the image of $\varphi_{1,2}$) is upper triangular with units along the diagonal, this shows that $\varphi_{1,2}(u) \in \mathrm{GL}_4(\mathcal{O})$. $\square$

Let $\mathrm{Isom}_\Lambda(M_1, M_2)$ denote the set of Λ-isomorphisms from M_1 to M_2 as before. Then the above result shows that $\mathrm{Isom}_\Lambda(M_1, M_2)$ can be computed as

$$H + (\pi^{i+j+k})^4,$$

where $H = \{u \in S | \varphi_{1,2}(u) \in \mathrm{GL}_4(\mathcal{O})\}$ is a finite subset of S. In particular, when $M_1 = M = M_2$, then $\varphi_{1,2} = \varphi_M : \mathbb{G}_m^4(\mathcal{O}) \to \mathrm{GL}_4(F)$ is a group homomorphism. One can compute

$$\mathrm{Aut}_\Lambda(M) = \varphi_M^{-1}(\mathrm{im}\varphi_M \cap \mathrm{GL}_4(\mathcal{O})),$$

which can be represented as $H + (\pi^{i+j+k})^4$, where $H = \{u \in S | \varphi_M(u) \in \mathrm{GL}_4(\mathcal{O})\}$. The reduction of H modulo π^{i+j+k}, $\overline{H} \subseteq \mathbb{G}_m^4(\mathcal{O})/(\pi^{i+j+k})^4$ is a subgroup.

To decide when $[a_1, b_1, c_1] = [a_2, b_2, c_2]$, one can in principle test every possible $u \in S$ for whether $\varphi_{1,2}(u) \in GL_4(\mathcal{O})$. In practice, when $[a_1, b_1, c_1] = [a_2, b_2, c_2]$, an element $u \in S$ is found quickly. Unfortunately, S can be very large and if two classes are distinct, one is forced to iterate through all possibilities for u. For example, if $\mathcal{O} = \mathbb{Z}_p$ and one is sorting classes along the tuple $(i, j, k) = (1, 1, 3)$, then $S = ((\mathbb{Z}/(p^5))^\times)^4$ has order $(p-1)^4 p^{16}$. One can reduce the number of iterations by dividing nontrivial automorphisms of M_1 and M_2 from S.

More precisely, $\mathrm{Isom}_\Lambda(M_1, M_2)$ possesses an action of $\mathrm{Aut}_\Lambda(M_1)$ defined by

$$\mathrm{Aut}_\Lambda(M_1) \times \mathrm{Isom}_\Lambda(M_1, M_2) \longrightarrow \mathrm{Isom}_\Lambda(M_1, M_2)$$

$$(\varphi, \psi) \mapsto \psi \circ \varphi^{-1}.$$

This action is simply transitive since $\psi \circ \varphi^{-1} = \psi'$ if and only if $\varphi = (\psi')^{-1} \circ \psi$. Hence $\mathrm{Isom}_\Lambda(M_1, M_2)$ is a single orbit under the action of $\mathrm{Aut}_\Lambda(M_1)$. Since all possible isomorphisms are parameterized by the torus $T = \mathbb{G}_m^4(\mathcal{O})$ via theorem 2.1.2, it is natural to extend the action of $\mathrm{Aut}_\Lambda(M_1)$ to $\mathrm{im}\varphi_{1,2}$. Also, $\mathrm{Aut}_\Lambda(M_1)$ can be identified with the subgroup $H + (\pi^{i+j+k})^4$ of T, and hence acts on T via translation.

Lemma 5.2.1. The map $\varphi_{1,2} : T \to \mathrm{im}\varphi_{1,2}$ is a bijection of $\mathrm{Aut}_\Lambda(M_1)$-sets. The orbits of $\mathrm{im}\varphi_{1,2}$ under the action of $\mathrm{Aut}_\Lambda(M_1)$ are in bijective correspondence with $T/\mathrm{Aut}_\Lambda(M_1)$.

Proof. Let $\varphi(u) = G_1 D(u) G_1^{-1} \in \mathrm{Aut}_\Lambda(M_1)$, so that $u \in H \times (\pi^{i+j+k})^4$, and let $\varphi_{1,2}(v) = G_2 D(v) G_1^{-1} \in \mathrm{im}\varphi_{1,2}$. By the definition of the action of $\mathrm{Aut}_\Lambda(M_1)$ on $\mathrm{Isom}_\Lambda(M_1, M_2)$, the extension of the action to $\mathrm{im}\varphi_{1,2}$ is given by

$$\begin{aligned}(\varphi(u), \varphi_{1,2}(v)) \mapsto \varphi_{1,2}(v)\varphi(u)^{-1} &= G_2 D(v) G_1^{-1} G_1 D(u^{-1}) G_1^{-1} \\ &= G_2 D(vu^{-1}) G_1^{-1} \\ &= \varphi_{1,2}(vu^{-1}).\end{aligned}$$

This proves the result. □

One has similarly an action of $\mathrm{Aut}_\Lambda(M_2)$ on $\mathrm{Isom}_\Lambda(M_1, M_2)$, and the quotient

$$\mathrm{im}\varphi_{1,2}/\mathrm{Aut}_\Lambda(M_1)\mathrm{Aut}_\Lambda(M_2)$$

is bijective with $T/\mathrm{Aut}_\Lambda(M_1)\mathrm{Aut}_\Lambda(M_2)$, so that the size of T is reduced even further.

By the above result, if $\mathrm{Isom}_\Lambda(M_1, M_2)$ is nonempty, it will be the only orbit in $\mathrm{im}\varphi_{1,2}$ contained in $\mathrm{GL}_4(\mathcal{O})$. Therefore, one only needs to search for an element in $\mathrm{GL}_4(\mathcal{O})$ among representatives for $\mathrm{im}\varphi_{1,2}$ modulo the action of $\mathrm{Aut}_\Lambda(M_1) = H_1 + (\pi^{i+j+k})^4$ and $\mathrm{Aut}_\Lambda(M_2) = H_2 + (\pi^{i+j+k})^4$. This is equivalent to calculating representatives v for the cosets in $T/(H_1H_2 + (\pi^{i+j+k})^4)$, and checking if $\varphi_{1,2}(v) \in GL_4(\mathcal{O})$. By theorem 5.2.1, one only needs to check representatives for the cosets in $\overline{T}/\overline{H_1H_2}$ where the bar denotes reduction modulo (π^{i+j+k}). In general, one expects the quotient $\overline{T}/\overline{H_1H_2}$ to be much smaller than $\overline{T}$. For example, it is easy to observe that the diagonal elements $(u, u, u, u) \in T$ are always in the automorphism group regarded in T, hence T is reduced by at least one dimension by passage to T/H_1H_2.

5.3 An Algorithm to Enumerate $\mathcal{M}_f$

The previous section suggests the following algorithm to decide if two modules M_1 and M_2, are Λ-isomorphic. Ideally, one wants distinct representatives $u_1, u_2, \ldots u_k$ for the cosets in $\overline{T}/\overline{H_1H_2}$. Since testing whether $u \in T$ is in H_1 or H_2 is easy and fast, one can quickly find a small number of exhaustive but not necessarily distinct representatives using the following procedure. Let $g_1, \ldots, g_n$ be generators for the abelian group $\overline{T}$, and let $\phi_{M_t} : T \longrightarrow \mathrm{GL}_4(F)$ be the homomorphism $\phi_{M_t}(u) = G_t D(u) G_t^{-1}$ for $t = 1, 2$. For each generator g_i one can calculate a bound for the order of g_i in $\overline{T}/\overline{H_1H_2}$ as $k_i = \min\{k | \phi_{M_1}(g_i^k)$ or $\phi_{M_2}(g_i^k) \in GL_4(\mathcal{O})\}$. Then one has a surjection

$$\bigoplus_{i=1}^{n} \mathbb{Z}/(k_i) \longrightarrow \overline{T}/\overline{H_1H_2}$$

so that $|\overline{T}/\overline{H_1H_2}| \leq \prod_{i=1}^n k_i$. As an example, one may think of $\mathcal{O} = \mathbb{Z}_p$. In this case $\overline{T} = ((\mathbb{Z}/(p^{i+j+k}))^\times)^4$ and in practice the generators $g_1 = (r, r, r, r), g_2 = (r, r, r, 1), g_3 = (r, r, 1, 1)$, and $g_4 = (r, 1, 1, 1)$ with r a primitive root of unity modulo p^{i+j+k} seem to produce small orders k_i. One then iterates over all products $u = \prod_{i=1}^n g_i^{\beta_i}$ for $0 \leq \beta_i < k_i$ and checks if $\phi_{1,2}(u) \in \mathrm{GL}_4(\mathcal{O})$.

Algorithm to decide if $M_1 \cong M_2$:

Input: $M_t = [i, j, k, a_t, b_t, c_t]$ for $t = 1, 2$

Output: True or False

1. Set $B_t = G(i, j, k, a_t, b_t, c_t)$ for $t = 1, 2$.

2. Choose generators $g_1, \ldots, g_n$ for $\overline{T}$.

3. For each generator compute $k_i = \min\{k | \phi_{M_1}(g_i^k) \text{ or } \phi_{M_2}(g_i^k) \in GL_4(\mathcal{O})\}$. If a k_i is achieved with $\phi_{M_1}(g_i^{k_i}) \in \mathrm{GL}_4(\mathcal{O})$ but $\phi_{M_2}(g_i^{k_i}) \notin \mathrm{GL}_4(\mathcal{O})$ (or vice versa), the modules are not isomorphic by theorem 2.1.4 and output False.

4. For each product $u = \prod_{i=1}^n g_i^{\beta_i}$ where $0 \leq \beta_i < k_i$, check if $\varphi_{1,2}(u) \in \mathrm{GL}_4(\mathcal{O})$, and if so output True and break. Otherwise, output False.

5.4 Elementary Types

One can form the obvious elements of $\mathcal{M}_f$ by grouping the factors of $f(T)$ and taking direct sums. For example $\Lambda/(T-\alpha_1) \oplus \Lambda/(T-\alpha_2) \oplus \Lambda/(T-\alpha_3)(T-\alpha_4)$ injects into E canonically with finite cokernel. Let $P = \{B_k\}$ be a partition of $\{1, 2, 3, 4\}$ with blocks B_k, and associate to P the elementary type

$$E_P := \bigoplus_{B_k \in P} \Lambda / \prod_{i \in B_k} (T - \alpha_i),$$

e.g. the example above corresponds to the partition $\{\{1\}, \{2\}, \{3, 4\}\}$. Hence there are $15 = B_4$ elementary types, where B_n is the nth Bell number. The next result is well known, but the proof is given here for lack of a reference.

Theorem 5.4.1. The elementary types are distinct up to isomorphism.

Proof. Suppose $\phi : E_{P_1} \longrightarrow E_{P_2}$ is a Λ-isomorphism. In particular, it is an isomorphism of free $\mathcal{O}$-modules of rank 4 and hence has a matrix representation

in $\mathrm{GL}_4(\mathcal{O})$ with respect to bases which will be choosen now. For each block B_k, the factor $\Lambda/\prod_{i\in B_k}(T-\alpha_i)$ has $\mathcal{O}$-basis $\{1, T, T^2, \ldots, T^{|B_k|-1}\}$ by the Division algorithm for Λ. With respect to this basis, T acts as the $|B_k| \times |B_k|$ companion matrix C_{B_k}, of the polynomial $\prod_{i\in B_k}(T-\alpha_i)$. Choosing this basis for each factor of E_P and taking their union to get a basis for the whole of E_P, T is then represented as the matrix block sum $[T]_P = C_{B_1} \oplus C_{B_2} \oplus \cdots \oplus C_{B_{|P|}}$. Let $[\phi] \in GL_4(\mathcal{O})$ be the matrix representation of ϕ with respect to the power bases constructed above. The additional requirement that ϕ be a Λ-morphism implies that one must have

$$[\phi][T]_{P_1} = [T]_{P_2}[\phi],$$

which holds if and only if $[T]_{P_1} \sim_{\mathcal{O}} [T]_{P_2}$. Since the matrices $[T]_{P_1}$ and $[T]_{P_2}$ are already in rational canonical form, they must have the same block submatrices up to order. Since different blocks in a partition will yield different companion matrices, the partitions P_1 and P_2 must be equal. □

Using the results for degrees 2 and 3, one can express the elementary types in the notation $[i, j, k, a, b, c]$.

Theorem 5.4.2. The elementary types expressed in the notation $[i, j, k, a, b, c]$ are:

- $4|123 \in [v_{1,2}, v_{1,3} + v_{2,3}, 0, \frac{u_{1,3}}{u_{1,2}}\pi^{v_{1,3}}, 0, 0]$
- $4|12|3 \in [v_{1,2}, 0, 0, 0, 0, 0]$
- $4|2|13 \in [0, v_{1,3}, 0, 0, 0, 0]$
- $4|1|23 \in [0, v_{2,3}, 0, 1, 0, 0]$
- $E_f = 4|1|2|3 \in [0, 0, 0, 0, 0, 0]$

- $12|34 \in [v_{1,2}, 0, v_{3,4}, 0, 0, 1]$
- $14|23 \in [0, v_{2,3}, v_{1,4}, 1, 0, 0]$
- $14|2|3 \in [0, 0, v_{1,4}, 0, 0, 0]$
- $24|1|3 \in [0, 0, v_{2,4}, 0, 1, 0]$
- $24|13 \in [0, v_{1,3}, v_{2,4}, 0, 1, 0]$
- $34|1|2 \in [0, 0, v_{3,4}, 0, 0, 1]$
- $124|3 \in [v_{1,2}, 0, v_{1,4} + v_{2,4}, 0, \frac{u_{1,4}}{u_{1,2}}\pi^{v_{1,4}}, 0]$
- $134|2 \in [0, v_{1,3}, v_{1,4} + v_{3,4}, 0, 0, \frac{u_{1,4}}{u_{1,3}}\pi^{v_{1,4}}]$
- $234|1 \in [0, v_{2,3}, v_{2,4} + v_{3,4}, 1, 1, \frac{u_{2,4}}{u_{2,3}}\pi^{v_{2,4}}]$
- $1234 \in [v_{1,2}, v_{1,3} + v_{2,3}, v_{1,4} + v_{2,4} + v_{3,4}, u_f\pi^{v_{1,3}}, v_f\pi^{v_{1,4}}, \frac{v_f w_f}{u_f}\pi^{v_{1,4}+v_{2,4}}]$

where for all $1 \leq m < n \leq 4$, write $\alpha_m - \alpha_n = u_{m,n}\pi^{v_{m,n}}$ for $u_{m,n} \in \mathcal{O}^\times$ and $u_f = \frac{u_{1,3}}{u_{1,2}}, v_f = \frac{u_{1,4}}{u_{1,2}}, w_f = \frac{u_{2,4}}{u_{2,3}}$.

Proof. This is just an exercise in taking the canonical maps from each elementary type to E_f, and using the matrix operations used in the proof of 2.0.4 to write the image of a power basis in the form G. One can also use the expression of the degree 3 elementary types in the notation $[i, j, a]$ to help see the result. □

Chapter 6

APPLICATIONS TO THE IWASAWA THEORY OF ELLIPTIC CURVES

The results given for the case $\lambda = 2$ can be used to determine the isomorphism class of the p-Selmer group of some elliptic curves over the cyclotomic $\mathbb{Z}_p$-extension. First some main definitions and results from [3] are discussed. Several examples are given at the end to illustrate how $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ can be determined when $\mu = 0$.

6.1 Selmer Groups

Let E be an elliptic curve over $\mathbb{Q}$ with good, ordinary reduction at a prime $p \geq 3$. Let $\mathbb{Q}_\infty$ denote the cyclotomic $\mathbb{Z}_p$ extension. First, recall the definition of the p-primary Selmer group of E over $\mathbb{Q}_\infty$ as in [3]. One would like to know about $E(\mathbb{Q}_\infty)$, the points of E defined over $\mathbb{Q}_\infty$, which are contained in $E(\overline{\mathbb{Q}})$ as the points fixed under the action of $G_{\mathbb{Q}_\infty} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$. If one fixes a prime power p^k, one can consider the short exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \longrightarrow E(\overline{\mathbb{Q}})[p^k] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{[p^k]} E(\overline{\mathbb{Q}}) \longrightarrow 0\,,$$

and taking $G_{\mathbb{Q}_\infty}$-cohomology gives the (usual) long exact sequence

$$0 \longrightarrow E(\mathbb{Q}_\infty)[p^k] \longrightarrow E(\mathbb{Q}_\infty) \xrightarrow{[p^k]} E(\mathbb{Q}_\infty) \xrightarrow{\delta} H^1(\mathbb{Q}_\infty, E[p^k]) \longrightarrow \cdots .$$

The injection induced by δ, denoted by $\kappa : E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_\infty, E[p^k])$, is called the Kummer homomorphism. If $P \in E(\mathbb{Q}_\infty)$, then $\delta(P)$ is the 1-cocycle defined by $\sigma \mapsto Q^\sigma - Q$ where $Q \in E(\overline{\mathbb{Q}})$ is chosen so that $[p^k]Q = P$. One has the following lemma.

Lemma 6.1.1. Let $\frac{1}{p^k}$ denote $\frac{1}{p^k} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Then $E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) \cong E(\mathbb{Q}_\infty) \otimes \langle \frac{1}{p^k} \rangle$.

Now consider the directed system of abelian groups $\{\langle 1/p^k\rangle | k \in \mathbb{N}\}$ indexed by inclusion maps given by

$$\frac{a}{p^k} \mapsto \frac{pa}{p^{k+1}}.$$

Tensoring with $E(\mathbb{Q}_\infty)$ gives the direct system $\{E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty)\}_{k\in\mathbb{N}}$ where the maps $E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) \longrightarrow E(\mathbb{Q}_\infty)/[p^{k+1}]E(\mathbb{Q}_\infty)$ are given by $P \mapsto [p]P$. The direct limit of this system is then

$$\begin{aligned}\varinjlim E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) &= \varinjlim E(\mathbb{Q}_\infty) \otimes \langle 1/p^k\rangle \\ &= E(\mathbb{Q}_\infty) \otimes \varinjlim \langle 1/p^k\rangle \\ &= E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p).\end{aligned}$$

One also has

Lemma 6.1.2. The diagram

$$\begin{array}{ccc} E(\mathbb{Q}_\infty)/[p^{k+1}]E(\mathbb{Q}_\infty) & \xrightarrow{\kappa} & H^1(\mathbb{Q}_\infty, E[p^{k+1}]) \\ \uparrow & & \uparrow \\ E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) & \xrightarrow{\kappa} & H^1(\mathbb{Q}_\infty, E[p^k]) \end{array}$$

is commutative, and the direct limit gives an injection $E(\mathbb{Q}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa} H^1(\mathbb{Q}_\infty, E[p^\infty])$.

The p-Selmer group is defined in [3] as a certain subgroup of $H^1(\mathbb{Q}_\infty, E[p^\infty])$ containing the image of the Kummer homomorphism κ. The idea is to first realize that each global point in $E(\mathbb{Q}_\infty)$, say $P \in E(\mathbb{Q}_n)$ at some layer $\mathbb{Q}_n$ in the cyclotomic $\mathbb{Z}_p$-extension, gives rise to a local point $P \in E((\mathbb{Q}_n)_\mathfrak{p})$ for every prime $\mathfrak{p}$ of $\mathbb{Q}_n$, via a chosen embedding $\mathbb{Q}_n \to (\mathbb{Q}_n)_\mathfrak{p}$. One can say this in an equivalent way by defining $(\mathbb{Q}_\infty)_\eta$ to be the union $\bigcup_n (\mathbb{Q}_n)_{\mathfrak{p}_n}$ for the prime $\eta = \bigcup_n \mathfrak{p}_n$ of $\mathbb{Q}_\infty$. Here, the prime ideals $\mathfrak{p}_n$ are chosen so that $\mathfrak{p}_n$ is a prime ideal of the ring of integers of $\mathbb{Q}_n$ and $\mathfrak{p}_n \subset \mathfrak{p}_{n+1}$. Then each global point

$E(\mathbb{Q}_\infty)$ gives rise to a local point of $E((\mathbb{Q}_\infty)_\eta)$, and this induces a map

$$E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to E((\mathbb{Q}_\infty)_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p).$$

Now realize what this map means in terms of the Kummer embedding. For a prime η of $\mathbb{Q}_\infty$ given in terms of the primes $\mathfrak{p}_n$ as above, one has chosen embeddings $\mathbb{Q}_n \hookrightarrow (\mathbb{Q}_n)_{\mathfrak{p}_n}$, and this choice fixes an embedding $\mathbb{Q}_\infty \hookrightarrow (\mathbb{Q}_\infty)_\eta$. Let $(\ell) = \eta \cap \mathbb{Z}$ where ℓ is a prime in $\mathbb{Z}$. Since each completion $(\mathbb{Q}_n)_{\mathfrak{p}_n}$ is a finite extension of $\mathbb{Q}_\ell$, one has $(\mathbb{Q}_\infty)_\eta \subset \overline{\mathbb{Q}_\ell}$. Choose an embedding $\overline{\mathbb{Q}} \overset{\imath}{\hookrightarrow} \overline{\mathbb{Q}_\ell}$ extending the chosen embedding $\mathbb{Q}_\infty \hookrightarrow (\mathbb{Q}_\infty)_\eta$, and this choice identifies $G_{\mathbb{Q}_\ell}$ with a subgroup of $G_{\mathbb{Q}}$ which is the decomposition group for a prime $\widetilde{\eta}|\eta$ in $\overline{\mathbb{Q}}$. Define the local Kummer homomorphism

$$E((\mathbb{Q}_\infty)_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\kappa_\eta} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty]),$$

in the same way as the global Kummer homomorphism above. Since $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/(\mathbb{Q}_\infty)_\eta)$ is identified with a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$ via the decomposition group of $\widetilde{\eta}$, one has the restriction map

$$H^1(\mathbb{Q}_\infty, E[p^\infty]) \xrightarrow{\mathrm{res}} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])$$

where $E[p^\infty] \subseteq E(\overline{\mathbb{Q}}_\ell)$ via the embedding $\imath$.

Lemma 6.1.3. The diagram

$$\begin{array}{ccc} E((\mathbb{Q}_\infty)_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\kappa_\eta} & H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty]) \\ \uparrow & & \uparrow \mathrm{res} \\ E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) & \xrightarrow{\kappa} & H^1(\mathbb{Q}_\infty, E[p^\infty]) \end{array}$$

is commutative.

Proof. This is essentially a version of the diagram $(**)$ from pg. 297 of [12] for the direct limit of the maps $E(\mathbb{Q}_\infty)/[p^k]E(\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_\infty, E[p^k])$ and

$E((\mathbb{Q}_\infty)_\eta)/[p^k]E((\mathbb{Q}_\infty)_\eta) \to H^1((\mathbb{Q}_\infty)_\eta, E[p^k])$. One can see this directly as follows. Let $P \otimes r/p^k \in E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Then $\kappa(P \otimes r/p^k)$ is the class of the 1-cocycle given by $\psi \mapsto \imath(Q^\psi - Q) = \imath(Q)^\psi - \imath(Q)$ for all $\psi \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$, where $Q \in E(\overline{\mathbb{Q}})$ is chosen such that $[p^k]Q = [r]P$. The left vertical map sends $P \otimes r/p^k$ to $\imath(P) \otimes r/p^k \in E((\mathbb{Q}_\infty)_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$, and $\kappa_\eta(\imath(P) \otimes r/p^k)$ can be given as the class of the 1-cocycle $\sigma \mapsto \imath(Q)^\sigma - \imath(Q)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/(\mathbb{Q}_\infty)_\eta)$, since $[p^k]Q = [r]P$ implies that $[p^k]\imath(Q) = [r]\imath(P)$. This is exactly the restriction of the cocycle defining $\kappa(P \otimes r/p^k)$ to the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/(\mathbb{Q}_\infty)_\eta) \leq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$. □

From this diagram, one can see that for every prime η of $\mathbb{Q}_\infty$, $\mathrm{res}(\mathrm{im}\kappa) \subseteq \mathrm{im}\kappa_\eta$ and hence,

$$\mathrm{im}\kappa \subseteq \ker(H^1(\mathbb{Q}_\infty, E[p^\infty]) \longrightarrow H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/\mathrm{im}\kappa_\eta).$$

Letting η vary over all primes of $\mathbb{Q}_\infty$, one makes the following definition as in [3]:

Definition 1. The p-primary Selmer group of E over $\mathbb{Q}_\infty$ is the subgroup of $H^1(\mathbb{Q}_\infty, E[p^\infty])$ defined by

$$\mathrm{Sel}_E(\mathbb{Q}_\infty)_p = \ker(H^1(\mathbb{Q}_\infty, E[p^\infty]) \longrightarrow \prod_\eta H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/\mathrm{im}\kappa_\eta).$$

From the discussion, it is clear that $\mathrm{im}\kappa \subseteq \mathrm{Sel}_E(\mathbb{Q}_\infty)_p$. The definition of the p-Selmer group in [3] holds for any algebraic extension $K/\mathbb{Q}$. Therefore at any finite layer $\mathbb{Q}_n$, one can define $\mathrm{Sel}_E(\mathbb{Q}_n)_p$ in the same way. If $\mathfrak{p}$ is a prime of the ring of integers in $\mathbb{Q}_n$, one has the local Kummer embedding

$$\kappa_\mathfrak{p} : E((\mathbb{Q}_n)_\mathfrak{p}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1((\mathbb{Q}_n)_\mathfrak{p}, E[p^\infty]),$$

so define

$$\mathrm{Sel}_E(\mathbb{Q}_n)_p = \ker(H^1(\mathbb{Q}_n, E[p^\infty]) \longrightarrow \prod_\mathfrak{p} H^1((\mathbb{Q}_n)_\mathfrak{p}, E[p^\infty])/\mathrm{im}\kappa_\mathfrak{p}),$$

where the product runs over all primes $\mathfrak{p}$ of $\mathbb{Q}_n$. The fundamental diagram from [3], which is discussed in section 6.3, relates the Λ-modules $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ and $\mathrm{Sel}_E(\mathbb{Q}_n)_p$.

6.2 The Λ-module $X_E(\mathbb{Q}_\infty)$

The abelian group $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is p-primary, and is therefore a module over $\mathbb{Z}_p$. There is also an action of the Galois group $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ on $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ which is compatible with the Kummer embedding $\kappa : E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to \mathrm{Sel}_E(\mathbb{Q}_\infty)_p$. To see what this action should be, let $\gamma \in \Gamma$. Let $P \otimes (n/p^k) \in E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Then recall $\kappa(P \otimes (n/p^k))$ is the class of the 1-cocycle which sends $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_\infty)$ to

$$Q^\sigma - Q \in E[p^\infty],$$

where Q is a point chosen in $E(\overline{\mathbb{Q}})$ such that $[p^k]Q = [n]P$. Γ acts on $E(\mathbb{Q}_\infty) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ in the usual way

$$\gamma \cdot (P \otimes (n/p^k)) = P^\gamma \otimes (n/p^k),$$

and one expects γ to act on 1-cocycles in a way that is geometrically compatible, so that $\kappa(\gamma \cdot (P \otimes (n/p^k))) = \gamma \cdot \kappa(P \otimes (n/p^k))$. Let $\widetilde{\gamma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote any extension of the automorphism γ to $\overline{\mathbb{Q}}$. Since Q satisfies $[p^k]Q = [n]P$, applying $\widetilde{\gamma}$ to both sides of this equation shows $Q^{\widetilde{\gamma}}$ satisfies $[p^k]Q^{\widetilde{\gamma}} = [n]P^{\overline{\gamma}}$, using the fact that addition on E is defined over $\mathbb{Q}$. Hence, a 1-cohomology class associated to $P^\gamma \otimes (n/p^k)$ can be given by the 1-cocycle

$$\sigma \mapsto (Q^{\widetilde{\gamma}})^\sigma - Q^{\widetilde{\gamma}} = (Q^{\widetilde{\gamma}\sigma\widetilde{\gamma}^{-1}} - Q)^{\widetilde{\gamma}}.$$

If $[\xi] \in H^1(\mathbb{Q}_\infty, E[p^\infty])$ is a cohomology class represented by a 1-cocycle ξ, then the action of Γ on 1-cocycles should then be $(\gamma \cdot \xi)(\sigma) = \xi(\widetilde{\gamma}\sigma\widetilde{\gamma}^{-1})^{\widetilde{\gamma}}$.

Now the idea for turning $H^1(\mathbb{Q}_\infty, E[p^\infty])$ into a module over the power series ring Λ is based on the following facts. Set $A = H^1(\mathbb{Q}_\infty, E[p^\infty])$.

1. The action of Γ described above is continuous, where Γ has its usual topology and A is discrete and p-primary. This is equivalent to showing $A = \bigcup A^{\Gamma_n}$ where $\Gamma_n = \Gamma^{p^n}$.

2. Letting T act as $\gamma - 1$ where γ is a topological generator of Γ, the continuity result above implies that the action of T is topologically nilpotent, i.e. for $a \in A$, there is an $n \gg 0$ so that $T^n a = 0$. This makes the action of a power series $f(T) \in \Lambda$ well-defined.

To see the second fact, suppose $a \in A^{\Gamma_{n_0}}$, so that $(\gamma^{p^{n_0}} - 1)a = 0$. Since $\Gamma_n \subset \Gamma_{n_0}$ for $n_0 \leq n$, one has $(\gamma^{p^n} - 1)a = 0$ for $n_0 \leq n$. Also, since A is p-primary, $p^m a = 0$ for some $m \geq 0$. Expressing the action of γ in terms of T, one has $((T+1)^{p^n} - 1)a = 0$ for $n \geq n_0$. This becomes

$$T^{p^n} a + \sum_{i=1}^{p^n - 1} \binom{p^n}{i} T^i a = 0.$$

By continuity of the polynomial function $P(X) = \binom{X}{i}$ on $\mathbb{Z}_p$, one can choose n large enough so that $n \geq n_0$ and $p^m \mid \binom{p^n}{i}$ for $i = 1, 2, \ldots p^n - 1$, and hence $T^{p^n} a = 0$. A proof of the first fact is given below.

Lemma 6.2.1. The action of Γ on A is continuous.

Proof. Let $\xi : G_{\mathbb{Q}_\infty} \to E[p^\infty]$ be a continuous 1-cocycle whose class is denoted $a \in A$. For $\mathbb{Q}_n$, the nth layer in $\mathbb{Q}_\infty/\mathbb{Q}$, $G_{\mathbb{Q}_\infty} \leq G_{\mathbb{Q}_n}$, and one has the restriction map

$$H^1(\mathbb{Q}_n, E[p^\infty]) \xrightarrow{h_n} H^1(\mathbb{Q}_\infty, E[p^\infty]).$$

The first task is to show that ξ is in the image of h_n for some n. Since $G_{\mathbb{Q}_\infty}$ is compact in its profinite topology, $\xi(G_{\mathbb{Q}_\infty})$ is compact in $E[p^\infty]$, and since $E[p^\infty]$ is discrete, $\xi(G_{\mathbb{Q}_\infty})$ must be finite. This implies that ξ factors through $G_{\mathbb{Q}_\infty}/H$ for some open normal subgroup H. Let F be the fixed field of H, so

that $F/\mathbb{Q}_\infty$ is a finite Galois extension. By lemma 6 in chapter 5.4 of [11], there is a finite extension F_n of $\mathbb{Q}_n$ for some n, so that $\mathrm{Gal}(F/\mathbb{Q}_\infty)$ can be identified isomorphically with $\mathrm{Gal}(F_n/\mathbb{Q}_n)$ by restricting automorphisms of F to F_n. Then F_n corresponds to a subgroup H' of $G_{\mathbb{Q}_n}$ and one has

$$G_{\mathbb{Q}_\infty}/H \cong \mathrm{Gal}(F/\mathbb{Q}_\infty) \cong \mathrm{Gal}(F_n/\mathbb{Q}_n) \cong G_{\mathbb{Q}_n}/H'.$$

Using this isomorphism, identify ξ with a 1-cocycle on $G_{\mathbb{Q}_n}/H'$, and pre-composing with the canonical surjection $G_{\mathbb{Q}_n} \to G_{\mathbb{Q}_n}/H'$ gives a 1-cocycle, on $G_{\mathbb{Q}_n}$ lifting ξ.

The claim is that a is fixed by the subgroup Γ_n. This is just a computation. Denote the lift of ξ by $\widetilde{\xi} : G_{\mathbb{Q}_n} \to E[p^\infty]$. Let $\sigma \in G_{\mathbb{Q}_\infty}$ and let $\gamma_n \in \Gamma_n$. Since $\widetilde{\gamma_n}$ is in $G_{\mathbb{Q}_n}$

$$\begin{aligned}
\xi(\widetilde{\gamma_n}\sigma\widetilde{\gamma_n}^{-1})^{\gamma_n} &= \widetilde{\xi}(\widetilde{\gamma_n}\sigma\widetilde{\gamma_n}^{-1})^{\widetilde{\gamma_n}} \\
&= (\widetilde{\xi}(\widetilde{\gamma_n}\sigma)^{\widetilde{\gamma_n}^{-1}} + \widetilde{\xi}(\widetilde{\gamma_n}^{-1}))^{\widetilde{\gamma_n}} \\
&= \widetilde{\xi}(\widetilde{\gamma_n}\sigma) + \widetilde{\xi}(\widetilde{\gamma_n}^{-1})^{\widetilde{\gamma_n}} \\
&= \widetilde{\xi}(\widetilde{\gamma_n})^\sigma + \widetilde{\xi}(\sigma) - \widetilde{\xi}(\widetilde{\gamma_n}) \\
&= \xi(\sigma) + \{1 - \text{coboundary}\}.
\end{aligned}$$

Hence $\gamma_n \cdot \xi$ is cohomologous to ξ and therefore $\gamma_n \cdot a = a$. □

The following definition is from [3].

Definition 2. Set $X_E(\mathbb{Q}_\infty) = \mathrm{Hom}_{cts}(\mathrm{Sel}_E(\mathbb{Q}_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$, the Pontryagin dual of the p-primary Selmer group of E over $\mathbb{Q}_\infty$.

The action of Λ on $X_E(\mathbb{Q}_\infty)$ is given in the usual way. More generally, if A is a discrete p-primary or compact pro-p abelian group with a continuous action of Γ, then for $f : A \to \mathbb{Q}_p/\mathbb{Z}_p$ in $\widehat{A}$, γf is defined by $(\gamma f)(a) = f(\gamma^{-1}a)$.

6.3 Some Known Results on $X_E(\mathbb{Q}_\infty)$

For ease of notation, set $X = X_E(\mathbb{Q}_\infty)$. Since X is a module over $\Lambda = \mathbb{Z}_p[[T]]$, one can ask whether it is finitely generated over Λ and whether it is Λ-torsion. One can also ask what these conditions imply for the sequence of curves $E(\mathbb{Q}_n)$. It is well known that X is always finitely generated over Λ, and the proof involves the usual Mordell Weil theorem combined with Nakayama's lemma (see [3]). By Kato's theorem [5], X is also Λ-torsion. Even though only the case where p is a good ordinary prime for $E/\mathbb{Q}$ is considered, Kato's result holds for E/F where F is a number field, and the primes above p in F are of good ordinary, or multiplicative type for E. One can now apply the structure theorem for Λ-modules. There is a short exact sequence of Λ-modules

$$0 \longrightarrow K \longrightarrow X \longrightarrow \bigoplus_i \Lambda/(f_i(T)^{e_i}) \longrightarrow C \longrightarrow 0,$$

with $|K|, |C| < \infty$, and each $f_i(T) \in \Lambda$ is either p or a distinguished irreducible polynomial. The characteristic polynomial of X is $f_X(T) = \mathrm{char}_\Lambda(X) = \prod f_i(T)^{e_i}$, which one can write as $p^\mu P(T)$, where $P(T)$ is a distinguished polynomial. Call the degree of $P(T)$ the λ-invariant of X, and denote it λ_X. Similarly, $\mu = \mu_X$ is called the μ-invariant. Even though the example given later only concerns the case $\mu = 0$, many examples are given in [3] where $\mu > 0$. The Main Conjecture of Iwasawa theory for elliptic curves relates $f_X(T)$ to the p-adic L-series of E, $L_p(E,T) \in \mathcal{O}[[T]]$ for a finite extension of $\mathcal{O}$ of $\mathbb{Z}_p$. The Main Conjecture of Iwasawa theory says that up to a unit multiple in $\mathcal{O}[[T]]$, f_X is equal to $L_p(E,T)$. In [17], it is shown that $L_p(E,T) \in \mathbb{Z}_p[[T]]$, and one can compute $L_p(E,T)$ and factor it into a unit power series and a distinguished polynomial $P(T)$, as in the example given in section 1.1. Hence, the Main Conjecture implies that f_X can be calculated explicitly as $P(T)$.

Theorem 1.9 in [3] implies that when X is Λ-torsion, the sequence of

ranks rank$E(\mathbb{Q}_n)$ is bounded by λ_X. The proof is recalled here because it uses ideas frequently encountered in Iwasawa theory. By the Mordell-Weil theorem, $E(\mathbb{Q}_n) \cong \mathbb{Z}^{r_n} \oplus T_n$ as abelian groups, where r_n is the rank and T_n is the finite torsion subgroup. Recall that one has the short exact sequence

$$0 \longrightarrow E(\mathbb{Q}_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \mathrm{Sel}_E(\mathbb{Q}_n)_p \longrightarrow Ш_E(\mathbb{Q}_n)_p \longrightarrow 0.$$

One loses the finite torsion part in this sequence since

$$E(\mathbb{Q}_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Z}^{r_n} \oplus T_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_n},$$

but the p-primary abelian group $\mathrm{Sel}_E(\mathbb{Q}_n)_p$ contains the copy of $(\mathbb{Q}_p/\mathbb{Z}_p)^{r_n}$. By a well-known conjecture for elliptic curves, one expects $Ш_E(\mathbb{Q}_n)_p$ to be finite, and this will be assumed from now on. Taking the dual of the short exact sequence then gives

$$0 \longrightarrow \widehat{Ш}_E(\mathbb{Q}_n)_p \longrightarrow X_E(\mathbb{Q}_n) \longrightarrow \mathbb{Z}_p^{r_n} \longrightarrow 0$$

where $X_E(\mathbb{Q}_n) := \widehat{\mathrm{Sel}_E(\mathbb{Q}_n)_p}$. Since finite groups are self dual, $\widehat{Ш}_E(\mathbb{Q}_n)_p \cong Ш_E(\mathbb{Q}_n)_p$, and is hence finite. Therefore one has $r_n = \mathrm{rank}_{\mathbb{Z}_p} X_E(\mathbb{Q}_n)$. In other words, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_E(\mathbb{Q}_n)_p$ is r_n, the rank of the elliptic curve $E(\mathbb{Q}_n)$. The next step is to relate X, which is defined over $\mathbb{Q}_\infty$, to $X_E(\mathbb{Q}_n)$.

The Fundamental Diagram

The crucial ingredient for relating X to the "finite levels" $X_E(\mathbb{Q}_n)$ is Mazur's Control Theorem [9]. Recall that $\Gamma_n = \Gamma^{p^n}$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)$. The restriction map $H^1(\mathbb{Q}_n, E[p^\infty]) \to H^1(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n}$ induces the map

$$\mathrm{Sel}_E(\mathbb{Q}_n)_p \xrightarrow{s_n} \mathrm{Sel}_E(\mathbb{Q}_\infty)_p^{\Gamma_n}.$$

The Control theorem asserts that $\ker(s_n)$ and $\mathrm{coker}(s_n)$ are finite with bounded order as $n \to \infty$. Then taking the Pontryagin dual of the sequence

$$0 \to \ker(s_n) \to \mathrm{Sel}_E(\mathbb{Q}_n)_p \to \mathrm{Sel}_E(\mathbb{Q}_\infty)_p^{\Gamma_n} \to \mathrm{coker}(s_n) \to 0$$

gives

$$0 \to \widehat{\mathrm{coker}(s_n)} \to X/(\omega_n(T))X \xrightarrow{\widehat{s_n}} X_E(\mathbb{Q}_n) \to \widehat{\ker(s_n)} \to 0$$

where $\omega_n(T) = (1+T)^{p^n} - 1$. Since the kernel and cokernel in this sequence are finite, one obtains

$$\mathrm{rank}_{\mathbb{Z}_p} X/(\omega_n(T))X = \mathrm{rank}_{\mathbb{Z}_p} X_E(\mathbb{Q}_n) = r_n.$$

Now using the structure theorem for finitely generated Λ-modules, X is pseudo-isomorphic to $\Lambda/(f(T))$ where $\mathrm{char}_\Lambda(X)$ has degree λ_X, hence X has $\mathbb{Z}_p$-rank λ_X, and therefore $r_n \leq \lambda_X$. Therefore the ranks of the elliptic curves $E(\mathbb{Q}_n)$ are bounded by λ_X, which is the result from theorem 1.9 in [3]. One sets $\lambda^{M-W} = \max\{r_n\}_{n=0}^{\infty} \leq \lambda_X$, which is equal to the rank of $E(\mathbb{Q}_\infty)$. In [3], a proof of the Control theorem is given which is based on the fundamental diagram which is recalled below. This diagram will be the basis of the technique for determining X up to isomorphism.

Fix a level n in the $\mathbb{Z}_p$-tower, and recall that the p-Selmer group is the kernel of $H^1(\mathbb{Q}_n, E[p^\infty]) \to \prod_{\mathfrak{p}} H^1((\mathbb{Q}_n)_{\mathfrak{p}}, E[p^\infty])/\mathrm{im}(\kappa_{\mathfrak{p}})$. The image of this map is denoted $\mathcal{G}_E(\mathbb{Q}_n)$ so one has the short exact sequence

$$0 \to \mathrm{Sel}_E(\mathbb{Q}_n)_p \to H^1(\mathbb{Q}_n, E[p^\infty]) \to \mathcal{G}_E(\mathbb{Q}_n) \to 0.$$

One similarly has

$$0 \to \mathrm{Sel}_E(\mathbb{Q}_\infty)_p \to H^1(\mathbb{Q}_\infty, E[p^\infty]) \to \mathcal{G}_E(\mathbb{Q}_\infty) \to 0.$$

Taking Γ_n-invariants of the latter and connecting them with the vertical restrictions maps gives

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}_E(\mathbb{Q}_n)_p & \longrightarrow & H^1(\mathbb{Q}_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E(\mathbb{Q}_n) & \longrightarrow & 0\,. \\
 & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\
0 & \longrightarrow & \mathrm{Sel}_E(\mathbb{Q}_\infty)_p^{\Gamma_n} & \longrightarrow & H^1(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E(\mathbb{Q}_\infty)^{\Gamma_n} & &
\end{array}$$

By the Snake lemma,

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

Some facts about these kernels and cokernels proven in [3] will be useful later on, and based on these facts some key assumptions will be made. For the applications later, one can restrict to the level $n = 0$. First, lemmas 3.1 and 3.2 in [3] imply that

1. $|\ker(h_n)| = |E(\mathbb{Q}_n)_p|$ and
2. $\operatorname{coker}(h_n) = 0$ for all n.

Our first assumption is that $E(\mathbb{Q})_p = 0$, so that at level 0 one has $\ker(h_0) = 0$ and hence $\ker(s_0) = 0$. Substituting this into the Snake lemma long exact sequence gives

$$\ker(g_0) \cong \operatorname{coker}(s_0).$$

Next one needs that $\mathrm{Sel}_E(\mathbb{Q})_p = 0$. This combined with the fact that $\ker(s_0) = 0$ gives

$$\ker(g_0) \cong \mathrm{Sel}_E(\mathbb{Q}_\infty)_p^\Gamma,$$

and hence

$$\widehat{\ker(g_0)} \cong \widehat{\mathrm{Sel}_E(\mathbb{Q}_\infty)_p^\Gamma} \cong X/(\omega_0(T))X = X/TX.$$

If one knows $\ker(g_0)$ for the curve E and prime p, and all possibilities for the Λ-module structure of X, then X can be determined by comparing $\ker(g_0)$ to each possible quotient X/TX. To apply the module theory developed so far, a condition is needed on the elliptic curve E to guarantee that X has no nontrivial finite Λ-submodules. By proposition 4.8 in [3], this is guaranteed by the assumptions that $E(\mathbb{Q})_p = 0$ and $\mathrm{Sel}_E(\mathbb{Q})_p = 0$.

Computing the local kernels

The focus in this section will be to show how to calculate $\ker(g_0)$ based on the facts discussed in section 3 of [3]. By definition

$$\mathcal{G}_E(\mathbb{Q}) = \mathrm{im}(H^1(\mathbb{Q}, E[p^\infty]) \longrightarrow \prod_\ell H^1(\mathbb{Q}_\ell, E[p^\infty])/\mathrm{im}(\kappa_\ell))$$

where the product runs over all primes ℓ in $\mathbb{Z}$. Note that one can ignore the image of κ_ℓ when $\ell \neq p$ since the theory of the formal group gives $E(\mathbb{Q}_\ell) \cong \mathbb{Z}_\ell \times T$ where T is the finite torsion part, and hence $E(\mathbb{Q}_\ell) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. One can define the map g_0 on a single local factor in the above product as follows. If η is any prime of $\mathbb{Q}_\infty$ dividing ℓ, then the restriction map $H^1(\mathbb{Q}_\ell, E[p^\infty]) \to H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])$ induces a map

$$H^1(\mathbb{Q}_\ell, E[p^\infty])/\mathrm{im}(\kappa_\ell) \xrightarrow{r_\ell} \prod_{\eta|\ell} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/\mathrm{im}(\kappa_\eta),$$

which is well-defined since the Kummer embedding commutes with the restriction map. The map g_0 is then given by $\prod_\ell r_\ell$. To see that this map is defined from $\mathcal{G}_E(\mathbb{Q})$ to $\mathcal{G}_E(\mathbb{Q}_\infty)$, one only needs to observe that the diagram

$$\begin{array}{ccc} H^1(\mathbb{Q}, E) & \longrightarrow & \prod_\ell H^1(\mathbb{Q}_\ell, E) \\ \downarrow & & \downarrow \\ H^1(\mathbb{Q}_\infty, E) & \longrightarrow & \prod_\eta H^1((\mathbb{Q}_\infty)_\eta, E) \end{array}$$

consisting of restriction maps throughout, is commutative. To simplify the map r_ℓ, one observes that all primes η of $\mathbb{Q}_\infty$ lying over a fixed ℓ are Galois conjugate due to a basic fact from algebraic number theory. This implies that the subgroups $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/(\mathbb{Q}_\infty)_\eta)$ are all conjugate, and a fact from group cohomology ([12] Ex. B.6) extended to continuous cohomology of profinite groups shows that the restriction maps to conjugate subgroups have the same kernel. Hence, for the purpose of calculating $\ker(g_0)$, one may choose a prime

η above ℓ and assume

$$r_\ell : H^1(\mathbb{Q}_\ell, E[p^\infty])/\mathrm{im}(\kappa_\ell) \to H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/\mathrm{im}(\kappa_\eta).$$

Then $\ker(g_0) = \prod_\ell \ker(r_\ell) \cap \mathcal{G}_E(\mathbb{Q})$.

For $E/\mathbb{Q}$, set $\Sigma = \{\ell | \ell \mid \Delta\} \cup \{p\}$, the set of primes where E has bad reduction along with p. By lemma 3.3 in [3], $\ker(r_\ell) = 0$ for $\ell \notin \Sigma$, therefore $\ker(g_0) = \prod_{\ell \in \Sigma} \ker(r_\ell) \cap \mathcal{G}_E(\mathbb{Q})$ and one has only a finite number of local kernels to compute. It also turns out that under the assumption that $E(\mathbb{Q})_p = 0$, a theorem of Cassels implies that intersecting with the global 1-cocycles $\mathcal{G}_E(\mathbb{Q})$ is unnecessary (see pg. 87 in [3]). Hence $\ker(g_0) = \prod_{\ell \in \Sigma} \ker(r_\ell)$. Now the focus will be on determining the algebraic structure of $\ker(r_\ell)$ for each type of prime $\ell \in \Sigma$. In [3], Greenberg proves Mazur's control theorem by showing that each one of these local kernels is finite.

If ℓ is a prime of bad reduction, let c_ℓ denote the Tamagawa number of $E(\mathbb{Q})$ at ℓ. This is the order of the group $E(\mathbb{Q}_\ell)/E^0(\mathbb{Q}_\ell)$ where $E^0(\mathbb{Q}_\ell)$ is the subgroup of local points which reduce to nonsingular points modulo ℓ. By the discussion on pg. 74 in [3], $\ker r_\ell$ is a cyclic group of order $c_\ell^{(p)}$, the exact power of p dividing c_ℓ.

For the good ordinary prime p, lemma 3.4 in [3] implies that $|\ker r_p| = |\widetilde{E}(\mathbb{F}_p)_p|^2$, the order of the p-torsion in the reduction $\widetilde{E}(\mathbb{F}_p)$ squared, but does not give its structure as a finite abelian group. If $\widetilde{E}(\mathbb{F}_p)_p \neq 0$, p is said to be anomalous for E. For p anomalous, the result is that

Theorem 6.3.1 (Lemma 6.3(b) in [7]). $\ker r_p \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

The proof given below is in [7], where slightly more is proved. One essentially needs to know the structure of $E(\mathbb{Q}_p)$ modulo the subgroup of points which are norms from above in the local $\mathbb{Z}_p$-extension $(\mathbb{Q}_\infty)_\eta/\mathbb{Q}_p$, which turns

out to be dual to $\ker r_p$. [7] cites the proof of the structure of this group from [9] which uses the machinery of pro-algebraic groups. The paper [6] cited in the proof below gives a more accessible proof of this result which uses Tate cohomology and formal groups.

Proof. By Tate local duality [15], there is a non-degenerate perfect pairing

$$E(\mathbb{Q}_p) \times H^1(\mathbb{Q}_p, E) \to \mathbb{Q}/\mathbb{Z}.$$

Taking the discrete p-primary part on the right gives

$$E(\mathbb{Q}_p) \times H^1(\mathbb{Q}_p, E)(p) \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Also, for a finite extension $L/\mathbb{Q}_p$, the kernel of restriction $H^1(\mathbb{Q}_p, E) \stackrel{r_L}{\to} H^1(L, E)$ is dual under the above pairing to the image of the norm map $E(L) \stackrel{N_L}{\to} E(\mathbb{Q}_p)$, and hence $\widehat{\ker r_L} \cong E(\mathbb{Q}_p)/N_L(E(L))$. Letting L range over the intermediate subfields $(\mathbb{Q}_n)_{\mathfrak{p}}$ in $(\mathbb{Q}_\infty)_\eta$, one can identify $\widehat{\ker r_p}$ with $E(\mathbb{Q}_p)/\mathcal{N}$ where $\mathcal{N}$ denotes the subgroup of universal norms

$$\mathcal{N} = \bigcap_{L=(\mathbb{Q}_n)_{\mathfrak{p}}} N_L(E(L))$$

from above in the $\mathbb{Z}_p$-extension $(\mathbb{Q}_\infty)_\eta/\mathbb{Q}_p$. The Kummer sequence for $E(\overline{\mathbb{Q}}_p)$ implies that

$$H_1(\mathbb{Q}_p, E[p^\infty])/\mathrm{im}\kappa_p \cong H^1(\mathbb{Q}_p, E)(p),$$

and similarly

$$H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])/\mathrm{im}\kappa_\eta \cong H^1((\mathbb{Q}_\infty)_\eta, E)(p),$$

hence $\widehat{\ker r_p} \cong E(\mathbb{Q}_p)/\mathcal{N}$.

By proposition 4.42 in [9], the structure of $E(\mathbb{Q}_p)/\mathcal{N}$ is given by the split exact sequence

$$0 \longrightarrow \mathbb{Z}_p/(1-u)\mathbb{Z}_p \longrightarrow E(\mathbb{Q}_p)/\mathcal{N} \longrightarrow \widetilde{E}(\mathbb{F}_p)_p \longrightarrow 0,$$

where u is the unit root of the characteristic polynomial of Frobenius $h(x) = x^2 - a_p x + p$. Writing $h(x) = (x-u)(x-p/u)$, one has $h(1) = |\widetilde{E}(\mathbb{F}_p)| = (1-u)(1-p/u)$. Since p is anomalous, $h(1) = p$ for $p > 5$ by the Hasse bound ([12] pg. 131), but for $p = 3, 5$ one has $h(1) = 6, 10$ respectively. In any event, $\mathrm{ord}_p(1-u) = 1$. From [6] which gives a different proof of the above short exact sequence, u acts on $\mathbb{Z}_p$ by multiplication, and since $\widetilde{E}(\mathbb{F}_p)_p$ is cyclic of order p, one concludes that $E(\mathbb{Q}_p)/\mathcal{N} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. □

6.4 Examples

One can now apply the results from chapter 3 to determine the isomorphism class of X. By the Main Conjecture of Iwasawa theory, one expects the characteristic polynomial $f_X(T)$ to be equal up to a unit to the p-adic L-series of E, $L_p(E,T) \in \mathbb{Z}_p[[T]]$. The p-adic L-series for E can be computed using SAGE [10] up to any desired precision modulo $\mathfrak{m} = (p, T)$. Assuming the Main Conjecture, the Weierstrauss preparation theorem gives $L_p(E,T) = f_X(T)U(T)$ for a unit $U(T) \in \Lambda$, and by the explicit version of the Weierstrauss preparation theorem 1.1.3, one can find $f_X(T)$ up to any desired precision by factoring the truncated output $L_p(E,T)$ mod $\mathfrak{m}^k$. The examples given below are for $\lambda = 2, \lambda^{M-W} = 0$, and $\mu = 0$.

$$y^2 + xy = x^3 - 2x - 5$$

Let E be the elliptic curve $y^2+xy = x^3-2x-5$, which is the curve 869c1 from Cremona's tables [2]. E has good ordinary reduction at 3. The Tamagawa numbers are $c_{11} = 2, c_{79} = 1$, with E having split multiplicative reduction at 11, and non-split multiplicative reduction at 79. Since $E(\mathbb{Q})_3 = 0$, X has no nontrivial finite Λ-submodules. The rank is 0, but the torsion subgroup is cyclic of order 2 generated by the point $(2, -1)$. The curve reduced mod 3 is $\widetilde{E} : y^2+xy = x^3+x+1$ with $\widetilde{E}(\mathbb{F}_3)_3$ consisting of the 3 points $\infty, (0,1), (0,2)$, hence 3 is an anomalous prime. By prop 5.3 (ii) in [3], $\mathrm{Sel}_E(\mathbb{Q}_\infty)_3$ is infinite.

One computes the 3-adic L-series mod $(3,T)^4$ as

$$L_3(E,T) \equiv (T-\alpha)(T-\beta)$$

where $\alpha \equiv 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + O(3^4)$ and $\beta = 3 + 3^2 + 3^3 + O(3^4)$, and by the Main Conjecture

$$X \hookrightarrow \Lambda/(T-\alpha) \oplus \Lambda/(T-\beta)$$

with finite cokernel. Since the discriminant of $(T-\alpha)(T-\beta)$ has 3-adic order 2, the degree 2 results from chapter 3 give two possibilities for X up to Λ-isomorphism: $X \in [N_0]$ or $X \in [N_1]$ where

$$N_0 = \langle (1,1), (0,1) \rangle$$

$$N_1 = \langle (1,1), (0,3) \rangle.$$

To decide which module X is isomorphic to, one calculates the abelian p-group structure of the quotients $N_i/\omega_n(T)N_i$, which just involves linear algebra. These turn out to be

$$N_1/TN_1 \cong \mathbb{Z}/9\mathbb{Z},$$

$$N_0/TN_0 \equiv \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Then $N_i \cong X$ implies that

$$N_i/\omega_n(T)N_i \cong X/\omega_n(T)X \cong \mathrm{Sel}_E(\mathbb{Q}_\infty)_3^{\Gamma_n}$$

by Pontryagin duality (here one is using the fact that the dual of a finite abelian p-group is itself). Using Cremona's tables, one can verify that $\mathrm{Sel}_E(\mathbb{Q})_3 = 0$, so at level 0 $\ker g_0 \cong \mathrm{coker} s_0 = \mathrm{Sel}_E(\mathbb{Q}_\infty)_3^\Gamma$. Since p is anomalous and the Tamagawa numbers are prime to p, $\ker g_0 \cong \ker r_3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ by section 6.3. Hence $X/TX \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, and one concludes that $X \cong N_0 \cong E_f$.

$$y^2 = x^3 + x^2 - 16x - 32$$

This is the curve 104a1 from Cremona's tables . One has $\Delta = -2^{11}13$ with Tamagawa numbers $c_2 = 1, c_{13} = 1$. The Weierstrauss factorization of the 3-adic L-series is $L_3(E,T) = f(T)U(T)$ with

$$f(T) = T^2 + (3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots)T + (3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 \cdots),$$

which is irreducible with discriminant $2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + \cdots$. Hence

$$\mathcal{M}_f = \{N_k = \langle T + b/2, 3^k \rangle_{\mathbb{Z}_p} | k = 0, 1\},$$

by theorem 3.0.6 where b is the linear coefficient of f. The quotients at level 0 are $N_0/TN_0 \cong \mathbb{Z}/9\mathbb{Z}$ and $N_1/TN_1 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. As in the last example, 3 is an anomalous prime for E, hence $\ker g_0 \cong \ker r_3 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Since $\mathrm{Sel}_E(\mathbb{Q})_3 = 0$, one has $X/TX \cong \ker g_0$, hence $X \cong N_1$.

$$y^2 = x^3 - x^2 - 12x - 40$$

This is $E = 212b1$ from Cremona's tables. One has $\Delta = -2^8 53^2$, with Tamagawa numbers $c_2 = 3, c_{53} = 2$. The prime $p = 3$ is not anomalous for E. The Weierstrauss Factorization is $L_3(E,T) = U(T)f(T)$ with

$$f(T) = T^2 + (2 \cdot 3 + 3^3 + O(3^5))T + (2 \cdot 3 + 3^3 + O(3^5)$$

with $\mathrm{ord}_3(disc(f)) = 1$. Hence $\mathcal{M}_f$ consists of the single class given by $\Lambda/(f(T))$, and $X \cong \Lambda/(f(T))$. Note that in this example, if one just assumes $\mathrm{Sel}_E(\mathbb{Q})_3$ is finite, the Euler characteristic result (theorem 4.1 in [3]) gives

$$\frac{|\mathrm{Sel}_E(\mathbb{Q}_\infty)_3^\Gamma|}{|\mathrm{Sel}_E(\mathbb{Q})_3|} = 3.$$

Since the top is already 3 by our result, $\mathrm{Sel}_E(\mathbb{Q})_3$ is forced to be trivial.

[1] J. Coates, R. Greenberg, Kummer theory for abelian varieties over local fields, Invent. Math. 124 (1996), 129–174

[2] J. Cremona, Algorithms for Modular Elliptic Curves. second ed., Cambridge University Press (1997)

[3] R. Greenberg, Iwasawa Theory for Elliptic Curves, Lecture Notes in Math., 1716 (1999), 51–144

[4] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959), 183–226

[5] Kato, Kazuya, p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmétiques. III Astérisque 295. Société Mathématique de France, Paris (2004)

[6] J. Lubin, M. Rosen, The Norm Map for Ordinary Abelian Varieties, J. Algebra 52 (1978), 236-240

[7] J. Manin, Cyclotomic fields and modular curves, Russ Math Surv. 26 (6) (1971), 7–78

[8] Koike, Masanobu, On the Isomorphism Classes of Iwasawa Modules Associated to Imaginary Quadratic Fields with $\lambda = 2$, J. Math. Sci. Univ. Tokyo 6 (1999), 371–396

[9] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972), 183–266

[10] SAGE, SAGE Mathematical Software, Version 4.6.1, http://www.sagemath.org

[11] J. P. Serre, Local Fields, Graduate Texts in Math. 67, Springer-Verlag (1979)

[12] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math. 106, Springer-Verlag 1986

[13] H. Sumida, Greenberg's conjecture and the Iwasawa polynomial, J. Math. Soc. Japan 49 (1997), 689–711

[14] H. Sumida, Isomorphism Classes and Adjoints of Certain Iwasawa Modules, Abh. Math. Sem. Univ. Hamburg 70 (2000), 113–117

[15] J. Tate, WC-groups over p-adic fields, Séminaire N. Bourbaki, exp. 156 (1956-1958), 265–277

[16] L. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Math. 83, Springer-Verlag 1982

[17] C. Wuthrich, Extending Kato's results to elliptic curves with p-isogenies, Math. Res. Lett. 13 (2006), no. 5, 713–718

BIOGRAPHICAL SKETCH

Chase Franks is from the seaside town of Corpus Christi, Texas. He holds a Bachelor of Science in Applied Mathematical Sciences from Texas A&M University, and a Master of Arts in Mathematics from the University of Oklahoma. He lives with his wife Nina, and two dogs Molly, a.k.a "the Jack Rat", and chihuahua Reese.