Università
di Genova

Ph.D. in Mathematics and Applications

XXXVI Cycle

Quaternionic Kolyvagin systems and Iwasawa theory for Hida families

Candidate:
Francesco Zerman

Supervisor:
Prof. Stefano Vigni

Academic Year 2023-2024

Abstract

In this thesis we build a Kolyvagin system for the Galois representation attached to a Hida family of modular forms, starting from the big Heegner point Euler system of Longo and Vigni built in [LV11] in towers of Shimura curves. We generalize the work of [Büy14] to a quaternionic setting, relaxing the classical *Heegner hypothesis* on the tame conductor of the family. As a byproduct of this construction, we give a proof of one divisibility of the anticyclotomic Iwasawa main conjecture for Hida families.

Contents

Introduction

Motivation

In his seminal series of papers [Kol88], [KL89] and [Kol90], Kolyvagin introduced a new method to approach the study of the Birch and Swinnerton-Dyer conjecture. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E without complex multiplication and K be an imaginary quadratic field of discriminant D_K that satisfies the *strong Heegner hypothesis*, meaning that every prime dividing N_E is split in K. Fix also an odd prime $p \nmid D_K N_E$, denote by $E[p]$ the group of p-torsion points of E and by $G_{\mathbb{Q}}$ the absolute Galois group of $\mathbb{Q}$. Under the hypothesis that the representation $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is surjective, Kolyvagin was able to find an infinite set of points y_n in E that satisfy some remarkable properties. These points are the images of some *Heegner points* on the modular curve $X_0(N_E)$ via a modular parametrization and are indexed in a set $\mathcal{N}$ of squarefree products of primes of $\mathbb{Q}$ inert in K not dividing $pD_K N_E$. Each y_n turns out to be rational over the ring class field H_n of K of conductor n. Kolyvagin proves that this set of points satisfies the following compatibility properties. For every prime $\ell \in \mathcal{N}$ and every $n \in \mathcal{N}$ such that $\ell \nmid n$, we fix a compatible set of primes $\mathfrak{l}_n$ of H_n that lie above ℓ. Then the set of points $\{y_n\}_{n\in\mathcal{N}}$ satisfies the following

(E1) $\mathrm{Tr}_{H_{n\ell}/H_n} y_{n\ell} = a_\ell y_n$, where $\mathrm{Tr}_{H_{n\ell}/H_n}$ is the trace of $\mathrm{Gal}(H_{n\ell}/H_n)$ and $\ell + 1 - a_\ell$ is the number of $\mathbb{F}_\ell$-rational points of the reduction $\tilde{E}/\mathbb{F}_\ell$ of E at ℓ;

(E2) $y_{n\ell} \equiv \mathrm{Fr}_{\mathfrak{l}_n} y_n \pmod{\mathfrak{l}_{n\ell}}$, where $\mathrm{Fr}_{\mathfrak{l}_n}$ is the arithmetic Frobenius at $\mathfrak{l}_n$;

(E3) $cy_n = \varepsilon\, \sigma(y_n)$ in $E(H_n) \otimes_{\mathbb{Z}} \mathbb{Q}$ for some $\varepsilon \in \{\pm 1\}$ and $\sigma \in \mathrm{Gal}(H_n/K)$, where c is the complex conjugation.

The key point of the work of Kolyvagin was to send these points into the cohomology over K of the p-torsion points of E via the Kummer map and to modify them by applying a suitable *derivative operator* D_n. The rigid properties of this new set of cohomology classes are the key ingredient for the proof of the following theorem, that is one of the main consequences of Kolyvagin's work (see [Kol90, Theorem A]).

Theorem (Kolyvagin). *Assume that the point* $\mathrm{Tr}_{H_1/K} y_1$ *has infinite order in* $E(K)$. *Then the group* $E(K)$ *has rank* 1 *and the Shafarevich–Tate group* $Ш(E/K)$ *is finite.*

As explained in the expository article [Gro91], the main step in the proof of this theorem is to show that the rank of the p-Selmer group of E over K is 1. This result, together with the famous Gross–Zagier limit formula [GZ86, §I, (6.5)], led to a proof of the Birch and Swinnerton-Dyer conjecture for elliptic curves of *analytic rank* 0 and 1.

The idea of building compatible systems of cohomology classes *à la Kolyvagin* has been generalized to Galois representations other than elliptic curves since the early '90s. One important step in this direction is the work [Nek92] of Nekovář, where he makes use of *Heegner cycles* in order to produce a compatible system of classes in the cohomology of the Galois representation attached to an even-weight cusp form. Similarly to the elliptic curves context, he was able to find bounds for the rank of the relevant Selmer group attached to the representation.

At the beginning of the new millennium, the incredible fertility of Kolyvagin's approach led to an axiomatization of the concepts of *Euler systems* and *Kolyvagin systems*. A system of cohomology classes for a Galois representation is called an Euler system if it satisfies a suitable generalization of the properties (E1), (E2) and (E3) above. The concept of Kolyvagin system, instead, was born to axiomatize the propery of Kolyvagin's cohomology classes that arise *after* the application of Kolyvagin's descent. Although the concept of Euler system has not been totally settled in literature (notwithstanding the seminal work [Rub00]), the theory of Kolyvagin systems was defined for a very general family of Galois representations thanks to the work of Mazur and Rubin in [MR04]. In the same year, Howard [How04b] showed that the set of cohomology classes built by Kolyvagin for elliptic curves is indeed a Kolyvagin system, in this new axiomatic language.

The existence of a Kolyvagin system for a Galois representation has many important consequences (for example, it can be used to deduce information on the rank of Selmer groups), but in this thesis we will mainly focus on its applications in anticyclotomic Iwasawa theory, in a sense that will soon be explained. Indeed, the core of our work is about building a Kolyvagin system for the anticyclotomic twist of the Galois representation attached to a Hida family of modular forms, starting from the Euler system of big Heegner classes of [LV11]. In Chapter 6 we explain how the existence of such a Kolyvagin system yields to a proof of one divisibility of the Iwasawa main conjecture. Let us get deeper in the subject and explain more precisely the content of this thesis.

Hida theory

Fix a positive squarefree integer N and a prime $p \nmid 6N\varphi(N)$, where φ is Euler's totient function. Fix once and for all embeddings of algebraic closures $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, $\mathbb{Q} \hookrightarrow \mathbb{C}$. If μ_{p-1} is the group of $p-1$-th roots of unity, denote by $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ the Teichmüller character, which we view also as a Dirichlet character modulo Np. Let

$$f(q) = \sum_{n=1}^{\infty} a_n(f) q^n \in S_k(\Gamma_0(Np); \omega^j)$$

be a normalized eigenform (for all Hecke operators T_ℓ for $\ell \nmid Np$ and U_ℓ for $\ell \mid Np$) of weight $k \geq 2$ and $j \equiv k \pmod 2$. Fix a finite extension $F/\mathbb{Q}_p$ which contains all Fourier coefficients of f and call $\mathcal{O}_F$ its ring of integers. Assume also that f is an ordinary p-stabilized newform, in the sense that $a_p \in \mathcal{O}_F^\times$ and the conductor of f is divisible by N (see §3.2.1). Call

$$\rho_f : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(F)$$

the Galois representation attached to f by Deligne, where the arithmetic Frobenius Fr_ℓ at every prime $\ell \nmid Np$ acts with characteristic polynomial

$$X^2 - a_\ell(f)X + \omega^j(\ell)\ell^{k-1}.$$

Assume also that the residual representation $\bar{\rho}_f$ is p-distinguished and absolutely irreducible (see Assumption 3.3.1).

Hida's theory [Hid86b; Hid86a] incorporates f and the p-adic representation ρ_f into an analytic family of modular forms and Galois representations. This construction is classical, but has encountered many variations in literature. In Chapter 3 we settle its different versions (mainly coming from the different approaches of [Hid86b], [How07, §2.1] and [LV11, §5]) and in the end we define a complete local Noetherian domain $\mathcal{R}$, finite and free over the Iwasawa algebra $\Lambda_F := \mathcal{O}_F[[1+p\mathbb{Z}_p]]$, whose set of *arithmetic prime ideals* (see §3.2.4) is in 1:1 correspondence with the set of p-adic modular forms in the Hida family passing through f (see Theorem 3.2.9).

Taking inverse limits over m of the p-adic Tate modules of the Jacobian varieties of the modular curves $X_1(\Gamma_0(N)\cap\Gamma_1(p^m))$, in §3.3.3 we introduce a self-dual $G_{\mathbb{Q}}$-representation $\mathbf{T}^\dagger$ which is free of rank 2 over $\mathcal{R}$ and has the property that, for every arithmetic prime p of $\mathcal{R}$, the representation $V_{\mathfrak{p}}^\dagger := \mathbf{T}^\dagger \otimes_{\mathcal{R}} \mathrm{Frac}(\mathcal{R}/\mathfrak{p})$ is a twist of the representation attached to the modular form corresponding to p.

Big Heegner points

The first construction of an Euler system of Heegner classes (called *big Heegner classes*) for the representation $\mathbf{T}^\dagger$ was pursued by Howard in [How07]. If, again, K is an imaginary quadratic field of discriminant D_K prime to Np that satisfies the strong Heegner hypothesis with respect to N, Howard was able to build a system of cohomology classes $X_n \in H^1(H_n;\mathbf{T}^\dagger)$ for every $n \nmid N$ that satisfy compatibility properties similar to (E1), (E2) and (E3) (see [How07, Propositions 2.3.1, 2.3.2 and 2.3.4]).

Howard's work was generalized by Longo and Vigni in [LV11], with the aim of building a system of big Heegner points for Hida families over imaginary quadratic fields that do not satisfy the strong Heegner hypothesis. Indeed, let's suppose that there is a factorization

$$N = N^+N^-$$

such that the primes dividing N^+ (respectively, N^-) are split (respectively, inert) in K. Although the construction of [LV11] is more general, for the work of this thesis we assume also that $D_K \neq -3,-4$, that the class number of K is prime to p and that the number of primes dividing N^- is even (see Assumption 2.2.6). Studying the arithmetic of a certain family of orders in quaternion algebras (see §1.1), Longo and Vigni built a compatible family of Heegner points in towers of Shimura curves (see §2.3). Moving to the cohomology, they construct a system of big Heegner classes

$$\kappa_n \in H^1(H_n;\mathbf{T}^\dagger)$$

satisfying compatibility properties generalizing (E1) and (E2) (see Propositions 3.5.5, 3.5.6 and 3.5.7). However, they do not prove a formula for the action of complex conjugation on the classes κ_n, and the different approach of [LV11] does not make clear how to generalize [How07, Proposition 2.3.4] to the quaternionic context. This is why, at a certain point, we will need to conjecture that the right generalization of (E3) holds also in our context (see Conjecture 5.5.7 and Remark 5.5.8). In a future work, we will present another family of big Heegner points for $\mathbf{T}^\dagger$ for which Conjecture 5.5.7 can be easily proven.

Anticyclotomic Iwasawa theory

The core of this thesis is to perform a suitable Kolyvagin's descent to the system of big Heegner classes $_n$. At a certain point, we follow some of the ideas of [Büy14], where the author explains how to construct a Kolyvagin system out of the set of Howard's big Heegner points. This is why we import some of his notation.

Let K_∞ be the anticyclotomic Z_p-extension of K and call K the -th layer of the extension K_∞/K, for every ≥ 1. Define $^{ac} := \mathrm{Gal}(K_\infty/K) \cong Z_p$ and $^{ac} := Z_p[[\ ^{ac}]]$. Set $L := H_1K$ and, for every n coprime with Np, set also $L\ (n) := H_nL$. See diagram (4.1) for a picture. Then we define the elements

$$z_{n;} := \mathrm{cor}_{H_{np\ +1}/L\ (n)} U_p^- \quad _{np\ +1} \in H^1(L\ (n); \mathbf{T}^\dagger);$$

where $\mathrm{cor}_{H_{np\ +1}/L\ (n)}$ is corestriction. The collection $\{z_{1;}\}_{\in \mathbb{N}}$ is compatible with respect to corestriction (see Lemma 5.3.3), therefore we may set

$$_\infty := \{\mathrm{cor}_{L\ /K}\ z_{1;}\}_{\in \mathbb{N}} \in \varprojlim H^1(K\ ; \mathbf{T}^\dagger);$$

where the inverse limit is taken with respect to corestriction maps. Shapiro's lemma (see §4.1.2) yields an isomorphism

$$H^1(K\ ; \mathbf{T}^\dagger) \cong H^1\big(K; \mathbf{T}^\dagger \otimes_{Z_p}\ ^{ac}/(\ ^p - 1)\big);$$

where is a fixed profinite generator of ^{ac}. This implies that $_\infty$ can be seen as an element of $H^1(K; \mathbf{T}^{\mathrm{lw}})$ where, by definition, we set $\mathbf{T}^{\mathrm{lw}} := \mathbf{T}^\dagger \otimes_{Z_p}\ ^{ac}$, allowing the group G_K to act also on the second factor of the tensor product.

Kolyvagin systems

In Chapter 4, we show how one can adapt the theory of Kolyvagin systems of [MR04] and [How04b] to our context, working with the representation $\mathbf{T}^{\mathrm{lw}}$, that is a free module of rank 2 over the ring $\mathcal{R}^{\mathrm{lw}} := \mathcal{R} \otimes_{Z_p}\ ^{ac} \cong \mathcal{R}[[\ ^{ac}]]$.

Following the ideas of [Büy14] and [Büy16], we define suitable finite quotients $R_{m;s;t}$ of $\mathcal{R}^{\mathrm{lw}}$ and work with the finite representations $T_{m;s;t} = \mathbf{T}^{\mathrm{lw}} \otimes_{\mathcal{R}} R_{m;s;t}$, for every $m; s; t \in Z_{>0}$. Then we define the set $\mathcal{P}_{m;s}$ of inert primes $= (`)$ of $K$ not dividing $Np$ such that $` + 1$ is divisible by p^s and the arithmetic Frobenius Fr at acts trivially on $T_{m;s;t}$.

In §4.2.5 we define the module of universal Kolyvagin systems $\overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}}; \mathcal{F}_{\mathrm{Gr}}; \mathcal{P}')$ for $\mathbf{T}^{\mathrm{lw}}$ with respect to the strict Greenberg condition (see §4.2.2) and a family of subsets of the sets of primes $\mathcal{P}_{m;s}$. The precise definition of this module is quite involved, so we refer to Definition 4.2.17.

Further assumptions and main result

Following the ideas of [Büy14], we have to make some technical hypotheses. The first assumption is used to bound the p-part of the Tamagawa numbers at the primes dividing N of the specializations of $\mathbf{T}^\dagger$. If p is an arithmetic prime of $\mathcal{R}$, we denote by $T(\mathrm{p})$ the associated G_Q-representation, with coe□cients in the integral closure $S(\mathrm{p})$ of $\mathcal{R}/\mathrm{p}$.

Assumption (Assumption 5.2.3). There is an arithmetic prime p of $\mathcal{R}$ such that, for every prime v of K dividing N,

(1) $\mathrm{Tam}_v^{(p)}(T(\mathfrak{p})) = 1$;

(2) $T(\mathfrak{p})^{I_v}$ is a free $S(\mathfrak{p})$-module of rank 1, where I_v is a fixed inertia group at v.

This assumption is [Büy14, Assumption 3.4] (see also [Büy14, Remark 3.5]). The number $\mathrm{Tam}_v^{(p)}(T(\mathfrak{p}))$ is the p-part of the Tamagawa number of $T(\mathfrak{p})$ at v, as defined in [FP94, §4] (see also our §5.2.2). Under this assumption, following closely [Büy14], we are able to bound the Tamagawa numbers of all specializations of $\mathbf{T}^\dagger$ (see Proposition 5.2.4) and to prove that $H^1(I_v;\mathbf{T}^\dagger)$ is $\mathcal{R}$-torsion-free (see Lemma 5.2.5). This last fact is crucial in order to prove that the classes $z_{n;}$ lie in the strict Greenberg Selmer group (see Lemma 5.3.7).

We remark here that one could replace this assumption with the hypotesis of $\mathbf{T}^\dagger$ being minimally ramified at every prime $v \mid N$ (see §5.2.1). In this way, one still obtains Theorem A. However, for our intended applications to Iwasawa theory of Chapter 6, we will need the full power of Assumption 5.2.3. For more on this, see Remark 5.2.6.

We also need to make an assumption on the local cohomology of $\mathbf{T}^\dagger$ at primes $v \mid p$. In this case, the representation $\mathbf{T}^\dagger$ comes with an exact sequence (see Proposition 3.3.7)

$$0 \longrightarrow F_v^+(\mathbf{T}^\dagger) \longrightarrow \mathbf{T}^\dagger \longrightarrow F_v^-(\mathbf{T}^\dagger) \longrightarrow 0$$

of $\mathcal{R}[[D_v]]$-modules, where D_v is a fixed decomposition group at v, $F_v^+(\mathbf{T}^\dagger)$ and $F_v^-(\mathbf{T}^\dagger)$ are free $\mathcal{R}$-modules of rank 1.

Assumption (Assumption 5.4.7). For every valuation $v \mid p$ of K we assume that

$$H^0(K_v;F_v^-(\mathbf{T}^\dagger)) = \{0\};$$

where $F_v^-(\mathbf{T}^\dagger)$ is the residual representation $F_v^-(\mathbf{T}^\dagger) \otimes_{\mathcal{R}} \mathcal{R}/\mathfrak{m}_{\mathcal{R}}$.

For the content of this assumption we refer to [Büy14, (H.stz)]. It can be thought as an assumption to rule out the existence of exceptional zeroes (in the sense of [Gre94]) at characters of ^{ac} of finite order.

Finally, we need to define a subset $\mathcal{P}'_{m;s}$ of $\mathcal{P}_{m;s}$ of primes with finer properties (see Lemma 5.5.6). In order to show that this set is infinite, we must assume that the image of G_Q inside $\mathrm{Aut}_{\mathcal{R}}(\mathbf{T}^\dagger)$ is *big* (see Assumption 5.5.4 for a precise statement). This type of hypothesis, although not present in [Büy14], is very classical and seems necessary to pursue Kolyvagin's descent. Then, our main result is the following.

Theorem A (Theorem 5.4.14). *Under the running assumptions and Conjecture 5.5.7, there is a universal Kolyvagin system* $\sim \in \overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{Iw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}')$ *such that*

$$\sim_1 = \quad_\infty \in \varprojlim H^1(K\ ;\mathbf{T}^\dagger).$$

The proof of this result occupies the whole Chapter 5. We first modify the classes $z_{n;}$ in order to find cohomology classes $^{(m;s;t)}_{n}$ that are rational over K with values in the finite quotients $T_{m;s;t}$ of $\mathbf{T}^{\mathrm{Iw}}$. Then, we show that these classes lie in the suitable Selmer group. Finally, in §5.5, we show how to build a universal Kolyvagin system out of them. We remark here that an easier version of the arguments that come into play in Chapter 5 can be used to build a universal Kolyvagin system for the representation $\mathbf{T}^\dagger$ in stead of $\mathbf{T}^{\mathrm{Iw}}$.

The Iwasawa main conjecture

Once we obtain a Kolyvagin system as in Theorem A, a quasi-standard argument gives a proof of one divisibility for an Iwasawa main conjecture, sometimes also called the *Heegner point main conjecture*. This is a generalization of the Heegner point main conjecture for elliptic curves forumulated by Perrin-Riou [Per87], first stated in [How07, Conjecture 3.3.1] and generalized in [LV11, Conjecture 10.8]. It has been recently proven under mild hypotheses (slightly different than ours) by Castella and Wan in [CW22].

Suppose that the ring $\mathcal{R}^{\mathrm{lw}}$ is regular (see Assumption 6.0.1) and let M be a $\mathcal{R}^{\mathrm{lw}}$-torsion module. We define the characteristic ideal of M to be

$$\mathrm{char}(M) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{length}(M_{\mathfrak{p}})}$$

where the product runs over all height-1 primes of $\mathcal{R}^{\mathrm{lw}}$. Define also

$$\mathbf{A}^{\mathrm{lw}} := \mathbf{T}^{\mathrm{lw}} \otimes_{\mathcal{R}^{\mathrm{lw}}} (\mathcal{R}^{\mathrm{lw}})^{\vee};$$

where $(\mathcal{R}^{\mathrm{lw}})^{\vee}$ is the Pontryagin dual of $\mathcal{R}^{\mathrm{lw}}$.

Theorem B (Theorem 6.2.6). *If* $\kappa_\infty \neq 0$ *then the modules* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})$ *and* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}})^{\vee}$ *have* $\mathcal{R}^{\mathrm{lw}}$*-rank* 1 *and*

$$\mathrm{char}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}})^{\vee}_{\mathrm{tors}}\right) \supseteq \mathrm{char}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})/(\kappa_\infty)\right)^2.$$

We devote the entire Chapter 6 to the proof of this theorem and we show how one can adapt the arguments of [Fou13] to our setting. We hope that our work will give more consistency to the first lines of the proof of [CW22, Theorem 5.5], where they implicitely use the fact that Longo-Vigni's Heegner points can be modified into a Kolyvagin system. As stated at the end of [CW22, §4], the class κ_∞ should be nonzero thanks to a generalization of the arguments in [CV07], therefore we suspect that one could drop this condition from the hypotheses of Theorem B.

Outline of the thesis

In Chapter 1 we review in great generality the theory of quaternion algebras and Shimura curves. We compare different level structures on families of abelian surfaces and explain how one can pass from the moduli to the analytic interpretation for some Shimura curves of interest. In the end, we define the action of Hecke operators on the Jacobian of these curves.

In Chapter 2 we review the definition of CM and Heegner points on Shimura curves. We recall the construction of the compatible family of Heegner points built in [LV11].

In Chapter 3 we review Hida theory. We compare two different versions of it and build the big Galois representation $\mathbf{T}^{\dagger}$ attached to a Hida family of modular forms. We then recall the construction of [LV11, §6], where they show how to compare classical with quaternionic Hida theory. In the end, we review the construction of the big Heegner classes built in [LV11].

In Chapter 4 we present the theory of universal Kolyvagin systems. First, we define the representation $\mathbf{T}^{\mathrm{lw}}$ and its quotients. We recall some Iwasawa theory and

define some relevant Galois groups and set of primes that will be used in §5. We then review the theory of Kolyvagin systems and, in the end, define the module of universal Kolyvagin systems for $\mathbf{T}^{\mathrm{lw}}$.

In Chapter 5 we apply a suitable Kolyvagin's descent to the big Heegner classes of [LV11]. We study the local properties of the modified classes and show that they lie in the appropriate Selmer group. Then, we prove that a suitable modification of them form a universal Kolyvagin system for $\mathbf{T}^{\mathrm{lw}}$.

In Chapter 6 we show how the existence of a nontrivial universal Kolyvagin system for $\mathbf{T}^{\mathrm{lw}}$ yields to a proof of one divisibility of the Iwasawa main conjecture for Hida families.

Notation

$R^\times$	the group of invertible elements of a ring R;
$R_{\geq 0}$	the nonnegative elements of a totally ordered ring;
$\mathbb{F}_q$	the field with q elements;
ℓ	a prime number;
$\mathbb{Z}_\ell$	the ℓ-adic integers;
R_ℓ	the ℓ-adic completion $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ of a ring R;
$\mathbb{Q}_\ell$	the field of fractions of $\mathbb{Z}_\ell$;
$\hat{\mathbb{Z}}$	the profinite completion of $\mathbb{Z}$;
$\hat{R}$	the profinite completion $R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ of a ring R;
F	a field;
$\overline{F}$	a fixed algebraic closure of F;
$\mathrm{GL}_2(F)$	the group of 2×2 invertible matrices with coefficients in F;
$\mathrm{SL}_2(F)$	the subgroup of $\mathrm{GL}_2(F)$ consisting of matrices with determinant equal to 1;
$\mathcal{H}$	the upper half plane $\{z \in \mathbb{C} \,:\, \mathrm{Im}(z) > 0\}$;
H	the set $\mathbb{C} \smallsetminus \mathbb{R}$.

Chapter 1

Shimura Curves

In this chapter we review the theory of Shimura curves, the main geometric object of interest in this thesis. These curves were introduced in the 60's by Goro Shimura in a series of papers and their study was developed by many other authors in the 70's in the broader context of Shimura varieties. They generalize the notion of modular curves to a quaternionic context, as we will see in detail in the next pages.

1.1 Quaternion algebras

Main reference: [Voi21]. In this section we introduce and study the arithmetic of quaternion algebras. We will use the following notation:

F	a field with $\mathrm{char}(F) \neq 2$;
$\overline{F}$	a fixed algebraic closure of F;
ℓ	a prime number.

1.1.1 Basics

Definition. An (associative) algebra B over F is a quaternion algebra if there exist $i, j \in B$ such that $1, i, j, ij$ is a F-basis for B and

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ji = -ij \tag{1.1}$$

for some $a, b \in F^\times$.

If F is a topological field, there is a unique topology induced on B as a finitely dimensional vector space over F. For $a, b \in F^\times$ we define $(a, b \mid F)$ to be the quaternion algebra over F with F-basis $1, i, j, ij$ subject to the multiplication (1.1). Note that the map that interchanges i and j gives an isomorphism $(a, b \mid F) \cong (b, a \mid F)$. If L/F is a field extension and $a, b \in F$, there is a canonical isomorphism

$$(a, b \mid F) \otimes_F L \cong (a, b \mid L).$$

Example 1.1.1. The quaternion algebra $\mathbb{H} := (-1, -1 \mid \mathbb{R})$ is called the algebra of Hamilton quaternions.

Example 1.1.2. There is an isomorphism $(1, 1 \mid F) \to \mathrm{M}_2(F)$ induced by

$$i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition. A quaternion algebra B over F is said to be split if $B \cong \mathrm{M}_2(F)$ as F-algebras.

Definition. If B is a quaternion algebra over F and L/F is a field extension, L is called a splitting field for B if $B \otimes_F L$ is split.

Lemma 1.1.3. *Every quaternion algebra B over F has $B \otimes_F F \cong \mathrm{M}_2(F)$.*

Proof. See [Voi21, Example 2.2.4]. □

Lemma 1.1.4. *Let B be a quaternion algebra over F and let $L \supseteq F$ be a quadratic extension of fields. Then L is a splitting field for B if and only if there is an injective F-algebra homomorphism $L \hookrightarrow B$.*

Proof. See [Voi21, Lemma 5.4.7]. □

Theorem 1.1.5. *If B is an algebra over F, the following statements are equivalent:*

(a) B is a quaternion algebra over F.

(b) B is a central simple algebra of dimension 4 over F.

(c) B is a central semisimple algebra of dimension 4 over F.

(d) The algebra $B \otimes_F F$ is isomorphic to the matrix algebra $\mathrm{M}_2(F)$.

(e) Either B is isomorphic to $\mathrm{M}_2(F)$ or B is a noncommutative division ring of degree 4 over F.

Proof. The equivalence between (a),(b),(c),(d) is [Voi21, Proposition 7.6.1]. For (e) see [Voi21, Corollary 3.5.6 and Main Theorem 5.4.4]. □

Following [Voi21, Chapter 3], we see that on B there exists a unique standard involution, i.e. an F-linear map $^* : B \to B$ which satisfies

1. $1^* = 1$.
2. $(\ ^*)^* =$ for all $\in B$.
3. $(\ \ )^* = \ ^*\ ^*$ for all $\ ; \ \in B$.
4. $\ ^* = \ ^* \in F$ for all $\in B$.
5. $\ + \ ^* \in F$ for all $\in B$.

Definition. Let B be a quaternion algebra over F and $\in B$. We define the (reduced) trace of $$ to be $\mathrm{Tr}(\ ) := \ + \ ^* \in F$ and the (reduced) norm of $$ to be $\mathrm{Nm}(\ ) := \ ^* \in F$.

Remark 1.1.6. If $B = (a; b \mid F)$, as noted in [Voi21, §3.2.9], the map

$$\begin{aligned} ^* : B &\longrightarrow B \\ b = t + xi + yi + zij &\longmapsto b^* = t - xi - yj - zij \qquad \text{for } t;x;y;z \in F \end{aligned}$$

is the unique standard involution on B. In particular, the element b^* is the only element in B such that $b + b^* = 2t$.

Example 1.1.7. The adjugate map

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto A^\dagger = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

is the standard involution on $\mathrm{M}_2(F)$. The operators $\mathrm{Tr}(A)$ and $\mathrm{Nm}(A)$ coincide respectively to the usual trace and determinant of A.

Lemma 1.1.8. *Let* $\varphi : B \to B'$ *be a morphism of quaternion algebras over* F*. Then*

$$\varphi(b^*) = \varphi(b)^*$$

for every $b \in B$*.*

Proof. Write $b = t + p$ with $t \in F$ and where p is an F-linear combination of i, j, ij. Remark 1.1.6 implies that $b^* = t - p$. Since φ is F-linear, we have that $\varphi(b) = t + \varphi(p)$ and $\varphi(b^*) = t - \varphi(p)$. Adding together, we obtain that $\varphi(b) + \varphi(b^*) = 2t$. By Remark 1.1.6, we conclude that $\varphi(b^*) = \varphi(b)^*$. □

Corollary 1.1.9. *Let* $\varphi : B \to B'$ *be a morphism of quaternion algebras over* F*. Then* $\mathrm{Tr}(b) = \mathrm{Tr}(\varphi(b))$ *and* $\mathrm{Nm}(b) = \mathrm{Nm}(\varphi(b))$*.*

Remark 1.1.10. As a consequence of Lemma 1.1.8 and Corollary 1.1.9, whenever there is an embedding $B \hookrightarrow \mathrm{M}_2(L)$ of a quaternion algebra B over F into a matrix algebra over a field L, the canonical involution on B corresponds to the adjugate map of Example 1.1.7 on $\mathrm{M}_2(L)$. Moreover, the reduced trace and the reduced norm on B correspond respectively to the trace and the determinant maps on $\mathrm{M}_2(L)$.

The following is a fundamental result about automorphisms of quaternion algebras, that descends from the Skolem-Noether theorem on simple algebras.

Theorem 1.1.11. *Let* B *be a quaternion algebra over* F*. Then every automorphism of* B *is an inner automorphism.*

Proof. See [Voi21, Corollary 7.1.4]. □

1.1.2 Lattices and orders

For this subsection let R be a Dedekind domain and consider $F := \mathrm{Frac}(R)$.

Definition. An R-lattice M of a finitely generated F-vector space V is a finitely generated R-submodule of V such that $M \otimes_R F = V$.

Definition. Let B be a finite F-algebra. An R-order O of B is an R-lattice that is also a subring of B. An R-order O of B is maximal if there is no order of B properly containing O.

If O is an R-order of B we will say that O' is a superorder of O if O' is an R-order containing O.

Definition. Let B be a quaternion algebra over F. An Eichler order $O \subseteq B$ is the intersection of two (not necessarily distinct) maximal orders.

The following result is an easy consequence of Theorem 1.1.11.

Lemma 1.1.12. *Two R-orders of a quaternion algebra B over F are isomorphic if and only if they are $B^\times$-conjugate.*

Proof. An isomorphism $f : O_1 \to O_2$ of R-orders extends to an isomorphism

$$f : B = O_1 \otimes_R F \longrightarrow O_2 \otimes_R F = B$$

of F-algebras. We conclude applying Theorem 1.1.11. □

Lemma 1.1.13. *Let B be a quaternion algebra over F and $O \subseteq B$ be an R-order. Then every element $\in O$ is integral over R and* Tr( ); Nm( ) $\in R$

Proof. See [Voi21, Corollary 10.3.6 and Lemma 10.3.7]. □

1.1.3 Quaternion algebras over various fields

Quaternion algebras over algebraically closed fields. If F is algebraically closed, by Lemma 1.1.3 we have that the only quaternion algebra over F is $M_2(F)$.

Quaternion algebras over the reals. When $F = \mathbb{R}$ we have the following theorem.

Theorem 1.1.14 (Frobenius). *The algebra of Hamilton quaternions* $\mathbb{H}$ *is the unique algebraic non-commutative division algebra over* $\mathbb{R}$ *up to isomorphism.*

Proof. See [Voi21, Corollary 3.5.8]. □

Theorem 1.1.5 immediately implies that, up to isomorphism, the only quaternion algebras over $\mathbb{R}$ are the split algebra $M_2(\mathbb{R})$ and the algebra $\mathbb{H}$ of Hamilton quaternions.

Quaternion algebras over finite fields. When F is a finite field, we have the following theorem.

Theorem 1.1.15 (Wedderburn's little theorem). *Every finite division ring is a field.*

Proof. See [Mac05]. □

This result, together with Theorem 1.1.5, implies that the only quaternion algebras over a finite field F is, up to isomorphism, the split algebra $M_2(F)$.

1.1.4 Quaternion algebras over finite extensions of $\mathbb{Q}_\ell$

For this subsection let ℓ be a prime, $F/\mathbb{Q}_\ell$ be a finite extension of fields and $\mathcal{O}_F$ be the valuation ring of F. Fix a uniformizer of F and set $\mathfrak{l} := ( )$. Set also $k_F := \mathcal{O}_F/\mathfrak{l}$ and call q the cardinality of k_F.

Theorem 1.1.16. *Let B be a quaternion algebra over F. Then B is a division algebra if and only if*

$$B \cong (e; \ | F)$$

where $e \in \mathcal{O}_F^\times$ is nontrivial in $k_F^\times/(k_F^\times)^2$.

Proof. See [Voi21, Corollary 12.3.12 and Theorem 13.3.11]. □

When B is a division quaternion algebra over F, there are a lot of similarities between B and finite field extensions of F. In particular, we can define valuations and valuation rings. Let $v : F \to \mathbb{Z} \cup \{\infty\}$ be the normalized valuation on F.

Lemma 1.1.17. *Let B be a division quaternion algebra over F. The map v can be uniquely extended to a discrete valuation $w : B \to \mathbb{R} \cup \{\infty\}$, i.e.:*

(a) $w(\ ) = \infty$ *if and only if* $\ = 0$.

(b) $w(\quad) = w(\quad) = w(\ ) + w(\ )$ *for all* $\ ; \ \in B$.

(c) $w(\ + \ ) \geq \min(w(\ ); w(\ ))$ *for all* $\ ; \ \in B$.

(d) $w(B^\times)$ *is discrete in* $\mathbb{R}$.

Proof. See [Voi21, Lemma 13.3.2]. □

A straightforward consequence of this lemma is that the set

$$O_B := \{ \ \in B \ : \ w(\ ) \geq 0\}$$

is a ring, called the valuation ring of B.

Proposition 1.1.18. *Let B be a division quaternion algebra over F. The ring O_B is the unique maximal $\mathcal{O}_F$-order in B, consisting of all elements of B that are integral over $\mathcal{O}_F$.*

Proof. See [Voi21, Proposition 13.3.4]. □

As a consequence, if B is a division quaternion algebra over F, then there is a unique maximal order in B that is also the unique Eichler order. When, insetad, B is the split quaternion algebra over F, we don't have a unique maximal order.

Proposition 1.1.19. *After fixing an isomorphism $\mathrm{M}_2(F) \cong \mathrm{End}_F(F^2)$, the maximal orders in $\mathrm{M}_2(F)$ are subrings of the form $\mathrm{End}_{\mathcal{O}_F}(M)$ where M is an $\mathcal{O}_F$-lattice in F^2. As a consequence, the maximal orders in $\mathrm{M}_2(F)$ are the conjugates of $\mathrm{M}_2(\mathcal{O}_F)$.*

Proof. See [Voi21, Lemma 10.5.4 and Corollary 10.5.5]. □

We pursue now the study of Eichler orders for the split algebra $\mathrm{M}_2(F)$. We have the following characterization.

Proposition 1.1.20. *Let $O \subseteq B = \mathrm{M}_2(F)$ be an $\mathcal{O}_F$-order. The following are equivalent:*

(a) O is an Eichler order.

(b) O is $B^\times$-conjugate to the order $\left(\begin{smallmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \mathfrak{l}^e & \mathcal{O}_F \end{smallmatrix}\right)$ for a unique $e \geq 0$.

(c) O contains an $\mathcal{O}_F$-subalgebra that is $B^\times$-conjugate to $\left(\begin{smallmatrix} \mathcal{O}_F & 0 \\ 0 & \mathcal{O}_F \end{smallmatrix}\right)$.

(d) O is the intersection of a uniquely determined pair of maximal orders.

Proof. See [Voi21, Proposition 23.4.3]. □

Definition. Let $O \subseteq B = \mathrm{M}_2(F)$ be an Eichler order. The ideal $\mathfrak{l}^e \subseteq \mathcal{O}_F$ determined by point (b) of the previous proposition is called the level of O.

Corollary 1.1.21. *Every superorder of an Eichler order in* $\mathrm{M}_2(F)$ *is Eichler.*

Proof. Straightforward from point (c) of Proposition 1.1.20. □

Proposition 1.1.22. *Let* B *be a quaternion algebra over* F *and let* O *be an Eichler order of* B*. Then*

(a) $\mathrm{Nm}(B^\times) = F^\times$*;*

(b) $\mathrm{Nm}(O^\times) = \mathcal{O}_F^\times$*.*

Proof. For (a) see [Voi21, Lemma 13.4.9]. When B is a division algebra, the Eichler order O is maximal and point (b) descends from [Voi21, Lemma 13.4.9]. When B is the split quaternion algebra, [Voi21, Lemma 13.4.9] implies that $\mathrm{Nm}(O^\times) \subseteq \mathcal{O}_F^\times$ and point (c) of Proposition 1.1.20 yields $\mathrm{Nm}(O^\times) \supseteq \mathcal{O}_F^\times$. □

We end this subsection with a remark on the topology of quaternion algebras over finite extensions of $\mathbb{Q}$.

Lemma 1.1.23. *Let* B *be a quaternion algebra over* F *and let* O *be an order of* B*. Then* O *and* $O^\times$ *are compact Hausdor spaces, whereas* B *and* $B^\times$ *are locally compact Hausdor spaces.*

Proof. See [Voi21, §13.5.2 and §13.5.6]. □

1.1.5 Quaternion algebras over number fields

For this subsection we let F be a number field and $\mathcal{O}_F$ be its ring of integers.

Definition. Let B be a quaternion algebra over F. For any place v of F, we define the localization B_v of B to be $B_v := B \otimes_F F_v$.

Definition. Let B be a quaternion algebra over F. For any place v of F we say that B splits at v if $B_v \cong \mathrm{M}_2(F_v)$. Otherwise, we say that B ramifies at v. We denote by $\mathrm{Ram}(B)$ the set of places of F which are of ramification for B.

Theorem 1.1.24. *The map* $B \mapsto \mathrm{Ram}(B)$ *gives a bijection*

$$\left\{\begin{array}{c}\textit{Quaternion algebras over } F\\ \textit{up to isomorphism}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{Finite subsets of noncomplex places}\\ \textit{of } F \textit{ of even cardinality}\end{array}\right\}.$$

Proof. See [Voi21, Main Theorem 14.6.1]. □

Remark 1.1.25. As a consequence, a quaternion algebra B over a number field F is split if and only if $\mathrm{Ram}(B) = \varnothing$. Moreover, two quaternion algebras B_1 and B_2 over F are isomorphic if and only if $\mathrm{Ram}(B_1) = \mathrm{Ram}(B_2)$.

For quaternion algebras over number fields there is a precise characterization of quadratic splitting fields, that extends Lemma 1.1.4.

Proposition 1.1.26. *Let* B *be a quaternion algebra over a number field* F *and let* L/F *be a quadratic extension of fields. The following statements are equivalent:*

(i) L *is a splitting field for* B*, i.e.* $B \otimes_F L \cong \mathrm{M}_2(L)$*;*

(ii) There is an embedding $L \hookrightarrow B$ *of* F*-algebras;*

(iii) Every place $v \in \mathrm{Ram}(B)$ does not split in the field L.

Proof. See [Voi21, Proposition 14.6.7]. □

Definition. Let B be a quaternion algebra over $\mathbb{Q}$. We say that B is definite if B is ramified at ∞, i.e. if $B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$. We say that B is indefinite if B is split at ∞, i.e. if $B_\infty \cong \mathrm{M}_2(\mathbb{R})$.

Definition. Let B be a quaternion algebra over $\mathbb{Q}$. The discriminant of B is

$$\mathrm{disc}(B) := \prod_{\ell \in \mathrm{Ram}(B) \setminus \{\infty\}} \ell. \tag{1.2}$$

Corollary 1.1.27. *Let B be an indefinite quaternion algebra over $\mathbb{Q}$. Then the field $\mathbb{Q}(\sqrt{-\mathrm{disc}(B)})$ is a splitting field for B.*

Proof. Apply Proposition 1.1.26, noticing that every prime dividing $\mathrm{disc}(B)$ is ramified in $\mathbb{Q}(\sqrt{-\mathrm{disc}(B)})$. □

Proposition 1.1.28. *Let B be a quaternion algebra over F. Then $\mathrm{Nm}(B^\times)$ is the subgroup of $F^\times$ consisting of the elements $\alpha \in F^\times$ such that $v(\alpha) > 0$ for every infinite (real) place $v \in \mathrm{Ram}(B)$.*

Proof. See [Voi21, Main Theorem 14.7.4]. □

Corollary 1.1.29. *Let $F = \mathbb{Q}$. If B is definite then $\mathrm{Nm}(B^\times) = \mathbb{Q}_{>0}$, whereas if B is indefinite then $\mathrm{Nm}(B^\times) = \mathbb{Q}^\times$.*

We now move on to study lattices and orders in quaternion algebras over global fields. We will mostly be interested in Eichler orders of quaternion algebras over $\mathbb{Q}$, as they will be the main arithmetic ingredient in the definition of the Shimura curves of interest.

Definition. If B is a quaternion algebra over F and M is an $\mathcal{O}_F$-lattice of B, we set $M_v := M \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$ for every finite place v of F, where $\mathcal{O}_{F_v}$ is the valuation ring of F_v. The lattice M_v is called the localization of M at v.

Proposition 1.1.30 (Local-global dictionary for lattices). *Let M be a lattice in a quaternion algebra B over F. There is a bijection between the set of lattices N of B and the set*

$$\{(N_v)_v \mid N_v \text{ lattice of } B_v,\ N_v = M_v \text{ for all but fin. many finite places } v \text{ of } \mathcal{O}_F\}$$

estabilished by the maps

$$N \mapsto (N_v)_v; \quad (N_v)_v \mapsto \{x \in B \mid x \in N_v \text{ for all finite places } v \text{ of } \mathcal{O}_F\}$$

which are inverse to each other.

Proof. See [Voi21, Theorem 9.4.9 and Lemma 9.5.3]. □

Definition. A property P of lattices of B is said to be local if a lattice M of B satisfies P if and only if M_v satisfies P for all finite places v of $\mathcal{O}_F$.

Proposition 1.1.31. *The properties for a lattice to be*

(a) an order;

(b) a maximal order;

(c) an Eichler order

are local.

Proof. This is a consequence of Proposition 1.1.30. □

Let now B be a quaternion algebra over $\mathbb{Q}$. We introduce the notion of reduced discriminant for an order of B and we pursue a deeper study of Eichler orders in B.

Definition. Let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subseteq B$ be an order. Fix a $\mathbb{Z}$-basis $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ for $\mathcal{O}$. The discriminant of $\mathcal{O}$ is

$$\operatorname{disc}(\mathcal{O}) := |\det(\operatorname{Tr}(\alpha_i \alpha_j))_{i,j}| \in \mathbb{Z}_{>0}.$$

Remark 1.1.32. The discriminant of an order $\mathcal{O}$ is integral thanks to Lemma 1.1.13, and it is independent on the chosen basis.

The discriminant of an order is always a square (see the first lines of [Voi21, §15.4]), therefore the following definition makes sense.

Definition. Let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subseteq B$ be an order. The reduced discriminant of $\mathcal{O}$ is

$$\operatorname{discrd}(\mathcal{O}) = \sqrt{\operatorname{disc}(\mathcal{O})} \in \mathbb{Z}_{>0}.$$

Let $\mathcal{O}$ be an Eichler order of a quaternion algebra B over $\mathbb{Q}$. By Proposition 1.1.31, we have that the completion $\mathcal{O}_\ell \subseteq B_\ell$ is Eichler. This implies that for every $\ell \mid \operatorname{disc}(B)$ we have that $\mathcal{O}_\ell$ is the unique maximal order of B_ℓ, while for $\ell \nmid \operatorname{disc}(B)$ Proposition 1.1.20 implies that $\mathcal{O}_\ell$ is conjugate to the order

$$\begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^e \mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix}$$

for a unique $e \geq 0$.

Lemma 1.1.33. *Let B be a quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O} \subseteq B$ be an Eichler order. Then there is a unique $N \in \mathbb{Z}_{>0}$ coprime with $\operatorname{disc}(B)$ such that*

(i) $\operatorname{discrd}(\mathcal{O}) = \operatorname{disc}(B) \cdot N$;

(ii) For every prime $\ell \nmid \operatorname{disc}(B)$, the order $\mathcal{O}_\ell$ is $B_\ell^\times$-conjugate to the order

$$\begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^{v_\ell(N)} \mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix};$$

where v_ℓ is the normalized ℓ-adic valuation on $\mathbb{Z}$.

Proof. See [Voi21, §23.4.19]. □

Definition. Let $\mathcal{O}$ be an Eichler order of a quaternion algebra B over $\mathbb{Q}$. The number $N = \prod_{\ell \nmid \operatorname{disc}(B)} \ell^e$ defined in Lemma 1.1.33 is called the level of $\mathcal{O}$.

Example 1.1.34. If $B \cong \mathrm{M}_2(\mathbb{Q})$ is the split quaternion algebra over $\mathbb{Q}$, the order

$$O_N = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{pmatrix}:$$

is an Eichler order of level N for every $N \in \mathbb{Z}_{>0}$.

Proposition 1.1.35. *Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and $N \in \mathbb{Z}_{>0}$ be coprime with $\operatorname{disc} B$. Then all Eichler orders in B of level N are $B^\times$-conjugate.*

Proof. By point (ii) of Lemma 1.1.33 and the discussion before it, we have that any two Eichler orders O and O' of level N are locally conjugated (meaning that their localizations at any prime are conjugated). Then, as a consequence of strong approximation (see [Voi21, Theorem 28.2.11]), we obtain that O is isomorphic to O'. By Lemma 1.1.12 we conclude that O and O' are $B^\times$-conjugate. □

1.1.6 The adelic framework

In this subsection, for simplicity, we work with a quaternion algebra B over $\mathbb{Q}$. We follow closely [Voi21, §27].

Denote by $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ the profinite completion of $\mathbb{Z}$ and with $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ the ring of finite adeles of $\mathbb{Q}$. There are natural continous diagonal embeddings $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$ and $\mathbb{Q} \hookrightarrow \hat{\mathbb{Q}}$. The group of invertible elements $\hat{\mathbb{Q}}^\times$ of $\hat{\mathbb{Q}}$ is the group of finite ideles of $\mathbb{Q}$. We recall that $\hat{\mathbb{Q}}^\times$ comes equipped with the topology induced by the embedding

$$\begin{aligned} \hat{\mathbb{Q}}^\times &\longrightarrow \hat{\mathbb{Q}} \times \hat{\mathbb{Q}} \\ x &\longmapsto (x; x^{-1}) \end{aligned}$$

rather than the embedding $\hat{\mathbb{Q}}^\times \hookrightarrow \hat{\mathbb{Q}}$, since the former makes $\hat{\mathbb{Q}}^\times$ a topological group. For details, see [Voi21, §27.2].

Definition. The adelization of B over $\mathbb{Q}$ is the algebra $\hat{B} := B \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}$.

We can explicitly describe the $\hat{\mathbb{Q}}$-algebra $\hat{B}$ as follows (see [Voi21, §27.3]). Let O be an order in B and set as usual $O_\ell := O \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ for every prime ℓ. Then we have the equality

$$\hat{B} = \{(x_\ell)_\ell \in \prod_\ell B_\ell \mid x_\ell \in O_\ell \text{ for all but finitely many primes } \ell\}:$$

Notice that the set on the right of this equality is independent on the choice of O, since any two orders are equal at all but finitely many places by Proposition 1.1.30. A fundamental system of open neighborhoods of 0 in $\hat{B}$ consists of all open neighborhoods of 0 in the subrings

$$\prod_{\ell \in S} B_\ell \times \prod_{\ell \notin S} O_\ell$$

for any fixed order O and with S varying among all finite sets of primes of $\mathbb{Q}$. Notice that this topology is finer than the one induced by the embedding $\hat{B} \hookrightarrow \prod_\ell B_\ell$. Therefore, this last map is *not* a homeomorphism onto its image, but it is continous.

Similarly, we can define the idelization $\hat{B}^\times$ of a quaternion algebra B over $\mathbb{Q}$. It is the group of invertible elements of $\hat{B}$ with the topology induced by the embedding

$$\begin{aligned} \hat{B}^\times &\longrightarrow \hat{B} \times \hat{B} \\ x &\longmapsto (x; x^{-1}): \end{aligned}$$

Let O be an order in B. Then we have the equality

$$\hat{B}^\times = \{(x_\ell)_\ell \in \prod_\ell B_\ell^\times \mid x_\ell \in O_\ell^\times \text{ for all but finitely many primes } \ell\}.$$

A fundamental system of neighborhoods of 1 in $\hat{B}^\times$ consists of all open neighborhoods of 1 in the subgroups

$$\prod_{\ell \in S} B_\ell^\times \times \prod_{\ell \notin S} O_\ell^\times$$

for any fixed order O and with S varying among all finite sets of primes of $\mathbb{Q}$. Again, the map $\hat{B}^\times \hookrightarrow \prod_\ell B_\ell^\times$ is *not* a homeomorphism onto its image, but it is continous.

Remark 1.1.36. The spaces $\hat{B}$ and $\hat{B}^\times$ are Hausdorff, since their topologies are finer than the ones coming from their embedding in $\prod_\ell B_\ell$ and $\prod_\ell B_\ell^\times$ respectively, which are Haudorff spaces (see Lemma 1.1.23).

For any order O of B, define

$$\hat{O} := \prod_\ell O_\ell \subseteq \hat{B} \quad \text{and} \quad \hat{O}^\times := \prod_\ell O_\ell^\times \subseteq \hat{B}^\times.$$

Remark 1.1.37. By definition, the spaces $\hat{O}$ and $\hat{O}^\times$ are open in $\hat{B}$ and $\hat{B}^\times$ respectively. Lemma 1.1.23 together with Tychonoff's theorem implies that $\hat{O}$ and $\hat{O}^\times$ are also compact.

We can define the reduced trace and the reduced norm on $\hat{B}$ componentwise as

$$\begin{aligned} \mathrm{Tr} : \hat{B} &\longrightarrow \hat{\mathbb{Q}} \\ (x_\ell)_\ell &\longmapsto (\mathrm{Tr}(x_\ell))_\ell \end{aligned} \quad \text{and} \quad \begin{aligned} \mathrm{Nm} : \hat{B}^\times &\longrightarrow \hat{\mathbb{Q}}^\times \\ (x_\ell)_\ell &\longmapsto (\mathrm{Nm}(x_\ell))_\ell. \end{aligned}$$

These two maps are well defined thanks to Lemma 1.1.13 and they extend the classical operators Tr and Nm under the embeddings $B \hookrightarrow \hat{B}$ and $B^\times \hookrightarrow \hat{B}^\times$ (see [Vig05, Proposition 1.2.20] for details). Proposition 1.1.22 implies that the idelic norm map Nm is surjective.

Lemma 1.1.38. *Let O be an order in B. Then $\hat{O}^\times \cap B^\times = O^\times$.*

Proof. One inclusion is trivial, the other follows from the local to global principle for lattices (see Proposition 1.1.30). In particular, if $x \in B^\times \smallsetminus O^\times$, then $x_\ell \notin O_\ell^\times$ for some prime ℓ, hence $x \notin \hat{O}^\times$. □

1.1.7 Strong approximation

In this subsection we let B be an indefinite quaternion algebra over $\mathbb{Q}$. For every subset A of B or $\hat{B}$, we denote by A_1 the subset of A consisting of elements of norm 1. Notice that $\hat{B}_1$ is a topological group, with topology induced by its embedding inside $\hat{B}^\times$.

Theorem 1.1.39 (Strong approximation). *B_1 is dense in $\hat{B}_1$.*

Proof. See [Voi21, Main theorem 28.5.3]. □

An important consequence of strong approximation is the following result.

Theorem 1.1.40. *Let O be an order of B. Then the norm map induces a bijection*

$$\mathrm{Nm}: B^\times\backslash\hat{B}^\times/\hat{O}^\times \xrightarrow{\cong} \mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(\hat{O}^\times):$$

Proof. See [Voi21, Theorem 28.5.5]. □

We now prove a slight generalization of the previous theorem.

Theorem 1.1.41. *Let U be an open compact subgroup of $\hat{B}^\times$. Then the norm map induces a bijection*

$$\mathrm{Nm}: B^\times\backslash\hat{B}^\times/U \xrightarrow{\cong} \mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U):$$

Proof. The surjectivity descends from the surjectivity of the norm $\mathrm{Nm}: \hat{B} \to \hat{\mathbb{Q}}$ together with the fact that $\mathrm{Nm}(B^\times) = \mathbb{Q}^\times$ (see Corollary 1.1.29). In order to prove injectivity, we proceed in two steps.

Step 1: $\hat{B}_1 \subseteq B^\times U$. Indeed, let $b \in \hat{B}_1$. Since bU_1 is open inside $\hat{B}_1$, by strong approximation we find $a \in B_1$ and $u \in U_1$ such that $a = bu$. But then $b = au^{-1} \in B^\times U$.

Step 2: Let $b; b' \in \hat{B}^\times$. Since $\mathrm{Nm}: B^\times \to \mathbb{Q}^\times$ and $\mathrm{Nm}: U \to \mathrm{Nm}(U)$ are surjective, to conclude the proof of injectivity it is enough to show that if $\mathrm{Nm}(b) = \mathrm{Nm}(b') \in \hat{\mathbb{Q}}^\times$ then $b'U = abU$ for some $a \in B^\times$. Since $b'b^{-1} \in \hat{B}_1$ and since bUb^{-1} is compact open, by step 1 we find $a \in B^\times$ and $u \in U$ such that $b'b^{-1} = abub^{-1}$. Therefore,

$$b'U = (b'b^{-1})(bU) = abub^{-1}bU = abU;$$

yielding the claim. □

Corollary 1.1.42. *Let U be an open compact subgroup of $\hat{B}^\times$ such that $\mathrm{Nm}(U) \supseteq \hat{\mathbb{Z}}^\times$. Then, for every $b \in \hat{B}^\times$ there are $a \in B^\times$ and $u \in U$ such that $b = au$.*

Proof. This descends from the isomorphism of Theorem 1.1.41 together with the fact that $\mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\hat{\mathbb{Z}}^\times = 1$, since $\mathbb{Q}$ has class number 1. □

Lemma 1.1.43. *Let U be an open compact subgroup of $\hat{B}^\times$ that contains an element of norm -1. Then the map*

$$\begin{aligned} : \mathbb{Q}_{>0}\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U) &\longrightarrow \mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U) \\ [x] &\longmapsto [x] \end{aligned}$$

is a bijection.

Proof. The map is clearly well defined and surjective. In order to prove injectivity, let b be an element of U of norm -1 and take $[x]; [y] \in \mathbb{Q}_{>0}\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U)$ such that $([x]) = ([y])$. This means that $x = qy$ with $q \in \mathbb{Q}^\times$ and $= \mathrm{Nm}(u)$ for some $u \in U$. If $q > 0$, then $[x] = [y]$. If $q < 0$ then

$$x = (-q)\cdot y \cdot (-) = (-q)\cdot y \cdot \mathrm{Nm}(bu);$$

and $bu \in U$. Hence also in this case $[x] = [y]$ and we are done. □

1.2 Shimura curves

For this section we fix an indefinite quaternion algebra B over $\mathbb{Q}$. Recall that *indefinite* means that B is split at infinity or, equivalently, that $\mathrm{disc}(B)$ is the product of an even number of primes.

For every prime ℓ set $B_\ell := B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $B_\infty := B \otimes_{\mathbb{Q}} \mathbb{R}$. Fix once and for all isomorphisms

$$\iota_\infty : B_\infty \xrightarrow{\cong} \mathrm{M}_2(\mathbb{R}) \quad \text{and} \quad \iota_\ell : B_\ell \xrightarrow{\cong} \mathrm{M}_2(\mathbb{Q}_\ell) \tag{1.3}$$

for every $\ell \nmid \mathrm{disc}(B)$. Note that there are natural inclusions $B \hookrightarrow B_\infty$ and $B \hookrightarrow B_\ell$, hence we can embed B inside $\mathrm{M}_2(\mathbb{R})$ and $\mathrm{M}_2(\mathbb{Q}_\ell)$ for every $\ell \nmid \mathrm{disc}(B)$. With a little abuse of notation, these embeddings will be denoted again with the symbols ι_∞ and ι_ℓ respectively. Finally, notice that the isomorphisms ι_∞ and ι_ℓ are also bicontinous, since they are linear maps between finitely generated normed vector spaces.

1.2.1 Shimura curves as Riemann surfaces

Denote by $\mathcal{H}$ the upper half plane of the complex numbers and set $H := \mathbb{C} \smallsetminus \mathbb{R}$. Let U be a compact open subgroup of $\hat{B}^\times$, which acts on $\hat{B}^\times$ on the right via multiplication and trivially on H. Moreover, $B^\times$ acts on the left on $\hat{B}^\times$ by multiplication, and on H via Möbius transformations induced by $B^\times \hookrightarrow B_\infty^\times \cong \mathrm{GL}_2(\mathbb{R})$.

Definition. The open Shimura $\mathbb{C}$-curve associated to U is the double coset

$$Y_U(\mathbb{C}) := B^\times \backslash (H \times \hat{B}^\times)/U;$$

taken with respect to the actions cited above.

In the next we will see that $Y_U(\mathbb{C})$ has the structure of a Riemann surface. Since U acts trivially on H, we can rewrite

$$Y_U(\mathbb{C}) = B^\times \backslash (H \times (\hat{B}^\times / U)).$$

Example 1.2.1. By Remark 1.1.37, an important example of compact open subgroups of $\hat{B}^\times$ are the groups $\hat{O}^\times$, where O is an order in B.

Recall that $B_1^\times = \ker(\mathrm{Nm} : B^\times \to \mathbb{Q}^\times)$ and $\hat{B}_1^\times = \ker(\mathrm{Nm} : \hat{B}^\times \to \hat{\mathbb{Q}}^\times)$. The following is the main structure theorem for open Shimura $\mathbb{C}$-curves.

Theorem 1.2.2. *Let U be a compact open subgroup of $\hat{B}^\times$, and let $a_1, \dots, a_h \in \hat{\mathbb{Q}}^\times$ be representatives for the classes in $\mathbb{Q}_{>0} \backslash \hat{\mathbb{Q}}^\times / \mathrm{Nm}(U)$. For each i choose $b_i \in \hat{B}^\times$ with $\mathrm{Nm}(b_i) = a_i$ and set*

$$\Gamma_i := B_1^\times \cap b_i U b_i^{-1}.$$

Then the maps

$$\begin{aligned} \Gamma_i \backslash \mathcal{H} &\longrightarrow B^\times \backslash (H \times \hat{B}^\times)/U = Y_U(\mathbb{C}) \\ [x] &\longmapsto [(x, b_i)] \end{aligned}$$

for $i \in \{1, \dots, h\}$ induce a homeomorphism

$$\coprod_{i=1}^{h} \Gamma_i \backslash \mathcal{H} \xrightarrow{\cong} Y_U(\mathbb{C});$$

where the space on the left is the disjoint union of the connected Riemann surfaces $\Gamma_i \backslash \mathcal{H}$, all of which are compact if B is a division algebra.

Proof. See [Vig05, §2.1.1]. □

Lemma 1.2.3. *Let U be an open compact subgroup of $\hat{B}^\times$ such that $\hat{Z}^\times \subseteq \mathrm{Nm}(U)$. Then the Riemann surface $Y_U(\mathbb{C})$ is connected and the maps*

$$\begin{aligned}(U\cap B_1^\times)\backslash\mathcal{H} &\longrightarrow B^\times\backslash(H\times\hat{B}^\times)/U;\\ [x]&\longmapsto[(x;1)]\end{aligned}\qquad\begin{aligned}(U\cap B^\times)\backslash H &\longrightarrow B^\times\backslash(H\times\hat{B}^\times)/U\\ [x]&\longmapsto[(x;1)]\end{aligned}$$

are homeomorphisms.

Proof. In order to prove the bijectivity of the first map, by Theorem 1.2.2 we just need to prove that the set $\mathbb{Q}_{>0}\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U)$ consists of one element.

Since U contains an element of norm -1, by Lemma 1.1.43 there is a bijection $\mathbb{Q}_{>0}\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U)\to\mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U)$. Since $\mathbb{Q}$ has class number one, the double coset $\mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\hat{Z}^\times$ consists of one element, and it surjects onto $\mathbb{Q}^\times\backslash\hat{\mathbb{Q}}^\times/\mathrm{Nm}(U)$. Therefore, this last set consists of one element and the claim is proved.

Turning to the second map, it is easy to see that it is well defined and injective. To show surjectivity, let $[(x;b)]\in B^\times\backslash H\times\hat{B}^\times/U$. Corollary 1.1.42 implies that there are $a\in B^\times$ and $u\in U$ such that $b=au$. Set $z:=a^{-1}x\in H$. We have

$$[z]\mapsto[(z;1)]=[a^{-1}(x;b)u^{-1}]=[(x;b)];$$

hence the map is surjective. The proof of bicontinuity is left to the reader. □

Since in general we want a compact Riemann surface, for every open compact subgroup U of $\hat{B}^\times$ we define $X_U(\mathbb{C})$ to be the Baily-Borel compactification (see [BB66]) of $Y_U(\mathbb{C})$. Notice that when B is a division algebra, by Theorem 1.2.2 we have that $X_U(\mathbb{C})=Y_U(\mathbb{C})$, while in the split case $X_U(\mathbb{C})$ is obtained from $Y_U(\mathbb{C})$ by adjoining a finite number of cusps.

Definition. Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and let U be a compact open subgroup of $\hat{B}^\times$. The Riemann surface $X_U(\mathbb{C})$ is called the (compact) Shimura $\mathbb{C}$-curve associated to B and U.

Remark 1.2.4. Let B be the split quaternion algebra $\mathrm{GL}_2(\mathbb{Q})$. If $\mathrm{Nm}(U)\supseteq\hat{\mathbb{Z}}^\times$, we recover the classical case of modular $\mathbb{C}$-curves. For example, if $\mathcal{O}_N$ is the Eichler order of level N of Example 1.1.34, the equality $\mathcal{O}_N^\times\cap B_1=\Gamma_0(N)$ implies that the Shimura $\mathbb{C}$-curve $X_{\mathcal{O}_N^\times}(\mathbb{C})$ is the classical modular $\mathbb{C}$-curve of level $\Gamma_0(N)$.

When, instead, $\mathrm{Nm}(U)\not\supseteq\hat{\mathbb{Z}}^\times$ then $X_U(\mathbb{C})$ is not connected and it is the disjoint union of connected modular curves. The reason to consider also nonconnected curves is that Shimura curves always have a model over $\mathbb{Q}$, whereas modular curves may not. See [Mil03, §2] for more details. Anyway, our Shimura curves of interest will always be connected.

Remark 1.2.5. Let U be an open compact subgroup of $\hat{B}^\times$. Some authors, such as [LV11] and [BD96], interchange left and right actions in the double quotients defining the open Shimura $\mathbb{C}$-curve $Y_U(\mathbb{C})$. We give here a dictionary to pass from one interpretation to the other.

First, denote by U^* the image of U under the standard involution of $\hat{B}$, that is induced by the standard involution on B in a natural way. Then, there is a map

$$\begin{aligned}Y_U(\mathbb{C})=B^\times\backslash\big(H\times\hat{B}^\times\big)/U&\longrightarrow U^*\backslash\big(H\times\hat{B}^\times\big)/B^\times=:Y'_U(\mathbb{C})\\ [(z;b)]&\longmapsto[(z;b^*)];\end{aligned}$$

where, in the second double quotient, U^* acts trivially on H and by left multiplication on $\hat{B}^\times$, whereas every $b \in B^\times$ acts by right multiplication on $\hat{B}^\times$ and by the Möbius transformation attached to b^* on H. One can easily prove that the map above is well defined and bijective.

In the remainder of this subsection, we give a different interpretation of the set $H = \mathbb{C} \smallsetminus \mathbb{R}$. Namely, let $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$ be the set of $\mathbb{R}$-algebra homomorphisms between $\mathbb{C}$ and B_∞. There is a left action of the group $B^\times$ on $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$ by conjugation.

Theorem 1.2.6. *There is a $B^\times$-equivariant bijection $H \overset{1:1}{\longleftrightarrow} \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$.*

Proof. See [Vig05, Proposition 3.1.3]. □

Therefore, the Shimura $\mathbb{C}$-curve attached to an open compact subgroup U of $\hat{B}^\times$ can be written also as

$$Y_U(\mathbb{C}) = B^\times \backslash \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty) \times \hat{B}^\times / U. \tag{1.4}$$

1.2.2 The analytic definition of the curves $X_{0;M}$, $X_{1;m}$ and X_m

In this subsection we introduce the Shimura curves that will be relevant in our work. Recall that B is an indefinite quaternion algebra over $\mathbb{Q}$ and that in (1.3) we fixed embeddings ι_∞ and ι_ℓ for every $\ell \nmid \mathrm{disc}(B)$. As a shortcut, we will use the notation

$$N^- := \mathrm{disc}(B).$$

Fix also a positive integer N^+ coprime with N^-, call $N := N^+N^-$ and fix a prime $p \nmid 6N$. The letter M will denote any positive integer coprime with N^-.

Fix once and for all a maximal order $\mathcal{O}_B$ of B such that $\iota_\ell(\mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell) = \mathrm{M}_2(\mathbb{Z}_\ell)$ for every $\ell \nmid N^-$. Indeed, up to changing the embeddings ι_ℓ, we may force every maximal order $\mathcal{O}_B$ to have this property, since any maximal order of $\mathrm{M}_2(\mathbb{Q}_\ell)$ is conjugated with the order $\mathrm{M}_2(\mathbb{Z}_\ell)$ by Proposition 1.1.19.

Definition. For every positive integer M coprime with N^-, let $R_M \subseteq \mathcal{O}_B$ be an Eichler order of level M such that

$$\iota_\ell(R_M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell) = \begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^{v_\ell(M)}\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix} \subseteq \mathrm{M}_2(\mathbb{Q}_\ell)$$

for every prime $\ell \mid M$, where v_ℓ is the ℓ-adic valuation. Set also $U_0(M) = \hat{R}_M^\times$.

Definition. For every integer $m \geq 0$ let $U_1(p^m) \subseteq \hat{\mathcal{O}}_B^\times$ be the subgroup

$$U_1(p^m) = \hat{\mathcal{O}}_B^\times \cap \iota_p^{-1}\left\{\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^m\mathbb{Z}_p & 1 + p^m\mathbb{Z}_p \end{pmatrix}\right\},$$

where, by abuse of notation, ι_p is seen also as a function on $\hat{B}$ by pre-composing with the projection $\hat{B} \twoheadrightarrow B_p$.

Definition. For all $m \geq 0$, we define

$$U_{0;1}(N^+; p^m) = U_0(N^+) \cap U_1(p^m) = U_0(N^+p^m) \cap U_1(p^m).$$

Lemma 1.2.7. *Let U be any of the groups $U_0(M)$, $U_1(p^m)$ or $U_{0;1}(N^+;p^m)$, for any $M \nmid N^-$ and $m \geq 0$. Then U is open and compact in $\hat{B}^\times$ and $\mathrm{Nm}(U) = \hat{\mathbb{Z}}^\times$.*

Proof. The characterization of the topology of $\hat{B}^\times$ pursued in Subsection 1.1.6 immediately implies that $U_0(M)$ is open. Moreover, the induced topology on $U_0(M)$ coincides with the product topology coming from the equalities

$$U_0(M) = \hat{R}_M^\times = \prod_\ell (R_M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times;$$

therefore $U_0(M)$ is also compact by Lemma 1.1.23 and Tychonoff's theorem.

The group $U_1(p^m)$ is closed an open since it is defined as the intersection between a closed and open subgroup of $\hat{B}^\times$ with the preimage under a continous map of a closed and open set. Since $U_1(p^m)$ is contained in the compact set $\hat{\mathcal{O}}_B^\times$, it is also compact.

The group $U_{0;1}(N^+;p^m)$ is the intersection of two open and compact sets, hence it is open and compact.

Proposition 1.1.22 implies that $\mathrm{Nm}((R_M \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times) = \mathbb{Z}_\ell^\times$ for every prime ℓ, hence $\mathrm{Nm}(U_0(M)) = \hat{\mathbb{Z}}^\times$. For the same reason, we have that $\mathrm{Nm}(U_{0;1}(N^+;p^m)_\ell) = \mathbb{Z}_\ell^\times$ for every $\ell \neq p$. So it is enough to show that $\mathrm{Nm}(U_{0;1}(N^+;p^m)_p) = \mathbb{Z}_p^\times$. As noticed in Remark 1.1.10, the norm map on $U_{0;1}(N^+;p^m)_p$ corresponds via ι_p to the determinant map. It is easy to see that for every $x \in \mathbb{Z}_p^\times$ there is an invertible matrix in $\left\{\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^m\mathbb{Z}_p & 1+p^m\mathbb{Z}_p \end{pmatrix}\right\}$ with determinant x. Therefore $\mathrm{Nm}(U_{0;1}(N^+;p^m)) = \hat{\mathbb{Z}}^\times$. Since $U_{0;1}(N^+;p^m) \subseteq U_1(p^m) \subseteq \hat{\mathcal{O}}_B^\times$, we also have that $\mathrm{Nm}(U_1(p^m)) = \mathrm{Nm}(\hat{\mathbb{Z}}^\times)$. □

Definition. For every $m \geq 0$ and $M \nmid N^-$, define the compact Shimura $\mathbb{C}$-curves

$$\begin{aligned} X_{0;M}(\mathbb{C}) &:= X_{U_0(M)}(\mathbb{C}) \\ X_{1;m}(\mathbb{C}) &:= X_{U_1(p^m)}(\mathbb{C}) \\ X'_m(\mathbb{C}) &:= X_{U_{0;1}(N^+;p^m)}(\mathbb{C}). \end{aligned}$$

When $M = N^+p^m$, we also set

$$X_m := X_{0;N^+p^m}.$$

Corollary 1.2.8. *For every $M \nmid N^-$ and $m \geq 0$, the Riemann surfaces $X_{0;M}(\mathbb{C})$, $X_{1;m}(\mathbb{C})$ and $X'_m(\mathbb{C})$ are connected.*

Proof. Combine Lemma 1.2.3 with Lemma 1.2.7. □

Example 1.2.9. When B is the split algebra $\mathrm{M}_2(\mathbb{Q})$, we can choose $\mathcal{O}_B = \mathrm{M}_2(\mathbb{Z})$ and the embeddings ι_ℓ and ι_∞ to be the natural embeddings induced by tensorization with $\mathbb{Q}_\ell$ and $\mathbb{R}$ respectively. Moreover, we can take

$$R_{N^+} = \left\{\begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ N^+\mathbb{Z} & \mathbb{Z} \end{pmatrix}\right\}.$$

Then $B_1^\times = \mathrm{SL}_2(\mathbb{Q})$ and one can see that

$$\begin{aligned} U_0(M) \cap B_1^\times &= \Gamma_0(M) \\ U_1(p^m) \cap B_1^\times &= \Gamma_1(p^m) \\ U_{0;1}(N^+;p^m) \cap B_1^\times &= \Gamma_0(N^+) \cap \Gamma_1(p^m). \end{aligned}$$

This implies that, by Lemma 1.2.3, the Shimura $\mathbb{C}$-curves $X_{0;M}(\mathbb{C})$, $X_{1;m}(\mathbb{C})$ and $X'_m(\mathbb{C})$ coincide with the classical modular $\mathbb{C}$-curves of level $\Gamma_0(M)$, $\Gamma_1(p^m)$ and $\Gamma_0(N^+) \cap \Gamma_1(p^m)$ respectively.

Remark 1.2.10. The reader familiar with [LV11] will notice that our curve $X_m(\mathbb{C})$ corresponds exactly to the curve denoted in the same way in [LV11, §2.2] via the bijection defined in Remark 1.2.5. Indeed, the image via the canonical involution of the group $U_{0;1}(N^+;p^m)$ is the group called U_m in loc. cit.

1.3 Moduli interpretation and canonical models of Shimura curves

In this section we see that the Riemann surfaces $X_{0;M}(\mathbb{C})$, $X_{1;m}(\mathbb{C})$ and $X_m(\mathbb{C})$ consist of the complex points of some curves defined over $\mathbb{Q}$ that are solutions of some moduli problems related to families of abelian surfaces with some additional structure. For this section we use the following notation:

B	an indefinite quaternion algebra over $\mathbb{Q}$;
$\mathcal{O}_B$	the maximal order of B fixed at the beginning of Subsection 1.2.2;
N^-	the discriminant $\mathrm{disc}(B)$ of B;
N^+	a positive integer coprime with N^-;
N	the product N^+N^-;
p	the prime fixed in Subsection 1.2.2, with the property that $p \nmid 6N$.

1.3.1 Complex abelian surfaces

It is a classical result that the Weierstrass $\wp$-function induces a one-to-one correspondence between complex tori of dimension 1 and elliptic curves over $\mathbb{C}$ (see e.g. [DS05, §1.4]). When, instead, the dimension of the torus is greater than 1, it may happen that there are not enough meromorphic functions in order to realize the torus as a projective algebraic variety. In the following, we study conditions for a complex torus of dimension 2 to be an abelian variety, mainly following [Voi21, §43.4 and §43.5].

Definition. A complex torus of dimension 2 is a complex manifold $A = \mathbb{C}^2/\Lambda$ where $\Lambda \subseteq \mathbb{C}^2$ is a $\mathbb{Z}$-lattice of rank 4. A morphism of complex tori $\mathbb{C}^2/\Lambda \to \mathbb{C}^2/\Lambda'$ is a $\mathbb{C}$-linear map $\varphi : \mathbb{C}^2 \to \mathbb{C}^2$ such that $\varphi(\Lambda) \subseteq \Lambda'$. An isogeny of tori of dimension 2 is a surjective morphism with finite kernel.

Choose a $\mathbb{Z}$-basis $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ of Λ. The matrix $\Omega \in M_{2\times 4}(\mathbb{C})$ whose columns are the coordinates of $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ with respect to the canonical basis of $\mathbb{C}^2$ is called the big period matrix of the lattice Λ with respect to the basis $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$. Notice that

$$A = \mathbb{C}^2/\Lambda = \mathbb{C}^2/(\Omega\mathbb{Z}^4).$$

Definition. A complex torus A of dimension 2 is a complex abelian surface if there exists a holomorphic embedding $A \hookrightarrow \mathbb{P}^n(\mathbb{C})$ for some $n \geq 1$.

Definition. A matrix $\Omega \in M_{2\times 4}(\mathbb{C})$ is a Riemann matrix if there is a skew-symmetric matrix $E \in M_4(\mathbb{Z})$ with $\det(E) \neq 0$ such that

1. $E^{-1}\,{}^t\Omega = 0$;
2. $i\,E^{-1}\,{}^t\overline{\Omega}$ is a positive definite Hermitian matrix, where $i \in \mathbb{C}$ is the imaginary unit and $\overline{\Omega}$ denotes the conjugate of Ω.

Theorem 1.3.1. *Let $A = \mathbb{C}^2/(\ \mathbb{Z}^4)$ be a complex torus with $\in M_{2\times 4}(\mathbb{C})$. Then A is an abelian surface if and only if is a Riemann matrix.*

Proof. See [Voi21, Theorem 43.4.6]. □

We upgrade the above to a basis-free formulation.

Definition. Let $E : \times \to \mathbb{Z}$ be an alternating $\mathbb{Z}$-bilinear map. Let $E_{\mathbb{R}} : V \times V \to \mathbb{R}$ be the scalar extension of E over $\mathbb{R}$ obtained by $\otimes_{\mathbb{Z}} \mathbb{R} =: V \cong \mathbb{C}^2$. We say that E is a Riemann form for $(V; \ )$ if the following conditions hold:

1. $E_{\mathbb{R}}(ix; iy) = E_{\mathbb{R}}(x; y)$:
2. The map

$$\begin{aligned} V \times V &\longrightarrow \mathbb{R} \\ (x; y) &\longmapsto E_{\mathbb{R}}(ix; y) \end{aligned}$$

defines a symmetric positive definite $\mathbb{R}$-bilinear form on V.

As noted in [Voi21, §43.4.10], after choosing a $\mathbb{Z}$-basis for , the matrix associated to E is a Riemann matrix and, conversely, the form associated to the Riemann matrix is a Riemann form.

Proposition 1.3.2. *If E is a Riemann form for $(V; \ )$, then the map*

$$\begin{aligned} H : V \times V &\longrightarrow \mathbb{C} \\ (x; y) &\longmapsto E_{\mathbb{R}}(ix; y) + iE_{\mathbb{R}}(x; y) \end{aligned}$$

is a positive definite Hermitian form on V.

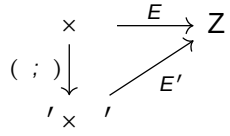
Conversely, if H is a positive definite Hermitian form on V such that $\operatorname{Im} H(\ )$ is contained in $\mathbb{Z}$, then $\operatorname{Im} H|$ is a Riemann form for $(V; \ )$ (here, Im denotes the imaginary part operator).

Proof. See [Voi21, Proposition 43.4.11]. □

The form H of the previous proposition is called the Hermitian form associated with E.

Definition. A complex torus $A = \mathbb{C}^2/$ equipped with a Riemann form is said to be polarized.

A morphism between two polarized complex tori $(\mathbb{C}^2/ \ ; E)$ and $(\mathbb{C}^2/ \ '; E')$ is a morphism $: \mathbb{C}^2/ \to \mathbb{C}^2/ \ '$ of complex tori that respects the polarizations, in the sense that the diagram



commutes.

Theorem 1.3.3. *A complex torus of dimension 2 is an abelian surface if and only if it is polarizable.*

Proof. See [Mil08, Theorem 2.8]. □

There is a normal form for skew-symmetric matrices, called Frobenius normal form. Namely, there is a basis of such that the matrix of E in this basis is $\left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)$, where D is a diagonal 2×2 matrix with entries in $\mathbb{Z}_{\geq 0}$.

Definition. A Riemann form E whose matrix D in the Frobenius normal form is the identity is called a principal Riemann form.

Following [Voi21, §43.4.19], we want to understand polarizations in terms of duality. In order to do that, let $A = V/$ be a complex torus of dimension 2, where $V \cong \mathbb{C}^2$.

Definition. A $\mathbb{C}$-antilinear functional on V is a function $f : V \to \mathbb{C}$ such that

1. $f(x + x') = f(x) + f(x')$ for every $x; x' \in V$;
2. $f(ax) = af(x)$ for every $a \in \mathbb{C}$ and $x \in V$.

Call V^* the $\mathbb{C}$-vector space of $\mathbb{C}$-antilinear functionals on V.

Then V^* is a $\mathbb{C}$-vector space with $\dim_{\mathbb{C}} V^* = \dim_{\mathbb{C}} V = 2$ and the underlying $\mathbb{R}$-vector space of V^* is canonically isomorphic to $\mathrm{Hom}_{\mathbb{R}}(V; \mathbb{R})$. The canonical $\mathbb{R}$-bilinear form

$$\begin{aligned} V^* \times V &\longrightarrow \mathbb{R} \\ (f; x) &\longmapsto \operatorname{Im} f(x) \end{aligned}$$

is nondegenerate, so

$$^* := \{ f \in V^* \ : \ \operatorname{Im} f(\ ) \subseteq \mathbb{Z} \}$$

is a lattice in V^*, called the dual lattice of , hence the quotient $A^\vee := V^*/\ ^*$ is a complex torus of dimension 2. Double antiduality and nondegeneracy gives a canonical identification $(V^*)^* \cong V$, giving a canonical identification $(A^\vee)^\vee \cong A$.

Suppose now that A is polarized with a Riemann form E for $(V; \ )$, and let H be the associated Hermitian form. Double duality induces a Riemann form E^* on $(V^*; \ ^*)$, so $A^\vee$ is a polarized abelian surface. There is a $\mathbb{C}$-linear map

$$\begin{aligned} {}_E : V &\longrightarrow V^* \\ x &\longmapsto H(x; -) \end{aligned}$$

with the property that ${}_E(\ ) \subseteq \ ^*$. Since the form H is nondegenerate, the induced homomorphism ${}_E : A \to A^\vee$ is an isogeny of polarized abelian varieties.

Lemma 1.3.4. *The degree of the isogeny ${}_E$ is the determinant of the matrix D appearing in the Frobenius normal form for E.*

Proof. See [Voi21, §43.4.19] □

In particular, if E is principal then ${}_E$ is an isomorphism of principally polarized abelian surfaces. In this case, we define the Rosati involution associated with E by

$$\begin{aligned} {}^\dagger : \ \operatorname{End}(A) &\longrightarrow \operatorname{End}(A) \\ &\longmapsto \ ^\dagger = {}_E^{-1} \circ \ ^\vee \circ \ {}_E; \end{aligned}$$

where $\operatorname{End}(A)$ is the set of endomorphisms of A as a complex torus (or, equivalently, as an abelian variety) and $^\vee : A^\vee \to A^\vee$ is the morphism induced by the pullback.

Definition. Let D be a finitely dimensional Q-algebra. We say that an involution $^* : D \to D$ is positive if $\mathrm{Tr}(\ \ ^*) > 0$ for all $\ \in D \setminus \{0\}$, where $\mathrm{Tr} : D \to \mathbb{Q}$ is the trace of the left multiplication operator.

Proposition 1.3.5. *Let A be a principally polarized complex abelian surface. The Rosati involution † is a positive involution on the* Q*-algebra* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. See [Voi21, Proposition 43.4.24]. □

Theorem 1.3.6 (Albert). *Let A be a principally polarized complex abelian surface. The* Q*-algebra $D = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is exactly one of the following:*

(i) $D = \mathbb{Q}$*, and we say that A is* ***typical****;*

(ii) $D = F$ *is a real quadratic field, and we say that A has* ***real multiplication****;*

(iii) $D = K$ *is a quartic CM field K;*

(iv) $D = B$ *is an indefinite quaternion algebra over* Q*;*

(v) $D = \mathrm{M}_2(K)$ *where K is an imaginary quadratic field.*

Proof. See [Voi21, §43.5.9]. □

Definition. Let A be a principally polarized complex abelian surface. We say that A has complex multiplication (CM) if $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a CM field.

If A has complex multiplication, then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ satisfies cases (iii) or (v) of Theorem 1.3.6. Let now B be an indefinite quaternion algebra and $\mathcal{O}_B$ be a maximal order in B.

Definition. Let A be a principally polarized complex abelian surface. We say that A has quaternionic multiplication (QM) by $\mathcal{O}_B$ if there is an injective ring homomorphism $i : \mathcal{O}_B \hookrightarrow \mathrm{End}(A)$.

If A has quaternionic multiplication by $\mathcal{O}_B$, then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ satisfies cases (iv) or (v) of Theorem 1.3.6. Abelian surfaces with QM are sometimes called *false elliptic curves*. We now specialize to the study of abelian surfaces with QM.

1.3.2 Complex abelian surfaces with QM

Recall that we fixed an indefinite quaternion algebra B over Q with discriminant N^- and a maximal order $\mathcal{O}_B$. Throughout, let A be a complex abelian surface.

Lemma 1.3.7. *There is an element $t \in \mathcal{O}_B$ such that $t^2 = -N^-$.*

Proof. Combining Proposition 1.1.26 and Corollary 1.1.27 we obtain that there is an embedding of $\mathbb{Q}(\sqrt{-N^-})$ in B. Therefore there is $t' \in B$ such that $(t')^2 = -N^-$, and t' lies in a maximal order $\mathcal{O}'$ of B. By Proposition 1.1.35 any two maximal orders are $B^\times$-conjugate, so there is a conjugate $t \in \mathcal{O}_B$ that satisfies $t^2 = -N^-$. □

From now on we fix $t \in \mathcal{O}_B$ with the property that $t^2 = -N^-$. Indeed, we could fix the couple $\{t; -t\}$, since our construction will be independent on the sign. Notice anyway that a priori there are many such couples of elements, depending on the number of embeddings of the ring of integers of $\mathbb{Q}(\sqrt{-N^-})$ in $\mathcal{O}_B$.

To the element t we attach the positive involution

$$\begin{aligned} {}^{\star} : B &\longrightarrow B \\ b &\longmapsto b^{\star} = t^{-1}b^{*}t; \end{aligned} \tag{1.5}$$

where * is the standard involution of B.

Definition. A quaternionic multiplication (QM) structure by $\mathcal{O}_B$ on A is an injective ring homomorphism $i : \mathcal{O}_B \hookrightarrow \mathrm{End}(A)$. In this case, we say that $(A; i)$ is an abelian surface with QM by $\mathcal{O}_B$.

Definition. A morphism $(A; i) \to (A'; i')$ of complex abelian surfaces with QM by $\mathcal{O}_B$ is a morphism of abelian surfaces that also respects $i; i'$, i.e. such that

$$i'(b) \ \ (a) = \ \ (i(b)a)$$

for every $a \in A$ and $b \in \mathcal{O}_B$. An isogeny is a surjective homomorphism with finite kernel.

Definition. A principal polarization E on a complex abelian surface $(A; i)$ with QM by $\mathcal{O}_B$ is compatible with the the couple $(\mathcal{O}_B; t)$ if the induced homomorphism $i : B \hookrightarrow \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ respects involutions, i.e. the diagram

$$\begin{array}{ccc} B & \xrightarrow{i} & \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \\ \downarrow{\scriptstyle \star} & & \downarrow{\scriptstyle \dagger} \\ B & \xrightarrow{i} & \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \end{array}$$

commutes, where * is the involution defined in (1.5) and † is the Rosati involution attached to E.

Theorem 1.3.8. *Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$. Then there is a unique principal polarization on A compatible with the couple $(\mathcal{O}_B; t)$.*

Proof. See [Voi21, Remark 43.6.27]. □

Thanks to this theorem, from now on we will just say "abelian surfaces with QM" instead of "principally polarized abelian surfaces with QM", understanding that every such surface is endowed with the unique principal polarization coming from our choice of t. Morally, we can say that we settled the problem about polarizations and from now on we can forget about them.

Lemma 1.3.9. *Let A_2 be an abelian surface, $(A_1; i_1)$ be an abelian surface with QM by $\mathcal{O}_B$ and $: A_1 \twoheadrightarrow A_2$ an isogeny with* ker *stable under $i_1(\mathcal{O}_B)$. Then there is a unique quaternionic multiplication $i_2 : \mathcal{O}_B \hookrightarrow \mathrm{End}(A_2)$ characterized by the property*

$$i_2(b) \cdot \ \ (a) = \ \ (i_1(b) \cdot a)$$

for every $b \in \mathcal{O}_B$ and $a \in A_1$.

Proof. In order to see that i_2 is well defined, take $a; a' \in A_1$ such that $\ \ (a) = \ \ (a')$, i.e. $a - a' \in \ker(\ \ )$. Then

$$(i_1(b) \cdot a) - \ \ (i_1(b) \cdot a') = \ \ (i_1(b) \cdot (a - a')) = 0$$

for every $b \in \mathcal{O}_B$, since ker is stable under $i_1(\mathcal{O}_B)$. This implies that i_2 is well defined.

In order to verify injectivity, take $b \in \mathcal{O}_B$ such that $i_2(b) \cdot (a) = 0$ for every $a \in A_1$. This implies that $(i_1(b) \cdot a) = 0$, i.e. $i_1(b) \cdot a \in \ker$ for every $a \in A_1$. Since ker is finite, this means that $i_1(b)$ has finite image, hence it is the zero morphism. The injectivity of i_1 implies that $b = 0$. □

Example 1.3.10. ([Voi21, §43.6.12]). Extend the embedding $_\infty$ fixed at the beginning of Section 1.2 to a map $_\infty : B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathrm{M}_2(\mathbb{C})$. Let be an element of the upper half plane $\mathcal{H}$ of $\mathbb{C}$. Define the lattice

$$:= {}_\infty(\mathcal{O}_B)\begin{pmatrix} \\ 1 \end{pmatrix} \subseteq \mathbb{C}^2$$

and let $A := \mathbb{C}^2/$ be the associated complex torus. The map $_\infty$ induces a natural injective ring homomorphism $i : \mathcal{O}_B \hookrightarrow \mathrm{End}(A)$ by left multiplication, since $_\infty(\mathcal{O}_B) \subseteq$, hence the couple $(A; i)$ is an abelian surface with QM by $\mathcal{O}_B$.

Proposition 1.3.11. *Every complex abelian surface with QM by $\mathcal{O}_B$ is isomorphic as such to one of the form $(A; i)$ for some $\in \mathcal{H}$.*

Proof. See [Voi21, Proposition 43.6.28]. □

Quaternionic action on torsion points

We give now a deeper look at the action of $\mathcal{O}_B$ on the torsion points of A. First of all, notice that if $(A; i)$ is a complex abelian surface with QM by $\mathcal{O}_B$ and M is a positive integer, there is an induced action of $\mathcal{O}_B$ on $A[M]$ that factors through $\mathcal{O}_B/M\mathcal{O}_B$.

Let now $M \in \mathbb{Z}_{>0}$ be coprime with N^-. Take $m \in \mathbb{Z}_{>0}$ and a prime ℓ such that $\ell^m \mid M$. The chosen isomorphism $_\ell : \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{M}_2(\mathbb{Z}_\ell)$ induces an isomorphism

$$\mathcal{O}_B/\ell^m\mathcal{O}_B = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^m\mathbb{Z} = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^m\mathbb{Z} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^m\mathbb{Z} = \mathrm{M}_2(\mathbb{Z}/\ell^m\mathbb{Z});$$

where the equal signs correspond to canonical isomorphisms. The Chinese remainder theorem then yields an isomorphism

$$_M : \mathcal{O}_B/M\mathcal{O}_B \xrightarrow{\cong} \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z}) \tag{1.6}$$

that only depends on the chosen embeddings $_\ell$ for all primes $\ell \mid M$. Therefore, the left $\mathcal{O}_B$-action on $A[M]$ induced by i can be interpreted as a left action of $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$.

Lemma 1.3.12. *Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and M be a positive integer coprime with N^-. Let $e_M := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $f_M := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ in $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$.*

(i) $A[M]$ splits as $\mathrm{Im}(e_M) \times \mathrm{Im}(1 - e_M)$ as a group.

(ii) The action of f_M induces an isomorphism between $\ker(e_M)$ and $\ker(1 - e_M)$.

Proof. (i) Since $P = e_M P + (1 - e_M)P$ for every $P \in A[M]$, we obtain the equality $A[M] = \mathrm{Im}(e_M) + \mathrm{Im}(1 - e_M)$. On the other hand, if there are $P; Q \in A[M]$ such that $e_M P = (1 - e_M)Q$, then $e_M P = e_M^2 P = e_M(1 - e_M)Q = O$, therefore the sum is direct.

(ii) Since f_M is invertible in $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$, it induces an isomorphism of $A[M]$. The equalities $e_M f_M e_M = 0$ and $(1-e_M)f_M(1-e_M) = 0$ together imply that $f_M(\mathrm{Im}(e_M)) \subseteq \mathrm{Im}(1-e_M)$ and $f_M(\mathrm{Im}(1-e_M)) \subseteq \mathrm{Im}(e_M)$. Since $f_M^2 = 1$, applying f_M to the previous relations we obtain that converse inclusions. □

Since $A[M] \cong (\mathbb{Z}/M\mathbb{Z})^4$ as groups, this lemma implies that both $\mathrm{Im}(e_M)$ and $\mathrm{Im}(1-e_M)$ are isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$ as abelian groups. It can also be seen easily that $\mathrm{Im}(e_M) = \ker(1-e_M)$ and viceversa.

Proposition 1.3.13. *Keep the notation as in Lemma 1.3.12 and fix a basis P_1, P_2 for $\mathrm{Im}(e_M)$ as a $\mathbb{Z}/M\mathbb{Z}$-module. Call $P_1' = f_M P_1$ and $P_2' = f_M P_2$. Then the map*

$$\begin{aligned} : A[M] = \mathrm{Im}(e_M) \times \mathrm{Im}(1-e_M) &\longrightarrow \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z}) \\ aP_1 + bP_2 + cP_1' + dP_2' &\longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

is a (noncanonical) isomorphism of left $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$-modules, where the action on the codomain is via left multiplication.

Proof. It is straightforward to see that the map is an isomorphism of abelian groups, therefore we just need to prove that is $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$-invariant. Notice that $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$ is generated as a $\mathbb{Z}/M\mathbb{Z}$-algebra by the three elements 1, e_M and f_M, therefore we just need to check the compatibility of with respect to the action of the last two elements. So let $Q = aP_1 + bP_2 + cP_1' + dP_2'$. Then

$$(e_M Q) = \quad (aP_1 + bP_2) = \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) = e_M \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = e_M \quad (Q):$$

Similarly,

$$(f_M Q) = \quad (cP_1 + dP_2 + aP_1' + bP_2') = \left(\begin{smallmatrix} c & d \\ a & b \end{smallmatrix}\right) = f_M \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = f_M \quad (Q):$$

□

This proposition, together with the isomorphism of (1.6), implies that $A[M]$ and $\mathcal{O}_B/M\mathcal{O}_B$ are isomorphic as left $\mathcal{O}_B$-modules. On the other hand, this isomorphism is not canonical. We will see in the next section that choosing such isomorphisms has something to do with the choice of a *level structure* on $(A;i)$. We now study $\mathcal{O}_B$-submodules of $A[M]$.

Lemma 1.3.14. *Let $(A;i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and let M be a positive integer coprime with N^-. Then there is a bijection*

$$\begin{aligned} \{\text{subgroups of } \mathrm{Im}(e_M)\} &\leftrightarrow \{\mathcal{O}_B\text{-submodules of } A[M]\} \\ C &\mapsto C \times f_M C \\ e_M(D) &\hookleftarrow D \end{aligned}$$

that restricts to a bijection

$$\left\{\text{cyclic subgroups of } \mathrm{Im}(e_M) \text{ of order } M'\right\} \leftrightarrow \left\{\begin{matrix}\text{cyclic } \mathcal{O}_B\text{-submodules of } A[M] \\ \text{isomorphic to } (\mathbb{Z}/M'\mathbb{Z})^2\end{matrix}\right\};$$

for every $M' \mid M$.

Proof. Let C be a subgroup of $\mathrm{Im}(e_M)$. The action of $\mathcal{O}_B$ corresponds to the left action of elements of $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$, and this last ring is generated by $1; e_M; f_M$. Therefore, the subgroup $C \times f_M C$ is an $\mathcal{O}_B$-submodule of $A[M]$.

On the other hand, let D be an $\mathcal{O}_B$-submodule of $A[M]$. Then the action of e_M restricts to D, therefore we may decompose $D = e_M(D) \times (1 - e_M)D$. Since also the action of f_M restricts to D, it induces an isomorphism between $e_M(D)$ and $(1 - e_M)D$. Therefore, we have the claimed bijection. □

Remark 1.3.15. In the case that M is a squarefree product of primes, the bijection of Lemma 1.3.14 restricts to a bijection

$$\left\{\text{cyclic subgroups of } \mathrm{Im}(e_M) \text{ of order } M'\right\} \leftrightarrow \left\{\begin{matrix}\text{cyclic } \mathcal{O}_B\text{-submodules of } A[M] \\ \text{of order } (M')^2\end{matrix}\right\};$$

for every $M' \mid M$. If, instead, M is not squarefree, this is false. Set for example $M = M' = \ell^2$ for a prime $\ell \nmid N^-$. Choosing an isomorphism $A[M] \cong \mathrm{M}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, one can see that the element $\left(\begin{smallmatrix}\ell & 0 \\ 0 & \ell\end{smallmatrix}\right)$ generates an $\mathrm{M}_2(\mathbb{Z}/\ell^2\mathbb{Z})$-submodule of $\mathrm{M}_2(\mathbb{Z}/\ell^2\mathbb{Z})$ of cardinality ℓ^4, but its projection to the e_{ℓ^2}-part is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$.

1.3.3 Level structures and moduli interpretation

In this subsection we show that the Shimura C-curves parametrize families of complex abelian varieties with QM and fixed level structure. We mainly follow [Mil79, §1] and [Buz97]. See also [Mag22, §2]. Our first aim is to define level structures on complex abelian surfaces with QM by $\mathcal{O}_B$ associated to open compact subgroups of $\hat{\mathcal{O}}_B^\times$. In literature, there are many different definitions of such objects: we check that they are all equivalent.

Milne's level structures

Definition. Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$. The (complete) Tate module of A is the inverse limit of the M-torsion groups of A

$$T(A) := \varprojlim_M A[M].$$

The structure theory of finite abelian groups implies that $T(A) \cong \prod_\ell T_\ell(A)$, where the product is taken among all primes ℓ and $T_\ell(A) = \varprojlim_m A[\ell^m]$ is the usual ℓ-adic Tate module of A.

By Proposition 1.3.13 we know that $A[M]$ and $\mathcal{O}_B/M\mathcal{O}_B$ are (noncanonically) isomorphic as left $\mathcal{O}_B$-modules, for every $M \nmid N^-$. One can prove that their profinite completions $T(A)$ and $\hat{\mathcal{O}}_B$ are isomorphic as left $\hat{\mathcal{O}}_B$-modules (see [Mil79, §1]). One can see this also noting that, by Proposition 1.3.11, $(A; i)$ is isomorphic to a QM abelian surface $(\mathbb{C}/\quad; i\ )$ for some $\in \mathcal{H}$ (see Example 1.3.10). Using the explicit description of , one can easily build an isomorphism $A[M] \cong \mathcal{O}_B/M\mathcal{O}_B$ for every positive M, yielding the desired isomorphism $T(A) \cong \hat{\mathcal{O}}_B$ as left $\hat{\mathcal{O}}_B$-modules.

Definition. Let U be an open compact subgroup of $\hat{\mathcal{O}}_B^\times$. Two isomorphisms of left $\hat{\mathcal{O}}_B$-modules $_1;\ _2 : \hat{\mathcal{O}}_B \to T(A)$ are U-equivalent if there is $u \in U$ such that $_1 = \ _2 \circ r_u$, where r_u is right multiplication by u.

The map $\mapsto \ \circ r_b$ for $b \in \hat{\mathcal{O}}_B^\times$ defines a left action of $\hat{\mathcal{O}}_B^\times$ on the set of $\hat{\mathcal{O}}_B$-isomorphisms between $\hat{\mathcal{O}}_B$ and $T(A)$.

Lemma 1.3.16. *The action of $\hat{\mathcal{O}}_B^\times$ on the set of $\hat{\mathcal{O}}_B$-isomorphisms between $\hat{\mathcal{O}}_B$ and $T(A)$ is free and transitive.*

Proof. Let $\varphi : \hat{\mathcal{O}}_B \to T(A)$ be an $\hat{\mathcal{O}}_B$-isomorphism and let $b \in \hat{\mathcal{O}}_B^\times$ with the property that $\varphi = \varphi \circ r_b$. Then, for every $b' \in \hat{\mathcal{O}}_B$, we have $\varphi(b') = \varphi(r_b(b')) = \varphi(b'b)$. Since φ is an isomorphism, this implies that $b' = b'b$. Choosing $b' = b^{-1}$, we obtain that $b^{-1} = 1$, hence $b = 1$. Therefore, the action is free.

Let now $\varphi_1, \varphi_2 : \hat{\mathcal{O}}_B \to T(A)$ be $\hat{\mathcal{O}}_B$-isomorphisms. Then $\varphi_2^{-1} \circ \varphi_1 : \hat{\mathcal{O}}_B \to \hat{\mathcal{O}}_B$ is an isomorphism of left $\hat{\mathcal{O}}_B$-modules. Basic non-commutative algebra implies that there is an element $\alpha \in \hat{\mathcal{O}}_B^\times$ such that $\varphi_2^{-1} \circ \varphi_1 = r_\alpha$ (more precisely, $\alpha := \varphi_2^{-1}(\varphi_1(1))$). Hence $\varphi_1 = \varphi_2 \circ r_\alpha$, therefore the action is transitive. □

Let U_1 and U_2 be two open compact subgroups of $\hat{\mathcal{O}}_B^\times$. The previous lemma implies that if A is a set of $\hat{\mathcal{O}}_B$-isomorphisms between $\hat{\mathcal{O}}_B$ and $T(A)$ that is a U_1-equivalence class and a U_2-equivalence class (with respect to the action defined above), then $U_1 = U_2$.

Definition ([Mil79]). Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and let U be an open compact subgroup of $\hat{\mathcal{O}}_B^\times$. A U-level structure A_U on $(A; i)$ is a U-equivalence class of $\hat{\mathcal{O}}_B$-isomorphisms between $\hat{\mathcal{O}}_B$ and $T(A)$. The triple $(A; i; A_U)$ is called a U-triple.

Definition. Let $(A; i; A_U)$ and $(A'; i'; A'_U)$ be two U-triples, for some open compact subgroup U contained in $\hat{\mathcal{O}}_B^\times$. An isomorphism between U-triples is an isomorphism $\varphi : (A; i) \to (A'; i')$ of QM abelian surfaces such that the map

$$\hat{\mathcal{O}}_B \longrightarrow T(A) \xrightarrow{\hat{\varphi}} T(A')$$

lies in A'_U for every $\alpha \in A_U$, where $\hat{\varphi}$ denotes the map induced by φ.

Definition. Let U be an open compact subgroup of $\hat{\mathcal{O}}_B^\times$. We define $\mathcal{C}_U$ to be the category whose objects are U-triples and whose morphisms are isomorphism of U-triples.

Equivalence classes of full level structures

Let M be a positive integer coprime with N^-.

Definition ([Buz97]). Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and $M \nmid N^-$. A full level M structure on $(A; i)$ is an $\mathcal{O}_B$-modules isomorphism

$$\varphi : \mathcal{O}_B/M\mathcal{O}_B \xrightarrow{\cong} A[M].$$

Let $\alpha \in (\mathcal{O}_B/M\mathcal{O}_B)^\times$ and call r_α the right multiplication by α on $\mathcal{O}_B/M\mathcal{O}_B$. For any full level M structure φ, the map $\varphi \mapsto \varphi \circ r_\alpha$ induces a left action of $(\mathcal{O}_B/M\mathcal{O}_B)^\times$ on the set of full level M structures on A.

Lemma 1.3.17. *The action of $(\mathcal{O}_B/M\mathcal{O}_B)^\times$ on the set full level M structures of $(A; i)$ is free and transitive.*

Proof. Follow verbatim the proof of Lemma 1.3.16, mutatis mutandis. □

Definition. Let H be a subgroup of $(\mathcal{O}_B/M\mathcal{O}_B)^\times \cong \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Two full level M structures φ_1, φ_2 on $(A; i)$ are H-equivalent if there is $h \in H$ such that $\varphi_1 = \varphi_2 \circ r_h$.

Let H_1 and H_2 be two subgroups of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Lemma 1.3.17 implies that if A is a set of full level M structures that is an H_1-equivalence class and an H_2-equivalence class, then $H_1 = H_2$.

Definition ([Buz97]). Let $(A; i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. An H-level structure A_H on $(A; i)$ is a H-equivalence class of full level M structures. The triple $(A; i; A_H)$ is called an H-triple.

Definition. Let M be a positive integer coprime with N^-. Let $(A; i; A_H)$ and $(A'; i'; A'_H)$ be two H-triples, for a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. An isomorphism of H-triples is an isomorphism $\varphi : (A; i) \to (A'; i')$ of QM abelian surfaces such that the map

$$\mathcal{O}_B/M\mathcal{O}_B \longrightarrow A[M] \longrightarrow A'[M]$$

lies in A'_H for every $\alpha \in A_H$.

Definition. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. We define $\mathcal{C}_H$ to be the category whose objects are H-triples and whose morphisms are isomorphism of H-triples.

A first equivalence between level structures

Notice that the isomorphism ε_M of (1.6) induces also a natural surjective map

$$\varepsilon_M : \hat{\mathcal{O}}_B = \mathcal{O}_B \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \twoheadrightarrow \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}/M\mathbb{Z} = \mathcal{O}_B/M\mathcal{O}_B \xrightarrow{\varepsilon_M} \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$$

and, on invertible elements, $\varepsilon_M : \hat{\mathcal{O}}_B^\times \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ and $U = \varepsilon_M^{-1}(H) \subseteq \hat{\mathcal{O}}_B^\times$. Define a functor $\Phi : \mathcal{C}_U \to \mathcal{C}_H$ in the following way:

- If $(A; i; A_U)$ is an object of $\mathcal{C}_U$, then its image under the functor Φ is the H-triple $(A; i; \Phi(A_U))$ where $\Phi(A_U)$ is the set of full level M structures induced by any $\alpha \in A_U$ via the commutative diagram

$$\begin{array}{ccc} \hat{\mathcal{O}}_B & \longrightarrow & T(A) \\ \downarrow{\scriptstyle \varepsilon_M} & & \downarrow \\ \mathcal{O}_B/M\mathcal{O}_B & \longrightarrow & A[M] \end{array} \tag{1.7}$$

  of $\mathcal{O}_B$-modules.

- If $\varphi : (A; i; A_U) \to (A'; i'; A'_U)$ is a morphism between objects of $\mathcal{C}_U$, call with the same letter φ the induced isomorphism between abelian surfaces with QM. Then $\Phi(\varphi) : (A; i; \Phi(A_U)) \to (A'; i'; \Phi(A'_U))$ is the morphism of $\mathcal{C}_H$ that has φ as underlying isomorphism between abelian surfaces with QM.

The following lemma gives some highlights on why Φ is a well defined functor.

Lemma 1.3.18. *With notation as above, we have the following:*

(i) $\Phi(A_U)$ *is an* H*-level structure for* A*.*

(ii) $\Phi(\varphi)$ *is a morphism of* H*-triples.*

Proof. (i) Let $\ ;\ ' \in A_U$. Then there is an element $u \in U$ such that $= \ ' \circ r_u$. Since $H = \ _M(U)$, the element $\ _M(u)$ lies in H and, following the diagram in equation (1.7), we have that $= \ ' \circ r_{\ _M(u)}$. This implies that $\ (A_U)$ contains an H-level structure. But now, if $\in \ (A_U)$ and $\sim := \ \circ r_h$ for some $h \in H$, then calling $\ $ an element of A_U corresponding to $\ $ via $\ $ and taking $u \in U$ such that $\ _M(u) = h$, it is easy to see that $(\ \circ r_u) \ = \sim$. Therefore $\ (A_U)$ is also contained in an H-level structure.

(ii) We need to prove that any isomorphism $\ : (A; i; A_U) \to (A'; i'; A'_U)$ of U-triples preserves also the induced H-level structures $\ (A_U)$ and $\ (A'_U)$. This is straightforward noting that, for every $\ \in A_U$, the diagram

$$\begin{array}{ccccc} \mathcal{O}_B & \longrightarrow & T(A) & \xrightarrow{\ \hat{}\ } & T(A') \\ \big\downarrow{\scriptstyle M} & & \big\downarrow & & \big\downarrow \\ \mathcal{O}_B/M\mathcal{O}_B & \longrightarrow & A[M] & \longrightarrow & A'[M] \end{array}$$

is commutative. □

Proposition 1.3.19. *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ and $U = \ ^{-1}_M(H)$. The functor $\ : \mathcal{C}_U \to \mathcal{C}_H$ defined above is an isomorphism of categories.*

Proof. (Idea). Using almost the same ideas as before, it is possible to build a functor $\ : \mathcal{C}_H \to \mathcal{C}_U$ in the following way.

If $(A; i; A_H)$ is an object of $\mathcal{C}_H$, then its image under $\ $ is the triple $(A; i; \ (A_H))$ where $\ (A_H)$ is set of all isomorphisms $\ $ that make the following diagram commutative

$$\begin{array}{ccc} \mathcal{O}_B & \longrightarrow & T(A) \\ \big\downarrow{\scriptstyle M} & & \big\downarrow \\ \mathcal{O}_B/M\mathcal{O}_B & \longrightarrow & A[M] \end{array}$$

for every $\ \in A_H$. If $\ : (A; i; A_H) \to (A'; i'; A'_H)$ is a morphism of objects of $\mathcal{C}_H$, call with the same letter $\ $ the induced isomorphism between abelian surfaces with QM. Then $(\ \ ) : (A; i; \ (A_H)) \to (A'; i'; \ (A'_H))$ is the morphism of $\mathcal{C}_U$ that has $\ $ as underlying isomorphism between abelian surfaces with QM.

Following the ideas of Lemma 1.3.18 one can prove that $\ $ is a well defined functor. It is also not hard to show that $\ = 1_{\mathcal{C}_H}$ and $\ = 1_{\mathcal{C}_U}$ as functors, giving the claimed isomorphism. □

Now we know that, whenever H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ and $U = \ ^{-1}_M(H)$, working with (isomorphism classes of) U-triples *is the same as* working with (isomorphism classes of) H-triples.

1.3.4 Level structures attached to $X_{0;M}$, $X_{1;m}$ and X'_m

We now give a more explicit interpretation of the level structures associated with the Shimura C-curves $X_{0;M}(\mathbb{C})$, $X_{1;m}(\mathbb{C})$ and $X'_m(\mathbb{C})$ defined in Subsection 1.2.2. For every $m \geq 0$ and $M + N^-$ define the groups

$$\begin{aligned} H_0(M) &= \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) \ : \ a; b; d \in \mathbb{Z}/M\mathbb{Z} \right\}; \\ H_1(p^m) &= \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z}) \ : \ a; b \in \mathbb{Z}/p^m\mathbb{Z} \right\}; \\ H_{0;1}(N^+; p^m) &= \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N^+p^m\mathbb{Z}) \ : \ a; b; d \in \mathbb{Z}/N^+p^m\mathbb{Z} \text{ and } d \equiv 1 \bmod p^m \right\}: \end{aligned}$$

Since we have that

$$\begin{aligned} U_0(M) &= \tfrac{-1}{N^+}(H_0(M)); \\ U_1(p^m) &= \tfrac{-1}{p^m}(H_1(p^m)); \\ U_{0;1}(N^+;p^m) &= \tfrac{-1}{N^+p^m}(H_{0;1}(N^+;p^m)) \end{aligned}$$

as subgroups of $\hat{\mathcal{O}}_B^\times$, the result of Proposition 1.3.19 is valid for these groups. We want to give an even more explicit notion of level structures for these three cases.

Let $(A;i)$ be a complex abelian surface with QM by $\mathcal{O}_B$. In Lemma 1.3.12 we defined the idempotent element e_M that acts on $A[M]$ and gives the decomposition $A[M] = \mathrm{Im}(e_M) \times \mathrm{Im}(1-e_M)$.

Definition. A $V_0(M)$-triple is a triple $(A;i;C)$ where $(A;i)$ is a complex abelian surface with QM by $\mathcal{O}_B$ and C is an $\mathcal{O}_B$-cyclic submodule of $A[M]$ isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$. The group C is called a $V_0(M)$-level structure on $(A;i)$.

By Lemma 1.3.14 any $\mathcal{O}_B$-cyclic submodule C of $A[M]$ isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$ decomposes as $C = e_M(C) \times (1-e_M)C$ and is uniquely determined by the M-cyclic group $e_M(C)$. Therefore, a $V_0(M)$-level structure on $(A;i)$ is equivalent to the choice of an M-cyclic subgroup of $\mathrm{Im}(e_M)$.

Definition. An isomorphism $\quad : (A;i;C) \to (A';i';C')$ of $V_0(M)$-triples is an isomorphism $\quad : (A;i) \to (A';i')$ of abelian surfaces with QM such that $\quad(C) = C'$.

Definition. We define $\mathcal{C}_0(M)$ to be the category whose objects are $V_0(M)$-triples and whose morphisms are isomorphisms of $V_0(M)$-triples.

Lemma 1.3.20. *The categories $\mathcal{C}_{H_0(M)}$ and $\mathcal{C}_0(M)$ are isomorphic.*

Proof. We build an explicit isomorphism $\quad : \mathcal{C}_{H_0(M)} \to \mathcal{C}_0(M)$ and its inverse.

Take $(A;i;A\ )$ to be an object of $\mathcal{C}_{H_0(M)}$, so that $A\ $ is an $H_0(M)$-equivalence class of full level M structures. Take $\ \in A\ $. The isomorphism $\ _M$ of (1.6) allows us to see $\ $ as an isomorphism

$$: \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z}) \xrightarrow{\cong} A[M]$$

of $\mathcal{O}_B$-modules, where $\mathcal{O}_B$ acts on the domain by left multiplication by the image of the map

$$\mathcal{O}_B \twoheadrightarrow \mathcal{O}_B/M\mathcal{O}_B \xrightarrow{\ M\ } \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z}):$$

Similarly, the right multiplication by elements of $(\mathcal{O}_B/M\mathcal{O}_B)^\times$ on $\mathcal{O}_B/M\mathcal{O}_B$ corresponds to the right multiplication of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ on $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$. The group of matrices

$$L_0 := \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}/M\mathbb{Z}) \ : \ b;d \in \mathbb{Z}/M\mathbb{Z} \right\}$$

is an $\mathcal{O}_B$-cyclic submodule of $\mathrm{M}_2(\mathbb{Z}/M\mathbb{Z})$, isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$ as an abelian group. Therefore its image $C_A := \ (L_0)$ is a well determined $\mathcal{O}_B$-cyclic submodule of $A[M]$ isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$. A straightforward computation shows that right multiplication by elements of $H_0(M)$ stabilizes L_0. Therefore, for any other $\ ' \in A\ $, we still have that $C_A = \ '(L_0)$. This implies that the group C_A depends only on the equivalence class $A\ $, and we can set

$$(A;i;A\ ) := (A;i;C_A\ ):$$

Let now $\varphi : (A; i; A\ ) \to (A'; i'; A\ ')$ be a morphism of $\mathcal{C}_{H_0(M)}$, i.e. an isomorphism of $H_0(M)$-triples, and call with the same letter the underlying isomorphism of abelian surfaces with QM. We define

$$(\ \ ) : (A; i; C_A\ ) \to (A'; i'; C_{A\ '})$$

to be the morphism induced by φ. We need to show that it preserves the level structures. If $\in A$, then $A\ '$ is the $H_0(M)$-equivalence class of $\circ$. But then

$$C_{A\ '} = (\ \circ\ )(L_0) = \ (\ (L_0)) = \ (C_A):$$

Therefore, φ induces an isomorphism of $V_0(M)$-triples.

We now build the inverse functor Ψ. Let $(A; i; C)$ be an object of $\mathcal{C}_0(M)$, where C is a given $\mathcal{O}_B$-cyclic submodule of $A[M]$ isomorphic to $(\mathbb{Z}/M\mathbb{Z})^2$. Let A_C be the set of all full level M structures that send L_0 (isomorphically) to C. The set A_C is nonempty because, using Lemma 1.3.14, one can complete a basis of C (as a $\mathbb{Z}/M\mathbb{Z}$-module) to a basis of $A[M]$ and find an element of A_C applying Proposition 1.3.13.

A direct computation shows that for any element $\in A_C$, the entire $H_0(M)$-orbit of $\ $ is contained in A_C. On the other hand, if there are $_1;\ _2 \in A_C$ that lie in di□erent $H_0(M)$-orbits, the transitivity of the action of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ proved in Lemma 1.3.17 implies that there exists a matrix $= \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ with $c \neq 0$ such that $_1 = \ _2 \circ r$. But $r\ (L_0)$ is not contained in L_0, therefore if $_2(L_0) = C$ one cannot have that $_1(L_0) = C$, yielding a contradiction. Therefore, A_C consists of a single orbit. We can hence define

$$\Psi(A; i; C) = (A; i; A_C):$$

Let now $\varphi : (A; i; C) \to (A'; i'; C')$ be a morphism of $\mathcal{C}_0(M)$, i.e. an isomorphism of $V_0(M)$-triples, and call with the same letter the underlying isomorphism of abelian surfaces with QM. We define

$$(\ \ ) : (A; i; A_C) \to (A'; i'; A'_C)$$

to be the morphism induced by φ. We need to show that it preserves the level structures. Since $\varphi(C) = C'$, for any $\in A_C$ we have that $\circ\ \in A_{C'}$, by definition of $\mathcal{A}_{C'}$. Therefore, φ induces an isomorphism of abelian surfaces with QM and $H_0(M)$-level structure.

Using their definition, it is now straightforward to see that Ψ and Φ are mutually inverse functors. □

The previous lemma together with Proposition 1.3.19 implies that there is a one to one correspondence between (isomorphism classes of) $U_0(M)$-triples, $H_0(M)$-triples and $V_0(M)$-triples.

Definition. Let $m \geq 0$. A $V_1(p^m)$-triple is a triple $(A; i; P)$ where $(A; i)$ is a complex abelian surface with QM by $\mathcal{O}_B$ and P is a point of order p^m in $\mathrm{Im}(e_{p^m}) \subseteq A[p^m]$. The point P is called a $V_1(p^m)$-level structure on $(A; i)$.

By Lemma 1.3.14 the $\mathcal{O}_B$-cyclic submodule generated by P has cardinality p^{2m}, and the choice of P in $\mathrm{Im}(e_{p^m})$ is equivalent to the choice of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) P$ in $\mathrm{Im}(1 - e_M)$.

Definition. An isomorphism $\varphi : (A; i; P) \to (A'; i'; P')$ of $V_1(p^m)$-triples is an isomorphism $\varphi : (A; i) \to (A'; i')$ of abelian surfaces with QM such that $\varphi(P) = P'$.

Definition. We define $\mathcal{C}_1(p^m)$ to be the category whose objects are $V_1(p^m)$-triples and whose morphisms are isomorphisms of $V_1(p^m)$-triples.

Lemma 1.3.21. *The categories $\mathcal{C}_{H_1(p^m)}$ and $\mathcal{C}_1(p^m)$ are isomorphic.*

Proof. As in the proof of Lemma 1.3.20, we start building explicitly an isomorphism $: \mathcal{C}_{H_1(p^m)} \to \mathcal{C}_1(p^m)$.

Take an object $(A; i; A\ )$ of $\mathcal{C}_{H_1(p^m)}$, so that A is an $H_1(p^m)$-equivalence class of full level p^m structures. Any $\in A$ corresponds to an isomorphism

$$: \mathrm{M}_2(\mathbb{Z}/p^m\mathbb{Z}) \xrightarrow{\cong} A[p^m]$$

of $\mathcal{O}_B$-modules. Then the point

$$P_A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in A[p^m]$$

lies in $\mathrm{Im}(e_{p^m})$ and has order p^m. Since the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ is fixed by the right multiplication of elements of $H_1(p^m)$, the point P_A is independent on the choice of $\in A$. We then define

$$(A; i; A\ ) := (A; i; P_A\ ).$$

Let now $: (A; i; A\ ) \to (A'; i'; A'\ )$ be a morphism of $\mathcal{C}_{H_1(p^m)}$, i.e. an isomorphism of $H_1(p^m)$-triples, and call with the same letter the underlying isomorphism of abelian surfaces with QM. We define

$$(\ ) : (A; i; P_A\ ) \to (A'; i'; P_{A'})$$

to be the morphism induced by . We need to show that it preserves the level structures. If $\in A$, then A' is the $H_1(p^m)$-equivalence class of $\circ$. But then

$$P_{A'} = (\ \circ\ )\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = (P_A\ ).$$

Therefore, induces an isomorphism of $V_1(p^m)$-triples.

We now build the inverse functor . Let $(A; i; P)$ be an object of $\mathcal{C}_1(p^m)$, where $P \in \mathrm{Im}(e_{p^m})$ is a point of order p^m. Let A_P be the set of full level p^m-structures that send $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ to P. Combining Proposition 1.3.13 and Lemma 1.3.14 one can see that A_P is not empty.

Since $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ is fixed by the right action of $H_1(p^m)$, for every $\in A_P$ the entire $H_1(p^m)$-orbit of lies inside A_P. On the other hand, if there are $_1;\ _2 \in A_P$ that lie in different $H_1(p^m)$-orbits, the transitivity of the action of $\mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ proved in Lemma 1.3.17 implies that there exists a matrix $= \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ with $c \neq 0$ or $d \neq 1$ such that $_1 = {}_2 \circ r$. Then r does not fix $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, therefore if ${}_2\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = P$ one cannot have that ${}_1\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = P$, yielding a contradiction. Therefore, A_P consists of a single orbit. We can hence define

$$(A; i; P) = (A; i; A_P).$$

Let now $: (A; i; P) \to (A'; i'; P')$ be a morphism of $\mathcal{C}_1(p^m)$, i.e. an isomorphism of $V_1(p^m)$-triples, and call with the same letter the underlying isomorphism of abelian surfaces with QM. We define

$$(\ ) : (A; i; A_P) \to (A'; i'; A_{P'})$$

to be the morphism induced by . Since $(P) = P'$, for any $\in A_P$ we have that $\circ \in \mathcal{A}_{P'}$, by definition of $A_{P'}$. Therefore, induces an isomorphism of $H_1(p^m)$-triples.

Using their definition, it is now straightforward to see that and are mutually inverse functors. □

The previous lemma together with Proposition 1.3.19 implies that there is a one to one correspondence between (isomorphism classes of) $U_1(p^m)$-triples, $H_1(p^m)$-triples and $V_1(p^m)$-triples.

Definition. Let $m \geq 0$. A $V_{0;1}(N^+;p^m)$-quadruple is a quadruple $(A;i;C;P)$ where $(A;i)$ is a complex abelian surface with QM by $\mathcal{O}_B$, C is a $V_0(N^+)$-level structure on $(A;i)$ and P is a $V_1(p^m)$-level structure on $(A;i)$.

Notice that the data of a $V_{0;1}(N^+;p^m)$-quadruple $(A;i;C;P)$ is equivalent to the data of the $V_{0;1}(N^+p^m;p^m)$-structure $(A;i;\langle C;P\rangle;P)$.

Definition. An isomorphism $: (A;i;C;P) \to (A';i';C';P')$ of $V_{0;1}(N^+;p^m)$-quadruples is an isomorphism $: (A;i) \to (A';i')$ of abelian surfaces with QM such that $(C) = C'$ and $(P) = P'$.

Definition. We denote by $\mathcal{C}_{0;1}(N^+;p^m)$ the category whose objects are $V_{0;1}(N^+;p^m)$-quadruples and whose morphisms are isomorphisms of $V_{0;1}(N^+;p^m)$-triples.

Lemma 1.3.22. *The categories $\mathcal{C}_{H_{0;1}(N^+;p^m)}$ and $\mathcal{C}_{0;1}(N^+;p^m)$ are isomorphic.*

Proof. Let $(A;i)$ be a complex abelian surface with QM by $\mathcal{O}_B$. The Chinese remainder theorem induces decompositions

$$\mathcal{O}_B/N^+p^m\mathcal{O}_B \cong \mathcal{O}_B/N^+\mathcal{O}_B \times \mathcal{O}_B/p^m\mathcal{O}_B \quad \text{and} \quad A[N^+p^m] \cong A[N^+] \times A[p^m];$$

and the left action of $\mathcal{O}_B$ coincides with the left action of

$$\mathrm{M}_2(\mathbb{Z}/N^+p^m\mathbb{Z}) \cong \mathrm{M}_2(\mathbb{Z}/N^+\mathbb{Z}) \times \mathrm{M}_2(\mathbb{Z}/p^m\mathbb{Z}):$$

Moreover, the group $H_{0;1}(N^+;p^m)$ decomposes as the product $H_0(N^+) \times H_1(p^m)$ in $\mathrm{GL}_2(\mathbb{Z}/N^+p^m\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/N^+\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ and acts on the right on the module $\mathcal{O}_B/N^+p^m\mathcal{O}_B$. This implies that there is a natural one-to-one correspondence between $H_{0;1}(N^+;p^m)$-level structures and couples of $H_0(N^+)$ and $H_1(p^m)$-level structures on $(A;i)$. We then conclude applying Lemma 1.3.20 and Lemma 1.3.21. □

The previous lemma together with Proposition 1.3.19 implies that there is a one to one correspondence between (isomorphism classes of) $U_{0;1}(N^+;p^m)$-triples, $H_{0;1}(N^+;p^m)$-triples and $V_{0;1}(N^+;p^m)$-triples.

Moduli interpretation of Shimura curves

Having settled the equivalence of all relevant level structures, we now see that the open Shimura C-curves parametrize triples of complex abelian surfaces with QM by $\mathcal{O}_B$ and level structure.

Theorem 1.3.23 (Milne). *Let U be an open compact subgroup of $\hat{\mathcal{O}}_B^\times$. There is a bijection between the open Shimura C-curve $Y_U(\mathbb{C}) = B^\times\backslash(H \times \hat{B}^\times)/U$ and the set of isomorphism classes of U-triples $(A;i;A_U)$.*

Proof. See [Mil79, Theorem 1.2]. See also [Mil03, Proposition 2.19 and Proposition 5.1]. □

Corollary 1.3.24. *Let $M \nmid N^-$ and $m \geq 0$. There is a bijection between the open Shimura C-curve $Y_{0;M}(\mathbb{C})$ (resp. $Y_{1;m}(\mathbb{C})$, resp. $Y_m(\mathbb{C})$) and the set of isomorphism classes of $V_0(M)$-triples (resp. $V_1(p^m)$-triples, resp. $V_{0;1}(N^+)$-quadruples).*

Proof. Combine Theorem 1.3.23 with, respectively, Lemma 1.3.20, Lemma 1.3.21 and Lemma 1.3.22. □

Remark 1.3.25. Let B be the split quaternion algebra $M_2(\mathbb{Q})$ and let $\mathcal{O}_B = M_2(\mathbb{Z})$ as in Example 1.2.9. A complex abelian variety $(A; i)$ with QM by $\mathcal{O}_B$ decomposes as a product of an elliptic curve with itself via

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} A \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} A:$$

All level structures on A easily correspond to the respective classical level structures on the elliptic curve $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) A$, giving the classical modular interpretation of modular curves.

1.3.5 Canonical models over $\mathbb{Q}$

In this subsection we see that all Shimura C-curves have a model over $\mathbb{Q}$, meaning that they consist of the complex points of some algebraic curves defined over $\mathbb{Q}$.

For a compact open subset U of $\hat{\mathcal{O}}_B^\times$ recall that $\mathcal{C}_U$ is the category of U-triples $(A; i; A_U)$. There is a natural action of $\mathrm{Aut}(\mathbb{C})$ on $\mathcal{C}_U$ and $\mathcal{C}_U/\cong$, defined in the following way. If A is a complex abelian variety and $\in \mathrm{Aut}(\mathbb{C})$, define A to be the fibre product

$$\begin{array}{ccc} A & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{C}) & \longrightarrow & \mathrm{Spec}(\mathbb{C}) \end{array}$$

in which the bottom arrow is induced by . More explicitly, if I_A is the homogeneous ideal attached to a model of A inside $\mathbb{P}^n(\mathbb{C})$, then A is associated to the ideal (I_A) obtained by twisting by the coe□cients of every polynomial in I_A. Every point $P = (x_1 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{C})$ that lies in A defines a point $P := (x_1 : \cdots : x_n) \in A$, and this correspondence induces an isomorphism $: A \to A$.

If $(A; i)$ has QM by $\mathcal{O}_B$, then there is an induced QM structure i on A defined as

$$i(b)(P) = (i(b)P):$$

for every $b \in \mathcal{O}_B$ and $P \in A$ (see Lemma 1.3.9).

If U is an open compact subgroup of $\hat{\mathcal{O}}_B^\times$ and A is an U-level structure, define A to be the set containing all $\circ$ for every $\in A$. Therefore, we get an action of $\mathrm{Aut}(\mathbb{C})$ on the set of all U-triples,

$$(A; i; A) := (A; i; A);$$

which preserves isomorphism classes.

Theorem 1.3.26. *Let U be a compact open subgroup of $\hat{\mathcal{O}}_B^\times$. Then there is a unique model Y_U of the Shimura* C*-curve $Y_U(\mathbb{C})$ over* Q *for which the identification*

$$Y_U(\mathbb{C}) = B^\times \backslash (H \times \hat{B}^\times)/U \overset{1:1}{\longleftrightarrow} \mathcal{C}_U/\cong$$

of Theorem 1.3.23 is compatible with the actions of $\mathrm{Aut}(\mathbb{C})$ *on $\mathcal{C}_U/\cong$ and on $Y_U(\mathbb{C})$ defined by its identification with the complex points of Y_U.*

Proof. For existence, see [Mil03, Theorem 3.1 and Theorem 5.2]. A discussion about unicity is given in [Mil03, Theorem 3.10] and at the end of [Mil03, §3]. □

The model Y_U is called in literature the canonical model for the Shimura curve. The study of canonical models of Shimura varieties has been started by Shimura and Taniyama in the 60's and continued later on by many other authors. For a summary of the earlier work of Shimura, see [Del06b].

Remark 1.3.27. Let U be an open compact subgroup of $\hat{\mathcal{O}}_B^\times$. When B is a division ring, the equality $X_U(\mathbb{C}) = Y_U(\mathbb{C})$ together with the previous theorem implies that there is a canonical model X_U for $X_U(\mathbb{C})$ over Q.

When, instead, B is the split algebra $\mathrm{M}_2(\mathbb{Q})$, our compact Shimura curves of interest are connected and correspond to compact modular curves which are defined over Q by classical results (see for example [DS05, §7.7]).

From now on the algebraic curve X_U over Q will be called the Shimura curve of level U, whose complex points are in bijection with the previously-called Shimura C-curve $X_U(\mathbb{C})$.

Remark 1.3.28. There is a purely algebraic way to define the scheme X_U over Q, namely as the solution of a moduli problem of families of abelian surfaces with level structure. This interpretation allows one to generalize the correspondence of Theorem 1.3.23 to Q-algbebras different from C.

One can indeed go further and discuss integral models of Shimura curves, finding that X_U has a proper and smooth model over $\mathbb{Z}[1/N^- M_U]$ for some $M_U \in \mathbb{Z}$ associated to the compact open subgroup U. The scheme X_U is the coarse moduli space for a moduli problem that involves families of QM abelian surfaces defined over schemes defined over $\mathbb{Z}[1/N^- M_U]$ with some level structure. The scheme X_U is the fine moduli space for this moduli problem if U is *small enough*. For more on this, see [Cla03], [Buz97] and [Mil03, §2]. We won't give more details since we will mainly work with some special complex points on Shimura curves, called *Heegner points*.

1.3.6 From the moduli to the analytic interpretation

In this subsection we focus on the curves X_m for $m \geq 0$ and build an explicit correspondence between isomorphism classes $[(A; i; C; P)]$ of QM abelian varieties with $V_{0;1}(N^+; p^m)$-level structure and elements of

$$Y_m(\mathbb{C}) = B^\times \backslash (\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty) \times \hat{B}^\times)/U_{0;1}(N^+; p^m);$$

where the equality comes from (1.4). In [Vig05, §3.2] and [BD98, §4.II] they treat the same construction for the curves $X_{0;M}$.

The set $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$ as a moduli space

Definition. A quaternionic space attached to B is a 2-dimensional complex vector space V equipped with a left action of B_∞, i.e. an injection of rings $B_\infty \hookrightarrow \mathrm{End}_{\mathbb{C}}(V)$. An isomorphism of quaternionic spaces is an isomorphism of vector spaces commuting with the action of B_∞.

If V is a 2-dimensional complex vector space, we denote by $V_{\mathbb{R}}$ the 4-dimensional real vector space underlying V. For a quaternionic space V we define $\mathrm{End}_{B_\infty}(V_{\mathbb{R}})$ to be the set of $\mathbb{R}$-linear endomorphisms commuting with the action of B_∞.

Lemma 1.3.29. *The algebra* $\mathrm{End}_{B_\infty}(V_{\mathbb{R}})$ *is (non-canonically) isomorphic to* B_∞.

Proof. See [BD98, Lemma 4.3]. □

Definition. A rigidification of a quaternionic space V is an isomorphism

$$: B_\infty \longrightarrow \mathrm{End}_{B_\infty}(V_{\mathbb{R}}):$$

A pair $(V; \ )$ consisting of a quaternionic space V and a rigidification $\ $ is called a rigidified quaternionic space.

A rigidification is usually seen as a way to define a right action of B_∞ on $V_{\mathbb{R}}$ or, equivalently, a left action of B_∞^{op} on $V_{\mathbb{R}}$. Look at the proof of Proposition 1.3.30 for more insights on this.

Definition. An isomorphism between two rigidified quaternionic spaces $(V; \ )$ and $(V'; \ ')$ is an isomorphism of quaternionic spaces $\ : V \to V'$ such that the diagram

$$\begin{array}{ccc} B_\infty & & \\ \downarrow & \searrow^{\ '} & \\ \mathrm{End}_{B_\infty}(V_{\mathbb{R}}) & \xrightarrow[f \mapsto \ f \ {}^{-1}]{} & \mathrm{End}_{B_\infty}(V'_{\mathbb{R}}) \end{array}$$

is commutative.

Proposition 1.3.30. *There is a canonical bijection between* $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$ *and the set of isomorphism classes of rigidified quaternionic spaces.*

Proof. See [BD98, Proposition 4.5]. We recall here how the bijection is built.

First, let $\in \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$. Then we define $V := B_\infty$, viewed as a two-dimensional complex vector space via the rule

$$v := v \ (\ ) \quad \text{for every } v \in V \text{ and } \in \mathbb{C}:$$

The left multiplication by B_∞ on V endows V with the structure of quaternionic space. We define also a rigidification on V by the composition of the canonical involution with right multiplication:

$$\begin{aligned} : \ B_\infty &\xrightarrow{\cong} \mathrm{End}_{B_\infty}(V_{\mathbb{R}}) \\ b &\longmapsto (v \mapsto vb^*): \end{aligned}$$

The element $\ $ then corresponds to the isomorphism class of $(V; \ )$.

On the other hand, let $(V; \ )$ be a rigidified quaternionic space. If $\in \mathbb{C}$, multiplication by $\ $ determines an element of $\mathrm{End}_{B_\infty}(V_{\mathbb{R}})$ denoted by $m \ $. Then the map

$$\begin{aligned} : \ \mathbb{C} &\longrightarrow B_\infty \\ &\longmapsto \ {}^{-1}(m \ ) \end{aligned}$$

determines the element of $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$ attached to $[(V; \ )]$. □

Orientations of the Eichler order R_{N^+}

Recall the Eichler order $R_{N^+p^m}$ of level N^+p^m defined in Subsection 1.2.2, for some $m \geq 0$. For every prime ℓ we set $(R_{N^+p^m})_\ell := R_{N^+p^m} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.

Lemma 1.3.31. *With the notation above,*

(i) if $\ell^n \| N^+p^m$ there are exactly two surjective homomorphisms of $\mathbb{Z}_\ell$-algebras

$$o_\ell^+ : (R_{N^+p^m})_\ell \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z};$$

(ii) if $\ell \mid N^-$ there are exactly two surjective ring homomorphisms

$$o_\ell^- : (R_{N^+p^m})_\ell = (\mathcal{O}_B)_\ell \longrightarrow \mathbb{F}_{\ell^2}$$

where $\mathbb{F}_{\ell^2}$ is the finite field with ℓ^2 elements.

Proof. See [Vig05, Lemma 3.2.2]. □

Definition. An orientation of the Eichler order $R_{N^+p^m}$ is the choice of one of the two homomorphisms o_ℓ^+ for all $\ell \mid N^+p^m$ and of one of the two homomorphisms o_ℓ^- for all $\ell \mid N^-$.

From now on we fix orientations o_ℓ^+ for all $\ell \mid N^+$ and o_ℓ^- for all $\ell \mid N^-$.

As seen in Lemma 1.1.17, for every $\ell \mid N^-$ the ring $(\mathcal{O}_B)_\ell = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a non-commutative valuation ring. We denote by $\mathfrak{m}_\ell$ the maximal ideal of $(\mathcal{O}_B)_\ell$. By Proposition 1.1.26, $(\mathcal{O}_B)_\ell$ contains the ring of integers of an unramified extension of $\mathbb{Q}_\ell$ of degree 2, therefore $(\mathcal{O}_B)_\ell/\mathfrak{m}_\ell \cong \mathbb{F}_{\ell^2}$. As pointed out in [BD98, §4.I], if A is an abelian surface with QM by $\mathcal{O}_B$, the subgroup $A[\mathfrak{m}_\ell] \subseteq A[\ell]$ of points of A killed by $\mathfrak{m}_\ell$ is a free $(\mathcal{O}_B)_\ell/\mathfrak{m}_\ell$-module of rank 1. We regard $A[\mathfrak{m}_\ell]$ as a one dimensional $\mathbb{F}_{\ell^2}$-vector space by means of the orientation $o_\ell^- : (\mathcal{O}_B)_\ell \twoheadrightarrow \mathbb{F}_{\ell^2}$ chosen above.

The rigidified quaternionic space attached to a QM surface

Let $(A; i; C; P)$ be an abelian surface with QM by $\mathcal{O}_B$ and $V_{0;1}(N^+; p^m)$-level structure. We regard A as a compact, connected, complex Lie group. Then $A = V/$ where $V = \mathrm{Lie}(A)$ is the Lie algebra of A (which is a 2-dimensional complex vector space) and is an $\mathcal{O}_B$-stable sublattice of V, explicitly given as the kernel of the exponential map $V \to A$. The left action of $\mathcal{O}_B$ on A induces an action of $\mathcal{O}_B$ on V. By extending scalars from $\mathbb{Z}$ to $\mathbb{R}$, we obtain an action of B_∞ on V, therefore V is a quaternionic space in a natural way.

Alternatively, by Proposition 1.3.11 we can suppose that $A = A$ and $i = i$ (see Example 1.3.10). Then $A = V/$ where V is a two dimensional $\mathbb{C}$-vector space with a left action of B_∞ obtained extending the map $_\infty$ to a map $B_\infty \xrightarrow{\infty} M_2(\mathbb{R}) \subseteq M_2(\mathbb{C})$, as explained in Example 1.3.10. In this way we recover the same quaternionic structure on V.

Let now $M_0(N^+) := \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) : a; b; d \in \mathbb{Z}/N^+\mathbb{Z}\}$ and $M_1(p^m) := \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a; b; d \in \mathbb{Z}/p^m\mathbb{Z}\}$. Recall also that the N^+-level structure C is equivalent to the data of the N^+-cyclic subgroup $e_{N^+}(C)$. A straightforward matrix computation shows that $e_{N^+}(C)$ is stable with respect to the left action of $M_0(N^+)$ induced by the action of $\mathcal{O}_B$ via the isomorphism (1.6).

Lemma 1.3.32. *(i) The ring $\mathcal{O}_B$ is (noncanonically) isomorphic to* $\mathrm{End}_{\mathcal{O}_B}(\ )$.

(ii) *The ring* $M_0(N^+) \subseteq \mathcal{O}_B/N^+\mathcal{O}_B$ *is (noncanonically) isomorphic to the subring of* $\mathrm{End}_{\mathcal{O}_B}(\ ) \otimes \mathbb{Z}/N^+\mathbb{Z}$ *preserving the* $V_0(N^+)$*-level structure* C *(or, equivalently,* $e_{N^+}(C)$*).*

(iii) *The multiplicative monoid* $M_1(p^m) \subseteq \mathcal{O}_B/p^m\mathcal{O}_B$ *is (noncanonically) isomorphic to the submonoid of* $\mathrm{End}_{\mathcal{O}_B}(\ ) \otimes \mathbb{Z}/p^m\mathbb{Z}$ *preserving the* $V_1(p^m)$*-level structure* P*.*

Proof. For (i) and (ii) see [BD98, Lemma 4.6]. Also (iii) can be proven in the same way, but we want here to build an explicit isomorphism.

Let A_{p^m} be the $H_1(p^m)$-level structure attached to P. Let $\in A_{p^m}$ be an isomorphism of left $\mathcal{O}_B$-modules between $\mathcal{O}_B/p^m\mathcal{O}_B \cong \mathrm{M}_2(\mathbb{Z}/p^m\mathbb{Z})$ and $A[p^m]$. In the proof of Proposition 1.3.21 we saw that $P = \left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$, and one can check that $(\ \circ r\ )\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right) = P$ for every $\in M_1(p^m)$, where r is right multiplication by . Moreover, this last property characterizes $M_1(p^m)$.

We define an injection

$$f : M_1(p^m) \longrightarrow \mathrm{End}_{\mathcal{O}_B}(A[p^m]) \cong \mathrm{End}_{\mathcal{O}_B}(\ ) \otimes \mathbb{Z}/p^m\mathbb{Z}$$

in the following way: for every $Q \in A[p^m]$ and $\in M_1(p^m)$ we define $f(\ )(Q)$ to be $(\ \circ r \circ {}^{-1})(Q)$. It is then straightforward that $f(\ )(P) = P$ for every $\in M_1(p^m)$, hence f induces an isomorphism between $M_1(p^m)$ and the subset of $\mathrm{End}_{\mathcal{O}_B}(A[p^m])$ preserving P.

A similar argument can also be used to find an explicit isomorphism for (ii). □

We now choose an isomorphism $: \mathcal{O}_B \to \mathrm{End}_{\mathcal{O}_B}(\ )$ such that its profinite completion

$$\hat{}: \hat{\mathcal{O}}_B \longrightarrow \mathrm{End}_{\mathcal{O}_B}(\ ) \otimes_{\mathbb{Z}} \hat{\mathbb{Z}};$$

has the following properties.

1. The reduction ${}_{N^+}$ of $\hat{}$ modulo N^+ induces an isomorphism between $M_0(N^+)$ and the subring of $\mathrm{End}_{\mathcal{O}_B}(\ ) \otimes \mathbb{Z}/N^+\mathbb{Z}$ preserving the $V_0(N^+)$-level structure C. We require also that the composition

$$R_{N^+p^m} \twoheadrightarrow M_0(N^+) \xrightarrow{{}_{N^+}} {}_{N^+}(M_0(N^+)) \to \mathbb{Z}/N^+\mathbb{Z}$$

corresponding to the action of ${}_{N^+}(M_0(N^+))$ on $e_{N^+}(C)$ is equal to the product of the chosen orientations o_ℓ^+ for all $\ell \mid N^+$.

2. The reduction ${}_{p^m}$ of $\hat{}$ modulo p^m induces an isomorphism between $M_1(p^m)$ and subring of $\mathrm{End}_{\mathcal{O}_B}(\ ) \otimes \mathbb{Z}/p^m\mathbb{Z}$ preserving the level p^m structure P. This choice automatically implies that ${}_{p^m}(M_0(p^m))$ preserves $\langle P \rangle$. Moreover, the choice of putting 1 in the lower right entry of the matrices in $M_1(p^m)$ determines uniquely the map

$$R_{N^+p^m} \twoheadrightarrow M_0(p^m) \xrightarrow{{}_{p^m}} {}_{p^m}(M_0(p^m)) \to \mathbb{Z}/p^m\mathbb{Z}$$

corresponding to the action of ${}_{p^m}(M_0(p^m))$ on $\langle P \rangle$. More precisely, this map sends $\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right) \in M_0(p^m)$ to d (and it determines a unique orientation o_p^+).

3. For each $\ell \mid N^-$, notice that the action of $((\mathcal{O}_B)_\ell) = ((R_{N^+p^m})_\ell)$ preserves $A[m_\ell]$, and its action commutes with the $\mathbb{F}_{\ell^2}$-action defined by the chosen orientation o_ℓ. We require the map

$$(\mathcal{O}_B)_\ell \longrightarrow ((\mathcal{O}_B)_\ell) \twoheadrightarrow \mathbb{F}_{\ell^2}$$

attached to this action to coincide with the chosen orientation o_ℓ.

Then, if we call U the subset of $\mathrm{End}_{\mathcal{O}_B}(\ ) \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ preserving C and P, we have that $\wedge^{-1}(U)^\times = U_{0;1}(N^+;p^m)$. Moreover, the map $\wedge$ is well defined up to conjugation by elements of $U_{0;1}(N^+;p^m)$ on the domain. By extension of scalars from $\mathbb{Z}$ to $\mathbb{R}$ the map induces an isomorphism

$$: B_\infty \xrightarrow{\cong} \mathrm{End}_{B_\infty}(V_{\mathbb{R}}):$$

Thus, the pair $(V; \ )$ associated to $(A; i; C; P)$ is a rigidified quaternionic space. It can be shown that it depends only on the isomorphism class of $(A; i; C; P)$ and it is defined up to the action of $:= U_{0;1}(N^+;p^m) \cap B^\times$ on by conjugation. By Proposition 1.3.30, the pair $(V; \ )$ gives a well defined point on the quotient $\backslash \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$, hence on the Shimura curve $X_m(\mathbb{C})$ by Lemma 1.2.3. This is the point of $X_m(\mathbb{C})$ that corresponds to $[(A; i; C; P)]$.

1.3.7 From the analytic to the moduli interpretation

In this subsection we give an idea on how one can pursue the converse of the construction of the previous subsection.

Let $:= U_{0;1}(N^+;p^m) \cap B^\times$ and take $[f] \in \backslash \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$. As shown in the proof of Proposition 1.3.30 the rigidified quaternionic space attached to f is $(V; \ )$ where $V = B_\infty$ (with $\mathbb{C}$-structure induced by f) and

$$\begin{aligned} : B_\infty &\xrightarrow{\cong} \mathrm{End}_{B_\infty}(V_{\mathbb{R}}) \\ b &\longmapsto (v \mapsto vb^*): \end{aligned}$$

The map is the extension of scalars of a map $_0 : \mathcal{O}_B \to \mathrm{End}_{\mathcal{O}_B}(\mathcal{O}_B)$. Calling $:= \mathcal{O}_B$, we see that $A = V/$ is an abelian surface with QM by $\mathcal{O}_B$ induced by left multiplication.

The group of N^+-torsion points corresponds to $\frac{1}{N^+} / \cong \mathcal{O}_B/N^+\mathcal{O}_B$, which corresponds to $M_2(\mathbb{Z}/N^+\mathbb{Z})$ via the isomorphism $_{N^+}$ of (1.6) induced by the chosen embeddings. We choose the $V_0(N^+)$-level structure on A to be the $\mathcal{O}_B$-submodule that coincides with $\left\{\left(\begin{smallmatrix} 0 & a \\ 0 & b \end{smallmatrix}\right) : a; b \in \mathbb{Z}/N^+\mathbb{Z}\right\}$ under these isomorphisms.

Similarly, take the $V_1(p^m)$-level structure P to be the point corresponding to $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ under the isomorphism $\mathcal{O}_B/p^m\mathcal{O}_B \cong M_2(\mathbb{Z}/p^m\mathbb{Z})$.

One can prove that $(A; i; C; P)$ is a $V_{0;1}(N^+; P)$-quadruple whose isomorphism class corresponds to the point $[f]$ on the Shimura curve $Y_m(\mathbb{C})$.

1.4 Hecke operators on Shimura curves

In this section we review the theory of Hecke operators for the curves $X_m := X_{0;N^+p^m}$ and X_m. Thanks to the work of the previous sections, we are able to give a complete description of their action both in the analytic and in the modular interpretation of the curves.

Definition. Call $\mathrm{Div}(X_m)$ and $\mathrm{Div}(X_m)$ the groups of divisors of the Riemann surfaces $X_m(\mathbb{C})$ and $X_m(\mathbb{C})$ respectively.

1.4.1 The Hecke operators T_ℓ

Let $m \geq 0$ and fix a prime $\ell \nmid Np^m$. For all $j \in \{0,\dots,\ell-1\}$ denote by $\xi_j \in \hat{B}^\times$ the idele whose ℓ-component is equal to $\left(\begin{smallmatrix} \ell & j \\ 0 & 1 \end{smallmatrix}\right)$ and whose components at all other primes are equal to 1. Similarly, let ξ_∞ be the idele whose ℓ-component is equal to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)$ and whose all other components are equal to 1.

Definition. ([LV11, §2.4]) The T_ℓ-operator on $\mathrm{Div}(X_m)$ and $\mathrm{Div}(\mathcal{X}_m)$ acts as

$$T_\ell([(f,b)]) = \sum_{j=0}^{\ell-1}[(f,b\xi_j)] + [(f,b\xi_\infty)]$$

for every $b \in \hat{B}^\times$ and $f \in \mathrm{Hom}_R(\mathbb{C}, B_\infty)$.

Passing to the modular interpretation, recall that any complex abelian surface (A,i) with QM by $\mathcal{O}_B$ has $\ell+1$ cyclic $\mathcal{O}_B$-submodules annihilated by ℓ (see Lemma 1.3.14 and Remark 1.3.15). Denote them by $D_0,\dots,D_\ell$. Then, the quotient isogenies $\varphi_j : A \to A/D_j$ induce a natural QM structure i_j on A/D_j by Lemma 1.3.9. Therefore, the action of the Hecke operator T_ℓ on $\mathrm{Div}(\mathcal{X}_m)$ can be described as

$$T_\ell([(A,i,C,P)]) = \sum_{j=0}^{\ell}[(A/D_j, i_j, C_j, P_j)],$$

where C_j and P_j are the images of C and P respectively under the quotient isogeny φ_j. A similar (and more classical) interpretation is also available for the curve X_m.

1.4.2 The Hecke operator U_p

Let $m \geq 1$. For all $j \in \{0,\dots,p-1\}$ denote by $\xi_j \in \hat{B}^\times$ the idele whose p-component is equal to $\left(\begin{smallmatrix} p & j \\ 0 & 1 \end{smallmatrix}\right)$ and whose components at all other primes are equal to 1.

Definition. ([LV11, §2.4]) The U_p-operator on $\mathrm{Div}(X_m)$ and $\mathrm{Div}(\mathcal{X}_m)$ acts as

$$U_p([(f,b)]) = \sum_{j=0}^{p-1}[(f,b\xi_j)]$$

for every $b \in \hat{B}^\times$ and $f \in \mathrm{Hom}_R(\mathbb{C}, B_\infty)$.

Let now $[(A,i,C,P)]$ be a $V_{0,1}(N^+,p^m)$-quadruple. Since $p \nmid N^-$ then any complex abelian surface (A,i) with QM by $\mathcal{O}_B$ has $p+1$ cyclic $\mathcal{O}_B$-submodules annihilated by p, one of whom is the one generated by P. Denote the other ones by $D_1,\dots,D_p$. Notice that two different cyclic $\mathcal{O}_B$-submodules annihilated by p intersect only in $\{O\}$. The quotient isogenies $\varphi_j : A \to A/D_j$ induce a natural QM structure i_j on A/D_j by Lemma 1.3.9. Therefore, the action of the Hecke operator U_p on $\mathrm{Div}(\mathcal{X}_m)$ can be described as

$$U_p([(A,i,C,P)]) = \sum_{j=1}^{p}[(A/D_j, i_j, C_j, P_j)],$$

where C_j and P_j are the images of C and P respectively under the quotient isogeny φ_j. A similar interpretation is also available for the curve X_m.

1.4.3 The diamond operators

Let $m \geq 0$. For any $a \in \mathbb{Z}_p^\times$, we denote with the same letter the idele of $\hat{\mathbb{Q}}^\times \subseteq \hat{B}^\times$ whose p-component is a and whose components at all other primes are equal to 1.

Definition. For any $a \in \mathbb{Z}_p^\times$, the diamond operator $\langle a \rangle$ on $\mathrm{Div}(X_m)$ and $\mathrm{Div}(\mathcal{X}_m)$ acts as

$$\langle a \rangle([(f;b)]) = [(f;ba)]$$

for every $b \in \hat{B}^\times$ and $f \in \mathrm{Hom}_R(\mathbb{C}; B_\infty)$.

Notice that $[(f;-b)] = [(-1)\cdot(f;-b)] = [(\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)\cdot f;b)] = [(f;b)]$, therefore we obtain the equality $\langle -1\rangle = \langle 1\rangle$.

If $[(A;i;C;P)]$ is a $V_{0;1}(N^+;p^m)$-quadruple, the diamond operator can be described as

$$\langle a \rangle([(A;i;C;P)]) = [(A;i;C;a\cdot P)].$$

Thanks to this interpretation, it is immediate that the action of diamond operators on $\mathrm{Div}(\mathcal{X}_m)$ factors through $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

1.5 The tower of curves

In the rest of the thesis, we will mainly work with the curves $X_m := X_{0;N^+p^m}$ and $\mathcal{X}_m$ defined in Subsection 1.2.2. In the previous section we have seen that these curves are defined over $\mathbb{Q}$ and have a modular interpretation.

If we let $m \geq 0$ vary, the inclusions $U_0(N^+p^{m+1}) \subseteq U_0(N^+p^m)$, $U_{0;1}(N^+;p^{m+1}) \subseteq U_{0;1}(N^+;p^m)$ and $U_{0;1}(N^+;p^m) \subseteq U_0(N^+p^m)$ yield a commutative diagram of curves

$$\begin{array}{ccccccc}
\cdots & \xleftarrow{\tilde{\ }_m} & \mathcal{X}_m & \xleftarrow{\tilde{\ }_{m+1}} & \mathcal{X}_{m+1} & \xleftarrow{\tilde{\ }_{m+2}} & \cdots \\
 & & \downarrow{\scriptstyle \pi_m} & & \downarrow{\scriptstyle \pi_{m+1}} & & \\
\cdots & \xleftarrow[\ ]{} & X_m & \xleftarrow[\ ]{} & X_{m+1} & \xleftarrow[\ ]{} & \cdots
\end{array} \tag{1.8}$$

in which all maps are finite coverings that are defined over $\mathbb{Q}$. Every such morphism has an easy modular interpretation as a map forgetting the suitable level structure. For example, the map π_m sends the class of a $V_{0;1}(N^+;p^m)$-quadruple $(A;i;C;P)$ to the class of the $V_0(N^+p^m)$-triple $(A;i;\langle C;P\rangle_{\mathcal{O}_B})$, where $\langle C;P\rangle_{\mathcal{O}_B}$ is the $\mathcal{O}_B$-submodule of $A[N^+p^m]$ generated by C and P.

Chapter 2

Heegner points on Shimura curves

In this chapter we introduce the theory of Heegner points on the curves X_m and $\tilde{X}_m$. In the modular interpretation, they correspond to abelian varieties with CM by an imaginary quadratic fields. Their arithmetic will be fundamental for our work. For this chapter, we mainly refer to [BD96], [BD98] and [LV11] and use the following notation:

Y_m	the open Shimura curve $Y_{0;N^+p^m}$ for some $m \geq 0$;
X_m	the open Shimura curve $X_{0;N^+p^m}$ for some $m \geq 0$.

2.1 Abelian surfaces with QM+CM

In Theorem 1.3.6 we classified all possible endomorphism algebras for a complex abelian surface. Among all complex abelian surfaces $(A;i)$ with QM by $\mathcal{O}_B$, those whose endomorphism algebra $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ is isomorphic to $\mathrm{M}_2(K)$ for some imaginary quadratic field K will play an important role for us.

Definition. Let $(A;i)$ be a complex abelian surface with QM by $\mathcal{O}_B$. Then

$$\mathrm{End}_{\mathcal{O}_B}(A) := \{f \in \mathrm{End}(A) \ : \ f \circ i(b) = i(b) \circ f \text{ for all } b \in \mathcal{O}_B\}$$

is the group of endomorphisms of A commuting with the action of $\mathcal{O}_B$.

Definition. Let $(A;i)$ be a complex abelian surface with QM by $\mathcal{O}_B$ and let $c \geq 1$. If

$$\mathrm{End}_{\mathcal{O}_B}(A) \cong \mathcal{O}_c$$

for the order $\mathcal{O}_c$ of conductor c in an imaginary quadratic field K, we say that $(A;i)$ has QM+CM by $(\mathcal{O}_B;\mathcal{O}_c)$. The number c is called the central conductor of A.

Lemma 2.1.1. *Let $(A;i)$ be a complex abelian surface with QM+CM by $(\mathcal{O}_B;\mathcal{O}_c)$ for an order $\mathcal{O}_c$ in an imaginary quadratic field K. Then*

(i) $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q} \cong \mathrm{M}_2(K)$;

(ii) *K embeds in B;*

(iii) *A is not simple and is isogenous to $E \times E$, where E is an elliptic curve with CM by an order of K.*

Proof. (i) Theorem 1.3.6 gives only two possibilities for $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$. If it were $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}\cong B$, the centrality of the $\mathbb{Q}$-algebra B would imply that $\mathrm{End}_{\mathcal{O}_B}(A)\otimes_{\mathbb{Z}}\mathbb{Q}=\mathbb{Q}$, which is not true. Therefore $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}\cong \mathrm{M}_2(K')$ for some imaginary quadratic field K'. But then $K'=K$ since $K=\mathcal{O}_c\otimes_{\mathbb{Z}}\mathbb{Q}$ is contained in $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$.

(ii) Since the center of B is $\mathbb{Q}$, we have that $\mathrm{End}_{\mathcal{O}_B}(A)$ is not contained in $i(\mathcal{O}_B)$. Then, we have that $\mathrm{End}(A)\cong i(\mathcal{O}_B)\otimes_{\mathbb{Z}}\mathrm{End}_{\mathcal{O}_B}(A)$, that yields $\mathrm{M}_2(K)\cong B\otimes_{\mathbb{Q}}K$. Therefore, K is a splitting field for B and we conclude applying Proposition 1.1.26.

(iii) Since $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$ is not a division algebra then A is not simple, therefore it is isogenous to the product of two elliptic curves $E_1\times E_2$. By (i) we know that $\mathrm{End}(E_1\times E_2)\otimes_{\mathbb{Z}}\mathbb{Q}\cong \mathrm{M}_2(K)$, hence we must have $\mathrm{End}(E_1)\otimes_{\mathbb{Z}}\mathbb{Q}=\mathrm{End}(E_2)\otimes_{\mathbb{Z}}\mathbb{Q}=K$, therefore E_1 and E_2 have CM by an order in K and are isogenous. □

Remark 2.1.2. For those who are aware of the theory of complex multiplication for abelian surfaces, in the language of [Mil07] or [Bil] we have that every abelian surface with QM+CM by $(\mathcal{O}_B;\mathcal{O}_c)$ has complex multiplication by the étale algebra $K\times K$.

One can go further in the characterization of abelian surfaces with QM+CM.

Theorem 2.1.3. *Let $(A;i)$ be an abelian surface with QM+CM by $(\mathcal{O}_B;\mathcal{O}_c)$ for some $c\geq 1$ and let E be an elliptic curve with CM by $\mathcal{O}_c$. Then there is an elliptic curve E' of conductor $c'\mid c$ such that*

$$A\cong E\times E'$$

as complex abelian surfaces.

Proof. See [Ufe12, Theorem 4.4]. □

Definition. If U is an open compact subgroup of $\hat{\mathcal{O}}_B$ and $(A;i)$ is an abelian surface with QM+CM by $(\mathcal{O}_B;\mathcal{O}_c)$ for some $c\geq 1$, we say that the point $[(A;i;A_U)]\in X_U(\mathbb{C})$ is a CM point of conductor $\mathcal{O}_c$, for any U-level structure A_U.

2.2 Heegner points on X_m and X_m^*

In this section, we define Heegner points on the curves X_m and X_m^* and study some of their properties.

2.2.1 Optimal embeddings

Just for this subsection, we let B be a quaternion algebra over any field F that is a finite extension of $\mathbb{Q}$ or of $\mathbb{Q}_\ell$ for some prime ℓ. Let also K/F be a quadratic F-algebra, fix an order $\mathcal{O}$ of K and an Eichler order R of B.

Definition. An optimal embedding of $\mathcal{O}$ into R is an embedding $f:K\hookrightarrow B$ such that $f^{-1}(R)=\mathcal{O}$ (equivalently, $f(\mathcal{O})=R\cap f(K)$).

2.2.2 Heegner points on X_m

We now focus on the Shimura curves $X_m:=X_{0;N^+p^m}$ for $m\geq 0$.

Definition. Let $(A;i;C)$ be a $V_0(N^+p^m)$-triple. Define $\underline{\mathrm{End}}_{\mathcal{O}_B}(A)$ to be the subset of $\mathrm{End}_{\mathcal{O}_B}(A)$ consisting of all endomorphisms that preserve the $\mathcal{O}_B$-submodule C of A.

Definition. Let c be an integer coprime with $N = N^+N^-$ and K be an imaginary quadratic field. A Heegner point of conductor c on X_m is a point on $X_m(\mathbb{C})$ corresponding to a $V_0(N^+p^m)$-triple $(A; i; C)$ such that

$$\underline{\mathrm{End}}_{\mathcal{O}_B}(A) \cong \mathcal{O}_c;$$

where $\mathcal{O}_c$ is the order of K of conductor c.

Remark 2.2.1. This definition follows [BD98, Definition 5.1]. For example, a triple $[(A; i; C)]$ with QM+CM is a Heegner point of conductor equal to its central conductor if C is stable under the action of $\mathrm{End}_{\mathcal{O}_B}(A)$. In general, the conductor of a Heegner point divides the central conductor of the corresponding surface with QM+CM.

In [BD98, §4.II] they describe how one can explicitly build the point of $X_m(\mathbb{C})$ corresponding to a $V_0(N^+p^m)$-triple $(A; i; C)$ (their contruction is indeed the inspiration for what we did in Subsection 1.3.6). We recall here some highlights.

Let $(A; i; C)$ be a $V_0(N^+p^m)$-triple. Then $A = V/$ where V is a two-dimensional $\mathbb{C}$-vector space and is an $\mathcal{O}_B$-stable sublattice of V. The left action of $\mathcal{O}_B$ on A induces a natural action of $\mathcal{O}_B$ (and hence of $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{R} = B_\infty$) on V. Therefore, V is a quaternionic space. One then defines a rigidification starting from an isomorphism

$$: \mathcal{O}_B \longrightarrow \mathrm{End}_{\mathcal{O}_B}( )$$

that must satisfy the properties corresponding to (1) and (3) of Subsection 1.3.6 (i.e. properties (1) and (2) of [BD98, §4.II]). In particular, we must have that induces a bijection between $R_{N^+p^m}$ and the subset of $\mathrm{End}_{\mathcal{O}_B}( )$ preserving the group C. Extending the scalars from $\mathbb{Z}$ to $\mathbb{R}$, we see that the space $(V;)$ is a rigidified quaternionic space. For every $\in \mathbb{C}$ call m the multiplication by in $\mathrm{End}_{B_\infty}(V_{\mathbb{R}})$. Then we define the homomorphism

$$\begin{aligned} : \mathbb{C} &\longrightarrow B_\infty \\ &\longmapsto {}^{-1}(m): \end{aligned}$$

This morphism induces a well defined element of $\backslash \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}; B_\infty)$, where $= R^\times_{N^+p^m}$. This quotient is in bijection with $Y_m(\mathbb{C})$ by Lemma 1.2.3.

Starting now with a triple $(A; i; C)$ whose isomorphism class is a Heegner point of conductor c, we see that $\underline{\mathrm{End}}_{\mathcal{O}_B}(A) \cong \mathcal{O}_c$ is contained in the subset of $\mathrm{End}_{\mathcal{O}_B}( )$ that preserves C. The map is then the extension of scalars of a map

$$_0 : \mathcal{O}_c \longrightarrow R_{N^+p^m}:$$

The map $_{\mathbb{Q}} := {}_0 \otimes \mathbb{Q}$ induces an optimal embedding of $\mathcal{O}_c$ inside $R_{N^+p^m}$. Indeed, if there was $\mathcal{O}_{c'}$ with $c' \mid c$ such that ${}_{\mathbb{Q}}(\mathcal{O}_{c'}) \subseteq R_{N^+p^m}$ then the multiplication by any element of $\mathcal{O}_{c'}$ would be an endomorphism of $\mathrm{End}_{\mathcal{O}_B}(A)$ that fixes C. Therefore $c = c'$. Then we have the following theorem.

Theorem 2.2.2. *Let c be a positive integer coprime with N. There is a bijection between the set of Heegner points of conductor c on $X_m(\mathbb{C})$ and the set of points*

$$[f] \in R^\times_{N^+p^m} \backslash \mathrm{Hom}_{\mathbb{Q}}(K; B)$$

such that f is an optimal embedding of $\mathcal{O}_c$ into $R_{N^+p^m}$.

Proof. With the discussion above (see also [BD98, Theorem 5.2]) we have seen that every Heegner point of conductor c corresponds to an optimal embedding.

Conversely, let $f \in \mathrm{Hom}_{\mathbb{Q}}(K;B)$ be an optimal embedding and take $(V;\ )$ to be the rigidified quaternionic space attached to $f \otimes_{\mathbb{Q}} \mathbb{R}$. With the same ideas of Subsection 1.3.7 one can build a $V_0(N^+p^m)$-triple $(A;i;C)$, where $A = V/\ $ with $V = B_\infty$ and $\ = \mathcal{O}_B$. Since f is an embedding of $\mathcal{O}_c$ in $R_{N^+p^m}$, the rigidification induces an embedding of $\mathcal{O}_c$ in $\underline{\mathrm{End}}_{\mathcal{O}_B}(A)$. The optimality of f implies that $\underline{\mathrm{End}}_{\mathcal{O}_B}(A) = \mathcal{O}_c$. □

Applying the isomorphism of Lemma 1.2.3, one easily finds that an element

$$[(f;b)] \in B^\times \backslash (\mathrm{Hom}_{\mathbb{R}}(K;B) \times \hat{B}^\times)/\hat{R}^\times_{N^+p^m} \subseteq Y_m(\mathbb{C})$$

is a Heegner point of conductor c if and only if

$$f(K) \cap b\hat{R}_{N^+p^m}b^{-1} = f(\mathcal{O}_c);$$

i.e. if and only if f is an optimal embedding of $\mathcal{O}_c$ into the order $b\hat{R}_{N^+p^m}b^{-1} \cap B$. Therefore, we recover the definition of [BD96, §2.1]. For more properties of Heegner points on X_m, see [Vig05, §3].

2.2.3 Heegner points on $\tilde{X}_m$

Recall that, for every $m \geq 0$, there are degeneracy maps $\ _m : \tilde{X}_m \to X_m$ defined in (1.8).

Definition. Let c be a positive integer coprime with $N = N^+N^-$ and K be an imaginary quadratic field. A pre-Heegner point of conductor c on $\tilde{X}_m(\mathbb{C})$ is any point $P \in \tilde{X}_m(\mathbb{C})$ such that $\ _m(P)$ is a Heegner point of conductor c on X_m.

Remark 2.2.3. Let $f \in \mathrm{Hom}_{\mathbb{Q}}(K;B)$ and $b \in \hat{B}^\times$. The discussion of the previous section implies that $[(f;b)] \in \tilde{X}_m(\mathbb{C})$ is a pre-Heegner point if and only if f is an optimal embedding of $\mathcal{O}_c$ into the Eichler order $b\hat{R}_{N^+p^m}b^{-1} \cap B$.

On the modular side, the class of a $V_{0;1}(N^+;p^m)$-quadruple $[(A;i;C;P)]$ is a pre-Heegner point of conductor c if the subset of $\mathrm{End}_{\mathcal{O}_B}(A)$ consisting of all endomorphisms that preserve the $\mathcal{O}_B$-submodule generated by C and P is isomorphic to the order $\mathcal{O}_c$ of K.

We now want to streghten the condition of being a pre-Heegner point, in order to control the field of rationality and to have compatibility when changing the parameter m. In literature, there are some different ways to do that. We present here the approach of [LV11, Definition 3.1].

Definition 2.2.4 ([LV11]). We say that a pre-Heegner point $P = [(f;b)] \in \tilde{X}_m(\mathbb{C})$ is a LV-Heegner point of conductor c on $\tilde{X}_m$ if

$$f_p^{-1}\left(f_p\left((\mathcal{O}_c \otimes \mathbb{Z}_p)^\times\right) \cap b_p^{-1}U_{m;p}b_p\right) = (\mathcal{O}_c \otimes \mathbb{Z}_p)^\times \cap (1 + p^m\mathcal{O}_K \otimes \mathbb{Z}_p)^\times;$$

where $U_m := U_{0;1}(N^+;p^m)$ and the subscript p means that we are taking the p-component of the object.

This definition has the merit of having a meaning both in the definite and in the indefinite case (although in this thesis we are only considering indefinite Shimura curves). We will see later that Longo and Vigni were able to build a family of big Heegner points starting from this definition.

Remark 2.2.5. There is a second possible approach to define Heegner points on $\mathcal{X}_m$. The construction is modular and is a direct translation of the work of Howard in [How07, §2.2] in the context of indefinite Shimura curves. The idea is to build explicitly a family of pre-Heegner points and prove directly the needed compatibility relations. We will present this construction in a future work.

Following [LV11, §3], we list some properties of LV-Heegner points on $\mathcal{X}_m$. In order to do this, we must fix once and for all an imaginary quadratic field K with the following properties.

Assumption 2.2.6. From now on we fix an imaginary quadratic field K such that

- The discriminant of K is not -3 or -4, so that $\mathcal{O}_K^\times = \{\pm 1\}$.
- The primes dividing Np do not ramify in K;
- The class number of K is prime to p;
- The primes dividing N^+ (respectively, N^-) are split (respectively, inert) in K.

This last condition, sometimes called the generalized Heegner hypothesis, implies that there is an embedding of K into B (see Proposition 1.1.26). The third condition will be exploited in Chapter 4.

For any $c \geq 1$ coprime with N we denote by $\mathcal{O}_c$ the order of K of conductor c and with H_c the ring class field of K of conductor c. We also denote by μ_{p^m} the group of p^m-th roots of unity.

Proposition 2.2.7. *Let $P \in \mathcal{X}_m(\mathbb{C})$ be a LV-Heegner point of conductor cp^m on $\mathcal{X}_m$. Then P is defined over $H_{cp^m}(\mu_{p^m})$, i.e. $P \in \mathcal{X}_m(H_{cp^m}(\mu_{p^m}))$.*

Proof. See [LV11, Propositions 3.2 and 3.3]. □

Proposition 2.2.8. *Let $P \in \mathcal{X}_m(\mathbb{C})$ be a LV-Heegner point of conductor cp^n on $\mathcal{X}_m$ for some $n \geq m \geq 1$ and let $Q \in \mathcal{X}_m(\mathbb{C})$ belong to the support of $U_p(P)$. Then*

$$U_p(P) = \mathrm{Tr}_{H_{cp^{n+1}}(\mu_{p^{n+1}})/H_{cp^n}(\mu_{p^{n+1}})}(Q)$$

in $\mathrm{Div}(\mathcal{X}_m)$.

Proof. See [LV11, Proposition 3.4]. □

Proposition 2.2.9. *Fix a prime $\ell \nmid Np^m c$ which is inert in K. Let $P \in \mathcal{X}_m(\mathbb{C})$ be a LV-Heegner point of conductor $c\ell p^m$ on $\mathcal{X}_m$ and let $Q \in \mathcal{X}_m(\mathbb{C})$ belong to the support of $T_\ell(P)$. Then*

$$T_\ell(P) = \mathrm{Tr}_{H_{c\ell p^m}(\mu_{p^m})/H_{cp^m}(\mu_{p^m})}(Q)$$

in $\mathrm{Div}(\mathcal{X}_m)$.

Proof. See [LV11, Proposition 3.5]. □

2.3 A compatible family of Heegner points

In this section we review the properties of the compatible family of LV-Heegner points built in [LV11, §4].

Let $c \geq 1$ and $m \geq 0$ be integers with $(c;N) = 1$. Using the theory of optimal embeddings, Longo and Vigni built in [LV11, §4] a family of Heegner points $P_{c;m}$ of conductor cp^m on X_m that satisfy the following compatibility properties. Write

$$\sim_{m;*} : \mathrm{Div}(X_m) \longrightarrow \mathrm{Div}(X_{m-1})$$

for the map between divisor groups induced by $\sim_m$ (see (1.8)).

Proposition 2.3.1. *Let $m \geq 0$ be an integer and $c \geq 1$ be coprime with N. Then*

(a) If $\ell \nmid Np^m c$ is a prime inert in K, then

$$T_\ell(P_{c;m}) = \mathrm{Tr}_{H_{c\ell p^m}(\mu_{p^m})/H_{cp^m}(\mu_{p^m})}(P_{c\ell;m})$$

in $\mathrm{Div}(X_m)$.

(b) If $m \geq 1$ then

$$U_p(P_{c;m}) = \mathrm{Tr}_{H_{cp^{m+1}}(\mu_{p^{m+1}})/H_{cp^m}(\mu_{p^{m+1}})}(P_{cp;m})$$

in $\mathrm{Div}(X_m)$.

(c) If $m \geq 1$ then

$$U_p(P_{c;m}) = \sim_{m+1;*}\left(\mathrm{Tr}_{H_{cp^{m+1}}(\mu_{p^{m+1}})/H_{cp^m}(\mu_{p^{m+1}})}(P_{c;m+1})\right)$$

in $\mathrm{Div}(X_m)$.

Proof. See [LV11, Propositions 4.7, 4.8 and 4.9]. Notice that the assumption at the end of [LV11, p.293] that $\mathcal{O}_{cp^m} = \{\pm 1\}$ is automatically verified here thanks to the first point of Assumption 2.2.6. □

Let $\varepsilon_{\mathrm{cyc}} : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character and set $p^* = (-1)^{\frac{p-1}{2}}p$. By class field theory, $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\mu_p)$ and $\mathbb{Q}(\sqrt{p^*}) \subseteq H_p$. The restriction of $\varepsilon_{\mathrm{cyc}}$ to $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q}(\sqrt{p^*}))$ takes values in $(\mathbb{Z}_p^\times)^2$, hence there is a unique continous homomorphism

$$\psi : \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}(\sqrt{p^*})) \longrightarrow \mathbb{Z}_p^\times/\{\pm 1\}$$

such that $\psi^2 = \varepsilon_{cyc}$.

Lemma 2.3.2. *Let $c;m \geq 1$ and $(c;N) = 1$. For every $\sigma \in \mathrm{Gal}(\mathbb{Q}/H_{cp^m})$ we have that*

$$\sigma(P_{c;m}) = \langle \psi(\sigma) \rangle P_{c;m}.$$

Proof. See [LV11, §4.4]. □

Chapter 3

Hida theory and big Heegner points

In his seminal papers [Hid86b] and [Hid86a], Hida described a way to build families of p-adic modular forms passing through a fixed ordinary modular form. These p-adic families have their own associated Galois representations, which will be fundamental for our work. Until today, Hida theory has been developed by many other authors in many different directions.

The aim of this chapter is to give an introduction to classical Hida theory, focusing on the Galois representation side of the matter. Nothing here is really new, but we hope that our work of summarizing and re-ordering results will be useful to somebody.

For this chapter we use the following notation:

N	a squarefree integer greater than 0;
p	a prime with the property that $p \nmid 6N$;
Γ_m	the group $\Gamma_0(N) \cap \Gamma_1(p^m)$ for some $m \geq 0$;
Γ_m	either the group $\Gamma_1(Np^m)$ or the group Γ_m for some $m \geq 0$;
	the group $1 + p\mathbb{Z}_p$;
F	a finite extension of $\mathbb{Q}_p$.

Notice that the assumptions on N and p are compatible with the choices of the same letters done in the previous chapters. We will eventually assume that they are the same numbers.

3.1 p-adic Hecke algebras

Let $m \geq 0$. Let $S_r(\Gamma_1(Np^m))$ and $S_r(\Gamma_m)$ be the spaces of cusp forms of weight $r \geq 2$ and level $\Gamma_1(Np^m)$ and $\Gamma_m := \Gamma_0(N) \cap \Gamma_1(p^m)$ respectively. We will use the letter Γ_m to denote any of the groups $\Gamma_1(Np^m)$ or Γ_m.

Definition. For any subalgebra A of $\mathbb{C}$ we define $S_r(\Gamma_m; A)$ to be the A-submodule of $S_r(\Gamma_m)$ consisting of all modular forms with Fourier coefficients in A.

We have the following integrality result.

Lemma 3.1.1. *For any subalgebra A of $\mathbb{C}$ and Γ_m as above, the map*

$$\begin{aligned} S_r(\Gamma_m; \mathbb{Z}) \otimes_{\mathbb{Z}} A &\xrightarrow{\cong} S_r(\Gamma_m; A) \\ f \otimes a &\longmapsto af \end{aligned}$$

is an isomorphism.

Proof. See [Hid00, Theorem 3.12]. □

This lemma allows us to define $S_r(\ _m; A)$ as $S_r(\ _m; \mathbb{Z}) \otimes_{\mathbb{Z}} A$ for any algebra A, not necessarily contained in $\mathbb{C}$. Since $S_r(\ _m; \mathbb{Z})$ is a finitely generated torsion-free $\mathbb{Z}$-module, it is also free over $\mathbb{Z}$. This implies that $S_r(\ _m; A)$ is finitely generated and free over A.

Definition. The space of p-adic cusp forms of level $\ _m$ and weight $r \geq 2$ is $S_r(\ _m; \mathbb{Q}_p) := S_r(\ _m; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$.

3.1.1 Hecke algebras

By [Hid00, Theorem 3.13], the usual Hecke operators T_ℓ for $\ell \nmid Np$, together with operators U_ℓ for $\ell \mid Np$ and diamond operators $\langle d \rangle$ for $d \in (\mathbb{Z}/Np^m\mathbb{Z})^\times$ acting on the space $S_r(\ _1(Np^m))$, restrict their action also to $S_r(\ _m)$. The same result implies that the space $S_r(\ _m; \mathbb{Z})$ is stable under their action, for $\ _m$ equal to $\ _1(Np^m)$ or $\ _m$. This last fact allows us to define the action of these operators on the space $S_r(\ _m; A)$ for every algebra A, by linearity.

Definition. Let A be any subring of $\mathbb{Q}_p$. Denote by $\mathbf{h}_r(\ _m; A)$ the A-algebra of all Hecke and diamond operators acting on $S_r(\ _m; A)$.

For every $A \subseteq \mathbb{Q}_p$, the space $S_r(\ _m; A)$ is generated as an A-module by $S_r(\ _m; \mathbb{Z})$ and all Hecke and diamond operators are A-linear. Hence, the A-algebra $\mathbf{h}_r(\ _m; A)$ can be naturally identified with the A-algebra generated by all Hecke and diamond operators acting on the space of p-adic cusp forms $S_r(\ _m; \mathbb{Q}_p)$. We will mainly deal with the case when A is the ring of integers of a finite extension of $\mathbb{Q}_p$.

Lemma 3.1.2. *Let F be a finite extension of $\mathbb{Q}_p$ and call $\mathcal{O}_F$ its ring of integers. Then*

$$\mathbf{h}_r(\ _m; \mathcal{O}_F) = \mathbf{h}_r(\ _m; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathcal{O}_F$$

is commutative, free of finite rank over $\mathcal{O}_F$ for every $r \geq 2$.

Proof. It is well known that $\mathbf{h}_r(\ _m; \mathbb{Z})$ is commutative, free of finite rank over $\mathbb{Z}$ (see for example [DI95, Corollary 12.4.3]). The equality $\mathbf{h}_r(\ _m; \mathcal{O}_F) = \mathbf{h}_r(\ _m; \mathbb{Z}) \otimes_{\mathbb{Z}} \mathcal{O}_F$ is just commutative algebra (see for example [Mat89, Theorem 7.11]), and the result follows. □

From now on F will be a fixed finite extension of $\mathbb{Q}_p$. The $\mathcal{O}_F$-algebra $\mathbf{h}_r(\ _m; \mathcal{O}_F)$ can be endowed with the structure of an $\mathcal{O}_F[(\mathbb{Z}/p^m N\mathbb{Z})^\times]$-algebra via the morphism

$$\begin{aligned} \mathcal{O}_F[(\mathbb{Z}/p^m N\mathbb{Z})^\times] &\longrightarrow \mathbf{h}_r(\ _1(Np^m); \mathcal{O}_F) \\ [d] &\longmapsto d^{r-2}\langle d \rangle \end{aligned} \tag{3.1}$$

for $d \in (\mathbb{Z}/p^m N\mathbb{Z})^\times$. Here we denote with square brackets the group elements of $\mathcal{O}_F[(\mathbb{Z}/p^m N\mathbb{Z})^\times]$ and with angled brackets the diamond operator in $\mathbf{h}_r(\ _m; \mathcal{O}_F)$. The choice of this map is made following [How07] and [LV11] rather than [Hid86b], [Hid86a] and [NP00], where they use a different normalization.

When $\ _m = \ _m$, the map in (3.1) factors via $\mathcal{O}_F[(\mathbb{Z}/p^m\mathbb{Z})^\times]$. For fixed $r \geq 2$ and $m \geq t \geq 1$, the inclusion of $S_r(\ _t; \overline{\mathbb{Q}}_p)$ into $S_r(\ _m; \overline{\mathbb{Q}}_p)$ induces a canonical surjective homomorphism

$$\pi_{m;t} : \mathbf{h}_r(\ _m; \mathcal{O}_F) \twoheadrightarrow \mathbf{h}_r(\ _t; \mathcal{O}_F) \tag{3.2}$$

defined by sending each Hecke operator in $h_r(\ _m;\mathcal{O}_F)$ to its corresponding one in $h_r(\ _t;\mathcal{O}_F)$.

Definition. Let $r \geq 2$. We define the big Hecke algebras of tame level N and weight r to be

$$h_{1;r} := \varprojlim_m h_r(\ _1(Np^m);\mathcal{O}_F) \quad \text{and} \quad h_r := \varprojlim_m h_r(\ _m;\mathcal{O}_F);$$

where the inverse limit is taken with respect to the maps $\ _{m;t}$ defined in (3.2).

Taking the inverse limit of the maps in (3.1), $h_{1;r}$ is naturally an algebra over

$$\mathcal{O}_F[[Z_N]] := \varprojlim_m \mathcal{O}_F[(\mathbb{Z}/p^mN\mathbb{Z})^\times];$$

where $Z_N = \varprojlim_m (\mathbb{Z}/p^mN\mathbb{Z})^\times \cong \varprojlim_m ((\mathbb{Z}/p^m\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times) = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. In particular, we can view $h_{1;r}$ also as a module over $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$. The structure map $\mathcal{O}_F[[\mathbb{Z}_p^\times]] \to h_{1;r}$ is explicitly given by

$$[z] \longmapsto z^{r-2}\langle z\rangle \tag{3.3}$$

for every $z \in \mathbb{Z}_p^\times$, where $\langle z\rangle \in h_{1;r}$ is the unique element that projects to $\langle z \pmod{p^m}\rangle$ on $h_r(\ _1(Np^m);\mathcal{O}_F)$, for every $m \geq 1$. In the same way, mutatis mutandis, also the big Hecke algebra h_r is naturally an $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$-algebra.

The decomposition $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$ induced by the Teichmuller character gives also an action of

$$\Gamma_F := \mathcal{O}_F[[1+p\mathbb{Z}_p]]$$

on $h_{1;r}$ and h_r.

3.1.2 The ordinary part

The algebras $h_{1;r}$ and h_r are too big to work with. For this reason, we are going to define canonical subalgebras, called *big ordinary Hecke algebras*. One reference for this construction is [Hid93, §7.2]. The construction is purely algebraic, so we give first a general treatment of the theory.

Lemma 3.1.3. *Let A be a ring, I an ideal of R. If R/I and I are finite, then R is finite.*

Proof. The function

$$\begin{aligned} R/I \times I &\longrightarrow R \\ (r+I;i) &\longmapsto r+i \end{aligned}$$

is clearly surjective, hence the lemma follows. □

Proposition 3.1.4. *Let $F/\mathbb{Q}_p$ be a finite extension, $\mathcal{O}_F$ the ring of integers of F. Let A be a commutative $\mathcal{O}_F$-algebra of finite rank over $\mathcal{O}_F$ and take $x \in A$.*

(a) The limit

$$e_x := \lim_n x^{n!}$$

exists in A and is an idempotent of A.

(b) If $e_x \neq 0$, then $e_x A$ is the greatest factor of A in which the projection of x is invertible.

Proof. (a) Suppose first that A is local, call $\mathfrak{m}$ its unique maximal ideal. Since A is finite over $\mathcal{O}_F$, then $A/\mathfrak{m}$ is a finite extension of the residue field of $\mathcal{O}_F$, hence the cardinality of $A/\mathfrak{m}$ is finite. Since A is Noetherian, the quotients $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ are finite vector spaces over $A/\mathfrak{m}$ for every $i \geq 1$, so, applying the previous lemma, the cardinality of $A/\mathfrak{m}^r$ is finite for every $r \geq 1$. Call

$$a_r := \#(A/\mathfrak{m}^r)^\times$$

and notice that $a_r \mid a_{r+1}$ for every $r \geq 1$. If $x \in A^\times$ (i.e. $x \notin \mathfrak{m}$), then $x^{a_r} \equiv 1 \pmod{\mathfrak{m}^i}$ for every $i \leq r$. By Krull intersection theorem, $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = 0$, hence the limit $\lim_n x^{n!}$ exists and is equal to 1, since a_r will eventually divide $n!$ for every r. If $x \notin A^\times$ (i.e. $x \in \mathfrak{m}$), then $x^{n!} \in \mathfrak{m}^{n!}$, hence $\lim_n x^{n!} = 0$.

We move now to the general case. Since A is a finite commutative algebra over a complete local noetherian ring, by [Eis13, Corollary 7.6] A is the (finite) product

$$A = \prod_{i=1}^{s} A_{\mathfrak{m}_i}$$

of the completions $A_{\mathfrak{m}_i}$ of A at all its maximal ideals $\mathfrak{m}_i$. Moreover, the topology of A as an $\mathcal{O}_F$-algebra corresponds to the product topology on $\prod_{i=1}^{s} A_{\mathfrak{m}_i}$ (this is clear when looking at the proof of [Eis13, Corollary 7.6]). We can now write our fixed element $x \in A$ as

$$x = (x_1, \dots, x_s)$$

where $x_i \in A_{\mathfrak{m}_i}$. Then, applying the result of the previous paragraph,

$$\lim_n x^{n!} = (\lim_n x_1^{n!}, \dots, \lim_n x_s^{n!}) \in \{0,1\}^s$$

is an idempotent.

(b) Follow the proof of point (a). If A is local, then $e_x \neq 0$ implies $e_x = 1$ and x invertible. If $A = \prod_{i=1}^{s} A_{\mathfrak{m}_i}$ is not local, then $e_x x$ corresponds to the s-uple where $(e_x x)_i$ is equal to x_i or 0 depending on whether $(e_x)_i = 1$ or $(e_x)_i = 0$, i.e. whether x_i is invertible or not in $A_{\mathfrak{m}_i}$. Since $e_x A$ corresponds to the product of those local factors $A_{\mathfrak{m}_i}$ such that $(e_x)_i = 1$, then $e_x x$ is invertible in $e_x A$, and $e_x A$ is maximal with this property. □

Remark 3.1.5. Point (a) of the proposition above is [Hid93, Lemma 7.2.1], but here we gave a slightly different proof, in order to have point (b) as an immediate consequence.

Now we apply this theory to our specific case, with $A = \mathbf{h}_r(\ _m; \mathcal{O}_F)$ and $x = U_p$.

Definition. Let $r \geq 2$ and $m \geq 0$. We define Hida's ordinary projector to be the idempotent

$$e^{\mathrm{ord}}_{r;m} := e_{U_p} = \lim_n U_p^{n!} \in \mathbf{h}_r(\ _m; \mathcal{O}_F);$$

whose existence is granted by point (a) of Proposition 3.1.4.

Definition. For any $\mathbf{h}_r(\ _m; \mathcal{O}_F)$-module M we define the ordinary part of M to be

$$M^{\mathrm{ord}} := e^{\mathrm{ord}}_{r;m} M:$$

Notice that when $M = \mathbf{h}_r(\ _m; \mathcal{O}_F)$ we have an algebra decomposition

$$\mathbf{h}_r(\ _m; \mathcal{O}_F) = \mathbf{h}_r(\ _m; \mathcal{O}_F)^{\mathrm{ord}} \times (1 - e^{\mathrm{ord}}_{r;m})\mathbf{h}_r(\ _m; \mathcal{O}_F).$$

By point (b) of Proposition 3.1.4, $\mathbf{h}_r(\ _m; \mathcal{O}_F)^{\mathrm{ord}}$ is the greatest factor of $\mathbf{h}_r(\ _m; \mathcal{O}_F)$ on which U_p is invertible.

By definition, the maps $\ _{m+1;m}$ defined in (3.2) satisfy

$$_{m+1;m}(e^{\mathrm{ord}}_{r;m+1}) = e^{\mathrm{ord}}_{r;m};$$

hence we can define $e^{\mathrm{ord}}_r = \varprojlim_m e^{\mathrm{ord}}_{r;m}$ in $\mathbf{h}_{1;r}$ and $\mathbf{h}_r$. This element is also called Hida's ordinary projector.

Definition. The big ordinary Hecke algebras or tame level N and weight $r \geq 2$ are the algebras

$$\mathbf{h}^{\mathrm{ord}}_{1;r} := e^{\mathrm{ord}}_r \mathbf{h}_{1;r} = \varprojlim_m \mathbf{h}_r(\ _1(Np^m); \mathcal{O}_F)^{\mathrm{ord}} \quad \text{and} \quad \mathbf{h}^{\mathrm{ord}}_r := e^{\mathrm{ord}}_r \mathbf{h}_r = \varprojlim_m \mathbf{h}_r(\ _m; \mathcal{O}_F)^{\mathrm{ord}}.$$

Also in this case, for an $\mathbf{h}_{1;r}$ or $\mathbf{h}_r$-module M we denote $e^{\mathrm{ord}}_r M$ by M^{ord}. Again, $\mathbf{h}^{\mathrm{ord}}_{1;r}$ and $\mathbf{h}^{\mathrm{ord}}_r$ are the greatest factors of $\mathbf{h}_{1;r}$ and $\mathbf{h}_r$ respectively where U_p is invertible.

3.1.3 Duality

Let A be any commutative ring and $\ _m$ be either $\ _1(Np^m)$ or $\ _m$ for some $m \geq 0$. For any cusp form $f \in S_r(\ _m; A)$ we denote with $a_n(f)$ the n-th coefficient of the Fourier expansion of f.

Definition. For every $r \geq 2$ and $m \geq 0$ we define the following pairing:

$$\begin{aligned} \langle\ ;\ \rangle : \mathbf{h}_r(\ _m; A) \times S_r(\ _m; A) &\longrightarrow A \\ (T; f) &\longmapsto a_1(Tf). \end{aligned}$$

Theorem 3.1.6. *The pairing $\langle\ ;\ \rangle$ is perfect, i.e. induces isomorphisms of A-modules*

$$\mathrm{Hom}_A(S_r(\ _m; A); A) \cong \mathbf{h}_r(\ _m; A) \quad \textit{and} \quad \mathrm{Hom}_A(\mathbf{h}_r(\ _m; A); A) \cong S_r(\ _m; A)$$

for every $r \geq 2$ and $m \geq 0$. The same pairing restricts to the ordinary parts and induces isomorphisms of A-modules

$$\mathrm{Hom}_A(S_r(\ _m; A); A)^{\mathrm{ord}} \cong \mathbf{h}_r(\ _m; A)^{\mathrm{ord}}; \quad \mathrm{Hom}_A(\mathbf{h}_r(\ _m; A)^{\mathrm{ord}}; A) \cong S_r(\ _m; A)^{\mathrm{ord}}.$$

Proof. The first part descends from [Hid00, Theorem 3.17]. The second statement is a consequence of the fact that

$$\langle T; e^{\mathrm{ord}}_{r;m} f \rangle = \langle e^{\mathrm{ord}}_{r;m} T; e^{\mathrm{ord}}_{r;m} f \rangle = \langle e^{\mathrm{ord}}_{r;m} T; f \rangle$$

for every $T \in \mathbf{h}_r(\ _m; A)$ and $f \in S_r(\ _m; A)$. □

Let now $\mathcal{O}_F$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Recall that the ring $\mathbf{h}_r(\ _m; \mathcal{O}_F)$ is an $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-algebra via the map $[d] \mapsto d^{r-2}\langle d \rangle$ (see (3.1)). We can make $S_r(\ _m; \mathcal{O}_F)$ an $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-module via

$$[d] \cdot f \mapsto d^{r-2}\langle d \rangle f. \tag{3.4}$$

This induces an $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-module structure also on $\mathrm{Hom}_A(S_r(\ _m; \mathcal{O}_F); \mathcal{O}_F)$. Then we have the following result.

Lemma 3.1.7. *If $A = \mathcal{O}_F$, the pairing $\langle\ ;\ \rangle$ and the isomorphisms of Theorem 3.1.6 are $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-equivariant.*

Proof. Straightforward. □

3.1.4 Structure theorems

In this section we sum up the most important structure theorems for the big ordinary Hecke algebras $\mathrm{h}^{\mathrm{ord}}_{1;r}$ and $\mathrm{h}^{\mathrm{ord}}_{r}$. The first has been widely studied in [Hid86b], [Hid86a] and [NP00], while the second has been used in [How07] and [LV11]. We try here to fill some gaps in literature and show how one can derive the properties of $\mathrm{h}^{\mathrm{ord}}_{r}$ from the known results about $\mathrm{h}^{\mathrm{ord}}_{1;r}$. The key result in this direction is the following lemma. Recall that at the end of Subsection 3.1.1 we defined a structure of $\quad_F$-modules for $\mathrm{h}_{1;r}$ and h_r that naturally induces a structure of $\quad_F$-modules on $\mathrm{h}^{\mathrm{ord}}_{1;r}$ and $\mathrm{h}^{\mathrm{ord}}_{r}$.

Lemma 3.1.8. *If the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$ is not divisible by p, we have that $\mathrm{h}^{\mathrm{ord}}_{r}$ is a direct summand of $\mathrm{h}^{\mathrm{ord}}_{1;r}$ as a $\quad_F$-module.*

Proof. Let $\quad$ be a fixed uniformizer of $\mathcal{O}_F$. [Hid00, Theorem 3.15] implies that the module $D_n := S^{\mathrm{ord}}_r(\quad_m; \mathcal{O}_F/\quad^n\mathcal{O}_F)$ corresponds to the submodule of fixed elements for the action of $G := (\mathbb{Z}/N\mathbb{Z})^\times$ on $E_n := S^{\mathrm{ord}}_r(\quad_1(Np^m); \mathcal{O}_F/\quad^n\mathcal{O}_F)$ via the diamond operators. The map

$$\begin{aligned} E_n &\longrightarrow E_n^G = D_n \\ x &\longmapsto \frac{1}{|G|}\sum_{g\in G} gx \end{aligned} \tag{3.5}$$

is well defined since $p \nmid |G|$ and it gives a G-equivariant splitting of the injection $D_n = E_n^G \hookrightarrow E_n$, hence D_n is a direct summand of E_n as an $(\mathcal{O}_F/\quad^n\mathcal{O}_F)$-module.

Taking inverse limits on n, we obtain that $S^{\mathrm{ord}}_r(\quad_m; \mathcal{O}_F)$ is a direct summand of $S^{\mathrm{ord}}_r(\quad_1(Np^m); \mathcal{O}_F)$ as an $\mathcal{O}_F$-module. It is immediate to see that the splitting induced by (3.5) is linear with respect to the action of $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$ on $S^{\mathrm{ord}}_r(\quad_1(Np^m); \mathcal{O}_F)$ defined in (3.4). Therefore, $S^{\mathrm{ord}}_r(\quad_m; \mathcal{O}_F)$ is a direct summand of $S^{\mathrm{ord}}_r(\quad_1(Np^m); \mathcal{O}_F)$ as an $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-module.

The duality between cusp forms and Hecke algebras (see Theorem 3.1.6 and Lemma 3.1.7) gives that $\mathrm{h}_r(\quad_m; \mathcal{O}_F)^{\mathrm{ord}}$ is a direct summand of $\mathrm{h}_r(\quad_1(Np^m); \mathcal{O}_F)^{\mathrm{ord}}$ as an $\mathcal{O}_F[(\mathbb{Z}/Np^m\mathbb{Z})^\times]$-module. Taking the inverse limit on m, we obtain the claim of the lemma. □

Theorem 3.1.9. *Let $r; r' \geq 2$.*

(a) There is a canonical isomorphism of $\quad_F$-algebras

$$\mathrm{h}^{\mathrm{ord}}_{1;r} \cong \mathrm{h}^{\mathrm{ord}}_{1;r'}$$

that sends Hecke operators T_ℓ, U_ℓ and $d^{r-2}\langle d\rangle$ to T_ℓ, U_ℓ and $d^{r'-2}\langle d\rangle$ respectively.

(b) The algebra $\mathrm{h}^{\mathrm{ord}}_{1;r}$ is finite and free over $\quad_F$ for any $r \geq 2$.

Proof. Point (a) is [Hid86a, Theorem 1.1], point (b) comes from [Hid86b, Theorem 3.1]. See also [NP00, Proposition 1.4.3]. □

Corollary 3.1.10. *If the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$ is not divisible by p, then:*

(a) The isomorphism of point (a) of Theorem 3.1.9 induces an isomorphism of $\quad_F$-algebras $\mathrm{h}^{\mathrm{ord}}_{r} \cong \mathrm{h}^{\mathrm{ord}}_{r'}$.

(b) The algebra $\mathrm{h}^{\mathrm{ord}}_{r}$ is finite and free over $\quad_F$ for any $r \geq 2$.

Proof. (a) By Lemma 3.1.8 we know that $\mathrm{h}_r^{\mathrm{ord}}$ is a direct summand of $\mathrm{h}_{1;r}^{\mathrm{ord}}$, therefore we can restrict the isomorphism of point (a) of Theorem 3.1.9 to $\mathrm{h}_r^{\mathrm{ord}}$. Since each Hecke operator is sent to the corresponding one in $\mathrm{h}_{1;r'}^{\mathrm{ord}}$, we see that $\mathrm{h}_r^{\mathrm{ord}}$ is sent surjectively to $\mathrm{h}_{r'}^{\mathrm{ord}}$.

(b) By Lemma 3.1.8, $\mathrm{h}_r^{\mathrm{ord}}$ is a direct summand of $\mathrm{h}_{1;r}^{\mathrm{ord}}$. Applying point (b) of Theorem 3.1.9 we have that $\mathrm{h}_r^{\mathrm{ord}}$ is finite and projective over $\ _F$, hence it is free since $\ _F$ is a local ring. □

Remark 3.1.11. This corollary is stated at the beginning of [How07, §2.1] and at the end of [LV11, §5.1] without proof and without the assumption of p not dividing the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$. However, we were able to derive it only assuming this further hypothesis and we still don't have a proof for the general case. An idea could be trying to follow the proof of [Hid86a, Theorem 1.1] using the group $\ _m$ instead of $\ _1(Np^m)$, but we haven't investigated further.

From now on we identify all big ordinary Hecke algebras $\mathrm{h}_{1;r}^{\mathrm{ord}}$ for all r and $\mathrm{h}_r^{\mathrm{ord}}$ for all r by means to the isomorphisms of Theorem 3.1.9 and Corollary 3.1.10 respectively, so we simply set

$$\mathrm{h}_1^{\mathrm{ord}} := \mathrm{h}_{1;2}^{\mathrm{ord}} \quad \text{and} \quad \mathrm{h}^{\mathrm{ord}} = \mathrm{h}_2^{\mathrm{ord}}.$$

We will also use the letter $\ $ to denote the group $1+p\mathbb{Z}_p$, so that $\ _F = \mathcal{O}_F[[\ ]]$, and we fix a profinite generator $\ $ of $\ $.

Definition 3.1.12. For every $r \geq 2$ and $m \geq 1$ define

- $!_{r;m} = [\ ]^{p^{m-1}} - \ ^{(r-2)p^{m-1}} \in \ _F$;
- $P_{r;\varepsilon} = [\ ] - \varepsilon(\ )\ ^{r-2} \in \mathcal{O}_F[\varepsilon][[\ ]]$ for every homomorphism $\varepsilon : \ / \ ^{p^{m-1}} \to \mathbb{Q}_p^\times$.

Notice that there are identifications $\ ^{p^{m-1}} = 1 + p^m\mathbb{Z}_p$ and $\ / \ ^{p^{m-1}} \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$.

Lemma 3.1.13. *Let $r \geq 2$ and $m \geq 1$. We have the equality*

$$!_{r;m} = \prod_{\varepsilon : \ / \ ^{p^{m-1}} \to \mathbb{Q}_p^\times} P_{r;\varepsilon} \in \ _F;$$

where the product runs over all possible homomorphisms $\varepsilon : \ / \ ^{p^{m-1}} \to \mathbb{Q}_p^\times$.

Proof. The roots of the polynomial $X^{p^{m-1}} - \ ^{(r-2)p^{m-1}}$ in $\mathbb{Q}_p$ are $\varepsilon(\ )\ ^{r-2}$ with ε varying among all possible characters of $\ / \ ^{p^{m-1}} \cong \mathbb{Z}/p^{m-1}\mathbb{Z}$. The lemma follows by substituting X with $[\ ]$. □

Corollary 3.1.14. *For a fixed $r \geq 2$, we have that $!_{r;m} \mid !_{r;m+1}$ in $\ _F$ for every $m \geq 1$.*

Proof. Appling Lemma 3.1.13 we find that

$$!_{r;m+1} = \prod_{\varepsilon : \ / \ ^{p^m} \to \mathbb{Q}_p^\times} P_{r;\varepsilon} = \prod_{\varepsilon : \ / \ ^{p^{m-1}} \to \mathbb{Q}_p^\times} P_{r;\varepsilon} \cdot \prod_{\substack{\varepsilon : \ / \ ^{p^m} \to \mathbb{Q}_p^\times \\ \varepsilon \text{ primitive}}} P_{r;\varepsilon} = !_{r;m} \cdot \prod_{\substack{\varepsilon : \ / \ ^{p^m} \to \mathbb{Q}_p^\times \\ \varepsilon \text{ primitive}}} P_{r;\varepsilon}.$$

□

Following the conventions of [Hid86b] and [Hid86a], for any congruence subgroup $_0(Np^m) \supseteq \quad \supseteq \ _1(Np^m)$ and for any character $\quad$ of $\ / \ _1(Np^m)$ we denote by $S_r(\ ;\ )$ the subspace of $S_r(\ _1(Np^m))$ made by all modular forms such that the modular action of matrices in $\quad$ factors via $\quad$ on them. We will use a similar notation for the corresponding algebras of Hecke operators.

Theorem 3.1.15. *The canonical maps* $h_1^{ord} \xrightarrow{\cong} h_{1;r}^{ord} \to h_r(\ _1(Np^m); \mathcal{O}_F)^{ord}$ *induce isomorphisms*

$$h_1^{ord}/P_{r;"}h_1^{ord} \xrightarrow{\cong} h_r(\ _1(Np) \cap \ _0(p^m); "; \mathcal{O}_F)^{ord}; \quad h_1^{ord}/!_{r;m}h_1^{ord} \xrightarrow{\cong} h_r(\ _1(Np^m); \mathcal{O}_F)^{ord}$$

for every $r \geq 2$, $m \geq 1$ *and* $" : \ / \ ^{p^{m-1}} \to \mathcal{O}_F^\times$.

Proof. This is a consequence of [Hid86a, Theorem 1.2]. In particular, the images of the elements $P_{r;"}$ of [Hid86a, Theorem 1.2] in h_1^{ord} via Hida's structure map (that differs from ours for a factor) correspond (up to a unit) to the images of our elements $P_{r;"} = [\ ] - "(\ )\ ^{r-2}$ in h_1^{ord} via our structure map.

Then our element $!_{r;m}$ coincides up to a unit with the element with the same name defined by Hida a few lines after [Hid86a, Theorem 1.2], and the lemma follows. See also [NP00, Proposition 1.4.3]. □

Corollary 3.1.16. *If* p *does not divide the cardinality of* $(\mathbb{Z}/N\mathbb{Z})^\times$, *the canonical maps* $h^{ord} \xrightarrow{\cong} h_r^{ord} \to h_r(\ _m; \mathcal{O}_F)^{ord}$ *induce isomorphisms*

$$h^{ord}/P_{r;"}h^{ord} \xrightarrow{\cong} h_r(\ _1(p) \cap \ _0(Np^m); "; \mathcal{O}_F)^{ord}; \quad h^{ord}/!_{r;m}h^{ord} \xrightarrow{\cong} h_r(\ _m; \mathcal{O}_F)^{ord}$$

for every $r \geq 2$, $m \geq 1$ *and* $" : \ / \ ^{p^{m-1}} \to \mathcal{O}_F^\times$.

Proof. Immediate from Theorem 3.1.15 and the splitting of Lemma 3.1.8. □

Remark 3.1.17. In the previous theorem, the character $"$ is seen as a character of $(\ _1(p) \cap \ _0(Np^m))/\ _1(Np^m)$ via the natural isomorphism

$$(\ _1(p) \cap \ _0(Np^m))/\ _1(Np^m) \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \mathbb{Z}/p^{m-1}\mathbb{Z} \cong (\mathbb{Z}/N\mathbb{Z})^\times \times \ / \ ^{p^{m-1}};$$

being by definition the trivial character on the factor $(\mathbb{Z}/N\mathbb{Z})^\times$.

3.2 Hida families

In the previous section we studied the structure of p-adic big ordinary Hecke algebras. We now fix a cusp form (with certain properties) and see that it defines a decomposition of the big ordinary Hecke algebra that is associated, by duality, to a family of p-adic cusp forms. We will then focus on the Galois representation attached to this family.

3.2.1 A fixed cusp form f

We review some terminology and some facts about cusp forms. Let $M \geq 1$ and $k \geq 2$ be integers. For every congruence subgroup $\quad$ contained in $SL_2(\mathbb{Z})$, there is the so called Petersson inner product, defined by

$$\langle f; g \rangle_P = \frac{1}{V} \int_{X(\ )} f(z)g(z)\,\mathrm{Im}(z)^k d\ (z)$$

for every $f;g \in S_k(\ )$, where $X(\ )$ is the compact modular curve attached to , $d\ (z) = \frac{dxdy}{y^2}$ is the hyperbolic measure of the upper-half plane (for $z = x+iy$), V is the volume of $X(\ )$ with respect to and g denotes the complex conjugate of g. For more details, see for example [DS05, §5.4]. The Petersson inner product is Hermitian-symmetric and positive definite.

Definition. For each divisor d of M we define

$$\begin{aligned} i_d : (S_k(\ _1(M/d)))^2 &\longrightarrow S_k(\ _1(M)) \\ (f;g) &\longmapsto f + \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) g. \end{aligned}$$

If $M = AB$ with $(A;B) = 1$, the subspace of B-old cusp forms of level M is

$$S_k^{B-\mathrm{old}}(\ _1(M)) := \sum_{\substack{d|M \\ (d;B)\neq 1}} i_d\,(S_k(\ _1(M/d)))^2.$$

The subspace $S_k^{B-\mathrm{new}}(\ _1(M))$ of B-new cusp forms of level M is the orthogonal complement of $S_k^{B-\mathrm{old}}(\ _1(M))$ with respect to the Petersson inner product.

When $B = M$ we will write S_k^{old} and S_k^{new} instead of $S_k^{M-\mathrm{old}}$ and $S_k^{M-\mathrm{new}}$ respectively. The spaces $S_k^{B-\mathrm{old}}(\ _1(M))$ and $S_k^{B-\mathrm{new}}(\ _1(M))$ are stable under the action of all Hecke and diamond operators (see [DS05, Proposition 5.6.2]). Notice that there is the decomposition

$$S_k(\ _1(M))^{B-\mathrm{new}} = \bigoplus_{B|P|M} \left[\bigoplus_{d|\frac{M}{P}} i_d(S_k(\ _1(P))^{\mathrm{new}})^2 \right];$$

as remarked also in [MT99, Equation 3.4].

Definition. Let $f \in S_k(\ _1(M))$. We say that f is an eigenform if it is an eigenvector for the action of all Hecke operators T_ℓ for $\ell \nmid M$, U_ℓ for $\ell \mid M$ and $\langle d \rangle$ for all $d \in \mathbb{Z}_{>0}$. An eigenform $f(z) = \sum_{n=1}^{\infty} a_n(f) q^n$ is normalized if $a_1(f) = 1$.

Proposition 3.2.1. *Let $f \in S_k(\ _1(M))$ be a normalized eigenform. Then there is a normalized eigenform $g \in S_k(\ _1(P))^{\mathrm{new}}$ for a uniquely determined $P \mid M$ such that $a_n(g) = a_n(f)$ for all n coprime with M.*

Proof. See [DS05, Proposition 5.8.4]. □

The level P of the newform g in the proposition is called the conductor of f.

Definition. Let $f \in S_k(\ _1(M); \mathcal{O}_F)$ for some finite extension F of $\mathbb{Q}_p$. We say that f is p-ordinary if $a_p(f) \in \mathcal{O}_F^\times$.

Definition. Let $f \in S_k(\ _1(Np^m); \mathcal{O}_F)$ with $k \geq 2$. We say that f is an ordinary p-stabilized newform of tame level N if $m \geq 1$, f is p-ordinary and the conductor of f is divisible by N.

As remarked in [NP00], f is an ordinary p-stabilized newform of tame level N if and only if f is p-ordinary and is either a newform on $\ _1(Np^t)$ for some $t \geq 1$ or it is equal to the p-stabilization of a newform on $\ _1(N)$. For more on p-stabilizations, see [NP00, §1.3.6] or [Vig22, §2.4].

We now fix embeddings $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and $\mathbb{Q} \hookrightarrow \mathbb{C}$, so that the Teichmuller character $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ can be seen as a Dirichlet character modulo p. For the rest of the thesis we fix

$$f = \sum_{n>0} a_n(f) q^n \in S_k(\Gamma_0(Np); \omega^j)$$

to be a normalized eigenform of weight $k \geq 2$ and character ω^j for some $j \geq 0$ (here, as usual, $q = e^{2\pi iz}$ for $z \in \mathcal{H}$). Since ω is an odd character (i.e. $\omega(-1) = -1$), the existence of such a form implies that $j \equiv k \pmod 2$.

Fix now a finite extension $F/\mathbb{Q}_p$ that contains all Fourier coefficients of f, that in fact lie in the ring of integers $\mathcal{O}_F$ of F (see [DS05, Theorem 6.5.1]).

Assumption 3.2.2. We require that f is an ordinary p-stabilized newform of tame level N without complex multiplication (in the sense of [Rib77, p. 34]).

3.2.2 The Hida family passing through f - Hida's version

In this subsection we describe the construction of Hida families following the work of Hida in [Hid86a, §1] (see also [LV11, §5.3] and [NP00, §1.4.4]). We will assume that p does not divide the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$, so that $\mathbf{h}^{\mathrm{ord}}$ is a direct summand of $\mathbf{h}_1^{\mathrm{ord}}$ as a Λ_F-module (here F is the field chosen at the end of the previous subsection).

Local decomposition

Since $\mathbf{h}^{\mathrm{ord}}$ and $\mathbf{h}_1^{\mathrm{ord}}$ are finitely generated commutative Λ_F-modules, a classical result in commutative algebra (see [Eis13, Corollary 7.6]) implies that they split as finite products

$$\mathbf{h}^{\mathrm{ord}} = \prod_{\mathfrak{m}} \mathbf{h}^{\mathrm{ord}}_{\mathfrak{m}} \quad \text{and} \quad \mathbf{h}_1^{\mathrm{ord}} = \prod_{\mathfrak{n}} \mathbf{h}^{\mathrm{ord}}_{1;\mathfrak{n}} \tag{3.6}$$

of their localizations (equivalently, completions) at their maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ respectively. Every summand appearing in these decompositions is a complete local ring, finite and free over Λ_F since $\mathbf{h}^{\mathrm{ord}}$ and $\mathbf{h}_1^{\mathrm{ord}}$ are so by Theorem 3.1.9 and Corollary 3.1.10. Moreover, since $\mathbf{h}^{\mathrm{ord}}$ is a direct summand of $\mathbf{h}_1^{\mathrm{ord}}$, it happens that each $\mathbf{h}^{\mathrm{ord}}_{\mathfrak{m}}$ coincides with one of the $\mathbf{h}^{\mathrm{ord}}_{1;\mathfrak{n}}$. In general, these local factors are not integral domains; to get a further decomposition we can proceed in two ways. In this subsection we follow the approach of Hida. Call $\mathcal{L}$ the fraction field of Λ_F.

Lemma 3.2.3. *There are splitting of $\mathcal{L}$-algebras*

$$\mathbf{h}^{\mathrm{ord}} \otimes_{\Lambda_F} \mathcal{L} = \left(\prod_{i \in I} \mathcal{F}_i\right) \oplus \mathcal{M} \quad \textit{and} \quad \mathbf{h}_1^{\mathrm{ord}} \otimes_{\Lambda_F} \mathcal{L} = \left(\prod_{j \in J} \mathcal{K}_j\right) \oplus \mathcal{N}$$

where $\mathcal{K}_j$ are finite field extensions of $\mathcal{L}$, $\{\mathcal{F}_i\}_{i\in I}$ is a subset of $\{\mathcal{K}_j\}_{j\in J}$, $\mathcal{M}$ and $\mathcal{N}$ are nilpotent.

Proof. The algebras $\mathbf{h}^{\mathrm{ord}} \otimes_{\Lambda_F} \mathcal{L}$ and $\mathbf{h}_1^{\mathrm{ord}} \otimes_{\Lambda_F} \mathcal{L}$ are finite-dimensional artinian algebras over $\mathcal{L}$. The field $\mathcal{L}$ has characteristic 0, therefore it is perfect. Moreover, for artinian algebras, the nilradical is nilpotent and coincides with the Jacobson radical (see [AM69, Corollary 8.2 and Proposition 8.4]). Therefore, by Weddeburn principal theorem, every finite dimensional algebra over $\mathcal{L}$ splits into the sum of a semisimple and a nilpotent algebra. A semisimple finitely generated artinian algebra over $\mathcal{L}$ is the product of finite field extensions of $\mathcal{L}$. □

In Hida's terminology, the fields $\mathcal{F}_i$ and $\mathcal{K}_j$ are called primitive components of $\mathfrak{h}_1^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}$ and $\mathfrak{h}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}$, respectively. The splittings of (3.6) induce the decompositions

$$\mathfrak{h}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L} = \prod_{\mathfrak{m}} (\mathfrak{h}_{\mathfrak{m}}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}) \quad \text{and} \quad \mathfrak{h}_1^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L} = \prod_{\mathfrak{n}} (\mathfrak{h}_{1;\mathfrak{n}}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}):$$

Definition. We say that $\mathcal{F}_i$ (resp. $\mathcal{K}_j$) belongs to $\mathfrak{m}$ (resp. $\mathfrak{n}$) if it is a direct summand of $\mathfrak{h}_{\mathfrak{m}}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}$ (resp. $\mathfrak{h}_{1;\mathfrak{n}}^{\mathrm{ord}} \otimes_{\mathcal{O}_F} \mathcal{L}$).

The Hida family passing through f

Recall that the algebras $\mathfrak{h}^{\mathrm{ord}}$ and $\mathfrak{h}_1^{\mathrm{ord}}$ are $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$-modules. Our fixed cuspform f determines, using the duality of Theorem 3.1.6, an $\mathcal{O}_F$-algebra map

$$\lambda_f : \mathfrak{h}^{\mathrm{ord}} \twoheadrightarrow \mathfrak{h}_k(\Gamma_0(N) \cap \Gamma_1(p); \mathcal{O}_F)^{\mathrm{ord}} \longrightarrow \mathcal{O}_F \tag{3.7}$$

characterized by $\lambda_f(T_\ell) = a_\ell(f)$ for $\ell \nmid Np$, $\lambda_f(U_\ell) = a_\ell(f)$ for $\ell \mid Np$ and

$$\lambda_f([\gamma]) = \gamma^{k+j-2}; \qquad \lambda_f([\delta]) = \delta^{k-2}$$

for $\gamma \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $\delta \in \Gamma = 1 + p\mathbb{Z}_p$. We define also a morphism $\lambda_{1;f} : \mathfrak{h}_1^{\mathrm{ord}} \to \mathcal{O}_F$ by pre-composing λ_f with the natural projection $\mathfrak{h}_1^{\mathrm{ord}} \twoheadrightarrow \mathfrak{h}^{\mathrm{ord}}$.

Since $\mathcal{O}_F$ is a domain, the maps λ_f and $\lambda_{1;f}$ factor through a unique local factor of $\mathfrak{h}^{\mathrm{ord}}$ and $\mathfrak{h}_1^{\mathrm{ord}}$ respectively. Call $\mathfrak{m}_f$ and $\mathfrak{n}_f$ the maximal ideals corresponding to these two local factors, respectively. Since $\mathfrak{h}^{\mathrm{ord}}$ is a direct summand of $\mathfrak{h}_1^{\mathrm{ord}}$, we have that $\mathfrak{h}_{\mathfrak{m}_f}^{\mathrm{ord}} = \mathfrak{h}_{1;\mathfrak{n}_f}^{\mathrm{ord}}$. Since from now on we will work with this local component, it happens that there is no difference in using $\mathfrak{h}^{\mathrm{ord}}$ or $\mathfrak{h}_1^{\mathrm{ord}}$, as long as the first is a direct summand of the second (that is always the case if we assume that p does not divide the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$).

Making a finite extension of F, we can assume that F is equal to the algebraic closure of $\mathbb{Q}_p$ in $\mathcal{K}$ for any field $\mathcal{K} = \mathcal{K}_j$ appearing in the decomposition of Lemma 3.2.3 (see [Hid86b, Proposition 3.4]). We define $\mathfrak{h}(\mathcal{K})$ to be the image of $\mathfrak{h}_1^{\mathrm{ord}}$ in $\mathcal{K}$, $\mathfrak{h}(\mathcal{K})$ to be the free $\mathcal{O}_F$-closure of $\mathfrak{h}(\mathcal{K})$ in $\mathcal{K}$ and $\mathcal{J}(\mathcal{K})$ to be the integral closure of $\mathcal{O}_F$ in $\mathcal{K}$. Equivalently, $\mathfrak{h}(\mathcal{K})$ is the intersection of all localizations of $\mathfrak{h}(\mathcal{K})$ at height one prime ideals of $\mathcal{O}_F$, and it is free of finite rank over $\mathcal{O}_F$. As noted in [NP00, §1.4.4], there are inclusions

$$\mathfrak{h}(\mathcal{K}) \subseteq \mathfrak{h}(\mathcal{K}) \subseteq \mathcal{J}(\mathcal{K}):$$

For every $r \geq 2$, $m \geq 1$ and character $\varepsilon : (\mathbb{Z}/p^{m-1}\mathbb{Z})^\times \to \mathcal{O}_F^\times$ we have a natural morphism

$$\pi_{r;\varepsilon} : \mathfrak{h}_1^{\mathrm{ord}}/P_{r;\varepsilon}\mathfrak{h}_1^{\mathrm{ord}} \longrightarrow \mathfrak{h}(\mathcal{K})/P_{r;\varepsilon}\mathfrak{h}(\mathcal{K})$$

induced by the projection of $\mathfrak{h}_1^{\mathrm{ord}}$ into $\mathfrak{h}(\mathcal{K})$.

Definition. Let $r \geq 2$, $m \geq 1$ and $\varepsilon : (\mathbb{Z}/p^{m-1}\mathbb{Z})^\times \to \mathcal{O}_F^\times$ be a character. Take $g \in S_r(\Gamma_1(Np) \cap \Gamma_0(p^m); \varepsilon; \mathcal{O}_F)^{\mathrm{ord}}$ and fix a local component $\mathcal{K}$ appearing in the decomposition of Lemma 3.2.3. We say that g belongs to $\mathcal{K}$ if there is a map λ' making the diagram

$$\begin{array}{ccc} \mathfrak{h}_1^{\mathrm{ord}}/P_{r;\varepsilon}\mathfrak{h}_1^{\mathrm{ord}} & \xrightarrow{\pi_{r;\varepsilon}} & \mathfrak{h}(\mathcal{K})/P_{r;\varepsilon}\mathfrak{h}(\mathcal{K}) \\ \cong\downarrow & & \downarrow\lambda' \\ \mathfrak{h}_r^{\mathrm{ord}}(\Gamma_1(Np) \cap \Gamma_0(p^m); \varepsilon; \mathcal{O}_F) & \xrightarrow[g]{} & \mathcal{O}_F \end{array}$$

commutative, where $_g$ is the map attached to g by duality.

Theorem 3.2.4 (Hida). *Let $r \geq 2$, $m \geq 1$ and $" : \ / \ ^{p^{m-1}} \to \mathcal{O}_F^\times$ be a character. If g is an ordinary p-stabilized newform of tame level N in $S_r(\ _1(Np) \cap \ _0(p^m); "; \mathcal{O}_F)$, there is a unique field $\mathcal{K}_g$ to which g belongs.*

Proof. See [Hid86a, Corollary 1.3]. □

We now fix the field $\mathcal{K}_f$ to which our fixed cusp form f belongs. Then $\mathcal{K}_f$ belongs to the maximal ideal $\mathfrak{n}_f$ of $\mathbb{h}_1^{\mathrm{ord}}$. Since the form f has trivial character at N, the field $\mathcal{K}_f$ is also a local component of $\mathbb{h}^{\mathrm{ord}} \otimes \ _F \mathcal{L}$ and the field $\mathcal{K}_f$ belongs to the maximal ideal $\mathfrak{m}_f$ of $\mathbb{h}^{\mathrm{ord}}$. We call $\mathcal{R}_f := \mathcal{J}(\mathcal{K}_f)$ the integral closure of $\ _F$ in $\mathcal{K}_f$.

Definition. The local ring $\mathbb{h}^{\mathrm{ord}}_{1;\mathfrak{n}_f} = \mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ is called the Hida family of f and the ring $\mathcal{R}_f$ is the branch of the Hida family on which f lives.

Theorem 3.2.5. *The ring $\mathcal{R}_f$ is a complete local Noetherian domain which is finitely generated over $\ _F$. Moreover, it is a Cohen-Macaulay ring, free over $\ _F$.*

Proof. The first part is [LV11, Proposition 5.2]. Since $\mathcal{R}_f$ has Krull dimension 2 and is integrally closed, Serre's criterion for normality implies that it is a Cohen-Macaulay ring. By miracle flatness, we conclude that $\mathcal{R}_f$ is free over $\ _F$. □

The natural map

$$f_\infty : \mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \longrightarrow \mathbb{h}(\mathcal{K}_f) \longrightarrow \mathcal{R}_f \tag{3.8}$$

gives a structure of $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$-module on $\mathcal{R}_f$.

3.2.3 The Hida family passing through f - Nekovář's version

In this section we relate Hida's version (used also in [LV11]) with Nekovář's version (used for example in [Nek06, §12.7], [How07] and [Büy14]) of Hida theory. The difference lies in the definition of the branch of the Hida family passing through the fixed cusp form f.

Lemma 3.2.6. *Let $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ and $\mathcal{K}_f$ be the components to which f belongs (in the sense of the previous section). Then the kernel of the natural map*

$$\ : \ \mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \twoheadrightarrow \mathbb{h}(\mathcal{K}_f)$$

is a minimal prime of $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ contained in the kernel of $\ _f$.

Proof. The kernel of $\ $ is prime since $\mathbb{h}(\mathcal{K}_f)$ is a domain. Moreover, since both $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}}$ and $\mathbb{h}(\mathcal{K}_f)$ have Krull dimension 2, the kernel of $\ $ must be a minimal prime. Since f belongs to $\mathcal{K}_f$, the map $\ _f$ factors through $\ $ and we obtain that $\ker(\ ) \subseteq \ker(\ _f)$. □

It is also known (see [Nek06, §12.7.5] or [Hid86a, Corollary 1.4]) that the localization of $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ at $\ker(\ _f)$ is a discrete valuation ring, unramified over the localization of $\ _F$ at $\ _F \cap \ker(\ _f)$. Therefore, $\ker(\ )$ is the unique minimal prime of $\mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ contained in $\ker(\ _f)$.

Definition. The Nekovář branch of the Hida family on which f lives is the ring $R_f := \mathbb{h}^{\mathrm{ord}}_{\mathfrak{m}_f} / \ker(\ )$.

Lemma 3.2.7. *The ring R_f is a complete local Noetherian domain which is finitely generated over $\_F$. It is a Cohen-Macaulay ring, free over $\_F$. The integral closure of R_f in its field of fractions $\mathcal{K}_f$ is $\mathcal{R}_f$.*

Proof. By Lemma 3.2.6 we know that R_f is isomorphic to $\mathrm{h}(\mathcal{K}_f)$, therefore the first and the last sentences are trivial. The fact that R_f is Cohen-Macaulay and free over $\_F$ is verified in [Fou13, Lemma 3.6]. □

Comparing Theorem 3.2.5 with Lemma 3.2.7 one can notice that $\mathcal{R}_f$ and R_f have the same relevant algebraic properties, except for normality. With the same notation as in Hida's setting we denote by $f_\infty := \ : \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \twoheadrightarrow R_f$ the quotient map.

3.2.4 Arithmetic primes

We now study some properties of Hida families. With this purpose, we introduce the concept of arithmetic primes following [NP00, §1.4.4], [How07, §2.1] and [LV11, §5.5].

Definition ([How07]). Let A be a finite commutative $\_F$-algebra. An $\mathcal{O}_F$-algebra map $A \to \mathbb{Q}_p$ is arithmetic if the composition

$$\xrightarrow{\mapsto[\ ]} A^\times \longrightarrow \mathbb{Q}_p^\times$$

has the form $\ \mapsto\ (\ )^{r-2}$ for some $r \geq 2$ and some finite order character $\ $ of $\ $. The kernel of an arithmetic map is called an arithmetic prime of A.

As noted in [Nek06, §12.7.2 and §12.7.4], the arithmetic primes of A are exactly all primes lying above $P_{r';\varepsilon'\ F'} \cap \ _F$ for some $r' \geq 2$, F' finite extension of F and $\varepsilon' : \ \to \mathcal{O}_{F'}$ finite order character.

Given an arithmetic prime $\mathfrak{p}$, the residue field $F_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = \mathrm{Frac}(A/\mathfrak{p})$ is a finite extension of F. The composition $\ \to A^\times \to F_\mathfrak{p}^\times$ has the form $\ \mapsto\ _\mathfrak{p}(\ )^{r_\mathfrak{p}-2}$ for a finite order character $\ _\mathfrak{p} : \ \to F_\mathfrak{p}^\times$ called the wild character of $\mathfrak{p}$ and an integer $r_\mathfrak{p} \geq 2$ called the weight of $\mathfrak{p}$.

Example 3.2.8. The map $\ _f : \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \to \mathcal{O}_F$ is an arithmetic map with trivial wild character and weight k.

Theorem 3.2.9 (Hida). *Ler $\mathcal{R}$ be any of R_f or $\mathcal{R}_f$ and fix an arithmetic prime $\mathfrak{p}$ of $\mathcal{R}$ of weight $r_\mathfrak{p}$ and character $\ _\mathfrak{p}$. Set $m_\mathfrak{p}$ to be the maximum between 1 and the p-adic order of the conductor of $\ _\mathfrak{p}$. Then the composition*

$$\mathrm{h}^{\mathrm{ord}} \longrightarrow \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \xrightarrow{f_\infty} \mathcal{R} \longrightarrow F_\mathfrak{p}$$

factors through $\mathrm{h}_{r_\mathfrak{p}}(\ _{m_\mathfrak{p}}; \mathcal{O}_F)$ and determines by duality an ordinary p-stabilized newform

$$f_\mathfrak{p} \in S_{r_\mathfrak{p}}(\ _0(Np^{m_\mathfrak{p}}); \ _\mathfrak{p}\, !^{k+j-r}; F_\mathfrak{p}).$$

Proof. See [How07, p.97], [LV11, p.300] and [Nek06, §12.7.4 and §12.7.5]. □

Remark 3.2.10. For more insights on why there is no difference in using $\mathcal{R}_f$ or R_f in Theorem 3.2.9, see [NP00, Proposition 1.4.6]. From now on we fix $\mathcal{R} := \mathcal{R}_f$, but everything can be probably done also using R_f instead.

3.3 The big Galois representations attached to a Hida family

Hida in [Hid86a, §2] showed a canonical way to build a Galois representation attached to a Hida family of modular forms. We will be interested in a twist of Hida's representation, therefore we will mainly follow [How07, §2] and [LV11, §5]. We first briefly recall how one can attach a p-adic Galois representation to the fixed modular form f.

3.3.1 Deligne's Galois representation attached to f

For the content of this subsection we mostly refer to [Vig22, §2]. According to Deligne [Del06a] there is an $\mathcal{O}_F$-module T_f of rank 2 with an action of $G_{\mathbb{Q}}$ such that the representation

$$\rho_f : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(T_f) \cong \mathrm{GL}_2(\mathcal{O}_F) \subseteq \mathrm{GL}_2(F)$$

attached to f has the property that the characteristic polynomial of the *arithmetic* Frobenius Fr_ℓ at every prime $\ell \nmid Np$ is

$$X^2 - a_\ell(f)X + \psi^j(\ell)\ell^{k-1}.$$

We also set $V_f := T_f \otimes_{\mathcal{O}_F} F$.

Definition. Let π_F be a uniformizer of $\mathcal{O}_F$. The composition

$$G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(T_f) \longrightarrow \mathrm{GL}(T_f/\pi_F T_f)$$

is called the residual representation attached to ρ_f, and will be denoted by $\bar{\rho}_f$.

From now on, as in [LV11, Assumption 5.1], we assume the following property on the residual representation attached to f.

Assumption 3.3.1. The residual representation $\bar{\rho}_f$ is p-distinguished and absolutely irreducible.

Here we recall that $\bar{\rho}_f$ is said to be p-distinguished if its restriction to a decomposition group D_p at p can be put in the shape $\bar{\rho}_f|_{\mathrm{D}_p} = \left(\begin{smallmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{smallmatrix}\right)$ for characters $\varepsilon_1 \neq \varepsilon_2$ (see [Gha05, Definition 4]). Notice that, since f is p-ordinary, it is a result due to Mazur and Wiles that $\bar{\rho}_f|_{\mathrm{D}_p}$ is always upper triangular (see [Gha05, §1]).

Remark 3.3.2. Absolute irreducibility of $\bar{\rho}_f$ is equivalent to irreducibility, as remarked for example in [Vig22, Remark 2.5]. Notice also that since $\bar{\rho}_f$ is irreducible, it coincides with its semisimplification.

3.3.2 Critical characters

We now go back to the context of Hida families and define critical characters, following [How07, p. 96] and [LV11, §5.4].

Definition. Factor the p-adic cyclotomic character $\varepsilon_{\mathrm{cyc}} : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ as the product $\varepsilon_{\mathrm{cyc}} = \varepsilon_{\mathrm{tame}} \cdot \varepsilon_{\mathrm{wild}}$ with $\varepsilon_{\mathrm{tame}} : G_{\mathbb{Q}} \to \quad_{p-1}$ and $\varepsilon_{\mathrm{wild}} : G_{\mathbb{Q}} \to \quad$. Define the critical character $\quad : G_{\mathbb{Q}} \to \quad_F^\times$ by

$$= \varepsilon_{\mathrm{tame}}^{\frac{k+j}{2}-1} \cdot \left[\varepsilon_{\mathrm{wild}}^{1/2}\right]$$

where $\varepsilon_{\mathrm{wild}}^{1/2}$ is the unique square root of $\varepsilon_{\mathrm{wild}}$ taking values in $\quad$.

Decompose $\mathbb{Z}_p^\times = \quad \times \quad$ and recall that $! : \quad \to \quad_{p-1}$ is the Teichmüller character. For each $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ define the idempotent

$$e_i := \frac{1}{p-1} \sum_{\in} !^{-i}(\ )[\ ] \in \mathcal{O}_F[[\mathbb{Z}_p^\times]];$$

that satisfies the relation

$$e_i \cdot [\ ] = \ ^i \cdot e_i \quad \text{for all} \quad \in \ _{p-1}:$$

We can see e_i in $\mathrm{h}^{\mathrm{ord}}$ via the structure map induced by (3.3). Since $\ _f(e_i) = 0$ for every $i \neq k+j-2$, we must have

$$e_{k+j-2}\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f} = \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f};$$

therefore the image of e_{k+j-2} is a unit in $\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$. Combining the last two equations, we obtain that $[\,''_{\mathrm{tame}}] = \ ''^{k+j-2}_{\mathrm{tame}}$ in $\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$. It follows that

$$^2 = [\,''_{\mathrm{cyc}}] \quad \text{in } \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f};$$

and therefore also in R_f and in $\mathcal{R} = \mathcal{R}_f$ via the map f_∞. In particular, for every prime $\ell \nmid p$, the relation

$$^2(\mathrm{Fr}_\ell) = [\,''_{\mathrm{cyc}}(\mathrm{Fr}_\ell)] = [\ell] \tag{3.9}$$

holds in $\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$, R_f and $\mathcal{R}$, for every chosen frobenius element Fr_ℓ at ℓ.

Definition. Let $\mathcal{R}^\dagger$ denote $\mathcal{R}$ as a module over itself but with $G_{\mathbb{Q}}$ acting through the character $\ ^{-1}$.

3.3.3 The big Galois representation

For every integer $m \geq 0$ denote by $X_{0;1}(N;p^m)$ the compactified modular curve of level structure $\ _m = \ _0(N) \cap \ _1(p^m)$, viewed as a scheme over $\mathbb{Q}$, by $\mathrm{Jac}(X_{0;1}(N;p^m))$ its Jacobian variety and by $\mathrm{Ta}_p(\mathrm{Jac}(X_{0;1}(N;p^m)))$ the p-adic Tate module of the Jacobian, i.e. the inverse limit of all the p^n-th torsion subgroups of the Jacobian. All Hecke and diamond operators act on $\mathrm{Jac}(X_{0;1}(N;p^m))$ and on $\mathrm{Ta}_p(\mathrm{Jac}(X_{0;1}(N;p^m)))$ via the Albanese action. There is also a natural action of $G_{\mathbb{Q}}$ on them, coming from the fact that the curve $X_{0;1}(N;p^m)$ is defined over $\mathbb{Q}$.

As in [How07, §2.1] and [LV11, §5.5], for every integer $m \geq 1$ we define $\mathrm{h}^{\mathrm{ord}}$-modules

$$\begin{aligned}
\mathrm{Ta}^{\mathrm{ord}}_{p;m} &:= e^{\mathrm{ord}}\Big(\mathrm{Ta}_p(\mathrm{Jac}(X_{0;1}(N;p^m))) \otimes_{\mathbb{Z}_p} \mathcal{O}_F\Big) \\
\mathbf{Ta}^{\mathrm{ord}} &:= \varprojlim_m \mathrm{Ta}^{\mathrm{ord}}_{p;m} \\
\mathbf{Ta}^{\mathrm{ord}}_{\mathfrak{m}_f} &:= \mathbf{Ta}^{\mathrm{ord}} \otimes_{\mathrm{h}^{\mathrm{ord}}} \mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f} \\
\mathbf{T} &:= \mathbf{Ta}^{\mathrm{ord}}_{\mathfrak{m}_f} \otimes_{\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}} \mathcal{R}:
\end{aligned}$$

All these modules are endowed with $\mathrm{h}^{\mathrm{ord}}$-linear actions of the Galois group $G_{\mathbb{Q}}$, and the inverse limit in the definition of $\mathbf{Ta}^{\mathrm{ord}}$ is taken with respect to the maps induced by the degeneracy maps $X_{0;1}(N;p^{m+1}) \to X_{0;1}(N;p^m)$.

Write $\mathfrak{m}_{\mathcal{R}}$ for the maximal ideal of the local ring $\mathcal{R}$ and set $\mathrm{F}_{\mathcal{R}} := \mathcal{R}/\mathfrak{m}_{\mathcal{R}}$ for the residue field of $\mathcal{R}$. Denote with $\mathbf{T} := \mathbf{T}/\mathfrak{m}_{\mathcal{R}}\mathbf{T}$ for the residual representation attached to $\mathbf{T}$.

Theorem 3.3.3. *The residual $G_{\mathbb{Q}}$-representation $\mathbf{T}$ is equivalent up to a finite base change to the residual representation $\ _f$ of f. In particular, it is absolutely irreducible.*

Proof. See [LV11, Proposition 5.4]. □

The big Galois representation has the following fundamental property with respect to the arithmetic specializations.

Theorem 3.3.4. *For every arithmetic prime $\mathfrak{p}$ of $\mathcal{R}$ the representation $\mathbf{T} \otimes_{\mathcal{R}} F_{\mathfrak{p}}$ is equivalent up to a finite base change to the representation $V_{f_{\mathfrak{p}}}$ attached by Deligne to the modular form $f_{\mathfrak{p}}$ attached to $\mathfrak{p}$ via Theorem 3.2.9.*

Proof. See [NP00, (1.5.5)] (see also [Vig22, §2.5]). □

Definition. The critical twist of $\mathbf{T}$ is the $G_{\mathbb{Q}}$-module

$$\mathbf{T}^\dagger := \mathbf{T} \otimes_{\mathcal{R}} \mathcal{R}^\dagger.$$

Corollary 3.3.5. *The residual $G_{\mathbb{Q}}$ representation $\mathbf{T}^\dagger = \mathbf{T}^\dagger/\mathfrak{m}\mathbf{T}^\dagger$ is absolutely irreducible.*

Proof. The representation $\mathbf{T}^\dagger$ is a one-dimensional twist of $\mathbf{T}$, and irreducibility is preserved by tensorization with one dimensional representations (see [Kow14, Exercise 2.2.14, (2)]). We conclude applying Theorem 3.3.3. □

Proposition 3.3.6. *The $\mathcal{R}$-module $\mathbf{T}^\dagger$ is free of rank two. As a $G_{\mathbb{Q}}$-representation, $\mathbf{T}^\dagger$ is unramified outside Np. The arithmetic Frobenius of a prime $\ell \nmid Np$ acts on $\mathbf{T}^\dagger$ with characteristic polynomial*

$$X^2 - \ ^{-1}(\mathrm{Fr}_\ell)T_\ell X + \ell;$$

where $\ $ is the critical character defined in Subsection 3.3.2.

Proof. We prove the claims for the representation $\mathrm{T}^\dagger := \mathbf{Ta}^{\mathrm{ord}}_{\mathfrak{m}_f} \otimes_{\mathbf{h}^{\mathrm{ord}}_{\mathfrak{m}_f}} R_f^\dagger$, since we rely on some results of [How07]. The proposition will easily follow from the fact that $\mathbf{T}^\dagger = \mathrm{T}^\dagger \otimes_{R_f} \mathcal{R}$.

The first claim follows then immediately from [How07, Proposition 2.1.2]. The second claim follows from [How07, Proposition 2.1.2] and the fact that the character $\ $ is unramified outside p (this is true since the p-adic cyclotomic character is unramified outside p).

In order to prove the third claim, we start from the fact that the action of Fr_ℓ on $\mathbf{Ta}^{\mathrm{ord}}_{\mathfrak{m}_f}$ has characteristic polynomial

$$X^2 - T_\ell X + [\ell]\ell;$$

as explained in [How07, Proposition 2.1.2]. When we move to $\mathrm{T}^\dagger$, the original action of $G_{\mathbb{Q}}$ becomes twisted by $\ ^{-1}$. Elementary computations show that the action of Fr_ℓ has characteristic polynomial

$$X^2 - \ ^{-1}(\mathrm{Fr}_\ell)T_\ell X + \ ^{-2}(\mathrm{Fr}_\ell)[\ell]\ell$$

on $\mathrm{T}^\dagger$. The relation of equation (3.9) yields a simplification in the characteristic polynomial, that becomes

$$X^2 - \ ^{-1}(\mathrm{Fr}_\ell)T_\ell X + \ell$$

as claimed. □

Proposition 3.3.7. *Let D_p a fixed decomposition group for p in $G_{\mathbb{Q}}$. Then there is an exact sequence of $\mathcal{R}[[D_p]]$-modules*

$$0 \longrightarrow F_p^+(\mathbf{T}^\dagger) \longrightarrow \mathbf{T}^\dagger \longrightarrow F_p^-(\mathbf{T}^\dagger) \longrightarrow 0$$

where $F_p^+(\mathbf{T}^\dagger)$ and $F_p^-(\mathbf{T}^\dagger)$ are free $\mathcal{R}$-modules of rank 1.

Proof. See [LV11, p.300] and [How07, Proposition 2.4.1]. □

3.4 Hida theory on indefinite quaternion algebras

In this section we recover the notation of the first chapter and see how one can join classical Hida theory with the theory of Galois representations coming from towers of Shimura curves attached to division quaternion algebras. We mainly follow [LV11, §6].

Recall the indefinite quaternion algebra B over $\mathbb{Q}$ of discriminant N^- and that $N := N^+N^-$ for a positive squarefree integer N^+ coprime with N^-. In this section we assume that B is a division algebra, the theory for the split case $B \cong M_2(\mathbb{Q})$ having been considered earlier.

Recall the curves $\mathcal{X}_m$ defined in Subsection 1.2.2 for every $m \geq 0$ and studied thereafter. Fix $m \geq 0$ and let $\mathrm{Div}(\mathcal{X}_m)$ and $\mathrm{Div}^0(\mathcal{X}_m)$ denote the groups of divisors and of degree zero divisors, respectively, on $\mathcal{X}_m(\mathbb{C})$.

Let $\mathrm{Princ}(\mathcal{X}_m)$ be the group of principal divisors on $\mathcal{X}_m(\mathbb{C})$ and denote, as usual, the Picard groups

$$\mathrm{Pic}(\mathcal{X}_m) := \mathrm{Div}(\mathcal{X}_m)/\mathrm{Princ}(\mathcal{X}_m) \quad \text{and} \quad \mathrm{Pic}^0(\mathcal{X}_m) := \mathrm{Div}^0(\mathcal{X}_m)/\mathrm{Princ}(\mathcal{X}_m).$$

The degree map induces the short exact sequence of abelian groups

$$0 \longrightarrow \mathrm{Pic}^0(\mathcal{X}_m) \longrightarrow \mathrm{Pic}(\mathcal{X}_m) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0. \tag{3.10}$$

3.4.1 Hecke modules

Thanks to Abel's theorem (see e.g. [DS05, Theorem 6.1.2]) the group $\mathrm{Pic}^0(\mathcal{X}_m)$ can be identified with the Jacobian variety $\mathrm{Jac}(\mathcal{X}_m)$ of $\mathcal{X}_m$, which is an abelian variety defined over $\mathbb{Q}$ of dimension equal to the genus of $\mathcal{X}_m$. More precisely, $\mathrm{Pic}(\mathcal{X}_m)$ identifies with the $\mathbb{Q}$-points of the Picard scheme of $\mathcal{X}_m$ and $\mathrm{Pic}^0(\mathcal{X}_m)$ with the identity component of this scheme.

In Section 1.4 we defined Hecke operators for every $\ell \nmid N$ and diamond operators acting on $\mathrm{Div}(\mathcal{X}_m)$. As explained for example in [Fou13, §2.1.3], it is possible to define also Hecke operators U_ℓ for all primes $\ell \mid N^+$, following the same construction of Subsection 1.4.2, but we don't recall the details since we don't need them explicitly. The $\mathcal{O}_F$-algebra generated by all these Hecke operators is called the full classical Hecke algebra and written $\mathbb{B}_m$. As in the classical case, we define Hida's ordinary projector

$$e_m^{\mathrm{ord}} := \lim_n U_p^{n!} \in \mathbb{B}_m$$

and set $\mathbb{B}_m^{\mathrm{ord}} := e_m^{\mathrm{ord}}\mathbb{B}_m$. Taking inverse limits with respect to the maps induced by the tower of curves (1.8), we set

$$\mathbb{B} := \varprojlim_m \mathbb{B}_m \quad \text{and} \quad \mathbb{B}^{\mathrm{ord}} := \varprojlim_m \mathbb{B}_m^{\mathrm{ord}}.$$

Write $\mathrm{Ta}_p(\mathrm{Jac}(\mathcal{X}_m))$ for the p-adic Tate module of $\mathrm{Jac}(\mathcal{X}_m)$ and define

$$T_m^{\mathrm{ord}} := e_m^{\mathrm{ord}}\Big(\mathrm{Ta}_p(\mathrm{Jac}(\mathcal{X}_m)) \otimes_{\mathbb{Z}_p} \mathcal{O}_F\Big);$$
$$T_\infty^{\mathrm{ord}} := \varprojlim_m e_m^{\mathrm{ord}} T_m;$$

which are left $\mathrm{B}_m^{\mathrm{ord}}[G_{\mathbb{Q}}]$ and $\mathrm{B}^{\mathrm{ord}}[G_{\mathbb{Q}}]$ modules, respectively.

3.4.2 New quotients and Jacquet-Langlands correspondence

Let $r \geq 2$, $m \geq 0$ and assume that p does not divide the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times$. We are now interested in the space $S_r^{N^-\text{-new}}(\ _m; \mathbb{Q}_p)$ of cusp forms of level $\ _m = \ _0(N) \cap \ _1(p^m)$ with coe□cients in $\mathbb{Q}_p$ that are new at N^-, as defined in Subsection 3.2.1. Write $\mathrm{T}_{r;m}$ for the image of $\mathrm{h}_r(\ _m; \mathcal{O}_F)$ in the endomorphism ring of $S_r^{N^-\text{-new}}(\ _m; \mathbb{Q}_p)$. Set also

$$\mathrm{T}_r := \varprojlim_m \mathrm{T}_{r;m}; \quad \mathrm{T}_{r;m}^{\mathrm{ord}} := e_m^{\mathrm{ord}} \mathrm{T}_{r;m} \quad \mathrm{T}_r^{\mathrm{ord}} := \varprojlim_m \mathrm{T}_{r;m}^{\mathrm{ord}};$$

where e_m^{ord} is Hida's ordinary idempotent projector. The isomorphisms of Corollary 3.1.10 yield isomorphisms of -modules

$$\mathrm{T}_r^{\mathrm{ord}} \cong \mathrm{T}_{r'}^{\mathrm{ord}}$$

for all weights $r; r' \geq 2$, so we identify the algebras $\mathrm{T}_r^{\mathrm{ord}}$ with $\mathrm{T}^{\mathrm{ord}} := \mathrm{T}_2^{\mathrm{ord}}$.

As explained in [LV11, §5.3] one can pursue Hida theory working with the algebra $\mathrm{T}^{\mathrm{ord}}$ in stead of $\mathrm{h}^{\mathrm{ord}}$, obtaining that the map $\ _f$ of (3.7) factors as

$$\ _f : \mathrm{h}^{\mathrm{ord}} \twoheadrightarrow \mathrm{T}^{\mathrm{ord}} \longrightarrow \mathcal{O}_F:$$

There is a unique maximal ideal $\mathfrak{n}_f$ of $\mathrm{T}^{\mathrm{ord}}$ through which $\ _f$ factors. The field $\mathcal{K}_f$ to which f belongs is isomorphic to the field appearing in the decomposition of $\mathrm{T}_{\mathfrak{n}_f}^{\mathrm{ord}} \otimes \ \mathcal{L}$ to which f belongs, in the same sense.

Since $\mathrm{T}_{\mathfrak{n}_f}^{\mathrm{ord}}$ is finite over $\ _F$, it is also integral over $\ _F$. This implies that the image of $\mathrm{T}_{\mathfrak{n}_f}^{\mathrm{ord}}$ in $\mathcal{K}_f$ is contained in $\mathcal{R}_f$. We denote by the symbol

$$f_\infty : \mathrm{T}_{\mathfrak{n}_f}^{\mathrm{ord}} \longrightarrow \mathcal{R}_f \tag{3.11}$$

the structure map.

There is a canonical way to define an $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$-algebra structure on $\mathrm{B}^{\mathrm{ord}}$ such that the following result holds.

Theorem 3.4.1 (Jacquet-Langlands). *There is a canonical isomorphism of $\mathcal{O}_F[[\mathbb{Z}_p^\times]]$-algebras*

$$\mathrm{JL}^{\mathrm{ord}} : \mathrm{T}^{\mathrm{ord}} \xrightarrow{\cong} \mathrm{B}^{\mathrm{ord}}$$

that sends every Hecke operator to the corresponding one.

Proof. See [LV11, Proposition 6.1]. See also [MT99, Theorem 20]. □

In light of this theorem, from now on we will identify that algebra $\mathrm{B}^{\mathrm{ord}}$ with $\mathrm{T}^{\mathrm{ord}}$, and use the latter symbol to denote both Hecke algebras.

3.4.3 Galois representations

In this subsection, as in [LV11, §6.4], we work under the following assumption, whose analogue for the Hida family $\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$ is true by [How07, Proposition 2.1.2].

Assumption 3.4.2. The $\mathcal{O}_F$-algebra $\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}$ is Gorenstein, that is

$$\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f} \cong \mathrm{Hom}_{\mathcal{O}_F}(\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}, \mathcal{O}_F)$$

as $\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}$-modules.

Define the Galois modules

$$T^{\mathrm{ord}}_{\infty;\mathfrak{n}_f} := T^{\mathrm{ord}}_{\infty} \otimes_{\mathrm{T}^{\mathrm{ord}}} \mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}, \quad \mathbf{T}_{\mathrm{Sh}} := T^{\mathrm{ord}}_{\infty;\mathfrak{n}_f} \otimes_{\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}} \mathcal{R}, \quad \mathbf{T}^{\dagger}_{\mathrm{Sh}} := \mathbf{T}_{\mathrm{Sh}} \otimes_{\mathcal{R}} \mathcal{R}^{\dagger}.$$

As in [LV11, §6.4] we need the following assumption.

Assumption 3.4.3. The residual $G_{\mathbb{Q}}$-representation $\mathbf{T}_{\mathrm{Sh}}/\mathfrak{m}_{\mathcal{R}}\mathbf{T}_{\mathrm{Sh}}$ is absolutely irreducible.

Now recall the $\mathcal{R}[G_{\mathbb{Q}}]$-module $\mathbf{T}$ defined in Subsection 3.3.3. The following result will be crucial.

Proposition 3.4.4. *There are isomorphisms of* $\mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f}[G_{\mathbb{Q}}]$*-modules* $\mathbf{T} \cong \mathbf{T}_{\mathrm{Sh}}$ *and* $\mathbf{T}^{\dagger} \cong \mathbf{T}^{\dagger}_{\mathrm{Sh}}$.

Proof. See [LV11, Corollary 6.5]. □

In light of this proposition, from now on we unify the notations and write $\mathbf{T}$ in place of $\mathbf{T}_{\mathrm{Sh}}$. Notice that, when we will study the action of the operators T_ℓ and U_p on (the cohomology of) $\mathbf{T}$, we always see them via the structure map $f_\infty : \mathrm{T}^{\mathrm{ord}}_{\mathfrak{n}_f} \longrightarrow \mathcal{R}_f$. This is because we have to work with points and cohomology classes that come from the Shimura world, and for them there is not an action of the bigger algebra $\mathrm{h}^{\mathrm{ord}}_{\mathfrak{m}_f}$. However, the entire philosophy of [LV11] makes clear that this is not a big deal, because the relations that they found (and that we sum up in the next section) are formally the same as those presented in [How07] for the classical split case.

3.5 Big Heegner points

In this section we review the contruction of big Heegner points in an indefinite quaternionic context, mainly following [LV11, §7-8]. We will stress that the construction and the properties of big Heegner points will depend only on the compatibility properties satisfied by the classes of points that will be used. This is why we work with the abstract data of a system of LV-Heegner points $P_{c;m} \in X_m$ of conductor cp^m for $m \geq 0$ and $c \geq 1$ such that $(c;N) = 1$ satisfying the properties of Proposition 2.3.1 and Lemma 2.3.2. An example of a system of points satisfying these properties is the set of points $P_{c;m}$ built in [LV11, §4] and recalled in Section 2.3.

3.5.1 Big Heegner classes

Recall that, by Proposition 2.2.7, the point $P_{c;m}$ is rational over $L_{c;m} := H_{cp^m}(\ _{p^m})$. Following [LV11, §6.2] we denote by J_m and J_m^0 the functors from the category of Q-algebras to the category of $\mathcal{O}_F$-modules which associate with any Q-algebra L the $\mathcal{O}_F$-modules

$$J_m(L) := \mathrm{Pic}(\mathcal{X}_m)(L) \otimes_{\mathbb{Z}} \mathcal{O}_F \quad \text{and} \quad J_m^0(L) := \mathrm{Jac}(\mathcal{X}_m)(L) \otimes_{\mathbb{Z}} \mathcal{O}_F;$$

respectively. Set also $J_m(L_{c;m})^{\mathrm{ord}} := e_m^{\mathrm{ord}} J_m(L_{c;m})$ and $J_m^0(L_{c;m})^{\mathrm{ord}} = e_m^{\mathrm{ord}} J_m^0(L_{c;m})$. From the short exact sequence (3.10) we obtain the Hecke equivariant exact sequence

$$0 \longrightarrow J_m^0(L_{c;m}) \longrightarrow J_m(L_{c;m}) \xrightarrow{\deg} \mathcal{O}_F \longrightarrow 0.$$

Since the action of U_p on $\mathcal{O}_F$ is via the multiplication by $p = \deg(U_p)$, the fact that $e_m^{\mathrm{ord}} = \lim_n U_p^{n!}$ yields an identification

$$J_m^0(L_{c;m})^{\mathrm{ord}} \cong J_m(L_{c;m})^{\mathrm{ord}}.$$

Viewing $P_{c;m}$ as a divisor on $\mathcal{X}_m$, we obtain an element

$$e_m^{\mathrm{ord}} P_{c;m} \in J_m^0(L_{c;m})^{\mathrm{ord}}.$$

We want to move to the component identified by the Hida family attached to f. This is why we define

$$\mathbf{J}_m^0(L_{c;m})^{\mathrm{ord}} := J_m^0(L_{c;m})^{\mathrm{ord}} \otimes_{\mathbb{T}^{\mathrm{ord}}} \mathcal{R} \quad \text{and} \quad \mathbf{J}_m^0(L_{c;m})^{\mathrm{ord},\dagger} := J_m^0(L_{c;m})^{\mathrm{ord}} \otimes_{\mathbb{T}^{\mathrm{ord}}} \mathcal{R}^\dagger.$$

Write also $P_{c;m}$ for the image of $e_m^{\mathrm{ord}} P_{c;m}$ in $\mathbf{J}_m^0(L_{c;m})^{\mathrm{ord},\dagger}$.

Lemma 3.5.1. *With the notation above, $P_{c;m} \in H^0(H_{cp^m}; \mathbf{J}_m^0(L_{c;m})^{\mathrm{ord},\dagger})$.*

Proof. As explained in [LV11, §7.1], the action of $(\ )$ coincides with the action of $\langle\ (\ )\rangle$ on $\mathbf{J}_m^0(L_{c;m})^{\mathrm{ord}}$ for every $\in G_{H_{c;m}}$. One then concludes by applying Lemma 2.3.2. □

One then defines

$$\mathcal{P}_{c;m} = \mathrm{Tr}_{H_{cp^m}/H_c}(P_{c;m}) \in H^0(H_c; \mathbf{J}_m^0(L_{c;m})^{\mathrm{ord},\dagger}).$$

Recall the reduction maps $\sim_m : \mathcal{X}_m \to \mathcal{X}_{m-1}$ of (1.8).

Lemma 3.5.2. *The equality*

$$\sim_m(\mathcal{P}_{c;m}) = U_p(\mathcal{P}_{c;m-1})$$

holds in $H^0(H_c; \mathbf{J}_{m-1}^0(L_{c;m-1})^{\mathrm{ord},\dagger})$ for all $m \geq 1$.

Proof. See [LV11, Corollary 7.2]. □

There is a twisted and Hecke-equivariant Kummer map

$$_m : H^0(H_c; \mathbf{J}_m^0(L_{c;m})^{\mathrm{ord},\dagger}) \longrightarrow H^1(H_c; \mathbf{T}_m^\dagger)$$

where $\mathbf{T}_m^\dagger := \mathrm{Ta}_{p;m}^{\mathrm{ord}} \otimes_{\mathbf{T}^{\mathrm{ord}}} \mathcal{R}^\dagger$. Set $\ _{c;m} := \ _m(\mathcal{P}_{c;m})$. The previous lemma gives the relation

$$\sim_m(\ _{c;m}) = U_p(\ _{c;m-1}):$$

Thanks to this relation and the isomorphism of $\mathbf{T}^{\mathrm{ord}}$-modules

$$\varprojlim_m H^1(H_c;\mathbf{T}_m^\dagger) \cong H^1(H_c;\mathbf{T}^\dagger);$$

we define, as in [LV11, Definition 7.4],

Definition 3.5.3. The big Heegner class of conductor c attached to the system $\{P_{c;m}\}_{m\geq 0}$ is the element

$$\ _c := \varprojlim_m U_p^{-m}(\ _{c;m}) \in H^1(H_c;\mathbf{T}^\dagger):$$

Remark 3.5.4. As noticed in [LV11, §7.4], one can be more precise and prove that the big Heegner class $\ _c$ is unramified outside Np, meaning that it lies in the kernel of the restriction map

$$H^1(H_c;\mathbf{T}^\dagger) \xrightarrow{\mathrm{res}} H^1(H_c^{(Np)};\mathbf{T}^\dagger)$$

where $H_c^{(Np)}$ is the maximal extension of H_c unramified at outside Np.

3.5.2 Euler system relations

We sum up the main compatibility properties of big Heegner points, proven in [LV11, §8]. Their proofs rely only on the fact that their points satisfy the relations of Proposition 2.3.1 and Lemma 2.3.2, therefore are still valid for our big Heegner points that are built starting from the more generic system $\{P_{c;m}\}_{c;m}$ defined at the beginning of this section.

Proposition 3.5.5. *Let $c \geq 1$ coprime with N. The relation*

$$U_p(\ _c) = \mathrm{cor}_{H_{cp}/H_c}(\ _{cp})$$

holds in $H^1(H_c;\mathbf{T}^\dagger)$.

Proof. See [LV11, Corollary 8.2]. □

Proposition 3.5.6. *Let $c \geq 1$ coprime with N and $\ell \nmid Npc$ be a prime which is inert in K. The relation*

$$T_\ell(\ _c) = \mathrm{cor}_{H_{c\ell}/H_c}(\ _{c\ell})$$

holds in $H^1(H_c;\mathbf{T}^\dagger)$.

Proof. See [LV11, Corollary 8.4]. □

Let $c \geq 1$ be an integer coprime with N and $\ell \nmid Npc$ be a prime which is inert in K. By class field theory, ℓ splits completely in the extension H_c/K. Fix a prime $\lambda \in H_c$ above ℓ. Then λ is totally ramified in $H_{c\ell}$, so $\mathcal{O}_{H_{c\ell}} = \sim^{\ell+1}$ for a prime ideal $\sim$ of the ring of integers $\mathcal{O}_{H_{c\ell}}$ of $H_{c\ell}$. Denote by $\mathrm{Fr}_\ell \in \mathrm{Gal}((H_c)_\lambda/\mathbb{Q}_\ell)$ the arithmetic Frobenius at ℓ.

Proposition 3.5.7 (Eichler-Shimura relation). *Let $\ell \nmid Npc$ be a prime inert in K. Then $\ _{c\ell}$ and $\mathrm{Fr}_\ell(\ _c)$ have the same image (via restriction) in $H^1((H_{c\ell})_\sim;\mathbf{T}^\dagger)$.*

Proof. See [LV11, Proposition 8.7]. □

Chapter 4

Kolyvagin systems

In this chapter we review the theory of Kolyvagin systems, first settled in the foundational work [MR04] and then developed by others. We will mainly follow [Büy14, §4], [Büy16] and [How04b] since our setting needs a greater generality than [MR04].

In the first section we fix some fields and define some quotients of the big representation. Then we present the general theory of Kolyvagin systems, with an eye at the examples coming from the objects we defined before. These examples will be part of the setting of the next chapters.

4.1 The anticyclotomic setting

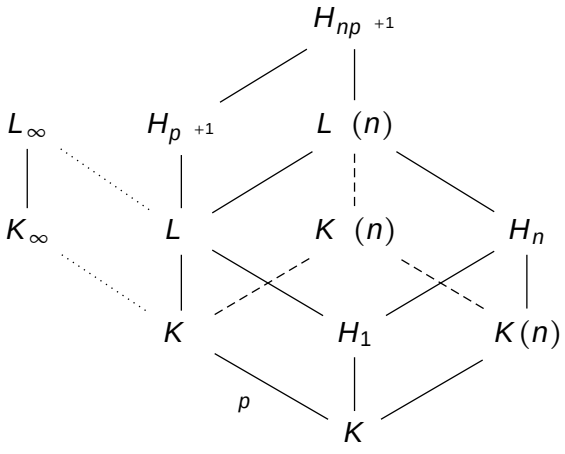
Let H_n be, as usual, the ring class field of K of conductor n. For $\in \mathbb{Z}_{>0}$ define L to be the maximal p-extension in H_{p+1}/H_1. The class number formula (see [Cox22, Theorem 7.24]) implies that $[L : H_1] = p$. By Assumption 2.2.6, the degree of the extension H_1/K is prime to p, therefore there exists a unique subextension of L/K of degree p disjoint with H_1. We call this extension K. Let

$$L_\infty := \bigcup_{\in\mathbb{Z}_{>0}} L \quad \text{and} \quad K_\infty := \bigcup_{\in\mathbb{Z}_{>0}} K :$$

We have that $\mathrm{Gal}(L_\infty/L) \cong \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

Definition. K_∞ is called the anticyclotomic $\mathbb{Z}_p$-extension of K.

For $n \in \mathbb{Z}_{>0}$ coprime with p we also set $K(n)$ to be the maximal p-extension of H_n/K, $L(n)$ to be the composite of L and H_n and $K(n)$ to be the composite of K and $K(n)$. The picture is the following:



(4.1)

Notice that the fields L and H_n are disjoint over H_1 by ramification issues. The fields K, H_1 and H_n are pairwise disjoint over K by ramification issues and from the hypothesis (see Assumption 2.2.6) that $[H_1 : K]$ is coprime with p. This implies that any prime v of K (resp. of H_1) that lies over p is totally ramified in K (resp. in L).

Definition 4.1.1. We define $\Gamma^{ac} = \mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(L_\infty/L)$, $\Lambda^{ac} = \mathbb{Z}_p[[\Gamma^{ac}]]$ and fix a profinite generator γ of Γ^{ac}.

For more properties on the anticyclotomic $\mathbb{Z}_p$-extension of K, see [Bri07]. We will use the ring Λ^{ac} to twist the big Galois representation, in order to get information about the anticyclotomic tower, and work out one divisibility of the Iwasawa main conjecture.

4.1.1 Quotients and anticyclotomic twist of the big representation

Let $r \geq 2$ and $m \geq 1$. In Definition 3.1.12 we defined elements $\ell_{r;m} \in \Lambda_F$ and $P_{r;\varepsilon} \in \Lambda_F[\varepsilon]$ for a character ε of Δ that factors through Δ/Δ^{p^m}. We can see these elements in $\mathcal{R}$ and $\mathcal{R}[\varepsilon]$ respectively via the structure morphism $\Lambda_F \to \mathcal{R}$.

Lemma 4.1.2. *The ring $\mathcal{R}/(\ell_{r;m})$ is a free $\mathcal{O}_F$-module of finite rank.*

Proof. Since $\mathcal{R}$ is finite and free over Λ_F by Theorem 3.2.5, then $\mathcal{R}/(\ell_{r;m})$ is free over $\Lambda_F/(\ell_{r;m})$, that is a free $\mathcal{O}_F$-module of finite rank because $\ell_{r;m}$ is not divisible by the uniformizer π_F of $\mathcal{O}_F$. □

Remark 4.1.3. By definition of the element $\ell_{2;m}$, the action of Δ on $\mathcal{R}/(\ell_{2;m})$ factors through $\Delta/\Delta^{p^{m-1}}$. Moreover, by Lemma 3.1.13 the element of $\ell_{2;m}$ is contained in any arithmetic prime of $\mathcal{R}$ of weight 2 and character ε that is trivial on $\Delta^{p^{m-1}}$.

Lemma 4.1.4. *Let π_F be a uniformizer of $\mathcal{O}_F$. The sequence $\{\ell_{r;m}; \pi_F^n\}$ is a regular sequence in $\mathcal{R}$ for every $r \geq 2$, $m \geq 1$ and $n \geq 1$.*

Proof. It is enough to show that the sequence $\{\ell_{r;m}; \pi_F\}$ is regular in $\mathcal{R}$. Clearly, $\{\ell_{r;m}; \pi_F\}$ is regular in Λ_F, since $\ell_{r;m}$ is not divisible by π_F. The lemma then follows from the fact that $\Lambda_F \to \mathcal{R}$ is finite and flat (see Theorem 3.2.5), therefore it preserves regular sequences. □

Definition. For each $m; s; t \in \mathbb{Z}_{>0}$, let

$$R_m := \mathcal{R}/(\ell_{2;m}); \quad R_{m;s} := \mathcal{R}/(\ell_{2;m}; p^s) \quad \text{and} \quad R_{m;s;t} := R_{m;s} \otimes_{\mathbb{Z}_p} \Lambda^{ac}/(\gamma^{p^t} - 1):$$

Define also

$$T_m := \mathbf{T}^\dagger \otimes_{\mathcal{R}} R_m; \quad T_{m;s} = \mathbf{T}^\dagger \otimes_{\mathcal{R}} R_{m;s} \quad \text{and} \quad T_{m;s;t} := \mathbf{T}^\dagger \otimes_{\mathcal{R}} R_{m;s;t}:$$

Since, by Corollary 3.1.14, $\ell_{2;m}$ divides $\ell_{2;m+1}$, we have that R_m is naturally a quotient of R_{m+1}. The modules T_m and $T_{m;s}$ are $G_{\mathbb{Q}}$-modules with respect to the action induced by the action on $\mathbf{T}^\dagger$. The module $T_{m;s;t}$ is naturally a G_K-module, where we allow G_K to act on both factors defining $T_{m;s;t}$ (on the right factor via the map $G_K \twoheadrightarrow \Gamma^{ac}$).

By the discussion in Remark 4.1.3, if p is an arithmetic prime of $\mathcal{R}$ of weight 2 and character ε that is trivial on $\Delta^{p^{m-1}}$, then the specialization map $\mathcal{R} \to \mathrm{Frac}(\mathcal{R}/\mathfrak{p})$ factors through R_m.

Lemma 4.1.5. *The rings $R_{m;s}$ and $R_{m;s;t}$ are finite for every $m;s;t \in \mathbb{Z}_{>0}$.*

Proof. It is enough to prove that $R_{m;s}$ is finite. By Lemma 4.1.4, we have that $\{\ell_{2;m}; p^s\}$ is a regular sequence in $\mathcal{R}$. It is known (see e.g. [AM69, Corollary 11.18]) that the quotient of a local Noetherian ring with a non zero divisor has dimension equal to the dimension of the ring minus one. Therefore, $R_{m;s}$ has dimension 0, hence it is an Artinian local ring. This implies that the descending chain of ideals $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots$ must stabilize, where $\mathfrak{m}$ is the maximal ideal of $R_{m;s}$. By Nakayama's lemma, this sequence stabilizes to 0. Also, all quotients of subsequent elements in the chain are finitely generated vector spaces over $R_{m;s}/\mathfrak{m} \cong \mathcal{R}/\mathfrak{m}_{\mathcal{R}}$ that is finite field, as $\mathcal{R}$ is a finite extension of . Therefore we have a finite chain

$$R_{m;s} \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^e = \{0\}$$

where all quotients of subsequent elements are finite. This implies that $R_{m;s}$ is finite. □

Since their residue fields have characteristic p, we have that the cardinality of $R_{m;s}$ and $R_{m;s;t}$ is a power of p.

Corollary 4.1.6. *The modules $T_{m;s}$ and $T_{m;s;t}$ are finite for every $m;s;t \in \mathbb{Z}_{>0}$ and they have cardinality equal to a power of p.*

While T_m and $T_{m;s}$ are quotients of $\mathbf{T}^\dagger$, the modules $T_{m;s;t}$ are quotients of $\mathbf{T}^\dagger \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$. This last object is a module over the ring $\mathcal{R} \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$, that is a local domain isomorphic to $\mathcal{R}[[\ ^{\mathrm{ac}}]]$, as noted at the beginning of [Och05, §1]. Again, we allow G_K to act also on $^{\mathrm{ac}}$ in the definition of $\mathbf{T}^\dagger \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$ and $\mathcal{R} \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$.

Definition. Call $\mathcal{R}^{\mathrm{lw}} := \mathcal{R} \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$ and set $\mathbf{T}^{\mathrm{lw}} := \mathbf{T}^\dagger \otimes_{\mathbb{Z}_p}$ $^{\mathrm{ac}}$.

Lemma 4.1.7. *The $\mathcal{R}^{\mathrm{lw}}$-module $\mathbf{T}^{\mathrm{lw}}$ is free of rank two. As a G_K-representation, it is unramified outside Np.*

Proof. Follows directly from 3.3.6 and the fact that $^{\mathrm{ac}}$ does not contain any inertia outside p. □

Call $\mathfrak{m}^{\mathrm{lw}}$ the maximal ideal of $\mathcal{R}^{\mathrm{lw}}$ and denote by $\mathbf{T}^{\mathrm{lw}}$ the residual representation $\mathbf{T}^{\mathrm{lw}}/\mathfrak{m}^{\mathrm{lw}}\mathbf{T}^{\mathrm{lw}}$.

Lemma 4.1.8. *There is an isomorphism of G_K-representations between $\mathbf{T}^\dagger$ and $\mathbf{T}^{\mathrm{lw}}$.*

Proof. By definition, there is a canonical isomorphism of $G_{\mathbb{Q}}$-modules

$$\mathbf{T}^{\mathrm{lw}}/\mathfrak{m}^{\mathrm{lw}}\mathbf{T}^{\mathrm{lw}} = \mathbf{T}^\dagger/\mathfrak{m}_{\mathcal{R}}\mathbf{T}^\dagger \otimes_{\mathbb{F}_{\mathcal{R}}} \mathbb{F}_{\mathcal{R}^{\mathrm{lw}}}$$

where $\mathbb{F}_{\mathcal{R}}$ is the residue field of $\mathcal{R}$ and $\mathbb{F}_{\mathcal{R}^{\mathrm{lw}}}$ is the residue field of $\mathcal{R}^{\mathrm{lw}}$, with Galois action induced by the action on $\mathcal{R}^{\mathrm{lw}}$. But since $[\ ]-1 \in \mathfrak{m}^{\mathrm{lw}}$, then the action of G_K is trivial on $\mathbb{F}_{\mathcal{R}^{\mathrm{lw}}}$. Moreover, the isomorphism $\mathcal{R}^{\mathrm{lw}} \cong \mathcal{R}[[\ ^{\mathrm{ac}}]] \cong \mathcal{R}[[X]]$ as $\mathcal{R}$-algebras (see [NSW13, Proposition 5.3.5]) implies that $\mathbb{F}_{\mathcal{R}^{\mathrm{lw}}} \cong \mathbb{F}_{\mathcal{R}}$ as fields. □

Remark 4.1.9. The reason of working with $\mathbf{T}^{\mathrm{lw}}$ (and with its quotients) instead of $\mathbf{T}^\dagger$ relies on the applications of Kolyvagin systems to Iwasawa theory. See Chapter 6 for more details.

The following lemma allows us to use the residual representation to deduce the absence of invariants in the actual representation.

Lemma 4.1.10. *Let $(A;\mathfrak{m}_A)$ be a local Noetherian ring and T be a finitely generated A-torsion-free module, with a continuous action of a profinite group G on it compatible with the A-module structure. If $H^0(G;T/\mathfrak{m}_A T)=\{0\}$, then $H^0(G;T)=\{0\}$.*

Proof. We need to prove that, under our hypotheses, $T^G=\{0\}$. Notice that the submodule $(T^G+\mathfrak{m}_A T)/\mathfrak{m}_A T$ is contained in $(T/\mathfrak{m}_A T)^G$, hence it is trivial. This implies that $T^G\subseteq \mathfrak{m}_A T$. Then, we can write any nonzero element $n\in T^G$ as $n=at$ with $a\in\mathfrak{m}_A\smallsetminus\{0\}$ and $t\in T$. For every $\sigma\in G$ the relation $\sigma n=n$ implies that

$$0=\sigma(at)-at=a(\sigma(t)-t).$$

Since T is A-torsion-free, we obtain that $\sigma(t)-t=0$, i.e. $t\in T^G$, hence we have that $T^G\subseteq \mathfrak{m}_A T^G$. Since T is finitely generated over a Noetherian ring, then also T^G is finitely generated over A. Applying Nakayama's lemma, we conclude that $T^G=\{0\}$. □

Corollary 4.1.11. *The $G_{\mathbb{Q}}$-representations $\mathbf{T}^\dagger$, T_m and $T_{m;s}$ have no $G_{\mathbb{Q}}$-invariants.*

Proof. We just need to check that all representations satisfy the hypotheses of Lemma 4.1.10. This is true because the rings $\mathcal{R}$, R_m, $R_{m;s}$ are Noetherian, the modules $\mathbf{T}^\dagger$, T_m, $T_{m;s}$ are free of rank 2 over the corresponding ring and the residual $G_{\mathbb{Q}}$-representation is irreducible by Corollary 3.3.5. □

We now improve the previous corollary showing that the relevant representations have no invariants over the absolute Galois group of some extensions of $\mathbb{Q}$.

Lemma 4.1.12. *Let D_K be the discriminant of K and let n be a positive integer coprime with NpD_K. The representations $\mathbf{T}^\dagger$, T_m and $T_{m;s}$ have no G_{H_n}-invariants.*

Proof. Let T be one of $\mathbf{T}^\dagger$, T_m or $T_{m;s}$, and denote by $\overline{T}$ the residual representation. Then $\overline{T}$ is free module of rank 2 over a finite field, unramified outside Np. Call $\mathbb{Q}(\overline{T})$ the finite extension of $\mathbb{Q}$ determined by the subgroup of $G_{\mathbb{Q}}$ that fixes $\overline{T}$ pointwise. We want to show that $\mathbb{Q}(\overline{T})\cap H_n=\mathbb{Q}$.

Let F be any field different from $\mathbb{Q}$ that is contained in $\mathbb{Q}(\overline{T})\cap H_n$. Since the Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself, there must be a prime ℓ that ramifies in F. Since the extension $\mathbb{Q}(\overline{T})/\mathbb{Q}$ is unramified outside Np, we must have that $\ell\mid Np$. From the fact that the extension $H_n/\mathbb{Q}$ is unramified outside nD_K, we must have that $\ell\mid nD_K$. But this is impossible, since Np is coprime with nD_K (see Assumption 2.2.6). Therefore, $\mathbb{Q}(\overline{T})\cap H_n=\mathbb{Q}$.

The action of $G_{\mathbb{Q}}$ on $\overline{T}$ factors through $\mathrm{Gal}(\mathbb{Q}(\overline{T})/\mathbb{Q})$, and it is possible to lift the elements of $\mathrm{Gal}(\mathbb{Q}(\overline{T})/\mathbb{Q})$ to elements of G_{H_n}. Since, by Corollary 3.3.5, $\overline{T}$ has no $G_{\mathbb{Q}}$-invariants we conclude that it does not have any G_{H_n}-invariant. The lemma follows applying Lemma 4.1.10. □

Corollary 4.1.13. *Let D_K be the discriminant of K and let n be a positive integer coprime with NpD_K. The representations $\mathbf{T}^{\mathrm{Iw}}$ and $T_{m;s;t}$ have no G_{H_n}-invariants.*

Proof. By Lemma 4.1.8 there is an isomorphism of G_K-representations between $\mathbf{T}^\dagger$ and $\mathbf{T}^{\mathrm{Iw}}$, therefore they are isomorphic also as G_{H_n}-representations. Then, by the proof of Lemma 4.1.12, the representation $\mathbf{T}^{\mathrm{Iw}}$ has no G_{H_n}-invariants, and we conclude applying Lemma 4.1.10. □

Finally, we study the action of the complex conjugation c on the representations $\mathbf{T}^\dagger$, T_m and $T_{m;s}$.

Lemma 4.1.14. *Let $p \geq 3$, let T be a $\mathbb{Z}_p[G_{\mathbb{Q}}]$-module and let $c \in G_{\mathbb{Q}}$ be the complex conjugation. Then $T = T_1 \oplus T_{-1}$ where $T_{\pm 1}$ is the ± 1-eigenspace for the action of c on T.*

Proof. Since c is an automorphism of T and 2 is invertible in $\mathbb{Z}_p$, we have that

$$T = 2cT \subseteq (c+1)T + (c-1)T \subseteq T:$$

The relation $c^2 = 1$ implies that if $x \in (c+1)T$ then $(c-1)x = 0$, and similarly if $y \in (c-1)T$ then $(c+1)y = 0$. Also, if $z \in (c+1)T \cap (c-1)T$ then $(c-1)z = (c+1)z = 0$, i.e. $2z = 0$. Since 2 is invertible, this yields that $z = 0$. □

Lemma 4.1.15. *The modules $\mathbf{T}^\dagger$, T_m and $T_{m;s}$ can be decomposed into the direct sum of their ± 1-eigenspaces under the action of the complex conjugation $c \in G_{\mathbb{Q}}$, each of which has rank 1.*

Proof. Lemma 4.1.14 implies that the action of c on $\mathbf{T}^\dagger$ is diagonalizable, and the same is true for T_m and $T_{m;s}$ just tensoring $\mathbf{T}^\dagger$ over $\mathcal{R}$ with R_m and $R_{m;s}$ respectively. Hence it remains to study the rank of the eigenspaces.

According to [How07, Equation (3)] there is a perfect, alternating, $G_{\mathbb{Q}}$-invariant, -bilinear pairing

$$: \mathbf{T}^\dagger \times \mathbf{T}^\dagger \longrightarrow \mathcal{R}(1):$$

Let $x;y \subseteq \mathbf{T}^\dagger$ be an $\mathcal{R}$-basis of $\mathbf{T}^\dagger$. Then

$$- \ (x;y) = c \cdot \ (x;y) = \ (cx;cy) = \det(c \mid \mathbf{T}^\dagger) \cdot \ (x;y);$$

therefore the determinant of the action of c on T is -1. This implies that the action of c on $\mathbf{T}^\dagger$ has eigenvalues 1 and -1. The same holds for T_m and $T_{m;s}$ just tensoring $\mathbf{T}^\dagger$ over $\mathcal{R}$ with R_m and $R_{m;s}$ respectively. □

4.1.2 Shapiro's lemma

Let F be a perfect field and F_∞/F be a $\mathbb{Z}_p$-extension. For any ≥ 1 call F the -th layer of the extension. Let T be a $\mathbb{Z}_p$-module together with an action of G_F. We allow G_F to act on both factors of $T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(F /F)]$ and $T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(F_\infty/F)]$ via the natural projection.

Lemma 4.1.16. *Let ≥ 1. Shapiro's lemma induces isomorphisms*

(i) $H^1\big(F; T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(F /F)]\big) \cong H^1(F ;T);$

(ii) $H^1\big(F; T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(F_\infty/F)]\big) \cong \varprojlim H^1(F ;T).$

Proof. This is essentially [Col98, Proposition II.1.1] (see also [MR04, Lemma 5.3.1]). Point (i) is a consequence of the isomorphisms

$$H^1\big(F; T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{Gal}(F /F)]\big) \cong H^1(F; \mathrm{Ind}_F^F \ T) \cong H^1(F ;T);$$

where the first is elementary (see e.g. [Mil20, Remark II.1.3] or the proof of [Col98, Proposition II.1.1]) and the second is Shapiro's lemma (see e.g. [Mil20, Proposition II.1.11]). Point (ii) descends from (i) by taking inverse limits on . □

Let now $\quad > \quad \geq 1$ and call $\quad ; : \mathrm{Z}[\mathrm{Gal}(F\ ;F)] \to \mathrm{Z}[\mathrm{Gal}(F\ ;F)]$ the map induced by the natural projection between Galois groups. As noted in the proof of [Col98, Proposition II.1.1], the following diagram

$$\begin{array}{ccc} H^1(F\ ;T) & \xrightarrow{\cong} & H^1\big(F;T\otimes_{\mathrm{Z}_p}\mathrm{Z}_p[\mathrm{Gal}(F\ /F)]\big) \\ {\scriptstyle \mathrm{cor}}\downarrow & & \downarrow{\scriptstyle \ ;} \\ H^1(F\ ;T) & \xrightarrow{\cong} & H^1\big(F;T\otimes_{\mathrm{Z}_p}\mathrm{Z}_p[\mathrm{Gal}(F\ /F)]\big) \end{array} \tag{4.2}$$

is commutative, where the two horizontal maps are the isomorphisms of Lemma 4.1.16, the left vertical map is corestriction and the right one is the map induced by $\quad ; \ .$

4.1.3 Choice of Galois groups and primes

In this subsection we define some set of primes of $\mathcal{O}_K$ that will be used when building Kolyvagin systems. For every field L and every finite G_L-representation T we denote by $L(T)$ the smallest extension of L such that $G_{L(T)}$ acts trivially on T.

Definition. Let $m;s;t \in \mathrm{Z}_{>0}$.

(a) We define $\mathcal{P}$ to be the set of all primes $\quad \subseteq \mathcal{O}_K$ inert over Q such that $\quad \nmid Np$.

(b) We define $\mathcal{P}_{m;s}$ to be the subset of $\mathcal{P}$ made by all primes $\quad = (\grave{}\,)$ such that

(i) $\grave{} \equiv -1 \pmod{p^s}$;

(ii) $\mathrm{Fr} \quad = \mathrm{Fr}_{\grave{}}^2$ acts as the identity on $T_{m;s}$.

(c) We define the sets $\mathcal{N}$ and $\mathcal{N}_{m;s}$ to be the sets of all square-free products of the rational primes that lie below the primes chosen among $\mathcal{P}$ and $\mathcal{P}_{m;s}$ respectively.

(d) For $n \in \mathcal{N}$, define $\mathcal{G}_n := \mathrm{Gal}(H_n/H_1)$.

Lemma 4.1.17. *Let* $(\grave{}\,) = \quad \in \mathcal{P}_{m;s}$. *Then* $\mathrm{Fr} \quad$ *acts trivially on* $T_{m;s;t}$.

Proof. The element $\mathrm{Fr} \quad$ acts trivially on $T_{m;s}$ by hypothesis and it acts trivially on $\quad^{\mathrm{ac}}$ since $\quad$ is split in K_∞/K by class field theory. □

Since $T_{m;s}$ and $T_{m;s;t}$ are unramified at $\grave{}$, we also have that any decomposition group at $\quad$ acts trivially on $T_{m;s}$ and $T_{m;s;t}$. We also have the following consequence of point (b).

Lemma 4.1.18. *Let* $\quad = (\grave{}\,) \in \mathcal{P}_{m;s}$. *Then the element* $T_{\grave{}}$ *is divisible by* p^s *in* R_m, *therefore it is* 0 *in* $R_{m;s}$ *and* $R_{m;s;t}$.

Proof. By condition (b), the characteristic polynomial of $\mathrm{Fr}_{\grave{}}$ on T_m divides X^2-1 modulo p^s. By Proposition 3.3.6 we know that the characteristic polynomial of $\mathrm{Fr}_{\grave{}}$ on T_m divides $X^2 - \quad^{-1}(\mathrm{Fr}_{\grave{}})T_{\grave{}}X + \grave{}$. Since $\grave{} \equiv -1 \pmod{p^s}$, comparing the two polynomials we obtain that $p^s \mid \quad^{-1}(\mathrm{Fr}_{\grave{}})T_{\grave{}}$. Since $\quad^{-1}(\mathrm{Fr}_{\grave{}})$ is a unit, we must have that $p^s \mid T_{\grave{}}$. □

Remark 4.1.19. As noted in [Bes97, Remark 3.1], Lemma 4.1.18 implies that Fr_ℓ is conjugated to the complex conjugation c in $\mathrm{Gal}(K(T_{m;s})/\mathbb{Q})$, where $K(T_{m;s})$ is the extension of K attached to the group of Galois morphisms that fix $T_{m;s}$ pointwise. This is clear after comparing the characteristic polynomial for the action of c on $T_{m;s}$ (which is X^2-1 by Lemma 4.1.15) with the characteristic polynomial of the action of the Frobenius (see Proposition 3.3.6).

For every prime $\mathfrak{q}$ of K we denote by $k_{\mathfrak{q}}$ the residue field of K at $\mathfrak{q}$.

Lemma 4.1.20. *For every $n \in \mathcal{N}$ we have that*

(a) $\mathcal{G}_n \cong \prod_{\ell \mid n} \mathcal{G}_\ell$ where ℓ varies among all prime divisors of n.

(b) For every prime $\ell \in \mathcal{N}$ the group $\mathcal{G}_\ell \cong k^\times/\mathbb{F}_\ell^\times$ is cyclic of order $\ell+1$, where $=(\ell)$.

Proof. See [Gro91, §3]. □

Definition. For every prime $\ell \in \mathcal{N}$ we fix a generator $_\ell$ for the group $\mathcal{G}_\ell$.

Since the primes $\in \mathcal{P}$ are principal, class field theory implies that they split completely in H_1 and in H_p for every ≥ 1. Moreover, every prime $_1$ of H_1 above is totally ramified in H_ℓ. This implies that is totally ramified in $K(\ell)$. For the same reason, we have that every prime above p in K (resp. in H_1) is totally ramified in K_∞ (resp. L_∞).

Lemma 4.1.21. *Let $=(\ell) \in \mathcal{P}_{m;s}$. The extension $K(\ell)/K$ is a maximal totally tamely ramified abelian p-extension of K.*

Proof. Local class field theory (see the proof of [Neu86, Theorem 7.9] and [Neu86, Corollary 7.18]) implies that every abelian totally ramified extension of K has degree that divides $\ell^{2n}(\ell^2-1)$ for some n. Then, maximal totally tamely ramified abelian extensions of K have degree ℓ^2-1. Since $\ell+1 \equiv 0 \pmod{p^s}$ and $p>2$, the p-part of ℓ^2-1 equals the p-part of $\ell+1$, that is equal to the cardinality of the p-Sylow of $k^\times/\mathbb{F}_\ell^\times \cong \mathcal{G}_\ell$. □

Lemma 4.1.22. *Let $s \geq m$ and $=(\ell) \in \mathcal{P}_{m;s}$. Then $(\mathrm{Fr}_\ell) = (-1)^{\frac{k+j}{2}-1}$ in R_m.*

Proof. Let $\varepsilon_{\mathrm{cyc}}$ benote the p-adic cyclotomic character, and recall that $\varepsilon_{\mathrm{cyc}}(\mathrm{Fr}_\ell)=\ell$. Since $\ell \equiv -1 \pmod{p^s}$, we have the decomposition

$$\begin{aligned} \mathbb{Z}_p^\times &\xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p) \\ \ell &\longmapsto (p-1;1+p^s x) \end{aligned}$$

for some $x \in \mathbb{Z}_p$. Then, by definition of , we obtain that

$$(\mathrm{Fr}_l) = (-1)^{\frac{k+j}{2}-1}[(1+p^s x)^{\frac{1}{2}}] \in \quad {}_F^\times;$$

where $(1+p^s x)^{\frac{1}{2}}$ is the unique square root of $1+p^s x$ in $1+p\mathbb{Z}_p$. Since $p>2$, the element $(1+p^s x)^{\frac{1}{2}}$ is of the form $1+p^s y$ for some $y \in \mathbb{Z}_p$. Since $s \geq m$, we have that $^{p^{s-1}}$ is trivial in R_m. Therefore $[1+p^s y] = \langle 1+p^s y \rangle = 1$ in R_m. □

Corollary 4.1.23. *Let $s \geq m$. The Frobenius Fr_ℓ of a prime ℓ that lies below a prime of $\mathcal{P}_{m;s}$ acts on T_m with characteristic polynomial*

$$X^2 - (-1)^{\frac{k+j}{2}-1} T_\ell X + \ell = 0.$$

Proof. Combine Proposition 3.3.6 with Lemma 4.1.22. □

4.2 Kolyvagin systems

4.2.1 Preliminaries

Throughout this subsection, let L be a finite extension of K and for each prime v of L define L_v^{ur} to be the maximal unramified extension of L_v. Let $I_v \subseteq D_v$ be a fixed choice of inertia and decomposition groups of v. Let R be any complete local Noetherian ring with finite residue field of characteristic p and let M be any $R[[G_L]]$-module which is finitely generated and free as an R-module and unramified outside a finite set of primes.

Definition. A Selmer structure $\mathcal{F}$ on M is a collection of local conditions on M (viewed as an $R[[D_v]]$-module) for every valuation v of L, i.e. a choice of an R-submodule $H^1_{\mathcal{F}}(L_v; M) \subseteq H^1(L_v; M)$ for every v.

Definition 4.2.1. Given an $R[[D_v]]$-submodule (resp. quotient) N of M and a local condition $\mathcal{F}$ on M we define the propagated condition, still denoted by $\mathcal{F}$, on N to be the preimage (resp. image) of $H^1_{\mathcal{F}}(L_v; M)$ under the natural map

$$H^1(L_v; N) \longrightarrow H^1(L_v; M)$$

(resp. $H^1(L_v; M) \to H^1(L_v; N)$).

Definition. Given a Selmer structure $\mathcal{F}$ on M, define the Selmer module to be

$$\mathrm{Sel}_{\mathcal{F}}(L; M) := \ker\left(H^1(L; M) \longrightarrow \prod_v H^1(L_v; M)/H^1_{\mathcal{F}}(L_v; M)\right)$$

where v runs over all places on L.

We will be concerned primarily with local conditions of the following type:

(i) The unramified condition

$$H^1_{\mathrm{ur}}(L_v; M) = \ker\left(H^1(L_v; M) \xrightarrow{\mathrm{res}} H^1(L_v^{\mathrm{ur}}; M)\right).$$

When L_v has residue characteristic different from p and M is unramified at v, we shall refer to the unramified condition on M as the finite condition $H_{\mathrm{f}}(L_v; M)$.

(ii) If L_v has residue characteristic different from p, we define the transverse condition

$$H^1_{\mathrm{tr}}(L_v; M) = \ker\left(H^1(L_v; M) \xrightarrow{\mathrm{res}} H^1(\mathcal{L}_v; M)\right);$$

where $\mathcal{L}_v$ is a maximal totally tamely ramified abelian p-extension of L_v.

Remark 4.2.2. The definition of the transverse condition is made following [Büy14, Definition 4.9] and [How07, Definition 1.1.1] rather than [MR04, §1.2]. The difference is that our field $\mathcal{L}_v$ is the maximal p-subextension of the field L'_v chosen in [MR04]. Nevertheless, notice that if M is a p-group unramified at v, then our transverse condition coincides with the one of [MR04]. This can be seen using inflation-restriction, the fact that M is unramified at v and noticing that all continous homomorphisms from $\mathrm{Gal}(L'_v/L_v)$ to a p-group must factor via $\mathrm{Gal}(\mathcal{L}_v/L_v)$.

Definition. When L_v has residue characteristic different from p and M is unramified at v, we define the singular quotient by the exactness of

$$0 \longrightarrow H_{\mathrm{f}}(L_v; M) \longrightarrow H(L_v; M) \longrightarrow H_{\mathrm{s}}(L_v; M) \longrightarrow 0;$$

4.2.2 The Greenberg Selmer structure on $\mathbf{T}^{\mathrm{Iw}}$

In this section we define a Selmer structure on the $\mathcal{R}[[G_K]]$-module $\mathbf{T}^{\mathrm{Iw}} = \mathbf{T}^{\dagger} \otimes_{\mathbb{Z}_p} {}^{\mathrm{ac}}$. This structure will then be propagated to quotients $T_{m;s;t}$. We follow and expand the ideas of [Büy14, §4.1.1].

Lemma 4.2.3. *Let v be a place of K above p, call D_v a fixed decomposition group for v. Then there is an exact sequence of $\mathcal{R}[[\mathrm{D}_v]]$-modules*

$$0 \longrightarrow F_v^+(\mathbf{T}^{\mathrm{Iw}}) \longrightarrow \mathbf{T}^{\mathrm{Iw}} \longrightarrow F_v^-(\mathbf{T}^{\mathrm{Iw}}) \longrightarrow 0$$

where $F_v^+(\mathbf{T}^{\mathrm{Iw}})$ and $F_v^-(\mathbf{T}^{\mathrm{Iw}})$ are free $\mathcal{R}^{\mathrm{Iw}}$-modules of rank 1.

Proof. The $\mathbb{Z}_p$-algebra ${}^{\mathrm{ac}} = \mathbb{Z}_p[[\ {}^{\mathrm{ac}}]]$ is flat over $\mathbb{Z}_p$, therefore the lemma follows by tensoring the exact sequence of Proposition 3.3.7. □

Remark 4.2.4. The $\mathcal{R}^{\mathrm{Iw}}$-modules $F_v^+(\mathbf{T}^{\mathrm{Iw}})$ and $F_v^-(\mathbf{T}^{\mathrm{Iw}})$ of the previous lemma coincide with $F_v^+(\mathbf{T}^{\dagger}) \otimes_{\mathbb{Z}_p} {}^{\mathrm{ac}}$ and $F_v^-(\mathbf{T}^{\dagger}) \otimes_{\mathbb{Z}_p} {}^{\mathrm{ac}}$ respectively.

Fix now a finite extension L/K.

Definition 4.2.5. The (strict) Greenberg Selmer structure $\mathcal{F}_{\mathrm{Gr}}$ on $\mathbf{T}^{\mathrm{Iw}}$ is defined by setting local conditions as

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(L_v;\mathbf{T}^{\mathrm{Iw}}) = \begin{cases} H^1_{\mathrm{ur}}(L_v;\mathbf{T}^{\mathrm{Iw}}) & \text{if } v \nmid p \\ \ker\left(H^1(L_v;\mathbf{T}^{\mathrm{Iw}}) \longrightarrow H^1(L_v;F_v^-(\mathbf{T}^{\mathrm{Iw}}))\right) & \text{if } v \mid p \end{cases}$$

with v running over all places of L, where the unnamed map is induced by the exact sequence of Lemma 4.2.3.

The Greenberg Selmer module for the representation $\mathbf{T}^{\mathrm{Iw}}$ is then

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L;\mathbf{T}^{\mathrm{Iw}}) := \ker\left(H^1(L;\mathbf{T}^{\mathrm{Iw}}) \longrightarrow \prod_v H^1(L_v;\mathbf{T}^{\mathrm{Iw}})/H^1_{\mathcal{F}_{\mathrm{Gr}}}(L_v;\mathbf{T}^{\mathrm{Iw}})\right)$$

where v runs over all places of L.

Remark 4.2.6. Following the definitions above, one can define the strict Greenberg Selmer structure and the Greenberg Selmer module also for the representation $\mathbf{T}^{\dagger}$ (as done in [Büy14, §4.1.1]), just erasing the tensorization with ${}^{\mathrm{ac}}$.

Notice that the natural surjective map $\mathbf{T}^{\mathrm{Iw}} \twoheadrightarrow T_{m;s;t}$ is $\mathcal{R}[[G_K]]$-equivariant for every $m;s;t \in \mathbb{Z}_{>0}$. We can hence propagate the structure $\mathcal{F}_{\mathrm{Gr}}$ to $T_{m;s;t}$, following Definition 4.2.1. We remark that in general

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(L_v;T_{m;s;t}) \neq \begin{cases} H^1_{\mathrm{ur}}(L_v;T_{m;s;t}) & \text{if } v \nmid p \\ \ker(H^1(L_v;T_{m;s;t}) \to H^1(L_v;F_v^-(T_{m;s;t}))) & \text{if } v \mid p \end{cases};$$

where $F_v^-(T_{m;s;t}) := F_v^-(\mathbf{T}^{\mathrm{Iw}}) \otimes_{\mathcal{R}^{\mathrm{Iw}}} R_{m;s;t}$. Anyway, we have the following partial result.

Lemma 4.2.7. *If $v \nmid Np$ is a prime of L, then*

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(L_v;T_{m;s;t}) = \ker\left(H^1(L_v;T_{m;s;t}) \to H^1(L_v^{ur};T_{m;s;t})\right) = H^1_{\mathrm{f}}(L_v;T_{m;s;t})$$

for every $m;s;t \in \mathbb{Z}_{>0}$.

Proof. This is [Rub00, Lemma 3.5, (iv)], but we give here a direct proof. The commutative diagram with exact rows

$$\begin{array}{ccccc} H^1_{\mathrm{f}}(L_v;\mathbf{T}^{\mathrm{Iw}}) & \longrightarrow & H^1(L_v;\mathbf{T}^{\mathrm{Iw}}) & \xrightarrow{\mathrm{res}} & H^1(L_v^{ur};\mathbf{T}^{\mathrm{Iw}}) \\ & & \downarrow & & \downarrow \\ H^1_{\mathrm{f}}(L_v;T_{m;s;t}) & \longrightarrow & H^1(L_v;T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(L_v^{ur};T_{m;s;t}) \end{array}$$

induces a map

$$: H^1_{\mathrm{f}}(L_v;T) \longrightarrow H^1_{\mathrm{f}}(L_v;T_{m;s;t}):$$

To conclude the proof, it su□ces to show that is surjective. By inflation-restriction, the map corresponds to the map

$$H^1(L_v^{ur}/L_v;(\mathbf{T}^{\mathrm{Iw}})^{\mathrm{I}_v}) \longrightarrow H^1(L_v^{ur}/L_v;T_{m;s;t}^{\mathrm{I}_v})$$

induced by the morphism $(\mathbf{T}^{\mathrm{Iw}})^{\mathrm{I}_v} \to T_{m;s;t}^{\mathrm{I}_v}$, where I_v is a fixed inertia at v. Since $v \nmid Np$, the inertia I_v acts trivially both on $\mathbf{T}^{\mathrm{Iw}}$ and on $T_{m;s;t}$ (see Lemma 4.1.7). The claim follows by applying the long exact sequence in cohomology to the surjective map $\mathbf{T}^{\mathrm{Iw}} \to T_{m;s;t}$, noticing that $\mathrm{Gal}(L_v^{ur}/L_v) \cong \hat{\mathbb{Z}}$ has cohomological dimension 1. □

In particular, Lemma 4.2.7 applies for every place v that lies above a prime $\in \mathcal{P}$.

4.2.3 The finite-singular isomorphism

For the following two subsections, we fix $m;s;t \in \mathbb{Z}_{>0}$. When working with the field K and with a place $\in \mathcal{P}$, we choose $K(`)_{,}$ to be the maximal totally tamely ramified abelian p-extension of K occurring in the definition of the transverse condition, where $'$ is a prime above . We can also improve Remark 4.2.2.

Lemma 4.2.8. *Let* $= (`) \in \mathcal{P}$ *and* M *be any finite* $\mathcal{R}[[G_K]]$*-module unramified at* . *Then*

$$H^1_{\mathrm{tr}}(K_{,};M) = \ker\Big(H^1(K_{,};M) \xrightarrow{\mathrm{res}} H^1((H_`)_{,};M)\Big);$$

where $_`$ *a prime of* $H_`$ *above* .

Proof. Let $'$ be the prime of $K(`)$ below $_`$. Using the functoriality of the restriction we can decompose the map that defines the right hand side as

$$H^1(K_{,};M) \xrightarrow{\mathrm{res}} H^1(K(`)_{,'};M) \xrightarrow{\mathrm{res}} H^1((H_`)_{,_`};M):$$

We just need to prove that the second restriction is injective. By inflation-restriction, its kernel is

$$H^1\Big(\mathrm{Gal}\big((H_`)_{,_`}/K(`)_{,'}\big);M^{G_{(H_`)_{,_`}}}\Big) = \mathrm{Hom}\Big(\mathrm{Gal}\big((H_`)_{,_`}/K(`)_{,'}\big);M^{G_{(H_`)_{,_`}}}\Big)$$

since $'$ is totally ramified in $(H_`)$ and $M$ is unramified at . Since $M$ is a finite $\mathcal{R}$-module it is also a finite $p$-group. Since, by definition of $K(`)$, the group $\mathrm{Gal}\big((H_`)_{,_`}/K(`)_{,'}\big)$ has cardinality coprime with p, we conclude that the object in the previous equation is $\{0\}$. □

Fix now $\in \mathcal{P}_{m;s}$ and call ℓ the prime of $\mathbb{Q}$ below . By definition of $\mathcal{P}_{m;s}$, we have that the action of G_K is unramified on $T_{m;s;t}$ and that the cardinality of the invertible elements of the residue field k of K equals ℓ^2-1, therefore it kills $T_{m;s;t}$ since $\ell+1$ is divisible by p^s. These conditions imply that our setting is compatible with the one of [MR04, §1.2]. We list here some of the key results that will lead to the definition of a Kolyvagin system for $T_{m;s;t}$.

Lemma 4.2.9. *Let $\in \mathcal{P}_{m;s}$. There are canonical functorial isomorphisms*

(i) $H^1_{\mathrm{f}}(K\ ;T_{m;s;t}) \cong T_{m;s;t}$.

(ii) $H^1_{\mathrm{s}}(K\ ;T_{m;s;t}) \otimes \mathcal{G}_\ell \cong T_{m;s;t}$.

Proof. Point (i) is [MR04, Lemma 1.2.1] combined with the fact that Fr acts trivially on $T_{m;s;t}$. Let's move to point (ii). From [MR04, Lemma 1.2.1] we have the isomorphism

$$H^1_{\mathrm{s}}(K\ ;T_{m;s;t}) \otimes k^\times \cong T_{m;s;t}.$$

Since $T_{m;s;t}$ is a finite p-group, then also $H^1_{\mathrm{s}}(K\ ;T_{m;s;t})$ is a p-torsion group. This implies that tensoring $H^1_{\mathrm{s}}(K\ ;T_{m;s;t})$ with $k^\times$ is the same as tensoring $H^1_{\mathrm{s}}(K\ ;T_{m;s;t})$ with the p-Sylow subgroup of $k^\times$. Since $p \mid (\ell+1)$ and $p>2$, the p-Sylow of $k^\times$ is isomorphic to the p-Sylow of $k^\times/\mathrm{F}^\times \cong \mathcal{G}_\ell$. □

Remark 4.2.10. As noticed in the proof of [How04b, Proposition 1.1.7] the isomorphism of point (i) of Lemma 4.2.9 is given by evaluating cocycles at the Frobenius automorphism Fr , whereas the isomorphism of point (ii) is given by sending $\otimes\ \ell$ to (σ_ℓ) for any lifting $\sigma_\ell \in \mathrm{Gal}(K\ /K^{\mathrm{ur}})$ of ℓ.

Definition 4.2.11. Let $\in \mathcal{P}_{m;s}$. We define the finite singular isomorphism

$$^{\mathrm{fs}} : H^1_{\mathrm{f}}(K\ ;T_{m;s;t}) \longrightarrow H^1_{\mathrm{s}}(K\ ;T_{m;s;t}) \otimes \mathcal{G}_\ell$$

to be the isomorphism induced by Lemma 4.2.9.

Remark 4.2.12. This definition does not coincide with [MR04, Definition 1.2.2], otherwise our finite-singular morphism would have been the zero map. Instead, our definition is compatible with [How04b, Definition 1.1.8] and [Büy14, Proposition 4.7].

Lemma 4.2.13. *Let $\in \mathcal{P}_{m;s}$. The transverse subgroup $H^1_{\mathrm{tr}}(K\ ;T_{m;s;t})$ projects isomorphically onto the singular quotient $H^1_{\mathrm{s}}(K\ ;T_{m;s;t})$ under the natural projection. In other words, there is a functorial splitting*

$$H^1(K\ ;T_{m;s;t}) = H^1_{\mathrm{f}}(K\ ;T_{m;s;t}) \oplus H^1_{\mathrm{tr}}(K\ ;T_{m;s;t}).$$

Proof. This descends from [MR04, Lemma 1.2.4] and Remark 4.2.2. □

4.2.4 Kolyvagin systems for $T_{m;s;t}$

We are going to define Kolyvagin systems for the $R_{m;s;t}$-module $T_{m;s;t}$. The first key ingredient is working with a slight modification of the strict Greenberg Selmer structure, that involves the transverse condition.

Definition. For $n \in \mathcal{N}_{m;s}$, we define the *modified (strict) Greenberg Selmer structure* on $T_{m;s;t}$ to be

$$H^1_{\mathcal{F}_{\mathrm{Gr}}(n)}(K_v; T_{m;s;t}) = \begin{cases} H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t}) & \text{if } v \nmid n \\ H^1_{\mathrm{tr}}(K_v; T_{m;s;t}) & \text{if } v \mid n \end{cases}$$

for every place v of K.

Definition. For $n \in \mathcal{N}$, define $\mathcal{G}(n) = \bigotimes_{\lambda \mid n} \mathcal{G}_\lambda$.

We recall now some basics about sheaves of graphs.

Definition. Let X be an (undirected) graph, R be a ring and Mod_R be the category of R-modules. A simplicial sheaf $\mathcal{S}$ on X with values in Mod_R is a rule assigning

- an R-module $\mathcal{S}(v)$ for every vertex v of X;
- an R-module $\mathcal{S}(e)$ for every edge e of X;
- an R-module homomorphism $\mathrm{res}^e_v : \mathcal{S}(v) \to \mathcal{S}(e)$ whenever the vertex v is an endpoint of the edge e.

Definition. Let $\mathcal{S}$ be a simplicial sheaf on a graph X. A global section of $\mathcal{S}$ is a collection

$$\{ s_v \in \mathcal{S}(v) \ : \ v \text{ is a vertex of } X \}$$

such that, for every edge $e = \{v; v'\}$ of X, we have

$$\mathrm{res}^e_v(s_v) = \mathrm{res}^e_{v'}(s_{v'})$$

in $\mathcal{S}(e)$. We write $\mathcal{S}(X)$ for the R-module of global sections of $\mathcal{S}$.

Definition. For any subset $\mathcal{P}'_{m;s}$ of $\mathcal{P}_{m;s}$, we define $\mathcal{N}'_{m;s}$ to be the set of all squarefree products of primes that lie below elements of $\mathcal{P}'_{m;s}$.

Fix now a subset $\mathcal{P}'_{m;s}$ of $\mathcal{P}_{m;s}$.

Definition. We define a graph $\mathcal{X} = \mathcal{X}(\mathcal{P}'_{m;s})$ attached to the triple $(T_{m;s;t}; \mathcal{F}_{\mathrm{Gr}}; \mathcal{P}'_{m;s})$ by taking the set of vertices of $\mathcal{X}$ to be $\mathcal{N}'_{m;s}$, and the edges to be $\{n; n\lambda\}$ whenever $n; n\lambda \in \mathcal{N}'_{m;s}$ and λ is prime.

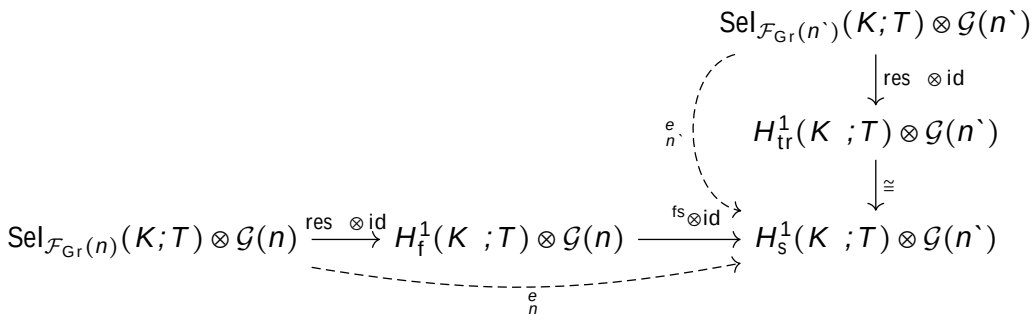
Definition. The (Greenberg) Selmer sheaf $\mathcal{H} = \mathcal{H}_{m;s;t}$ is the simplicial sheaf on $\mathcal{X}$ given as follows. We take:

- $\mathcal{H}(n) := \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K; T_{m;s;t}) \otimes \mathcal{G}(n)$ for $n \in \mathcal{N}'_{m;s}$;
- $\mathcal{H}(e) := H^1_{\mathrm{s}}(K_\mathfrak{p}; T_{m;s;t}) \otimes \mathcal{G}(n\lambda)$ if e is the edge $\{n; n\lambda\}$ and $\mathfrak{p}$ is the prime of K above λ.

We define the vertex-to-edge maps to be (see the next remark for more details)

- $\mathrm{res}^e_{n\lambda} : \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n\lambda)}(K; T_{m;s;t}) \otimes \mathcal{G}(n\lambda) \to H^1_{\mathrm{s}}(K_\mathfrak{p}; T_{m;s;t}) \otimes \mathcal{G}(n\lambda)$ is restriction at $\mathfrak{p}$ followed by the projection to the singular cohomology;
- $\mathrm{res}^e_n : \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K; T_{m;s;t}) \otimes \mathcal{G}(n) \to H^1_{\mathrm{s}}(K_\mathfrak{p}; T_{m;s;t}) \otimes \mathcal{G}(n\lambda)$ is restriction at $\mathfrak{p}$ followed by the finite-singular comparison map $\mathrm{fs}_\mathfrak{p}$.

Remark 4.2.14. Let $T := T_{m;s;t}$. The vertex-to-edge maps of the previous proposition are described by the following diagram



where for the most left arrow and for the upper arrow we are using the definition of the Greenberg Selmer group and Lemma 4.2.7, for the horizontal right arrow we are using the finite-singular isomorphism and for the bottom vertical arrow we are using the isomorphism coming from Lemma 4.2.13.

Definition. A Kolyvagin system for the triple $(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s})$ is any element of $\mathcal{H}(\mathcal{X})$, i.e. any global section for the sheaf $\mathcal{H}$. We call

$$\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s}) := \mathcal{H}(\mathcal{X})$$

the set of all Kolyvagin systems for the triple $(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s})$.

More explicitely, an element $\in \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s})$ is a collection of cohomology classes $\{\ _n\}_{n\in\mathcal{N}'_{m;s}}$ such that, for every $n;n` \in \mathcal{N}_{m;s}$ with $`$ prime, we have:

(i) $_n \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T_{m;s;t})\otimes\mathcal{G}(n)$;

(ii) $\partial^e_n(\ _n) = \partial^e_{n`}(\ _{n`})$

where e is the edge $\{n;n`\}$. Since all involved maps are $R_{m;s;t}$-linear, the set $\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s;t})$ is naturally an $R_{m;s;t}$-module.

4.2.5 Kolyvagin systems for $\mathbf{T}^{\mathrm{Iw}}$

In this subsection we show how to patch together the $R_{m;s;t}$-modules of Kolyvagin systems $\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s;t})$ when $(m;s;t)\in\mathrm{Z}^3_{>0}$ vary, in order to build what we will call a *universal Kolyvagin system* for the big representation $\mathbf{T}^{\mathrm{Iw}}$. We mainly adapt the definitions of [Büy16, §3].

Definition. For any two triples $(m;s;t)$ and $(i;j;r)$ in $\mathrm{Z}^3_{>0}$, we say that

$$(m;s;t)\preceq(i;j;r)$$

if $m\le i$, $s\le j$ and $t\le r$. A similar definition can be done for couples of positive integers.

Notice that if $(m;s)\preceq(i;j)$ then $\mathcal{P}_{m;s}\supseteq\mathcal{P}_{i;j}$. We also suppose that $\mathcal{P}'_{m;s}\supseteq\mathcal{P}'_{i;j}$. In this case we denote by $\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i;j})$ the set of global sections for the sheaf $\mathcal{H}_{m;s;t}$ restricted to the subgraph $\mathcal{X}(\mathcal{P}'_{i;j})$ of $\mathcal{X}(\mathcal{P}'_{m;s})$. For $(m;s)\preceq(i;j)\preceq(i';j')$ we also have a natural map

$$\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i;j})\longrightarrow\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i';j'}) \tag{4.3}$$

defined by restricting global sections on $\mathcal{X}(\mathcal{P}'_{i;j})$ to global sections on $\mathcal{X}(\mathcal{P}'_{i';j'})$. With respect to these maps, with $(m;s;t) \in \mathsf{Z}^3_{>0}$ fixed, one can define the direct limit

$$\varinjlim_{(i;j)} \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathsf{Gr}};\mathcal{P}'_{i;j})$$

for all $(i;j) \geq (m;s)$. Now we want to make $(m;s;t)$ vary.

Lemma 4.2.15. *Let $(m;s;t) \preceq (m';s';t')$, $n \in \mathcal{N}'_{m';s'}$ and v be a valuation of K.*

(i) If $v \mid n$, the natural projection $T_{m';s';t'} \twoheadrightarrow T_{m;s;t}$ yields a morphism

$$H^1_{\mathsf{tr}}(K_v;T_{m';s';t'}) \longrightarrow H^1_{\mathsf{tr}}(K_v;T_{m;s;t}).$$

(ii) If $v \nmid n$, the natural projection $T_{m';s';t'} \twoheadrightarrow T_{m;s;t}$ yields a surjection

$$H^1_{\mathcal{F}_{\mathsf{Gr}}}(K_v;T_{m';s';t'}) \twoheadrightarrow H^1_{\mathcal{F}_{\mathsf{Gr}}}(K_v;T_{m;s;t}).$$

Proof. Let $v \mid n$. The commutative diagram with exact rows

$$\begin{array}{ccccc} H^1_{\mathsf{tr}}(K_v;T_{m';s';t'}) & \longrightarrow & H^1(K_v;T_{m';s';t'}) & \xrightarrow{\mathrm{res}} & H^1(K(\grave{})_{v'};T_{m';s';t'}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1_{\mathsf{tr}}(K_v;T_{m;s;t}) & \longrightarrow & H^1(K_v;T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(K(\grave{})_{v'};T_{m;s;t}) \end{array}$$

induces a map

$$H^1_{\mathsf{tr}}(K_v;T_{m';s';t'}) \longrightarrow H^1_{\mathsf{tr}}(K_v;T_{m;s;t}).$$

Let $v \nmid n$. Recall that the Selmer structure $\mathcal{F}_{\mathsf{Gr}}$ on the quotients of $\mathbf{T}^{\mathrm{lw}}$ is propagated (in the sense of Definition 4.2.1) from the Selmer structure of $\mathbf{T}^{\mathrm{lw}}$. This yields the commutative diagram

$$\begin{array}{ccc} H^1_{\mathcal{F}_{\mathsf{Gr}}}(K_v;\mathbf{T}^{\mathrm{lw}}) & \twoheadrightarrow & H^1_{\mathcal{F}_{\mathsf{Gr}}}(K_v;T_{m';s';t'}) \\ & \searrow & \downarrow \\ & & H^1_{\mathcal{F}_{\mathsf{Gr}}}(K_v;T_{m;s;t}) \end{array}$$

where the vertical arrow is surjective since the diagonal arrow is so. □

When $v \nmid Np$, combining the previous lemma with Lemma 4.2.7, we obtain a surjection

$$H^1_{\mathsf{f}}(K_v;T_{m';s';t'}) \twoheadrightarrow H^1_{\mathsf{f}}(K_v;T_{m;s;t}).$$

Proposition 4.2.16. *Let $(m;s;t) \preceq (m';s';t') \preceq (i';j';r')$. Call $\pi : T_{m';s';t'} \twoheadrightarrow T_{m;s;t}$ the natural projection. Then the map*

$$\begin{aligned} \pi_* : \mathbf{KS}(T_{m';s';t'};\mathcal{F}_{\mathsf{Gr}};\mathcal{P}'_{i';j'}) &\longrightarrow \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathsf{Gr}};\mathcal{P}'_{i';j'}) \\ \{\kappa'_n\} &\longmapsto \{\pi_*(\kappa'_n)\} \end{aligned}$$

is a well-defined morphism of $\mathcal{R}^{\mathrm{lw}}$-modules.

Proof. Fix $n \in \mathcal{N}'_{i';j'}$. Let's first show that

$$*(\ {}'_n) \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T_{m;s;t}) \otimes \mathcal{G}(n):$$

Call $T' := T_{m';s';t'}$ and $T := T_{m;s;t}$. The definition of the modified Selmer group and Lemma 4.2.15 yield the following commutative diagram with exact rows

$$\begin{array}{ccccc}
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T') & \longrightarrow & H^1(K;T') & \xrightarrow{\mathrm{res}} & \prod_v H^1(K_v;T')/H^1_{\mathcal{F}_{\mathrm{Gr}}(n)}(K_v;T') \\
 & & \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle \prod_v *} \\
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T) & \longrightarrow & H^1(K;T) & \xrightarrow{\mathrm{res}} & \prod_v H^1(K_v;T)/H^1_{\mathcal{F}_{\mathrm{Gr}}(n)}(K_v;T);
\end{array}$$

where v runs over all places of K. This diagram yields the desired map

$$\begin{aligned}
{}_* : \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T') \otimes \mathcal{G}(n) &\longrightarrow \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T) \otimes \mathcal{G}(n) \\
{}'_n &\longmapsto {}_*(\ {}'_n):
\end{aligned}$$

Fix now $\ = (\ `) \in \mathcal{P}'_{i';j'}$. We need to show that $\ {}^e_n(\ {}_*(\ {}'_n)) = \ {}^e_{n`}(\ {}_*(\ {}'_{n`}))$, where $e$ is the edge $\{n;n`\}$. The strategy is to prove that $\ {}_*$ commutes with $\ {}^e_n$ and $\ {}^e_{n`}$, and then conclude just using that $\{\ {}'_n\}$ is a Kolyvagin system. In order to prove the commutativity above, we show that $\ {}_*$ commutes step by step with all maps defining $\ {}^e_n$ and $\ {}^e_{n`}$ (look at Remark 4.2.14 for a picture). Consider the diagram

$$\begin{array}{ccccc}
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T') \otimes \mathcal{G}(n) & \xrightarrow{\mathrm{res}\ \otimes \mathrm{id}} & H^1_{\mathrm{f}}(K\ ;T') \otimes \mathcal{G}(n) & \xrightarrow{\mathrm{fs}\otimes \mathrm{id}} & H^1_{\mathrm{s}}(K\ ;T') \otimes \mathcal{G}(n`) \\
\downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} \\
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T) \otimes \mathcal{G}(n) & \xrightarrow{\mathrm{res}\ \otimes \mathrm{id}} & H^1_{\mathrm{f}}(K\ ;T) \otimes \mathcal{G}(n) & \xrightarrow{\mathrm{fs}\otimes \mathrm{id}} & H^1_{\mathrm{s}}(K\ ;T) \otimes \mathcal{G}(n`):
\end{array}$$

The left square is well defined by definition of the Selmer group, by Lemma 4.2.7 and by Lemma 4.2.15, and it is commutative since the restriction map is functorial (see [NSW13, Proposition 1.5.2]). The right square is well defined and commutes since the finite-singular morphism is functorial by Lemma 4.2.9. Hence $\ {}^e_n \circ \ {}_* = \ {}_* \circ \ {}^e_n$. Consider the diagram

$$\begin{array}{ccccc}
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n`)}(K;T') \otimes \mathcal{G}(n`) & \xrightarrow{\mathrm{res}\ \otimes \mathrm{id}} & H^1_{\mathrm{tr}}(K\ ;T') \otimes \mathcal{G}(n`) & \xrightarrow{\cong} & H^1_{\mathrm{s}}(K\ ;T') \otimes \mathcal{G}(n`) \\
\downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} \\
\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n`)}(K;T) \otimes \mathcal{G}(n`) & \xrightarrow{\mathrm{res}\ \otimes \mathrm{id}} & H^1_{\mathrm{tr}}(K\ ;T) \otimes \mathcal{G}(n`) & \xrightarrow{\cong} & H^1_{\mathrm{s}}(K\ ;T) \otimes \mathcal{G}(n`):
\end{array}$$

The left square is well defined by definition of the Selmer group and by Lemma 4.2.15, and it is commutative since the restriction map is functorial. The right square is well defined and commutative since it is induced by the right square of the following diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_{\mathrm{f}}(K\ ;T') & \longrightarrow & H^1(K\ ;T') & \longrightarrow & H^1_{\mathrm{s}}(K\ ;T') & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle *} & & \\
0 & \longrightarrow & H^1_{\mathrm{f}}(K\ ;T) & \longrightarrow & H^1(K\ ;T) & \longrightarrow & H^1_{\mathrm{s}}(K\ ;T) & \longrightarrow & 0;
\end{array}$$

that is commutative since the left square is commutative by Lemma 4.2.15. This shows that $\ {}^e_{n`} \circ \ {}_* = \ {}_* \circ \ {}^e_{n`}$. As remarked above, this implies that the map $\ {}_*$

between Kolyvagin systems is well defined. The fact that it is a morphism of $\mathcal{R}^{\mathrm{lw}}$-modules descends from the fact that all maps that come into play are morphisms of $\mathcal{R}^{\mathrm{lw}}$-modules. □

Fix $(m';s';t') \geq (m;s;t)$. It is easy to see that the maps $\ _*$ of the proposition above commute with the maps defined in (4.3), hence we have a well defined morphism of $\mathcal{R}^{\mathrm{lw}}$-modules

$$\sim_* : \varinjlim_{(i';j')} \mathbf{KS}(T_{m';s';t'};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i';j'}) \longrightarrow \varinjlim_{(i;j)} \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i;j});$$

where the limits are taken for $(i';j') \geq (m';s')$ and for $(i;j) \geq (m;s)$. The set

$$\left\{ \varinjlim_{(i;j;r)} \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i;j;r}) \right\}_{(m;s;t)\in \mathbb{Z}^3_{>0}}$$

is an inverse system with respect to the maps $\ _*$. This implies that we can take the inverse limit with respect to these maps. This fact leads us to the following final definition (see also [Büy16, Definition 3.4]).

Definition 4.2.17. The $\mathcal{R}^{\mathrm{lw}}$-module

$$\overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}') := \varprojlim_{(m;s;t)} \varinjlim_{(i;j)} \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{i;j})$$

is called the module of universal Kolyvagin systems for the representation $\mathbf{T}^{\mathrm{lw}}$.

In [Büy14, Definition 4.12], it is stated that there is an equality

$$\overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}') = \varprojlim_{(m;s;t)} \mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s}):$$

We will use this fact at the end of the next chapter. It is possible that a proof of this equality follows the steps showed in [Büy16, Definition 3.6 and Lemma 5.7]. This seems possible under the assumption that the local condition $\mathcal{F}_{\mathrm{Gr}}$ is cartesian, which will be the case under some new assumptions to be made in the course of the next chapter. Indeed, one can prove (exactly as in Proposition 6.2.5) that $\mathcal{F}_{\mathrm{Gr}}$ coincides with the Bloch–Kato condition, which is cartesian by [How04a, §2.2].

Chapter 5

The big Heegner point Kolyvagin system

In this chapter we build a universal Kolyvagin system for the representation $\mathbf{T}^{\mathrm{Iw}}$, starting from the set of big Heegner classes of Definition 3.5.3.

5.1 Summary

We fixed a prime $p \geq 5$ and a positive squarefree integer N coprime with p and such that p does not divide the cardinality on $(\mathbb{Z}/N\mathbb{Z})^{\times}$. We assume that there are $N^{+}; N^{-} \in \mathbb{Z}_{>0}$ such that

$$N = N^{+}N^{-};$$

where N^{-} is a squarefree product of an even number of primes. We fixed an imaginary quadratic field K of discriminant D_K prime to $6Np$ with class number prime to p such that the primes dividing N^{+} (respectively, N^{-}) are split (respectively, inert) in K (see Assumption 2.2.6).

In Subsection 3.2.1 we fixed a normalized eigenform $f \in S_k(\ _0(N) \cap\ _1(p); !^j)$ that is an ordinary p-stabilized newform of tame level N whithout complex multiplication, for fixed $k \geq 2$ and $j \geq 0$. We are also assuming that the residual representation $\ _f$ attached to f is p-distinguished and absolutely irreducible (see Assumption 3.3.1). We called F a finite extension of $\mathbb{Q}_p$ containing the Fourier coe□cients of f and $\mathcal{O}_F$ its ring of integers.

We denoted by $\mathcal{R}$ the branch of the Hida family where f lives, $\mathbf{T}^{\dagger}$ is the twisted Galois representation attached to the Hida family and $\mathbf{T}^{\mathrm{Iw}}$ is $\mathbf{T}^{\dagger} \otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}}$. This last is a module over the complete Noetherian local domain $\mathcal{R} \otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}} \cong \mathcal{R}[[\ ^{\mathrm{ac}}]]$. The residual $G_{\mathbb{Q}}$-representation $\mathbf{T}^{\dagger}$ is absolutely irreducible (see Corollary 3.3.5).

In Subsection 4.1.1, for every triple $(m; s; t) \in \mathbb{Z}^3_{>0}$ we defined the rings R_m, $R_{m;s}$ and $R_{m;s;t}$ together with the Galois modules T_m, $T_{m;s}$ and $T_{m;s;t}$. By Lemma 4.1.12 and Corollary 4.1.13, all these modules have no H_n-invariants, for n coprime with NpD_K.

At the beginning of Section 4.1 we defined some abelian extensions H_{np} , L , $L\ (n)$, K , $K\ (n)$, $K(n)$, K_∞ and L_∞ of K, for $\in \mathbb{Z}_{>0}$ and n coprime with p (see diagram (4.1)). We have also the set $\mathcal{P}$ of primes of K that are inert and coprime with Np, together with its subset $\mathcal{P}_{m;s}$ of primes $= (`)$ of $\mathcal{P}$ such that $` \equiv -1 \pmod{p^s}$ and with the property that Fr acts trivially on $T_{m;s}$ and $T_{m;s;t}$. We called $\mathcal{N}$ and $\mathcal{N}_{m;s}$ the set of squarefree products of primes lying below primes of $\mathcal{P}$ and $\mathcal{P}_{m;s}$,

respectively. Also, for every $n \in \mathcal{N}$ there are groups $\mathcal{G}_n := \mathrm{Gal}(H_n/H_1) \cong \prod_{\ell|n} \mathcal{G}_\ell$ and $\mathcal{G}(n) := \bigotimes_{\ell|n} \mathcal{G}_\ell$. For $(\ell) \in \mathcal{P}$, the groups $\mathcal{G}_\ell$ are cyclic of order $\ell+1$, and we fixed a generator σ_ℓ.

For every $c \in \mathbb{Z}_{>0}$ coprime with N we have the big Heegner class $\kappa_c \in H^1(H_c; \mathbf{T}^\dagger)$ of conductor c defined in Definition 3.5.3. This class can be built from any system of compatible points on towers of Shimura curves (see Section 3.5). An example of a compatible family that satisfies these properties is the one built in [LV11].

5.2 Controlling Tamagawa elements

In this section, following the ideas of [Büy14, §3] and [Fou13, §5] we study the p-part of the Tamagawa numbers attached to the specializations of $\mathbf{T}^\dagger$. We also make two assumptions that will be fundamental when checking the local properties of our classes at the primes dividing N.

5.2.1 Minimally ramified modules

In this subsection we introduce the notion of minimally ramified module, as presented in [Fou13, Definition 5.6].

Definition. Let L be a finite extension of $\mathbb{Q}$, v be a place of L, S be a local Noetherian commutative domain with maximal ideal $\mathfrak{m}_S$ and T be an $S[G_L]$-module. We say that T is minimally ramified at v if the nautural map

$$T^{I_v} \longrightarrow (T/\mathfrak{m}_S T)^{I_v}$$

is a surjection, where I_v is a fixed inertia group at v.

If T is minimally ramified at v, we then have that $(T/\mathfrak{m}_S T)^{I_v}$ is isomorphic to $T^{I_v}/\mathfrak{m}_S T^{I_v}$ under the natural map.

Lemma 5.2.1. *Let T be a $S[G_L]$-module minimally ramified at v and let B be a quotient of S. Then*

(i) The module $T \otimes_S B$ is minimally ramified at v.

(ii) The map $T^{I_v} \to (T \otimes_S B)^{I_v}$ is surjective and $(T \otimes_S B)^{I_v} = T^{I_v} \otimes_S B$.

Proof. Since B is a quotient of S, the surjective morphism $T^{I_v} \twoheadrightarrow (T/\mathfrak{m}_S T)^{I_v}$ factors through the module $(T \otimes_S B)^{I_v}$. This fact yields the surjectivity of the natural morphism $(T \otimes_S B)^{I_v} \to (T/\mathfrak{m}_S T)^{I_v} \cong T^{I_v}/\mathfrak{m}_S T^{I_v}$. This last isomorphism yields also the equality $(T \otimes_S B)^{I_v} = T^{I_v} \otimes_S B$. □

Lemma 5.2.2. *Let T be a $S[G_L]$-module minimally ramified at v. Then*

(i) $H^1(I_v; T)$ is S-torsion-free.

(ii) If S is a DVR then an $S[G_L]$-module T' is minimally ramified at v if and only if $H^1(I_v; T)$ is S-torsion-free.

Proof. (i) Suppose that T is minimally ramified at v and let $x \in S \setminus \{0\}$. The multiplication-by-x map induces the long exact sequence

$$T^{I_v} \longrightarrow (T/xT)^{I_v} \longrightarrow H^1(I_v; T) \xrightarrow{\cdot x} H^1(I_v; T): \tag{5.1}$$

Thanks to point (ii) of Lemma 5.2.1, the first map is surjective and hence the multiplication by x in $H^1(\mathrm{I}_v;T)$ is injective.

(ii) When S is a DVR, we let x be a generator of its maximal ideal. Then, the exact sequence (5.1) with T' in place of T yields the needed converse implication. □

For the applications to Iwasawa theory, we would like to control minimal ramification under tensorization with respect to maps $S \to S'$ where S' is a discrete valuation ring. This seems impossible without a careful study of Tamagawa elements, as done in [Büy14, §3]. We explain this approach in the next subsection.

5.2.2 Tamagawa numbers

In this subsection we briefly recall the work of [Büy14, §3]. Notice that our assumption $p \nmid \#(\mathbb{Z}/N\mathbb{Z})^\times$ is enough to replace [Büy14, Assumption 3.1] in the arguments of [Büy14, §3].

Since we assumed N to be squarefree, [BCS23, Proposition 4.25] implies that, for every place v of K dividing N, there is an exact sequence of $\mathcal{R}[\mathrm{D}_v]$-modules

$$0 \longrightarrow \mathcal{R}(1)\otimes \quad \longrightarrow \mathbf{T}^\dagger \longrightarrow \mathcal{R}\otimes \quad \longrightarrow 0$$

where $\quad : \mathrm{D}_v \to \{\pm 1\}$ is a quadratic character. With this exact sequence in hand, the whole work of [Büy14, §3] is available, as we now recall. See also [BCS23, §4.4] for a further discussion on this subject.

Let now T be a G_K-module that is finite and free over the ring of integers S of a finite extension of $\mathbb{Q}_p$. For every place v of K dividing N, following [FP94, §4] (see in particular [FP94, Proposition 4.2.2]), we define the *p-part of the Tamagawa number at v* to be

$$\mathrm{Tam}_v^{(p)}(T) := \#H^1(\mathrm{I}_v;T)^{\mathrm{Fr}_v=1}_{\mathrm{tors}}.$$

As noticed at the end of the proof of [Büy14, Proposition 3.2] (see also [Rub00, Lemma I.3.5]), there is an equality

$$\mathrm{Tam}_v^{(p)}(T) = \#\Big((T\otimes_S(\mathrm{Frac}(S)/S))^{\mathrm{I}_v}/(T\otimes_S(\mathrm{Frac}(S)/S))^{\mathrm{I}_v}_{\mathrm{div}}\Big)^{\mathrm{Fr}_v=1},$$

where the subscript "div" means that we are taking the divisible part of the module.

Let now $\mathfrak{p}$ be an arithmetic prime of $\mathcal{R}$ and call $S(\mathfrak{p})$ the integral closure of $\mathcal{R}/\mathfrak{p}$, that is the ring of integer of a finite extension of $\mathbb{Q}_p$. Call $T(\mathfrak{p}) = \mathbf{T}^\dagger \otimes_{\mathcal{R}} S(\mathfrak{p})$ the twisted Galois representation attached to $\mathfrak{p}$ by Hida theory. For the content of the following assumption, see [Büy14, Assumption 3.4 and Remark 3.5].

Assumption 5.2.3. There is an arithmetic prime $\mathfrak{p}$ such that, for every $v \mid N$

(1) $\mathrm{Tam}_v^{(p)}(T(\mathfrak{p})) = 1$.

(2) $T(\mathfrak{p})^{\mathrm{I}_v}$ is a free $S(\mathfrak{p})$-module of rank 1.

Under Assumption 5.2.3, Büyükboduk builds a Tamagawa element $\quad \in \mathcal{R}$ that contains informations about the Tamagawa numbers at any specialization of $\mathbf{T}^\dagger$. In particular, under the same assumptions, we have the following result.

Proposition 5.2.4. *Let $\mathfrak{s} : \mathcal{R} \to S$ be any $\mathcal{O}_F$-algebra map, where S is a discrete valuation ring. Under the running assumptions, $\mathrm{Tam}_v^{(p)}(\mathbf{T}^\dagger\otimes_{\mathfrak{s}} S) = 1$ for every $v \mid N$.*

Proof. See [Büy14, Proposition 3.9]. □

The second fundamental consequence of the assumptions of this subsection is the following result.

Lemma 5.2.5. *Under the running assumptions, the module $H^1(\mathsf{I}_v;\mathbf{T}^\dagger)$ is $\mathcal{R}$-torsion-free for every $v \mid N$.*

Proof. See [Büy14, Lemma 3.11]. □

Remark 5.2.6. In this remark we investigate the relation between working under Assumption5.2.3 (as done in [Büy14]) and working under the assumption of $\mathbf{T}^\dagger$ being minimally ramified at every prime $v \mid N$ (as suggested in [Fou13, Assumption 5.10]).

First, notice that Lemma 5.2.5 is true in both contexts (see Lemma 5.2.2). Moreover, minimal ramification alone would be enough for the work of this chapter, since we will just need the surjectivity of $(\mathbf{T}^\dagger)^{\mathsf{I}_v} \to T^{\mathsf{I}_v}_{m;s}$, which follows from Lemma 5.2.1.

On the other hand, also Assumption5.2.3 gives the surjectivity of $(\mathbf{T}^\dagger)^{\mathsf{I}_v} \to T^{\mathsf{I}_v}_{m;s}$ (see [Büy14, Lemma 4.27]) and have the plus of giving Proposition 5.2.4 in its full generality, which will be used in Chapter 6. For this reason, from now on we work under Assumption 5.2.3.

5.3 Construction of the classes

Recall the big Heegner classes $_c \in H^1(H_c;\mathbf{T}^\dagger)$ of conductor c coprime with N defined in Definition 3.5.3.

Definition 5.3.1. Let $;n \in \mathsf{Z}_{>0}$ with n prime to Np. We define

$$\mathsf{z}_{n;} := \mathrm{cor}_{H_{np\ +1}/L\ (n)}\, U_p^-\ \ _{np\ +1} \in H^1(L\ (n);\mathbf{T}^\dagger);$$

where $U_p \in \mathcal{R}$ is the image of the Hecke operator U_p in $\mathcal{R}$.

Remark 5.3.2. The operator U_p is invertible in $\mathcal{R}$ since it is the image of an invertible element in the big ordinary Hecke algebra $\mathsf{T}^{\mathrm{ord}}_{\mathsf{n}_f}$ (see point (b) of Proposition 3.1.4) via the map $f_\infty : \mathsf{T}^{\mathrm{ord}}_{\mathsf{n}_f} \to \mathcal{R}$.

The aim of this section is to massage these classes in order to build a system of elements in the cohomology over K of some quotients of $\mathbf{T}^{\mathrm{Iw}}$.

5.3.1 Compatibility

Let's look at the compatibility properties of the classes $\mathsf{z}_{n;}$.

Lemma 5.3.3. *Let $n \in \mathsf{Z}_{>0}$ be prime to Np and ≥ 2. Then*

$$\mathrm{cor}_{L\ (n)/L\ _{-1}(n)}(\mathsf{z}_{n;}\ ) = \mathsf{z}_{n;\ -1};$$

Proof. From Proposition 3.5.5 we have that $\mathrm{cor}_{H_{np\ +1}/H_{np}}(U_p^{-1}\ _{np\ +1}) =\ _{np}$. The claim follows applying $\mathrm{cor}_{H_{np}\ /L\ _{-1}(n)} \circ U_p^{-\ +1}$ to both sides, remembering that the Hecke algebra is a commutative algebra defined over Q, hence it also commutes with corestriction. □

Lemma 5.3.4. *Let $n \in \mathsf{Z}_{>0}$ be prime to Np, $\grave{}$ be a prime not dividing nNp and ≥ 1. Then*

$$\mathrm{cor}_{L\ (n\grave{})/L\ (n)}(\mathsf{z}_{n\grave{};}\ ) = T_{\grave{}}(\mathsf{z}_{n;}\ );$$

Proof. From Proposition 3.5.6 we have that $\mathrm{cor}_{H_{n\ell p^{+1}}/H_{np^{+1}}}(\quad_{n\ell p^{+1}}) = T_\ell(\quad_{np^{+1}})$. The claim follows applying $\mathrm{cor}_{H_{np^{+1}}/L\ (n)} \circ U_p^-$ to both sides, remembering that the Hecke algebra is a commutative algebra defined over Q, hence it commutes also with corestriction. □

5.3.2 The classes lie in the Selmer group

Let $n \in \mathsf{Z}_{>0}$ be prime to Np and let $\quad \geq 1$. We want to work with classes that lie in the Greenberg Selmer group $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L\ (n); \mathbf{T}^\dagger)$ (see Subsection 4.2.2 for details on the Greenberg conditions). This goal is usually reached by multiplying the classes $\mathsf{z}_{n;}$ by a fixed element of $\mathcal{R}$ (see [LV11, Proposition 10.1]). In our setting, Assumption 5.2.3 allow us to get rid of this extra element.

Proposition 5.3.5. *For every $n \in \mathsf{Z}_{>0}$ and $\quad \geq 1$ we have*

$$_{np} \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(H_{np}\ ; \mathbf{T}^\dagger).$$

Proof. Following the proof of [LV11, Proposition 10.1], one shows that the restriction of $_{np}$ to $H^1((H_{np}\ )_v; \mathbf{T}^\dagger)$ lies in the Greenberg condition for every $v \nmid N^-$. For those primes v dividing N^-, one is able to show that the restriction of $_{np}$ to $H^1((H_{np}\ )_v^{\mathrm{ur}}; \mathbf{T}^\dagger)$ is $\mathcal{R}$-torsion. By class field theory, $K_{(\ell)} = (H_{np}\ )_v$ where ℓ is the rational prime below v. By Lemma 5.2.5 we know that $H^1(K_{(\ell)}^{\mathrm{ur}}; \mathbf{T}^\dagger)$ is $\mathcal{R}$-torsion-free, hence the restriction of $_{np}$ to it is zero. This implies that $_{np}$ satisfies also the Greenberg condition at v. □

Remark 5.3.6. Without Assumption 5.2.3, one can choose an element $a \in \mathcal{R}$ (independent on n and $\quad$) that lives in the annihilator of the finitely generated $\mathcal{R}$-module $\prod_{\ell \mid N^-} H^1(K_{(\ell)}^{\mathrm{ur}}; \mathbf{T}^\dagger)_{\mathrm{tors}}$ and work with the modified classes $a \cdot {}_{np}$ in place of $_{np}$, as done in [LV11, §10]. In this setting the results of this chapter remain true, modulo assuming further that $\mathbf{T}^\dagger$ is minimally ramified at every prime dividing N (see Remark 5.2.6). However, in Chapter 6 we will need Assumption 5.2.3, therefore we assume them to be true and get rid of the unwanted factor a.

Proposition 5.3.7. *Let $n \in \mathsf{Z}_{>0}$ be prime to Np and $\quad \geq 1$. Then*

$$\mathsf{z}_{n;} \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L\ (n); \mathbf{T}^\dagger).$$

Proof. We need to check that $\mathsf{z}_{n;} \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(L\ (n)_v; \mathbf{T}^\dagger)$ for every place v of $L\ (n)$. In order to ease the notation, for primes w of $H_{np^{+1}}$ and v of $L\ (n)$ we write $\mathsf{L}_w := (H_{np^{+1}})_w$ and $\mathsf{K}_v := (L\ (n))_v$.

Fix primes $w \mid v \mid \quad \nmid p$ where w (resp. v, resp. $\quad$) is a prime of $H_{np^{+1}}$ (resp. of $L\ (n)$, resp. of K). By Proposition 5.3.5 we have that

$$\mathrm{res}_w(\quad_{np^{+1}}) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathsf{L}_w; \mathbf{T}^\dagger). \tag{5.2}$$

A careful study of restriction and corestriction maps (see Corollary A.1.2) yields a commutative diagram

$$\begin{array}{ccccc} H^1(H_{np^{+1}}; \mathbf{T}^\dagger) & \xrightarrow{\oplus \mathrm{res}_w} & \oplus_{w\mid v} H^1(\mathsf{L}_w; \mathbf{T}^\dagger) & \xrightarrow{\mathrm{res}} & \oplus_{w\mid v} H^1(\mathsf{L}_w^{\mathrm{ur}}; \mathbf{T}^\dagger) \\ {\scriptstyle U_p^- \circ \mathrm{cor}}\downarrow & & \downarrow{\scriptstyle U_p^- \circ} & & \downarrow{\scriptstyle U_p^- \circ} \\ H^1(L\ (n); \mathbf{T}^\dagger) & \xrightarrow{\mathrm{res}_v} & H^1(\mathsf{K}_v; \mathbf{T}^\dagger) & \xrightarrow{\mathrm{res}} & H^1(\mathsf{K}_v^{\mathrm{ur}}; \mathbf{T}^\dagger) \end{array} \tag{5.3}$$

for some morphisms and , where w runs over all places of $H_{np^{+1}}$ over v (that is supposed to be fixed here). Then, using (5.2) and chasing the diagram above, we conclude that

$$\mathrm{res}_v(z_{n;\ }) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v;\mathbf{T}^\dagger).$$

If $w \mid v \mid \ \mid p$, using the commutative diagram

$$\begin{array}{ccc} H^1(L_w;\mathbf{T}^\dagger) & \longrightarrow & H^1(L_w;F_v^-(\mathbf{T}^\dagger)) \\ \downarrow U_p^- \circ \mathrm{cor} & & \downarrow U_p^- \circ \mathrm{cor} \\ H^1(K_v;\mathbf{T}^\dagger) & \longrightarrow & H^1(K_v;F_v^-(\mathbf{T}^\dagger)) \end{array}$$

together with Proposition 5.3.5 we conclude that

$$\mathrm{res}_v(z_{n;\ }) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v;\mathbf{T}^\dagger).$$

□

5.3.3 Kolyvagin's derivative

Our aim is building out of these classes $z_{n;\ }$ a universal Kolyvagin system for the representation $\mathbf{T}^{\mathrm{Iw}} = \mathbf{T}^\dagger \otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}}$ over the field K. The first step is, for now, fixing $m;s;t \in \mathbb{Z}_{>0}$ in order to define classes in the cohomology of $T_{m;s;t}$.

Notice that if $\geq t$, then $^p - 1 \in (\ ^{p^t} - 1)$ in $^{\mathrm{ac}}$, where is a fixed generator of $^{\mathrm{ac}}$. Therefore the augmentation ideal

$$\mathcal{A}\ = \ker\left(\mathcal{O}_F[[\mathrm{Gal}(K_\infty/K\ )]] \longrightarrow \mathcal{O}_F\right)$$

is contained in $(\ ^{p^t}-1)$. This implies that, for every $\geq t$, the action of $\mathrm{Gal}(K_\infty/K\ )$ is trivial on $R_{m;s;t}$.

Remark 5.3.8. A similar fact is also used [Büy14, (4.2)], but here the result is easier since we are using the elements $^{p^t} - 1$ instead of $(\ -1)^t$. One can also easily prove (see [Was97, p.116]) that $^{p^t} - 1 \in (p;\ -1)^{t+1}$ and that $p \nmid\ ^{p^t} - 1$. This implies that the sequence $p^s;\ ^{p^t} - 1$ is regular in $^{\mathrm{ac}}$.

Let now $n \in \mathcal{N}_{m;s}$. Recall that $\mathcal{G}_n = \mathrm{Gal}(H_n/H_1)$ is isomorphic to the product $\prod_{\grave{}\mid n}\mathcal{G}_{\grave{}}$ of cyclic groups of order $\grave{}+1$ generated by $_{\grave{}}$, for every prime divisor $\grave{}$ of n. Ramification issues imply also that

$$\mathcal{G}_n = \mathrm{Gal}(H_n/H_1) \cong \mathrm{Gal}(L\ (n)/L\ ) \cong \mathrm{Gal}(K\ (n)/K\ )$$

for every ≥ 1.

Definition. Define the derivative operators $D_{\grave{}} = \sum_{i=1}^{\grave{}} i\ ^i \in \mathbb{Z}[\mathcal{G}_{\grave{}}]$ for a prime $\grave{} \mid n$ and $D_n = \prod_{\grave{}\mid n} D_{\grave{}} \in \mathbb{Z}[\mathcal{G}_n]$.

Notice that the action of D_n on any $\mathcal{G}_n$-module is a product of the action of elements that lie in inertia groups above the primes that divide n. Since $\mathbf{T}^\dagger$ and $\mathbf{T}^{\mathrm{Iw}}$ are unramified outside Np (see Proposition 3.3.6 and Lemma 4.1.7), we can lift D_n to an element of $\mathbb{Z}[G_{\mathbb{Q}}]$ that acts trivially on $\mathbf{T}^\dagger$ and $\mathbf{T}^{\mathrm{Iw}}$.

Since $\mathcal{G}_n$ is a normal subgroup of $\mathrm{Gal}(H_n/\mathbb{Q}) \cong \mathrm{Gal}(H_n/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$, the complex conjugation $c \in \mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathcal{G}_n$ with the relation $c\ c = \ ^{-1}$, for all $\in \mathcal{G}_n$.

Lemma 5.3.9. *For* $= (\ell) \in \mathcal{P}_{m;s}$ *and* $n \in \mathcal{N}_{m;s}$ *we have the relations*

(a) $(\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_{\mathcal{G}_\ell}$ *:*

(b) $cD_n \equiv (-1)^{!(n)} D_n c \pmod{p^s}$ *in* $\mathbb{Z}[\mathrm{Gal}(H_\ell/\mathbb{Q})]$*, where* $!(n)$ *is the number of prime factors of* n*.*

Proof. Point (a) is a classical straightforword computation (see [Gro91, Equation (3.5)]). Turning to point (b), let ℓ be a prime factor of n. Using the fact that $p^s \mid \ell + 1$, we obtain that

$$\begin{aligned} cD_\ell &= \sum_{i=1}^{\ell} ic^{\,i} = \sum_{i=1}^{\ell} i\,\sigma_\ell^{-i} c = \sum_{i=1}^{\ell} i\,\sigma_\ell^{\ell+1-i} c = \sum_{i=1}^{\ell} (\ell + 1 - i)\,\sigma_\ell^{\,i} c = (\ell+1)\sum_{i=1}^{\ell} \sigma_\ell^{\,i} c - \sum_{i=1}^{\ell} i\,\sigma_\ell^{\,i} c \\ &= -D_\ell c + p^s(\text{something}) \end{aligned}$$

in $\mathbb{Z}[\mathrm{Gal}(H_\ell/\mathbb{Q})]$. Then, for every $\ell \mid n$, we can compute

$$cD_n = cD_\ell D_{n/\ell} = -D_\ell c D_{n/\ell} + p^s(\text{something});$$

and point (b) follows by induction on the number of prime factors of n. □

We now fix $m; s; t;$ $\in \mathbb{Z}_{>0}$ and $n \in \mathcal{N}_{m;s}$ and massage the elements $z_{n;}$ using cohomology operators in order to build classes in $H^1(K; T_{m;s;t})$.

Definition. For any element $z \in H^1(L\ (n); \mathbb{T}^\dagger)$ we write $\bar{z}$ for the image of z in $H^1(L\ (n); T_{m;s})$.

Proposition 5.3.10. *For every* $n \in \mathcal{N}_{m;s}$*, we have* $\overline{D_n z_{n;}} \in H^1(L\ (n); T_{m;s})^{\mathcal{G}_n}$.

Proof. By the functoriality of the Galois action on cohomology groups (see [NSW13, Proposition 1.5.2]), we have that

$$\overline{D_n z_{n;}} = D_n \bar{z}_{n;} :$$

Since $\mathcal{G}_n = \prod_{\ell \mid n} \mathcal{G}_\ell$, it suffices to prove that

$$(\ell - 1) D_n \bar{z}_{n;} = 0$$

in $H^1(L\ (n); T_{m;s})$ for every prime $\ell \mid n$. Using Lemma 5.3.9 and the fact that $\mathcal{G}_n$ is abelian, we obtain that

$$\begin{aligned} (\ell - 1) D_n \bar{z}_{n;} &= (\ell - 1) D_\ell D_{n/\ell} \bar{z}_{n;} = (\ell + 1 - \mathrm{Tr}_{\mathcal{G}_\ell}) D_{n/\ell} \bar{z}_{n;} = \\ &= (\ell + 1) D_{n/\ell} \bar{z}_{n;} - D_{n/\ell} \mathrm{Tr}_{\mathcal{G}_\ell}(\bar{z}_{n;}) : \end{aligned}$$

Since ℓ lies below a prime in $\mathcal{P}_{m;s}$ we have that $p^s \mid \ell + 1$, hence $\ell + 1$ is zero in $R_{m;s}$. It suffices now to prove that $\mathrm{Tr}_{\mathcal{G}_\ell}(\bar{z}_{n;}) = 0$.

By [NSW13, Corollary 1.5.7] there is a commutative diagram

$$\begin{array}{ccc} H^1(L\ (n); T_{m;s}) & \xrightarrow{\mathrm{Tr}_{\mathcal{G}_l}} & H^1(L\ (n); T_{m;s}) \\ \downarrow{\scriptstyle \mathrm{cor}} & \nearrow{\scriptstyle \mathrm{res}} & \\ H^1(L\ (n/\ell); T_{m;s}) & & \end{array}$$

Using the functoriality of the corestriction together with Lemma 5.3.4 we obtain that

$$\mathrm{cor}_{L\ (n)/L\ (n/\ell)}(\bar{z}_{n;}) = T_\ell(z_{n/\ell;}) ;$$

and the lemma follows from the fact that T_ℓ is zero on $T_{m;s}$ by Lemma 4.1.18.

□

The end of the proof of the previous proposition yields the following corollary, that has some importance on its own.

Corollary 5.3.11. *With the notation of the proof of the previous proposition, we have that*

$$\mathrm{cor}_{L\ (n)/L\ (n/\ell)}(\bar{z}_{n;\ }) = 0$$

in $H^1(L\ (n/\ell); T_{m;s})$.

Lemma 5.3.12. *The restriction map*

$$\mathrm{res} : H^1(L\ ; T_{m;s}) \longrightarrow H^1(L\ (n); T_{m;s})^{\mathcal{G}_n}$$

is an isomorphism.

Proof. We will prove that $H^0(L\ (n); T_{m;s}) = \{0\}$ and then conclude via the inflation-restriction exact sequence.

By Lemma 4.1.12, we have that $H^0(H_n; T_{m;s}) = \{0\}$. We can write

$$\{0\} = H^0(H_n; T_{m;s}) = H^0\big(L\ (n)/H_n; H^0(L\ (n); T_{m;s})\big);$$

and notice that the group $\mathrm{Gal}(L\ (n)/H_n)$ has order $p\ $. Suppose by contradiction that $H^0(L\ (n); T_{m;s}) \neq \{0\}$. Then, since $T_{m;s}$ is a finite abelian p-group, the cardinality of $H^0(L\ (n); T_{m;s})$ is equal to p^c for some $c \geq 1$. By [Ser77, Lemma 3], we have that p divides the cardinality of $H^0(L\ (n)/H_n; H^0(L\ (n); T_{m;s}))$. But since the element 0 is always stabilized, the cardinality of $H^0(L\ (n)/H_n; H^0(L\ (n); T_{m;s}))$ is greater then 0, hence greater or equal then p. This is absurd since we know that $H^0(H_n; T_{m;s}) = \{0\}$. □

Definition. For $n \in \mathcal{N}_{m;s}$ and $\ \geq t$, define $\ _{[n;\ ]} := \mathrm{res}^{-1}\, \overline{D_n z_{n;\ }} \in H^1(L\ ; T_{m;s})$.

Point (i) of Lemma 4.1.16 yields an isomorphism

$$\mathrm{Sh}\ \ : H^1(L\ ; T_{m;s}) \xrightarrow{\cong} H^1\big(H_1; T_{m;s} \otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}}/(\ ^{p}\ - 1)\big) = H^1(H_1; T_{m;s;\ }) \qquad (5.4)$$

Whenever $\ \geq t$, the fact that $\ ^{p^t} - 1 \mid \ ^{p}\ - 1$ implies that there is a natural map

$$_{;t} : H^1\big(H_1; T_{m;s;\ }\big) \longrightarrow H^1\big(H_1; T_{m;s;t}\big):$$

Definition. For every $n \in \mathcal{N}_{m;s}$ define $\ _{[n]} := \mathrm{Sh}_t(\ _{[n;t]}) \in H^1(H_1; T_{m;s;t})$.

The following lemma explains the compatibility in the anticyclotomic tower satisfied by the classes $\ _{[n]}$.

Lemma 5.3.13. *For every* $\ \geq t$, *there is an equality*

$$_{[n]} = (\ \ _{;t} \circ \mathrm{Sh}\ )(\ _{[n;\ ]}):$$

Proof. Lemma 5.3.3 yields the relation

$$\mathrm{cor}_{L\ (n)/L_t(n)}(z_{n;\ }) = z_{n;t}:$$

Corestriction commutes with the action of D_n (see [NSW13, Proposition 1.5.4]), with reduction to $T_{m;s}$ and, since $L\ $ and $L_t(n)$ are disjoint over L_t, also with the inverse

of the restriction defining $[n;\ ]$ and $[n;t]$ (see [NSW13, Corollary 1.5.8]). Therefore, we obtain that

$$\mathrm{cor}_{L\ /L_t}(\ [n;\ ]) = \ [n;t]:$$

As noted in (4.2), there is a commutative diagram

$$\begin{array}{ccc} H^1(L\ ;T_{m;s}) & \xrightarrow{\mathrm{Sh}} & H^1(H_1;T_{m;s}\otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}}/(\ ^{p}\ -1)) \\ {\scriptstyle \mathrm{cor}}\downarrow & & \downarrow{\scriptstyle ;t} \\ H^1(L_t;T_{m;s}) & \xrightarrow{\mathrm{Sh}} & H^1(H_1;T_{m;s}\otimes_{\mathbb{Z}_p}\ ^{\mathrm{ac}}/(\ ^{p^t}-1)) \end{array}$$

where $_{;t}$ is the map attached to the projection $^{\mathrm{ac}}/(\ ^{p}\ -1) \twoheadrightarrow\ ^{\mathrm{ac}}/(\ ^{p}\ -1)$. This implies that the image of Sh $(\ [n;\ ])$ in $H^1(H_1;T_{m;s;t})$ coincides with Sh$(\ [n;t])$. □

Definition. For $n \in \mathcal{N}_{m;s}$ we define

$$_n := \mathrm{cor}_{H_1/K}\ \ [n] \in H^1(K;T_{m;s;t}):$$

The main goal of the rest of this chapter will be to prove that a slight modification of the classes $\{\ _n\}_{n\in\mathcal{N}_{m;s}}$ form a Kolyvagin system for $T_{m;s;t}$ over K with respect to the Greenberg condition. The first step in this direction will be proving that they lie in the proper Selmer group.

5.4 Local properties of the classes

The aim of this section is to show that the classes $_n$ lie in $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T_{m;s;t})$, by checking all local conditions at the primes of K. In order to do this, we keep working with fixed $m;s;t \in \mathbb{Z}_{>0}$ and $n \in \mathcal{N}_{m;s}$.

Remark 5.4.1. Let ≥ 1, v be a prime of L and w be a fixed place of $L\ (n)$ above v. Since $D_n \in \mathbb{Z}[\mathcal{G}_n]$, its action is well defined on $H^1(L\ (n);T_{m;s})$ but it is not defined on a single local component $H^1(L\ (n)_w\ ;T_{m;s})$, since the action of an element of $\mathcal{G}_n$ may twist local components. This is why we will extensively make use of the following semilocal commutative diagram

$$\begin{array}{ccc} H^1(L\ (n);T_{m;s}) & \xrightarrow{\oplus\,\mathrm{res}_w} & \oplus_{w|v}\ H^1(L\ (n)_w;T_{m;s}) \\ \downarrow{\scriptstyle D_n} & & \downarrow{\scriptstyle D_n} \\ H^1(L\ (n);T_{m;s}) & \xrightarrow[\oplus\,\mathrm{res}_w]{} & \oplus_{w|v}\ H^1(L\ (n)_w;T_{m;s}); \end{array}$$

where w runs over all places of $L\ (n)$ over v. See also Section A.1 and [Rub00, §B.5] for a discussion on semilocal Galois cohomology.

5.4.1 Local properties away from Np

Proposition 5.4.2. *Fix a place $v \nmid Nnp$ of K and let v be a place of L over v. Then, for all ≥ 1 we have*

(a) $\mathrm{res}_v(\ [n;\ ]) \in H^1_{\mathrm{f}}((L\ )_v\ ;T_{m;s}) = H^1_{\mathcal{F}_{\mathrm{Gr}}}((L\ )_v\ ;T_{m;s})$.

(b) $\mathrm{res}_v(\ _n) \in H^1_{\mathrm{f}}(K_v;T_{m;s;t}) = H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v;T_{m;s;t})$.

Proof. Before starting the actual proof, notice that the equality signs in (a) and (b) between local conditions come from Lemma 4.2.7.

(a) Let w be a place of $L\ (n)$ above v . Since the extensions $L\ (n)_w/(L\ )_v\ /K_v$ are unramified, then $L\ (n)_w^{ur} = (L\ )_v^{ur} = K_v^{ur}$. Thanks to the functoriality of the restriction (see [NSW13, Proposition 1.5.2] and [NSW13, Proposition 1.5.4]) and to the commutative diagram of Remark 5.4.1 we obtain the commutative diagram

$$\begin{array}{ccccc}
H^1(L\ (n);\mathbf{T}^\dagger) & \xrightarrow{\oplus\,\mathrm{res}_w} & \oplus_{w|v}\ H^1(L\ (n)_w;\mathbf{T}^\dagger) & \xrightarrow{\mathrm{res}} & \oplus_{w|v}\ H^1(L\ (n)_w^{\mathrm{ur}};\mathbf{T}^\dagger) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(L\ (n);T_{m;s}) & \xrightarrow{\oplus\,\mathrm{res}_w} & \oplus_{w|v}\ H^1(L\ (n)_w;T_{m;s}) & \xrightarrow{\mathrm{res}} & \oplus_{w|v}\ H^1(L\ (n)_w^{\mathrm{ur}};T_{m;s}) \\
{\scriptstyle D_n}\downarrow & & {\scriptstyle D_n}\downarrow & & {\scriptstyle D_n}\downarrow \\
H^1(L\ (n);T_{m;s}) & \xrightarrow[\oplus\,\mathrm{res}_w]{} & \oplus_{w|v}\ H^1(L\ (n)_w;T_{m;s}) & \xrightarrow[\mathrm{res}]{} & \oplus_{w|v}\ H^1(L\ (n)_w^{\mathrm{ur}};T_{m;s}).
\end{array}$$

Following the path of $z_{n;\ }$ from the upper left to the bottom right of the previous diagram and applying Proposition 5.3.7 we obtain that

$$\mathrm{res}_w(\overline{D_n z_{n;\ }}) \in H^1_{\mathrm{f}}(L\ (n)_w;T_{m;s})$$

for every $w \mid v$. Point (a) descends from the following commutative diagram

$$\begin{array}{ccccc}
H^1(L\ (n);T_{m;s}) & \xrightarrow{\mathrm{res}_w} & H^1(L\ (n)_w;T_{m;s}) & \xrightarrow{\mathrm{res}} & H^1(L\ (n)_w^{\mathrm{ur}};T_{m;s}) \\
{\scriptstyle \mathrm{res}}\uparrow & & {\scriptstyle \mathrm{res}}\uparrow & & \| \\
H^1(L\ ;T_{m;s}) & \xrightarrow[\mathrm{res}_v]{} & H^1((L\ )_v\ ;T_{m;s}) & \xrightarrow[\mathrm{res}]{} & H^1((L\ )_v^{\mathrm{ur}};T_{m;s}).
\end{array}$$

(b) Let now v_1 be a place of H_1 above v and take $\quad = t$. Semilocal Shapiro's lemma (see e.g. [Rub00, Proposition B.4.2]) yields the following commutative diagram

$$\begin{array}{ccccc}
H^1(L_t;T_{m;s}) & \xrightarrow{\oplus\,\mathrm{res}_{v_t}} & \oplus_{v_t|v_1} H^1((L_t)_{v_t};T_{m;s}) & \xrightarrow{\oplus\,\mathrm{res}} & \oplus_{v_t|v_1} H^1((L_t)_{v_t}^{\mathrm{ur}};T_{m;s}) \\
{\scriptstyle \mathrm{Sh}_t}\downarrow & & {\scriptstyle \mathrm{Sh}_t}\downarrow & & {\scriptstyle \mathrm{Sh}_t}\downarrow \\
H^1(H_1;T_{m;s;t}) & \xrightarrow{\mathrm{res}_{v_1}} & H^1((H_1)_{v_1};T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1((H_1)_{v_1}^{\mathrm{ur}};T_{m;s;t}).
\end{array}$$

Following the path of $_{[n;t]}$ from the upper left to the bottom right and applying point (a), we obtain that

$$\mathrm{res}_{v_1}(\ _{[n]}) \in H^1_{\mathrm{f}}((H_1)_{v_1};T_{m;s;t}).$$

Corollary A.1.2 yields a commutative diagram

$$\begin{array}{ccccc}
H^1(H_1;T_{m;s;t}) & \xrightarrow{\oplus\,\mathrm{res}_{v_1}} & \oplus_{v_1|v} H^1((H_1)_{v_1};T_{m;s;t}) & \xrightarrow{\oplus\,\mathrm{res}} & \oplus_{v_1|v} H^1((H_1)_{v_1}^{\mathrm{ur}};T_{m;s;t}) \\
\downarrow{\scriptstyle \mathrm{cor}} & & \downarrow & & \downarrow \\
H^1(K;T_{m;s;t}) & \xrightarrow{\mathrm{res}_v} & H^1(K_v;T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(K_v^{\mathrm{ur}};T_{m;s;t})
\end{array}$$

that gives point (b). □

Proposition 5.4.3. *Let* $\quad = (\ell)$ *be a prime of* K *such that* $\ell \mid n$. *Then*

$$\mathrm{res}\quad _n \in H^1_{\mathrm{tr}}(K\ ;T_{m;s;t}).$$

Proof. Fix ≥ 1 and let v (resp. w, resp. w') be a place of L (resp. L (`), resp. L (n)) that lies above (resp. above v, resp. above w). By Lemma 4.2.8, we must prove that res $_n$ lies in the kernel of

$$\mathrm{res} : H^1(K\ ; T_{m;s;t}) \longrightarrow H^1((H^{`})_{v^{`}}; T_{m;s;t});$$

where $v^{`}$ is the prime below w.

First step: prove that the restriction of $D_n z_{n;}$ to $H^1((L\ (n))_{w'}; T_{m;s})$ is trivial, where $z_{n;}$ is the reduction of $z_{n;}$ to $H^1(L\ (n); T_{m;s})$.

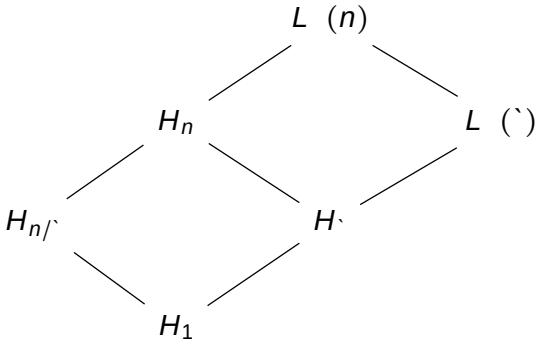
First, by Proposition 5.3.7 and Lemma 4.2.7 we know that $\mathrm{res}_{w'} z_{n;}$ lies in $H^1_{\mathrm{f}}((L\ (n))_{w'}; T_{m;s})$. Since the operator D_n commutes with restriction (in the sense of Remark 5.4.1), the same is true for $\mathrm{res}_{w'} D_n z_{n;}$.

By the explicit description of the isomorphism of point (i) of Lemma 4.2.9 (see Remark 4.2.10) and the fact that $D_n = \prod_{`'|n} D_{`'}$, it su□ces to show that the evaluation $(D_{`} z_{n;})(\mathrm{Fr}_{w'})$ of a cocycle representing $D_{`} z_{n;}$ at $\mathrm{Fr}_{w'}$ is trivial. Since $T_{m;s}$ is unramified outside Np, we know that $_{`}$ (our fixed generator for $\mathcal{G}_{`}$) can be lifted to an element that acts trivially on $T_{m;s}$. This, together with the fact that the cocycle $\mathrm{res}_{w'} z_{n;}$ is inflated by an unramified cocycle, implies that the action of $_{`}$ on $\mathrm{res}_{w'} z_{n;}$ is trivial, therefore

$$(D_{`} z_{n;})(\mathrm{Fr}_{w'}) = \sum_{i=1}^{`} i \cdot (\ ^{i} z_{n;})(\mathrm{Fr}_{w'}) = \sum_{i=1}^{`} i \cdot z_{n;}\ (\mathrm{Fr}_{w'}) = \frac{`(`+1)}{2} \cdot z_{n;}\ (\mathrm{Fr}_{w'}) = 0$$

since $(`+1)/2$ is zero on $T_{m;s}$.

Second step: prove that the restriction of $_{[n;\ ]}$ to $H^1(L\ (`)_w; T_{m;s})$ is trivial. Recall that there are disjoint field extensions



Since $= (`)$ is a principal prime in $K$, by class field theory we have that splits completely in $H_{n/`}$. Elementary algebraic number theory shows that this implies that w splits completely in $L\ (n)$. This implies that $L\ (`)_w = L\ (n)_{w'}$.

Our claim now follows easily from the first step of this proof together with the commutativity of the following diagram

$$\begin{array}{ccccc} H^1(L\ (n); T_{m;s}) & & \xrightarrow{\quad\mathrm{res}_{w'}\quad} & & H^1(L\ (n)_{w'}; T_{m;s}) \\ \uparrow{\scriptstyle \mathrm{res}} & & & & \| \\ H^1(L\ ; T_{m;s}) & \xrightarrow{\mathrm{res}_v} & H^1((L\ )_v\ ; T_{m;s}) & \xrightarrow{\mathrm{res}} & H^1(L\ (`)_w; T_{m;s}): \end{array}$$

Third step: we conclude as in the proof of point (b) of Proposition 5.4.2. Precisely,

setting $\quad = t$, we have the commutative diagram

$$\begin{array}{ccccc}
H^1(L_t;T_{m;s}) & \xrightarrow{\oplus \mathrm{res}_{v_t}} & \oplus_{v_t|\quad} H^1((L_t)_{v_t};T_{m;s}) & \xrightarrow{\oplus \mathrm{res}} & \oplus_{w|\quad} H^1((L_t(\grave{}))_w;T_{m;s}) \\
\downarrow{\scriptstyle \mathrm{Sh}_t} & & \downarrow{\scriptstyle \mathrm{Sh}_t} & & \downarrow{\scriptstyle \mathrm{Sh}_t} \\
H^1(H_1;T_{m;s;t}) & \xrightarrow{\oplus \mathrm{res}_{v_1}} & \oplus_{v_1|\quad} H^1((H_1)_{v_1};T_{m;s;t}) & \xrightarrow{\oplus \mathrm{res}} & \oplus_{v\grave{}|\quad} H^1((H\grave{})_{v\grave{}};T_{m;s;t}) \\
\downarrow{\scriptstyle \mathrm{cor}} & & \downarrow & & \downarrow \\
H^1(K;T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(K\ \ ;T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1((H\grave{})_{v\grave{}};T_{m;s;t});
\end{array}$$

where the two upper squares are induced by semilocal Shapiro's lemma and the two bottom squares are a consequence of [NSW13, Proposition 1.5.6] (see also Corollary A.1.2). In particular, since $\quad$ is split in H_1, the bottom vertical central and right maps are just a sum of Galois actions, and in the bottom right cohomology group the field $(H\grave{})_{v\grave{}}$ is intended to correspond to the intersection between the chosen decomposition group at $\quad$ with $G_{H\grave{}}$. □

5.4.2 Local properties at p

For this subsection, we fix a place v of K above p. Since $F_v^-(\mathbf{T}^\dagger)$ is flat over $\mathcal{R}$, by tensoring the exact sequence of Proposition 3.3.7 over $\mathcal{R}$ with $R_{m;s}$, we obtain the exact sequence of $R_{m;s}[[G_{K_v}]]$-modules

$$0 \longrightarrow F_v^+(T_{m;s}) \longrightarrow T_{m;s} \longrightarrow F_v^-(T_{m;s}) \longrightarrow 0$$

where, by definition, $F_v^\pm(T_{m;s}) := F_v^\pm(\mathbf{T}^\dagger)\otimes_{\mathcal{R}}\mathcal{R}_{m;s}$. For a similar reason, from Lemma 4.2.3 we obtain the exact sequence

$$0 \longrightarrow F_v^+(T_{m;s;t}) \longrightarrow T_{m;s;t} \longrightarrow F_v^-(T_{m;s;t}) \longrightarrow 0 \tag{5.5}$$

where, by definition, $F_v^\pm(T_{m;s;t}) := F_v^\pm(\mathbf{T}^{\mathrm{Iw}}) \otimes_{\mathcal{R}^{\mathrm{Iw}}} \mathcal{R}_{m;s;t}$.

Proposition 5.4.4. *Let* $\quad \geq 1$. *For any place* $v \quad$ *of* $L \quad$ *above* v, *we have*

$$\mathrm{res}_v\ (\quad_{[n;\ ]}) \in \ker\Big(H^1((L\ \ )_v\ ;T_{m;s}) \longrightarrow H^1((L\ \ )_v\ ;F_v^-(T_{m;s}))\Big):$$

Proof. Let $a \geq \quad$ be a positive integer, fix v_a a valuation of L_a abowe v . We have the following commutative diagram

$$\begin{array}{ccccc}
H^1(L_a(n);\mathbf{T}^\dagger) & \xrightarrow[\oplus \mathrm{res}_w]{} & \oplus_{w|v_a} H^1(L_a(n)_w;\mathbf{T}^\dagger) & \longrightarrow & \oplus_{w|v_a} H^1(L_a(n)_w;F_v^-(\mathbf{T}^\dagger)) \\
\downarrow{\scriptstyle D_n} & & {\scriptstyle D_n}\downarrow & & {\scriptstyle D_n}\downarrow \\
H^1(L_a(n);\mathbf{T}^\dagger) & \xrightarrow[\oplus \mathrm{res}_w]{} & \oplus_{w|v_a} H^1(L_a(n)_w;\mathbf{T}^\dagger) & \longrightarrow & \oplus_{w|v_a} H^1(L_a(n)_w;F_v^-(\mathbf{T}^\dagger)) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(L_a(n);T_{m;s}) & \xrightarrow[\oplus \mathrm{res}_w]{} & \oplus_{w|v_a} H^1(L_a(n)_w;T_{m;s}) & \longrightarrow & \oplus_{w|v_a} H^1(L_a(n)_w;F_v^-(T_{m;s}))
\end{array}$$

where w varies among all places of $L_a(n)$ above v_a, and:

(i) the commutativity of the two upper squares follows from the fact that D_n commutes with the restriction (see Remark 5.4.1) and from the fact that the action of D_n is functorial (see [NSW13, Proposition 1.5.2]);

(ii) the commutativity of the two bottom squares comes from the fact that tensoring over $\mathcal{R}$ commutes with restriction in cohomology and with $\mathcal{R}$-linear maps.

From the commutativity of the diagram above and the fact that, by Proposition 5.3.7, $z_{n;a} \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L_a(n); \mathbf{T}^\dagger)$ we obtain that the image of $z_{n;a}$ inside the sum $\oplus_{w|v_a} H^1((L_a(n))_w; F_v^-(T_{m;s}))$ is zero. This implies that, chasing the commutative diagram

$$\begin{array}{ccccc} H^1(L_a(n); T_{m;s}) & \xrightarrow{\mathrm{res}_w} & H^1(L_a(n)_w; T_{m;s}) & \longrightarrow & H^1(L_a(n)_w; F_v^-(T_{m;s})) \\ \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} \\ H^1(L_a; T_{m;s}) & \xrightarrow[\mathrm{res}_{v_a}]{} & H^1((L_a)_{v_a}; T_{m;s}) & \longrightarrow & H^1((L_a)_{v_a}; F_v^-(T_{m;s})); \end{array}$$

the image of $\quad_{[n;a]}$ is zero in $H^1(L_a(n)_w; F_v^-(T_{m;s}))$ for every place w above v_a. Our claim reduces to show that the image of $\quad_{[n;a]}$ in $H^1((L_a)_{v_a}; F_v^-(T_{m;s}))$ is zero when $a =$. For any $a \geq$, call this image $c_{[n;a]}$.

From the discussion above we know that $c_{[n;a]}$ lies in the kernel of the right vertical restriction map of the last diagram. We call this kernel M_a.

Chasing the norm compatibility properties of the $z_{n;a}$ (shown in Lemma 5.3.3) in the diagrams above (mainly using [NSW13, Corollary 1.5.8] and observing at a certain point that any prime above v is totally ramified in the extension L_∞/H_1), one is able to prove that

$$\mathrm{cor}_{(L_a)_{v_a}/(L_{a-1})_{v_{a-1}}}(c_{[n;a]}) = c_{[n;a-1]};$$

for every $a \geq$. Therefore, our claim reduces to prove that $c_{[n;a]} = 0$ for some $a \geq$. Moreover, the corestriction maps naturally restrict to

$$\mathrm{cor}_{(L_a)_{v_a}/(L_{a-1})_{v_{a-1}}} : M_a \longrightarrow M_{a-1};$$

By inflation-restriction

$$M_a \cong H^1\Big(L_a(n)_w/(L_a)_{v_a}; H^0(L_a(n)_w; F_v^-(T_{m;s}))\Big) =: N_a;$$

and the corestriction maps on the M_a's correspond, on the N_a's, to

$$\begin{aligned} {}_a : N_a &\longrightarrow N_{a-1} \\ [f] &\longmapsto [\mathrm{Tr}_{L_a(n)_w/L_{a-1}(n)_w} \circ f \circ i_a^{-1}] \end{aligned}$$

on classes of cocycles, where i_a is the natural isomorphism

$$i_a : \mathrm{Gal}(L_a(n)_w/(L_a)_{v_a}) \longrightarrow \mathrm{Gal}(L_{a-1}(n)_w/(L_{a-1})_{v_{a-1}})$$

and where the trace acts on the codomain of the cocycle. The proof of this fact is just bookkeeping up to making a smart choice for representatives of the group $\mathrm{Gal}((L_a)_{v_a}/(L_{a-1})_{v_{a-1}})$ inside $G_{(L_{a-1})_{v_{a-1}}}$.

Notice that, since by Corollary 4.1.6 the module $T_{m;s}$ is finite, the size of the modules $H^0(L_a(n)_w; F_v^-(T_{m;s}))$ is bounded independently on a, hence these modules stabilize for large enough a. For these large enough values of a, the trace map in the defintion of $\quad_a$ equals the multiplication by the cardinality of $\mathrm{Gal}((L_a)_{v_a}/(L_{a-1})_{v_{a-1}})$,

that is p (since the primes of H_1 above v are totally ramified in L_∞). This implies that, for big enough a, there is an $\bar{a} > a$ such that

$$\kappa_{a+1} \circ \kappa_{a+2} \circ \cdots \circ \kappa_{\bar{a}}$$

is the zero map. Since $c_{[n;a]}$ lies in the image of this map, it is zero. Therefore, $c_{[n;\,]} = 0$. □

Corollary 5.4.5. $\mathrm{res}_v(\kappa_n) \in \ker\left(H^1(K_v; T_{m;s;t}) \longrightarrow H^1(K_v; F_v^-(T_{m;s;t}))\right)$.

Proof. The exact sequence (5.5) yields the commutative diagram

$$\begin{array}{ccccc}
H^1(L_t; T_{m;s}) & \xrightarrow{\oplus \mathrm{res}_{v_t}} & \oplus_{v_t|v} H^1((L_t)_{v_t}; T_{m;s}) & \longrightarrow & \oplus_{v_t|v} H^1((L_t)_{v_t}; F_v^-(T_{m;s})) \\
\downarrow \mathrm{Sh}_t & & \downarrow \mathrm{Sh}_t & & \downarrow \mathrm{Sh}_t \\
H^1(H_1; T_{m;s;t}) & \xrightarrow{\oplus \mathrm{res}_{v_1}} & \oplus_{v_1|v} H^1((H_1)_{v_1}; T_{m;s;t}) & \longrightarrow & \oplus_{v_1|v} H^1((H_1)_{v_1}; F_v^-(T_{m;s;t})) \\
\downarrow \mathrm{cor} & & \downarrow & & \downarrow \\
H^1(K; T_{m;s;t}) & \xrightarrow{\mathrm{res}_v} & H^1(K_v; T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(K_v; F_v^-(T_{m;s;t}))
\end{array}$$

where the bottom vertical maps come from Corollary A.1.2 and the functoriality of corestriction and Galois action in cohomology. Following the path of $\kappa_{[n;t]}$ from the upper left to the bottom right and applying Proposition 5.4.4, we conclude. □

Remark 5.4.6. Thanks to the exact sequence (5.5), Corollary 5.4.5 is equivalent to

$$\mathrm{res}_v(\kappa_n) \in \mathrm{Im}\left(H^1(K_v; F_v^+(T_{m;s;t})) \longrightarrow H^1(K_v; T_{m;s;t})\right).$$

As we noticed before Lemma 4.2.7, the result of Corollary 5.4.5 is not enough to conclude that $\mathrm{res}_v(\kappa_n) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t})$, because

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t}) = \mathrm{Im}\left(H^1(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}})) \longrightarrow H^1(K_v; T_{m;s;t})\right).$$

This is why, following the ideas of [Büy14, Hypothesis (H.stz)], we make the following assumption.

Assumption 5.4.7. For every valuation $v \mid p$ of K we assume that

$$H^0(K_v; F_v^-(\mathbf{T}^\dagger)) = \{0\};$$

where $F_v^-(\mathbf{T}^\dagger) := F_v^-(\mathbf{T}^\dagger) \otimes_{\mathcal{R}} \mathcal{R}/\mathfrak{m}_{\mathcal{R}}$.

Remark 5.4.8. By Lemma 4.1.8, the residual G_K-representation $\mathbf{T}^\dagger$ coincides with $\mathbf{T}^{\mathrm{Iw}}$. Therefore Assumption 5.4.7 is equivalent to assume that

$$H^0(K_v; F_v^-(\mathbf{T}^{\mathrm{Iw}})) = \{0\}.$$

Notice that $F_v^-(\mathbf{T}^{\mathrm{Iw}}) \cong F_v^-(\mathbf{T}^\dagger)$ is a vector space of dimension 1 over a finite field. Moreover, the action of G_{K_v} on it factors through the product of characters $\varepsilon_v \, \psi_v^{-1}$, where $\psi_v : G_{K_v} \to \mathcal{R}^\times$ is the unramified character defined by sending Fr_v to U_p (see [LV11, p. 300]). Therefore, Assumption 5.4.7 is equivalent to require that the character $\varepsilon_v \, \psi_v^{-1}$ is not identically congruent to 1 modulo $\mathfrak{m}_{\mathcal{R}}$.

We will also see in Chapter 6 that Assumption 5.4.7 will be useful to compare different local conditions on some specializations of $\mathbf{T}^{\mathrm{Iw}}$ (see Proposition 6.2.5). For more insights on this Assumption 5.4.7, see [Büy14, Remark 4.24].

Proposition 5.4.9. *Under Assumption 5.4.7 we have that*

$$\mathrm{res}_v(\ \ _n) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t}).$$

Proof. Let's use the letter T to denote one of $\mathbf{T}^{\mathrm{Iw}}$, $\mathbf{T}^{\mathrm{Iw}}/(\ !_{2;m})$, $\mathbf{T}^{\mathrm{Iw}}/(\ !_{2;m}; p^s)$ or $\mathbf{T}^{\mathrm{Iw}}/(\ !_{2;m}; p^s;\ \ ^{p^t}-1) = T_{m;s;t}$. Assumption 5.4.7 together with Nakayama's lemma (see Lemma 4.1.10) yields that $H^0(K_v; F_v^-(T)) = \{0\}$. The duality between $F_v^-(T)$ and $F_v^+(T)$ coming from the perfect alternating pairing of [How07, (3)] together with Tate local duality implies that

$$H^2(K_v; F_v^+(T)) = \{0\}; \tag{5.6}$$

as noted also in [Büy14, p. 809]. Since $F_v^+(\mathbf{T}^{\mathrm{Iw}})$ is free over $\mathcal{R}^{\mathrm{Iw}}$, multiplication by $!_{2;s}$ yields the exact sequence

$$0 \longrightarrow F_v^+(\mathbf{T}^{\mathrm{Iw}}) \xrightarrow{!_{2;s}} F_v^+(\mathbf{T}^{\mathrm{Iw}}) \longrightarrow F_v^+(\mathbf{T}^{\mathrm{Iw}}/(\ !_{2;m})) \longrightarrow 0.$$

Taking the long exact sequence in cohomology, equation (5.6) gives a surjection

$$H^1(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}})) \twoheadrightarrow H^1\big(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}}/(\ !_{2;m}))\big).$$

Repeating the same argument to the exact sequences attached to the multiplication by p^s and $\ ^{p^t}-1$, we eventually obtain a surjection

$$H^1(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}})) \twoheadrightarrow H^1(K_v; F_v^+(T_{m;s;t})).$$

Then we have the commutative diagram

$$\begin{array}{ccc} H^1(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}})) & \longrightarrow & H^1(K_v; \mathbf{T}^{\mathrm{Iw}}) \\ \big\downarrow & & \big\downarrow \\ H^1(K_v; F_v^+(T_{m;s;t})) & \longrightarrow & H^1(K_v; T_{m;s;t}) \end{array}$$

where the left vertical map is surjective. By Remark 5.4.6 we know that $\mathrm{res}_v(\ \ _n)$ lies in the image of the bottom horizontal map, hence it comes from an element of $H^1(K_v; F_v^+(\mathbf{T}^{\mathrm{Iw}}))$. By definition of the Greenberg condition on $T_{m;s;t}$, this implies that

$$\mathrm{res}_v(\ \ _n) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t}).$$

□

5.4.3 Local properties at primes dividing N

For this subsection, fix a place $v \mid N$ of K.

Proposition 5.4.10. *Let v be a place of L such that $v \mid v$. Then for every ≥ 1 we have that*

(a) $\mathrm{res}_v(\ \ _{[n;\ ]}) \in \ker\Big(H^1((L\ \ )_v\ ; T_{m;s}) \longrightarrow H^1((L\ \ )_v^{\mathrm{ur}}; T_{m;s})\Big)$.

(b) $\mathrm{res}_v(\ \ _n) \in \ker\Big(H^1(K_v; T_{m;s;t}) \longrightarrow H^1(K_v^{\mathrm{ur}}; T_{m;s;t})\Big)$.

Proof. The proof of Proposition 5.4.2 goes through verbatim. □

As in the case of the previous subsection, when $v \mid p$, this proposition is not enough to conclude that $\mathrm{res}_v(\ _n) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t})$. However, since we are working under Assumption 5.2.3, we have a control on Tamagawa factors and we can deduce the following result.

Proposition 5.4.11. *With notation as above, we have that*

$$\mathrm{res}_v(\ _n) \in H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v; T_{m;s;t}):$$

Proof. The commutative diagram with exact rows

$$\begin{array}{ccccc} H^1_{\mathrm{ur}}(K_v; \mathbf{T}^{\mathrm{Iw}}) & \longrightarrow & H^1(K_v; \mathbf{T}^{\mathrm{Iw}}) & \xrightarrow{\mathrm{res}} & H^1(K_v^{\mathrm{ur}}; \mathbf{T}^{\mathrm{Iw}}) \\ & & \downarrow & & \downarrow \\ H^1_{\mathrm{ur}}(K_v; T_{m;s;t}) & \longrightarrow & H^1(K_v; T_{m;s;t}) & \xrightarrow{\mathrm{res}} & H^1(K_v^{\mathrm{ur}}; T_{m;s;t}) \end{array}$$

induces a map

$$: H^1_{\mathrm{ur}}(K_v; \mathbf{T}^{\mathrm{Iw}}) \longrightarrow H^1_{\mathrm{ur}}(K_v; T_{m;s;t}):$$

To conclude the proof, it su□ces to show that is surjective. By inflation-restriction, the map corresponds to the map

$$H^1(K_v^{\mathrm{ur}}/K_v; (\mathbf{T}^{\mathrm{Iw}})^{\mathrm{I}_v}) \longrightarrow H^1(K_v^{\mathrm{ur}}/K_v; T_{m;s;t}^{\mathrm{I}_v})$$

induced by the morphism $: (\mathbf{T}^{\mathrm{Iw}})^{\mathrm{I}_v} \to T_{m;s;t}^{\mathrm{I}_v}$. As proven in [Büy14, Lemma 4.27] (see also Remark 5.2.6), under Assumption 5.2.3 the natural morphism $' : (\mathbf{T}^{\dagger})^{\mathrm{I}_v} \to T_{m;s}^{\mathrm{I}_v}$ is surjective. Since I_v acts trivially on $^{\mathrm{ac}}$, semilocal Shapiro's lemma on the 0-th cohomology groups (see [Rub00, Proposition 4.2]) implies that also is surjective. The claim now follows by applying the long exact sequence in cohomology and noticing that $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$ has cohomological dimension 1, exactly as in the end of the proof of [Büy14, Proposition 4.26]. □

5.4.4 The Kolyvagin system

Under the running assumptions, the results of Proposition 5.4.2, Proposition 5.4.3, Proposition 5.4.9 and Proposition 5.4.11 lead to the following theorem.

Theorem 5.4.12. *Let $m; s; t \in \mathbb{Z}_{>0}$ and let $n \in \mathcal{N}_{m;s}$. Then*

$$_n \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K; T_{m;s;t}):$$

We want to build a Kolyvagin system out of the classes $_n$. Denote by $^*_{[n;t]} := \mathrm{cor}_{L_t/K_t}\ _{[n;t]}$. The diagram

$$\begin{array}{ccc} H^1(L_t; T_{m;s}) & \longrightarrow & H^1(H_1; T_{m;s;t}) \\ {\scriptstyle \mathrm{cor}}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}} \\ H^1(K_t; T_{m;s}) & \longrightarrow & H^1(K; T_{m;s;t}) \end{array}$$

is commutative, where the horizontal maps are Shapiro's maps Sh_t, so the classes $^*_{[n;t]}$ are another byproduct of the descent procedure of Subsection 5.3.3 (they are closer to the classes used in [Büy14]).

We now study what happens when we move the parameters $m;s;t$. With this aim, we denote by $\kappa_n^{(m;s;t)}$ what we called κ_n, in order to make clear the dependence on $m;s;t$. If we take $m := (m;s;t) \leq i := (i;j;r)$ (see Subsection 4.2.5), there are natural maps

$$\iota_{i;m} : H^1(K;T_i) \longrightarrow H^1(K;T_m):$$

Lemma 5.4.13. *For every $m \leq i$ and $n \in \mathcal{N}_i$ we have*

$$\iota_{i;m}(\kappa_n^{(i)}) = \kappa_n^{(m)}:$$

Proof. By the compatibility of Lemma 5.3.13, both $\kappa_n^{(i)}$ and $\kappa_n^{(m)}$ come from a unique class $z_{n;r} \in H^1(L_r(n);\mathbf{T}^{\mathrm{lw}})$, and the maps used to define $\kappa_n^{(i)}$ and $\kappa_n^{(m)}$ from $z_{n;r}$ commute with $\iota_{i;m}$, since they just involve restrictions, corestrictions, Galois actions and Shapiro's maps. □

From the fact that $\varprojlim_{(m;s;t)} T_{m;s;t} = \mathbf{T}^{\mathrm{lw}}$, we obtain that

$$\varprojlim_{(m;s;t)} H^1(K;T_{m;s;t}) \cong \varprojlim_t H^1(K;\mathbf{T}^\dagger \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/(p^t-1)) \cong \varprojlim_t H^1(K_t;\mathbf{T}^\dagger);$$

where the last isomorphism comes from Lemma 4.1.16. When $n = 1$, the system of elements $\{\kappa_1^{(m;s;t)}\}_{m;s;t\in\mathbb{Z}_{>0}}$, that is compatible with respect to the maps of Lemma 5.4.13, yields an element of $\varprojlim_t H^1(K_t;\mathbf{T}^\dagger)$, that coincides with $\kappa_\infty := \{\kappa^*_{[1;t]}\}_{t\in\mathbb{Z}_{>0}}$. Explicitely,

$$\kappa^*_{[1;t]} = \mathrm{cor}_{L_t/K_t} z_{1;t} = \mathrm{cor}_{H_{p^{t+1}}/K_t} U_p^{-t}\,\kappa_{p^{t+1}};$$

where $\kappa_{p^{t+1}}$ is the big Heegner class of Definition 3.5.3. The main result of this chapter is that the system of elements $\{\kappa_1^{(m;s;t)}\}_{m;s;t\in\mathbb{Z}_{>0}}$ can be slightly modified in order to obtain a universal Kolyvagin system whose set of classes at $n = 1$ coincides with κ_∞. However, we are not able to get this result in great generality, but we need to work under some (technical) assumptions and to select a subset $\mathcal{P}'_{m;s;t}$ of $\mathcal{P}_{m;s;t}$ of primes to work with.

Theorem 5.4.14. *Under Assumption 5.5.4 and Conjecture 5.5.7, there is a universal Kolyvagin system $\kappa \in \overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}')$ such that*

$$\kappa_1 = \{\kappa_1^{(m;s;t)}\}_{m;s;t\in\mathbb{Z}_{>0}} = \kappa_\infty \in \varprojlim_t H^1(K_t;\mathbf{T}^\dagger):$$

For a precise statement and a proof of this theorem, see Corollary 5.5.11 and the assumptions made in the next section.

Remark 5.4.15. At this point, our arithmetic context is formally equivalent to the one of [Büy14, Theorem 4.28]. There, Theorem 5.4.14 is claimed without any further assumptions. However, we were not able to find a proof that works in great generality. In particular, it seems fundamental to require some "big image" condition for the $G_{\mathbb{Q}}$-representation $\mathbf{T}^\dagger$ (see Assumption 5.5.4) and to work with some well-chosen subsets of $\mathcal{P}_{m;s}$.

5.5 On the proof of Theorem 5.4.14

In this section we prove that a slight modification of the set of elements $\{\ \ _n\}_{n\in\mathcal{N}_{s;m}}$ form a Kolyvagin system for $T_{m;s;t}$, and that these Kolyvagin systems can be put together in order to form a universal Kolyvagin system for the representation $\mathbf{T}^{\mathrm{lw}}$. The main idea is to adapt arguments of [Nek92, §7-12], [Bes97] and of [How04b, §1.7] to our context.

5.5.1 The arithmetic context

In this subsection we prove that our arithmetic context satisfies conditions (i)-(x) described in Subsection A.3.2, and we derive a key formula.

Fix $m;s;t\in\mathbb{Z}_{>0}$ with $s\geq m$. Let $n\in\mathcal{N}_{s;m}$ and $(\ell)=\ \in\mathcal{P}_{m;s}$ such that $\ell\nmid n$. Choose a prime $\ _\lambda$ of H_λ above $\ $. For every element $\ \in H^1(-;\mathbf{T}^\dagger)$ denote by $\ '$ the image of $\ $ in $H^1(-;T_m)$.

Set $\bar{G}=G_{L_t(n)^+}$ (where $L_t(n)^+$ is the maximal real subfield of $L_t(n)$), $G=G_{L_t(n)}$, $H=G_{L_t(n\ell)}$, $\bar{G}=G_{\mathbb{Q}_\lambda}$, $G_0=G_K$, $H_0=G_{(H_\lambda)_\wp}$, $\ =\ _\ell$, $A=T_m$, $S=R_m$, $\ =\mathrm{Fr}_\lambda$, $d=\ell$, $M=\ell+1$, $M_1=T_\lambda\in R_m$, $x=D_n z'_{n;t}\in H^1(L_t(n);T_m)$ and $y=D_n z'_{n\ell;t}\in H^1(L_t(n\ell);T_m)$. The goal of this subsection is to check that these elements satisfy conditions (i)-(x) of Subsection A.3.2.

Point (i), (ii) and (iv) can be easily verified. Point (iii) descends from a study of the maximal tamely ramified extension of $\mathbb{Q}_\lambda$ (see Section A.2). Point (vi) descends from the fact that $\ \in\mathcal{P}_{m;s}$, point (vii) is a consequence of Lemma 5.3.4 and point (viii) is a direct consequence of the proof of Lemma 5.3.12. Point (v) is a consequence of the following proposition.

Proposition 5.5.1. *Let L be a finite extension of $\mathbb{Q}_\lambda$ and recall that $s\geq m$. The inflation map*

$$\inf: H^1(L^{\mathrm{ur}}/L;T_m)\longrightarrow H^1(L;T_m)$$

is an isomorphism.

Proof. Let ℓ^d be the cardinality of the resudue field of L. In order to apply Lemma A.2.2, we need to check that ℓ^d is not an eigenvalue for the action of Fr_L on T_m.

Let $\mathfrak{p}$ be an arithmetic prime of $\mathcal{R}$ of weight 2 and character $\varepsilon:\ /\ ^{p^m}\to\mathbb{Q}_p^\times$. Then $\mathfrak{p}$ contains $\ _{2;m}$ and $\ _{2;s}$, and gives an arithmetic map

$$\mathcal{R}\longrightarrow R_s\longrightarrow R_m\longrightarrow \mathrm{Frac}(R/\mathfrak{p})$$

that yields a specialization

$$\mathbf{T}^\dagger\longrightarrow T_s\longrightarrow T_m\otimes_{R_m}\mathrm{Frac}(\mathcal{R}/\mathfrak{p}):$$

The representation $T_m\otimes_{R_m}\mathrm{Frac}(\mathcal{R}/\mathfrak{p})$ is the twist by $\ ^{-1}$ of the representation attached by Deligne to the modular form of the Hida family passing throug f that corresponds to the arithmetic prime $\mathfrak{p}$ (see Theorem 3.3.4). Lemma 4.1.22 implies that $\ (\mathrm{Fr}_L)$ acts as ±1 on T_m, hence by Weil conjectures we obtain that ℓ^d is not an eigenvalue for Fr_L on $T_m\otimes_{R_m}\mathrm{Frac}(\mathcal{R}/\mathfrak{p})$ (see also the end of the proof of [Nek92, Lemma 4.1]). The Galois equivariancy of the specialization map implies that $\pm\ell^d$ is not an eigenvalue for Fr_L on T_m, and we conclude by applying Lemma A.2.2. □

Point (ix) of Subsection A.3.2 is a consequence of the following lemma.

Lemma 5.5.2 (Eichler-Shimura relation). *Let $!(n)$ denote the number of prime divisors of n.*

(a) The classes $z'_{n\ell;t}$ and $\mathrm{Fr}_\ell(z'_{n;t})$ coincide when restricted to $L_t(n\ell)_{\mathfrak{n}_\ell} = (H_\ell)_{\mathfrak{n}_\ell}$ for any prime $\mathfrak{n}_\ell$ above ℓ.

(b) The classes $D_n z'_{n\ell;t}$ and $(-1)^{!(n)}\mathrm{Fr}_\ell(D_n z'_n)$ coincide modulo p^s when restricted to $L_t(n\ell)_{\mathfrak{n}_\ell} = (H_\ell)_{\mathfrak{n}_\ell}$.

Proof. Point (a) descends from Proposition 3.5.7 together with the functoriality of the action of Fr_ℓ and its commutativity with the operators U_p and cor.

Turning to point (b), Remark 4.1.19 says that the action of Fr_ℓ on T_m coincides with the action of the complex conjugation c modulo p^s. Then the claim follows by applying the operator D_n to point (a), together with the commutativity relation proved in point (b) of Lemma 5.3.9. □

Finally, by Corollary 4.1.23 we know that the characteristic polynomial of the action of Fr_ℓ on T_m is

$$X^2 - (-1)^{\frac{k+j}{2}-1}T_\ell X + \ell;$$

therefore point (x) of Subsection A.3.2 is satisfied. Then, applying the machinery explained in Subsection A.3.2, the key formula (A.6) translates to

$$\big((-1)^{!(n)}(\ell+1)\,\mathrm{Fr}_\ell - T_\ell\big)a_X = \big((-1)^{\frac{k+j}{2}-1}T_\ell\,\mathrm{Fr}_\ell - (\ell+1)\big)\big(a - p^s(\text{something})\big) \quad (5.7)$$

in T_m, where $a_X \in T_m$ is congruent to $(D_n z'_{n;t})(\mathrm{Fr}_\mathfrak{n})$ modulo $(\mathrm{Fr}_\mathfrak{n} - 1)T_m$ and a is congruent to $-(\mathrm{res}^{-1}_{L_t(n)/L_t(n\ell)} D_{n\ell} z'_{n\ell;t})(\sigma_\ell)$ modulo p^s, where σ_ℓ is a fixed lifting of σ_ℓ to $\mathrm{Gal}(K_\infty/K^{\mathrm{ur}})$ (see (A.4)). Applying Lemma 5.3.12, using bars in order to denote projections to $T_{m;s}$ and the fact that $\mathrm{Fr}_\mathfrak{n} = \mathrm{Fr}_\mathfrak{n}^2$ is the identity on $T_{m;s}$ we obtain that

- $a_X = \kappa_{[n;t]}(\mathrm{Fr}_\mathfrak{n})$ in $T_{m;s}$;
- $a = -\kappa_{[n\ell;t]}(\sigma_\ell)$ in $T_{m;s}$.

Remark 5.5.3. Here we comment the importance of the relation (5.7). Suppose that one wants to prove that the set $\{\kappa_n \otimes \sigma_\ell|_{n\ell}\}_{n\in\mathcal{N}_{m;s}}$ is a Kolyvagin system. Then, by definition (see also Remark 4.2.14), one needs to check that for every $n\ell \in \mathcal{N}_{m;s}$ the equality

$$\mathrm{fs}(\mathrm{res}_\mathfrak{n}(\kappa_n)) = \mathrm{res}_{\mathfrak{n}_\ell}(\kappa_{n\ell}) \otimes \sigma_\ell$$

holds in $H^1_s(K_\infty; T_{m;s;t}) \otimes \mathcal{G}_\ell$. By the explicit description of the isomorphisms of Lemma 4.2.9 (see Remark 4.2.10), this amounts to check that

$$\kappa_n(\mathrm{Fr}_\mathfrak{n}) = \kappa_{n\ell}(\sigma_\ell).$$

Equation (5.7) is then a first step in finding a relation between the left and the right-hand side of this equation. As we will see, we will not be able to prove that the set $\{\kappa_n \otimes \sigma_\ell|_{n\ell}\}_{n\in\mathcal{N}_{m;s;t}}$ is a Kolyvagin system, but we will need to do some slight modifications.

5.5.2 A finer choice of primes

Let's continue to work with fixed $m;s;t \in \mathbb{Z}_{>0}$ with $s \geq m$. Recall that, by Lemma 4.1.18, for every prime $(\ell) = \in \mathcal{P}_{m;s}$ we have that $p^s \mid \ell + 1$ and $p^s \mid T_\ell$ as elements of R_m. We need to control also the non-divisibility at p of a linear combination of these elements.

In order to do that we need to study the image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}_{R_m}(T_m)$. In particular, we will need the following big image result.

Assumption 5.5.4. The image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}(T_m)$ contains the scalars $1 + p^s\mathbb{Z}_p$.

Remark 5.5.5. We present here an infinite set of representations for which Assumption 5.5.4 is verified, but we suspect it to be true for many other families.

First, suppose that the cusp form f fixed in Subsection 3.2.1 has weight $k = 2$. This is not a strong assumption, since inside the Hida family of any fixed (admissible) cuspform there is always a p-adic form of weight 2. Then, thanks to [Fis02, Theorem 4.8], there is a set of primes of density 1 (called $_f$ in [Fis02, p.355]) with the property that if $p \in {}_f$ then the image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}_{\mathcal{R}}(\mathbf{T})$ contains $\mathrm{SL}_2(\mathcal{R})$ (see also the proof of [Vig22, Theorem 4.15]). This implies that the image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}_{R_m}(\mathbf{T}/(\ell_{2;m}))$ contains $\mathrm{SL}_2(R_m)$.

Call the image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}_{R_m}(T_m)$. Since T_m is a twist of $\mathbf{T}/(\ell_{2;m})$ by a character of finite order, every element of $\mathrm{Aut}_{R_m}(T_m)$ has a scalar multiple that lies in . Since $\mathrm{SL}_2(R_m)$ is the commutator of $\mathrm{Aut}_{R_m}(T_m)$, then must contain $\mathrm{SL}_2(R_m)$.

For all $\ell \nmid Np$, the image of Fr_ℓ has determinant ℓ in $\mathrm{Aut}_{R_m}(T_m)$ by Proposition 3.3.6, therefore contains all matrices of determinant ℓ. The set of primes $\ell \nmid Np$ is dense in $\mathbb{Z}_p^\times$, is closed and the determinant map is continuous, therefore contains the whole $\mathrm{GL}_2(\mathbb{Z}_p)$. In particular, T_m satisfies Assumption 5.5.4 for every $m \geq 1$.

Now we present the main consequence of Assumption 5.5.4.

Lemma 5.5.6. *There is an infinite subset $\mathcal{P}'_{m;s}$ of $\mathcal{P}_{m;s}$ such that*

(a) for every $(\ell) \in \mathcal{P}'_{m;s}$ we have that

$$p^{s+1} \nmid \ell + 1 \pm T_\ell$$

as elements of R_m;

(b) for every $(\ell);(\ell') \in \mathcal{P}'_{m;s}$ we have that

$$\ell + 1 \equiv \ell' + 1 \pmod{p^{2s}} \quad \textit{and} \quad T_\ell \equiv T_{\ell'} \pmod{p^{2s}}.$$

Proof. Fix a prime λ below a prime of $\mathcal{P}_{m;s}$. By Corollary 4.1.23 we know that the action of Fr_λ on T_m has the properties

$$\mathrm{Tr}(\mathrm{Fr}_\lambda) = (-1)^{\frac{k+j}{2}-1}T_\lambda \quad \text{and} \quad \det(\mathrm{Fr}_\lambda) = \lambda.$$

Let now $\in 1 + p^s\mathbb{Z}_p$. By Assumption 5.5.4 there is an element $\in G_{\mathbb{Q}}$ such that the image of in $\mathrm{Aut}(T_m)$ is . Then, on T_m, we have

$$\mathrm{Tr}(\mathrm{Fr}_\lambda \quad) = (-1)^{\frac{k+j}{2}-1}\ T_\lambda \quad \text{and} \quad \det(\mathrm{Fr}_\lambda \quad) = {}^2\lambda.$$

Take now a prime ℓ such that Fr_ℓ is conjugated to Fr_{τ} in $\mathrm{Gal}(K(T_{m;2s})/\mathbb{Q})$. By Chebotarev's density theorem, we can find infinitely many such primes. One can check directly that $(\ell) \in \mathcal{P}_{m;s}$, since

$$T_\ell \equiv T_\tau \pmod{p^{2s}} \quad \text{and} \quad \ell \equiv \tau^2 \pmod{p^{2s}} \tag{5.8}$$

in R_m (see also Remark 4.1.19).

Let $\mathfrak{p}$ be an arithmetic prime of R_m of weight 2 and character $\varepsilon : (\mathbb{Z}/p^s)^\times \to \mathbb{Q}_p^\times$ and consider the two relations

$$\tau^2 \pm \alpha T_\tau + 1 \tag{5.9}$$

with coefficients in $R_m/\mathfrak{p}$ and variable α. Our claim is that there is always $\tau \in 1+p^s\mathbb{Z}_p$ (depending on our choice of α) that makes both these relations not congruent to 0 modulo p^{s+1}. This can be checked directly in the following way. Set $\tau = 1 + xp^s$, $\alpha = -1 + ap^s$ and $T_\ell = bp^s$ for fixed $a \in \mathbb{Z}$, $b \in R_m/\mathfrak{p}$ and variable $x \in \mathbb{Z}_p$. A direct computation yields that equation (5.9) becomes

$$(a - 2x \pm c)p^s + p^{2s} \cdot (\text{something}).$$

Since p is a power of a prime element in $R_m/\mathfrak{p}$, we just need to ask that $p \nmid (a-2x\pm c)$. Since $p \geq 5$, there is an $x \in \mathbb{Z}_p$ such that its reduction x modulo p satisfies $x \neq (a\pm c)/2$. We then have that $\tau := 1 + xp^s$ satisfies the claim.

Lifting to R_m, one obtains then that $\tau^2 \pm \alpha T_\tau + 1 \not\equiv 0 \pmod{p^{s+1}}$. Define now $\mathcal{P}'_{m;s}$ to be the set of all primes ℓ such that Fr_ℓ is conjugated to $\mathrm{Fr}_{\tau\sigma}$ in $\mathrm{Gal}(K(T_{m;2s})/\mathbb{Q})$. For every $(\ell) \in \mathcal{P}'_{m;s}$, since $\ell + 1 \pm T_\ell$ is congruent to (5.9) modulo p^{s+1}, we have that

$$\ell + 1 \pm T_\ell \not\equiv 0 \pmod{p^{s+1}};$$

yielding point (a). By (5.8) we also have that

$$T_\ell \equiv \alpha T_\tau \pmod{p^{2s}} \quad \text{and} \quad \ell \equiv \alpha^2 \pmod{p^{2s}};$$

yielding point (b). □

Definition. We define $\mathcal{N}'_{m;s}$ to be the set of squarefree products of primes lying below elements of $\mathcal{P}'_{m;s}$.

5.5.3 The result

Before stating the main result, we need to spend a few words on the action of the complex conjugation. In particular, we will work under the following conjecture.

Conjecture 5.5.7. For every $n \in \mathcal{N}_{m;s}$ the complex conjugation c acts on the element $\kappa_{[n;t]} \in H^1(L_t; T_{m;s})$ as

$$c\,\kappa_{[n;t]} = \varepsilon_n\,\kappa_{[n;t]}$$

for some $\sigma \in \mathrm{Gal}(L_t/K)$ and some $\varepsilon_n \in \{\pm 1\}$ that depends only on the number of prime factors $\omega(n)$ of n.

Remark 5.5.8. This conjecture should descend from a quaternionic counterpart of [How07, Proposition 2.3.5], that gives an explicit description for the action of the complex multiplication on classical big Heegner points. The dependence on $\omega(n)$ would then be a consequence of the action of D_n on our starting points, as explained

for example in [Nek06, Proposition 10.2, (1)] (it is essentially a consequence of point (b) of Lemma 5.3.9).

The problem in proving this conjecture is that we do not have a clear modular description of Longo and Vigni's big Heegner points, therefore the generalization of [How07, Proposition 2.3.5] is not straightforward. However, we believe that a deeper study of Longo and Vigni's points would give this result. In a future work, we will also present another family of big Heegner points for which this conjecture can be easily proven.

From now on, we assume Conjecture 5.5.7 to be true. Let now $= (\ ) \in \mathcal{P}_{m;s}$ and $\ : H^1(K\ ; T_{m;s}) \otimes \mathcal{G} \to T_{m;s}$ be the isomorphism coming from point (b) of Lemma 4.2.9. The following lemma studies the behaviour of the action of the complex conjugation c under the isomorphism $\ $.

Lemma 5.5.9. *Let* $= (\ ) \in \mathcal{P}_{m;s}$ *and* $\otimes \ \in H^1(K\ ; T_{m;s}) \otimes \mathcal{G}$. *Then*

$$c \cdot \ (\ \otimes \ ) = - \ (c \otimes \ ):$$

Proof. As noticed in Remark 4.2.10, the isomorphism $\ $ is given by sending the element $\otimes \ $ to $(\sim)$ for any lifting $\sim$ of $\ $ to $\mathrm{Gal}(K\ /K^{\mathrm{ur}})$. However, since $\ $ does not depend on the chosen lifting, the value $(\sim)$ only depends on the class of $\sim$ in $\mathrm{Gal}(K^{\mathrm{ur}}(H\ )\ /K^{\mathrm{ur}})$, that is a quotient of $\mathrm{Gal}(K^{ab}/K^{\mathrm{ur}})$. Then, we can compute

$$(c \otimes \ ) = c \cdot \ (c\sim c) = c \cdot \ (\sim^{-1});$$

where the last equality comes from the fact that the class of $c\sim c$ modulo $G_{K^{ab}}$ coincides with the class of $\sim^{-1}$ modulo $G_{K^{ab}}$. But then, since $\sim^{-1}$ acts trivially on $T_{m;s}$, we have that

$$c \cdot \ (\sim^{-1}) = -c \cdot \ (\sim):$$

□

This lemma implies that the natural action of the complex conjugation on the module $H^1(K\ ; T_{m;s}) \otimes \mathcal{G}$ is sent, under the isomorphism $\ $, to the action of $-c$ on $T_{m;s}$. We are now ready to prove the first main result of this section.

Theorem 5.5.10. *Let* $m \geq s$. *Then there is a Kolyvagin system* $\{\ _n'\}_{n \in \mathcal{N}'_{m;s}}$ *for the triple* $(T_{m;s;t}; \mathcal{F}_{\mathrm{Gr}}; \mathcal{P}'_{m;s})$ *such that* $\ _1' = \ _1$.

Proof. Let $n \in \mathcal{P}'_{m;s}$ and call $= (\ )$ the prime of K above $\ $. From the key formula (5.7) we know that

$$\big((-1)^{!(n)}(\ +1)\,\mathrm{Fr} \ - T \ \big)a_x = \big((-1)^{\frac{k+j}{2}-1} T \ \mathrm{Fr} \ - (\ +1)\big)\big(a - p^s(\text{something})\big) \quad (5.10)$$

on T_m, where, denoting with a bar the reduction to $T_{m;s}$,

- $a_x = \ _{[n;t]}(\mathrm{Fr}\ )$ in $T_{m;s}$;
- $a = - \ _{[n\ ;t]}(\sim\ )$ in $T_{m;s}$

for any fixed lifting $\sim$ of $\ $ to $\mathrm{Gal}(K\ /K^{\mathrm{ur}})$. Notice that both members of equation (5.10) are divisible by p^s, hence we can first divide and then quotient by p^s, obtaining

$$\left(\frac{(-1)^{!(n)}(\ +1)}{p^s}\,\mathrm{Fr} \ - \frac{T \ }{p^s}\right)a_x = \left(\frac{(-1)^{\frac{k+j}{2}-1} T \ }{p^s}\,\mathrm{Fr} \ - \frac{\ +1}{p^s}\right)a \quad \text{on } T_{m;s}:$$

By Remark 4.1.19, Fr_ℓ acts as the complex conjugation c on $T_{m;s}$. Applying the isomorphism ι_ℓ^{-1} to both members of the previous equation, Lemma 5.5.9 yields

$$\left(\frac{\pm(\ell+1)}{p^s}c-\frac{T_\ell}{p^s}\right)\ {}^{\mathrm{fs}}(\mathrm{res}\quad_{[n;t]})=-\left(\frac{\pm T_\ell}{p^s}c-\frac{\ell+1}{p^s}\right)(\mathrm{res}\quad_{[n\ell;t]}\otimes\quad_\ell);$$

where ${}^{\mathrm{fs}}$ is the finite-singular isomorphism defined in Definition 4.2.11. Thanks to Conjecture 5.5.7, applying semilocal Shapiro's map followed by corestriction we obtain the relation

$$\left(\frac{\pm(\ell+1)}{p^s}-\frac{T_\ell}{p^s}\right)\ {}^{\mathrm{fs}}(\mathrm{res}\quad_n)=-\left(\frac{\pm T_\ell}{p^s}-\frac{\ell+1}{p^s}\right)(\mathrm{res}\quad_{n\ell}\otimes\quad_\ell)$$

in $H^1_S(K\ ;T_{m;s;t})\otimes\mathcal{G}_\ell$. Since $\quad\in\mathcal{P}'_{m;s}$, point (a) of Lemma 5.5.6 implies that the coefficients in the last relation are not divisible by p, hence they are units of $R_{m;s;t}$. The $\pm$ signs in the previous relation are either fixed or depend only on $!(n)$. Therefore, applying point (b) of Lemma 5.5.6, we find elements $u_n\in R^\times_{m;s;t}$ for every $n\in\mathcal{N}'_{m;s}$ that depend only on $!(n)$ such that

$$\mathrm{res}\quad_{n\ell}\otimes\quad_\ell=u_{n\ell}\ {}^{\mathrm{fs}}(\mathrm{res}\quad_n)\quad\text{on } T_{m;s;t}. \tag{5.11}$$

Set also $u_1=1$ and take $n\in\mathcal{N}'_{m;s}$. Factor $n=\ell_1\cdots\ell_i$ as product of primes. We define

$$'_n:=\left(u_{\ell_1}^{-1}\cdot u_{\ell_1\ell_2}^{-1}\cdots u_{\ell_1\ell_2\cdots\ell_i}^{-1}\right)\ {}_n\otimes\left(\bigotimes_{\ell\mid n}\quad_\ell\right)\in H^1(K;T_{m;s;t})\otimes\mathcal{G}(n).$$

Since u_m depends only on $!(m)$, the definition of $\ {}'_n$ does not depend on the chosen order for the prime factors of n. Notice that $\ {}'_n\in\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}(n)}(K;T_{m;s;t})\otimes\mathcal{G}(n)$ by Theorem 5.4.12. Equation (5.11) implies that

$$\mathrm{res}\quad{}'_{n\ell}\otimes\quad_\ell={}^{\mathrm{fs}}(\mathrm{res}\quad{}'_n)\quad\text{on } T_{m;s;t}$$

for every $n\ell\in\mathcal{N}_{m;s}$, therefore the set $\{\ {}'_n\}_{n\in\mathcal{N}'_{m;s}}$ is a Kolyvagin system for the triple $(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s})$. □

Denote by $\overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'):=\varprojlim_{(m;s;t)}\mathbf{KS}(T_{m;s;t};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}'_{m;s})$. As in Subsection 5.4.4, denote by $\ {}^{(m;s;t)}_n$ the elements $\ {}_n$, and similarly let $\ {}^{(m;s;t)'}_n$ the elements $\ {}'_n$, in order to make clear the dependence on $m;s;t$. Recall that we defined

$$\ {}_\infty=\{\ {}^{(m;s;t)}_1\}_{m;s;t\in\mathbb{Z}_{>0}}=\{\ {}^*_{[1;t]}\}_{t\in\mathbb{Z}_{>0}}.$$

Corollary 5.5.11. *There is a universal Kolyvagin system* $\kappa\in\overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P}')$ *such that*

$$\kappa_1=\ {}_\infty\in\varprojlim_t H^1(K_t;\mathbf{T}^\dagger).$$

Proof. For a fixed n, the elements $\ {}^{(m;s;t)'}_n$ defined in the previous theorem are compatible, thanks to Lemma 5.4.13 and to the fact that the factors u_n come from global elements of $\mathcal{R}$ and depend only on n. Taking the inverse limit on $m;s;t$, we obtain the claim. □

Chapter 6

Anticyclotomic Iwasawa theory

In this chapter we study Iwasawa theory for the representation $\mathbf{T}^\dagger$. The main goal is to explain the connection between Kolyvagin systems for $\mathbf{T}^{\mathrm{Iw}}$ and the Iwasawa main conjecture for the representation $\mathbf{T}^\dagger$. In particular, we will see that the existence of a Kolvagin system with nontrivial first element implies one divisibility of the Iwasawa main conjecture. The whole conjecture has been proven under mild hypotheses (slightly different than ours) in [CW22] with a different method. We will instead adapt some ideas from [Fou13] to our context.

For this chapter, we keep the setting of the previous one and further make the following assumption, that is often satisfied (see for example [FO12, Lemma 2.7]).

Assumption 6.0.1. The ring $\mathcal{R}$ is regular.

6.1 The Iwasawa main conjecture

In this section we introduce the material that will be needed for the statement of the Iwasawa main conjecture.

6.1.1 Duality

Let R be a complete noetherian regular local ring with maximal ideal $\mathfrak{m}_R$, of Krull dimension $d \geq 1$, with finite residue field $k = R/\mathfrak{m}_R R$ of characteristic p. If M is an R-module and $I \subseteq R$ is an ideal, denote by $M[I]$ the I-torsion R-submodule of M.

Definition. Denote by $M^* := \mathrm{Hom}_R(M; R)$ the R-linear dual of R (where Hom_R denotes the set of R-linear homomorphisms) and by $M^\vee := \mathrm{Hom}_{\mathrm{cont}}(M; \mathbb{Q}_p/\mathbb{Z}_p)$ the Pontryagin dual of M (where $\mathrm{Hom}_{\mathrm{cont}}$ denotes the set of continuous group homomorphisms).

By [Nek06, §2.9.1, §2.9.2], if M is a finitely generated R module or a discrete cofinitely generated R-module then

$$M^\vee = \mathrm{Hom}_R(M; R^\vee). \tag{6.1}$$

Following [Nek06, §0.4], define $\mathbb{D}(M) := M \otimes_R R^\vee$. By [Nek06, (0.4.4)] we have that $(M^*)^\vee \cong \mathbb{D}(M)$ and $(\mathbb{D}(M))^\vee \cong M^*$. Further, by basic properties of Pontryagin duality, if I is an ideal of R then $(M[I])^\vee \cong M^\vee/IM^\vee$ and, if M is a G-module for some profinite group G, we have $(M^G)^\vee \cong (M^\vee)_G$.

6.1.2 Modules over Iwasawa algebras

In this subsection we specialize to the case $R = \mathcal{R}$ or $\mathcal{R}^{\mathrm{lw}}$ and study the properties of some relevant modules, mainly following [KL23, §2]. Recall that $\mathcal{R}$ is a complete Noetherian regular local domain of dimension 2, by Theorem 3.2.5 and Assumption 6.0.1.

Recall also that $\mathcal{R}^{\mathrm{lw}} = \mathcal{R} \otimes_{\mathbb{Z}_p} \Gamma^{\mathrm{ac}} \cong \mathcal{R}[[\Gamma^{\mathrm{ac}}]]$ is isomorphic to the power series ring $\mathcal{R}[[X]]$ via the map that sends a topological generator γ of Γ^{ac} to $1+X$ (see [NSW13, Proposition 5.2.5]). Therefore, the Krull dimension of $\mathcal{R}^{\mathrm{lw}}$ is 3.

Proposition 6.1.1. *The rings $\mathcal{R}$ and $\mathcal{R}^{\mathrm{lw}}$ are complete noetherian regular local integrally closed UFDs whose height 1 prime ideals are principal.*

Proof. The fact that $\mathcal{R}^{\mathrm{lw}}$ is a complete noetherian regular local ring descends from [Mat89, Theorem 3.3, Exercise 8.6, Theorem 19.5]. Then, by Auslander-Buchsbaum's theorem (see [Mat89, Theorem 20.3]), both $\mathcal{R}$ and $\mathcal{R}^{\mathrm{lw}}$ are UFD. Then, they are also integrally closed (see [Mat89, Example 1]) and every high 1 prime ideal is principal by [Mat89, Theorem 20.1]. □

Remark 6.1.2. The proof of Proposition 6.1.1 goes through with R_f in place of $\mathcal{R}$ and $R_f[[\Gamma^{\mathrm{ac}}]]$ in place of $\mathcal{R}^{\mathrm{lw}}$ (see Subsection 3.2.3 for the definition and properties of these objects), under the assumption that R_f is regular. Since, by Lemma 3.2.7, $\mathcal{R}$ is the integral closure of R_f, we find that the regularity of R_f implies that $R_f = \mathcal{R}$. Therefore, all the work done in literature under the assumption that R_f is regular fits also our hypotheses.

Following [Bou98, §VII.4.4] we now review the theory of pseudo-isomorphisms and characteristic ideals for modules over $\mathcal{R}^{\mathrm{lw}}$.

Definition. Let M be a module over a commutative ring R. We define $\mathrm{Supp}_R(M)$ to be the support of M over R, that is the set of all primes p of R such that the localization $M_{\mathfrak{p}} \neq \{0\}$.

Definition. ([Bou98, §VII.4.4, Definition 2]). A finitely generated $\mathcal{R}^{\mathrm{lw}}$-module M is said to be pseudo-null if $\mathrm{Supp}_{\mathcal{R}^{\mathrm{lw}}}(M)$ contains only prime ideals of height at least 2.

Definition. Let M and N be finitely generated $\mathcal{R}^{\mathrm{lw}}$-modules. We say that M is pseudo-isomorphic to N if there is an exact sequence

$$0 \longrightarrow A \longrightarrow M \longrightarrow N \longrightarrow B \longrightarrow 0$$

where A and B are pseudo-null $\mathcal{R}^{\mathrm{lw}}$-modules. In this case, we write $M \sim N$.

Remark 6.1.3. The relation of pseudo-isomorphism between finitely generated $\mathcal{R}^{\mathrm{lw}}$-modules is not symmetric. Nevertheless, it can be shown that if we restrict to torsion $\mathcal{R}^{\mathrm{lw}}$-modules, then pseudo-isomorphism is an equivalence relation.

Proposition 6.1.4. *Let M be a finitely generated $\mathcal{R}^{\mathrm{lw}}$-module. Then*

$$M \sim (\mathcal{R}^{\mathrm{lw}})^r \oplus \left(\bigoplus_{i=1}^{m} \mathcal{R}^{\mathrm{lw}}/(g_i^{n_i}) \right)$$

for some $r; n_i \geq 0$, $m \geq 1$ and g_i prime (hence irreducible) elements of $\mathcal{R}^{\mathrm{lw}}$.

Proof. By [Bou98, §VII.4.4, Theorem 4] we have that M is pseudo-isomorphic to $F \times T$ where F is a free $\mathcal{R}^{\mathrm{lw}}$-module and T is $\mathcal{R}^{\mathrm{lw}}$-torsion. Then the result follows from the explicit description of T made in [Bou98, §VII.4.4, Theorem 5] together with the fact that all primes of height 1 of $\mathcal{R}^{\mathrm{lw}}$ are principal (see Proposition 6.1.1). □

The elements $g_i^{n_i}$ of Proposition 6.1.4 are unique up to multiplication by units, as stated in [Bou98, §VII.4.4, Theorem 5], and the number r is called the $\mathcal{R}^{\mathrm{lw}}$-rank of M. Therefore, we can make the following definition.

Definition. Let M be a finitely generated $\mathcal{R}^{\mathrm{lw}}$-module and keep the notation of Proposition 6.1.4. Define the characteristic ideal $\mathrm{char}_{\mathcal{R}^{\mathrm{lw}}}(M)$ of M to be 0 if $r \neq 0$ and

$$\mathrm{char}_{\mathcal{R}^{\mathrm{lw}}}(M) = \left(\prod_{i=1}^{m} g_i^{n_i}\right) \subseteq \mathcal{R}^{\mathrm{lw}}$$

otherwise.

6.1.3 Iwasawa Selmer modules

In this subsection we introduce the objects that appear in the statement of the Iwasawa main conjecture.

Definition. Define

$$\mathbf{A}^{\dagger} := \quad (\mathbf{T}^{\dagger}) = \mathbf{T}^{\dagger} \otimes_{\mathcal{R}} \mathcal{R}^{\vee} \quad \text{and} \quad \mathbf{A}^{\mathrm{lw}} := \quad (\mathbf{T}^{\mathrm{lw}}) = \mathbf{T}^{\mathrm{lw}} \otimes_{\mathcal{R}^{\mathrm{lw}}} (\mathcal{R}^{\mathrm{lw}})^{\vee};$$

Remark 6.1.5. These definitions follow [KL23]. As noticed in [Nek06, §0.4], the operator on $\mathcal{R}$ and $\mathcal{R}^{\mathrm{lw}}$-modules is the correct generalization of the operator $(-) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ on finite free $\mathbb{Z}_p$-modules. This last operator is frequently used to define A-objects starting from representations attached to elliptic curves or modular forms (see e.g. [How04b], [LV19]).

As remarked in [KL23, §2.4], there is an isomorphism

$$(\mathcal{R}^{\mathrm{lw}})^{\vee} \cong \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}^{\mathrm{lw}}; \mathcal{R}^{\vee});$$

where we use the standard $\mathcal{R}^{\mathrm{lw}}$-action on $\mathrm{Hom}_{\mathcal{R}}(\mathcal{R}^{\mathrm{lw}}; \mathcal{R}^{\vee})$ induced by the relation $(\ \cdot\ )(x) = (\ ^{-1}x)$ for $\in {}^{\mathrm{ac}}$. We can hence endow $\mathbf{A}^{\mathrm{lw}}$ with a natural action of G_K. As explained in [KL23, §2.4] we have an isomorphism of $\mathcal{R}^{\mathrm{lw}}$-modules

$$\mathbf{A}^{\mathrm{lw}} \cong \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}^{\mathrm{lw}}; \mathbf{A}^{\dagger});$$

Let v be a place of K dividing p. Applying the operator to the filtrations of Proposition 3.3.7 and Lemma 4.2.3 we obtain exact sequences of $\mathcal{R}[[G_{K_v}]]$-modules

$$0 \longrightarrow F_v^{+}(\mathbf{A}) \longrightarrow \mathbf{A} \longrightarrow F_v^{-}(\mathbf{A}) \longrightarrow 0$$

for $\mathbf{A}$ equal to $\mathbf{A}^{\dagger}$ and $\mathbf{A}^{\mathrm{lw}}$ respectively. Therefore, we can define the (strict) Greenberg local conditions on $\mathbf{A}^{\dagger}$ and on $\mathbf{A}^{\mathrm{lw}}$ exactly as done in Definition 4.2.5 and the (strict) Greenberg Selmer modules $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K; \mathbf{A}^{\dagger})$ and $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K; \mathbf{A}^{\mathrm{lw}})$.

Lemma 6.1.6. *Let be the profinite generator of* $^{\mathrm{ac}}$ *fixed in Definition 4.1.1. There are -modules isomorphisms*

(a) $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}}) \cong \varprojlim_{m;s;t} \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;T_{m;s;t}) = \varprojlim_{t} \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K_t;\mathbf{T}^{\dagger})$, *where the last limit is taken with respect to corestriction maps in cohomology.*

(b) $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}}) \cong \varinjlim_{t} \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}}[\ p^t - 1]) = \varinjlim_{t} \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K_t;\mathbf{A}^{\dagger})$, *where the last limit is taken with respect to restriction maps in cohomology.*

Proof. The proof goes through exactly as in [KL23, Lemma 2.8], applying limits, Lemma 4.1.16 and taking track of the local conditions defining the appropriate Selmer groups. □

If M is either $\mathbf{T}^{\dagger}$, $\mathbf{T}^{\mathrm{lw}}$, $\mathbf{A}^{\dagger}$ or $\mathbf{A}^{\mathrm{lw}}$ and $L/\mathbb{Q}$ is a finite extension of fields, one has also a family of extended Selmer groups $\text{Ш}^i_f(L;M)$ defined by Nekovář [Nek06] using similar local conditions to those defining $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}$, but with the local conditions imposed to the level of cochain complexes rather than on cohomology. As noticed in [KL23, (6), (7)] and [How07, (21)] (see also (6.3)), Assumption 5.4.7 implies that there are isomorphisms

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K_t;\mathbf{A}^{\dagger}) \cong \text{Ш}^1_f(K_t;\mathbf{A}^{\dagger}) \quad \text{and} \quad \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K_t;\mathbf{T}^{\dagger}) \cong \text{Ш}^1_f(K_t;\mathbf{T}^{\dagger})$$

for every $t \geq 1$ and, taking direct (resp. inverse) limits with respect to the canonical restriction (resp. corestriction) maps,

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}}) \cong \varinjlim_{t} \text{Ш}^1_f(K_t;\mathbf{A}^{\dagger}) \quad \text{and} \quad \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}}) \cong \varprojlim_{t} \text{Ш}^1_f(K_t;\mathbf{T}^{\dagger}): \quad (6.2)$$

Remark 6.1.7. The Selmer groups appearing in the equation (6.2) are sometimes called Iwasawa Selmer modules (cfr. [How07, §3.3], [Büy14, §5] and [LV11, §10.3]).

Proposition 6.1.8. *The modules* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\dagger})$ *and* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})$ *are* $\mathcal{R}$ *and* $\mathcal{R}^{\mathrm{lw}}$*-torsion-free respectively.*

Proof. See [Büy16, Remark 4.5], [Fou13, Proposition 6.2, (ii)] or [CW22, Lemma 3.3]. If follows from the discussion of [Per00, §1.3.3]. □

Proposition 6.1.9. *The modules* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})$ *and* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}})^{\vee}$ *have the same* $\mathcal{R}^{\mathrm{lw}}$*-rank.*

Proof. See [CW22, Lemma 3.2]. □

6.1.4 The Iwasawa main conjecture

Recall that, thanks to Theorem 5.4.14, there is a universal Kolyvagin system in $\boldsymbol{\kappa} \in \overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}};\mathcal{F}_{\mathrm{Gr}};\mathcal{P})$ such that $\boldsymbol{\kappa}_1 = \ _{\infty} \in \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})$. We are now ready to state our version of the anticyclotomic Iwasawa main conjecture for the representation $\mathbf{T}^{\dagger}$ (see [How07, Conjecture 3.3.1], [LV11, Conjecture 10.8] and [Fou13, (1.1.2)]).

Conjecture 6.1.10. Assume that $\ _{\infty} \neq 0$. Then the modules $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})$ and $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}})^{\vee}$ have $\mathcal{R}^{\mathrm{lw}}$-rank 1 and

$$\mathrm{char}_{\mathcal{R}^{\mathrm{lw}}}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{lw}})/(\ _{\infty})\right)^2 = \mathrm{char}_{\mathcal{R}^{\mathrm{lw}}}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{lw}})^{\vee}_{\mathrm{tors}}\right)$$

Remark 6.1.11. A few comments about this conjecture:

(i) A conjecture of this form for Hida families was first stated in [How07, Conjecture 3.3.1] as an extension of the Heegner point main conjecture for elliptic curves formulated by Perrin-Riou in [Per87]. It is usually stated using Nekovář's extended Selmer groups, but we will see in the next chapter that our formulation is equivalent to the classical one.

(ii) Howard's conjecture was generalized to the quaternionic setting in [LV11, Conjecture 10.8] and [Fou13, (1.1.2)]. It has been proven by Castella and Wan in [CW22, Theorem 5.5] with a slightly different set of hypotheses than ours.

(iii) The assumption that $\kappa_\infty \neq 0$ is a counterpart of [LV11, Conjecture 10.3]. Fouquet noticed after [Fou13, Theorem 6.3] that it should hold in general, thanks to some results of Cornut and Vatsal. Castella and Wan, at the end of [CW22, §4], claim that the class κ_∞ is not zero thanks to a generalization of the arguments in [CV07].

6.2 Kolyvagin systems and the Iwasawa main conjecture

The main goal of this section is to show that the existence of a nontrivial Kolyvagin system yields a proof of one divisibility of Conjecture 6.1.10. The arguments are quite standard and we mainly follow [Fou13, §5-6].

6.2.1 Specializations

In Subsection 3.2.4 we defined arithmetic specializations for finite $\mathcal{O}_F$-algebras. We generalize now this concept with the following definition.

Definition. Let A be a complete local Noetherian $\mathcal{O}_F$-algebra.

(i) An $\mathcal{O}_F$-algebra morphism $\mathfrak{s}$ from A to a complete local Noetherian domain S with finite residue field of characteristic p is called an S-specialization of A.

(ii) If T is an A module, denote by $T_\mathfrak{s} := T \otimes_\mathfrak{s} S$ the specialization of T associated with the S-specialization $\mathfrak{s}$.

If $\mathfrak{s}$ is an S-specialization of $\mathcal{R}^{\mathrm{lw}}$, the Greenberg local conditions on $\mathbf{T}^{\mathrm{lw}}$ induce local conditions on $\mathbf{T}^{\mathrm{lw}}_\mathfrak{s}$ (to be denoted in the same way) and a canonical map

$$\mathfrak{s} : \overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}}; \mathcal{F}_{\mathrm{Gr}}; \mathcal{P}') \longrightarrow \overline{\mathbf{KS}}(\mathbf{T}^{\mathrm{lw}}_\mathfrak{s}; \mathcal{F}_{\mathrm{Gr}}; \mathcal{P}')$$

induced by the natural map $H^1(K_v; \mathbf{T}^{\mathrm{lw}}) \otimes_\mathfrak{s} S \to H^1(K_v; \mathbf{T}^{\mathrm{lw}} \otimes_\mathfrak{s} S)$, as noticed in [MR04, Remark 3.1.4] and [How07, Remark 1.2.4]. From now on we will denote $\mathbf{T}^{\mathrm{lw}}_\mathfrak{s}$ with $T_\mathfrak{s}$.

Definition. Let $\mathfrak{s} : \mathcal{R}^{\mathrm{lw}} \to S$ be a specialization of $\mathcal{R}$ to a discrete valuation ring S finite over $\mathcal{O}_F$. Define $V_\mathfrak{s}$, $A_\mathfrak{s}$, $F^\pm_v(T_\mathfrak{s})$, $F^\pm_v(V_\mathfrak{s})$ and $F^\pm_v(A_\mathfrak{s})$ to be $T_\mathfrak{s} \otimes_S \mathrm{Frac}(S)$, $T_\mathfrak{s} \otimes_S (\mathrm{Frac}(S)/S)$, $F^\pm_v(\mathbf{T}^{\mathrm{lw}}) \otimes_\mathfrak{s} S$, $F^\pm_v(T_\mathfrak{s}) \otimes_S \mathrm{Frac}(S)$ and $F^\pm_v(T_\mathfrak{s}) \otimes_S (\mathrm{Frac}(S)/S)$ respectively.

Definition. A specialization $T_\mathfrak{s}$ of $\mathbf{T}^{\mathrm{lw}}$ is said to be exceptional if there exists a finite extension L of $\mathbb{Q}_p$ such that $H^0(L; F^-_v(T_\mathfrak{s})) \neq 0$.

The natural maps

$$: T_s \to V_s \quad \text{and} \quad : V_s \to A_s$$

induce maps $: H^1(L;T_s) \to H^1(L;V_s)$ and $: H^1(L;V_s) \to H^1(L;A_s)$ for every finite extension L of K.

Definition. ([Fou13, Definition 5.20]). Let L be a finite extension of K and s be a non-exceptional specialization of $\mathcal{R}^{\mathrm{lw}}$ to a discrete valuation ring S finite over $\mathcal{O}_F$. Define the Bloch–Kato Selmer structure $\mathcal{F}_{\mathrm{BK}}$ on T_s by setting local conditions as

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(L_v;T_s) = \begin{cases} {}^{-1}(H^1_{\mathrm{ur}}(L_v;V_s)) & \text{if } v \mid N \\ {}^{-1}(H^1(L_v;F_v^+(V_s))) & \text{if } v \mid p \\ H^1_{\mathrm{f}}(L_v;T_s) & \text{if } v \nmid Np. \end{cases}$$

Similarly, we define the Bloch–Kato Selmer structure $\mathcal{F}_{\mathrm{BK}}$ on A_s by setting local conditions as

$$H^1_{\mathcal{F}_{\mathrm{BK}}}(L_v;A_s) = \begin{cases} (H^1_{\mathrm{ur}}(L_v;V_s)) & \text{if } v \mid N \\ (H^1(L_v;F_v^+(V_s))) & \text{if } v \mid p \\ H^1_{\mathrm{f}}(L_v;A_s) & \text{if } v \nmid Np. \end{cases}$$

The Bloch–Kato Selmer module for the specialization T_s is then

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(L;T_s) := \ker\Big(H^1(L;T_s) \longrightarrow \prod_v H^1(L_v;T_s)/H^1_{\mathcal{F}_{\mathrm{BK}}}(L_v;T_s)\Big)$$

where v runs over all places of L. In the same way we can define the Bloch–Kato Selmer module for A_s. In next subsection we see how to relate the Bloch–Kato Selmer group with the Greenberg Selmer group. We remark here that there are inequalities

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L;T_s) \subseteq \mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(L;T_s) \quad \text{and} \quad \mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(L;A_s) \supseteq \mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(L;A_s)$$

that descend directly from the definitions and [Rub00, Lemma 3.5]. Also, one can define the S-module of universal Kolyvagin systems $\overline{\mathbf{KS}}(T_s;\mathcal{F}_{\mathrm{BK}};\mathcal{P}')$ with respect to the Bloch–Kato local conditions following what was done in Chapter 4 using Greenberg local conditions. The inclusion $\mathcal{F}_{\mathrm{Gr}} \subseteq \mathcal{F}_{\mathrm{BK}}$ in the cohomology of T_s yields an injective map

$$\overline{\mathbf{KS}}(T_s;\mathcal{F}_{\mathrm{Gr}};\mathcal{P}') \longrightarrow \overline{\mathbf{KS}}(T_s;\mathcal{F}_{\mathrm{BK}};\mathcal{P}');$$

as noticed in [MR04, Remark 3.1.4].

Now we state the first fundamental step in the proof of the Iwasawa main conjecture. For every S-module M we denote by $\ell_S(M)$ the lenght of M as an S-module

Theorem 6.2.1. *Let $s : \mathcal{R}^{\mathrm{lw}} \to S$ be a non-exceptional specialization with values in a discrete valuation ring S flat over $\mathbb{Z}_p$, and let $\in \overline{\mathbf{KS}}(T_s;\mathcal{F}_{\mathrm{BK}};\mathcal{P}')$ with the property that $_1 \neq 0$. Then $\mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(K;T_s)$ is free of rank 1 over S and there exists a torsion module M finitely generated over S with*

$$\ell_S(M) \leq \ell_S\big(\mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(K;T_s)/(\ _1)\big)$$

such that

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{BK}}}(K;A_s) \cong \mathrm{Frac}(S)/S \oplus M \oplus M.$$

Proof. The arguments in the proof of [Fou13, Corollary 5.21] carry over verbatim to our setting. They consist in checking that the module T_s and the condition $\mathcal{F}_{BK}$ satisfy the conditions (H1)-(H5) of [How04a, §2.2] (or, equivalently, conditions (H0)-(H5) of [How04b, §1.3]) in order to apply [How04a, Theorem 2.2.2] (or, equivalently, [How04b, Theorem 1.6.1]). □

We now apply this result to the Kolyvagin system κ of Theorem 5.4.14.

Corollary 6.2.2. *In the setting of Theorem 6.2.1, if the image $\kappa_{\infty;S}$ of κ_∞ under the map induced by s is not zero then $\mathrm{Sel}_{\mathcal{F}_{BK}}(K;T_s)$ is free of rank 1 over S and there exists a torsion module M finitely generated over S with*

$$\lambda_S(M) \le \lambda_S\big(\mathrm{Sel}_{\mathcal{F}_{BK}}(K;T_s)/(\kappa_{\infty;S})\big)$$

such that

$$\mathrm{Sel}_{\mathcal{F}_{BK}}(K;A_s) \cong \mathrm{Frac}(S)/S \oplus M \oplus M.$$

6.2.2 Relations between Bloch–Kato and Greenberg Selmer groups

In this subsection we restrict to consider specializations $s : \mathcal{R}^{lw} \to S$ where S is a discrete valuation ring flat over $\mathbb{Z}_p$ and finite over $\mathrm{Im}(s)$. In concrete examples, S is usually the integral closure of $\mathrm{Im}(s)$.

Lemma 6.2.3. *Let G be a profinite group, T be an $\mathcal{R}^{lw}[G]$-module and call T_s the specialization via s. Then the residual G-representation $\overline{T}_s$ is equivalent to $\overline{T}$ up to a finite base change.*

Proof. With the obvious notations, there is an isomorphism

$$T_s/\mathfrak{m}_S T_s \cong T/\mathfrak{m}_{\mathcal{R}^{lw}} T \otimes_{F_{\mathcal{R}^{lw}}} F_S,$$

where the residue field F_S of S is a finite extension of $F_{\mathcal{R}^{lw}}$ by assumption. □

Corollary 6.2.4. *With the notation as above, if T is $\mathcal{R}^{lw}$-torsion-free and $H^0(G;\overline{T}) = 0$ then $H^0(G;T_s) = 0$.*

Proof. Combine Lemma 6.2.3 with Proposition 4.1.10. □

As a consequence of Assumptions 5.2.3 and 5.4.7 we obtain the following result.

Proposition 6.2.5. *Let $s : \mathcal{R}^{lw} \to S$ be a specialization where S is a discrete valuation ring flat over $\mathbb{Z}_p$ and finite over $\mathrm{Im}(s)$. Then*

$$\mathrm{Sel}_{\mathcal{F}_{BK}}(K;T_s) = \mathrm{Sel}_{\mathcal{F}_{Gr}}(K;T_s) \quad \text{and} \quad \mathrm{Sel}_{\mathcal{F}_{BK}}(K;A_s) = \mathrm{Sel}_{\mathcal{F}_{Gr}}(K;A_s).$$

Proof. We check that the local conditions $\mathcal{F}_{Gr}$ and $\mathcal{F}_{BK}$ coincide at every place v of K. Let X denote T_s or A_s.

If $v \nmid p$, [Rub00, Lemma 3.5, (iii) and (iv)] together Proposition 5.2.4 imply that $H^1_{\mathcal{F}_{Gr}}(K_v;X) = H^1_{\mathcal{F}_{BK}}(K_v;X)$.

Let now $v \mid p$. There is a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(K_v;F_v^+(T_s)) & \longrightarrow & H^1(K_v;T_s) & \longrightarrow & H^1(K_v;F_v^-(T_s)) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(K_v;F_v^+(V_s)) & \longrightarrow & H^1(K_v;V_s) & \longrightarrow & H^1(K_v;F_v^-(V_s)) & \longrightarrow & 0.
\end{array}$$

The module $H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v;T_s)$ is the kernel of the third upper horizontal arrow, whereas $H^1_{\mathcal{F}_{\mathrm{BK}}}(K_v;T_s)$ is the kernel of the map from $H^1(K_v;T_s)$ to $H^1(K_v;F_v^-(V_s))$. In order to show the desired equality, it is enough to prove that the right-most vertical arrow is injective. Its kernel coincides with $H^0(K_v;F_v^-(A_s))$ and this group is trivial combining Assumption 5.4.7 together with Corollary 6.2.4, recalling that $F_v^-(A_s) = F_v^-(T_s)\otimes_S \mathrm{Frac}(S)/S$.

Consider now the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(K_v;F_v^+(V_s)) & \longrightarrow & H^1(K_v;V_s) & \longrightarrow & H^1(K_v;F_v^-(V_s)) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1(K_v;F_v^+(A_s)) & \longrightarrow & H^1(K_v;A_s) & \longrightarrow & H^1(K_v;F_v^-(A_s)) & \longrightarrow & 0. \end{array}$$

The module $H^1_{\mathcal{F}_{\mathrm{Gr}}}(K_v;A_s)$ is the image of the second bottom horizontal arrow, whereas $H^1_{\mathcal{F}_{\mathrm{BK}}}(K_v;A_s)$ coincides with the image of $H^1(K_v;F_v^+(V_s))$ in $H^1(K_v;A_s)$. In order to show that they are equal, it is enough to prove that the left-most vertical arrow is surjective. Its cokernel coincides with $H^2(K_v;F_v^+(T_s))$ and this group is trivial combining Corollary 6.2.4 with Assumption 5.4.7 (and local duality), exactly as done at the beginning of the proof of Proposition 5.4.9. □

Combining the exact sequence of [Fou13, (5.1.4)] with Assumption 5.4.7 and Corollary 6.2.4, we have isomorphisms

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;X) \cong \text{Ш}^1_f(K;X) \tag{6.3}$$

where $\text{Ш}^1_f(K;X)$ is Nekovář's extended Selmer group and X coincides with one of $\mathbf{T}^{\mathrm{Iw}}$, $\mathbf{T}^\dagger$ or T_s.

6.2.3 Main result

The results of the previous subsections enable us to apply the machinery of [Fou13, §6.3], and to obtain the following result.

Theorem 6.2.6. *Assume that* $\varepsilon_1 = \quad_\infty \neq 0$. *Then the modules* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{Iw}})$ *and* $\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{Iw}})^\vee$ *have* $\mathcal{R}^{\mathrm{Iw}}$*-rank* 1 *and*

$$\mathrm{char}_{\mathcal{R}^{\mathrm{Iw}}}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{Iw}})^\vee_{\mathrm{tors}}\right) \supseteq \mathrm{char}_{\mathcal{R}^{\mathrm{Iw}}}\left(\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{T}^{\mathrm{Iw}})/(\quad_\infty)\right)^2.$$

Proof. We first recall that equation (6.2) yields an isomorphism

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{Iw}}) \cong \text{Ш}^1_f(K;\mathbf{A}^{\mathrm{Iw}})$$

where $\text{Ш}^1_f(K;\mathbf{A}^{\mathrm{Iw}}) = \varinjlim_t \text{Ш}^1_f(K_t;\mathbf{A}^\dagger)$ is Nekovář's extended Selmer group (see [Nek06, §0.11-0.13]). As noticed in [How07, Remark 3.3.3], the global duality of [Nek06, §0.13] yields an isomorphism

$$\mathrm{Sel}_{\mathcal{F}_{\mathrm{Gr}}}(K;\mathbf{A}^{\mathrm{Iw}})^\vee = \text{Ш}^2_f(K;\mathbf{T}^{\mathrm{Iw}})$$

where, again, $\text{Ш}^2_f(K;\mathbf{T}^{\mathrm{Iw}})$ is Nekovář's extended Selmer group. Using also the isomorphism of (6.3), we can translate the statement of the theorem as

$$\mathrm{char}_{\mathcal{R}^{\mathrm{Iw}}}\left(\text{Ш}^2_f(K;\mathbf{T}^{\mathrm{Iw}})_{\mathrm{tors}}\right) \supseteq \mathrm{char}_{\mathcal{R}^{\mathrm{Iw}}}\left(\text{Ш}^1_f(K;\mathbf{T}^{\mathrm{Iw}})/(\quad_\infty)\right)^2.$$

Let $s : \mathcal{R}^{\mathrm{lw}} \to S$ be a specialization to a discrete valuation ring flat over $\mathbb{Z}_p$ and finite over $\mathrm{Im}(s)$. Combining Corollary 6.2.2 with Proposition 6.2.5, if the image $\kappa_{\infty;S}$ of κ_∞ via the map induced by s is non-zero, there is an inequality of lengths

$$\ell_S(H^2_f(K;T_s)_{\mathrm{tors}}) \leq 2\ell_S(H^1_f(K;T_s)/(\kappa_{\infty;S})). \tag{6.4}$$

Then, the arguments of [Fou13, §6.3] carry on verbatim, with the easier equation (6.4) in place of [Fou13, (6.3.2)]. Our claim then follows from the same arguments that occur in the proof of [Fou13, Theorem 6.3]. See also [CW22, Theorem 5.5]. □

Remark 6.2.7. As noticed in point (iii) of Remark 6.1.11, under our assumptions the class κ_∞ should always be nontrivial.

Appendix A

Some Galois cohomology

A.1 (Semi-)local Galois cohomology

The aim of this section is to study the commutativity properties of restriction and corestriction in Galois cohomology, that are intensively used in Chapter 5. We will mainly rely on [NSW13, §1.5].

For this section, let L/K be a Galois extension of number fields, let v be a prime of K and fix a decomposition group D_v of v in G_K. Let $w_1;\dots;w_n$ be the primes of L above v, where w_1 has fixed decomposition group $\mathrm{D}_{w_1} = \mathrm{D}_v \cap G_L$ in G_L. For any element $\in \mathrm{Gal}(L/K)$ fix a lifting $\sim$ to G_K. Let also $_i \in \mathrm{Gal}(F/K)$ such that $w_i = w_1 \circ \ _i$ and set $\mathrm{D}_{w_i} := \sim_i^{-1} \mathrm{D}_{w_1} \sim_i$. Then, D_{w_i} is a fixed decomposition group for w_i. Let I_{w_i} be the inertia inside D_{w_i} and fix a G_K-module T.

Proposition A.1.1. *(a) If v is split in L then $\mathrm{D}_{w_1} = \mathrm{D}_v$, $\mathrm{I}_{w_1} = \mathrm{I}_v$ and there is a commutative diagram*

$$\begin{array}{ccccc} H^1(L;T) & \xrightarrow{\oplus_i \mathrm{res}_{w_i}} & \oplus_{i=1}^n H^1(\mathrm{D}_{w_i};T) & \xrightarrow{\oplus_i \mathrm{res}} & \oplus_{i=1}^n H^1(\mathrm{I}_{w_i};T)^{\mathrm{D}_{w_i}/\mathrm{I}_{w_i}} \\ \downarrow{\scriptstyle \mathrm{cor}_{L/K}} & & \downarrow{\scriptstyle \sum_i \sim_i} & & \downarrow{\scriptstyle \sum_i \sim_i} \\ H^1(K;T) & \xrightarrow{\mathrm{res}_v} & H^1(\mathrm{D}_v;T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_v;T)^{\mathrm{D}_v/\mathrm{I}_v}. \end{array}$$

(b) If v is totally ramified in L there is a commutative diagram

$$\begin{array}{ccccc} H^1(L;T) & \xrightarrow{\mathrm{res}_{w_1}} & H^1(\mathrm{D}_{w_1};T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_{w_1};T)^{\mathrm{D}_{w_1}/\mathrm{I}_{w_1}} \\ \downarrow{\scriptstyle \mathrm{cor}_{L/K}} & & \downarrow{\scriptstyle \mathrm{cor}_{\mathrm{D}_{w_1}/\mathrm{D}_v}} & & \downarrow{\scriptstyle \mathrm{cor}_{\mathrm{I}_{w_1}/\mathrm{I}_v}} \\ H^1(K;T) & \xrightarrow{\mathrm{res}_v} & H^1(\mathrm{D}_v;T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_v;T)^{\mathrm{D}_v/\mathrm{I}_v}. \end{array}$$

(c) If v is inert in L then $\mathrm{I}_{w_1} = \mathrm{I}_v$ and there is a commutative diagram

$$\begin{array}{ccccc} H^1(L;T) & \xrightarrow{\mathrm{res}_{w_1}} & H^1(\mathrm{D}_{w_1};T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_{w_1};T)^{\mathrm{D}_{w_1}/\mathrm{I}_{w_1}} \\ \downarrow{\scriptstyle \mathrm{cor}_{L/K}} & & \downarrow{\scriptstyle \mathrm{cor}_{\mathrm{D}_{w_1}/\mathrm{D}_v}} & & \downarrow{\scriptstyle \mathrm{Tr}_{\mathrm{D}_v/\mathrm{D}_{w_1}}} \\ H^1(K;T) & \xrightarrow{\mathrm{res}_v} & H^1(\mathrm{D}_v;T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_v;T)^{\mathrm{D}_v/\mathrm{I}_v}. \end{array}$$

Proof. Point (a) descends directly from [NSW13, Proposition 1.5.6] and [NSW13, Proposition 1.5.4]. Point (b) is a consequence of [NSW13, Corollary 1.5.8]. Point (c) again descends from [NSW13, Proposition 1.5.6]. □

We don't usually need Proposition A.1.1 in its full power, so we state here an easier-to-remember corollary.

Corollary A.1.2. *In the setting of this section, there are two morphisms and that make the following diagram*

$$\begin{array}{ccccc} H^1(L;T) & \xrightarrow{\oplus_i \mathrm{res}_{w_i}} & \oplus_{i=1}^n H^1(\mathrm{D}_{w_i};T) & \xrightarrow{\mathrm{res}} & \oplus_{i=1}^n H^1(\mathrm{I}_{w_i};T)^{\mathrm{D}_{w_i}/\mathrm{I}_{w_i}} \\ \downarrow{\scriptstyle \mathrm{cor}_{L/K}} & & \downarrow & & \downarrow \\ H^1(K;T) & \xrightarrow{\mathrm{res}_v} & H^1(\mathrm{D}_v;T) & \xrightarrow{\mathrm{res}} & H^1(\mathrm{I}_v;T)^{\mathrm{D}_v/\mathrm{I}_v} \end{array}$$

commutative.

Proof. Just decompose the extension L/K into a chain of split, inert and totally ramified extensions and apply Proposition A.1.1. □

A.2 Tame ramification and cohomology

In this section we review the structure of the maximal tamely ramified extension of a local field and investigate its role when computing the first cohomology group of some relevant Galois representations. Let ℓ be a prime of $\mathbb{Q}$ and L be a finite extension of $\mathbb{Q}_\ell$.

Definition. The maximal tamely ramified extension L^t of L is the union of all finite tamely ramified extensions of L, i.e. the union of all finite extensions of L whose ramification index is coprime with ℓ.

Lemma A.2.1. *With the notation as above, we have that*

(i) The profinite group $\mathrm{Gal}(\mathbb{Q}_\ell/L^t)$ *is a pro-*ℓ*-group.*

(ii) $\mathrm{Gal}(L^t/L^{\mathrm{ur}}) \cong \prod_{q\neq\ell} \mathbb{Z}_q$.

(iii) $\mathrm{Gal}(L^t/L) \cong \mathrm{Gal}(L^t/L^{\mathrm{ur}}) \rtimes \mathrm{Gal}(L^{\mathrm{ur}}/L) \cong \prod_{q\neq\ell} \mathbb{Z}_q \rtimes \hat{\mathbb{Z}}$, *where the action of* $\mathrm{Gal}(L^{\mathrm{ur}}/L) \cong \hat{\mathbb{Z}}$ *on* $\mathrm{Gal}(L^t/L^{\mathrm{ur}}) \cong \prod_{q\neq\ell} \mathbb{Z}_q$, *defined by the relation* $\cdot := {}^{-1}$ *for any* $\in \mathrm{Gal}(L^{\mathrm{ur}}/L)$ *and* $\in \mathrm{Gal}(L^t/L^{\mathrm{ur}})$, *is via the product of the* q*-adic cyclotomic characters.*

Proof. Point (i) is [Cla10, Theorem 2.64]. Point (ii) and (iii) descend from [Cla10, Theorem 2.67]. □

Aiming to include the action of the semidirect product in the notation, we will write

$$\mathrm{Gal}(L^t/L) \cong \prod_{q\neq\ell} \mathbb{Z}_q(1) \rtimes \hat{\mathbb{Z}}$$

in order to say that the action of $\hat{\mathbb{Z}}$ on $\prod_{q\neq\ell} \mathbb{Z}_q(1)$ is via the product of the q-adic cyclotomic characters prime to ℓ.

Let ℓ^d be the cardinality of the residue field of L. The procyclic group $\hat{\mathbb{Z}} \cong \mathrm{Gal}(L^{\mathrm{ur}}/L)$ is topologically generated by Fr_L, and the q-adic cyclotomic character computed at Fr_L equals ℓ^d, for any $q \neq \ell$. This implies that, if is a topological generator for $\mathrm{Gal}(L^t/L^{\mathrm{ur}})$, the action of $\mathrm{Gal}(L^{\mathrm{ur}}/L)$ on $\mathrm{Gal}(L^t/L^{\mathrm{ur}})$ is characterized by the relation

$$\mathrm{Fr}_L \quad \mathrm{Fr}_L^{-1} = \quad {}^{\ell^d}.$$

Lemma A.2.2. *Let p be a prime different from ℓ and let T be an unramified $\mathbb{Z}_p[G_L]$-module with the property that ℓ^d is not an eigenvalue for the action of Fr_L on T. Then the inflation map*

$$\inf : H^1(L^{\mathrm{ur}}/L;T) \longrightarrow H^1(L;T)$$

is an isomorphism.

Proof. Since T is unramified, we have that

$$H^1(L^t;T) = \mathrm{Hom}(\mathrm{Gal}(L/L^t);T) = \{0\};$$

the last equality coming from the fact that $\mathrm{Gal}(L/L^t)$ is a pro-ℓ-group by Lemma A.2.1 and T is a $\mathbb{Z}_p$-module. This implies that

$$\inf : H^1(L^t/L;T) \longrightarrow H^1(L;T):$$

is an isomorphism. The inflation-restriction sequence yields the exact sequence

$$\{0\} \longrightarrow H^1(L^{\mathrm{ur}}/L;T) \xrightarrow{\inf} H^1(L^t/L;T) \xrightarrow{\mathrm{res}} H^1(L^t/L^{\mathrm{ur}};T_s)^{\mathrm{Gal}(L^{\mathrm{ur}}/L)} :$$

Again, the unramifiedness of T yields

$$H^1(L^t/L^{\mathrm{ur}};T) = \mathrm{Hom}(\mathrm{Gal}(L^t/L^{\mathrm{ur}});T):$$

Looking just at the group structure, we have that

$$\mathrm{Hom}(\mathrm{Gal}(L^t/L^{\mathrm{ur}});T) \cong \mathrm{Hom}(\prod_{q\neq\ell} \mathbb{Z}_q;T) \cong \mathrm{Hom}(\mathbb{Z}_p;T) \cong T$$

as groups, where the isomorphism is induced by the evaluation at a fixed generator σ of $\mathrm{Gal}(L^t/L^{\mathrm{ur}})$. Let now τ be an element of $\mathrm{Gal}(L^{\mathrm{ur}}/L)$, $\tilde{\tau}$ be a lifting of τ to $\mathrm{Gal}(L^t/L)$ and $\varphi \in \mathrm{Hom}(\mathrm{Gal}(L^t/L^{\mathrm{ur}});T)$. Then, by Lemma A.2.1 we have that

$$(\tau\cdot\varphi)(\sigma) = \tilde{\tau}\,(\varphi(\tilde{\tau}^{-1}\sigma\tilde{\tau})) = \tilde{\tau}\left(\varphi\left(\chi_p^{-1}(\tau)\sigma\right)\right) = \chi_p^{-1}(\tau)\,\tilde{\tau}\,(\varphi(\sigma))$$

where χ_q is the q-adic cyclotomic character. This implies that we have an isomorphism

$$\mathrm{Hom}(\mathrm{Gal}(L^t/L^{\mathrm{ur}});T) \cong T(-1)$$

as $\mathrm{Gal}(L^{\mathrm{ur}}/L)$-modules, where $T(-1)$ is T with the Galois action twisted by the inverse of the p-adic cyclotomic character. We must show that $T(-1)^{\mathrm{Gal}(L^{\mathrm{ur}}/L)} = \{0\}$. Notice that

$$T(-1)^{\mathrm{Gal}(L^{\mathrm{ur}}/L)} = \{t \in T \ : \ (\mathrm{Fr}_L - \ell^d)(t) = 0\};$$

where ℓ^d is the cardinality of the residue field of L. Since ℓ^d is not an eigenvalue for the action of Fr_L on T, we conclude that $T(-1)^{\mathrm{Gal}(L^{\mathrm{ur}}/L)} = \{0\}$. □

A.3 Kolyvagin's corestriction and Nekovář's work

In this section we generalize the ideas of [Nek92, §7-9] to our context. These results are the key for the proof of Theorem 5.4.14. We collect them here because the work is quite long and general.

A.3.1 Kolyvagin's corestriction

Let $M \in \mathbb{Z}_{>0}$, G be a topological group, H be a closed normal subgroup of G such that G/H is cyclic of order M. Fix a generator $\quad$ of G/H and let A be a G-module killed by M. Let $[x] \in H^1(H;A)$ be a cohomology class with $\mathrm{cor}_G^H[x] = 0 \in H^1(G;A)$.

Call $D := \sum_{i=1}^{M-1} i \quad ^i$. Choosing a cocycle x representing $[x]$, we find that $\mathrm{cor}_G^H[x]$ can be represented by the cocycle

$$\begin{aligned} \mathrm{cor}\, x : G &\longrightarrow A \\ h &\longmapsto \sum_{i=0}^{M-1} \sim^i x(\sim^{-i} h \sim^i) \quad \text{for } h \in H \\ \sim &\longmapsto x(\sim^M) \end{aligned}$$

for a fixed lifting $\sim$ of $\quad$ to G. Since $\mathrm{cor}_G^H[x] = 0$, on the cocycle level we also have that

$$\begin{aligned} \mathrm{cor}\, x : G &\longrightarrow A \\ g &\longmapsto (g-1)a \end{aligned} \tag{A.1}$$

for some $a \in A$. Notice that the element a is determined modulo A^G, therefore when $A^G = 0$ we have that a is uniquely determined. Define the cocycle

$$\begin{aligned} Dx : H &\longrightarrow A \\ h &\longmapsto \sum_{i=1}^{M-1} i \sim^i x(\sim^{-i} h \sim^i): \end{aligned}$$

Then Nekovář proved in [Nek92, §7] that the function

$$\begin{aligned} f_x : G &\longrightarrow A \\ h &\longmapsto (Dx)(h) \quad \text{for } h \in H \\ \sim &\longmapsto -\sim a \end{aligned} \tag{A.2}$$

defines a cocycle which satisfies $\mathrm{res}_H^G f_x = Dx$. Moreover, when $A^G = \{0\}$, the class $[f_x] \in H^1(G;A)$ depends only on $[x]$ and satisfies

$$\mathrm{res}_H^G[f_x] = D[x]:$$

A.3.2 Localization of Kolyvagin's corestriction

We set up some more notation, following [Nek92, §9].

(i) Let $\mathbf{G}$ be a profinite group, ℓ and p be two distinct odd prime numbers. Let $H \trianglelefteq G \trianglelefteq \mathbf{G}$ be a chain of normal closed subgroups with $\mathbf{G}/H = \langle \quad \rangle \rtimes \langle c \rangle$ dihedral, where $\langle \quad \rangle$ is cyclic of order M, $\langle c \rangle$ is cyclic of order 2 acting on $\langle \quad \rangle$ by $c \quad c = \quad^{-1}$. Moreover, $G/H = \langle \quad \rangle$ and $\mathbf{G}/G = \langle c \rangle$.

(ii) Let $\mathbf{G}_0$ be a closed subgroup of $\mathbf{G}$ and call $G_0 := \mathbf{G}_0 \cap G$ and $H_0 := G_0 \cap H$. Suppose that G_0/H_0 is cyclic of order M, generated by an element $\quad_0$ and that $\mathbf{G}_0/H_0 = \langle \quad_0 \rangle \rtimes \langle c_0 \rangle$ is dihedral with c_0 element of order 2.

(iii) The group G_0 is equipped with a surjective homomorphism

$$: G_0 \longrightarrow \prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes \hat{\mathbb{Z}};$$

where $\prod_{q\neq \ell} \mathbb{Z}_q(1)$ and $\hat{\mathbb{Z}}$ have fixed generators and respectively, satisfying the relation $^{-1} = ^{d}$ for some integer d prime to p. One also requires to induce surjections

$$G_0 \longrightarrow \prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}}; \quad H_0 \longrightarrow M \prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}};$$

and we also want the generator $_0$ of G_0/H_0 to correspond to modulo M (i.e., is a lift of $_0$ to G_0).

(iv) Let A be a torsion-free module of finite rank over a finite extension S of $\mathbb{Z}_p$ with a continous action of G.

(v) G_0 acts on A through its quotient $\hat{\mathbb{Z}}$, ker( ) has order prime to p as a profinite group and every arrow in the diagram

$$\begin{array}{ccc} H^1(G_0;A) & \xrightarrow{\inf^{-1}} & H^1(\prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}};A) \\ & & \downarrow{\scriptstyle \inf^{-1}} \\ & & H^1(2\hat{\mathbb{Z}};A) \\ & & \uparrow{\scriptstyle \inf^{-1}} \\ H^1(H_0;A) & \xrightarrow{\inf^{-1}} & H^1(M \prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}};A) \end{array}$$

is an isomorphism.

(vi) ^{2} acts as the identity on A/p^sA for some $s \geq 1$ such that $p^s \mid M$.

(vii) Let $y \in H^1(H;A)$ and $x \in H^1(G;A)$ with $\mathrm{cor}_G^H(y) = M_1 x$ with $M_1 \in S$ divisible by p^s.

(viii) $(A/p^sA)^G = 0$.

We now combine all these assumptions in order to find a relation between x and y that has a particular importance for us. First, notice that assumption (v) yields

$$H^1(H_0;A) \cong H^1(G_0;A) \cong H^1(2\hat{\mathbb{Z}};A) \cong A/(^2 - 1)A; \tag{A.3}$$

where the last isomorphism is given by evaluating cocycles at ^{2} (see [Rub00, Lemma B.2.8]). Equation (A.3) is true also with A replaced by any of its finite quotients.

Let now $F \in Z^1(\prod_{q\neq \ell} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}};A)$ be a 1-cocycle. Assumption (v) implies that F is inflated by an 1-cocycle $\bar{F} \in Z^1(2\hat{\mathbb{Z}};A)$, up to summing a coboundary. Hence

$$F(^u\ ^{2v}) = \bar{F}(^{2v}) + (^u\ ^{2v} - 1)b = (1 + ^2 + \cdots + ^{2(v-1)})\bar{F}(^2) + (^{2v} - 1)b$$

for any $u; v \in \mathbb{Z}_{\geq 0}$ and some $b \in A$, where we used the fact that acts trivially on A (see assumption (v)). Calling $a_F := \bar{F}(^2) \in A$, the cohomology class of F corresponds to $[a_F] \in A/(^2 - 1)A$ via the last isomorphism in equation (A.3). A similar argument can be pursued starting from a cocycle $F \in Z^1(M \prod_{q\neq l} \mathbb{Z}_q(1) \rtimes 2\hat{\mathbb{Z}};A)$.

Consider now the following commutative diagram with exact rows

$$\begin{array}{ccccccc} & & & & H^1(G;A/p^sA) & \xrightarrow{\text{res}} & H^1(H;A/p^sA) \\ & & & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} \\ 0 & \longrightarrow & H^1(G_0/H_0;A/p^sA) & \xrightarrow[\text{inf}]{} & H^1(G_0;A/p^sA) & \xrightarrow[\text{res}]{} & H^1(H_0;A/p^sA) \end{array}$$

where $(A/p^sA)^{H_0} = A/p^sA$, since by point (v) and (vi) the action of H_0 is trivial on A/p^sA. Call $x \in H^1(G;A/p^sA)$ and $y \in H^1(H;A/p^sA)$ the elements corresponding respectively to x and y via the natural projection map. Thanks to assumptions (vii) and (viii) the cocycle $f_y \in Z^1(G;A/p^sA)$ defined in equation (A.2) that has the following property

$$\text{res}^G_H([f_y]) = Dy \in H^1(H;A/p^sA);$$

where $D = \sum_{i=1}^{M-1} i \quad ^i$. By assumptions (iii), (v) and (vi), one can prove (exactly as in the first step of the proof of Proposition 5.4.3) that the image of the operator D in $H^1(H;A/p^sA)$ goes to zero when restricted to $H^1(H_0;A/p^sA)$[1], hence $\text{res}^G_{H_0}([f_y])$ is trivial. Following the diagram above, we find an element $y_0 \in H^1(G_0/H_0;A/p^sA) = \text{Hom}(G_0/H_0;A/p^sA)$ such that $\text{inf}^{G_0/H_0}_{G_0} y_0 = \text{res}^G_{G_0}[f_y]$.

We now have to do some computations at the level of cocycles, to be denoted with the same letters as their cohomology class. According to assumption (vii) there is an element $a \in A$ such that

$$(\text{cor}^H_G(y))(g) - M_1 x(g) = (g-1)a$$

for every $g \in G$. When quotienting A by p^sA, the explicit description of the corestriction from the previous section yields that the element a is congruent modulo p^sA to the one defined in equation (A.1), and its class modulo p^sA is uniquely determined. Then, the definition of f_y (see equation (A.2)) implies that, for any lifting $\sim_0$ of $\quad_0$ to G_0 whose projection to $2\hat{\mathbb{Z}}$ is trivial,

$$y_0(\quad_0) = (\text{res}^G_{G_0} f_y)(\sim_0) = f_y(\sim_0) = -\sim_0 a = -a \tag{A.4}$$

since $\sim_0$ acts trivially on A by assumption (v), where a is the reduction of a modulo p^sA. Since $\quad$ is a lifting of $\quad_0$ to G_0, we can choose $\sim_0 = \quad$.

Restricting to $g = g_0 \in H_0$, we get the relation

$$\sum_{i=0}^{M-1} y(\quad^{-i} g_0 \quad^i) - M_1 x(g_0) = (g_0 - 1)a:$$

The isomorphisms in equation (A.3) (coming from assumption (v)) allows us to consider $\text{res}^G_{G_0} x$ and $\text{res}^H_{H_0} y$ coming (via inflation) from cocycles on the abelian quotient $2\hat{\mathbb{Z}}$ of G_0 and H_0, respectively. This implies that the previous relation becomes

$$My(g_0) - M_1 x(g_0) = (g_0 - 1)a:$$

[1] By (A.3) it is enough to prove that $(D\xi)(\phi^2) = 0$ for every cocycle $\xi \in Z^1(H_0, A/p^sA)$. By (iii) and (v), τ is a lift of σ_0 and it acts trivially on A/p^sA. By (A.3), the cocycle ξ is inflated by an element of $Z^1(2\hat{\mathbb{Z}}, A/p^sA)$ and therefore $\tau\xi = \xi$. This implies that $(D\xi)(\phi^2) = \frac{M(M-1)}{2}\xi(\phi^2)$, that is zero in A/p^sA.

Moreover, the computations above yield, for $(g_0) = {}^{u}{}^{2v}$, the following

$$x(g_0) = (1 + {}^{2} + \cdots + {}^{2(v-1)})a_x + ({}^{2v} - 1)b_x$$
$$y(g_0) = (1 + {}^{2} + \cdots + {}^{2(v-1)})a_y + ({}^{2v} - 1)b_y$$

for some $a_x; a_y; b_x; b_y \in A$, where a_x and a_y correspond, modulo $({}^{2}-1)A$, to $\mathrm{res}^{G}_{G_0}(x)$ and $\mathrm{res}^{H}_{H_0}(y)$ respectively via the last isomorphism of equation (A.3). When $v = 1$, putting the last three equations together we obtain

$$M a_y - M_1 a_x = ({}^{2} - 1)(a - M b_y + M_1 b_x) \tag{A.5}$$

on A. We impose the last two assumptions

(ix) $a_y \equiv {}''\ (a_x) \pmod{({}^{2} - 1)A}$ for some ${}'' \in \{\pm 1\}$;

(x) ${}^{2} - \ M_1 \ + d = 0$ on A for some $\ \in \{\pm 1\}$.

Using Assumption (ix), relation (A.5) becomes

$$({}''M \ - M_1)a_x = ({}^{2} - 1)(a - p^{s}(\text{something}))$$

on A. Applying assumption (x), we obtain the key formula

$$({}''M \ - M_1)a_x = (\ M_1 \ - (d+1))(a - p^{s}(\text{something})). \tag{A.6}$$

Bibliography

[AM69] Michael F. Atiyah and Ian G. Macdonald. *Introduction To Commutative Algebra*. Basic Books, 1969. ISBN: 9780201003611.

[BB66] Walter L. Baily and Armand Borel. "Compactification of arithmetic quotients of bounded symmetric domains". In: *Annals of mathematics* (1966), pp. 442–528.

[BD96] Massimo Bertolini and Henri Darmon. "Heegner points on Mumford-Tate curves". In: *Inventiones mathematicae* 126.3 (1996), pp. 413–456.

[BD98] Massimo Bertolini and Henri Darmon. "Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization". In: *Inventiones mathematicae* 131 (1998), pp. 453–491.

[Bes97] Amnon Besser. "On the finiteness of X for motives associated to modular forms". In: *Documenta Mathematica* 2 (1997), pp. 31–46.

[Bil] Margaret Bilu. *Complex multiplication of abelian varieties*. Available at https://www.math.u-bordeaux.fr/ mbilu/.

[Bou98] Nicolas Bourbaki. *Commutative algebra: chapters 1-7*. Vol. 1. Springer Science & Business Media, 1998.

[Bri07] David Brink. "Prime decomposition in the anti-cyclotomic extension". In: *Mathematics of Computation* 76.260 (2007), pp. 2127–2138.

[Büy14] Kâzım Büyükboduk. "Big Heegner point Kolyvagin system for a family of modular forms". In: *Selecta Mathematica* 20.3 (2014), pp. 787–815.

[Büy16] Kâzım Büyükboduk. "Deformations of Kolyvagin systems". In: *Annales mathématiques du Québec* 40 (2016), pp. 251–302.

[BCS23] Kâzım Büyükboduk, Daniele Casazza, and Ryotaro Sakamoto. "On the Artin formalism for p-adic Garrett–Rankin L-functions". In: *arXiv preprint arXiv:2301.08383* (2023).

[Buz97] Kevin Buzzard. "Integral models of certain Shimura curves". In: *Duke Math. J.* 90.1 (1997), pp. 591–612.

[CW22] Francesc Castella and Xin Wan. "The Iwasawa Main Conjectures for GL_2 and derivatives of p-adic L-functions". In: *Advances in Mathematics* 400 (2022), p. 108266.

[Cla03] Pete L. Clark. *Rational points on Atkin-Lehner quotients of Shimura curves*. Harvard University, 2003.

[Cla10] Pete L. Clark. *Algebraic Number Theory II: Valuations, Local Fields and Adeles*. Available at http://alpha.math.uga.edu/~pete/expositions2012.html. 2010.

[Col98] Pierre Colmez. "Théorie d'Iwasawa des représentations de de Rham d'un corps local". In: *Annals of Mathematics* (1998), pp. 485–571.

[CV07] Christophe Cornut and Vinayak Vatsal. "Nontriviality of Rankin-Selberg L-functions and CM points". In: *London Mathematical Society Lecture Note Series* 320 (2007), p. 121.

[Cox22] David A. Cox. *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions*. Vol. 387. American Mathematical Soc., 2022.

[Del06a] Pierre Deligne. "Formes modulaires et representations `-adiques". In: *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*. Springer, 2006, pp. 139–172.

[Del06b] Pierre Deligne. "Travaux de shimura". In: *Séminaire Bourbaki vol. 1970/71 Exposés 382–399*. Springer, 2006, pp. 123–165.

[DI95] Fred Diamond and John Im. "Modular forms and modular curves". In: *Seminar on Fermat's Last Theorem, Providence, RI*. 1995, pp. 39–133.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*. Vol. 228. Springer, 2005.

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Vol. 150. Springer Science & Business Media, 2013.

[Fis02] Ami Fischman. "On the image of -adic Galois representations". In: *Annales de l'institut Fourier*. Vol. 52. 2. 2002, pp. 351–378.

[FP94] Jean-Marc Fontaine and Bernadette Perrin-Riou. "Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions *L*". In: *Proceedings of Symposia in Pure Mathematics*. American Mathematical Society. 1994, pp. 599–706.

[Fou13] Olivier Fouquet. "Dihedral Iwasawa theory of nearly ordinary quaternionic automorphic forms". In: *Compositio Mathematica* 149.3 (2013), pp. 356–416.

[FO12] Olivier Fouquet and Tadashi Ochiai. "Control theorems for Selmer groups of nearly ordinary deformations". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 2012.666 (2012), pp. 163–187.

[Gha05] Eknath Ghate. "Ordinary forms and their local Galois representations". In: *Algebra and Number Theory: Proceedings of the Silver Jubilee Conference University of Hyderabad*. Springer. 2005, pp. 226–242.

[Gre94] Ralph Greenberg. "Trivial zeros of p-adic L-functions". In: *Contemporary Mathematics* 165 (1994), pp. 149–149.

[Gro91] Benedict H Gross. "Kolyvagin's work on modular elliptic curves". In: *L-functions and arithmetic (Durham, 1989)* 153 (1991), pp. 235–256.

[GZ86] Benedict H. Gross and Don B. Zagier. "Heegner points and derivatives of *L*-series." In: *Inventiones Mathematicae* 84 (1986), p. 225.

[Hid86a] Haruzo Hida. "Galois representations into $GL_2(Z_p[[X]])$ attached to ordinary cusp forms". In: *Inventiones mathematicae* 85 (1986), pp. 545–613.

[Hid86b] Haruzo Hida. "Iwasawa modules attached to congruences of cusp forms". In: *Annales scientifiques de l'École Normale Supérieure*. Vol. 19. 2. 1986, pp. 231–273.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series*. 26. Cambridge University Press, 1993.

[Hid00] Haruzo Hida. *Modular forms and Galois cohomology*. Cambridge University Press, 2000.

[How04a] Benjamin Howard. "Iwasawa theory of Heegner points on abelian varieties of GL_2 type". In: *Duke Math. J.* 124 (2004), pp. 1–45.

[How04b] Benjamin Howard. "The Heegner point Kolyvagin system". In: *Compositio Mathematica* 140.6 (2004), pp. 1439–1472.

[How07] Benjamin Howard. "Variation of Heegner points in Hida families". In: *Inventiones mathematicae* 167 (2007), pp. 91–128.

[KL23] Chan-Ho Kim and Matteo Longo. "Anticyclotomic main conjecture and the non-triviality of Rankin–Selberg L-values in Hida families". In: *Journal of Number Theory* 250 (2023), pp. 183–205.

[Kol90] Victor A. Kolyvagin. "Euler Systems". In: *The Grothendieck Festschrift, Volume II* 87 (1990), pp. 435–483.

[KL89] Victor A. Kolyvagin and Dmitry Y. Logachëv. "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties". In: *Algebra and Analysis* 1.5 (1989), pp. 171–196.

[Kol88] Viktor A. Kolyvagin. "Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves". In: *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 52.3 (1988), pp. 522–540.

[Kow14] Emmanuel Kowalski. *An introduction to the representation theory of groups*. Vol. 155. American Mathematical Society, 2014.

[LV11] Matteo Longo and Stefano Vigni. "Quaternion algebras, Heegner points and the arithmetic of Hida families". In: *Manuscripta mathematica* 135 (2011), pp. 273–328.

[LV19] Matteo Longo and Stefano Vigni. "Kolyvagin systems and Iwasawa theory of generalized Heegner cycles". In: *Kyoto Journal of Mathematics* 59.3 (2019), pp. 717–746.

[Mac05] Joseph H. Maclagan-Wedderburn. "A theorem on finite algebras". In: *Transactions of the American Mathematical Society* 6.3 (1905), pp. 349–352.

[Mag22] Paola Magrone. "Generalized Heegner cycles and p-adic L-functions in a quaternionic setting". In: *Annali Scuola Normale Superiore - Classe di Scienze* XXIII (2022), pp. 1807–1870.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*. 8. Cambridge university press, 1989.

[MR04] Barry Mazur and Karl Rubin. *Kolyvagin systems*. American Mathematical Society, 2004.

[Mil79] James S. Milne. "Points on Shimura varieties mod p". In: *Proc. Symp. Pure Math*. Vol. 33. Part 2. 1979, pp. 165–184.

[Mil03] James S. Milne. *Canonical models of Shimura curves (v.0.0)*. Available at www.jmilne.org/math/. 2003.

[Mil07] James S. Milne. "The fundamental theorem of complex multiplication". In: *arXiv:0705.3446* (2007).

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Available at www.jmilne.org/math/. 2008.

[Mil20] James S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[MT99] Andrea Mori and Lea Terracini. "A canonical map between Hecke algebras". In: *Bollettino dell'unione matematica italiana* 8 (1999), pp. 429–452.

[Nek92] Jan Nekovář. "Kolyvagin's method for Chow groups of Kuga-Sato varieties". In: *Inventiones mathematicae* 107.1 (1992), pp. 99–125.

[Nek06] Jan Nekovář. *Selmer complexes*. Vol. 310. Société mathématique de France, 2006.

[NP00] Jan Nekovář and Andrew Plater. "On the parity of ranks of Selmer groups". In: *Asian Journal of Mathematics* 4.2 (2000), pp. 437–498.

[Neu86] Jürgen Neukirch. *Class field theory*. Vol. 280. Springer, 1986.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Vol. 323. Springer Science & Business Media, 2013.

[Och05] Tadashi Ochiai. "Euler system for Galois deformations". In: *Annales de l'institut Fourier*. Vol. 55. 1. 2005, pp. 113–146.

[Per87] Bernadette Perrin-Riou. "Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner". In: *Bulletin de la Société mathématique de France* 115 (1987), pp. 399–456.

[Per00] Bernadette Perrin-Riou. *p-adic L-functions and p-adic representations*. American Mathematical Society, Providence, RI, 2000.

[Rib77] Kenneth A. Ribet. "Galois representations attached to eigenforms with nebentypus". In: *Lecture Notes in Mathematics* vol. 601 (1977), pp. 18–52.

[Rub00] Karl Rubin. *Euler systems*. 147. Princeton University Press, 2000.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Vol. 42. Springer, 1977.

[Ufe12] Dominik Ufer. "Abelian varieties with quaternion and complex multiplication". In: *arXiv:1208.5599* (2012).

[Vig05] Stefano Vigni. *A Gross-Zagier formula for a certain anticyclotomic p-adic L-function*. Ph.D. Thesis, Università di Milano. 2005.

[Vig22] Stefano Vigni. "On Shafarevich-Tate groups and analytic ranks in families of modular forms, I. Hida families". In: *Annali Scuola Normale Superiore - Classe di Scienze* (2022), pp. 2–38.

[Voi21] John Voight. *Quaternion algebras*. Springer Nature, 2021.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.