CM-values of p-adic Theta-functions

Daas, M.A.

CM-values of p-adic Θ-functions

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof.dr.ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op woensdag 30 oktober 2024
klokke 16:00 uur

door

Michael Alexander Daas
geboren te Zaandijk, Nederland
in 1997

Promotores:

Prof. dr. J. B. Vonk

Prof. dr. P. Stevenhagen

Promotiecommissie:

Prof. dr. ir. G. L. A. Derks

Prof. dr. D. S. T. Holmes

Prof. dr. P. Charollois (Sorbonne Université)

Prof. dr. H. Darmon (McGill University)

Dr. A. Pozzi (University of Bristol)

Publications and preprints

Parts of this thesis are based on the following paper:

Michael A. Daas. CM-values of p-adic Θ-functions. *arXiv preprint arXiv:2309.17251*, 2023

Contents

A guide to notation

Keeping track of notation in a long text on mathematics can be a daunting task for a reader of any level of mathematical experience. Especially when proofs become increasingly technical with many moving parts and auxilliary variables, maps and objects, it is very easy to lose track of every little bit of notation that was introduced beforehand. Even though the author likes to convince himself that every reader will carefully go through their work from start to finish, reading every page with equal interest and energy, reality is often different, and skipping certain proofs, sections or chapters is a common cause for confusion about notation.

For this reason, this thesis aims to approach the problem of identifying missing pieces of notation in a very systematic manner that should, if executed without error by the author, in principle allow one to get a hold of notation after checking only a few easy to locate places in the thesis, without having to skim many pages of mathematics, tracking down the seemingly first instance of a certain symbol.

If in any instance while perusing this thesis, a certain piece of notation is used, you should find its meaning in a finite number of quick steps:

- It could be that the notation is introduced *earlier in the proof* you are reading; this happens for example with dummy variables used in some matrix manipulations.

- If not, then it is possible that this notation is either introduced or repeated from earlier sections *at the very start of the current section*; this happens for example when notation from a previous section is carried over to the next and is thus repeated for the reader's convenience.

- If not, then it is possible that this notation is either introduced or repeated from earlier chapters *at the very start of the current chapter*; this happens for example when specific objects from the main results from earlier chapters are used again in the present chapter.

- If not, then the notation is *introduced below*; this is the case for some of the most fundamental pieces of notation that will be used many times throughout the entire thesis.

If any instance of notation fails to be tracked down after following the steps outlined above, the author would be happy to receive their well-deserved reprimand through any medium of the reader's preference.

The relevant fields

As is standard, we let $\mathbb{Z}$ denote the integers and $\mathbb{N} := \mathbb{Z}_{\geq 1}$ the positive integers. Next, we let $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rationals, reals and complex numbers respectively. Furthermore, $\mathcal{H} \subset \mathbb{C}$ denotes the complex upper half plane $\mathcal{H} := \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$. For any field M, we let $\overline{M}$ be an algebraic closure of M and we let $G_M := \mathrm{Gal}(\overline{M}/M)$ denote its absolute Galois group.

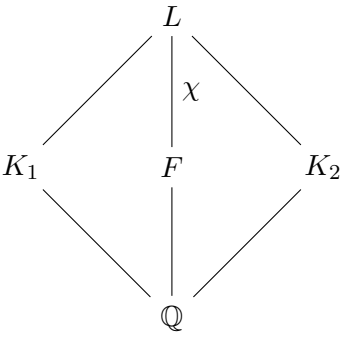
If M is a number field, then $\mathcal{O}_M$ denotes its ring of integers and $\mathrm{Pic}(M)$ the ideal class group of the maximal order $\mathcal{O}_M$. Furthermore, we let H_M denote the Hilbert class field of M, so that the Artin map yields an isomorphism $\mathrm{Pic}(M) \xrightarrow{\sim} \mathrm{Gal}(H_M/M)$.

For any rational prime p, by $\mathbb{Q}_p$ we will mean the field of p-adic numbers. Let $\mathbb{C}_p$ be a completion of $\overline{\mathbb{Q}}_p$. We may now define the *p-adic upper half plane* as

$$\mathcal{H}_p := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p),$$

where $\mathbb{P}^1(-)$ denotes the projective line over the field considered. For any number field M and rational prime ℓ, we define $M_\ell := M \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

Throughout this thesis, we specify two *coprime* fundamental discriminants $D_1, D_2 < 0$. Write $K_i := \mathbb{Q}(\sqrt{D_i})$ for $i \in \{1, 2\}$ with rings of integers $\mathcal{O}_1$ and $\mathcal{O}_2$ and Hilbert class fields H_1 and H_2 respectively. We write $w_i := \#\mathcal{O}_i^\times$ for $i \in \{1, 2\}$ and let $D := D_1 D_2 > 0$. Next, we let $F := \mathbb{Q}(\sqrt{D})$ be the real quadratic field and $L := \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ be the biquadratic field completing the following field diagram:



Explicitly, we will denote the elements of these Galois groups by

$$\mathrm{Gal}(F/\mathbb{Q}) = \{1, \sigma\} \quad \text{and} \quad \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_F\},$$

where σ_1, σ_2 and σ_F are all involutions with fixed fields K_1, K_2 and F respectively.

For any subset $S \subset F$, we let $S^+ \subset S$ denote the subset of totally positive elements of S. For $x \in F$, the notation $x \gg 0$ also denotes that x is totally positive and these are used interchangeably.

The Artin map induces an isomorphism

$$\mathrm{Pic}(F)^+ \xrightarrow{\sim} \mathrm{Gal}(H_F^+/F),$$

where H_F^+ denotes the narrow Hilbert class field of F. Because precisely those primes dividing the discriminant ramify, the field extension L/F is unramified at all finite places. Since L/F is also abelian, the field L must be contained in H_F^+ and as such, we obtain a natural quotient map by restriction

$$\chi : G_F \to \mathrm{Gal}(H_F^+/F) \to \mathrm{Gal}(L/F) \cong \{\pm 1\}.$$

The composition of the above two maps also defines a character on the narrow ideal class group of F, which we will, by slight abuse of notation, also denote by $\chi : \mathrm{Pic}(F)^+ \to \{\pm 1\}$.

We let $\mathcal{D}_F$ denote the different ideal of F and we define

$$\rho(I) := \#\left\{J \subset \mathcal{O}_L \mid \mathrm{Nm}_F^L(J) = I\right\}$$

for any ideal $I \subset \mathcal{O}_F$.

We let N be a positive integer that is the product of two distinct prime numbers p and q, so we may write $N = pq$. But for the coprimality of D_1 and D_2, all the notation introduced above has so far been independent of one another. However, we must make the following crucial assumption about how the integer N interacts with the fields introduced above.

> Throughout this thesis, we will make the assumption that both p and q are *inert* in both K_1 and K_2.

As a result, both p and q must split in F and we let $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_F$ denote the two primes above p respectively, and similarly $\mathfrak{q}_1, \mathfrak{q}_2 \subset \mathcal{O}_F$. Also, both p and q are in particular *unramified* in $L/\mathbb{Q}$.

Quaternion algebras

For any ring R, we let $R^\times$ denote the subgroup of units in R.

For any positive squarefree integer M, we let B_M denote the unique (up to isomorphism) quaternion algebra for which a finite prime is ramified if and only if it divides M. In particular, if M contains an even number of prime factors, B_M must be indefinite, and if M contains an odd number of prime factors, B_M must be definite.

For any such quaternion algebra B_M we let $R_M \subset B_M$ denote a maximal order; this choice need not be unique, even up to conjugation.

Because we assume the prime q to be inert in both K_1 and K_2, we can find embeddings $\alpha_1 : \mathcal{O}_1 \to B_q$ and $\alpha_2 : \mathcal{O}_2 \to B_q$, see [Voi21].

> We assume throughout that R_q is the only maximal order of B_q up to conjugation. That is, we assume that $q \in \{2, 3, 5, 7, 13\}$.

Choose any splitting $B_q \hookrightarrow M_2(\mathbb{Q}_p)$. This matrix algebra acts on $\mathbb{C}_p$ through fractional linear transformations:

$$\text{if } \; A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad A \cdot z = \frac{az+b}{cz+d}.$$

We compute the fixed points for the action of A through

$$z = \frac{az+b}{cz+d} \iff cz^2 + (d-a)z - b = 0.$$

This also shows that every element in the ring $\mathbb{C}_p[A]$ shares the same fixed points. If $c \neq 0$, one checks that the two fixed points coincide if and only if $(2A - \mathrm{tr}(A))^2 = 0$, so the ring $\mathbb{C}_p[A]$ would not be reduced. If $c = 0$, then A satisfies the equation $(A-a)(A-d) = 0$ over $\mathbb{Q}_p$.

Through the embeddings $\alpha_i : \mathcal{O}_i \to R_q$ for $i \in \{1, 2\}$ and this splitting, the orders $\mathcal{O}_i$ act on $\mathbb{C}_p$ too. Clearly, their images in $M_2(\mathbb{Q}_p)$ must be reduced. In addition, any element from $K_i \setminus \mathbb{Q}$ for $i \in \{1, 2\}$ is quadratic over $\mathbb{Q}_p$, because p is inert in both fields. As such, their images under the splitting cannot be upper-triangular and so these images always have two conjugate fixed points in $\mathcal{H}_p$.

> We will denote the common fixed points for the action of $\mathcal{O}_i$ on $\mathcal{H}_p$ through the embedding $\alpha_i : \mathcal{O}_i \to R_q$ with τ_i and τ_i', for $i \in \{1, 2\}$.

CHAPTER 1

The work of Gross and Zagier

Let $E/\mathbb{Q}$ an elliptic curve and let r_{alg} denote the rank of the group $E(\mathbb{Q})$, which is finite by the Mordell-Weil theorem. We may associate to E an L-function

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

which converges as soon as $\text{Re}(s) > 3/2$ and which by the modularity theorem, proved by Wiles and Taylor, allows an analytic continuation to the whole complex plane. The *Conjecture of Birch and Swinnerton-Dyer* predicts that the order of vanishing r_{an} of $L(E,s)$ at $s=1$, often referred to as the *analytic rank* of E, is equal to the *algebraic rank* r_{alg}. More precisely, it relates the non-zero value of the r_{an}-th derivative $L^{(r_{\text{an}})}(E,1)$ to various arithmetic invariants associated with the elliptic curve $E/\mathbb{Q}$.

In its complete generality, this *BSD-conjecture*, as it has come to be known, is still open. In fact, it is listed as one of the *Millennium Problems* by the Clay Mathematics Institute and is widely recognised as one of the most important and influencial conjectures in all of modern mathematics. As of today, almost all the partial progress towards the conjecture has been achieved for curves with rank at most 1.

The work of Gross, Kohnen and Zagier in [GZ86, GKZ87] constitutes a rare instance of such progress on this notoriously difficult open problem. The former gave a relation between the heights of Heegner divisor classes on the Jacobian of modular curves and the first derivatives at $s=1$ of the L-series of certain modular forms. The latter computed the height pairings of two distinct Heegner divisor classes to show that related quantities can be suitably combined to form the Fourier coefficients of a Jacobi form.

More concretely, using the theory of Heegner points, Theorem 7.4 in [GZ86] shows the following for elliptic curves $E/\mathbb{Q}$ with $L(E,1)=0$. If Ω_E denotes the real period of a regular differential on E, then for the explicitly computable $\alpha \in \mathbb{Q}$ as predicted by the BSD-conjecture and for some $P \in E(\mathbb{Q})$, it holds that

$$L'(E,1) = \alpha \cdot \Omega_E \cdot \langle P, P \rangle,$$

where $\langle -,- \rangle$ denotes the canonical global height pairing on $E(\mathbb{Q})$. In particular, this proves that, if $r_{\text{an}} = 1$, then we must have $r_{\text{alg}} \geq 1$.

Later, by varying one of the discriminants instead, the heights of Heegner cycles were also shown in [KRY04] to be connected to the derivative of a weight $3/2$ Eisenstein series for $\text{SL}_2(\mathbb{Z})$. The *Kudla program* aims to study the arithmetic properties of the first derivative of certain Eisenstein series and to connect these with a specific class of arithmetic

cycles and the special values of certain L-functions. Another relevant instance of a result in this direction can be found in [Sch09].

This thesis aims to generalise the collaborative work [GZ84] by Gross and Zagier that precedes the results of [GZ86, GKZ87] described above. In view of these results, the setting in [GZ84] can be regarded as the $X_0(1)$-case of the work done in [GZ86] and [GKZ87], the height pairing on whose Jacobian vanishes by virtue of the curve being of genus zero. Similarly, our main theorems will reflect the results in [GZ84] and we explain in Remark 2.3.1 how these results are to be interpreted in a more general framework as is done above.

This first introductory chapter contains very little original work and its purpose is mainly to provide the reader with the necessary background information to fully appreciate the context within which the main results of this thesis are best viewed. In particular, we investigate the main results of [GZ84] and interpret both its statement and its proofs to justify the ways in which this thesis aims to generalise them.

1.1 Classical CM-theory

The formulation of *class field theory* in the 20th century has been one of the greatest achievements in the field of algebraic number theory, describing the structure of all abelian extensions of a number field in terms of the arithmetic inside this field. In particular, it promises for every number field K an abelian extension called the *Hilbert class field* H_K which is unramified at every prime and maximal for this property. Even though its existence is known, its explicit construction and that of other class fields in complete generality has been a long standing open problem, known both as Kronecker's *Jugendtraum* and as Hilbert's 12th Problem. At the International Congress of Mathematicians in the year 1900, Hilbert called this problem "one of the most profound and far reaching in the theory of numbers and of functions".

All abelian extensions of $\mathbb{Q}$ are described by the Kronecker-Weber Theorem, which produces these extensions as generated by values of the function $r \mapsto e^{i\pi r}$ for $r \in \mathbb{Q}$; also known as roots of unity. The most natural next step would be to consider the class fields associated with quadratic extensions of $\mathbb{Q}$ and to attempt to find a function similar to the one above that mimics this striking property.

For *imaginary* quadratic fields, such results were obtained through study of Klein's j-function, given by

$$j(\tau) = \mathbf{q}^{-1} + 744 + 196884\mathbf{q} + 21493760\mathbf{q}^2 + \dots,$$

where $\mathbf{q} = e^{i\pi\tau}$ and $\tau \in \mathcal{H}$. This function is also integral to the study of isomorphism classes of elliptic curves, as it yields an isomorphism

$$j : \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

This work does not introduce the concept of elliptic curves; we assume the reader to be familiar with these objects. For a comprehensive introduction to elliptic curves, we refer the reader to Silverman's excellent *The Arithmetic of Elliptic Curves* [Sil09].

Throughout this section, K will be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. One may compute for instance that

$$j(\sqrt{-5}) = 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}).$$

One may then observe that $H = K(\sqrt{5})$ is in fact the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$, the field over which the input is defined. One of the key results of classical CM theory is that this is no coincidence, and in fact holds very generally. Until recently, the case of CM-fields were the only class of number fields for which explicit class field theory had been provably realised, though large breakthroughs have been made recently by Dasgupta and Kakde in their works [DK23a] and [DK23b]. The CM-values of the j-function are often called *singular moduli*.

To explain the results from CM theory most conceptually, we opt to approach the classical theory of complex multiplication in a modern adèlic language that will allow for swift and intuitive generalisations to the setting of Shimura curves in Chapter 2, as will be the focus of this thesis. Let $\widehat{\mathbb{Z}}$ denote the profinite integers and let $\mathcal{K} \subset \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be a compact open subgroup. Examples of $\mathcal{K}$ include the closures of congruence subgroups of $\mathrm{GL}_2(\mathbb{Z})$ inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each such $\mathcal{K}$, we may define the open modular curve $Y_{\mathcal{K}}$ through the following adèlic description:

$$Y_{\mathcal{K}}(\mathbb{C}) = (\mathcal{K} \cap \mathrm{SL}_2(\mathbb{Z})) \setminus \mathcal{H} \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^{\pm} \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})/\ \mathcal{K}\right),$$

where $\mathcal{H}^{\pm} = \mathbb{C} \setminus \mathbb{R}$ denotes the union of the two half planes. This isomorphism sends $\tau \in \mathcal{H}$ to the object $\mathrm{GL}_2(\mathbb{Q})\,(\tau, 1 \cdot \mathcal{K})$.

We will fix an embedding $\alpha : \mathcal{O}_K \to M_2(\mathbb{Z})$ and we let $\tau \in \mathcal{H}$ denote the unique fixed point of the image of α under its action on $\mathcal{H}^{\pm}$. Then $\tau \in \mathcal{H}$ denotes a choice of a *CM-point* in the upper half plane. Since $K^{\times}$ is a dense subgroup of $\mathbf{A}_K^{\mathrm{fin},\times}$, by continuity α extends uniquely to an embedding $\mathbf{A}_K^{\mathrm{fin},\times} \to \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})$, which we will by slight abuse of notation also denote by α. Then we obtain a natural map

$$K^{\times} \setminus \mathbf{A}_K^{\mathrm{fin},\times} \to \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^{\pm} \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})\right),$$

which sends some idèle $s \in \mathbf{A}_K^{\mathrm{fin},\times}$ to the pair $(\tau, \alpha(s))$. Note that this is well-defined, as the image of $K^\times$ fixes τ by definition. We stress that $K^\times \setminus \mathbf{A}_K^{\mathrm{fin},\times} = K^\times \mathbb{C}^\times \setminus \mathbf{A}_K^\times$, and thus by global class field theory this is isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ using the Artin map, denoted by $[-, K]$. The following theorem is often referred to as the *Main Theorem of Complex Multiplication*, see Theorem 4.19 in [Del71].

Theorem 1.1.1. *Consider the following commutative diagram:*

$$\begin{array}{ccc} K^\times \setminus \mathbf{A}_K^{\mathrm{fin},\times} & \longrightarrow & \mathrm{GL}_2(\mathbb{Q}) \setminus \left(\mathcal{H}^\pm \times \mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})\right) \\ {\scriptstyle [-,K]}\downarrow & & \downarrow{\scriptstyle /\ \mathcal{K}} \\ \mathrm{Gal}(K^{\mathrm{ab}}/K) & \overset{\eta}{\dashrightarrow} & Y_{\mathcal{K}}(\mathbb{C}). \end{array}$$

Then the image of η is contained in $Y_{\mathcal{K}}(\overline{\mathbb{Q}})$ and η is Galois-equivariant.

We illustrate its power by deducing from this an adèlic version of *Shimura reciprocity*, specialising to the CM-points on the curve $Y_0(1)$. Recall that every left-ideal in $M_2(\mathbb{Z})$ is principal.

Corollary 1.1.2. *Let $\tau \in \mathcal{H}$ be the CM-point associated with the embedding $\alpha : \mathcal{O}_K \to M_2(\mathbb{Z})$. Then it holds that $j(\tau) \in H$. Further, let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal and let $x \in M_2(\mathbb{Z})$ be such that $\alpha(\mathfrak{a})M_2(\mathbb{Z}) = x \cdot M_2(\mathbb{Z})$. Then it holds that*

$$j(\tau)^{[\mathfrak{a}, H_K/K]} = j(x^{-1} \cdot \tau),$$

where $x^{-1} \cdot \tau \in \mathcal{H}$ is a CM-point for the embedding $x^{-1}\alpha(-)x$.

Proof. We apply Theorem 1.1.1 in that case that $\mathcal{K} = \mathrm{GL}_2(\widehat{\mathbb{Z}})$. For $s \in \mathbf{A}_K^{\mathrm{fin},\times}$, the map η from Theorem 1.1.1 is given by

$$\eta([s, K]) = \mathrm{GL}_2(\mathbb{Q}) \left(\tau, \alpha(s)\mathrm{GL}_2(\widehat{\mathbb{Z}})\right).$$

To work out which point on the modular curve this corresponds to, we recall the easy to check equality of groups $\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}} = \mathbb{Q}\widehat{\mathbb{Z}}$, and using strong approximation results, one can deduce from this that also

$$\mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}}) = \mathrm{GL}_2(\mathbb{Q})\mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

We may then decompose

$$\alpha(s) = xy \quad \text{with} \quad x \in \mathrm{GL}_2(\mathbb{Q}) \quad \text{and} \quad y \in \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

We then find that

$$\begin{aligned}\mathrm{GL}_2(\mathbb{Q})\left(\tau, \alpha(s)\mathrm{GL}_2(\widehat{\mathbb{Z}})\right) &= \mathrm{GL}_2(\mathbb{Q})\left(\tau, xy\mathrm{GL}_2(\widehat{\mathbb{Z}})\right)\\ &= \mathrm{GL}_2(\mathbb{Q})\left(x^{-1}\tau, 1\cdot \mathrm{GL}_2(\widehat{\mathbb{Z}})\right).\end{aligned}$$

In other words, we may describe the map $\eta : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to Y_0(1)(\overline{\mathbb{Q}})$ by the formula

$$\eta([s,K]) = x^{-1}\tau \in \mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H};$$

this is well-defined because the ambiguity in the choices of x and y is measured by $\mathrm{GL}_2(\mathbb{Q})\cap\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \mathrm{GL}_2(\mathbb{Z})$. Set $U = \prod_v \mathcal{O}_v^\times$, where the product is taken over all finite places v of K. If $s \in U$, then by continuity it follows that $\alpha(s) \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$ and therefore we may take $x = 1$. This shows once again that the CM-point τ is defined over the Hilbert class field H of K.

To refine this, we must consider more general $s \in \mathbf{A}_K^{\mathrm{fin},\times}$ such that $[s,K]|_H = [\mathfrak{a}, H/K]$. We claim that the $M_2(\mathbb{Z})$-ideal generated by the image $\alpha(\mathfrak{a})$ is equal to $x\cdot M_2(\mathbb{Z})$ with x as defined above. To see this, we recall that the quotient

$$\mathrm{GL}_2(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})/\mathrm{GL}_2(\widehat{\mathbb{Z}})$$

is in bijection with set of fractional $M_2(\mathbb{Z})$-ideals inside $M_2(\mathbb{Q})$. Indeed, any such class can be represented by an element from $\mathrm{GL}_2(\mathbb{Q})$, which defines a fractional $M_2(\mathbb{Z})$-ideal inside $M_2(\mathbb{Q})$ as this element is well-defined up to an element from $\mathrm{GL}_2(\mathbb{Z})$, which does not affect the resulting $M_2(\mathbb{Z})$-ideal. This shows that indeed $\alpha(s)$ induces the ideal $x\cdot M_2(\mathbb{Z})$ and thus so will $\alpha(\mathfrak{a})$ by virtue of our choice of s. □

1.2 Singular moduli

In their paper [GZ84], Gross and Zagier studied the differences between singular moduli. For example,

$$j\left(\frac{1+\sqrt{-43}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) = 2^{19}\cdot 3^6\cdot 5^3\cdot 7^3\cdot 37\cdot 433. \tag{1.1}$$

Aside from this number being rather smooth, one may observe that all its prime divisors are inert in both $\mathbb{Q}(\sqrt{-43})$ and $\mathbb{Q}(\sqrt{-163})$. More precisely, all of these primes occur as the factor of a number of the form $43\cdot 163 - x^2$ for some $|x| < \sqrt{43\cdot 163}$, as the equality $43\cdot 163 - 9^2 = 16\cdot 433$

exemplifies. These patterns persist when repeating the experiment with other, possibly non-rational singular moduli if one takes the norm down to $\mathbb{Q}$. This thesis aims to study factorisation phenomena that display a parallel with the observations made and subsequently explained by Gross and Zagier in [GZ84].

Before stating the factorisation formulas, we require some notation. Suppose that m is an integer supported at primes that are not inert in $F/\mathbb{Q}$. Assume that there is a unique prime ℓ both dividing m an odd number of times, say $2k+1$ times, with the additional property that any prime ideal $\mathfrak{l}$ of F above ℓ satisfies $\chi(\mathfrak{l}) = -1$. We will call such primes the *special* primes of the integer m; terminology that we will use again in Chapter 6. Further, let $\{c_i\}$ be the set of exponents of primes dividing m with the property that all primes of F lying above them split in L/F. Then we set

$$F(m) := \ell^X \quad \text{where} \quad X = (k+1)\prod(c_i+1),$$

and simply $F(m) = 1$ for all other $m \in \mathbb{Q}$. Finally, let $\tau_1, \tau_2 \in \mathcal{H}$ be CM-points of discriminants D_1 and D_2 respectively. Then Gross and Zagier proved the following in [GZ84].

Theorem 1.2.1. *With all notation from above, it holds that*

$$\mathrm{Nm}_{\mathbb{Q}}\big(j(\tau_1) - j(\tau_2)\big)^{\frac{8}{w_1 w_2}} = \pm \prod_{\substack{x^2 < D \\ x^2 \equiv D \bmod 4}} F\left(\frac{D-x^2}{4}\right).$$

We illustrate this theorem in a few simple cases for discriminants of class number 1. We record here the following CM curves:

$$E_7 : y^2 + xy = x^3 - x^2 - 2x - 1 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right];$$

$$E_{11} : y^2 + y = x^3 - x^2 - 7x + 10 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right];$$

$$E_{19} : y^2 + y = x^3 - 38x + 90 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right];$$

$$E_{43} : y^2 + y = x^3 - 860x + 9707 \quad \text{has CM by} \quad \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right].$$

One computes from this the quantities

$$j(E_7) = -3^3 5^3; \quad j(E_{11}) = -2^{15};$$
$$j(E_{19}) = -2^{15} 3^3; \quad j(E_{43}) = -2^{18} 3^3 5^3.$$

Example 1.2.2. Let us first choose $D_1 = -7$ and $D_2 = -11$. Then $D = D_1 D_2 = 77$, and so we make the following table.

x	± 1	± 3	± 5	± 7
$\frac{D-x^2}{4}$	19	17	13	7
$F(\frac{D-x^2}{4})$	19	17	13	7

Indeed, one computes that

$$j(E_7) - j(E_{11}) = -3^3 5^3 + 2^{15} = 29393 = 7 \cdot 13 \cdot 17 \cdot 19,$$

as predicted by Theorem 1.2.1. Note here that the norm of the rational invariant down to $\mathbb{Q}$ is just the identity, and the exponent $8/(w_1 w_2) = 2$ corresponds to the fact that we double count each entry in our table by virtue of $\pm x$ giving the same outcome.

Example 1.2.3. Let us now choose $D_1 = -7$ and $D_2 = -19$. Then $D = D_1 D_2 = 171$, and so we make the following table.

x	± 1	± 3	± 5	± 7	± 9	± 11
$\frac{D-x^2}{4}$	$3 \cdot 11$	31	3^3	$3 \cdot 7$	13	3
$F(\frac{D-x^2}{4})$	3^2	31	3^2	3^2	13	3

One might enjoy verifying that

$$j(E_7) - j(E_{19}) = -3^3 5^3 + 2^{15} 3^3 = 881361 = 3^7 \cdot 13 \cdot 31,$$

which agrees with Theorem 1.2.1.

Example 1.2.4. Finally, we choose $D_1 = -7$ and $D_2 = -43$. Then $D = D_1 D_2 = 301$, and so we make the following table.

x	± 1	± 3	± 5	± 7	± 9	± 11	± 13	± 15	± 17
$\frac{D-x^2}{4}$	$3 \cdot 5^2$	73	$3 \cdot 23$	$3^2 \cdot 7$	$5 \cdot 11$	$3^2 \cdot 5$	$3 \cdot 11$	19	3
$F(\frac{D-x^2}{4})$	3	73	3^2	7	5^2	5	3^2	19	3

We leave it to the reader to check that indeed,

$$j(E_7) - j(E_{43}) = -3^3 5^3 + 2^{18} 3^3 5^3 = 884732625 = 3^6 \cdot 5^3 \cdot 7 \cdot 19 \cdot 73,$$

in perfect accordance with Theorem 1.2.1.

Gross and Zagier in [GZ84] gave two proofs of this formula, and the dissimilarities between these proofs cannot be overstated. In this section we briefly discuss their first proof, and leave a discussion of the second to Section 1.6. The idea of this first proof is to count and compare the prime factors of both sides of the equality proposed by Theorem 1.2.1. As the right hand side is already expressed in fairly elementary terms, the difficulty comes from analysing the left hand side. The starting point for this method is Proposition 2.3 in [GZ84], which reads as follows.

Theorem 1.2.5. *Let ℓ be a prime number and let A be the complete discrete valuation ring of a finite field extension of $\mathbb{Q}_\ell^{\mathrm{unr}}$. Let π be a uniformiser and let v be the discrete valuation on A satisfying $v(\pi) = 1$. Let E_1 and E_2 be elliptic curves over A with good reduction and associated j-invariants $j_1, j_2 \in A$. For any positive integer n, let $\mathrm{Iso}_n(E_1, E_2)$ denote the number of isomorphisms from E_1 to E_2 defined over the ring A/π^n. Then*

$$2v(j_1 - j_2) = \sum_{n \geq 1} \mathrm{Iso}_n(E_1, E_2).$$

This formula refines the elementary observation that for elliptic curves $E_1, E_2/\mathbb{Q}$ with good reduction at a rational prime ℓ, it holds that

$$\ell \mid j_1 - j_2 \iff \overline{E}_1 \xrightarrow{\sim} \overline{E}_2 \quad \text{over } \overline{\mathbb{F}}_\ell.$$

According to Theorem II.6.1 in [Sil94], the algebraic numbers j_1 and j_2 are in fact algebraic integers, implying that both E_1 and E_2 have potentially good reduction at the prime ℓ. Therefore, the assumption of good reduction in Theorem 1.2.5 above is not in fact a restriction and may be assumed without loss of generality.

We thus reduce to determining the numbers $\mathrm{Iso}_n(E_1, E_2)$ for each positive integer n. The next key observation is that if E_1 and E_2 have CM by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively, in case this quantity is non-zero, both $\overline{E}_1 \cong \overline{E}_2/\overline{\mathbb{F}}_\ell$ must have supersingular reduction at ℓ. Indeed, for $i \in \{1, 2\}$, we have an injective map

$$\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}/\overline{\mathbb{F}}_\ell).$$

If E_1 and E_2 instead had ordinary reduction at ℓ, this endomorphism ring would have been an order in an imaginary quadratic field, and as such would not have been able to receive embeddings from two such orders of different coprime discriminants.

We recall the Deuring correspondence. Let B_ℓ denote the definite rational quaternion algebra ramified only at ℓ and ∞. We fix a maximal order $R_\ell \subset B_\ell$.

Let $E/\overline{\mathbb{F}}_\ell$ be a fixed supersingular elliptic curve equipped with an isomorphism $\eta : \mathrm{End}(E) \xrightarrow{\sim} R_\ell$ which we may $\mathbb{Q}$-linearly extend to an isomorphism $\eta : \mathrm{End}(E)\otimes\mathbb{Q} \xrightarrow{\sim} B_\ell$. For any integral left R_ℓ-ideal $I \subset R_\ell$, one may define the group scheme theoretic intersection

$$E[I] := \bigcap_{\alpha\in I} E[\eta^{-1}(\alpha)] \quad \text{and set} \quad E_I := E/E[I].$$

The elliptic curve E_I is again supersingular and comes with a natural projection morphism $\phi_I : E \to E_I$. Lemma 42.2.7 in [Voi21] states that the map

$$f_I : \mathrm{Hom}(E_I, E) \xrightarrow{\sim} I : \psi \mapsto \eta(\psi\phi_I)$$

is an isomorphism of left R-modules. Now the Deuring correspondence, Theorem 42.3.2 in [Voi21], states the following.

Theorem 1.2.6. *Let $E_0/\overline{\mathbb{F}}_\ell$ be a fixed supersingular elliptic curve with $\mathrm{End}(E_0) \cong R_\ell$. Then the associations*

$$E \mapsto \mathrm{Hom}(E, E_0) \quad \textit{and} \quad E_I \nleftarrow I$$

define an equivalence between the categories of supersingular elliptic curves over $\overline{\mathbb{F}}_\ell$ and the category of invertible left R_ℓ-modules.

This allows us to transpose the problem at hand into a counting problem inside the quaternion algebra B_ℓ. Let $x_2 \in A$ denote a fixed element satisfying a quadratic equation over $\mathbb{Q}$ with discriminant D_2. As is explained in [GZ84], each $f \in \mathrm{Iso}_n(E_1, E_2)$ gives rise, through the association $f \mapsto f^{-1} \circ [x_2] \circ f$, to an endomorphism of E_1 modulo π^n with trace and norm equal to that of x_2, also inducing multiplication by x_2 on $\mathrm{Lie}(E_1)$. To prove this is a bijective correspondence, one requires the following refinement of a theorem by Deuring; this is Proposition 2.7 in [GZ84].

Proposition 1.2.7. *Given any elliptic curve $\widetilde{E}$ over A/π^n and an endomorphism $\widetilde{[x_2]} : \widetilde{E} \to \widetilde{E}$ with the properties above, there exists an elliptic curve E over A and an endomorphism $[x_2]$ of E, unique up to isomorphism, lifting the pair $(\widetilde{E}, \widetilde{[x_2]})$ such that $[x_2]$ induces multiplication by x_2 on $\mathrm{Lie}(E)$.*

This means that, to determine the sizes of the sets

$$\left\{ f^{-1} \circ [x_2] \circ f \;\middle|\; f \in \mathrm{Iso}_n(E_1, E_2) \right\} \subset \mathrm{End}(E_1 \mod \pi^n),$$

we may instead consider the sets

$$S_n := \big\{ g \in \mathrm{End}(E_1 \mod \pi^n) \mid \mathrm{tr}(g) = \mathrm{tr}(x_2), \\ \mathrm{Nm}(g) = \mathrm{Nm}(x_2), \quad g = x_2 \text{ on } \mathrm{Lie}(E_1) \big\}.$$

To determine the cardinalities of these sets, we use the explicit description of $\mathrm{End}(E_1 \mod \pi^n)$ from Lemma 3.5 in [GZ84]. It claims that

$$B_\ell \cong \left\{ \begin{pmatrix} \alpha & \beta \\ -\ell\overline{\beta} & \overline{\alpha} \end{pmatrix} \mid \alpha, \beta \in K_1 \right\} \subset M_2(K_1),$$

and this isomorphism sends $\mathrm{End}(E_1 \mod \pi^n)$ to those matrices satisfying that $\alpha \in \mathcal{D}_{K_1}^{-1}$, the inverse different of K_1, and $\beta \in \mathcal{D}_{K_1}^{-1}\ell^{n-1}\overline{\mathfrak{a}}/\mathfrak{a}$, further satisfying that $\alpha \equiv \lambda\beta \mod \mathcal{O}_1$. Here λ is such that $\lambda^2 \equiv -\ell \mod \mathcal{D}_{K_1}$ and $\mathfrak{a} \subset K_1$ is a fractional ideal of K_1 determined by the precise prime above ℓ of H_1 we are considering.

Finally, this counting problem is solved in the remainder of Section 3 in [GZ84] for all possible splitting behaviours of the prime ℓ in the fields K_1 and K_2. This allows one to finally compare the result to the right hand side of Theorem 1.2.1, completing the first proof.

1.3 Intersection numbers of embeddings

In this section, we describe an alternative formulation of Theorem 1.2.1 described above. Namely, key to the algebraic proof of Theorem 1.2.1 were the existence of two embeddings

$$\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}),$$

where the latter ring is a maximal order inside the quaternion algebra B_ℓ. Both to formulate and to prove our generalisations of Theorem 1.2.1, which will be the main focus of this thesis, in the chapters that follow we will also work with such embeddings, so we elaborate on how these concepts occur in the original setting of [GZ84] as well.

Suppose that a prime ℓ is inert in both $\mathcal{O}_1$ and $\mathcal{O}_2$. Fix a set of representative left R_ℓ-ideals $\mathrm{Cl}_L(R) = \{I_1, I_2, \ldots, I_n\}$ for the left-class set of R. Define $R_j := R_{I_j}$ as the associated right order for the ideal I_j for $j \in \{1, \ldots, n\}$, so that all conjugacy classes of maximal orders of B_ℓ occur either once or twice among the R_j.

By Corollary 1.1.2, for $i \in \{1, 2\}$, the elliptic curves E_i with CM by $\mathcal{O}_i$ are a principal homogeneous space for the action of $\mathrm{Pic}(K_i)$. Therefore,

the number of elliptic curves E_i with CM by $\mathcal{O}_i$ is given by h_i, where h_i denotes $\#\mathrm{Pic}(K_i)$.

Let $\alpha_1 : K_1 \to B_\ell$ and $\alpha_2 : K_2 \to B_\ell$ denote embeddings. For $\mathcal{O} \in \{\mathcal{O}_1, \mathcal{O}_2\}$ and $R \subset B_\ell$ a maximal order, define

$$\mathrm{Emb}(\mathcal{O}, R, R^\times) := \{\alpha : \mathcal{O} \to R\}/\sim,$$

where $\alpha \sim \beta$ if and only if $\alpha = \xi\beta\xi^{-1}$ for some $\xi \in R^\times$. Theorem 30.4.7 in [Voi21] states for $i \in \{1, 2\}$ that

$$\sum_{j=1}^{n} \#\mathrm{Emb}(\mathcal{O}_i, R_j, R_j^\times) = 2h_i.$$

Therefore, this set is in bijection with the set of elliptic curves with CM by $\mathcal{O}_i$ as considered above if we identify embeddings if they are equal after applying the involution on B_ℓ. This bijection suggests that $\mathrm{Pic}(K_i)$ acts on this set too and indeed that is so; we explore this further in Section 4.5. We stress here that we count each maximal order separately for each time it occurs as the right order of a left ideal class in the class group of B_ℓ, which can happen either once or twice, as explained in the first two sections of [Gro87].

Let $\mathfrak{l}$ be a prime above the prime number ℓ in the compositum of the fields $\mathbb{Q}(j(E_1))$ and $\mathbb{Q}(j(E_2))$, and let $v_\mathfrak{l}$ denote the $\mathfrak{l}$-adic valuation. Since ℓ is assumed inert in both K_i, it must split completely in the extension H_i/K_i for $i \in \{1, 2\}$. As such, the prime ℓ must split completely in $\mathbb{Q}(j(E_i))/\mathbb{Q}$ as well, and so both the set of primes $\mathfrak{l}$ above ℓ and the set of pairs of CM elliptic curves (E_1, E_2) up to isomorphism are principal homogeneous spaces for the action of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$.

We may consider both E_1 and E_2 to be defined over $\mathbb{Q}(j(\tau_1), j(\tau_2))$, and we wish to determine

$$v_\mathfrak{l}\big(j_1(E_1) - j_2(E_1)\big).$$

In the previous section, we considered the reductions of E_1 and E_2 modulo $\mathfrak{l}$ and appealed to Theorem 1.2.5. Alternatively, one may note that the reduction maps induce embeddings $\alpha_i : \mathcal{O}_i \to \mathrm{End}(\overline{E}_i) \subset B_\ell$. Varying $\mathfrak{l}$, for both curves we get different reductions over $\overline{\mathbb{F}}_\ell$, which may induce embeddings into different maximal orders.

We write Γ_1 and Γ_2 for the subgroups stabilising the images of α_1 and α_2 respectively. It is easy to show that for $i \in \{1, 2\}$, it holds that $\#\Gamma_i = \#\mathcal{O}_i^\times$. As B_ℓ is a definite quaternion algebra, the group $R^\times$ is finite for any maximal order $R \subset B_\ell$. We will need the following definition, in the style of the PhD thesis of James Rickards [Ric21].

Definition 1.3.1. Let $i, j \in \{1, \dots, n\}$ and let $\alpha_1 : \mathcal{O}_1 \to R_i$ and $\alpha_2 : \mathcal{O}_2 \to R_j$ be two embeddings. If $i = j$, define the *intersection number* $(\alpha_1 \cap \alpha_2)_\ell$ to be the greatest $t \in \mathbb{N}$ for which $\mathrm{im}(\alpha_1)$ and $\mathrm{im}(\alpha_2)$ agree modulo $\ell^{t-1}R_i = \ell^{t-1}R_j$. If $i \neq j$, we set $(\alpha_1 \cap \alpha_2)_\ell = 0$.

It should be noted that embeddings into the same maximal order always have a positive intersection number. However, even if $R_i = R_j$ as sets but $i \neq j$, we still say that embeddings into R_i and R_j do not intersect. We now claim the following theorem.

Theorem 1.3.2. *Let E_1 and E_2 be elliptic curves with complex multiplication by $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively and let ℓ be a rational prime that is inert in both $\mathcal{O}_1$ and $\mathcal{O}_2$. Let $\mathfrak{l}$ be a prime of $\mathbb{Q}(j(E_1), j(E_2))$ above ℓ and let $\alpha_1 : \mathcal{O}_1 \to R_i$ and $\alpha_2 : \mathcal{O}_2 \to R_j$ for some $i, j \in \{1, \dots, n\}$ be the pair of embeddings that corresponds to it. Suppose that both E_1 and E_2 have good reduction at $\mathfrak{l}$. If $i \neq j$, then $\mathfrak{l} \nmid j(E_1) - j(E_2)$. If $i = j$, then*

$$v_{\mathfrak{l}}\big(j(E_1) - j(E_2)\big) = \sum_{\Gamma_1 \backslash R^\times / \Gamma_2} \big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell,$$

where $R = R_i = R_j$ and $u \in \Gamma_1 \setminus R^\times / \Gamma_2$.

Proof. For the sake of exposition, we assume throughout the proof that $D_i \notin \{-3, -4\}$ for $i \in \{1, 2\}$, so that $\Gamma_1 \setminus R^\times / \Gamma_2 = R^\times / \{\pm 1\}$.

We appeal to Theorem 1.2.5 to reduce to showing that

$$2 \sum_{R^\times / \{\pm 1\}} \big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell = \sum_{n \geq 1} \mathrm{Iso}_n(E_1, E_2).$$

Clearly both curves are supersingular at $\mathfrak{l}$. Theorem 1.2.6 immediately yields that $\overline{E}_1 \cong \overline{E}_2$ if and only if $i = j$. This proves the result in case $i \neq j$, for $\mathfrak{l} \mid j(E_1) - j(E_2)$ if and only if $\overline{E}_1 \cong \overline{E}_2$.

Now assume that $i = j$, so $\overline{E}_1 \cong \overline{E}_2$ and therefore $\mathrm{Iso}_1(E_1, E_2) \neq \varnothing$. We will prove the theorem by establishing for any n a bijection between $\mathrm{Iso}_n(E_1, E_2)$ and the set of $u \in R^\times / \{\pm 1\}$ such that

$$\big(\alpha_1 \cap (u\alpha_2 u^{-1})\big)_\ell \geq n,$$

from which the desired equality would immediately follow.

Let us first illustrate the simple case of $n = 1$. Then, the isomorphisms from E_1 to E_2 over $\overline{\mathbb{F}}_\ell$ are in bijection with the automorphisms of either $\overline{E}_i$ over that same field, which thus biject with $R^\times$. On the other hand, any $u \in R^\times$ will contribute at least 1 to the sum of intersection numbers on the left hand side. The factor of 2 makes up for our

dividing out by $\{\pm 1\}$. This concludes this case. For $n > 1$, we suppose that $\mathrm{Iso}_n(E_1, E_2) \neq \varnothing$, so there exists some isomorphism $f : E_1 \mod \ell^n \xrightarrow{\sim} E_2 \mod \ell^n$. As explained in the previous section, through the association $f \mapsto g_f := f^{-1} \circ [x_2] \circ f$ we obtain for each element $f \in \mathrm{Iso}_n(E_1, E_2)$ a unique endomorphism $g_f \in \mathrm{End}(E_1 \mod \ell^n)$ that satisfies the same equation as some fixed x_2 with $\mathcal{O}_2 = \mathbb{Z}[x_2]$. First note that $g_f \in \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R$. Indeed, from the explicit description of $\mathrm{End}(E_1 \mod \ell^n)$ from the previous section, we deduce, using the observation that $\ell^{n-1} \mid \beta$, that

$$\mathrm{End}(E \mod \ell^n) \equiv \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} \right\} = \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R,$$

where we also used that modulo ℓ^{n-1}, there is no difference between taking α inside $\mathcal{O}_1$ or D_{K_1} by the coprimality of D_1 with ℓ. The element g_f for each $f \in \mathrm{Iso}_n(E_1, E_2)$ defines an embedding $\mathcal{O}_2 \to R$. This embedding must be conjugate to α_2 through an element $u \in R^\times$ and by construction, the images of these embeddings must agree $\mod \ell^{n-1}R$. This element u is only uniquely defined in the group $R^\times/\{\pm 1\}$, so the association we constructed is injective. It remains to show that it is also surjective for each $n \geq 1$. Now suppose that some embedding $\beta_2 = u^{-1}\alpha_2(-)u : \mathcal{O}_2 \to R$ agrees with $\alpha_1 : \mathcal{O}_1 \to R$ modulo $\ell^{n-1}R$. Then in particular, we find that $\beta_2(x_2) \in \alpha_1(\mathcal{O}_1) \mod \ell^{n-1}R$. Using the isomorphism from Lemma 3.5 in [GZ84] as above, we conclude that it even holds that $\beta(x_2) \in \mathrm{End}(E \mod \ell^n)$ with trace, norm and action on $\mathrm{Lie}(E_1)$ identical to the element $x_2 \in \mathcal{O}_2$. As reasoned in the beginning of Section 3 of [GZ84], using their Proposition 2.7, every endomorphism with these properties must be of the form $f^{-1} \circ [x_2] \circ f$ for some $f \in \mathrm{Iso}_n(E_1, E_2)$. This proves surjectivity. □

1.4 Extended example

We illustrate Theorem 1.3.2 using the following singular moduli;

$$\begin{aligned} j\left(\frac{1+\sqrt{-67}}{2}\right) &= -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3; \\ j\left(\frac{1+\sqrt{-163}}{2}\right) &= -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3; \\ j\left(\frac{1+\sqrt{-67}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) &= 2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 139 \cdot 331. \end{aligned}$$

We will verify the formula from Theorem 1.3.2 for various rational primes. Throughout this section, we will for $x, y \in \mathbb{Q}^\times$ adopt the notation $(x,y)_\mathbb{Q}$ for the quaternion algebra over $\mathbb{Q}$ with the explicit $\mathbb{Q}$-basis

$$(x,y)_\mathbb{Q} := \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

with the multiplication rules

$$i^2 = x, \quad j^2 = y \quad \text{and} \quad ij = -ji = k.$$

The trace form is given by $\mathrm{tr}(a + bi + cj + dk) = 2a$, and the norm by

$$\mathrm{Nm}(a + bi + cj + dk) = a^2 - xb^2 - yc^2 + xyd^2.$$

The prime $\ell = 2$

The algebra $B_2 = \mathbb{H} = (-1,-1)_\mathbb{Q}$ is that of the *Hamilton quaternions*. Its unique maximal order (up to conjugacy) is given by

$$R_2 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2}.$$

Computing its units of norm 1 is equivalent to solving $a^2+b^2+c^2+d^2 = 1$ in integers, or all half-integers. This yields 24 solutions, so the group of interest $\Gamma_1 \setminus R_2^\times / \Gamma_2$ consists of 12 elements.

To give embeddings of the rings of integers $\mathbb{Z}[(1+\sqrt{-67})/2]$ and $\mathbb{Z}[(1+\sqrt{-163})/2]$ into R_2, we must find quaternions satisfying

$$x^2 - x + 17 = 0 \quad \text{and} \quad x^2 - x + 41 = 0$$

respectively. This means that we are looking for $x \in R_2$ satisfying $\mathrm{tr}(x) = 1$ and $\mathrm{nrd}(x) = 17$ or $\mathrm{nrd}(x) = 41$ respectively. Clearly, the first condition amounts to specifying $a = 1/2$, so all other coefficients are half integers, and we reduce to expressing 67 and 163 as the sum of three odd squares respectively. We find among the solutions

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1 \pm 3i \pm 3j \pm 7k}{2}$$

and

$$\alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1 \pm 9i \pm 9j \pm k}{2}.$$

Since the images x and $1-x$ are considered to induce the same embedding, one easily finds all 12 embeddings from the above examples for both discriminants.

To examine the formula from Theorem 1.3.2, we note that, since the quaternion algebra has a unique maximal order, by definition each of the 12 terms in the sum contributes at least 1. This already gives us 12 factors of 2, so we are left to justify the remaining $15 - 12 = 3$.

We let α_1 be given by the embedding above with only plus signs and investigate for which choices of α_2 the images of the embeddings agree modulo $2R_2$. One checks that this means that the coefficients in the numerators of the generators must all agree mod 4. This gives us

$$\frac{1-9i-9j-k}{2}, \quad \frac{1-i-9j-9k}{2}, \quad \text{and} \quad \frac{1-9i-j-9k}{2}.$$

One verifies that in each case, these elements do not agree modulo $4R_2$. We have thus found three embeddings for which the intersection number is 2. This brings our final number of factors of 2 in the difference to $9 + 2 \cdot 3 = 15$, as predicted by Theorem 1.3.2.

The prime $\ell = 3$

To analyse the situation at the prime $\ell = 3$, we must introduce $B_3 = (-1, -3)_{\mathbb{Q}}$. It has a maximal order given by

$$R_3 = \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k.$$

This time, we obtain 12 units of norm 1, so after dividing out by ± 1, the group $\Gamma_1 \backslash R_3^{\times} / \Gamma_2$ contains 6 elements. To construct the embeddings α_1 and α_2, we are again looking for elements of norms 17 and 41 respectively, of which the rational part equals 1/2. Similar to before, we find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+j}{2} + 2i + 2k.$$

For α_2, all possible images are given by

$$\frac{1 \pm 7j}{2} \pm i \pm k \quad \text{and} \quad \frac{1 \pm 7j}{2} \pm 2i.$$

Again, all of these embeddings contribute at least 1 to the sum of intersection numbers from Theorem 1.3.2, meaning that we have already found at least 6 factors of 3 in the difference between the j-invariants. Now we are left to compare the image of α_1 to the image of every possibility for α_2 modulo $3R_3$. One verifies that only $\frac{1+7j}{2} - i - k$ will do the trick. However, modulo $9R_3$, these images are distinct. This means that we get an intersection number of 2 for one embedding, bringing our final total of factors of 3 to $5 \cdot 1 + 2 = 7$, once more in accordance with our computations.

The prime $\ell = 5$

We once again start by introducing the quaternion algebra $B_5 = (-2, -5)_{\mathbb{Q}}$. Its unique conjugacy class of maximal orders has the representative

$$R_5 = \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + \mathbb{Z}k.$$

Now we find 6 units in total, so that the group $\Gamma_1 \setminus R_5^\times / \Gamma_2$ consists of 3 elements. Examples of the embeddings are

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{2+3i+5k}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{2+9i+7k}{4}.$$

The only other possibilities for the image of α_2 are

$$\frac{2-9i-7k}{4} \quad \text{and} \quad \frac{1}{2} \pm \left(\frac{11}{4}i - \frac{3}{4}k\right) \pm 2j.$$

We leave it to the reader to check that these are the only choices of signs that produces an element in R_5. There are no congruences to be found this time, yielding 3 factors of 5, as Theorem 1.3.2 predicts.

The prime $\ell = 7$

We continue to study $B_7 = (-1, -7)_{\mathbb{Q}}$. It has the maximal order

$$R_7 = \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k.$$

It is easy to see that in this case, we only have ± 1 and $\pm i$ as units of norm 1, so $\Gamma_1 \setminus R_5^\times / \Gamma_2$ has order 2. As for the embeddings, we find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+2i+3j}{2} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1 \pm 10i \pm 3j}{2}$$

indeed giving us the $4/2 = 2$ embeddings that we expected. One checks that no choice of signs will result in orders that agree modulo $7R_7$. Therefore, both embeddings will only contribute 1 to the sum, giving 2 factors of 7 in total, once more as expected by Theorem 1.3.2.

The primes $\ell = 11$

This example is interesting because it is the smallest prime for which there is not a unique maximal order, but in fact there are two distinct conjugacy classes. We have $B_{11} = (-1, -11)_{\mathbb{Q}}$ and

$$R_{11}^1 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}\frac{1+j}{2}$$

and

$$R_{11}^2 = \mathbb{Z}\frac{1+j+2k}{2} + \mathbb{Z}\frac{i+2j+5k}{4} + \mathbb{Z}j + 2\mathbb{Z}k$$

are two representatives. For the possible embeddings, we only find

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{1+13i-3k}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{1+3j}{2} + 4i.$$

We see that α_1 and α_2 embed into different maximal orders of B_{11}, thus giving intersection number zero. Indeed, we did not find any factors of 11 in our difference of j-invariants.

The primes $\ell \geq 13$

For our last small prime that we will check, we record that $B_{13} = (-2,-13)_{\mathbb{Q}}$ and now there is a unique conjugacy class of maximal order again, given by

$$R_{13} = \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + \mathbb{Z}k.$$

The units of norm 1 are given by ± 1, so that we will get *unique* embeddings α_1 and α_2, given by

$$\alpha_1\left(\frac{1+\sqrt{-67}}{2}\right) = \frac{2 \pm (11i+k)}{4} \quad \text{and} \quad \alpha_2\left(\frac{1+\sqrt{-163}}{2}\right) = \frac{2 \pm (i-5k)}{4}.$$

A moment's inspection now shows that these embeddings do not agree modulo $13R_{13}$, thus giving an intersection number of 1. We therefore get 1 factor of 13 in the difference of j-invariants, as expected from the numbers themselves and Theorem 1.3.2.

For embeddings α_1 and α_2 to exist in the first place, the prime ℓ must be inert in both K_1 and K_2. In our case, this already shows that our difference in j-invariants will have no factors of ℓ for all $13 < \ell < 31$. Using this elementary observation, we may already disregard 75% of all primes from our considerations. Of those that remain, one should find that only for $\ell = 139$ and $\ell = 331$ there will be embeddings that map into the same maximal order; for all other primes, the embeddings will land inside distinct maximal orders. The number of distinct maximal orders grows approximately as $\ell/12$ as ℓ increases; a precise formula can be found in the first chapter of [Gro87]. Therefore, it will become increasingly unlikely that two embeddings will belong to the same maximal order, thus contributing a prime factor to the difference of j-invariants.

1.5 Irrational examples

To illustrate the way in which Theorem 1.3.2 is in some sense more refined than Theorem 1.2.1, we must consider irrational singular moduli. Recall that the field $\mathbb{Q}(\sqrt{-5})$ has class number 2, whereas $\mathbb{Q}(\sqrt{5})$ has class number 1. In this section, we will consider the following values:

$$\begin{aligned} j\left(\sqrt{-5}\right) &= 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}); \\ j\left(\frac{1+\sqrt{-7}}{2}\right) &= -3^3 \cdot 5^3; \\ j\left(\sqrt{-5}\right) - j\left(\frac{1+\sqrt{-7}}{2}\right) &= (2+\sqrt{5}) \cdot 5\sqrt{5} \cdot 13 \cdot 17 \cdot (8+3\sqrt{5}) \cdot (6+\sqrt{5}). \end{aligned}$$

Note that $\mathrm{Nm}(2+\sqrt{5}) = 2^2 - 5 = -1$, so the first factor is a mere unit. Also, $\mathrm{Nm}(8+3\sqrt{5}) = 8^2 - 5 \cdot 3^2 = 19$ and $\mathrm{Nm}(6+\sqrt{5}) = 6^2 - 5 = 31$, so that the last two factors represent primes above 19 and 31 respectively. These will be the most interesting primes for us.

The case $\ell = 19$

We start by writing $B_{19} = (-1,-19)_{\mathbb{Q}}$, which has two distinct conjugacy classes of maximal orders, given by

$$\begin{aligned} R_{19}^1 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k; \\ R_{19}^2 &= \mathbb{Z}\frac{1+j+2k}{2} + \mathbb{Z}\frac{i+2j+k}{4} + \mathbb{Z}j + 2\mathbb{Z}k. \end{aligned}$$

Using this, it is easy to establish that in R_{19}^1 the units are given by ± 1 and $\pm i$, whereas in R_{19}^2 the only units are given by ± 1. We expect to find two different $R_{19}^{i,\times}$-conjugacy classes of embeddings of $\mathbb{Z}[\sqrt{-5}]$, corresponding to its class number. We are looking for traceless elements of norm 5, and naively one would find $\frac{\pm i \pm j}{2}$ and $\frac{\pm i \pm k}{2}$ as the only possibilities. Only the latter family lands in one of the above two maximal orders. In fact, it is contained in *both* maximal orders, provided we choose the right signs in the case of R_{19}^2. We therefore must interpret the two distinct families of embeddings as

$$\alpha_1^1(\sqrt{-5}) = \frac{i+k}{2} \in R_{19}^1 \quad \text{and} \quad \alpha_1^2(\sqrt{-5}) = \frac{i+k}{2} \in R_{19}^2.$$

The situation for the other seems more familiar, as there we expect and find only the embedding

$$\alpha_2\left(\frac{1+\sqrt{-7}}{2}\right) = \frac{1}{2} \pm \frac{3i-k}{4} \in R_{19}^2.$$

So we are left to interpret these results properly. Each of the two embeddings α_1 corresponds to one of the primes above 19 in the factorisation of the difference between singular moduli. The first embeds into R_{19}^1, and thus when comparing it to the embedding α_2 landing inside R_{19}^2, they have intersection number 0. The second embedding does reach R_{19}^2, so for each of the embeddings α_2, of which there is only one, we get a prime factor. This is the single factor of the prime above 19 that we observe in the factorisation, in perfect accordance with Theorem 1.3.2.

The case $\ell = 31$

To illustrate the arithmetic complexity of the right hand side of Theorem 1.3.2, we conclude this example by analysing the algebra $B_{31} = (-1,-31)_{\mathbb{Q}}$. This has *three* distinct conjugacy classes of maximal orders, representatives of which are given by

$$\begin{aligned} R_{31}^1 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i+k}{2} + \mathbb{Z}j + \mathbb{Z}k; \\ R_{31}^2 &= \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{i-k}{4} + \mathbb{Z}j + 2\mathbb{Z}k. \\ R_{31}^3 &= \mathbb{Z}\frac{3+i+j-k}{6} + 2k + \mathbb{Z}\frac{i+j-k}{3} + \mathbb{Z}\frac{i+k}{2} + 3\mathbb{Z}k. \end{aligned}$$

The units in R_{31}^1 are ± 1 and $\pm i$, whereas the other two orders only contain ± 1. Searching for the possible embeddings α_1 leaves us with

$$\alpha_1^1(\sqrt{-5}) = \pm\frac{7i+k}{4} \in R_{31}^2 \quad \text{and} \quad \alpha_1^2(\sqrt{-5}) = \pm\frac{5i+2j+k}{6} \in R_{31}^3.$$

For the other we indeed find a single embedding,

$$\alpha_2\left(\frac{1+\sqrt{-7}}{2}\right) = \frac{1}{2} \pm \frac{i+j-k}{6} \in R_{31}^3.$$

We find ourselves in a very similar situation as before. Indeed, the embedding α_1^1 reaches a different maximal order than α_2, and so for one of the two primes above 31 we will not get any factors. For the other, however, the unicity of α_2 gives us via α_1^2 one factor, as expected from Theorem 1.3.2.

Two irrational non-singular moduli

Let us conclude our numerous illustrative examples with one in which both singular moduli are irrational. To be precise, we explore

$$\begin{aligned} j\left(\sqrt{-5}\right) &= 2^6 \cdot 5 \cdot (1975 + 884\sqrt{5}); \\ j\left(\sqrt{-13}\right) &= -2^6 \cdot 3^3 \cdot 5^3 \cdot (15965 + 4428\sqrt{13}); \\ j\left(\sqrt{-5}\right) - j\left(\frac{1+\sqrt{-7}}{2}\right) &= 2^8 \cdot 5 \cdot (2693600 - 221\sqrt{5} + 747225\sqrt{13}). \end{aligned}$$

Factoring this difference is a tad tricky, so for now we will content ourselves with its norm

$$2^{40} \cdot 5^6 \cdot 13^2 \cdot 37^2 \cdot 139 \cdot 179 \cdot 211 \cdot 251.$$

We will focus on the prime $\ell = 37$. Even though the discriminants -20 and -52 are not in fact coprime, one only expects the formula to fail for the shared prime 2, so we are free to consider the prime $\ell = 37$ here. One final time, we introduce $B_{37} = (-2, -37)_{\mathbb{Q}}$, which has three conjugacy classes of maximal orders, of which only two are distinct, which is caused by two of the ideal classes in the quaternion algebra having the same maximal order. This is actually the smallest prime at which this phenomenon occurs. The maximal orders are then given by

$$\begin{aligned} R_{37}^1 &= \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{2-i+k}{4} + \mathbb{Z}\frac{1-i+j}{2}; \\ R_{37}^2 = R_{37}^3 &= \mathbb{Z}\frac{1+j+k}{2} + \mathbb{Z}\frac{i+6j+k}{8} + \mathbb{Z}(j+k) + 2\mathbb{Z}k. \end{aligned}$$

All orders only have the numbers ± 1 as units. For the possible images of $\sqrt{-5}$ we find

$$\alpha_1(\sqrt{-5}) = \pm\frac{7i+2j-k}{8} \in R_{37}^2 = R_{37}^3.$$

For the images of $\sqrt{-13}$, we establish

$$\alpha_2(\sqrt{-13}) = \pm\frac{3i+2j+3k}{8} \in R_{37}^2 = R_{37}^3.$$

We reiterate that the order $R_{37}^2 = R_{37}^3$ is to be considered twice; once for each ideal class. Namely, in doing so, for each of the two (identical) embeddings α_1, we find that only one of the two (identical) embeddings α_2 lands in the *same* order, hence contributing a factor of some prime above 37. Hence we have explained the two factors of 37 in the above norm, which is what we sought to do.

1.6 Analytic proof

Whereas the first proof of Theorem 1.2.1 in [GZ84], outlined in Section 1.2, made use of CM-theory, the other analysed a family of Hilbert Eisenstein series. More precisely, the second strategy employed by Gross and Zagier in [GZ84] was to consider a family $E_{1,\chi}(s)$ of non-holomorphic parallel weight 1 Hilbert Eisenstein series, indexed by a complex parameter s. Some of the properties of its $s = 0$-specialisation $E_{1,\chi}$ are described in Section A.2 in Appendix A. For the ideal class of the inverse different $\mathcal{D}_F^{-1}$, this specialisation vanishes, which implies that the first derivative of this family with respect to the weight parameter s, is a meaningful object to study.

Gross and Zagier in [GZ84] studied the *diagonal restriction*, denoted by Δ below, of this first derivative with respect to the weight-parameter s, which must be a real analytic modular form of weight 2 for $\mathrm{SL}_2(\mathbb{Z})$. One then applies the *holomorphic projection* operator e^{hol} to find

$$e^{\mathrm{hol}}\left(\Delta \frac{d}{ds} E_{1,\chi}(s)\Big|_{s=0}\right) \in M_2(\Gamma_0(1)) = \{0\}. \tag{1.2}$$

Most of the effort that goes into this analytic proof of Theorem 1.2.1 is to compute the Fourier coefficients of the expression on the left hand side, without appealing to its eventual vanishing as found above. With careful analysis to circumvent convergence issues, one finds that the first of these coefficients splits up in two terms; one equal to the logarithm of the norm of $j(\tau_1) - j(\tau_2)$, and the other to the logarithm of the explicit formula that was to be proved. It is crucial to note that this proof does not use any CM-theory whatsoever. It is a p-adic analogue of this proof that will be the main focus of this thesis.

To understand this approach in greater detail, we would need to explain why both the difference between the two j-invariants occurs as a result of these operations, as well as the finite elementary formula from Theorem 1.2.1. Let us start with the difference between j-invariants.

Roughly, a *Green's function* $G(x, y)$ on a Riemann surface X with a distinguished point ∞ is a symmetric function with the property that for fixed $y \in X$, the function $G(-, y)$ is harmonic on $X \setminus \{y, \infty\}$, having a log-pole at the removed points. If such a function exists, it must be unique up to a constant and this function can then be used to define an archimedean height pairing between certain divisors on X. On $\mathbb{P}^1$, there is an obvious choice for such a function: $G(x, y) = \log|x - y|^2$. Therefore, the function

$$\log|j(\tau_1) - j(\tau_2)|^2 : (\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H})^2 \to \mathbb{C}$$

is a natural Green's function on $\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$. There are general strategies to construct Green's functions on modular curves, however. To this end, we define the weight 0 Eisenstein series

$$E(\tau,s) := \frac{1}{2}\sum_{\substack{c,d\in\mathbb{Z}\\ \gcd(c,d)=1}} \frac{\mathrm{im}(\tau)^s}{|c\tau+d|^{2s}}.$$

Next, one constructs a function $G_s(x,y)$ using an average over $\mathrm{SL}_2(\mathbb{Z})$ of functions built from a Legendre function Q_{s-1} of the second type. One may then show that

$$\lim_{s\to 1} G_s(\tau_1,\tau_2) + 4\pi E(\tau_1,s) + 4\pi E(\tau_2,s) - 4\pi\varphi(s) - 24,$$

describes another Green's function on $\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$, where φ is a function expressed in elementary terms. Comparing their asymptotics, it follows that it must equal $\log|j(\tau_1)-j(\tau_2)|^2$. Next, one proves the expression

$$\frac{4}{w_1w_2}G_s(\tau_1,\tau_2) = -2\sum_{\substack{n>\sqrt{D}\\ n\equiv D \bmod 2}} \mu(n)Q_{s-1}\left(n/\sqrt{D}\right), \tag{1.3}$$

where the numbers $\mu(n)$ are integers related to a certain counting problem for integral binary quadratic forms. These numbers can be shown to be linked to the explicit formula that appears in Theorem 1.2.1.

The non-holomorphic Hilbert Eisenstein series $E_{1,\chi}(z,z',s)$ introduced by Hecke of weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$ is defined by

$$\sum_{[\mathfrak{a}]\in\mathrm{Pic}(F)^+}\chi(\mathfrak{a})\mathrm{Nm}(\mathfrak{a})^{1+2s}\sum_{\substack{(m,n)\in\mathfrak{a}^2/\{\pm1\}\\ (m,n)\neq(0,0)}}\frac{y^sy'^s|mz+n|^{-2s}|m'z'+n'|^{-2s}}{(mz+n)(m'z'+n')},$$

where $z=x+iy$ and $z'=x'+iy'$, which specialises to the Hilbert Eisenstein series $E_{1,\chi}$ for $s=0$. The Fourier expansion of this object is known, and this allows one to compute the diagonal restriction of the derivative

$$\frac{d}{ds}E_{1,\chi}(z,z,s)|_{s=0}.$$

By construction, this function on $\mathcal{H}$ transforms like a modular form of weight 2 under the action of $\mathrm{SL}_2(\mathbb{Z})$ and is asymptotically given by $A\log(y)+B+O(y^{-\epsilon})$ for some $A,B\in\mathbb{C}$ and $\epsilon>0$. We can write this function as a Fourier expansion of the form

$$\sum_{m=-\infty}^{\infty} a_m(y)e^{2\pi imz}.$$

A result of Sturm then allows us to compute the *holomorphic projection*, the first coefficient of which is defined by

$$\lim_{s\to 0}\left(4\pi\int_0^\infty a_1(y)e^{-4\pi y}y^s\ dy+\frac{24A}{s}\right).$$

This result must vanish, since the computed object is now contained in $M_2(\Gamma_0(1))=\{0\}$. Performing the computation, we find the same terms appearing as in Equation 1.3, establishing an equality and ultimately the result of Theorem 1.2.1.

The results of [GZ84] and [GKZ87] show that the outcome of this procedure for a family of Hilbert Eisenstein series, consisting of taking a diagonal restriction, a derivative and a holomorphic projection, is very generally related to the height pairing of certain divisors on the relevant modular curves. Since these height pairings are given by Green's functions and $\log|j(\tau_1)-j(\tau_2)|^2$ describes such a Green's function, the appearance of the difference between singular moduli in the result of this computation, need not be surprising. In fact, it is the vanishing of this height pairing, by virtue of the genus of the curve $Y_0(1)=\mathrm{SL}_2(\mathbb{Z})\setminus\mathcal{H}$ being zero, that ensures the algebraicity of this difference, as opposed to its transcendence.

We conclude this section by sketching a more direct connection between the logarithm of the explicit elementary formula that occurs in Theorem 1.2.1 and the diagonal restriction of the derivative with respect to the weight parameter of a family of Hilbert modular forms specialising to $E_{1,\chi}$. Recall that an ideal $\mathfrak{m}\subset\mathcal{O}_F$ is said to be *primitive* if it is not divisible by any rational prime. We need the following result.

Proposition 1.6.1. *Let $\mathfrak{m}\subset\mathcal{O}_F$ be a primitive ideal with at least one special prime. Then*

$$\log(F(\mathrm{Nm}(\mathfrak{m})))=-\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)).$$

Proof. Let us abbreviate the equality and conditions from the proposition to saying that $(*)$ holds. We use implicit induction to extend the set of ideals $\mathfrak{m}$ for which we know that $(*)$ holds until we have reached the full set of primitive integral ideals with $\chi(\mathfrak{m})=-1$.

Throughout, we let r be a rational prime that is not inert in $F/\mathbb{Q}$ and we let $\mathfrak{r}\subset\mathcal{O}_F$ be a prime above it. We assume that $r\nmid\mathrm{Nm}(\mathfrak{m})$.

First suppose that $\chi(\mathfrak{r}) = -1$. We will show that $(*)$ holds for $\mathfrak{r}^{2k+1}$ for any non-negative integer k. Indeed, we compute that

$$\sum_{I|\mathfrak{r}^{2k+1}} \chi(I)\log(\mathrm{Nm}(I)) = \log(r)\sum_{n=0}^{2k+1}(-1)^n n = -(k+1)\log(r);$$

which by definition equals $-\log(F(r^{2k+1}))$.

Suppose now that $(*)$ holds for $\mathfrak{m}$ and suppose that $\chi(\mathfrak{r}) = 1$. We claim that $(*)$ also holds for $\mathfrak{m}\mathfrak{r}^k$ for any $k > 0$. We compute that

$$\begin{aligned}\sum_{I|\mathfrak{m}\mathfrak{r}^k} \chi(I)\log(\mathrm{Nm}(I)) &= \sum_{n=0}^{k}\sum_{I|\mathfrak{m}} \chi(I\mathfrak{r}^n)\log(\mathrm{Nm}(I\mathfrak{r}^n)) \\ &= (k+1)\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)) + \sum_{n=0}^{k} n\log(r)\sum_{I|\mathfrak{m}}\chi(I) \\ &= -(k+1)\log(F(\mathrm{Nm}(\mathfrak{m})) = -\log(F(\mathrm{Nm}(\mathfrak{m}\mathfrak{r}^k))\end{aligned}$$

where we used Lemma A.2.10 and the observation that having a special prime means that $\rho(\mathfrak{m}) = 0$, as follows from its proof.

Suppose now that $(*)$ holds for $\mathfrak{m}$ and suppose that $\chi(\mathfrak{r}) = -1$. We claim that $(*)$ also holds for $\mathfrak{m}\mathfrak{r}^k$ for any $k > 0$. We compute that

$$\begin{aligned}\sum_{I|\mathfrak{m}\mathfrak{r}^k} \chi(I)\log(\mathrm{Nm}(I)) &= \sum_{n=0}^{k}\sum_{I|\mathfrak{m}} \chi(I\mathfrak{r}^n)\log(\mathrm{Nm}(I\mathfrak{r}^n)) \\ &= \sum_{n=0}^{k}(-1)^n\sum_{I|\mathfrak{m}}\chi(I)\log(\mathrm{Nm}(I)) + \sum_{n=0}^{k}(-1)^n n\log(r)\sum_{I|\mathfrak{m}}\chi(I) \\ &= \begin{cases} -\log(F(\mathrm{Nm}(\mathfrak{m})) & \text{if } k \text{ is even;} \\ 0 & \text{if } k \text{ is odd.}\end{cases}\end{aligned}$$

Here we again used Lemma A.2.10 in view of the information that $\mathfrak{m}$ has at least one special prime. If k is even, then by definition, $F(\mathrm{Nm}(\mathfrak{m})) = F(\mathrm{Nm}(\mathfrak{m}\mathfrak{r}^k))$, so the desired conclusion follows. If k is odd, then the ideal $\mathfrak{m}\mathfrak{r}^k$ would have more than 1 special prime. By definition, this causes the F-value of its norm to vanish, completing the proof of this case too. □

What follows is mostly heuristic, but it will hint at something profound. By Proposition 2.1 in [DDP11], for each positive integer k, there

exists a parallel weight k Hilbert modular form $E_{1,\chi}(k)$ with normalised Fourier coefficients $\mathfrak{m} \subset \mathcal{O}_F$ given by

$$a(\mathfrak{m}, E_{1,\chi}(k)) = \sum_{I|\mathfrak{m}} \chi(I)\mathrm{Nm}(I)^{k-1},$$

of which the object from Proposition A.2.9 is the $k = 1$-specialisation. Of course, the parameter k is discrete, so naively taking a derivative with respect to this weight parameter, is mathematically unsound. Disregarding this and formally doing so anyway, we would obtain

$$\frac{d}{dk} a(\mathfrak{m}, E_{1,\chi}(k)) = \sum_{I|\mathfrak{m}} \chi(I)\log(\mathrm{Nm}(I))\mathrm{Nm}(I)^{k-1}.$$

As such, specialising at $k = 1$ would yield

$$\frac{d}{dk} a(\mathfrak{m}, E_{1,\chi}(k))|_{k=1} = \sum_{I|\mathfrak{m}} \chi(I)\log(\mathrm{Nm}(I)),$$

which is the same quantity as appears in Proposition 1.6.1. We now consider the diagonal restriction of this hypothetical object for the ideal class $\mathcal{D}_F^{-1}$. The nth Fourier coefficient of the result will introduce a sum over all elements $\nu \in \mathcal{D}_F^{-1,+}$ of fixed trace n. It is easy to check that these elements are precisely those integral elements of the form $\nu = (x + n\sqrt{D})/2\sqrt{D}$ where $x^2 < n^2 D$. Putting all these observations together, we obtain for the first coefficient of the result the expression

$$\sum_{\nu \in \mathcal{D}_F^{-1,+}} \sum_{I|\nu\mathcal{D}_F} \chi(I)\log(\mathrm{Nm}(I)) = \sum_{\substack{x^2<D \\ x^2 \equiv D \bmod 4}} \log F\left(\frac{D-x^2}{4}\right);$$

this is the right hand side of Theorem 1.2.1.

Even though this argument is heuristic and not rigorous, it still illustrates why the precise order of operations as carried out by Gross and Zagier in [GZ84] might lead to an explicit formula as it appears in Theorem 1.2.1. Indeed, taking a derivative with respect to the weight parameter and subsequently a diagonal restriction seems to produce the terms that we are after. As we will explain in the next chapter, this deep phenomenon seems to allow itself for various generalisations, of which this thesis is but one example. However, this still leaves much to be explored in the future.

CHAPTER 2

Main results

Ever since the conception of Theorem 1.2.1 by Gross and Zagier in [GZ84], people have searched for generalisations of these kinds of factorisation phenomena. One place for such investigations has been the arithmetic of Shimura curves; the main results of this thesis will be such generalisations. Major contributions to the field in this setting were previously achieved by Shou-Wu Zhang in [Zha01, YZZ13], vastly generalising the work of [GZ86, GKZ87] on modular curves to the Shimura curve setting. This thesis, however, will venture in a slightly direction.

2.1 Shimura curves over $\mathbb{C}$

To motivate the definition of Shimura curves, we recall that the open modular curve $Y_0(1)$ is defined as

$$Y_0(1) := \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}.$$

If $X_0(1)$ denotes its compactification by adding the cusp at infinity, the j-function exhibits an isomorphism

$$j : X_0(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

The group $\mathrm{SL}_2(\mathbb{Z})$ can be viewed as an index 2 subgroup of the unit group $\mathrm{GL}_2(\mathbb{Z})$ of the ring $M_2(\mathbb{Z})$, which in turn is a maximal order in the split quaternion algebra $M_2(\mathbb{Q})$. If we regard the determinant form $\det : M_2(\mathbb{Q}) \to \mathbb{Q}$ as the natural *norm* on the algebra $M_2(\mathbb{Q})$, then one may obtain the group $\mathrm{SL}_2(\mathbb{Z})$ from this quaternion algebra by first choosing a maximal order and subsequently considering the subgroup of units of norm 1. It is the generalisation of this procedure that defines the family of Shimura curves over $\mathbb{C}$ as we will consider them in this thesis.

Let N be a squarefree positive integer divisible by an even number of primes. Now let B_N denote the quaternion algebra over $\mathbb{Q}$ with discriminant N; that is, it is ramified at all primes dividing N, and is split at all other places. Since it is indefinite, it has a maximal order R_N that is unique up to conjugation and B_N can be embedded into $M_2(\mathbb{R})$. Choosing such a splitting, the subgroup $R_{N,1}^\times \subset R_N^\times$ consisting of all elements of unit norm can be regarded as acting on the complex upper half plane $\mathcal{H}$. In view of the above discussion, we now consider the quotient

$$X_N := R_{N,1}^\times \setminus \mathcal{H}.$$

This is called the *Shimura curve* of level N. In contrast to the case of $X_1 = X_0(1)$, if $N > 1$, we need not add any cusps, as one can show that

this quotient is already compact. Furthermore, as is the case for modular curves, X_N is an algebraic curve and in fact has a model defined over $\mathbb{Q}$.

Next, we observe that each element of the normaliser

$$\mathcal{N}(R_{N,1}^\times) = \left\{ b \in B_N^\times \mid bR_{N,1}^\times = R_{N,1}^\times b \right\}$$

induces an automorphism of the curve X_N. Indeed, the left-multiplication by b-map $\mathbb{C} \to \mathbb{C}$ decends to a map $X_N \to X_N$, as

$$b \cdot \left(R_{N,1}^\times z \right) = R_{N,1}^\times (b \cdot z) .$$

Clearly $\mathbb{Q}^\times R_{N,1}^\times \subset \mathcal{N}(R_{N,1}^\times)$, but all of these elements induce trivial automorphisms of X_N. The following lemma classifies what remains after this realisation.

Lemma 2.1.1. *The normaliser $\mathcal{N}(R_{N,1}^\times)$ satisfies*

$$\mathcal{N}(R_{N,1}^\times)/\mathbb{Q}^\times R_{N,1}^\times = \{ w_d \mid d > 0, \quad d \mid N \} \cong \prod_{r \mid N} \mathbb{Z}/2\mathbb{Z},$$

where the product $r \mid N$ is taken over all prime divisors r of N.

Proof. This is stated early in Chapter 43 of [Voi21]. □

This group is called the *Atkin-Lehner group* and is typically denoted by W_N. As the lemma above suggests, it is generated by commuting involutions w_r for every rational prime $r \mid N$. Note that for the modular curve $X_0(1)$ the Atkin-Lehner group is trivial, as $X_0(1)$ can be regarded as the $N = 1$-case of the construction above.

The following result is crucial for us, which will be a special case of Proposition 2.1 in [Pad23], which was originally proved by Ogg in [Ogg83].

Proposition 2.1.2. *Let φ denote the Euler totient function. Then the algebraic curve X_N has genus equal to*

$$g(X_N) = 1 + \frac{\varphi(N)}{12} - \frac{\epsilon_4(N)}{4} - \frac{\epsilon_3(N)}{3},$$

where for $k \in \mathbb{Z}$,

$$\epsilon_k(N) := \prod_{p \mid N} \left(1 - \left(\frac{-k}{p} \right) \right).$$

Corollary 2.1.3. *The Shimura curve X_N is of genus 0 if and only if*

$$N \in \{1, 6, 10, 22\}.$$

Proof. Clearly $g(X_1) = g(X_0(1)) = 0$. Let $N \in \mathbb{N}$ be such that $g(X_N) = 0$ and let $\tau(N)$ denote the number of primes dividing N. Suppose that we can find $\alpha, \beta, \gamma > 0$ such that

$$\varphi(N) \geq \alpha 2^{\tau(N)}\sqrt{N}, \quad \epsilon_4(N) \leq \beta 2^{\tau(N)} \quad \text{and} \quad \epsilon_3(N) \leq \gamma 2^{\tau(N)}.$$

Then it follows from Proposition 2.1.2 that

$$g(X_N) \geq 1 + 2^{\tau(N)}\frac{\alpha\sqrt{N} - 3\beta - 4\gamma}{12}, \text{ so } g(X_N) \geq 1 \text{ if } N \geq \left(\frac{3\beta + 4\gamma}{\alpha}\right)^2.$$

More sharply, if $\tau(N) = 2$, we even have that

$$g(X_N) \geq 1 + \frac{\alpha\sqrt{N} - 3\beta - 4\gamma}{3}, \text{ so } g(X_N) > 0 \text{ if } N > \left(\frac{3\beta + 4\gamma - 3}{\alpha}\right)^2.$$

To compute α, we note that

$$\frac{\varphi(N)}{2^{\tau(N)}\sqrt{N}} = \prod_{p|N}\frac{p-1}{2\sqrt{p}}, \quad \text{and} \quad \frac{p-1}{2\sqrt{p}} > 1 \quad \text{if} \quad p \geq 7.$$

If N is odd, then we may take $\alpha = 1/2$ and trivially $\beta = \gamma = 1$ to find that $g(X_N) \geq 1$ as soon as $N \geq 196$. Since $2 \cdot 3 \cdot 5 \cdot 7 > 196$, it follows that $\tau(N) = 2$, and therefore $g(X_N) > 0$ as soon as $N > 64$. If N contains a prime factor $p > 3$ that is not $-1 \mod 12$, then either $\epsilon_4(N) = 0$ or $\epsilon_3(N) = 0$ and we may take either $\beta = 0$ or $\gamma = 0$, to find $g(X_N) > 0$ always. This only leaves the curve X_{33}, but one checks that $g(X_{33}) = 1$.

Therefore N must be even, so henceforth we may take $\beta \leq 1/2$.

Suppose that N is not divisible by 3. Noting that indeed $g(X_{10}) = 0$ but $g(X_{14}) = 1$, we may assume that N contains a prime factor $p \geq 11$. We may then again take $\alpha = 1/2$, $\beta = 1/2$ and $\gamma = 1$ to find that $g(X_N) \geq 1$ as soon as $N \geq 121$. Thus again $\tau(N) = 2$ and we find $g(X_N) > 0$ as soon as $N > 25$. This leaves only the curve X_{22}, which indeed satisfies $g(X_{22}) = 0$.

It remains to study the case that $6 \mid N$, when we may also take $\gamma \leq 1/2$. Checking that $g(X_6) = 0$, we may assume that $\tau(N) \geq 4$. We may then take $\alpha = 1/5$, $\beta = \gamma = 1/2$ to find that $g(X_N) \geq 1$ as soon as $N > 306$. Since $2 \cdot 3 \cdot 5 \cdot 11 > 306$, this leaves only the curve X_{210}. But one checks that $g(X_{210}) = 5$, so the proof is complete. □

We assume throughout the rest of this thesis that $N \in \{6, 10, 22\}$. Then X_N admits an isomorphism

$$j_N : X_N \xrightarrow{\sim} \mathbb{P}^1,$$

which yields a generator j_N of the function field of X_N. However, in contrast to the modular curve case, we now longer have a cusp that we may use to normalise j_N in a natural way, as was done with Klein's j-function. As such, there is no canonical choice for this function j_N and it is so far defined only up to automorphism of $\mathbb{P}^1$. Recall that

$$\mathrm{Aut}(\mathbb{P}^1) \cong \mathrm{PGL}_2 \quad \text{through} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} [z_1 : z_2] := [az_1 + bz_2, cz_1 + dz_2].$$

If all primes dividing N are inert in some imaginary quadratic field K, we can find an embedding $\alpha : \mathcal{O}_K \to R_N$ and for each such embedding, there is a unique point $P \in \mathcal{H}$ fixed by the action of the image of the embeddings under the fixed splitting $B_N \to M_2(\mathbb{R})$. Then P is called the *CM-point* associated with the embedding α.

By Shimura's reciprocity law, as explained on the first pages of [Shi67], if j_N is chosen appropriately, the value $j_N(P)$ for a point $P \in X_N$ with complex multiplication by $\mathcal{O}_K$ is defined over the Hilbert class field H of the field K. In fact, this is a natural consequence of the adèlic *Main Theorem of Complex Multiplication* in the setting of Shimura curves, again see Theorem 4.19 in [Del71]. It requires only minimal adjustments compared to Theorem 1.1.1, illustrating the power of this formulation. For the sake of exposition, we specialise to the maximal compact open subgroup case.

Theorem 2.1.4. *Let $B_N/\mathbb{Q}$ be an indefinite quaternion algebra and let $N \in \mathbb{N}$ be its discriminant. Consider the following commutative diagram:*

$$\begin{array}{ccc} K^\times \setminus \mathbf{A}_K^{\mathrm{fin},\times} & \longrightarrow & B_N^\times(\mathbb{Q}) \setminus \left(\mathcal{H}^\pm \times B_N^\times(\mathbf{A}_{\mathbb{Q}}^{\mathrm{fin}})\right) \\ {\scriptstyle [-,K]}\downarrow & & \downarrow{\scriptstyle /\ B_N^\times(\widehat{\mathbb{Z}})} \\ \mathrm{Gal}(K^{\mathrm{ab}}/K) & \overset{\eta}{\dashrightarrow} & X_N(\mathbb{C}). \end{array}$$

Then the image of η is contained in $X_N(\overline{\mathbb{Q}})$ and η is Galois-equivariant.

As a result we have the following corollary; a version of Shimura reciprocity that we will need later.

Corollary 2.1.5. *For a CM point $P \in X_N$ associated with the embedding $\alpha : \mathcal{O}_K \to R_N$, it holds that $P \in X_N(H)$. Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal and let $x \in R_N$ be such that $\alpha(\mathfrak{a})R_N = xR_N$. Then*

$$P^{[\mathfrak{a},H_K/K]} = x^{-1} \cdot P \in X_N,$$

where $x^{-1} \cdot P$ is a CM-point for the embedding $x^{-1}\alpha(-)x : \mathcal{O}_K \to R_N$.

Proof. The power of the formulation of Theorem 2.1.4 lies in the fact that one may deduce Corollary 2.1.5 from it very similariy as to how we deduced Corollary 1.1.2 from Theorem 1.1.1. One merely needs to replace the algebraic group GL_2 by the algebraic group $B_N^\times$ and all arguments will go through without difficulty. □

With these algebraicity results known, and their strong analogy with the $X_0(1)$-setting from the previous chapter, one may wonder about a generalisation of Theorem 1.2.1 as proved by Gross and Zagier in [GZ84].

Elkies in [Elk98] numerically computed the CM-values for certain choices of a generator of the function field of certain *Atkin-Lehner quotients* of X_N, but not all values could be proved. However, the apparent smoothness of the resulting numbers did not go unnoticed. Using the theory of Borcherds lifts, Errthum in [Err11] was able to prove the correctness of many of Elkies's computations, but no conjectures as to the general structure of the values were posed. Some further explicit computations for particular choices of the generator of the function field can be found in [Voi09] and more general rational points on Atkin-Lehner quotients are studied in [Cla03].

Instead of choosing a function j_N, one may observe that the cross-ratio of its values is well-defined and independent of any choices. We recall that for any distinct x, y, z, w in some field, the cross-ratio is defined as

$$[x, y, z, w] := \frac{z - x}{z - y} \cdot \frac{w - y}{w - x}.$$

We invite the reader to check that if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then indeed} \quad [Ax, Ay, Az, Aw] = [x, y, z, w].$$

In 2022, Sofia Giampietro and Henri Darmon in [GD22], as part of the first author's master thesis, chose a prime $p \mid N$ and conducted extensive numerical computations with the quantities

$$\frac{j_N(P_1) - j_N(P_2)}{j_N(P_1') - j_N(P_2)} \cdot \frac{j_N(P_1') - j_N(P_2')}{j_N(P_1) - j_N(P_2')},$$

where for a CM-point P on the curve X_N, we write $P' := w_p(\mathrm{Frob}_p(P))$ where Frob_p denotes Frobenius at p in the CM-field of definition for P. The definition of P' may seem very little intuitive at first, but the logic behind this construction will become apparent in the next section.

As an example of these computations, Section 5 in [GD22] elaborates on the case of $N = 6$, $D_1 = -43$ and $D_2 = -163$, computing that

$$\mathrm{Nm}_{\mathbb{Q}}^{F}\left[\frac{j_N(P_1)-j_N(P_2)}{j_N(P_1')-j_N(P_2)}\cdot\frac{j_N(P_1')-j_N(P_2')}{j_N(P_1)-j_N(P_2')}\right]=\left(\frac{2\cdot 29\cdot 257\cdot 277}{73\cdot 137\cdot 241}\right)^2.$$

In parallel with Equation 1.1, one can check that all primes that occur on the right hand side are inert in both K_1 and K_2. More strongly, they are even prime divisors of a number of the form $43\cdot 163 - x^2$ for some $|x| < \sqrt{43\cdot 163}$, as the equality $43\cdot 163 - 19^2 = 24\cdot 277$ exemplifies. In fact, in this case, the authors did conjecture a general formula for this quantity. If we let $\{a, -a, b, -b\}$ denote the four square roots of $D = D_1D_2$ modulo $2N$, and define

$$\delta(x) = \begin{cases} +1 & \text{if } x \equiv \pm a \mod 2N; \\ -1 & \text{if } x \equiv \pm b \mod 2N, \end{cases} \tag{2.1}$$

then the following was conjectured in [GD22]. Its proof will be one of the main focusses of this thesis and can be found in Chapter 3.

Theorem A. *Let $N \in \{6, 10, 22\}$. For any pair of points P_1 and P_2 on X_N with CM by $\mathcal{O}_i$, the norm*

$$\mathrm{Nm}_{\mathbb{Q}}^{H_1H_2}\left[\frac{j_N(P_1)-j_N(P_2)}{j_N(P_1')-j_N(P_2)}\cdot\frac{j_N(P_1')-j_N(P_2')}{j_N(P_1)-j_N(P_2')}\right]^{\frac{\pm 2}{w_1w_2}}$$

is equal to the finite product

$$\pm\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}} F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

The similarity with Theorem 1.2.1 is apparent, even though, as our explicit examples show, the changed argument of the F-function causes most of the primes occurring in the two factorisations to be different. Finally, it is worth noting that in the concluding section of [GD22], the computations from [Err11] are shown to all be in accordance with the above result, giving strong validity to the statement above.

The statement of this theorem seems to suggest a resolution in the language of CM abelian varieties over the complex numbers $\mathbb{C}$, and in Chapter 3, we will carry out such a proof. However, following the treatment in [GD22], we also opt to approach this problem over the p-adics instead, for reasons we will explain in Section 2.3. The next section outlines how several powerful results combine to facilitate this.

2.2 The p-adic point of view

Using the p-adic uniformisation of Shimura curves, the authors of [GD22] related the quantity from Theorem A to one of a p-adic nature as follows. Recall that $N \in \{6, 10, 22\}$ and write $N = pq$ in such a way that $q \in \{2, 3, 5\}$, so as to ensure that B_q contains a unique maximal order R_q. We let $\mathcal{H}_p = \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$ denote Drinfeld's p-adic upper half plane. By choosing a splitting $B_q \to M_2(\mathbb{Q}_p)$, we obtain an action of B_q on $\mathcal{H}_p$. Furthermore, we let $R_q[1/p]$ be a maximal $\mathbb{Z}[1/p]$-order in B_q and by $R_q[1/p]_1^\times$ we will denote its units of unit norm. This group is infinite, and the quotient $R_q[1/p]_1^\times \setminus \mathcal{H}_p$ is a compact curve over $\mathbb{C}_p$.

A priori, it is not clear that this quotient should be related to the curve X_N in any way, since these objects are constructed using different quaternion algebras. Therefore, all the more surprising becomes the following celebrated theorem of Čerednik and Drinfeld, originally proved in [Čer76, Dri76] and well explained in [BC91].

Theorem 2.2.1. *The quotient $R_q[1/p]_1^\times \setminus \mathcal{H}_p$ is isomorphic to X_N over $\mathbb{C}_p$, with the isomorphism itself being defined over $\mathbb{Q}_{p^2}$, the unique quadratic unramified extension of $\mathbb{Q}_p$. The Čerednik-Drinfeld isomorphism*

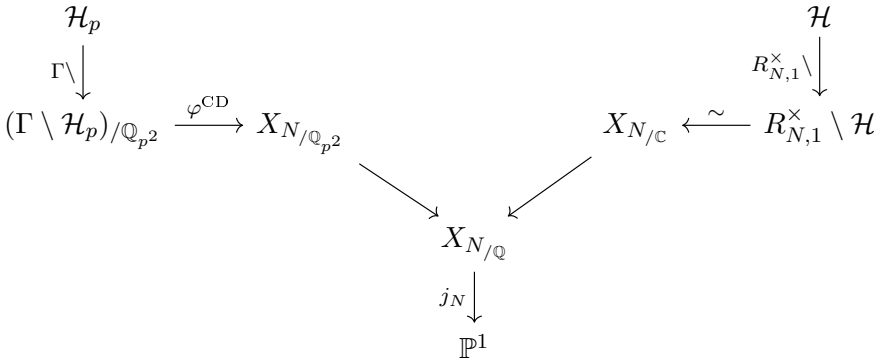
$$\varphi^{\mathrm{CD}} : R_q[1/p]_1^\times \setminus \mathcal{H}_p \xrightarrow{\sim} X_N(\mathbb{C}_p),$$

satisfies the property that for any $\tau \in R_q[1/p]_1^\times \setminus \mathcal{H}_p$ and $\delta \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, it holds that

$$\varphi^{\mathrm{CD}}(\delta(\tau)) = \begin{cases} \delta(\varphi^{\mathrm{CD}}(\tau)) & \text{if } \delta \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^2}); \\ w_p \cdot \delta(\varphi^{\mathrm{CD}}(\tau)) & \text{if } \delta \notin \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^2}). \end{cases}$$

This is a deep result, and we refrain from commenting on its proof. We relate the two stories told above by summarising everything in the single diagram below, where we wrote $\Gamma = R_q[1/p]_1^\times$ for clarity.

One of the advantages of this p-adic viewpoint is that the function $j_N : X_N(\mathbb{C}_p) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}_p)$ enjoys a more explicit description after appealing to the isomorphism from Theorem 2.2.1. Namely, the function



fields of such curves are generated by the titular p-adic Θ-functions. For a comprehensive treatment of these objects, we refer to Section 2.2 of [GvdP06]. We recall their definitions and main properties. We define for any $w_1, w_2 \in \mathcal{H}_p$ the infinite p-adic product

$$\Theta(w_1, w_2; z) := \prod_{\gamma \in R_q[1/p]_1^{\times}} \frac{z - \gamma w_1}{z - \gamma w_2}. \tag{2.2}$$

As shown in Section 2.2 of [GvdP06], this product converges for any value of $z \in \mathcal{H}_p$ as long as the denominator never vanishes. This function satisfies for any $\gamma \in R_q[1/p]_1^{\times}$ the relation

$$\Theta(w_1, w_2; \gamma z) = c(\gamma)\Theta(w_1, w_2; z)$$

for a certain factor of automorphy $c(\gamma) \in \mathbb{C}_p^{\times}$. As explained in Section 3 of [GD22], if X_N is of genus 0, as we are assuming, this factor of automorphy vanishes and as such, the expression above describes a rational function on the quotient $R_q[1/p]_1^{\times} \setminus \mathcal{H}_p$ with divisor $2(w_1) - 2(w_2)$. The factor of 2 here is caused by the trivially acting element $-1 \in R_q[1/p]_1^{\times}$, which is the only such element other than the identity itself.

Recall that for $i \in \{1, 2\}$, we fixed embeddings $\alpha_i : \mathcal{O}_i \to R_q$ and that for its image inside $M_2(\mathbb{Q}_p)$, there now exist two Galois conjugate common fixed CM-points in $\mathcal{H}_p$. It follows from Theorem 2.2.1 that if the CM-point $\tau_i \in \mathcal{H}_p$ maps to the CM-point $P_i \in X_N$ under the Čerednik-Drinfeld isomorphism φ^{CD}, then τ_i' will map to $P_i' = w_p(\mathrm{Frob}_p(P))$, explaining the perhaps somewhat non-obvious definition of the point P_i' from the previous section.

Comparing divisors, we obtain the equality

$$\Theta(w_1, w_2; z) = c(w_1, w_2) \left(\frac{j_N \circ \varphi^{\mathrm{CD}}(z) - j_N \circ \varphi^{\mathrm{CD}}(w_1)}{j_N \circ \varphi^{\mathrm{CD}}(z) - j_N \circ \varphi^{\mathrm{CD}}(w_2)} \right)^2,$$

where $c(w_1, w_2) \in \mathbb{C}_p^\times$ is some unknown constant. This constant seemingly prevents us from relating the precise norms of the expressions on both sides of this equation to achieve a p-adic analogue of Theorem A. However, a simple trick allows us to circumvent these concerns. Indeed, we may evaluate the above expression at two different values z_1 and z_2, and subsequently divide out the constant $c(w_1, w_2)$ to find the unconditional equality

$$\frac{\Theta(w_1, w_2; z_1)}{\Theta(w_1, w_2; z_2)} = \big[j_N \circ \varphi^{\mathrm{CD}}(z_1), j_N \circ \varphi^{\mathrm{CD}}(z_2), j_N \circ \varphi^{\mathrm{CD}}(w_1), j_N \circ \varphi^{\mathrm{CD}}(w_2)\big]^2.$$

In fact, a cross-ratio also appears on the right hand side, as

$$\begin{aligned}\frac{\Theta(w_1, w_2; z_1)}{\Theta(w_1, w_2; z_2)} &= \prod_{\gamma \in R_q[1/p]_1^\times} \frac{z_1 - \gamma w_1}{z_2 - \gamma w_2} \frac{z_2 - \gamma w_2}{z_2 - \gamma w_1} \\ &= \prod_{\gamma \in R_q[1/p]_1^\times} [z_1, z_2, \gamma w_1, \gamma w_2].\end{aligned}$$

In view of Theorem A, it should now be natural to set $z_1 = \tau_1$, $z_2 = \tau_1'$, $w_1 = \tau_2$ and $w_2 = \tau_2'$. If we let P_i be the image of τ_i for $i \in \{1, 2\}$ under the isomorphism φ^{CD}, then we obtain the equality

$$\prod_{\gamma \in R_q[1/p]_1^\times} [\tau_1, \tau_1', \gamma\tau_2, \gamma\tau_2'] = [j_N(P_1), j_N(P_1'), j_N(P_2), j_N(P_2')]^2.$$

In Section 4.5, we will define an action of the class group $\mathrm{Pic}(K_i)$ on the set of embeddings $\mathcal{O}_i \to R_q$ and as such, also on the set of CM-points for the orders $\mathcal{O}_i$ for $i \in \{1, 2\}$. A product over $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ then corresponds to taking the norm of the p-adic quantities above, which should conjecturally be algebraic and contained in the field H_1H_2, down to the field L. However, these algebraic numbers are in fact always contained in a degree $2h_1h_2$ subfield of H_1H_2, which will cause this norm to L to always be contained in the real quadratic field F.

To algebraically describe the final step down to $\mathbb{Q}$, we let $\pi \in R_q$ denote any quaternion with $\mathrm{Nm}(\pi) = p$. We now define

$$\Theta(D_1, D_2) := \prod_{[c_1], [c_2]} \frac{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \tau_2\big)}{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \tau_2'\big)}$$

and

$$\Theta_p(D_1, D_2) := \prod_{[c_1], [c_2]} \frac{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \pi\tau_2\big)}{\Theta\big([c_1] \cdot \tau_1, [c_1] \cdot \tau_1'; [c_2] \cdot \pi\tau_2'\big)},$$

where the products are taken over all $[c_1] \in \mathrm{Pic}(K_1)$ and $[c_2] \in \mathrm{Pic}(K_2)$. We then also claim the following p-adic version of Theorem A, the proof of which will be the main focus of this thesis.

Theorem B. *It holds that*

$$\left(\frac{\Theta(D_1,D_2)}{\Theta_p(D_1,D_2)}\right)^{\frac{\pm 2}{w_1 w_2}} = \pm \prod_{\substack{x^2<D \\ x^2 \equiv D \bmod 4N}} F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

Clearly, Theorem A and Theorem B are equivalent.

We conclude this section by recording a proposition that aims to relate the result from Theorem 1.3.2 to the differences between the fixed points associated with the embeddings $\alpha_i : \mathcal{O}_i \to R_q$. It illustrates that these fixed points contain a lot of arithmetic information about the pair of embeddings that defined them.

Since we expect only primes ℓ that are inert in both K_1 and K_2 to contribute to the eventual norm of the algebraic quantities we are considering in Theorems A and B, we will restrict ourselves to this class of primes when formulating and proving the following result, once more strengthening the ties between our results and Theorem 1.2.1. Finally, we remark that, even though the following proposition is formulated in terms of the matrix algebra $M_2(\mathbb{Z}_\ell)$, by choosing a splitting it is actually applicable to every rational quaternion algebra B_M as long as $\ell \nmid M$.

Proposition 2.2.2. *Let ℓ be a rational prime that is inert in both K_1 and K_2. Let $\alpha_1 : \mathcal{O}_1 \to M_2(\mathbb{Z}_\ell)$ and $\alpha_2 : \mathcal{O}_2 \to M_2(\mathbb{Z}_\ell)$ be embeddings with associated fixed points $\tau_1 \in \mathbb{Z}_{\ell^2}$ and $\tau_2 \in \mathbb{Z}_{\ell^2}$. Then $v_\ell(\tau_1 - \tau_2)$ is equal to the largest $k \in \mathbb{Z}_{\geq 0}$ such that the images of α_1 and α_2 coincide modulo $\ell^k M_2(\mathbb{Z}_\ell)$.*

Proof. Let us suppose that the image $\alpha_1(\sqrt{D_1})$ is given by

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \quad \text{with fixed point} \quad \tau_1 = \frac{a+\sqrt{D_1}}{c},$$

where $D_1 = a^2 + bc$ is one of the discriminants in question. Further suppose that the image $\alpha_2(\sqrt{D_2})$ is given by

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix} \quad \text{with fixed point} \quad \tau_2 = \frac{x+\sqrt{D_2}}{z},$$

where $D_2 = x^2 + yz$ is the other discriminant. First, we claim that $b, c, y, z \in \mathbb{Z}_\ell^\times$. Indeed, if this were not the case, then $D_1 \equiv a^2 \mod \ell$ and $D_2 \equiv x^2 \mod \ell$. However, then the prime ℓ would not have been inert in the fields K_1 and K_2; a contradiction. Therefore we find that

$$\tau_1 - \tau_2 \in \ell^k \mathbb{Z}_{\ell^2} \iff z(a + \sqrt{D_1}) - c(x + \sqrt{D_2}) \in \mathbb{Z}_{\ell^2}.$$

Now note that we can write $\mathbb{Z}_{\ell^2} = \mathbb{Z}_\ell + \mathbb{Z}_\ell \sqrt{D_1}$. Therefore, we find that

$$\tau_1 - \tau_2 \in \ell^k \mathbb{Z}_{\ell^2} \iff za - cx \in \ell^k \mathbb{Z}_\ell \quad \text{and} \quad zD_1 - c\sqrt{D} \in \ell^k \mathbb{Z}_\ell.$$

Suppose that these congruences hold for some value of k. Then

$$zD_1 \equiv c\sqrt{D} \mod \ell^k \mathbb{Z}_\ell \implies z^2 D_1^2 \equiv c^2 D_1 D_2 \mod \ell^k \mathbb{Z}_\ell.$$

We continue to compute that

$$z^2 D_1 \equiv c^2 D_2 \mod \ell^k \mathbb{Z}_\ell \implies z^2(a^2 + bc) \equiv c^2(x^2 + yz) \mod \ell^k \mathbb{Z}_\ell.$$

Using that $za \equiv cx \mod \ell^k \mathbb{Z}_\ell$, we conclude that $z^2 bc \equiv c^2 yz \mod \ell^k \mathbb{Z}_\ell$, and so $zb \equiv cy \mod \ell^k \mathbb{Z}_\ell$. Now define $t \in \mathbb{Z}_\ell^\times$ to solve the equation $z = tc$. Then we find that $tca \equiv cx \mod \ell^k \mathbb{Z}_\ell$, and as such, $ta \equiv c \mod \ell^k \mathbb{Z}_\ell$. Furthermore, we find that $tcb \equiv cy \mod \ell^k \mathbb{Z}_\ell$, and as such $tb \equiv y \mod \ell^k \mathbb{Z}_\ell$. This means that

$$\begin{pmatrix} x & y \\ z & -x \end{pmatrix} \equiv t \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \mod \ell^k M_2(\mathbb{Z}_\ell).$$

As the images $\alpha_1(\sqrt{D_1})$ and $\alpha_2(\sqrt{D_2})$ are both traceless, this is equivalent to the images of the embeddings agreeing modulo $\ell^k \mathbb{Z}_\ell$.

Conversely, suppose that the above matrix congruence holds true for some $t \in \mathbb{Z}_\ell^\times$. Then we find that $za \equiv tca \equiv cx \mod \ell^k \mathbb{Z}_\ell$, and similarly, as now $D_2 \equiv t^2 D_1 \mod \ell^k \mathbb{Z}_\ell$, we find that $zD_1 \equiv tcD_1 \equiv c\sqrt{D} \mod \ell^k \mathbb{Z}_\ell$, proving the other direction too. □

2.3 Parallels with RM-theory

In the spirit of the original paper by Gross and Zagier [GZ84], our approach to proving Theorem A and Theorem B is two-fold. First we present a direct proof of Theorem A using CM-theory, which one could say is the standard approach for problems of this nature. It is not surprising that such a proof exists, and in fact, using the results from Phillips's thesis [Phi15], the proof is rather straightforward.

Much more interesting is our second proof, which proves Theorem B directly, not relying on any CM-theory whatsoever and is done purely by studying the infinitesimal p-adic deformation theory of the Galois representation associated with an appropriate p-stabilisation of the parallel weight 1 Hilbert Eisenstein series $E_{1,\chi}$ described in Section A.2 and studied in Section 1.6. Captured in one equation, letting Δ once again denote the diagonal restriction, Theorem B will be a consequence of the claim that the first Fourier coefficient of the ordinary projection

$$e^{\mathrm{ord}}\left(\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon)\right)\in S_2(\Gamma_0(N)),$$

must vanish, once more strengthening the parallels with the analytic proof in [GZ84] that we sketched in Section 1.6 and which we similarly captured succinctly in Equation 1.2.

Our main motivation for this second proof, which constitutes the focus of this manuscript, originates from the recent advancements in the theory of real multiplication, as we will now explain.

A most naive attempt at using the j-function also to generate abelian extensions of *real* quadratic fields to mimic the results of Corollary 1.1.2 is complicated by the observation that the real line $\mathbb{R}$ is not contained in the field of definition $\mathcal{H}$ of j. A more conceptual way of phrasing this obstruction, is that the infinite place of a real quadratic field is split, whereas it is not for imaginary quadratic fields. As $\mathcal{H}_p=\mathbb{P}^1(\mathbb{C}_p)\backslash\mathbb{P}^1(\mathbb{Q}_p)$ and all p-adic embeddings of a number field land inside $\mathbb{Q}_p$ if and only if p splits completely, a real quadratic field *does have points* inside the p-adic upper half plane as soon as p does *not* split.

Building upon this insight and influences from the theory of linking numbers of modular knots, in [DV21], Darmon and Vonk proposed a p-adic real quadratic analogue of the differences between singular moduli as studied in [GZ84]; a certain *rigid meromorphic cocycle* for the group $\mathrm{SL}_2(\mathbb{Z}[1/p])$, whose RM-values conjecturally often generate the appropriate Hilbert class fields for real quadratic fields. Certain cases of these conjectures have recently been proved and while this emerging theory should be well connected with many other areas of mathematics, notable among these the theory of Borcherds products and their ostensible connections to both p-adic heights and intersection numbers of geodesics on Shimura curves, many aspects remain to be explored.

The RM-values of the rigid meromorphic cocycles introduced in [DV21] in many ways behave like a p-adic real quadratic analogue of the differences between singular moduli as studied in [GZ84], as these RM-values conjecturally display factorisations of an intricacy similar to those

claimed by Theorem 1.2.1. More recently, these constructions were generalised to different quaternion algebras than the matrix algebra in [Geh20, GMX21], reflecting the step from modular curves to Shimura curves as outlined earlier in this chapter, and to more general orthogonal groups in [DGL23].

Historically, the study of CM-theory has largely been facilitated by its connection to the geometry of abelian varieties and the moduli spaces that govern them. The development of an analogous RM-theory is complicated by the lack of such obvious connections to geometry. It is for this reason that the analytic proof in [GZ84] is of particular interest, as its independence from CM-theory contrasted strongly with the other, more algebraic, proof.

Darmon, Pozzi and Vonk used similar ideas in [DPV21, DPV23], studying the ordinary projection of the diagonal restriction of the first derivative with respect to the weight parameter of a p-adic family of Hilbert modular Eisenstein series attached to more general odd characters of the narrow class group of a real quadratic field. They computed its Fourier coefficients and these quantities proved to be related to both Stark-Heegner points and Gross-Stark units, enriching the analogy between the classical theory of complex multiplication and its extension to real quadratic fields.

In a similar spirit, Dasgupta and Kakde in [DK23a, DK23b] recently proved the Brumer-Stark conjecture away from 2 and used these ideas to prove the p-part of the integral Gross-Stark conjecture for the Brumer-Stark p-units in CM abelian extensions of a totally real field using the theory of group ring valued Hilbert modular forms. Another recent breakthrough towards Hilbert's 12th problem was recently established in [BCG23], highlighting the buzzing research activity surrounding the ideas and techniques that drive the main concepts explored in this thesis.

The p-adic nature of these advancements in the RM setting raises the question of the applicability of some of these techniques in the CM setting, where the theory is much more understood and other methods than those employed in this thesis are also available. The main motivation for this manuscript is to answer this question in one particular setting, proving the same theorem both using the geometric moduli interpretation of the Shimura curve X_N, and not using this interpretation at all, and instead relying purely on the newly developed techniques from modern RM theory. This is especially interesting in view of the presently still unknown geometric framework within which the modern developments in RM-theory should best be described. Finally, we remark that

the present work serves as a direct p-adic transposition of the analytic proof by Gross and Zagier in [GZ84] because we study an appropriate p-stabilisation of the exact same Hilbert Eisenstein series $E_{1,\chi}$, but using p-adic instead of archimedean methods.

Additionally, our work hints at an occurrence of a non-archimedean instance of the Kudla program, which is presently being investigated more intensively than ever. Even though it has classically been mostly studied in an archimedean context, recent years have seen some instances of similar results in non-archimedean settings. Examples of this include the results from [DPV21, DPV23], but also for instance the works [DT08] and [LN19]. This emerging "p-adic Kudla program" still leaves much to be explored in the forthcoming years. It is also for this reason that in the present work, we do not explore the possibly third approach using Borcherds lifts in a similar style of [Err11] when proving the CM-values from [Elk98], even though the success of such an approach should be expected as well.

Remark 2.3.1. If we relax the condition that the Shimura curve X_N be of genus zero, then the quotient $\Theta(D_1, D_2)/\Theta_p(D_1, D_2)$ from Theorem B can no longer be expected to be algebraic and indeed it generally will not be, for it will consist of both an algebraic part, determined above, and a transcendental part given by an appropriate p-adic height pairing on the Jacobian of the Shimura curve X_N, which vanishes in the genus zero case. Define for $i \in \{1, 2\}$ the divisors on X_N by the formulas

$$\mathcal{D}_i = \sum_{[c_i] \in \mathrm{Pic}(K_i)} [c_i] \cdot (P_i - P_i').$$

Let T_m denote the natural Hecke correspondence on the Jacobian of X_N and let $(-,-)_p$ denote the p-adic Schneider height pairing as computed in [Gro86, Wer96]. Even though Werner's result in [Wer96] only pertains to the quotient by Schottky groups, using the results from Section 4 of [vdP92], one expects this to be extendable to quotients by groups such as $R_q[1/p]_1^\times$. One may conjecture an equality of the form

$$e^{\mathrm{ord}}\left(\Delta \frac{d}{d\epsilon} E_{1,\chi}^{(p)}(\epsilon)\right) = \sum_{m \geq 1} (\mathcal{D}_1, T_m \mathcal{D}_2)_p \; q^m \in S_2(\Gamma_0(N)).$$

This p-adic instance of the Kudla program would bear strong resemblance to various previous works in an archimedean setting; most notably to Theorem V.1 in [GKZ87]. It would also resemble some of the results by Zhang in [Zha01, YZZ13].

2.4 Outline of the thesis

In Chapter 3, we describe an approach that mirrors the ideas behind Gross and Zagier's original algebraic proof in [GZ84], exploiting the moduli interpretation of the Shimura curve X_N and the theory of complex multiplication. We appeal to the main result of the PhD thesis of Andrew Phillips [Phi15], which computes the intersection numbers of certain substacks of the full moduli stack that parametrise CM abelian varieties, following ideas of Howard and Yang in [HY12]. Using these results, the proof of Theorem A is rather straightforward.

The weight of this thesis is concentrated in our proof of Theorem B. For this, we follow the general strategy of the main arguments presented in [DPV23]. The core idea is to deform $E_{1,\chi}^{(p)}$ as a p-adic *cusp form*. To obtain such a family of deformations, we first deform a rigidification ρ_η of the decomposable representation $\rho = \mathbb{1} \oplus \chi$ associated with $E_{1,\chi}^{(p)}$. We then justify that these representations come from modular forms by means of proving a so-called $R = T$-theorem. With this family of modular forms in hand, we finish the proof through a computation.

Our second proof can thus be divided into three distinct steps.

Step 1: In Chapter 4, we describe an F-quadratic form $\det_F$ on B_q refining the quaternion norm to F. Together with a construction that associates to a quaternion an $\mathcal{O}_L$-ideal, we derive a bijection between the elements of R_q with a fixed $\det_F$-value and the set of $\mathcal{O}_L$-ideals of a certain norm. In Section 6.1, we use this to rewrite the left hand side of Theorem B in a more useful form.

Step 2: Chapter 5 proves an $R = T$ theorem using similar methods as in Pozzi's thesis [Poz19] and the works [BDP22, BD16, BDS20, BC06], using fundamental results from Hida in [Hid89b, Hid89a]. This is done by constructing a lift of ρ_η to Hida's cuspidal nearly ordinary Hecke algebra and comparing the dimensions of this Hecke algebra T and the nearly ordinary deformation ring R. This is used in Section 6.2.

Step 3: In Chapter 6, we consider one particular deformation and, supported by the result of Chapter 5, compute the infinitesimal family of deformations of $E_{1,\chi}^{(p)}$ that corresponds to it. After taking its diagonal restriction, its derivative with respect to the weight parameter and applying the ordinary projection operator, we argue why the result must vanish identically. Ultimately, we conclude the proof of Theorem B by computing explicitly the Fourier coefficients and equating the first of these coefficients to zero.

CHAPTER 3

Moduli of false elliptic curves

Assisted by the PhD thesis written by Andrew Phillips [Phi15], this chapter aims to approach Theorem A geometrically to give a first proof of Giampietro's conjectures. We stress here once again that using these results, our proof of Theorem A is rather straightforward. Therefore, the weight and novelty of this thesis rests mostly on the forthcoming chapters instead. Throughout this chapter, we fix $N \in \{6, 10, 22\}$.

Recall that modular curve $X_0(1)$ acts as a coarse moduli space for the set of elliptic curves up to isomorphism. This is done by sending $\tau \in \mathcal{H}$ to the elliptic curve $E_\tau = \mathbb{C}/\Lambda_\tau$ where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. As one can choose various bases for the lattice Λ_τ, this induces a bijection

$$Y_0(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \xrightarrow{\sim} \big\{E/\mathbb{C} \text{ an elliptic curve}\big\}/\text{ iso.}$$

A similar construction realises X_N as the coarse moduli space of *false elliptic curves*; roughly speaking, these are abelian surfaces A with the property that the maximal order $R_N \subset B_N$ embeds into the endomorphism ring of A. We say that such surfaces have *quaternionic multiplication* by R_N. To $\tau \in \mathcal{H}$ one associates the lattice

$$\Lambda_\tau := R_N \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} \subset \mathbb{C}^2.$$

By construction, this lattice is stable under left-multiplication by R_N and as such, this maximal order embeds into $\mathrm{End}(A_\tau)$, where $A = \mathbb{C}^2/\Lambda_\tau$. This association yields a bijection

$$X_N(\mathbb{C}) = R_{N,1}^\times \setminus \mathcal{H} \xrightarrow{\sim} \big\{A/\mathbb{C} \text{ a false elliptic curve}\big\}/\text{ iso.}$$

We use this description to illustrate why it is natural to define CM-points on the Shimura curve X_N as the fixed point in $\mathcal{H}$ for the action of the fields K_i on $\mathcal{H}$ through some fixed embeddings $\alpha_i : \mathcal{O}_i \to R_N$ for $i \in \{1, 2\}$. Roughly, we say a false elliptic curve A has CM by an imaginary quadratic order $\mathcal{O}$ if there exists an embedding $\mathcal{O} \to \mathrm{End}_{R_N}(A)$; in other words, there must be a subring of endomorphisms isomorphic to $\mathcal{O}$ that commutes with the given subring of endomorphisms isomorphic to R_N. The following lemma explains that with these definitions, CM-points on X_N correspond to false elliptic curves with CM.

Lemma 3.0.1. *Let $P \in \mathcal{H}$ be the fixed point for the action of some embedding $\alpha_i : \mathcal{O}_i \to R_N$. Then $P \in X_N$ corresponds to a false elliptic curve with complex multiplication by $\mathcal{O}_i$.*

Proof. Let $A = \mathbb{C}^2/\Lambda_P$ with Λ_P as defined above. We must find for any $x \in \mathcal{O}_i$ an endomorphism $\kappa(x)$ that commutes with the R_N-action on A. Note that if for some $x \in \mathcal{O}$,

$$\alpha_i(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{then} \quad \alpha_i(x) \cdot \begin{pmatrix} P \\ 1 \end{pmatrix} = \begin{pmatrix} aP + b \\ cP + d \end{pmatrix} = (cP + d) \begin{pmatrix} P \\ 1 \end{pmatrix}.$$

So we set $\kappa(x)$ to be scalar multiplication by $cP + d$ on $A = \mathbb{C}^2/\Lambda_P$. It remains to show that this is a ring homomorphism. To this end, choose an embedding $K_i \to \mathbb{C}$ and assume without loss of generality that $c > 0$ if and only if $x \in \mathcal{H}$. This is possible since $\alpha_i(\sqrt{D_i})$ cannot be upper triangular, for if so, its square would have positive trace, whereas $D_i < 0$. For $x \in \mathcal{H}$ we compute that

$$cP^2 + dP = aP + b \iff P = \frac{a - d + \sqrt{D_i(x)}}{2c}$$

where

$$D_i(x) = (a-d)^2 + 4bc = \mathrm{Tr}(\alpha_i(x))^2 - 4\det(\alpha_i(x)) = \mathrm{tr}(x)^2 - 4\ \mathrm{Nm}(x).$$

Therefore, we find that

$$cP + d = \frac{\mathrm{tr}(\alpha_i(x)) + \sqrt{D_i(x)}}{2} = \frac{\mathrm{tr}(x) + \sqrt{\mathrm{tr}(x)^2 - 4\ \mathrm{Nm}(x)}}{2}.$$

This describes the unique solution in $\mathcal{H}$ to the equation $X^2 - \mathrm{tr}(x)X + \mathrm{Nm}(x) = 0$, which is x. Whence $cP + d = x$ and the homomorphism property is immediate. □

3.1 Arakelov degrees of stacks

Unfortunately, the curve X_N is only a coarse moduli space for false elliptic curves. To obtain a fine moduli space, we will need to work with algebraic stacks. An overview of the theory of stacks will not be given here, but for a brief yet clear introduction, we refer the reader to Section 7 of [Vis89]. We start with some definitions.

Definition 3.1.1. A *false elliptic curve* over a scheme S is a pair (A, ι) where $A \to S$ is an abelian scheme of relative dimension 2 and $\iota\colon R_N \to \mathrm{End}_S(A)$ is a ring homomorphism. For $i \in \{1, 2\}$, a false elliptic curve over an $\mathcal{O}_L$-scheme S with *complex multiplication* by $\mathcal{O}_i$ is a triple (A, ι, κ) where (A, ι) is a false elliptic curve over S and $\kappa\colon \mathcal{O}_i \to \mathrm{End}_{R_N}(A)$ is a ring map such that the action on the Lie algebra is through the natural structure map $\mathcal{O}_i \to \mathcal{O}_L \to \mathcal{O}_S(S)$.

Definition 3.1.2. Let $\mathcal{M}$ be the algebraic stack, regular and flat of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_L)$, such that $\mathcal{M}(S)$ for any $\mathcal{O}_L$-scheme S denotes the category of false elliptic curves (A, ι) over S satisfying for any $x \in R_N$ the property that any $s \in S$ has an affine open neighbourhood $\mathrm{Spec}(R) \to S$ such that $\mathrm{Lie}(A_{/R})$ is a free R-module of rank 2 and there is an equality of polynomials in $R[T]$ of the form

$$\mathrm{char}(\iota(x), \mathrm{Lie}(A_{/R}) = (T - x)(T - \overline{x}),$$

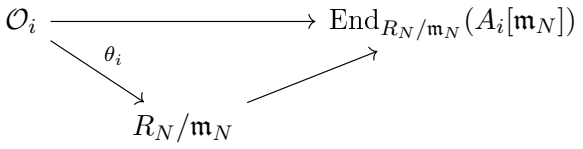
where $\overline{(\ldots)}$ denotes the main involution on B_N. This 2-dimensional stack $\mathcal{M}$ is usually referred to as (the integral model of) a Shimura curve.

We are interested in two particular substacks of this stack; those defining the false elliptic curves with complex multiplication by $\mathcal{O}_i$ for $i \in \{1, 2\}$. Let $\mathcal{Y}_i$ for $i \in \{1, 2\}$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{Y}_i(S)$ the category of false elliptic curves over the $\mathcal{O}_L$-scheme S with complex multiplication by $\mathcal{O}_i$. By forgetting the CM-structure, we have a morphism of stacks $\mathcal{Y}_i \to \mathcal{M}$. We further define

$$\mathcal{J} := \mathcal{Y}_1 \times_{\mathcal{M}} \mathcal{Y}_2.$$

By definition of the pullback of stacks, $\mathcal{J}$ now denotes the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{J}(S)$ the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ where $\mathbf{A}_i = (A_i, \iota_i, \kappa_i)$ for $i \in \{1, 2\}$ is a false elliptic curve over the $\mathcal{O}_L$-scheme S with complex multiplication by $\mathcal{O}_i$ and where $f \colon \mathbf{A}_1 \to \mathbf{A}_2$ is an isomorphism of false elliptic curves.

Following [Phi15], we proceed to refine the stack $\mathcal{J}$ by associating to every triple $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{J}(S)$ a pair of objects (ϑ, ν) as follows. It is easy to show that there exists a unique ideal $\mathfrak{m}_N \subset R_N$ of index N^2. For $i \in \{1, 2\}$, there is a unique surjective ring map $\theta_i \colon \mathcal{O}_i \to R_N/\mathfrak{m}_N$ making the following diagram commute, where $A_i[\mathfrak{m}_N]$ denotes the group



scheme of the $\mathfrak{m}_N$-torsion inside A_i.

Since $\mathcal{O}_L = \mathcal{O}_1 \otimes_{\mathbb{Z}} \mathcal{O}_2$, we obtain a well-defined surjective ring map $\vartheta \colon \theta_1 \otimes \theta_2 \colon \mathcal{O}_L \to R_N/\mathfrak{m}_N$. For brevity, we will denote

$$\mathcal{V} := \mathrm{Hom}(\mathcal{O}_L, R/\mathfrak{m}_N).$$

We let $\mathfrak{a}_\vartheta = \ker(\vartheta) \cap \mathcal{O}_F$ be the *reflex ideal*. Since $\ker(\vartheta)$ is an $\mathcal{O}_L$-ideal of norm N^2, it follows that $\mathfrak{a}_\vartheta$ is an $\mathcal{O}_F$-ideal of norm N. As such, as $N = pq$, there are precisely four possibilities for $\mathfrak{a}_\vartheta$;

$$\mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\} =: \mathcal{I}.$$

Next, as in Proposition 2.3 in [HY12], one can construct a map

$$\deg_{\mathrm{CM}} \colon \mathrm{Hom}_{R_N}(A_1, A_2) \to \mathcal{D}_F^{-1}$$

satisfying the defining property that $\mathrm{tr}^F_{\mathbb{Q}}(\deg_{\mathrm{CM}}(f)) = \deg^*(f)$, where $\deg^*(f)$ denotes the *false degree* of the morphism f as in Definition 2.2.15 in [Phi15], which satisfies the property that $\deg^*(f) = 1$ for all isomorphisms f. This construction is very similar to the one to be outlined in Section 4.4 of this thesis, so we will not give more details here. As such, we may consider the element $\nu = \deg_{\mathrm{CM}}(f) \in \mathcal{D}_F^{-1}$. Then $\mathrm{tr}(\nu) = 1$.

For any $\vartheta \in \mathcal{V}$, we define $\mathcal{X}_\vartheta$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{X}_\vartheta(S)$ for any $\mathcal{O}_L$-scheme S the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{J}(S)$ with the property that the pair $(\mathbf{A}_1, \mathbf{A}_2)$ induces the map $\vartheta \in \mathcal{V}$ by the construction outlined above.

For any $\nu \in \mathcal{D}_F^{-1}$, we let $\mathcal{X}_{\vartheta,\nu}$ denote the algebraic stack over $\mathrm{Spec}(\mathcal{O}_L)$ with $\mathcal{X}_{\vartheta,\nu}(S)$ for any $\mathcal{O}_L$-scheme S the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathcal{X}_\vartheta(S)$ with the property that $\deg_{\mathrm{CM}}(f) = \nu$ on every component of S.

We then obtain the decompositions

$$\mathcal{J} = \bigsqcup_{\vartheta \in \mathcal{V}} \mathcal{X}_\vartheta \quad \text{and} \quad \mathcal{X}_\vartheta = \bigsqcup_{\substack{\nu \in \mathcal{D}_F^{-1} \\ \mathrm{tr}(\nu)=1}} \mathcal{X}_{\vartheta,\nu}.$$

The main result of [Phi15] concerns the *Arakelov degree* of the stacks $\mathcal{X}_\vartheta$, which is defined as

$$\deg(\mathcal{X}_\vartheta) := \sum_{\mathfrak{r} \subset \mathcal{O}_L} \log(|\mathbb{F}_\mathfrak{r}|) \sum_{x \in \mathcal{X}_\vartheta(k)} \frac{\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta, x})}{|\mathrm{Aut}(x)|},$$

where $\mathfrak{r} \subset \mathcal{O}_L$ is a prime, where $k = \overline{\mathbb{F}}_\mathfrak{r}$ and where $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta, x}$ denotes the strictly Henselian local ring of $\mathcal{X}_\vartheta$ for the étale topology at the geometric point x. By the decomposition above, we have

$$\deg(\mathcal{X}_\vartheta) = \sum_{\substack{\nu \in \mathcal{D}_F^{-1} \\ \mathrm{tr}(\nu)=1}} \deg(\mathcal{X}_{\vartheta,\nu}). \tag{3.1}$$

Lastly, we define the finite set

$$\mathrm{Diff}_\vartheta(\nu) = \mathrm{Diff}_{\mathfrak{a}_\vartheta}(\nu) := \{\mathfrak{r} \subset \mathcal{O}_F \mid \chi_\mathfrak{r}(\nu\mathfrak{a}_\vartheta^{-1}\mathcal{D}_F) = -1\},$$

where $\chi_\mathfrak{r}$ denotes the character defined by the unramified extension of local fields $L_\mathfrak{r}/F_\mathfrak{r}$, obtained by completing these fields at the prime $\mathfrak{r}$ and a prime of L above it. For $I \subset \mathcal{O}_F$, it holds that $\chi_\mathfrak{r}(I) = \chi(\mathfrak{r})^{\mathrm{ord}_\mathfrak{r}(I)}$. Theorem 2 in [Phi15] then says the following.

Theorem 3.1.3. *Let $\nu \in F$ satisfy $\mathrm{tr}(\nu) = 1$. Suppose that $\mathrm{Diff}_\vartheta(\nu) = \{\mathfrak{r}\}$ for some prime $\mathfrak{r} \subset \mathcal{O}_F$. If $r \nmid N$, the degree of $\mathcal{X}_{\vartheta,\nu}$ satisfies*

$$\exp(\deg(\mathcal{X}_{\vartheta,\nu})) = r^{t_r/2} \quad \textit{where} \quad t_r = \mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r}\mathcal{D}_F) \cdot \rho(\nu\mathfrak{a}_\vartheta^{-1}\mathfrak{r}^{-1}\mathcal{D}_F).$$

If $r \mid N$, depending on whether $\mathfrak{r}$ divides $\mathfrak{a}_\vartheta$ or not, we must replace the term $\mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r}\mathcal{D}_F)$ by $\mathrm{ord}_\mathfrak{r}(\nu)$ or $\mathrm{ord}_\mathfrak{r}(\nu\mathfrak{r})$ respectively.

If $\nu \notin \mathcal{D}_F^{-1}$ or $\#\mathrm{Diff}_\vartheta(\nu) \neq 1$, then the degree is always 0. In addition, if $\nu \not\gg 0$, then the degree is always 0.

This result gives us an explicit formula for the Arakelov degrees of the stacks $\mathcal{X}_{\vartheta,\nu}$ and as such, also of the degrees of the stacks $\mathcal{X}_\vartheta$. It is also clear from the result that the degree of the stack $\mathcal{X}_{\vartheta,\nu}$ only depends on the ideal $\mathfrak{a}_\vartheta \in \mathcal{I}$ and not on the precise map $\vartheta \in \mathcal{V}$. Therefore, the same holds true for the degree of $\mathcal{X}_\vartheta$ too. This allows us to define for any $\mathfrak{a} \in \mathcal{I}$ and $\nu \in F$ the quantities

$$X(\mathfrak{a}, \nu) := \deg(\mathcal{X}_{\vartheta,\nu}) \quad \text{and} \quad X(\mathfrak{a}) := \deg(\mathcal{X}_\vartheta),$$

where $\vartheta \in \mathcal{V}$ is arbitrary such that $\mathfrak{a}_\vartheta = \mathfrak{a}$. In the next section we will show that these expressions, when combined appropriately, constitute the right hand side of Theorem A. The remainder of this chapter aims to relate the degrees of the stacks $\mathcal{X}_\vartheta$ to the left hand side, ultimately establishing equality.

3.2 An elementary formula

We first prove a sequence of smaller lemmas, that each will take care of a separate part of the translation process between Phillips's more abstract ideal arithmetic and Gross and Zagier's and Giampietro's elementary formulas involving the F-function defined in Section 1.2.

Recall the definition of a *special prime* for a positive integer m as being a prime ℓ that divides m an odd number of times and such that each prime $\mathfrak{l}$ of F above ℓ satisfies $\chi(\mathfrak{l}) = -1$.

Lemma 3.2.1. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu) = 1$. Then the ideal $\nu\mathcal{D}_F$ is integral, principal and primitive.*

Proof. We write $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some odd integer x. Using that $\mathcal{D}_F = (\sqrt{D})$, we find that $\nu\mathcal{D}_F = ((x+\sqrt{D})/2)$. This is clearly integral and principal, and it is primitive because no rational prime r can divide it. Indeed, the element $(x+\sqrt{D})/2r$ can never be integral for a prime r. This completes the proof. □

Lemma 3.2.2. *Let $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some integer x be such that some $\mathfrak{a} \in \mathcal{I}$ satisfies $\mathfrak{a} \mid \nu\mathcal{D}_F$. If $\mathfrak{r} \in \mathrm{Diff}_{\mathfrak{a}}(\nu)$ and $r = \mathfrak{r} \cap \mathbb{Z}$, then r is a special prime of the integer $(D-x^2)/4N$.*

Proof. Recall that for $I \subset \mathcal{O}_F$, it holds that $\chi_{\mathfrak{r}}(I) = \chi(\mathfrak{r})^{\mathrm{ord}_{\mathfrak{r}}(I)}$.

Suppose that $\mathfrak{r} \in \mathrm{Diff}_{\vartheta}(\nu)$, or in other words, $\chi_{\mathfrak{r}}(\nu\mathfrak{a}\mathcal{D}_F) = -1$. By the explicit description of $\chi_{\mathfrak{r}}$, it now follows that $\chi(\mathfrak{r}) = -1$, so $\mathfrak{r}$ is inert in L/F. Therefore, r is not inert in F.

Now note that $\chi_{\mathfrak{r}}(\nu\mathfrak{a}\mathcal{D}_F) = \chi_{\mathfrak{r}}(\nu\mathfrak{a}^{-1}\mathcal{D}_F)$, as squares of ideals are always in the kernel of $\chi_{\mathfrak{r}}$. By Lemma 3.2.1, this latter ideal is both integral and still primitive, and as such, only one of the two primes above r in F can occur in its factorisation. This multiplicity is then equal to the multiplicity with which r occurs in the norm of the ideal. As $\chi_{\mathfrak{r}}(\nu\mathcal{D}_F) = -1$, this number must be odd, establishing that r is indeed a special prime of the integer $(D-x^2)/4N$. □

Lemma 3.2.3. *Let $I \subset \mathcal{O}_F$ be an ideal with explicit prime factorisation $I = \prod_i \mathfrak{r}_i^{2m_i} \prod_j \mathfrak{s}_j^{n_j}$ where all the primes $\mathfrak{s}_j$ split in L/F and all $\mathfrak{r}_i$ are inert in L/F. Then we have*

$$\rho(I) = \prod_j (n_j + 1).$$

Proof. We look prime by prime. The unique ideal $\mathfrak{R}_i$ of L lying over $\mathfrak{r}_i$ has norm $\mathfrak{r}_i^2$. Hence only $\mathfrak{R}^{m_i}$ has norm $\mathfrak{r}^{2m_i}$.

For any of the $\mathfrak{s}_j$, we find two primes in L lying above it, say $\mathfrak{S}_j$ and $\mathfrak{S}'_j$. The norm of $\mathfrak{S}_j^a\mathfrak{S}_j'^b$ is equal to $\mathfrak{s}^{a+b}$ and so we find n_j+1 possible ideals with norm $\mathfrak{s}_j^{n_j}$, corresponding to $a \in \{0,\ldots,n_j\}$. □

Lemma 3.2.4. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu) = 1$. Then there is at most one ideal $\mathfrak{a} \in \mathcal{I}$ such that $\rho(\nu\mathfrak{a}^{-1}\mathcal{D}_F) > 0$.*

Proof. A necessary condition for the quantity $\rho(\nu\mathfrak{a}^{-1}\mathcal{D}_F)$ to be positive, is that the ideal $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ be integral. In other words, we must have

$\mathfrak{a} \mid \nu\mathcal{D}_F$. However, by Lemma 3.2.1, this latter ideal is primitive, and two different such $\mathfrak{a} \in \mathcal{I}$ dividing it would mean that either p or q would also divide it. This proves the lemma. □

Now note that $\mathfrak{a} \mid \nu\mathcal{D}_F$ if and only if $(x+\sqrt{D})/2 \in \mathfrak{a}$. Applying the nontrivial automorphism σ of $F/\mathbb{Q}$ to this inclusion, we see that

$$(x+\sqrt{D})/2 \in \mathfrak{a} \iff (-x+\sqrt{D})/2 \in \sigma(\mathfrak{a}).$$

The norm of $\nu\mathcal{D}_F$ is given by $(x^2-D)/4$, so if this is divisible by N, then x^2-D must be divisible by $2N$, and so $x^2 \equiv D \mod 2N$. Therefore, $\nu\mathcal{D}_F$ can only be divisible by some $\mathfrak{a} \in \mathcal{I}$ if $x \equiv \pm a, \pm b \mod 2N$, where a and b are as in Equation 2.1. Recall from the previous section that the *reflex ideal* $\mathfrak{a}_\vartheta$ must be an element of the set

$$\mathcal{I} := \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\}.$$

The first and last are Galois conjugate and so are the second and third. Combining all this, we define

$$\delta(\vartheta) = \delta(\mathfrak{a}_\vartheta) := \begin{cases} +1 & \text{if } \mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2\}; \\ -1 & \text{if } \mathfrak{a}_\vartheta \in \{\mathfrak{p}_1\mathfrak{q}_2, \mathfrak{p}_2\mathfrak{q}_1\}, \end{cases}$$

with these Galois orbits chosen in such a way that this sign agrees with the choices from Equation 2.1. The following theorem will be the key consequence of Phillips's work in [Phi15]. It connects the degrees of certain stacks to the explicit formula found in Theorem A.

Theorem 3.2.5. *Let $\nu \in \mathcal{D}_F^{-1,+}$ with $\operatorname{tr}(\nu) = 1$. Then we can write $\nu = (x+\sqrt{D})/2\sqrt{D}$ for some integer x with $x^2 < D$. Furthermore,*

$$F\left(\frac{D-x^2}{4N}\right)^{\delta(x)} = \prod_{\mathfrak{a}\in\mathcal{I}} \exp\big(\delta(\mathfrak{a})X(\mathfrak{a},\nu)\big).$$

Proof. If the norm of $\nu\mathcal{D}_F$ is not divisible by N, then the ideal $\nu\mathfrak{a}_\vartheta^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$ is not integral for any choice of $\mathfrak{a}_\vartheta$ and $\mathfrak{r}$. So no matter the case of Theorem 3.1.3 we are in, $X(\mathfrak{a},\nu) = 0$. The right hand side of the equation will thus be 1, as is the left hand side.

We thus assume that some $\mathfrak{a} \in \mathcal{I}$ divides $\nu\mathcal{D}$. By Lemma 3.2.4, there is then only one such $\mathfrak{a}$. By the same argument as above, any other ideal in $\mathcal{I}$ will not contribute to the product on the right hand side. Hence we

may restrict our view to the unique $\mathfrak{a} \in \mathcal{I}$ dividing $\nu\mathcal{D}$. By definition, the signs $\delta(x)$ and $\delta(\mathfrak{a})$ will agree in this case. Thus we are left to prove

$$F\left(\frac{D-x^2}{4N}\right) = \exp(\deg(\mathcal{X}_{\vartheta,\nu})).$$

We distinguish two cases. First suppose that $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ does not consist of exactly one prime. Then Theorem 3.1.3 tells us that the right hand side again becomes equal to 1. On the other hand, we note that we are in the situation of Lemma 3.2.2 and thus the primes occuring in $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ biject with the special primes of $(D-x^2)/(4N)$. By definition, now that we do *not* have exactly one such prime, F equals 1 too.

We may thus from now on suppose that $\mathrm{Diff}_{\mathfrak{a}}(\nu)$ consists of exactly one prime $\mathfrak{r}$. We again distinguish two cases. First suppose that $r \nmid N$. Then we may use Theorem 3.1.3 to reduce to checking that

$$F\left(\frac{D-x^2}{4N}\right) = r^{t_r/2} \quad \text{where} \quad t_r = \mathrm{ord}_{\mathfrak{r}}(\nu\mathfrak{r}\mathcal{D}) \cdot \rho(\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F).$$

We claim that the ideal factorisation of $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$ is of the form as in Lemma 3.2.3. Let $\mathfrak{l}$ be a prime divisor of this ideal lying over the rational prime ℓ and let $n \in \mathbb{N}$ be such that $\mathfrak{l}^n \| \nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$.

If $\mathfrak{l}$ splits in L/F, there is nothing to show. If not, n being odd would imply that $\mathfrak{l} \in \mathrm{Diff}_{\mathfrak{a}}(\nu) = \{\mathfrak{r}\}$, yielding a contradiction unless $\mathfrak{l} = \mathfrak{r}$. However, in that case, the added factor of $\mathfrak{r}^{-1}$ makes the odd multiplicity of $\mathfrak{r}$ in $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ even again.

We are thus in the position to apply Lemma 3.2.3 to $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$. Using the notation from said lemma, we compute that

$$\rho(\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F) = \prod_j (n_j + 1),$$

where the n_j are the multiplicities with which primes in F that split in L/F divide $\nu\mathfrak{a}^{-1}\mathfrak{r}^{-1}\mathcal{D}_F$. Again, by Lemma 3.2.1, this ideal is primitive so its ideal factorisation in F reflects the factorisation of its norm in $\mathbb{Z}$. Let $2k+1$ denote the odd multiplicity with which $\mathfrak{r}$ divides $\nu\mathcal{D}_F$. Then since $r \nmid N$, we compute that

$$\frac{\mathrm{ord}_{\mathfrak{r}}(\nu\mathfrak{r}\mathcal{D}_F)}{2} = k + 1.$$

So, the right hand side becomes $(k+1)\prod_j (n_j+1)$. Indeed, this agrees with our definition of F, as the norm of $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ is $(D-x^2)/(4N)$, completing the proof in this case.

Finally, we must consider the case of $r \mid N$. We claim that we are always in the case that the prime $\mathfrak{r} \in \mathrm{Diff}_\vartheta(\nu)$ above r divides $\mathfrak{a}$. Namely, by Lemma 3.2.4, the only prime ideals over r dividing $\nu\mathcal{D}_F$ are, by our choice of $\mathfrak{a}$, those occuring in $\mathfrak{a}$. Hence any prime over r occuring at all in the factorisation of $\nu\mathfrak{a}^{-1}\mathcal{D}_F$ must also divide $\mathfrak{a}$. Hence, we use Theorem 3.1.3 to reduce ourselves to proving that

$$F\left(\frac{D-x^2}{4N}\right) = r^{t_r/2} \quad \text{where} \quad t_r = \mathrm{ord}_{\mathfrak{p}}(\nu) \cdot \rho(\nu\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathcal{D}_F).$$

Our accounting for the factor contributed by $\rho(\nu\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathcal{D}_F)$ is very similar to the argument given above. For the other factor, we note that $\mathrm{ord}_{\mathfrak{p}}(\nu) = \mathrm{ord}_{\mathfrak{p}}(\nu\mathcal{D}_F)$ as we assume D and N to be coprime. Let $2k+1$ be the multiplicity with which $\mathfrak{r}$ divides $\nu\mathfrak{a}\mathcal{D}_F$, so it divides $\nu\mathcal{D}_F$ exactly $2k$ times. Together with the factor $1/2$, this contributes a factor of k to the exponent t_r on the right hand side. On the left hand side, we note that $2k$ is equal to the multiplicity with which r divides the norm $(D-x^2)/4$ of $\nu\mathcal{D}_F$. Hence the number $(D-x^2)/(4N)$ contains precisely $2k-1 = 2(k-1)+1$ factors of r. Thus indeed, using the definition of F, we also find on this side an added factor of $(k-1)+1 = k$. □

3.3 From $\mathcal{M}$ to X_N

The main goal of the sections that follow will be to reinterpret the Arakelov degrees of the stacks $\mathcal{X}_\vartheta$ for $\vartheta \in \mathcal{V}$ as quantities involving cross-ratios of the function $j_N : X_N \xrightarrow{\sim} \mathbb{P}^1$. Most terms appearing in the formula of the Arakelov degree are straightforward, the most profound one being the length of certain strictly Henselian local rings on stacks. This section aims to relate these numbers to lengths of rings associated with the algebraic curve X_N instead.

Proposition 3.3.1. *Recall that $w_i := \#\mathcal{O}_i^\times$. Then we have*

$$\deg(\mathcal{X}_\vartheta) = \frac{1}{w_1 w_2} \sum_{\mathfrak{r} \subset \mathcal{O}_L} \log(|\mathbb{F}_{\mathfrak{r}}|) \sum_{x \in \mathcal{X}_\vartheta(k)} \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{1,x}} \otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathcal{M}_x}} \mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{2,x}}),$$

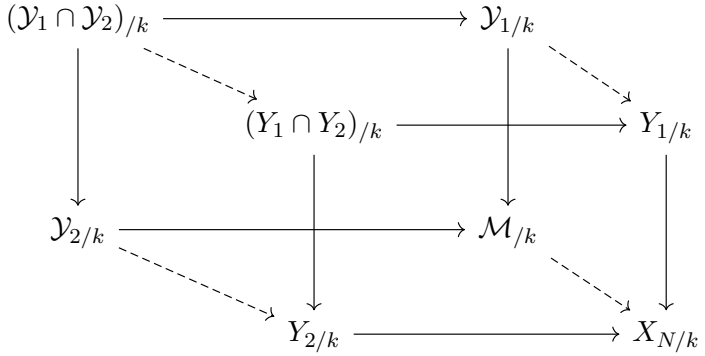
where the sum is taken over all isomorphism classes $x = (\boldsymbol{A}_1, \boldsymbol{A}_2, f) \in \mathcal{X}_\vartheta(k)$ and where $k = \overline{\mathbb{F}}_{\mathfrak{r}}$.

Proof. Recall that by definition, $\mathcal{J} = \mathcal{Y}_1 \times_{\mathcal{M}} \mathcal{Y}_2$. This means that

$$\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_{\vartheta,x}} = \mathcal{O}^{\mathrm{sh}}_{\mathcal{J}_x} = \mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{1,x}} \otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathcal{M}_x}} \mathcal{O}^{\mathrm{sh}}_{\mathcal{Y}_{2,x}}.$$

Further invoking Theorem 4.1.3 in [Phi15], which says that $|\mathrm{Aut}(x)| = w_1 w_2$ for all points x, the result follows from the definition of the Arakelov degree. □

Let $Y_i \to X_N$ be the closed subscheme supported on the $4h_i$ points with CM by $\mathcal{O}_i$ for $i \in \{1, 2\}$. As is outlined in Section II of [Vis89], we have a natural map $\pi : \mathcal{M} \to X_N$. As X_N is smooth and $\mathcal{M}$ is a Deligne-Mumford stack, by the *miracle flatness theorem*, the map π must in fact be flat. We have summarised the situation in the cube below.



We proceed with the following useful lemma.

Lemma 3.3.2. *Two triples $(\boldsymbol{A}_1, \boldsymbol{A}_2, f), (\boldsymbol{A}_1', \boldsymbol{A}_2', g) \in \mathcal{X}_\vartheta(k)$ are isomorphic if and only if $\boldsymbol{A}_i \cong \boldsymbol{A}_i'$ for $i \in \{1, 2\}$.*

Proof. To give a morphism $(\mathbf{A}_1, \mathbf{A}_2, f) \to (\mathbf{A}_1', \mathbf{A}_2', g)$ is to give morphisms $\varphi : \mathbf{A}_1 \to \mathbf{A}_1'$ and $\psi : \mathbf{A}_2 \to \mathbf{A}_2'$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbf{A}_1 & \xrightarrow{\varphi} & \mathbf{A}_1' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ \mathbf{A}_2 & \xrightarrow{\psi} & \mathbf{A}_2' \end{array}$$

Such a morphism $(\mathbf{A}_1, \mathbf{A}_2, f) \to (\mathbf{A}_1', \mathbf{A}_2', g)$ is an isomorphism if and only if both φ and ψ are isomorphisms. This proves one direction.

Conversely, consider two triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ and $(\mathbf{A}_1', \mathbf{A}_2', g)$ and suppose that $\mathbf{A}_i$ and $\mathbf{A}_i'$ are isomorphic for $i \in \{1, 2\}$. Choose $\varphi : \mathbf{A}_1 \to \mathbf{A}_1'$ as such an isomorphism and set $\psi = g \circ \varphi \circ f^{-1}$. Being the composition of isomorphisms, this map is also an isomorphism and it makes the diagram commute; thus this describes an isomorphism between the triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ and $(\mathbf{A}_1', \mathbf{A}_2', g)$ and the bijection has been proved. □

This is useful, as the set of CM-points without any additional information has a very well-understood structure, as we will see in the next section. For now, we content ourselves with proving the following key proposition, which establishes our goal for this section.

Proposition 3.3.3. *Fix a prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ and a geometric point $x = (\boldsymbol{A}_1, \boldsymbol{A}_2, f) \in \mathcal{X}_\vartheta(k)$ where $k = \overline{\mathbb{F}}_\mathfrak{r}$. Then*

$$\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta,x}\big) = 2\,\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x} \otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N,x}} \mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big).$$

Proof. We will use a few results on stacky intersection theory from [Vis89] for the map $\pi : \mathcal{M} \to X_N$. All local rings we consider are for the étale topology on the respective schemes. On the rational Chow group, Definition 3.6 states that the proper push forward of a cycle D on a stack is defined to be the image cycle multiplied by the relative degree of the map from the cycle and its image. Since k is perfect and the number of automorphisms for CM false elliptic curves is constant, Corollary 2.5 in [Vis89] implies that this degree is the reciprocal of the size of the automorphism group of our point. Using Lemma 4.1.3 in [Phi15], we then find

$$\pi_*(\mathcal{Y}_i) = \frac{1}{w_i} Y_i.$$

In addition, the above also shows that pushing forward the stacky intersection $\mathcal{Y}_1 \cap \mathcal{Y}_2$ along π will divide the result by $\operatorname{Aut}(x) = w_1 w_2$; whence

$$\pi_*(\mathcal{Y}_1 \cdot \mathcal{Y}_2)_x = \frac{1}{w_1 w_2} \operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta,x}\big).$$

As we know π to be flat, we have a well-defined notion of a pull-back of cycles along π. A general false elliptic curve admits only two automorphisms, namely ± 1. Therefore, $\deg(\pi) = 1/2$. Very generally, one has the formulae

$$\pi^*(Y_i) = \deg(\pi) w_i \mathcal{Y}_i = \frac{w_i}{2} \mathcal{Y}_i, \quad \text{so that} \quad \pi^*\pi_* = \deg(\pi) = \frac{1}{2}.$$

We may now use the *projection formula* from stacky intersection theory (compare with the Stacks Project [0B0C]) to compute that on the other

hand, it holds that

$$\begin{aligned}\pi_*(\mathcal{Y}_1 \cdot \mathcal{Y}_2)_x &= \pi_*\Big(\frac{2}{w_1}\pi^*(Y_1)\cdot \mathcal{Y}_2\Big)_x \\ &= \frac{2}{w_1}\pi_*\left(\pi^*(Y_1)\cdot \mathcal{Y}_2\right)_x = \frac{2}{w_1}\left(Y_1 \cdot \pi_*(\mathcal{Y}_2)\right)_x \\ &= \frac{2}{w_1}\Big(Y_1 \cdot \frac{1}{w_2}Y_2\Big)_x = \frac{2}{w_1 w_2}(Y_1 \cdot Y_2)_x \\ &= \frac{2}{w_1 w_2}\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x} \otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N,x}} \mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big).\end{aligned}$$

Now compare these two expressions for $\pi_*(\mathcal{Y}_1 \cdot \mathcal{Y}_2)_x$. □

For notational convenience, we let $(Y_1 \times Y_2)_\vartheta(k)$ denote the set of pairs of CM-points over k that induce $\vartheta : \mathcal{O}_L \to R_N/\mathfrak{m}_N$.

Corollary 3.3.4. *It holds that*

$$\deg(\mathcal{X}_\vartheta) = \frac{2}{w_1 w_2}\sum_{\mathfrak{r}\subset\mathcal{O}_L}\log(|\mathbb{F}_\mathfrak{r}|)\sum_{(Y_1\times Y_2)_\vartheta(k)}\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,\boldsymbol{A}_1}\otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N}}\mathcal{O}^{\mathrm{sh}}_{Y_2,\boldsymbol{A}_2}\big).$$

Proof. Starting with Proposition 3.3.1, we use the independence proved in Lemma 3.3.2 of the isomorphism class of a triple from its third component to replace the sum over $x \in \mathcal{X}_\vartheta(k)$ by a sum $(\mathbf{A}_1, \mathbf{A}_2) \in (Y_1 \times Y_2)_\vartheta(k)$, using that those pairs for which $\mathbf{A}_1$ and $\mathbf{A}_2$ are not isomorphic yield no contribution because the points do not intersect. Next, we replace $\mathrm{length}\big(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\vartheta,x}\big)$ by its scheme-theoretic analogue using Proposition 3.3.3 above to complete the proof. □

3.4 Group actions

Let $W_N = \{1, w_p, w_q, w_N\}$ denote the Atkin-Lehner group, consisting of the identity and three non-trivial involutions. It is explained in Phillips's thesis [Phi15] how the group $\mathrm{Pic}(K_i)\times W_N$ acts on the set of false elliptic curves with CM by $\mathcal{O}_i$ over any $\mathcal{O}_L$-scheme S. It is important to know how the group actions on these embeddings relate to the reflex ideal. This is established in the following quick lemmas.

Lemma 3.4.1. *Let $(\boldsymbol{A}_1, \boldsymbol{A}_2)$ be a CM-pair inducing the morphism $\vartheta \in \mathcal{V}$. Then for any pair of ideals $([c_1], [c_2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$, the CM-pair $([c_1]\cdot\boldsymbol{A}_1, [c_2]\cdot\boldsymbol{A}_2)$ also induces the map $\vartheta \in \mathcal{V}$.*

Proof. This is almost immediate from the disccusion in [Phi15] on page 39. There the action of the product of the Picard groups on the CM pairs of Shimura curves is described and it is shown that this leaves the induced ring maps $\mathcal{O}_{K_j} \to B_N/m_N$ invariant. □

Lemma 3.4.2. *Let $(\boldsymbol{A}_1, \boldsymbol{A}_2)$ be a CM-pair inducing the reflex ideal $\mathfrak{a} = \mathfrak{p}_i\mathfrak{q}_j \in \mathcal{I}$. Then the CM-pairs $(w_p \cdot \boldsymbol{A}_1, \boldsymbol{A}_2)$ and $(\boldsymbol{A}_1, w_p \cdot \boldsymbol{A}_2)$ induce reflex ideal $\mathfrak{p}_k\mathfrak{q}_j$ with $k \neq i$, and the CM-pairs $(w_q \cdot \boldsymbol{A}_1, \boldsymbol{A}_2)$ and $(\boldsymbol{A}_1, w_q \cdot \boldsymbol{A}_2)$ induce reflex ideal $\mathfrak{p}_i\mathfrak{q}_l$ with $l \neq j$.*

Proof. As described in [Phi15], the action of w_p is given by conjugation with an element π in B_N of norm p on the embedding $\iota : R_N \to \mathrm{End}(A)$. This means that the action on ϑ, which is induced by ι and κ, is also given by conjugation by π. Extending scalars to $\mathbb{Q}_p$, Equation (2.20) in [HY12] shows that we have the decomposition $R_N = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\pi$ with the action of π given by $x\pi = \pi x^\sigma$, where σ is the unique automorphism of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$. Here we may choose $\mathbb{Z}_{p^2} = \vartheta_1(K_1) \otimes \mathbb{Z}_p$. Then this shows that conjugating with π induces the non-trivial automorphism on the image of ϑ and thus will change the reflex prime above p, as claimed. The situation for w_q is analogous. □

Corollary 3.4.3. *For any given $\vartheta \in \mathcal{V}$, the space $(Y_1 \times Y_2)_\vartheta(k)$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$. In addition, the set $\mathcal{V}$ itself is a principal homogenous space for the action of $W_N \times W_N$ and the set $\mathcal{I}$ is so for $W_N \subset W_N \times W_N$ acting diagonally.*

Proof. The first two claims follow from Lemma 3.4.1 and Lemma 3.4.2 above, together with the elementary fact that $\#\mathcal{V} = 16$ and the knowledge that the set of CM-points for $\mathcal{O}_i$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_i) \times W_N$, as shown in [Phi15]. For the third, note that w_p and w_q change the reflex ideal at one prime, so in order to leave it invariant, we must act by the same operator on both CM-points. □

Lemma 3.4.4. *For any CM-point P, it holds that $P' \in \mathrm{Pic}(K_i) \cdot w_q(P)$.*

Proof. Recall that $P' := w_p(\mathrm{Frob}_p(P))$. By applying w_p to the above equation, it follows that it suffices to show that $\mathrm{Frob}_p(P) \in \mathrm{Pic}(K_i) \cdot w_N(P)$. As the set of CM-points for $\mathcal{O}_i$ is a principal homogeneous space for the action of $\mathrm{Pic}(K_i) \times W_N$, by Lemma 3.4.3 above we reduce to comparing the reflex ideal associated with the pairing of the points $\mathrm{Frob}_p(P)$ and $w_N(P)$ with any other CM-point. Now indeed, by Lemma 3.4.2, the latter induces the Galois conjugate reflex ideal compared to P, which coincides with the Galois action of $\mathrm{Frob}_p(P)$. □

3.5 Proof of Theorem A

In order to obtain a new formula for $\deg(X_\vartheta)$ for $\vartheta \in \mathcal{V}$, as a result of Corollary 3.3.4, we must proceed to analyse the quantities

$$\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,\mathbf{A}_1} \otimes_{\mathcal{O}^{\mathrm{sh}}_{X_N}} \mathcal{O}^{\mathrm{sh}}_{Y_2,\mathbf{A}_2}\big)$$

for $(\mathbf{A}_1, \mathbf{A}_2) \in (Y_1 \times Y_2)_\vartheta(k)$. This analysis is facilitated by the existence of the isomorphism

$$j_N : X_N \xrightarrow{\sim} \mathbb{P}^1.$$

We will need the following theorem.

Theorem 3.5.1. *For any positive integer N, the Shimura curve X_N is semistable and has good reduction at all the primes not dividing N.*

This is proved for instance in Morita's master thesis [Mor70]. Let $\mathfrak{r} \subset \mathcal{O}_L$ be a prime and let $\mathfrak{X}_{N,\mathfrak{r}}$ be a semistable model of X_N over $\operatorname{Spec}(\mathcal{O}_{L,\mathfrak{r}})$. Further, let $W_\mathfrak{r}$ denote the ring of integers of the completion of the maximal unramified extension of $L_\mathfrak{r}$. By Theorem 3.5.1, if $\mathfrak{r} \nmid N$, the completed local ring of any $W_\mathfrak{r}$-point on $\mathfrak{X}_{N,\mathfrak{r}}$ must be isomorphic to $W_\mathfrak{r}[\![x]\!]$. If $\mathfrak{r} \mid N$, then because we chose a semistable model of $\mathfrak{X}_{N,r}$, at all geometric singular points on the special fibre the completed local ring is isomorphic to $W_\mathfrak{r}[\![x,y]\!]/(xy - \varpi)$, where ϖ denotes a uniformiser inside $W_\mathfrak{r}$. Because all CM-points are globally defined over the fields H_i for $i \in \{1,2\}$ by Corollary 2.1.5, both of which are unramified at r because we assume r be coprime to both D_i for $i \in \{1,2\}$, CM-points can never reduce to singular points on the special fibre of $\mathfrak{X}_{N,\mathfrak{r}}$ by Remark 2.4.3 in [Rom13]. As such, the completed local ring at a geometric CM-point on $\mathfrak{X}_{N,\mathfrak{r}}$ is always isomorphic to $W_\mathfrak{r}[\![x]\!]$.

Similar to Proposition 2.26 in [HY12], we find that the completion of the strictly Henselian local ring of a CM point on the special fibre is isomorphic to $W_\mathfrak{r}$. Therefore, for $x \in (Y_1 \times Y_2)_\vartheta(k)$, we obtain two maps

$$\operatorname{Spec}(W_\mathfrak{r}) \to \operatorname{Spec}(\mathcal{O}^{\mathrm{sh}}_{\mathfrak{X}_N,x}) \xrightarrow{\sim} \operatorname{Spec}(W_\mathfrak{r}[\![X]\!])$$

induced by the unique (up to local units) scalar multiple $j_{N,\mathfrak{r}}$ of j_N that induces an isomorphism over $W_\mathfrak{r}$ away from the singular points, if there are any. These maps correspond to two ring maps $W_\mathfrak{r}[\![X]\!] \to W_\mathfrak{r}$.

Lemma 3.5.2. *Let R be a commutative ring and consider two maps $f_1, f_2 \colon R[x] \to R$ defined by $f_1(x) = a$ and $f_2(x) = b$ for certain $a, b \in R$. Then*

$$R \otimes_{f_1,R[x],f_2} R \cong R/(a-b).$$

We omit the proof, as it is just commutative algebra. If we let $P_{\mathbf{A}_i}$ denote the CM-point on X_N defining the CM-false elliptic curve $\mathbf{A}_i$, then the lemma above has the following immediate corollary.

Corollary 3.5.3. *For any prime $\mathfrak{r} \subset \mathcal{O}_L$ and pair of CM points $x = (\boldsymbol{A}_1, \boldsymbol{A}_2) \in (Y_1 \times Y_2)_\vartheta(k)$ where $k = \overline{\mathbb{F}}_\mathfrak{r}$, it holds that*

$$\operatorname{length}\big(\mathcal{O}^{\mathrm{sh}}_{Y_1,x} \otimes_{\mathcal{O}^{\mathrm{sh}}_{\mathfrak{X}_N,x}} \mathcal{O}^{\mathrm{sh}}_{Y_2,x}\big) = v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{\boldsymbol{A}_1}) - j_{N,\mathfrak{r}}(P_{\boldsymbol{A}_2})\big).$$

Proof. We apply Lemma 3.5.2 to equate the left hand side of the above expression to length $\big(W_\mathfrak{r}/\big(j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})\big)\big)$. We leave it to the reader to check that this length is just the $\mathfrak{r}$-adic valuation. □

Corollary 3.5.4. *Let $\vartheta \in \mathcal{V}$. Then it holds that*

$$\deg(\mathcal{X}_\vartheta) = \frac{2}{w_1 w_2} \sum_{\mathfrak{r} \subset \mathcal{O}_L} \log(|\mathbb{F}_\mathfrak{r}|) \sum_{[c_1],[c_2]} v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{[c_1]\cdot \boldsymbol{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot \boldsymbol{A}_2})\big),$$

where the latter sum ranges over all $[c_1] \in \operatorname{Pic}(K_1)$ and $[c_2] \in \operatorname{Pic}(K_2)$.

Proof. First substitute the result from Corollary 3.5.3 into the expression found in Corollary 3.3.4. The proof is then complete by Corollary 3.4.3, which identifies $(Y_1 \times Y_2)_\vartheta(k)$ as a principal homogeneous space for the action of the group $\operatorname{Pic}(K_1) \times \operatorname{Pic}(K_2)$. □

Now let $\mathcal{V}' = (W_q \times W_q) \cdot \vartheta \subset \mathcal{V}$ where $W_q = \{1, w_q\} \subset W_N$. We will study the sum

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) \deg(\mathcal{X}_\vartheta).$$

Proposition 3.5.5. *Let $\vartheta \in \mathcal{V}$. Then it holds that*

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) \deg(\mathcal{X}_\vartheta) = \frac{2}{w_1 w_2} \log \operatorname{Nm}\big[j_N(P_{\boldsymbol{A}_1}), j_N(P'_{\boldsymbol{A}_1}), j_N(P_{\boldsymbol{A}_2}), j_N(P'_{\boldsymbol{A}_2})\big].$$

Proof. The key idea is that for any prime $\mathfrak{r} \subset \mathcal{O}_L$, the sum

$$\sum_{\vartheta \in \mathcal{V}'} \delta(\vartheta) v_\mathfrak{r}\big(j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})\big)$$

is equal to

$$v_\mathfrak{r}\left(\frac{j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})}{j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{\mathbf{A}_2})} \cdot \frac{j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P_{\mathbf{A}_1}) - j_{N,\mathfrak{r}}(w_q P_{\mathbf{A}_2})}\right).$$

This cross-ratio is independent of the precise way we scaled our function $j_{N,\mathfrak{r}}$, and as such, we may replace every instance of it by our original fixed choice of j_N. Next, by Lemma 3.4.4, we find that for certain classes $[d_i] \in \mathrm{Pic}(K_i)$ for $i \in \{1,2\}$, we have the equality $w_q P_{\mathbf{A}_i} = [d_i] \cdot P'_{\mathbf{A}_i}$. Therefore, we may further rewrite this sum to

$$v_{\mathfrak{r}}\left(\frac{j_N(P_{\mathbf{A}_1}) - j_N(P_{\mathbf{A}_2})}{j_N([d_1]\cdot P'_{\mathbf{A}_1}) - j_N(P_{\mathbf{A}_2})} \cdot \frac{j_N([d_1]\cdot P'_{\mathbf{A}_1}) - j_N([d_2]\cdot P'_{\mathbf{A}_2})}{j_N(P_{\mathbf{A}_1}) - j_N([d_2]\cdot P'_{\mathbf{A}_2})}\right).$$

If we now introduce the sum over $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$, the twist by the classes $[d_i] \in \mathrm{Pic}(K_i)$ for $i \in \{1,2\}$ can be ignored, and we obtain

$$\sum_{([c_1],[c_2])} v_{\mathfrak{r}}\left(\frac{j_{N,\mathfrak{r}}(P_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P'_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P_{[c_2]\cdot\mathbf{A}_2})} \cdot \frac{j_{N,\mathfrak{r}}(P'_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P'_{[c_2]\cdot\mathbf{A}_2})}{j_{N,\mathfrak{r}}(P_{[c_1]\cdot\mathbf{A}_1}) - j_{N,\mathfrak{r}}(P'_{[c_2]\cdot\mathbf{A}_2})}\right).$$

Now recall Shimura's reciprocity law, Corollary 2.1.5, which has the consequence that taking an average over the class groups amounts to taking the norm of the cross ratio above in the unramified field extension H_1H_2/L. In other words,

$$\prod_{[c_1],[c_2]} \left[j_N(P_{[c_1]\cdot\mathbf{A}_1}), j_N(P'_{[c_1]\cdot\mathbf{A}_1}), j_N(P_{[c_2]\cdot\mathbf{A}_2}), j_N(P'_{[c_2]\cdot\mathbf{A}_2})\right]$$

is equal to the norm $\mathrm{Nm}_L^{H_1H_2}[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})]$. Combining all of this, using Corollary 3.5.4, we have proved that the left hand side of the proposition is equal to

$$\frac{2}{w_1w_2}\sum_{\mathfrak{r}\subset\mathcal{O}_L} \log(|\mathbb{F}_{\mathfrak{r}}|)v_{\mathfrak{r}}\left(\mathrm{Nm}_L^{H_1H_2}\left[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})\right]\right).$$

We thus complete the proof is we can show for any $x \in L$ that

$$\sum_{\mathfrak{r}\subset\mathcal{O}_L} \log(|\mathbb{F}_{\mathfrak{r}}|)v_{\mathfrak{r}}(x) = \log(\mathrm{Nm}(x)), \quad \text{so that} \quad \prod_{r\subset\mathcal{O}_L} |\mathbb{F}_{\mathfrak{r}}|^{v_{\mathfrak{r}}(x)} = \mathrm{Nm}(x).$$

Indeed, this follows by factoring the principal ideal $x\mathcal{O}_L$ into prime ideals and then using the definition of the ideal norm. □

Proof. (of Theorem A) We exponentiate the result of Proposition 3.5.5 to find that

$$\prod_{\vartheta\in\mathcal{V}'} \exp\big(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\big) = \mathrm{Nm}\left[j_N(P_{\mathbf{A}_1}), j_N(P'_{\mathbf{A}_1}), j_N(P_{\mathbf{A}_2}), j_N(P'_{\mathbf{A}_2})\right]^{\frac{2}{w_1w_2}}$$

so that we reduce to showing that

$$\prod_{\vartheta\in\mathcal{V}'}\exp\bigl(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\bigr)=\pm\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}}F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}.$$

Now we recall the result of Theorem 3.2.5, and on both sides we now take a product over all $\nu\in\mathcal{D}_F^{-1,+}$ with $\mathrm{tr}(\nu)=1$. We then obtain that

$$\begin{aligned}\prod_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}}F\left(\frac{D-x^2}{4N}\right)^{\delta(x)}&=\prod_{\substack{\nu\in\mathcal{D}_F^{-1,+}\\ \mathrm{tr}(\nu)=1}}\prod_{\mathfrak{a}\in\mathcal{I}}\exp\bigl(\delta(\mathfrak{a})X(\mathfrak{a},\nu)\bigr)\\ &=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\Bigl(\delta(\mathfrak{a})\sum_{\substack{\nu\in\mathcal{D}_F^{-1,+}\\ \mathrm{tr}(\nu)=1}}X(\mathfrak{a},\nu)\Bigr)=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\bigl(\delta(\mathfrak{a})X(\mathfrak{a})\bigr).\end{aligned}$$

We have thus reduced to showing that

$$\prod_{\vartheta\in\mathcal{V}'}\exp\bigl(\delta(\vartheta)\deg(\mathcal{X}_\vartheta)\bigr)=\prod_{\mathfrak{a}\in\mathcal{I}}\exp\bigl(\delta(\mathfrak{a})X(\mathfrak{a})\bigr).$$

Both sides of this equation display a product with four factors, so we complete the proof if we make four pairs of equal factors. Choose $\vartheta\in\mathcal{V}'$ arbitrarily and assume without loss of generality that its associated reflex ideal equals $\mathfrak{a}_\vartheta=\mathfrak{p}_1\mathfrak{q}_1\in\mathcal{I}$. Then by construction,

$$\delta(\vartheta)\deg(\mathcal{X}_\vartheta)=\delta(\mathfrak{a})X(\mathfrak{a}).$$

By Lemma 3.4.2, the other elements of $\mathcal{V}'$, explicitly $(w_q,1)\cdot\vartheta$, $(1,w_q)\cdot\vartheta$ and $(w_q,w_q)\cdot\vartheta$, induce reflex ideals $\mathfrak{p}_1\mathfrak{q}_2$, $\mathfrak{p}_1\mathfrak{q}_2$ and $\mathfrak{a}$ respectively. To complete the proof, we will show that $X(\mathfrak{a})=X(\sigma(\mathfrak{a}))$ for any $\mathfrak{a}\in\mathcal{I}$. For if so, then the latter two elements of $\mathcal{V}'$ also have equal contributions as the ideals $\sigma(\mathfrak{p}_1\mathfrak{q}_2)=\mathfrak{p}_2\mathfrak{q}_1$ and $\sigma(\mathfrak{a})=\mathfrak{p}_2\mathfrak{q}_2$ respectively, and we win.

As $X(\mathfrak{a})$ is the sum over all $X(\mathfrak{a},\nu)$, it suffices to examine these latter quantities. Indeed, Theorem 3.1.3 shows that $X(\mathfrak{a},\nu)=X(\sigma(\mathfrak{a}),\sigma(\nu))$, as is obtained by applying σ to all quantities occurring in that theorem. Since we sum over all $\nu\in\mathcal{D}_F^{-1,+}$ of unit trace, a set which is stable under the action of σ, equality follows and the proof is complete. □

CHAPTER 4

Genus theory and quaternion algebras

In this chapter we carry out **Step 1** of our p-adic analytic proof of Theorem B as outlined in Section 2.4. First, we construct two exact sequences using elementary arithmetic in biquadratic fields and basic class field theory. Next, we will explore genus theory, a study pioneered by Carl Friedrich Gauß, which allows us to describe a map connecting these two exact sequences to form a longer one. We proceed to define an F-quadratic form $\det_F$ on B_q that refines the quaternion norm in the sense that $\mathrm{tr} \circ \det_F = \mathrm{Nm}$ and we give various formulae to compute it concretely. Finally, we combine these preliminaries to prove the bijective nature of an explicit and purely algebraic construction that links quaternions in a rational quaternion algebra with class number 1 (or equivalently, with type number 1) to $\mathcal{O}_L$-ideals of a specified norm. This construction is used to rewrite the left hand side of Theorem B into a more useful form in Section 6.1.

Throughout this chapter, we will let $\epsilon_F \in \mathcal{O}_F^\times$ denote a fundamental unit for the field F. By Dirichlet's Unit Theorem, the group $\mathcal{O}_L^\times$ is, up to torsion, also free of rank 1 and as such, we may also specify a fundamental unit $\epsilon_L \in \mathcal{O}_L^\times$. In particular, this means that

$$\mathcal{O}_F^\times = \{\pm 1\} \times \langle \epsilon_F \rangle \quad \text{and} \quad \mathcal{O}_L^\times = \mu_L \times \langle \epsilon_L \rangle,$$

where $\mu_L \subset \mathcal{O}_L^\times$ denotes the finite subgroup of roots of unity in L.

Our efforts are aimed at studying B_q; the definite quaternion algebra over $\mathbb{Q}$ with discriminant $-q$. Recall that $R_q \subset B_q$ denotes a maximal order and that we assume that it is *unique* up to conjugation. In Section 4.4, we will explain how the two embeddings $\alpha_i : \mathcal{O}_i \to R_q$ for $i \in \{1, 2\}$ allow us to view B_q as a 1-dimensional L-vector space. In Section 4.5, we explain how the set of all pairs of embeddings $\mathcal{O}_i \to B_q$ for $i \in \{1, 2\}$ carries a faithful action of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ and how one can associate a *reflex ideal* $\mathfrak{q}_1 \subset \mathcal{O}_F$ to any pair of embeddings in the orbit of (α_1, α_2).

For any choice of $[c_1] \in \mathrm{Pic}(K_1)$ and $[c_2] \in \mathrm{Pic}(K_2)$, we will show the existence of an F-quadratic form $\det_F[c_1, c_2] : B_q \to F$ with the property that $\mathrm{tr} \circ \det_F[c_1, c_2] = \mathrm{Nm}$. The following is proved in [HY12] and encompasses the main result of this chapter.

Theorem 4.0.1. *For any $\nu \in F^+$, the number of triples*

$$(b, [c_1], [c_2]) \in (\mathcal{O}_1^\times \setminus R_q \,/\, \mathcal{O}_2^\times) \times \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$$

satisfying the property that $\det_F[c_1, c_2](b) = \nu$, equals $\rho(\nu \mathfrak{q}_1^{-1} \mathcal{D}_F)$.

Proof. The assumption that R_q is the only maximal order of B_q means for $i \in \{1, 2\}$ that any elliptic curve E_i with CM by $\mathcal{O}_i$ with supersingular

reduction at q must satisfy $\mathrm{End}(E_i) \cong R_q$. Then $\mathrm{Hom}(E_1, E_2) \cong R_q$ and we may identify the form $\deg_{\mathrm{CM}}$ in [HY12] by the form $\det_F$ introduced above. Without defining $O_\ell(\nu, E_1, E_2)$ here, we remark that the proof of Proposition 2.18 in [HY12] shows that the quantity we are trying to count is equal to

$$\frac{2}{\#\mathcal{O}_1^\times \#\mathcal{O}_2^\times} \sum_{[c_1],[c_2]} \sum_{\substack{\phi \in B \\ \det_F [c_1,c_2](\phi) = \nu}} \mathbb{1}_{R_q}(\phi) = \prod_\ell O_\ell(\nu, E_1, E_2) = \rho(\nu \mathfrak{q}_1^{-1} \mathcal{D}_F),$$

where the second equality follows from Corollary 2.34 in [HY12]. □

In [HY12], this counting problem is tackled using an adèlic approach, which has the drawback that it is not very explicit. The main purpose of this chapter is to describe an explicit bijection between the two sets whose cardinalities are related in Theorem 4.0.1 in the case that the quaternion algebra B_q has a unique maximal order, which has the added benefit of being global and not adèlic in nature. We sketch this now.

Any pair $([c_1], [c_2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ yields an L-vector space structure on B and thus allows us to choose an L-linear isomorphism $\iota[c_1, c_2] : B_q \xrightarrow{\sim} L$. Even though this isomorphism is not unique, one may define an L-ideal associated with $b \in B_q$ by writing $I[c_1, c_2]_b := \iota[c_1, c_2](b)/\iota[c_1, c_2](R_q)$. The following is this chapter's main result.

Theorem 4.0.2. *For any $\nu \in F^+$, the association $(b, [c_1], [c_2]) \mapsto I[c_1, c_2]_b$ establishes a bijection between the set of*

$$(b, [c_1], [c_2]) \in (\mathcal{O}_1^\times \setminus R_q \,/\, \mathcal{O}_2^\times) \times \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$$

with the property that $\det_F[c_1, c_2](b) = \nu$ and the set of integral ideals $I \subset \mathcal{O}_L$ such that $\mathrm{Nm}_{L/F}(I) = \nu \mathfrak{q}_1^{-1} \mathcal{D}_F$.

Before we start, we record here some important properties of the field F and the character χ that we will use numerous times throughout all remaining chapters.

Lemma 4.0.3. *It holds that $\chi(\mathcal{D}_F) = -1$. In addition, $\epsilon_F \gg 0$, and therefore $\#\mathrm{Pic}(F)^+ = 2\#\mathrm{Pic}(F)$.*

Proof. The extension L/F is a CM-extension unramified at all finite places, so χ is totally odd and the first statement is immediate. Therefore, the ideal $(\sqrt{D})$ cannot be trivial in the narrow class group. If ϵ_F were not totally positive, then $(\sqrt{D}) = (\epsilon_F \sqrt{D})$ would have been trivial; therefore $\epsilon_F \gg 0$. The final statement also follows. □

4.1 Two exact sequences

To get started, we need the following simple lemma.

Lemma 4.1.1. *The torsion subgroup $\mu_L \subset \mathcal{O}_L^\times$ is given by $\mathcal{O}_1^\times \mathcal{O}_2^\times$.*

Proof. For $\zeta_n \in L$ it must hold that $\varphi(n) \leq 4$, where φ denotes Euler's totient function. This leaves only a few options: if $n \in \{5, 10\}$, then $L = \mathbb{Q}(\zeta_5)$ is not biquadratic. If $\zeta_8 \in L$, then $L = \mathbb{Q}(\zeta_8)$ and L has the quadratic subfields $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, but none of these have coprime discriminants, so $L = \mathbb{Q}(\zeta_8)$ is not among the fields we consider. If $\zeta_{12} \in L$, then $L = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{3})$, satisfying the claim from the lemma. In all other cases, the torsion of $\mathcal{O}_L^\times$ only defines at most a quadratic extension of $\mathbb{Q}$, and as such will come from one of the imaginary quadratic subfields of L. □

Proposition 4.1.2. *The following sequence is exact:*

$$1 \to \{\pm 1\} \to \mathcal{O}_1^\times \times \mathcal{O}_2^\times \xrightarrow{(x,y)\mapsto xy} \mathcal{O}_L^\times \xrightarrow{\mathrm{Nm}_{L/F}} \mathcal{O}_F^{\times,+}.$$

Proof. We check each entry. Exactness at $\{\pm 1\}$ is trivial. Exactness at $\mathcal{O}_1^\times \times \mathcal{O}_2^\times$ is also clear, because we assume $D_1 \neq D_2$ and because $\mathcal{O}_i^\times = \{\pm 1\}$ unless $D \in \{-3, -4\}$, both unit groups only share $\{\pm 1\}$ in all cases. It remains to prove exactness at $\mathcal{O}_L^\times$. Clearly, for any $u_i \in \mathcal{O}_i^\times$, we have that

$$\mathrm{Nm}_{L/F}(u_i) = \mathrm{Nm}_{K_i/\mathbb{Q}}(u_i) = 1,$$

because the norm from an imaginary quadratic field is positive definite. For the other inclusion, let $u \in \mathcal{O}_L^\times$ be given such that $\mathrm{Nm}_{L/F}(u) = 1$. By Lemma 4.1.1 above, we have

$$\mathcal{O}_L^\times = (\mathcal{O}_1^\times \mathcal{O}_2^\times) \times \langle \epsilon_L \rangle$$

As a result, we may write that $u = u_1 u_2 \epsilon_L^k$ for some $u_1 \in \mathcal{O}_1^\times$ and $u_2 \in \mathcal{O}_2^\times$, so that

$$1 = \mathrm{Nm}_{L/F}(u) = \mathrm{Nm}_{L/F}(u_1)\mathrm{Nm}_{L/F}(u_2)\mathrm{Nm}_{L/F}(\epsilon_L^k) = \mathrm{Nm}_{L/F}(\epsilon_L)^k.$$

So $\mathrm{Nm}_{L/F}(\epsilon_L) \in F$ is a kth root of unity. However, F is totally real, and as such, it follows that if $k \neq 0$, it must hold that $\mathrm{Nm}_{L/F}(\epsilon_L) \in \{\pm 1\}$. However, this would imply that the image of $\mathcal{O}_L^\times$ under the map $\mathrm{Nm}_{L/F}$ is at most $\{\pm 1\}$, which is nonsense, as $\mathcal{O}_F^\times \subset \mathcal{O}_L^\times$ and on this free subgroup of rank 1, the map $\mathrm{Nm}_{L/F}$ is just squaring. □

Remark 4.1.3. Note that if $u \in \mathcal{O}_L^\times$, then

$$u^2 \in \mathcal{O}_1^\times \mathcal{O}_2^\times \mathrm{Nm}_{L/F}(\mathcal{O}_L^\times) \subset \mathcal{O}_1^\times \mathcal{O}_2^\times \mathcal{O}_F^{\times,+}.$$

Indeed, since $\mathrm{Nm}_{K_i/\mathbb{Q}}$ is positive definite, it follows for any $u \in \mathcal{O}_L^\times$ that

$$\mathrm{Nm}_{L/\mathbb{Q}}(u) = \mathrm{Nm}_{K_i/\mathbb{Q}}(\mathrm{Nm}_{L/K_i}(u)) = 1.$$

We may then employ the pretty trick of invoking the equality

$$\begin{aligned} u^2 &= u^2 \mathrm{Nm}_{L/\mathbb{Q}}(u) = u^3 \sigma_1(u)\sigma_2(u)\sigma_F(u) \\ &= \mathrm{Nm}_{L/K_1}(u) \cdot \mathrm{Nm}_{L/K_2}(u) \cdot \mathrm{Nm}_{L/F}(u), \end{aligned}$$

showing the claim. This also shows that

$$[\mathcal{O}_F^{\times,+} : \mathrm{Nm}_{L/F}(\mathcal{O}_L^\times)] \leq 2.$$

There are natural maps $\mathrm{Pic}(K_i) \to \mathrm{Pic}(L)$ by sending $I \subset \mathcal{O}_i$ to the ideal $I\mathcal{O}_L \subset \mathcal{O}_L$. Multiplied together, these combine to form a map

$$\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \to \mathrm{Pic}(L).$$

For the second exact sequence, we will again require a small lemma.

Lemma 4.1.4. *For any* $[J] \in \mathrm{Pic}(L)$*,*

$$[J] = [\sigma_F(J)] \in \mathrm{Pic}(L) \big/ \big(\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)\big).$$

Proof. We use a trick similar to the one in Remark 4.1.3. Indeed, we have that

$$\mathrm{Nm}_{L/\mathbb{Q}} : \mathrm{Pic}(L) \to \mathrm{Pic}(\mathbb{Q}) = \{0\}$$

is the trivial map. As such, we find that

$$\begin{aligned} [J] &= [J] + [\mathrm{Nm}_{L/\mathbb{Q}}(J)] = 2[J] + [\sigma_1(J)] + [\sigma_2(J)] + [\sigma_F(J)] \\ &= [\mathrm{Nm}_{L/K_1}(J)] + [\mathrm{Nm}_{L/K_2}(J)] + [\sigma_F(J)] \\ &\equiv [\sigma_F(J)] \mod \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2), \end{aligned}$$

completing the proof. □

Proposition 4.1.5. *The following sequence is exact:*

$$\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \to \mathrm{Pic}(L) \xrightarrow{\mathrm{Nm}_{L/F}} \mathrm{Pic}(F)^+ \xrightarrow{\chi} \{\pm 1\} \to 1.$$

Proof. This time we start checking exactness on the left hand side. At $\{\pm 1\}$ it is clear from the definition and the surjectivity of the restriction map $\mathrm{Gal}(H_F^+/F) \to \mathrm{Gal}(L/F)$. For exactness at $\mathrm{Pic}(F)^+$, we employ a commutative square from class field theory:

$$\begin{array}{ccc} \mathrm{Pic}(L) & \xrightarrow{\sim} & \mathrm{Gal}(H_L/L) \\ {\scriptstyle \mathrm{Nm}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathrm{Pic}(F)^+ & \xrightarrow{\sim} & \mathrm{Gal}(H_F^+/F). \end{array}$$

The image of the norm map in the left column coincides with the image of the restriction map on the right, which is equal to $\mathrm{Gal}(H_F^+/L)$. By definition, this equals the kernel of χ. Finally, we show exactness at $\mathrm{Pic}(L)$. First, similar to before, we have for any $[I_i] \in \mathrm{Pic}(K_i)$,

$$\mathrm{Nm}_{L/F}(I_i) = \mathrm{Nm}_{K_i/\mathbb{Q}}(I_i) \in \mathrm{Pic}(\mathbb{Q}) = \{0\},$$

and as such, indeed $[I_i]$ will be in the kernel. We now let $M \subset H_L$ denote the fixed field of the image of $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ inside of $\mathrm{Pic}(L) \cong \mathrm{Gal}(H_L/L)$. By the above, we may again use class field theory to note that

$$\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \subset \ker(\mathrm{Nm}_{L/F})$$

if and only if

$$\mathrm{Gal}(H_L/M) \subset \ker\big(\mathrm{Gal}(H_L/L) \to \mathrm{Gal}(H_F^+/F)\big) = \mathrm{Gal}(H_L/H_F^+).$$

As such, it follows that $H_F^+ \subset M$. It also follows that to show exactness, it suffices to show that the fields H_F^+ and M are in fact equal. To this end, let $\tau \in \mathrm{Gal}(H_L/L)$ be arbitrary. Then by class field theory, it corresponds to some class $[J] \in \mathrm{Pic}(L)$ and the class $[\sigma_F(J)]$ will correspond to $\sigma_F \tau \sigma_F^{-1} \in \mathrm{Gal}(H_L/L)$. We know that $[J]$ and $[\sigma_F(J)]$ agree up to $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$, and as such, it follows that τ and $\sigma_F \tau \sigma_F^{-1}$ agree in the quotient group $\mathrm{Gal}(M/L)$, i.e. their restrictions to M coincide.

Note that M/L is unramified everywhere because $M \subset H_L$. Hence M/F is only ramified at infinity. If it would be abelian, then by the maximiality of H_F^+ for these properties, it would follow that $M \subset H_F^+$, completing the proof. Indeed, let $\tau \in \mathrm{Gal}(M/L)$. Then the above says that $\tau = \sigma_F \tau \sigma_F^{-1}$ on M. In other words, τ and σ_F commute. Now $\mathrm{Gal}(M/L)$ is abelian by definition of H_L and since $\mathrm{Gal}(M/F)$ is generated by $\mathrm{Gal}(M/L)$ and σ_F, all of which commute, it follows that the whole group $\mathrm{Gal}(M/F)$ is abelian, as desired. □

Our next goal will be to describe a rather subtle map $\mathcal{O}_F^{\times,+} \to \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ that connects the two exact sequences from Propositions 4.1.2 and 4.1.5. To do this, however, we will need some results from genus theory.

4.2 Genus theory

We briefly review Gauß's genus theory in the language of group cohomology. Throughout this section, we let $I(F)$ denote the group of $\mathcal{O}_F$-ideals and $P(F) \subset I(F)$ the subgroup of principal ideals. Also, we let $P(F)^+ \subset P(F)$ denote the subgroup of principal ideals generated by a totally positive element. Then by definition, we have

$$\mathrm{Pic}(F) := I(F)/P(F) \quad \text{and} \quad \mathrm{Pic}(F)^+ := I(F)/P(F)^+.$$

Because $F/\mathbb{Q}$ is of degree 2, its Galois group $G := \mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$ is cyclic. We may use the elements

$$\mathcal{N} := 1 + \sigma \quad \text{and} \quad \Delta := 1 - \sigma$$

in the group ring $\mathbb{Z}[G]$ to define for any G-module the group $H^0(G, A) := \ker(\Delta) = A^\sigma$, the group of σ-invariants, and for any $n \geq 1$:

$$H^{2n-1}(G, A) := \frac{\ker(\mathcal{N})}{\mathrm{im}(\Delta)} \quad \text{and} \quad H^{2n}(G, A) := \frac{A^\sigma}{\mathrm{im}(\mathcal{N})}$$

which makes sense since $\mathcal{N}\Delta = \Delta\mathcal{N} = 1 - \sigma^2 = 0$. We get to where we want to be through a series of quick lemmas.

Lemma 4.2.1. *It holds that $H^1(G, F^{\times,+}) = 0$ and $H^2(G, \mathcal{O}_F^{\times,+}) = 0$.*

Proof. For the first claim, let $x \in F^{\times,+}$ be such that $\mathrm{Nm}(x) = 1$. We must find $y \in F^{\times,+}$ such that $y/\sigma(y) = x$. The existence of such a $y \in F^\times$ is assured by Hilbert 90, so it suffices to verify that it can be chosen totally positively. Indeed, if not, then $y/\sigma(y)$ would be negative under some embedding $F \to \mathbb{R}$, contradicting that $x \gg 0$.

For the second, we take $x \in \mathcal{O}_F^{\times,+}$ such that $\sigma(x) = x$. This means that $x \in \mathbb{Z}^{\times,+} = \{1\}$, and as such, the cohomology group is trivial. □

Lemma 4.2.2. *It holds that $H^1(G, \mathcal{O}_F^{\times,+}) \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. We consider those $x \in \mathcal{O}_F^{\times,+}$ such that $\mathrm{Nm}(x) = 1$. Because they are totally positive, this set equals all of $\mathcal{O}_F^{\times,+}$. Since $\mathcal{O}_F^\times = \{\pm 1\} \times$

$\langle \epsilon_F \rangle$, using Lemma 4.0.3, we find that $\mathcal{O}_F^{\times,+} = \langle \epsilon_F \rangle$. Since $\epsilon_F \sigma(\epsilon_F) = \mathrm{Nm}(\epsilon_F) = 1$, it follows that $\epsilon_F^k / \sigma(\epsilon_F^k) = \epsilon_F^{2k}$, so the elements of the form $y/\sigma(y)$ as $y \in \mathcal{O}_F^{\times,+}$ form a subgroup of index 2. □

Lemma 4.2.3. *It holds that* $P(F)^{+,\sigma}/\mathbb{Q}^{\times,+} \cong \mathbb{Z}/2\mathbb{Z}$. *In addition, it also holds that* $H^1(G, P(F)^+) = 0$.

Proof. The short exact sequence defining $P(F)^+$ reads

$$1 \to \mathcal{O}_F^{\times,+} \to F^{\times,+} \to P(F)^+ \to 1.$$

Using that $F^\sigma = \mathbb{Q}$ and Lemma 4.2.1, part of the long exact sequence associated with this will then read

$$0 \to \mathbb{Q}^{\times,+} \to P(F)^{+,\sigma} \to H^1(G, \mathcal{O}_F^{\times,+}) \to 0 \to H^1(G, P(F)^+) \to 0 \to \dots$$

By Lemma 4.2.2, the first claim follows. Since the latter group we are after is now in between two zeroes, it must be zero itself as well. □

Lemma 4.2.4. *It holds that* $\mathrm{Pic}(F)^+[2] = \mathrm{Pic}(F)^{+,\sigma}$.

Proof. Note that for any ideal $I \in I(F)$, it holds that

$$I \cdot \sigma(I) = (\mathrm{Nm}(I)) \in P(F)^+, \quad \text{and thus} \quad [I] + [\sigma(I)] = 0 \in \mathrm{Pic}(F)^+.$$

As such, it follows that

$$[I] \in \mathrm{Pic}(F)^+[2] \iff [I] = [\sigma(I)] \in \mathrm{Pic}(F)^+ \iff [I] \in \mathrm{Pic}(F)^{+,\sigma},$$

as claimed. □

Theorem 4.2.5. *Let* s *denote the number of primes dividing* $D = D_1 D_2 > 0$. *Then* $\mathrm{Pic}(F)^+[2]$ *is a finite abelian 2-group of rank* $s - 1$, *generated by the ramified primes.*

Proof. The short exact sequence defining $\mathrm{Pic}(F)^+$ reads

$$1 \to P(F)^+ \to I(F) \to \mathrm{Pic}(F)^+ \to 1.$$

As such, the start of its long exact sequence will read

$$1 \to P(F)^{+,\sigma} \to I(F)^\sigma \to \mathrm{Pic}(F)^+[2] \to 1,$$

where we used both Lemma 4.2.3 and Lemma 4.2.4 above. It thus suffices to determine the rank of

$$\frac{I_F^\sigma}{P(F)^{+,\sigma}} \cong \frac{I(F)^\sigma/\mathbb{Q}^{\times,+}}{P(F)^{+,\sigma}/\mathbb{Q}^{\times,+}} \cong \frac{I(F)^\sigma/\mathbb{Q}^{\times,+}}{\mathbb{Z}/2\mathbb{Z}},$$

where we again used Lemma 4.2.3. We complete the proof by establishing an isomorphism

$$I(F)^\sigma/\mathbb{Q}^{\times,+} \to \prod_{r|D} \mathbb{Z}/2\mathbb{Z},$$

in which we send an ideal $I \in I(F)^\sigma$ to the s-tuple $\{v_r(\mathrm{Nm}(I))\}_{r|D}$ mod 2. Since all ramified prime ideals $\mathfrak{r}$ lying over $r \mid D$ are fixed by the Galois action, it is clear that this map is surjective. To show injectivity, let $I = \sigma(I)$ be any ideal in the kernel. By dividing out $\mathfrak{r}^2 = (r) \in \mathbb{Q}^+$ enough times, we may assume without loss of generality that $\mathrm{Nm}(I)$ is coprime with D. Similarly, we may divide I by any inert prime to assume without loss of generality that I is only divisible by primes that split in $F/\mathbb{Q}$. But if $(t) = \mathfrak{t}\sigma(\mathfrak{t})$ for some prime t and $\mathfrak{t} \mid I$, then $\sigma(\mathfrak{t}) \mid \sigma(I) = I$ and as such, it follows that even $t \mid I$. Thus we may divide out such primes too to find that there are no primes left to consider; $I = (1)$ and the claim is proved. □

In other words, the s ramified primes generate the 2-torsion in the narrow class group but since its rank is $s-1$, there must be some relation between them. We wish to identify this relation explicity. It turns out that the origin of this relation depends on the fundamental unit of F.

Theorem 4.2.6. *There exists some $y_F \in \mathcal{O}_F$ with the properties that $\epsilon_F = y_F/\sigma(y_F)$ and $\mathrm{Nm}(y_F) \mid D$. Further,*

$$\sum_{r|\mathrm{Nm}(y_F)} [\mathfrak{r}] = 0 \in \mathrm{Pic}(F)^+.$$

Proof. Since $\epsilon_F \gg 0$ by Lemma 4.0.3, it follows that $\mathrm{Nm}(\epsilon_F) = 1$. The existence of some $y_F \in F^\times$ such that $y_F/\sigma(y_F) = \epsilon_F$ is then assured by Hilbert 90. As in Lemma 4.2.1, it follows that even $y_F \in F^{\times,+}$. In particular it follows that $(y_F) = (\sigma(y_F))$ and as such $(y_F) \in I(F)^\sigma$. Using the same argument as in the proof of Theorem 4.2.5, it follows that we may adjust (y_F) by a rational number $c \in \mathbb{Q}$ to obtain an ideal (cy_F) of norm dividing D. Since $cy_F/\sigma(cy_F) = y_F/\sigma(y_F) = \epsilon_F$, we may rename cy_F to y_F to obtain $\mathrm{Nm}(y_F) \mid D$. Finally, it follows from its norm that the ideal $[(y_F)] = 0 \in \mathrm{Pic}(F)^+$ must factor as the product of the prime ideals lying over the ramified primes dividing it.

It now remains to show that this relation is non-trivial. In other words, we must exclude that $\mathrm{Nm}(y_F) = 1$, or equivalently, that $y \in \mathcal{O}_F^{\times,+}$. However, this is immediate from the proof of Lemma 4.2.2, which shows that the generator ϵ_F of $\mathcal{O}_F^{\times,+}$ cannot be of the form $y_F/\sigma(y_F)$ if y_F itself is taken from $\mathcal{O}_F^{\times,+}$. □

4.3 The key exact sequence

We can now describe the map

$$\varphi : \mathcal{O}_F^{\times,+} \to \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$$

whose existence was claimed before.

- If the map $\mathrm{Nm}_F^L : \mathcal{O}_L^\times \to \mathcal{O}_F^{\times,+}$ is surjective, then $\varphi := 0$.
- Otherwise, we let $\varphi(\epsilon_F)$ be the pair $([I_1],[I_2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ where I_1 and I_2 are such that $\mathrm{Nm}(I_1) \cdot \mathrm{Nm}(I_2) = \mathrm{Nm}(y_F) \mid D$, where y_F is as in the second part of Theorem 4.2.6.

Note that the I_i for $i \in \{1,2\}$ are uniquely determined as the product over all primes in $\mathcal{O}_i$ above the primes dividing $\gcd(D_i, \mathrm{Nm}(y_F))$. We now verify that these choices correctly combine the exact sequences from Propositions 4.1.2 and 4.1.5. This connection requires a relation between the sizes of the class groups involved in terms of the fundamental units of the fields F and L. This relation is given by the analytic class number formula. Recall that the Dedekind zeta-function associated with a number field M is defined by

$$\zeta_M(s) = \prod_{\mathfrak{r} \subset \mathcal{O}_M} \left(1 - \mathrm{Nm}_{M/\mathbb{Q}}(\mathfrak{r})^{-s}\right)^{-1}.$$

One conventionally writes $\zeta_{\mathbb{Q}} = \zeta$, the Riemann-zeta function.

Proposition 4.3.1. *The following equality holds true:*

$$\zeta_L(s) \cdot \zeta(s)^2 = \zeta_{K_1}(s) \cdot \zeta_{K_2}(s) \cdot \zeta_F(s).$$

Proof. We use the Euler product expansion to reduce to showing an equality between the factors contributed by a single rational prime r. There are three cases: either r splits completely in L, or it is inert in precisely two of the fields K_1, K_2 and F and split in the third, or it is ramified in precisely two subfields. For primes of the first kind, we must verify that

$$\left(1 - r^{-s}\right)^4 \cdot \left(1 - r^{-s}\right)^2 = \left(1 - r^{-s}\right)^2 \cdot \left(1 - r^{-s}\right)^2 \cdot \left(1 - r^{-s}\right)^2,$$

which is obviously true. For primes of the second kind, we check that

$$\left(1 - r^{-2s}\right)^2 \cdot \left(1 - r^{-s}\right)^2 = \left(1 - r^{-2s}\right) \cdot \left(1 - r^{-2s}\right) \cdot \left(1 - r^{-s}\right)^2,$$

which is again clearly true. In the final case, depending on the splitting of the prime in the unramified field extension, we must check that

$$\left(1-r^{-s}\right)^2\cdot\left(1-r^{-s}\right)^2=\left(1-r^{-s}\right)\cdot\left(1-r^{-s}\right)\cdot\left(1-r^{-s}\right)^2,$$

and that

$$\left(1-r^{-2s}\right)\cdot\left(1-r^{-s}\right)^2=\left(1-r^{-s}\right)\cdot\left(1-r^{-s}\right)\cdot\left(1-r^{-2s}\right).$$

This completes the proof. □

Recall the *analytic class number formula* for any number field M,

$$\lim_{s\to 1}(s-1)\zeta_M(s)=\frac{2^r(2\pi)^s\mathrm{Reg}_M h_M}{w_M\sqrt{D_M}},$$

where r denotes the number of real embeddings of M and s the number of pairs of complex embeddings; Reg_M denotes the regulator, h_M the class number, w_M the number of roots of unity and D_M the discriminant. In combination with Proposition 4.3.1, this yields the following.

Proposition 4.3.2. *The following equality holds true;*

$$2|\log|\epsilon_L||h_L=|\log|\epsilon_F||h_1h_2h_F.$$

Proof. We obtain the following residues from the class number formula, using Lemma 4.1.1 to write $w_L=w_1w_2$,

$$\begin{aligned}
\lim_{s\to 1}(s-1)\zeta(s)&=1;\\
\lim_{s\to 1}(s-1)\zeta_{K_1}(s)&=\frac{2\pi h_1}{w_1\sqrt{D_1}};\\
\lim_{s\to 1}(s-1)\zeta_{K_2}(s)&=\frac{2\pi h_2}{w_2\sqrt{D_2}};\\
\lim_{s\to 1}(s-1)\zeta_F(s)&=\frac{|\log|\epsilon_F||h_F}{\sqrt{D_1D_2}};\\
\lim_{s\to 1}(s-1)\zeta_L(s)&=\frac{(2\pi)^2|\log|\epsilon_L||h_L}{w_1w_2\sqrt{D_L}/2}.
\end{aligned}$$

Hence Proposition 4.3.1 gives us that

$$\frac{(2\pi)^2|\log|\epsilon_L||h_L}{w_1w_2\sqrt{D_L}/2}=\frac{2\pi h_1}{w_1\sqrt{D_1}}\cdot\frac{2\pi h_2}{w_2\sqrt{D_2}}\cdot\frac{|\log|\epsilon_F||h_F}{\sqrt{D_1D_2}}.$$

Cancelling some terms on both sides, we obtain

$$\frac{2|\log|\epsilon_L||h_L}{\sqrt{D_L}} = \frac{|\log|\epsilon_F||h_1h_2h_F}{D_1D_2}.$$

According to Theorem 3 in [Wil70], we have $D_L = D_1^2D_2^2$ because we assumed D_1 and D_2 to be coprime, and as such, the equality reduces to the one from the proposition. □

Theorem 4.3.3. *With $\varphi : \mathcal{O}_F^{\times,+} \to \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ as defined at the start of this section, the following sequence is exact:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \mathcal{O}_1^\times \times \mathcal{O}_2^\times & \longrightarrow & \mathcal{O}_L^\times & \longrightarrow & \mathcal{O}_F^{\times,+} \\ \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) & \longrightarrow & \mathrm{Pic}(L) & \longrightarrow & \mathrm{Pic}(F)^+ & \longrightarrow & \{\pm 1\} & \longrightarrow & 1. \end{array}$$

Proof. By Proposition 4.1.2 and 4.1.5, it suffices to show exactness at $\mathcal{O}_F^{\times,+}$ and $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$. Recall from Lemma 4.0.3, we know that $\epsilon_F \gg 0$ and $2h_F = h_F^+$. We must distinguish two cases.

First suppose that the map $\mathcal{O}_L^\times \to \mathcal{O}_F^{\times,+} = \langle \epsilon_F \rangle$ is surjective, so that $\varphi = 0$ by definition. The sequence is then trivially a complex, so we reduce to showing that the map $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \to \mathrm{Pic}(L)$ is injective. To this end, we note that $\mathrm{Nm}_F^L(\epsilon_L) = \epsilon_F$ and from Remark 4.1.3 we conclude that $\epsilon_L^2 \in \mathcal{O}_1^\times \mathcal{O}_2^\times \langle \epsilon_F \rangle$. As such, $\epsilon_L^2 = \zeta \epsilon_F^k$ for some root of unity ζ, and by applying σ_F to this expression, also $\sigma_F(\epsilon_L)^2 = \zeta^{-1}\epsilon_F^k$. Multiplying these two expressions yields $\mathrm{Nm}_F^L(\epsilon_L)^2 = \epsilon_F^{2k}$ and so it follows that $k = 1$. Taking absolute values, we find that $|\epsilon_L|^2 = |\epsilon_F|$ and as such, $2\log|\epsilon_L| = \log|\epsilon_F|$. Appealing to Proposition 4.3.2, which now yields that $h_L = h_1h_2h_F$, we obtain that $2h_L = h_1h_2h_F^+$ and so Proposition 4.1.5 implies the desired injectivity.

It remains to examine the case in which $\epsilon_F \gg 0$ and the map $\mathcal{O}_L^\times \to \mathcal{O}_F^{\times,+} = \langle \epsilon_F \rangle$ is *not* surjective. We first show that our choice of φ makes the whole into a complex. Indeed, the composition

$$\mathcal{O}_L^\times \to \mathcal{O}_F^{\times,+} \xrightarrow{\varphi} \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$$

is trivial because $\mathrm{Nm}_F^L(\epsilon_L) = \epsilon_F^2$ maps to the pair $([I_1^2], [I_2^2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$; these classes are trivial because I_1 and I_2 are supported only at ramified primes, which are all 2-torsion. Next, we note that

$$\langle \epsilon_F \rangle = \mathcal{O}_F^{\times,+} \xrightarrow{\varphi} \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \to \mathrm{Pic}(L)$$

is always the zero map. Indeed, the ideal $I_1 I_2 \subset \mathcal{O}_L$ by construction contains the same primes as the ideal $y_F \mathcal{O}_L$, so they must be equal.

Exactness at $\mathcal{O}_F^{\times,+}$ is equivalent to the claim that $\varphi(\epsilon_F)$ is nontrivial. Suppose the contrary and write $I_1 = (y_1)$ and $I_2 = (y_2)$ for some $y_1 \in \mathcal{O}_1$ and $y_2 \in \mathcal{O}_2$. Now set $u = y_F/(y_1 y_2) \in L$. Then it is immediate that $\mathrm{Nm}(u) = 1$. We even claim that $u \in \mathcal{O}_L^\times$. Indeed, its possible non-zero valuations are supported on the ramified primes and by the norm equality, one will divide y_F if and only if it divides one of the y_i. The ramified primes in two quadratic subfields extend to the same primes in L, hence they will cancel out. We may now compute that

$$\mathrm{Nm}_F^L(u) = u\sigma_F(u) = \frac{y_F^2}{\mathrm{Nm}(y_1)\mathrm{Nm}(y_2)} = \frac{y_F^2}{\mathrm{Nm}(y_F)} = \frac{y_F^2}{y_F \sigma(y_F)} = \epsilon_F,$$

by construction of the element y_F. This contradicts the norm map $\mathcal{O}_L^\times \to \mathcal{O}_F^{\times,+} = \langle \epsilon_F \rangle$ not being surjective.

Finally, as $\mathrm{Nm}_F^L(\epsilon_L) = \epsilon_F^2$ now, using an argument analogous to the one used in the previous case, we deduce that $\log|\epsilon_L| = \log|\epsilon_F|$ in this case. One final application of Proposition 4.3.2, combined with $2h_F = h_F^+$, now yields that $4h_L = h_1 h_2 h_F^+$. Proposition 4.1.5 shows that the kernel of the map $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2) \to \mathrm{Pic}(L)$ contains exactly 1 non-trivial element. As the image $\varphi(\epsilon_F)$ hits such an element, it surjects onto the kernel and exactness of the whole sequence has been established. □

4.4 An F-quadratic form

We now pivot to a seemingly unrelated algebraic construction, which mimics the construction of the form $\deg_{\mathrm{CM}}$ in [HY12] and which will turn out to be intimately linked with the results proved hitherto. The setting for the remainder of this chapter will be as follows.

Recall that we fixed two embeddings $\alpha_i : K_i \to B_q$ for $i \in \{1, 2\}$. This turns B_q into a 1-dimensional L-vector space as follows. Let $x \in K_1$ and $y \in K_2$. Then the action of the element $xy \in L$ on some $\gamma \in B_q$ is defined by $(xy) * \gamma := \alpha_1(x)\gamma\alpha_2(y)$. We may extend this definition to the whole of L by $\mathbb{Q}$-linearity and the observation that $L = K_1 \otimes K_2$. Since $[L : \mathbb{Q}] = [B_q : \mathbb{Q}] = 4$, indeed B_q must be 1-dimensional over L.

For notational convenience, we define

$$A := \alpha_1(\sqrt{D_1}) \quad \text{and} \quad B := \alpha_2(\sqrt{D_2}).$$

Note that $A^2 = \alpha_1(\sqrt{D_1})^2 = \alpha_1(D_1) = D_1$ and similarly $B^2 = D_2$. Furthermore, as they are traceless, we have $\overline{A} = -A$ and $\overline{B} = -B$.

The goal of this section is to refine the usual $\mathbb{Q}$-quadratic norm form $\mathrm{Nm} : B_q \to \mathbb{Q}$ to an F-quadratic form $B_q \to F$ whose trace to $\mathbb{Q}$ coincides with the reduced norm pairing. To this end, let us commence with a brief intermezzo on linear algebra over various base fields. In the forthcoming, both K and M number fields such that M/K is a finite extension. Let V be a finite dimensional M-vector space.

Lemma 4.4.1. *Every K-linear map $f : V \to K$ is uniquely of the form $\mathrm{tr}_{M/K} \circ g$ for some M-linear map $g : V \to M$.*

Proof. Let $d = \dim_M(V)$ and $n = [M : K]$, so that $\dim_K(V) = nd$. It is then obvious that the set $\{f : V \to K \mid f \text{ is } K\text{-linear}\}$ is an nd-dimensional K-vector space. Similarly, the set $\{g : V \to M \mid g \text{ is } M\text{-linear}\}$ is a d dimensional M-vector space, and hence also an nd-dimensional K-vector space. Composing with the trace gives a K-linear map between these two vector spaces, so to establish the bijection it suffices to show injectivity. If $\mathrm{tr} \circ g = 0$, then restricted to any 1-dimensional M-subspace V' of V, the map $\mathrm{tr} \circ g|_{V'} : V' \cong M \to M$ is the zero map. Every M-linear map $M \to M$ is given by mutliplication by some element $a \in M$. However, since the trace form is non-degenerate, the trace of this map is only identically zero when $a = 0$. It follows that $g|'_V = 0$ for all 1-dimensional $V' \subset V$, and thus $g = 0$, proving the injectivity and hence the claim. □

Recall that a K-bilinear form $f : V \times V \to K$ is called *M-equivariant* if $f(v, \lambda w) = f(\lambda v, w)$ for all $v, w \in V$ and $\lambda \in M$.

Lemma 4.4.2. *Every M-equivariant K-bilinear form $f : V \times V \to K$ is the trace of a unique M-bilinear form $g : V \times V \to M$.*

Proof. Let $w \in V$ be arbitrary. Then the map $f(-, w) : V \to K$ is K-linear and thus by the above uniquely of the form $\mathrm{tr}(g_w(-))$ for some M-linear map $g_w : V \to M$. We claim that the formula $g(v, w) = g_w(v)$ constitutes the desired M-bilinear map. This is clearly M-linear in the first component. For the second, for $\lambda \in M$, note that since

$$\begin{aligned}\mathrm{tr}(g_{w_1+\lambda w_2}(v)) &= f(v, w_1 + \lambda w_2) = f(v, w_1) + f(v, \lambda w_2) \\ &= \mathrm{tr}(g_{w_1}(v)) + f(\lambda v, w_2) = \mathrm{tr}(g_{w_1}(v) + \lambda g_{w_2}(v)),\end{aligned}$$

the non-degeneracy of the trace allows us to conclude that $g_{w_1+\lambda w_2} = g_{w_1} + \lambda g_{w_2}$. This establishes M-linearity in the second argument. The uniqueness is clear from the construction. □

Proposition 4.4.3. *There exists a unique F-quadratic form $\det_F : B_q \to F$ with the property that $\mathrm{tr}_{F/\mathbb{Q}}(\det_F(\gamma)) = \mathrm{Nm}(\gamma)$ for all $\gamma \in B_q$. In addition, $\det_F(\gamma)$ is totally positive for any $\gamma \in B_q^\times$.*

Proof. Consider the $\mathbb{Q}$-bilinear form

$$f : B_q \times B_q \to \mathbb{Q} : (\gamma_1, \gamma_2) \mapsto \mathrm{tr}\left(\gamma_1 \overline{\gamma_2}\right)/2.$$

We claim that it is F-equivariant. Indeed, by $\mathbb{Q}$-linearity it suffices to compute, using cyclicity of the trace, that

$$f\left(\sqrt{D} * \gamma_1, \gamma_2\right) = \mathrm{tr}\left(A\gamma_1 B\overline{\gamma_2}\right)/2 = \mathrm{tr}\left(\gamma_1 \overline{A\gamma_2 B}\right)/2 = f\left(\gamma_1, \sqrt{D} * \gamma_2\right),$$

where we used the anticommutivity of conjugation. We may then apply Proposition 4.4.2 to the F-equivariant quadratic form $f(\gamma, \gamma) = \mathrm{Nm}(\gamma)$ to obtain a unique F-bilinear form $g : B_q \times B_q \to F$ whose trace equals f. It follows that $\det_F(x) = g(x, x)$ satisfies the required property.

It remains to verify that its values are totally positive. Let $\gamma \in B_q^\times$ be arbitrary and write $\det_F(\gamma) = a$ for convenience. Since $\det_F$ is F-quadratic, we have that $\det_F(x\gamma) = x^2 a$ for all $x \in F$. Since B_q is positive definite, it follows that $\mathrm{tr}(x^2 a) > 0$ for all $x \in F^\times$.

Identify a with its image under one of the real embeddings, so that $\sigma(a)$ is the image under the other. We see that $a + (\sigma(x)/x)^2 \sigma(a) > 0$ for all possible $x \in F^\times$. Choosing any $x \in F^\times$ with $|\sigma(x)| < |x|$ ensures that $\lim_{n\to\infty}(\sigma(x)/x)^n = 0$; whence $a > 0$ and similarly $\sigma(a) > 0$. □

Even though it is convenient to know that a form

$$\det_F : B_q \to F$$

satisfying the properties from Proposition 4.4.3 exists, it might also be desirable to be able to compute it. It is natural to start with identifying the F-bilinear form $g : B_q \times B_q \to F$ whose trace is supposed to equal the $\mathbb{Q}$-bilinear form $f : B_q \times B_q \to \mathbb{Q} : (\gamma_1, \gamma_2) \mapsto \mathrm{tr}\left(\gamma_1 \overline{\gamma_2}\right)/2$. This is established in the next lemma.

Lemma 4.4.4. *The form*

$$g : B_q \times B_q \to F : (\gamma_1, \gamma_2) \mapsto \frac{\mathrm{tr}(\gamma_1 \overline{\gamma_2})}{4} + \frac{\mathrm{tr}(A\gamma_1 B\overline{\gamma_2})}{4\sqrt{D}}$$

is F-bilinear and satisfies $\mathrm{tr} \circ g = f$.

Proof. The second property is clear, and so by $\mathbb{Q}$-linearity it suffices to show that

$$g(\sqrt{D} * \gamma_1, \gamma_2) = \sqrt{D} g(\gamma_1, \gamma_2) = g(\gamma_1, \sqrt{D} * \gamma_2)$$

for any $\gamma_1, \gamma_2 \in B_q$. To this end, we compute that

$$\begin{aligned} g(\sqrt{D} * \gamma_1, \gamma_2) &= \frac{\mathrm{tr}(A\gamma_1 B\overline{\gamma_2})}{4} + \frac{\mathrm{tr}(A^2\gamma_1 B^2\overline{\gamma_2})}{4\sqrt{D}} \\ &= \frac{\mathrm{tr}(A\gamma_1 B\overline{\gamma_2})}{4} + \sqrt{D}\frac{\mathrm{tr}(\gamma_1\overline{\gamma_2})}{4} \\ &= \sqrt{D} g(\gamma_1, \gamma_2). \end{aligned}$$

Similarly, we may use cyclicity of the trace to compute that

$$\begin{aligned} g(\gamma_1, \sqrt{D} * \gamma_2) &= \frac{\mathrm{tr}(\gamma_1\overline{A\gamma_2 B})}{4} + \frac{\mathrm{tr}(A\gamma_1 B\overline{A\gamma_2 B})}{4\sqrt{D}} \\ &= \frac{\mathrm{tr}(\gamma_1 B\overline{\gamma_2} A)}{4} + \frac{\mathrm{tr}(A\gamma_1 B^2\overline{\gamma_2} A)}{4\sqrt{D}} \\ &= \frac{\mathrm{tr}(A\gamma_1 B\overline{\gamma_2})}{4} + D_2\frac{\mathrm{tr}(A^2\gamma_1\overline{\gamma_2})}{4\sqrt{D}} \\ &= \sqrt{D} g(\gamma_1, \gamma_2); \end{aligned}$$

this proves the lemma. □

Corollary 4.4.5. *It holds that*

$$\det_F : B_q \to F : \gamma \mapsto \frac{\mathrm{Nm}(\gamma)}{2} + \frac{\mathrm{tr}(A\gamma B\overline{\gamma})}{4\sqrt{D}}.$$

Proof. This is immediate from the above by restricting to the diagonal where $\gamma_1 = \gamma_2$, as this is how $\det_F$ is constructed. □

We next want to relate this expression to the fixed points τ_i, τ_i' for the actions of K_i for $\mathbb{C}_p$ for $i \in \{1, 2\}$. The following lemma connects the trace above to these fixed points.

Lemma 4.4.6. *Let $a, b, c \in \mathbb{C}_p$ be such that τ_1 is a root of the polynomial $aT^2 + bT + c$, normalised such that a equals the bottom left entry of A. Let $\gamma \in B_q$ be arbitrary and let $x, y, z \in \mathbb{C}_p$ be such that $\gamma\tau_2$ is a root of the polynomial $xT^2 + yT + z$, normalised such that x equals the bottom left entry of $\gamma B\gamma^{-1}$. Then*

$$-2\mathrm{tr}(A\gamma B\overline{\gamma}) = (2cx + 2az - by)\mathrm{Nm}(\gamma).$$

Proof. We prove this first for $\gamma = 1$, and we write

$$A = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}.$$

Then

$$\mathrm{tr}(AB) = \mathrm{tr}\begin{pmatrix} s_1t_1 + s_2t_3 & s_1t_2 - s_2t_1 \\ s_3t_1 - s_1t_3 & s_3t_2 + s_1t_1 \end{pmatrix} = 2s_1t_1 + s_2t_3 + s_3t_2.$$

Since the matrices A and B fix τ_1 and τ_2 respectively, these numbers must satisfy the equations

$$s_3\tau_1^2 - 2s_1\tau_1 - s_2 = 0 \quad \text{and} \quad t_3\tau_2^2 - 2t_1\tau_2 - t_2 = 0.$$

Now note that the discriminants of these equations are given by

$$4(s_1^2 + s_2s_3) = 4D_1 \quad \text{and} \quad 4(t_1^2 + t_2t_3) = 4D_2$$

respectively, where these equalities are a result of the equations $A^2 = D_1$ and $B^2 = D_2$ respectively. It follows that

$$(a, b, c) = (s_3, -2s_1, -s_2) \quad \text{and} \quad (x, y, z) = (t_3, -2t_1, -t_2).$$

We may then finally compute that

$$2cx + 2az - by = -2s_2t_3 - 2s_3t_2 - 4s_1t_2 = 2\,\mathrm{tr}(AB);$$

this proves the claim for $\gamma = 1$. Now for arbitrary $\gamma \in B_q$, consider the embedding $\alpha_2' : K_2 \to B_q$ defined as $\gamma\alpha_2(-)\gamma^{-1}$. It is easy to see that now $\gamma\tau_2$ is a fixed point for the image of α_2'. For these two embeddings, the special case above implies that

$$-2\mathrm{tr}(A\gamma B\gamma^{-1}) = 2cx + 2az - by.$$

Multiplying both sides by $\mathrm{Nm}(\gamma)$ and using that $\gamma^{-1} = \overline{\gamma}/\mathrm{Nm}(\gamma)$ then yields the desired formula. □

Corollary 4.4.7. *Let $a, b, c, x, y, z \in \mathbb{C}_p$ be as in Lemma 4.4.6. Then*

$$\det_F : B_q \to F : \gamma \mapsto \mathrm{Nm}(\gamma)\left(\frac{1}{2} - \frac{2cx + 2az - by}{8\sqrt{D}}\right).$$

Proof. This is a direct consequence of combining Corollary 4.4.5 and Lemma 4.4.6 above. □

The following is crucial, though it will require a slightly laborious computation to verify. However, it will allow us to deduce the expression for $\det_F$ that will be most useful for our purposes. We invite the reader to compare these expressions to Equation 2.2.

Proposition 4.4.8. *Let $a, b, c, x, y, z \in \mathbb{C}_p$ be as in Lemma 4.4.6. Then*

$$\frac{(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')}{(\tau_1 - \tau_1')(\gamma\tau_2 - \gamma\tau_2')} = \frac{1}{2} \pm \frac{2cx + 2az - by}{8\sqrt{D}};$$

the change of sign being caused by exchanging τ_i, τ_i' for some $i \in \{1, 2\}$.

Proof. We may label the two roots τ_1 and τ_1' of $aT^2 + bT + c$ in such way that $\tau_1 - \tau_1' = 2\sqrt{D_1}/a$, which follows from its equation and discriminant. Similarly, we choose τ_2 and τ_2' in such a way that $\gamma\tau_2 - \gamma\tau_2' = 2\sqrt{D_2}/x$. Then one computes that

$$\frac{(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')}{(\tau_1 - \tau_1')(\gamma\tau_2 - \gamma\tau_2')} = ax\frac{(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')}{4\sqrt{D}}.$$

One may now expand $(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')$ to find it equals

$$\begin{aligned}
&\left(\frac{-b + 2\sqrt{D_1}}{2a} - \frac{-y + 2\sqrt{D_2}}{2x}\right)\left(\frac{-b - 2\sqrt{D_1}}{2a} - \frac{-y - 2\sqrt{D_2}}{2x}\right) \\
&= \frac{(-bx + 2x\sqrt{D_1} + ay - 2a\sqrt{D_2})(-bx - 2x\sqrt{D_1} + ay + 2a\sqrt{D_2})}{(2ax)^2} \\
&= \frac{(b^2 - 4D_1)x^2 + a^2(y^2 - 4D_2) - 2axby + 8ax\sqrt{D_1 D_2}}{(2ax)^2} \\
&= \frac{4acx^2 + 4a^2xz - 2axby + 8ax\sqrt{D}}{(2ax)^2} \\
&= \frac{2cx + 2az - by + 4\sqrt{D}}{2ax}.
\end{aligned}$$

Combining this with the above proves the proposition. □

Theorem 4.4.9. *The form $\det_F : B_q \to F$ is given by*

$$\det_F(\gamma) = \mathrm{Nm}(\gamma)\frac{(\tau_1 - \gamma\tau_2)(\tau_1' - \gamma\tau_2')}{(\tau_1 - \tau_1')(\gamma\tau_2 - \gamma\tau_2')},$$

for all $\gamma \in B_q$ and where τ_i and τ_i' for $i \in \{1, 2\}$ are the fixed points for the action of the image of $\alpha_i : \mathcal{O}_i \to B_q \to M_2(\mathbb{Q}_p)$ on $\mathbb{C}_p$.

Proof. This follows from combining the results of Corollary 4.4.7 and Proposition 4.4.8 above. □

4.5 From quaternions to ideals

The goal of this section is to prove Theorem 4.0.1 from [HY12] using an explicit, global bijection. Recall that the embeddings α_1 and α_2 turn B_q into a 1-dimensional L-vector space, and as such, we may choose some isomorphism

$$\iota : B_q \xrightarrow{\sim} L$$

of L-vector spaces. We use this to define for any $b \in B_q$ the ideal

$$I_b := \iota(b)/\iota(R_q) \subset L.$$

Lemma 4.5.1. *The set $\iota(R_q)$ defines a fractional ideal in L and for any $b \in R_q$, the ideal I_b is both integral and independent of the choice of isomorphism $\iota : B_q \xrightarrow{\sim} L$ of L-vector spaces.*

Proof. Recall that a fractional ideal in L is a finitely generated sub-$\mathcal{O}_L$-module of L, so since it is clearly finitely generated, for the first claim it suffices to verify that $\iota(R_q)$ is an $\mathcal{O}_L$-module. To this end, we observe that if $x \in \mathcal{O}_1$ and $y \in \mathcal{O}_2$, it follows that for any $b \in R_q$,

$$(xy)\iota(b) = \iota((xy) * b) = \iota(\alpha_1(x)b\alpha_2(y)) \in \iota(R_q),$$

because for $i \in \{1, 2\}$, the embeddings α_i map $\mathcal{O}_i$ into R_q, so that indeed $\alpha_1(x)b\alpha_2(y) \in R_q$. Now to complete the proof of the first claim we need merely observe that, by the coprimality of D_1 and D_2, we have

$$\mathcal{O}_L = \mathcal{O}_1 \otimes_{\mathbb{Z}} \mathcal{O}_2.$$

To see that I_b is an integral ideal for any $b \in R_q$, by definition

$$\iota(R)^{-1} = \{z \in L \mid z\iota(R_q) \subset \mathcal{O}_L\},$$

so that indeed for any $z \in \iota(R_q)^{-1}$, it holds that in $z\iota(b) \in \mathcal{O}_L$, whence $I_b \subset \mathcal{O}_L$. Finally, to see the independence of I_b from ι, we note that any two isomorphisms of 1-dimensional L-vector spaces agree up to a scalar, so any other ι' can be written as $\lambda\iota$ for some $\lambda \in L^\times$. Then indeed

$$\begin{aligned}
\iota'(b)\iota'(R_q)^{-1} &= \lambda\iota(b) \cdot \{z \in L \mid z\iota'(R_q) \subset \mathcal{O}_L\} \\
&= \{\lambda\iota(b)z \in L \mid \lambda z\iota(R_q) \subset \mathcal{O}_L\} \\
&= \{\iota(b)z' \in L \mid z'\iota(R_q) \subset \mathcal{O}_L\} \\
&= \iota(b)\iota(R_q)^{-1},
\end{aligned}$$

using the bijective substitution $z' = \lambda z$. □

It is through the norm of the ideal I_b from L down to F that the importance of the form $\det_F : B_q \to F$ from the previous section becomes apparent. We will use some of the results proved in [HY12]. Their strategy to compute this norm is to do this locally at every prime. There are two cases to consider: those primes above q, and all the others. This gives rise to the following two results from [HY12], the proofs of which we do not include here for to avoid needless repetition.

Proposition 4.5.2. *Let $\ell \neq q$ be any prime number. Then there is some $\delta_\ell \in F_\ell^\times$ that is a generator of the $\mathcal{O}_{F,\ell}$-ideal $\mathcal{D}_{F,\ell}$ such that we may choose the isomorphism $\iota : B_q \to L$ in such a way that*

$$\det_F(-) = \delta_\ell^{-1}\mathrm{Nm}_{L_\ell/F_\ell}(\iota(-))$$

and such that ι takes $R_q \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ to $\mathcal{O}_{L,\ell}$.

Proof. This is Lemma 2.16 in [HY12]. □

To state the second result, we must define the *reflex ideal* of $\mathcal{O}_F$ above the rational prime q associated with the pair of embeddings α_1, α_2. Let $\Pi \in R_q$ be an element of norm q. Then the *reflex ideal* is defined as

$$F \cap \ker\left(\mathcal{O}_L \to R_q \to R_q/\Pi \cong \mathbb{F}_{q^2}\right),$$

where the first map, given by $z \mapsto z * 1$, is not a ring morphism, but by the commutativity of the rightmost ring, it is not difficult to see that this composite is actually a ring morphism and as such, defines an ideal in $\mathcal{O}_F$. We make our choice of $\mathfrak{q}_1, \mathfrak{q}_2 \subset \mathcal{O}_F$ in such a way that $\mathfrak{q}_1$ is the relevant reflex ideal for the fixed pair of embeddings α_1, α_2.

Proposition 4.5.3. *For some $\beta \in F_q^\times = F_{\mathfrak{q}_1}^\times \times F_{\mathfrak{q}_2}^\times$ such that $v_{\mathfrak{q}_1}(\beta) = 1$ and $v_{\mathfrak{q}_2}(\beta) = 0$ we can choose ι in such a way that*

$$\det_F(-) = \beta\ \mathrm{Nm}_{L_q/F_q}(\iota(-))$$

and such that ι takes $R_q \otimes_{\mathbb{Z}} \mathbb{Z}_q$ to $\mathcal{O}_{L,q}$.

Proof. This is Proposition 2.22 in [HY12]. □

These two results combine to prove the following key result.

Proposition 4.5.4. *For any $b \in B_q$, the ideal I_b satisfies*

$$\mathrm{Nm}_{L/F}(I_b) = \det_F(b)\mathfrak{q}_1^{-1}\mathcal{D}_F.$$

Proof. By unique ideal factorisation into primes, it suffices to check the claimed equality everywhere locally. First consider any prime $\ell \neq q$. Then on the right hand side, we have the ideal $\det_F(b)\mathcal{D}_{F,\ell}$. On the left hand side, we use the independence of I_b from our choice of ι to make the choice from Proposition 4.5.2. This maps $\iota(R)^{-1}$ simply to the unit ideal, whereas from $\det_F(b) = \delta_\ell^{-1}\mathrm{Nm}_{L_\ell/F_\ell}(\iota(b))$ it follows that the ideal generated by the norm of $\iota(b)$ agrees with $\delta_\ell \det_F(b)$. By definition of δ_ℓ, these two ideals agree. For the primes above q, the argument is similar, now noting that the right hand side of the theorem localises to $\det_F(b)\mathfrak{q}_1^{-1}$ because we assumed q to be coprime to D_1 and D_2. As β from Proposition 4.5.3 generates the ideal $\mathfrak{q}_1$, the claim follows. □

Lemma 4.5.5. *Let $u_i \in \mathcal{O}_i^\times$ for $i \in \{1,2\}$. Then for any $b \in B_q$,*

$$\det_F(u_1u_2 * b) = \det_F(b).$$

Proof. We use Corollary 4.4.5 to reduce the lemma to observing that $\mathrm{Nm}(u_1u_2 * b) = \mathrm{Nm}(u_1bu_2) = \mathrm{Nm}(b)$ by multiplicativity, and

$$\begin{aligned}\mathrm{tr}(A(u_1u_2 * b)B(\overline{u_1u_2 * b})) &= \mathrm{tr}(Au_1bu_2B\overline{u_2}\overline{b}\overline{u_1}) \\ &= \mathrm{tr}(\overline{u_1}u_1AbBu_2\overline{u_2}\overline{b}) = \mathrm{tr}(AbB\overline{b}),\end{aligned}$$

using both cyclicity of the trace and the fact that $u_1 \in K_1$ and $u_2 \in K_2$ commute with A and B respectively. □

Any attempt at constructing a bijection between quaternions and ideals using only one choice of embeddings is doomed to fail for the simple fact that $\iota(R_q)$, and as such I_b, will always be in the same ideal class. We must take into account the action of the Picard groups on the embeddings, the definition of which we shall now recall. Recall that we assume that B_q has class number 1. Under this assumption, Corollary 30.4.23 in [Voi21] gives us group actions of $\mathrm{Pic}(K_i)$ for $i \in \{1,2\}$ on the set of $R_q^\times$-conjugacy classes of embeddings $\mathcal{O}_i \to R_q$. For $[J] \in \mathrm{Pic}(K_1)$, this action is given by

$$[J] \cdot \alpha_1(-) = \xi^{-1}\alpha_1(-)\xi \quad \text{where} \quad \alpha_1(J)R_q = \xi R_q.$$

The action of $\mathrm{Pic}(K_2)$ is similar, but now $\alpha_2(J)$ acts from the right. From now on, we will write $\iota[c_1, c_2]$ for an isomorphism of 1-dimensional L-vector spaces $B \to L$ where B is equipped with the L-vector space structure induced by the embeddings $[c_1] \cdot \alpha_1$ and $[c_2] \cdot \alpha_2$, where $[c_1] \in \mathrm{Pic}(K_1)$ and $[c_2] \in \mathrm{Pic}(K_2)$ are any representatives. This leaves some ambiguity coming from conjugation by $R_q^\times$, but this does not affect the

counting problem we aim to solve, so we may ignore it. Further, let $I[c_1, c_2]_b$ denote the ideal associated with b using the embedding $\iota[c_1, c_2]$ and let $\det_F[c_1, c_2]$ be the resulting F-bilinear quadratic form.

Proposition 4.5.6. *Let* $[c_1] \in \mathrm{Pic}(K_1)$ *and* $[c_2] \in \mathrm{Pic}(K_2)$ *be given. Then the class of* $I[c_1, c_2]_b$ *inside of* $\mathrm{Pic}(L)$ *is given by* $[c_1] + [c_2] + [I_b]$.

Proof. It suffices to show this for $[c_2] = 0 \in \mathrm{Pic}(K_2)$, for two applications of this special case are enough to deduce the general case. Let now $J \subset \mathcal{O}_1$ be any ideal and let ι' be any L-vector space isomorphism $\iota' : B \to L$ using the modified action $(xy) \star b = ([J] \cdot \alpha_1)(x) b \alpha_2(y)$. We must show that

$$[\iota'(R_q)] = [\iota(R_q)] + [J] \in \mathrm{Pic}(L).$$

Without loss of generality we set $\iota(1) = \iota'(1) = 1$, so that $\iota(x * 1) = x\iota(1) = x$ for all $x \in L$ and similarly for $\star$. If $x = yz$ for $y \in K_1$ and $z \in K_2$, we may then write that

$$\begin{aligned}
x \in \iota'(R_q) &\iff x \star 1 \in R_q \iff (yz) \star 1 \in R_q \\
&\iff (J \cdot \alpha_1)(y)\alpha_2(z) \in R_q \iff \xi^{-1}\alpha_1(y)\xi\alpha_2(z) \in R_q \\
&\iff \alpha_1(y)\xi\alpha_2(z) \in \xi R_q = \alpha_1(J)R_q \\
&\iff (yz) * \xi \in \alpha_1(J)R_q \iff x * \xi \in \alpha_1(J)R_q \\
&\iff x\iota(\xi) \in \iota(J)\iota(R_q) = J\iota(R_q).
\end{aligned}$$

This holds for all $x \in L$ by linearity. Since $\iota(\xi)$ is a fixed scalar, it follows that $[\iota'(R_q)] = [\iota(R_q)] + [J]$, as desired. □

The following result connects this construction with the most subtle part of the exact sequence from Theorem 2.3.3. Indeed, now the explicit map $\varphi : \mathcal{O}_F^{\times,+} \to \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ comes into the picture. The following proposition relates the values of the $\det_F$-function for two pairs of ideals in $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ whose image in $\mathrm{Pic}(L)$ are the same.

Proposition 4.5.7. *Let* $([c_1], [c_2]), ([d_1], [d_2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ *be two* distinct pairs *satisfying that* $[c_1] + [c_2] = [d_1] + [d_2] \in \mathrm{Pic}(L)$. *Then*

$$\det_F[c_1, c_2](R_q) \cap \epsilon_F \cdot \det_F[d_1, d_2](R_q) \neq \varnothing,$$

where $\det_F[-,-](R_q)$ *denotes the set of values of* $\det_F[-,-]$ *on the elements of* R_q.

Proof. The existence of such distinct pairs is by Theorem 4.3.3 ensured when $\mathrm{Nm}_F^L(\mathcal{O}_L^\times)$ does not surject onto $\mathcal{O}_F^{\times,+}$, so we find ourselves in this case. For notational convenience, we will also assume that $([d_1],[d_2]) = ([0],[0])$, so that $([c_1],[c_2]) = \varphi(\epsilon_F)$. The reader will find it easy to deduce the general case from this special one.

Denote the form induced by $([c_1],[c_2])$ by $\det'_F$. We observe that it suffices to establish an element $b \in R_q$ such that $\det'_F(1) = \epsilon_F \det_F(b)$. Still under the simplifying assumption that R_q has class number 1, we may choose $\xi_1, \xi_2 \in R_q$ such that $\alpha_1(c_1)R_q = \xi_1 R_q$ and $R_q\alpha_2(c_2) = R_q\xi_2$. We then claim that

$$f : B_q \to F : b \mapsto \frac{\mathrm{Nm}(\xi_1)}{\mathrm{Nm}(\xi_2)}\det_F(\xi_1^{-1}b\xi_2).$$

satisfies the defining property for $\det'_F(b)$. Indeed,

$$\mathrm{Tr}(f(b)) = \frac{\mathrm{Nm}(\xi_1)}{\mathrm{Nm}(\xi_2)}\mathrm{Tr}(\det_F(\xi_1^{-1}b\xi_2)) = \frac{\mathrm{Nm}(\xi_1)}{\mathrm{Nm}(\xi_2)}\mathrm{Nm}(\xi_1^{-1}b\xi_2) = \mathrm{Nm}(b).$$

Also, it is F-quadratic for the action $\star$ induced by the embeddings $\alpha'_1 = \xi_1\alpha_1\xi_1^{-1}$ and $\alpha'_2 = \xi_2\alpha_2\xi_2^{-1}$, because

$$\begin{aligned} f(\sqrt{D}\star b) &= \frac{\mathrm{Nm}(\xi_1)}{\mathrm{Nm}(\xi_2)}\det_F\big(\xi_1^{-1}\xi_1\alpha_1(\sqrt{D_1})\xi_1^{-1}b\xi_2\alpha_2(\sqrt{D_2})\xi_2^{-1}\xi_2\big) \\ &= \frac{\mathrm{Nm}(\xi_1)}{\mathrm{Nm}(\xi_2)}\det_F(\sqrt{D} * \xi_1^{-1}b\xi_2) = D\cdot f(b); \end{aligned}$$

proving our claim. By considering the index of both ideals, it must follow that $\mathrm{Nm}(\xi_i) = \mathrm{Nm}(c_i)$ for $i \in \{1,2\}$. By our definition of the connecting map φ in Theorem 4.3.3, we thus have $\mathrm{Nm}(\xi_1\xi_2) = \mathrm{Nm}(y_F)$ where $y_F/\sigma(y_F) = \epsilon_F$. We now set

$$b = \frac{\sigma(y_F)}{\mathrm{Nm}(\xi_2)} * (\xi_1^{-1}\xi_2) \in R_q.$$

Indeed, using the F-linearity of $\det_F$, we compute that

$$\begin{aligned} \epsilon_F\det_F(b) &= \frac{y_F}{\sigma(y_F)}\det_F\left(\frac{\sigma(y_F)}{\mathrm{Nm}(\xi_2)} * (\xi_1^{-1}\xi_2)\right) = \frac{y_F\sigma(y_F)}{\mathrm{Nm}(\xi_2)^2}\det_F(\xi_1^{-1}\xi_2) \\ &= \frac{\mathrm{Nm}(y_F)}{\mathrm{Nm}(\xi_2)^2}\frac{\mathrm{Nm}(\xi_2)}{\mathrm{Nm}(\xi_1)}\det'_F(1) = \det'_F(1), \end{aligned}$$

as claimed. This completes the proof. □

We are now ready to prove the main result of this chapter.

Theorem 4.0.2. *For any $\nu \in F^+$, the association $(b, [c_1], [c_2]) \mapsto I[c_1, c_2]_b$ establishes a bijection between the set of*

$$(b, [c_1], [c_2]) \in (\mathcal{O}_1^\times \setminus R_q \,/\, \mathcal{O}_2^\times) \times \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$$

with the property that $\det_F[c_1, c_2](b) = \nu$ and the set of integral ideals $I \subset \mathcal{O}_L$ such that $\mathrm{Nm}_{L/F}(I) = \nu \mathfrak{q}_1^{-1} \mathcal{D}_F$.

Proof. Well-definedness of the association has already been established. Our strategy is to take some ideal $I \subset \mathcal{O}_L$ with norm as described and to reason that there is a unique triple $(b, [c_1], [c_2])$ mapping to it.

We start by observing that I maps under the norm map to the ideal class of $[\mathfrak{q}^{-1}\mathcal{D}_F]$ inside $\mathrm{Pic}(F)^+$. Similarly, for any given $(b, [c_1], [c_2])$, we have by Proposition 4.5.4 that the ideal class of $\mathrm{Nm}_F^L(I[c_1, c_2]_b)$ equals the class of $[\mathfrak{q}^{-1}\mathcal{D}_F]$ as well. By Theorem 4.3.3, these two ideal classes in $\mathrm{Pic}(L)$ must therefore differ up to an element from $\mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$. Using Proposition 4.5.6, this means that there exist $[c_1] \in \mathrm{Pic}(K_1)$ and $[c_2] \in \mathrm{Pic}(K_2)$ such that the class $[I]$ agrees with the class $[I[c_1, c_2]_b]$ for any choice $b \in B_q$.

The ambiguity in the choice of $([c_1], [c_2]) \in \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$ here is, by Theorem 4.3.3, measured by $\mathcal{O}_F^{\times,+} / \mathrm{Nm}_{L/F}(\mathcal{O}_L^\times)$. On the other hand, for any such choice of $([c_1], [c_2])$, the ideal $I \cdot \iota[c_1, c_2](R_q)$ will be principal. Because $\iota[c_1, c_2]$ is bijective, we find some $b \in B_q$ with $I \cdot \iota[c_1, c_2](R_q) = (\iota[c_1, c_2](b))$; in other words, we obtain some $b \in B_q$ with $I = I[c_1, c_2]_b$. Using Proposition 4.5.4, comparing norms to F yields that $\det_F(b) \in F$ and $\nu \in F$ generate the same $\mathcal{O}_F$-ideal, and as such, they must agree up to a unit from $\mathcal{O}_F^{\times,+}$, where we used that $\det_F(b)$ and ν are both totally positive. We may only modify b by an element of $\mathcal{O}_L^\times$ without changing $I[c_1, c_2]_b$, which will modify $\det_F(b)$ by an element of $\mathrm{Nm}_{L/F}(\mathcal{O}_L^\times)$ by a computation similar to that in the proof of Lemma 4.5.5. The failure to equate $\det_F(b)$ and ν is thus again measured by $\mathcal{O}_F^{\times,+} / \mathrm{Nm}_{L/F}(\mathcal{O}_L^\times)$. By Proposition 4.5.7, there is a unique choice of $([c_1], [c_2])$ such that this obstruction can be lifted.

We make this choice and find some $b \in B_q$ such that $I = I[c_1, c_2]_b$ and $\det_F(b) = \nu$. Because the first condition determines b uniquely up to multiplication by an element $u \in \mathcal{O}_L^\times$ and $\mathrm{Nm}_F^L(u) = 1$ if and only if $u \in \mathcal{O}_1^\times \mathcal{O}_2^\times$, this shows that b is determined uniquely up to an element from $\mathcal{O}_1^\times \mathcal{O}_2^\times$. By Lemma 4.5.5, this ambiguity remains. To complete the proof, we must still show that $b \in R_q$. One can check this locally using Proposition 4.5.2 and Proposition 4.5.3; in this instance, we opt to leave the details to the reader. □

CHAPTER 5

Deformation theory

The aim of this chapter is to carry out **Step 2** of the proof of Theorem B as explained in Section 2.4. We remind the reader that our stategy is ultimately to perform certain operations on a cuspidal p-adic family of modular forms passing through the appropriate p-stabilisation $E_{1,\chi}^{(p)}$ of the Hilbert Eisenstein series $E_{1,\chi}$. However, there are no easy ways to obtain such a family. Our approach is therefore to obtain this by deforming the Galois representation $\rho = \mathbb{1} \oplus \chi$ associated with the Eisenstein series $E_{1,\chi}^{(p)}$ instead, and compute from this the associated family of modular forms that we need to carry out our proof.

However, this approach requires us to show that these deformations are in fact modular; that is, that these Galois representations actually come from modular forms. This is done by proving a so-called $R = T$ theorem, where R typically denotes a certain universal deformation ring, and T a certain Hecke algebra. Proving such a theorem is the main focus of this chapter.

Similar results have been obtained in Pozzi's thesis [Poz19] for the ground field $\mathbb{Q}$ and in the case that the prime p is *irregular*, as opposed to the *regular* case as we are in here, since $\chi(\mathfrak{p}_i) \neq 1$ for $i \in \{1, 2\}$. For other closely related works in these directions, see [BDP22, BD16, BDS20, BC06, DKV18]. With small adjustments, our $R = T$ theorem can also be deduced from the results of [Bet20], where very similar methods to the ones we will employ throughout this chapter were used.

We start by recalling some results from class field theory and use these to compute various Galois cohomology groups, that will play a key role throughout. For representability reasons that we will explain in Section 5.2, we should rigidify the decomposable representation $\rho = \mathbb{1} \oplus \chi$ before attempting to deform it. This rigidified representation is denoted ρ_η. We will consider a class of deformations that are called *nearly ordinary* and show that it admits a universal deformation ring $R_{\rho_\eta}^{\mathrm{no}}$. Next, we construct from a key result of Hida in [Hid89a] a Galois representation onto Hida's *nearly ordinary cuspidal Hecke algebra* $\mathbb{T}$ localised at the Eisenstein series $E_{1,\chi}^{(p)}$ from Appendix A.2. We show that it must be a lift of ρ_η, so that by universality, this will yield a map $\mathcal{T} : R_{\rho_\eta}^{\mathrm{no}} \to \mathbb{T}$, where $\mathbb{T}$ denotes the appropriate Hecke algebra. Using various results from commutative algebra, we can then show the following.

Theorem 5.0.1. *The map $\mathcal{T} : R_{\rho_\eta}^{\mathrm{no}} \to \mathbb{T}$ is an isomorphism.*

Throughout this chapter, we let $\mathbb{Q}_p := \mathbb{Q}_p(\mathbb{1})$ denote the Galois module with trivial G_F-action, whereas $\mathbb{Q}_p(\chi)$ denotes the same module but with the action of G_F through the character $\chi : G_F \to \{\pm 1\}$.

Furthermore, for any G_F-module A, we let $Z^1(G_F, A)$ denote the group of *continuous* 1-cocycles for G_F with values in A. All cohomology groups in this chapter will be derived from group cohomology and will as such be quotients of the groups $Z^1(G_F, A)$.

Finally, throughout this chapter, we will denote

$$G := \mathrm{Gal}(L/F) = \langle \sigma_F \rangle \cong \mathbb{Z}/2\mathbb{Z}$$

and to simplify notation, we write for $i \in \{1, 2\}$ the decomposition group

$$G_{\mathfrak{p}_i} := G_{F_{\mathfrak{p}_i}} \cong \mathrm{Gal}(\overline{F}_{\mathfrak{p}_i}/F_{\mathfrak{p}_i}) \quad \text{inside } G_F.$$

5.1 Some Galois cohomology

Our main tool to compute Galois cohomology groups comes from the following result, which relies on global class field theory. It can be found as Lemma 1.1.1 in [Poz19] or as Lemma 3.2 in [DPV23].

Proposition 5.1.1. *We have the following exact sequence:*

$$0 \to \mathrm{Hom}(G_L^{\mathrm{ab}}, \mathbb{Q}_p) \to \prod_{v|p} \mathrm{Hom}(L_v^\times, \mathbb{Q}_p) \to \mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p).$$

We opt to omit its proof, for it is standard, yet somewhat lengthy. However, we do stress that the proof of this result uses the fact that L is totally imaginary, allowing us to easily identify the connected component of the identity inside the idele class group. Therefore, we may not use this proposition with the field L replaced by either F or $\mathbb{Q}$. The next result aims to connect the cohomology groups for G_F to those for G_L.

Lemma 5.1.2. *Restriction to $G_L \subset G_F$ yields isomorphisms*

$$H^1(G_F, \mathbb{Q}_p) \cong \mathrm{Hom}(G_L, \mathbb{Q}_p)^G;$$
$$H^1(G_F, \mathbb{Q}_p(\chi)) \cong \mathrm{Hom}(G_L, \mathbb{Q}_p(\chi))^G.$$

Proof. Note that the action of G_L on $\mathbb{Q}_p(\chi)$ is trivial. We may then use the inflation-restriction sequence to obtain that

$$0 \to H^1(G, \mathbb{Q}_p) \to \mathrm{Hom}(G_F, \mathbb{Q}_p) \to \mathrm{Hom}(G_L, \mathbb{Q}_p)^G \to H^2(G, \mathbb{Q}_p)$$

is exact, and similarly that also

$$0 \to H^1(G, \mathbb{Q}_p(\chi)) \to H^1(G_F, \mathbb{Q}_p(\chi)) \to \mathrm{Hom}(G_L, \mathbb{Q}_p(\chi))^G \to H^2(G, \mathbb{Q}_p(\chi))$$

is exact. To prove the lemma, we thus reduce to showing that the groups $H^1(G,\mathbb{Q}_p)$, $H^2(G,\mathbb{Q}_p)$, $H^1(G,\mathbb{Q}_p(\chi))$ and $H^2(G,\mathbb{Q}_p(\chi))$ are all trivial. Using that G is cyclic, we identify these spaces with

$$H^1(G,-) = \frac{\ker(\mathcal{N})}{\mathrm{im}(\Delta)} \quad \text{and} \quad H^2(G,-) = \frac{\ker(\Delta)}{\mathrm{im}(\mathcal{N})},$$

where $\Delta = 1 - \sigma_F$ and $\mathcal{N} = 1 + \sigma_F$ in the group ring $\mathbb{Z}[G]$. In both cases, one of these maps is zero, whereas the other is multiplication by 2, which is a bijective map on $\mathbb{Q}_p$. All claims follow. □

We now identify the spaces on the right hand side of Lemma 5.1.2. Any finite dimensional G-representation V can be decomposed as a finite sum of copies of $\mathbb{1}$ and χ. Henceforth, for $\varphi \in \{1, \chi\}$, we will let V^φ denote the sum of all φ-eigenspaces inside V.

Lemma 5.1.3. *For $\varphi \in \{\mathbb{1}, \chi\}$, it holds that*

$$\mathrm{Hom}(G_L, \mathbb{Q}_p(\varphi))^G \cong \mathrm{Hom}(G_L, \mathbb{Q}_p)^\varphi.$$

Proof. Recall that the action of some $g \in G_F$ on some homomorphism $f \in \mathrm{Hom}(G_L, \mathbb{Q}_p(\varphi))$ is defined as $g \cdot f : x \mapsto \varphi(g) f(gxg^{-1})$. To be invariant under this action, we thus require that $\varphi(g) f(gxg^{-1}) = f(x)$ for all $x \in G_L$. On the other hand, the action of some $g \in G_F$ on some homomorphism $f \in \mathrm{Hom}(G_L, \mathbb{Q}_p)$ is defined as $g \cdot f : x \mapsto f(gxg^{-1})$. So, to be in the φ-eigenspace, we thus require that $\varphi(g) f(gxg^{-1}) = f(x)$ for all $x \in G_L$. These two conditions agree. □

Lemma 5.1.4. *It holds that*

$$\dim\left(\mathrm{Hom}(G_L, \mathbb{Q}_p)^{\mathbb{1}}\right) = 1 \quad \textit{and} \quad \dim\left(\mathrm{Hom}(G_L, \mathbb{Q}_p)^{\chi}\right) = 2.$$

Proof. For $i \in \{1, 2\}$, the space $\mathrm{Hom}(L_{\mathfrak{p}_i}^\times, \mathbb{Q}_p)$ is 3-dimensional and spanned by $\mathrm{ord}_{\mathfrak{p}_i}$, the p-adic logarithm $\log_p$ and its composition with the non-trivial element from $\mathrm{Gal}(L_{\mathfrak{p}_i}/\mathbb{Q}_p)$. Since the primes above p in F are inert in L, the action of G fixes the former, but interchanges the latter two basis elements. It follows that

$$\dim\left(\mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p)^{\mathbb{1}}\right) = 4 \quad \text{and} \quad \dim\left(\mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p)^{\chi}\right) = 2.$$

For the rightmost term, we observe that the image of the norm map

$$\mathcal{O}_L[1/p]^\times \to \mathcal{O}_F[1/p]^\times$$

has finite index. Indeed, we know that the map $\mathcal{O}_L^\times \to \mathcal{O}_F^\times$ has index at most 2, and since the primes above p in F are inert in L, the claim follows. After tensoring with $\mathbb{Q}_p$, these Galois modules are therefore isomorphic. Therefore, using Dirichlet's unit theorem, we find that

$$\dim\left(\mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p)^{\mathbb{1}}\right) = 3 \quad \text{and} \quad \mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p)^\chi = 0.$$

We now consider the short exact sequence from Proposition 5.1.1:

$$0 \to \mathrm{Hom}(G_L, \mathbb{Q}_p) \to \mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p) \to \mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p).$$

All of these spaces are finite dimensional G-representations. As such, they can be decomposed into a direct sum of $\mathbb{1}$ and χ-eigenspaces. First, we take $\mathbb{1}$-eigenspaces to find

$$0 \to \mathrm{Hom}(G_L, \mathbb{Q}_p)^{\mathbb{1}} \to \mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p)^{\mathbb{1}} \to \mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p)^{\mathbb{1}}.$$

Surjectivity on the right is equivalent with Leopoldt's conjecture for L. Since $L/\mathbb{Q}$ is abelian, and as such, this conjecture is known and the claim about the dimension now follows. Next, taking χ-eigenspaces, we obtain a sequence

$$0 \to \mathrm{Hom}(G_L, \mathbb{Q}_p)^\chi \to \mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p)^\chi \to \mathrm{Hom}(\mathcal{O}_L[1/p]^\times, \mathbb{Q}_p)^\chi = 0,$$

and the proof is complete by our dimension computations above. □

Combining all the above, we obtain the following two core results.

Corollary 5.1.5. *The group* $\mathrm{Hom}(G_F, \mathbb{Q}_p)$ *is 1-dimensional and spanned by the p-adic cyclotomic character:*

$$\phi_p : G_F \to \mathrm{Gal}(F(\zeta_p^\infty)/F) \cong \mathbb{Z}_p^\times \xrightarrow{\log_p} \mathbb{Q}_p.$$

Proof. Combining Lemma 5.1.2 with Lemma 5.1.3, we obtain an isomorphism $\mathrm{Hom}(G_F, \mathbb{Q}_p) \cong \mathrm{Hom}(G_L, \mathbb{Q}_p)^{\mathbb{1}}$ and by Lemma 5.1.4, this space is 1-dimensional, as claimed. As it contains the p-adic cyclotomic character as defined above, which is clearly non-zero, this character must span the space, completing the proof. □

Corollary 5.1.6. *For* $i \in \{1, 2\}$*, the groups* $H^1(G_{\mathfrak{p}_i}, \mathbb{Q}_p(\chi))$ *are both 1-dimensional, and restriction gives an isomorphism*

$$H^1(G_F, \mathbb{Q}_p(\chi)) \cong H^1(G_{\mathfrak{p}_1}, \mathbb{Q}_p(\chi)) \oplus H^1(G_{\mathfrak{p}_2}, \mathbb{Q}_p(\chi)).$$

Proof. Using analogous arguments to those in the proofs of Lemma 5.1.2 and Lemma 5.1.3, one can show that

$$H^1(G_{\mathfrak{p}_i}, \mathbb{Q}_p(\chi)) \cong \mathrm{Hom}(G_{L_{\mathfrak{p}_i}}, \mathbb{Q}_p(\chi)) \cong \mathrm{Hom}(G_{L_{\mathfrak{p}_i}}, \mathbb{Q}_p)^\chi.$$

In the proof of Lemma 5.1.4, we showed that the natural map

$$\mathrm{Hom}(G_L, \mathbb{Q}_p)^\chi \xrightarrow{\sim} \mathrm{Hom}(L_{\mathfrak{p}_1}^\times \times L_{\mathfrak{p}_2}^\times, \mathbb{Q}_p)^\chi$$

is an isomorphism. Another application of Lemma 5.1.2 and Lemma 5.1.3 now yields the claimed isomorphism. The dimension of the spaces $\mathrm{Hom}(G_{L_{\mathfrak{p}_i}}, \mathbb{Q}_p)^\chi$ were also computed as part of the proof of Lemma 5.1.4, and indeed both of these spaces contributed 1 dimension to the total 2-dimensional space $\mathrm{Hom}(G_L, \mathbb{Q}_p)^\chi$, completing the proof. □

To conclude this section, we will record one more result about the G_F-modules $\mathbb{Q}_p$ and $\mathbb{Q}_p(\chi)$ that we will need later.

Lemma 5.1.7. *It holds that*

$$H^2(G_F, \mathbb{Q}_p) = 0 \quad \textit{and} \quad H^2(G_F, \mathbb{Q}_p(\chi)) = 0.$$

Proof. We use the global Euler characteristic formula, also used by Pozzi in [Poz19] in the proof of Lemma 1.5.2; see [Lu11]. Now, since F has two real places, we compute that

$$\begin{aligned} \dim H^2(G_F, \mathbb{Q}_p) &= \dim H^1(G_F, \mathbb{Q}_p) - \dim H^0(G_F, \mathbb{Q}_p) \\ &\quad + 2 \dim H^0(G_{\mathbb{R}}, \mathbb{Q}_p) - 2 \dim \mathbb{Q}_p \\ &= 1 - 1 + 2 - 2 = 0, \end{aligned}$$

where we used Corollary 5.1.5 and Corollary 5.1.6. Similarly, using Proposition 5.1.4, we compute that

$$\begin{aligned} \dim H^2(G_F, \mathbb{Q}_p(\chi)) &= \dim H^1(G_F, \mathbb{Q}_p(\chi)) - \dim H^0(G_F, \mathbb{Q}_p(\chi)) \\ &\quad + 2 \dim H^0(G_{\mathbb{R}}, \mathbb{Q}_p(\chi)) - 2 \dim \mathbb{Q}_p(\chi) \\ &= 2 - 0 + 0 - 2 = 0, \end{aligned}$$

because complex conjugation in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts non-trivially through χ, as the field L is not totally real. □

5.2 Nearly ordinary deformation rings

We now start our journey into deformation theory. Similar treatments in various settings can be found in Pozzi's thesis [Poz19] and the works [BDP22, BD16, BDS20, BC06, DKV18].

In this section we start our study of the infinitesimal deformations of the representation $\rho = \mathbb{1} \oplus \chi$. The following lemma connects these deformations to the results from the previous section. From now on, $\mathbb{Q}_p[\epsilon]$ denotes the ring of dual numbers over $\mathbb{Q}_p$. Therefore, $\epsilon^2 = 0$.

Lemma 5.2.1. *Let $\tilde{\rho} : G_F \to \mathrm{GL}_2(\mathbb{Q}_p[\epsilon])$ be a group homomorphism that reduces to $\rho = \mathbb{1} \oplus \chi$ after composition with the natural map $\mathbb{Q}_p[\epsilon] \to \mathbb{Q}_p$. Let $a, b, c, d : G_F \to \mathbb{Q}_p$ be those functions such that*

$$\tilde{\rho}(x) = \left(1 + \epsilon \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}\right) \cdot \rho(x)$$

for all $x \in G_F$. Then these functions must respectively satisfy

$$a, d \in \mathrm{Hom}(G_F, \mathbb{Q}_p), \quad \textit{and} \quad b, c \in Z^1(G_F, \mathbb{Q}_p(\chi)).$$

Proof. This will follow from the condition that $\tilde{\rho}$ is a group homomorphism. Indeed, one may write out that for any $x, y \in G_F$,

$$\tilde{\rho}(xy) = \begin{pmatrix} 1 + a(xy)\epsilon & \chi(xy)b(xy)\epsilon \\ c(xy)\epsilon & \chi(xy)(1 + d(xy)\epsilon) \end{pmatrix}.$$

On the other hand, we expand the product $\tilde{\rho}(x)\tilde{\rho}(y)$ to obtain

$$\begin{pmatrix} 1 + (a(x) + a(y))\epsilon & \chi(xy)(\chi(x)b(y) + b(x))\epsilon \\ (c(x) + \chi(x)c(y))\epsilon & \chi(xy)(1 + (d(x) + d(y))\epsilon) \end{pmatrix}.$$

Comparing coefficients, we find that

$$\begin{aligned} a(xy) = a(x) + a(y), \quad & b(xy) = b(x) + \chi(x)b(y), \\ c(xy) = c(x) + \chi(x)c(y), \quad & d(xy) = d(x) + d(y). \end{aligned}$$

This is our lemma. □

However, in order to obtain a good theory of deformations, it is essential to work with a residually indecomposable representation, as becomes appararent from Proposition 1 in Mazur's [Maz89]. We have many ways to rigidify the reducible representation $\rho = \mathbb{1} \oplus \chi$, some of which are classified in the following proposition.

Proposition 5.2.2. *For any $\eta \in Z^1(G_F, \mathbb{Q}_p(\chi))$, the representation*

$$\rho_\eta : G_F \to \mathrm{GL}_2(\mathbb{Q}_p) : \tau \mapsto \begin{pmatrix} 1 & \chi(\tau)\eta(\tau) \\ 0 & \chi(\tau) \end{pmatrix}$$

has no non-scalar endomorphisms if and only if $\eta \neq 0 \in H^1(G_F, \mathbb{Q}_p(\chi))$.

Proof. We first verify that ρ_η is a group homomorphism:

$$\begin{pmatrix} 1 & \chi(\sigma\tau)\eta(\sigma\tau) \\ 0 & \chi(\sigma\tau) \end{pmatrix} = \begin{pmatrix} 1 & \chi(\sigma)\eta(\sigma) \\ 0 & \chi(\sigma) \end{pmatrix} \begin{pmatrix} 1 & \chi(\tau)\eta(\tau) \\ 0 & \chi(\tau) \end{pmatrix}.$$

Comparing the top-right entries, we obtain equality if and only if

$$\eta(\sigma\tau) = \eta(\sigma) + \chi(\sigma)\eta(\tau) \iff \eta \in Z^1(G_F, \mathbb{Q}_p(\chi)).$$

To show the claim about endomorphisms, it suffices to show that the centraliser of the image of ρ_η consists of solely scalar matrices. To this end, we must investigate when

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \chi(\tau)\eta(\tau) \\ 0 & \chi(\tau) \end{pmatrix} = \begin{pmatrix} 1 & \chi(\tau)\eta(\tau) \\ 0 & \chi(\tau) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for some fixed $a, b, c, d \in \mathbb{Q}_p$. Comparing the top-left entry yields the relation that $a = a + c\chi(\tau)\eta(\tau)$. Hence choosing τ such that $\eta(\tau) \neq 0$ forces $c = 0$. The relation above is then satisfied if and only if the top-right entries match up, yielding

$$a\chi(\tau)\eta(\tau) + b\chi(\tau) = b + d\chi(\tau)\eta(\tau) \iff (a-d)\eta(\tau) = b(\chi(\tau) - 1).$$

If $a = d$, then the above forces $b = 0$ and as such the matrix is scalar. If $a \neq d$, then η is a scalar multiple of the map $\tau \mapsto \chi(\tau) - 1$. This means that η is a coboundary, completing the proof. □

Definition 5.2.3. Let $\mathcal{C}_{\mathbb{Q}_p}$ denote the category of local complete Noetherian $\mathbb{Q}_p$-algebras with residue field $\mathbb{Q}_p$. For any $A \in \mathcal{C}_{\mathbb{Q}_p}$, we let $\mathfrak{m}_A$ denote its maximal ideal. Given any object $(A, \mathfrak{m}_A)$ of $\mathcal{C}_{\mathbb{Q}_p}$, a *lift* of ρ_η to A is a representation $\rho : G_F \to \mathrm{GL}_2(A)$ that reduces to ρ_η after composing with the natural map $\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{Q}_p)$ induced by the natural map $A \mapsto A/\mathfrak{m}_A \cong \mathbb{Q}_p$. We say that two lifts are equivalent if they are conjugate by a matrix in the kernel of the map $\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{Q}_p)$ above. A *deformation* of ρ_η to A is an equivalence class of lifts of ρ_η to A.

Definition 5.2.4. We define the functor $D_{\rho_\eta} : \mathcal{C}_{\mathbb{Q}_p} \to \mathbf{Set}$ by sending any $(A, \mathfrak{m}_A) \in \mathcal{C}_{\mathbb{Q}_p}$ to the set of deformations of ρ_η to A. The *tangent space* to such a deformation functor is defined as $D_{\rho_\eta}(\mathbb{Q}_p[\epsilon])$.

Proposition 5.2.5. *If $\eta \neq 0 \in H^1(G_F, \mathbb{Q}_p(\chi))$, the functor D_{ρ_η} is represented by a universal deformation ring R_{ρ_η}.*

Proof. This is done analogously to the proof of Proposition 1.2.6 in [Poz19], where the burden is reduced to showing the absence of non-scalar endomorphisms and finite dimensionality of the tangent spaces, by virtue of Proposition 1 in [Maz89]. The former is taken care of by Proposition 5.2.2, and for the latter we may bound the dimension of the tangent space of the functor D_{ρ_η} by the dimension of the tangent space of its semisimplification; $D_{\rho_0}(\mathbb{Q}_p[\epsilon])$. The structure of this tangent space has already been established in Lemma 5.2.1; we leave it to the reader to check that two lifts are equivalent if and only if all four matrix entries are cohomologous. By Corollary 5.1.5 and Corollary 5.1.6, the dimension of this tangent space is $1+2+2+1=6$; in particular, it is finite. □

From now on, we assume that $\eta \neq 0 \in H^1(G_F, \mathbb{Q}_p(\chi))$ to ensure that the results from Proposition 5.2.2 and Proposition 5.2.5 apply. Next, we introduce the notion of being *nearly ordinary*. In fact, to proceed, we must additionally require that $\eta|_{G_{\mathfrak{p}_2}} = 0$. The reason as to why is immediate from the following observation; the line $\langle e_2 \rangle$ is only fixed by $G_{\mathfrak{p}_2}$ if this condition on η is satisfied. Note that this fixes η uniquely up to scalar multiplication, as a result of Corollary 5.1.6.

Definition 5.2.6. Consider triples (ρ, L_1, L_2) where ρ is a lift of ρ_η to some $(A, \mathfrak{m}_A) \in \mathcal{C}_{\mathbb{Q}_p}$ and L_i is a free direct summand of A^2 such that L_i lifts the line $\langle e_i \rangle$ of $\mathbb{Q}_p^2$ for $i \in \{1,2\}$. We say that two such triples (ρ, L_1, L_2) and (ρ', L_1', L_2') are equivalent if for some $g \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{Q}_p))$ it holds that $\rho = g\rho' g^{-1}$ and $L_i = gL_i'$ for $i \in \{1,2\}$. We let $D_{\rho_\eta}^{\mathrm{fil}}$ be the functor sending an object $(A, \mathfrak{m}_A)$ to the set of equivalence classes of triples (ρ, L_1, L_2) as defined above.

Proposition 5.2.7. *The functor $D_{\rho_\eta}^{\mathrm{fil}}$ is represented by $R_{\rho_\eta}[\![X, Y]\!]$.*

Proof. This mildly generalises Lemma 1.3.2 in [Poz19]. We define a bijection

$$\mathrm{Hom}(R_{\rho_\eta}[\![X,Y]\!], A) \to D_{\rho_\eta}^{\mathrm{fil}}(A)$$

by sending some map $f : R_{\rho_\eta}[\![X,Y]\!] \to A$ to the representation

$$G_F \to \mathrm{GL}_2(R_{\rho_\eta}) \to \mathrm{GL}_2(R_{\rho_\eta}[\![X,Y]\!]) \to \mathrm{GL}_2(A)$$

induced by the universal representation and the map f itself, together with the lines $L_{f,1} = \langle e_1 + f(X)e_2 \rangle \subset A^2$ and $L_{f,2} = \langle f(Y)e_1 + e_2 \rangle \subset A^2$. Because f is a morphism of local rings, $f(X), f(Y) \in \mathfrak{m}_A$ and thus after

composing with the quotient map $A/\mathfrak{m}_A \cong \mathbb{Q}_p$, the line $L_{f,i}$ will reduce to $\langle e_i \rangle$ for $i \in \{1,2\}$, as desired. This shows that the map is well defined.

For surjectivity, we consider an arbitrary triple (ρ_A, L_1, L_2). By the universal property of R_{ρ_η}, possibly after conjugation with an element from $\ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{Q}_p))$, there exists a map $R_{\rho_\eta} \to A$ such that ρ_A is obtained from the universal representation after composing with this map. It remains to choose an appropriate image of X. To this end, we note that $L_1 = \langle a \cdot e_1 + b \cdot e_2 \rangle \subset A^2$ lifts $\langle e_1 \rangle$ by definition. After composing with the quotient map $A/\mathfrak{m}_A \to \mathbb{Q}_p$, this shows that $a \notin \mathfrak{m}_A$, or equivalently $a \in A^\times$, and that $b \in \mathfrak{m}_A$. We then map X to $a^{-1}b$, so that indeed $\langle e_1 + a^{-1}be_2 \rangle = \langle ae_1 + be_2 \rangle = L_A$. Very similarly, we construct the appropriate image for Y, showing surjectivity.

For injectivity, we must consider two morphisms $f, f' : R_{\rho_\eta}[\![X,Y]\!] \to A$ that have the same images $(\rho, L_1, L_2) = (\rho', L_1', L_2')$ under the above association. In particular, this means that they give rise to the same deformation, and hence by the universal property of R_{ρ_η}, there exists a unique map $R_{\rho_\eta} \to A$ that induces them from the universal deformation. However, by construction, these two deformations are induced by the two maps $R_{\rho_\eta} \to R_{\rho_\eta}[\![X,Y]\!] \to A$ induced by f and f'. These maps must thus coincide; in other words, f and f' must agree when restricted to R_{ρ_η}. This means that ρ and ρ' are not only equivalent, they are in fact equal. Note that $\rho = g\rho g^{-1}$ for some $g \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(\mathbb{Q}_p))$ would entail finding an endomorphism for ρ; as we have shown before, this forces g to be scalar. Hence $L_1 = gL_1' = L_1'$, so $\langle e_1 + f(X)e_2 \rangle = \langle e_1 + f'(X)e_2 \rangle$, and so it follows that $f(X) = f'(X)$. Very similarly, we find $f(Y) = f'(Y)$, completing the proof. □

Definition 5.2.8. Let $D^{\mathrm{no}}_{\rho_\eta} : \mathcal{C}_{\mathbb{Q}_p} \to \mathbf{Set}$ be the subfunctor of $D^{\mathrm{fil}}_{\rho_\eta}$ sending an object $(A, \mathfrak{m}_A) \in \mathcal{C}_{\mathbb{Q}_p}$ to the equivalence class of triples (ρ, L_1, L_2) as above with the properties that the line L_1 is $G_{\mathfrak{p}_1}$-stable and the line L_2 is $G_{\mathfrak{p}_2}$-stable. We call such deformations *nearly ordinary*, and these induce for $i \in \{1,2\}$ characters $\vartheta_i : G_{\mathfrak{p}_i} \to (A/L_i)^\times \cong A^\times$, called the associated *quotient characters*. Note that, since the line L_i lifts $\langle e_i \rangle$ for $i \in \{1,2\}$, it holds that $\vartheta_1 \equiv \chi \mod \mathfrak{m}_A$ and $\vartheta_2 \equiv \mathbb{1} \mod \mathfrak{m}_A$.

This practice of keeping track of the lines fixed by the decomposition groups is necessary in case the prime defining the decomposition group is *irregular*, because the line fixed by this group need not be unique. For us, $\chi(\mathfrak{p}_i) \neq 1$ for $i \in \{1,2\}$, so we are in the *regular* case, and therefore the fixed line will be unique, as Proposition 5.3.8 below will show. However, there is no harm in keeping track of this line at first in the regular case too, and we will do so in this section.

Proposition 5.2.9. *The functor $D^{\mathrm{no}}_{\rho_\eta}$ is represented by a universal deformation ring $R^{\mathrm{no}}_{\rho_\eta}$.*

Proof. This resembles part of Proposition 1.3.5(i) in [Poz19], but we repeat the argument here. The idea is to find an ideal $I \subset R_{\rho_\eta}[\![X,Y]\!]$ such that in the bijection

$$\mathrm{Hom}(R_{\rho_\eta}[\![X,Y]\!], A) \to D^{\mathrm{fil}}_{\rho_\eta}(A),$$

the image of an element on the left is contained in the subset $D^{\mathrm{no}}_{\rho_\eta}(A)$ if and only if it factors through $R_{\rho_\eta}[\![X,Y]\!]/I$. This would yield a bijection

$$\mathrm{Hom}(R_{\rho_\eta}[\![X,Y]\!]/I, A) \to D^{\mathrm{no}}_{\rho_\eta}(A),$$

establishing the desired conclusion $R^{\mathrm{no}}_{\rho_\eta} \cong R_{\rho_\eta}[\![X,Y]\!]/I$. It remains to identify I. Let us consider a representative for the universal deformation

$$\rho^{\mathrm{univ}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and investigate when its universal line $L^{\mathrm{univ}} = \langle e_1 + Xe_2 \rangle$ is stable under the action of $G_{\mathfrak{p}_1}$ via ρ^{univ}. By changing bases, this happens when

$$\begin{pmatrix} 1 & 0 \\ -X & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ X & 1 \end{pmatrix} = \begin{pmatrix} a + bX & b \\ c + (d-a)X - bX^2 & d - bX \end{pmatrix}$$

fixes the line $\langle e_1 \rangle$ on $G_{\mathfrak{p}_1}$. This is easy to read off; it happens when

$$c(\sigma) + (d(\sigma) - a(\sigma))X - b(\sigma)X^2 \quad \text{vanishes for all } \sigma \in G_{F_{\mathfrak{p}_1}}.$$

Let $I_1 \subset R_{\rho_\eta}[\![X,Y]\!]$ be the ideal generated by all the elements above. Then for any A, using linearity of the map $f : R_{\rho_\eta}[\![X,Y]\!] \to A$ and all conditions involved, the line L_1 is fixed by $G_{\mathfrak{p}_1}$ if and only if $f(I_1) = 0$; in other words, when f factors through the quotient ring $R_{\rho_\eta}[\![X,Y]\!]/I_1$.

Similarly, we define an ideal $I_2 \subset R_{\rho_\eta}[\![X,Y]\!]$ with the property that $G_{\mathfrak{p}_2}$ fixes the line L_2 when f factors through the quotient ring $R_{\rho_\eta}[\![X,Y]\!]/I_2$. It is now easy to see that we may set $I = I_1 + I_2$ to complete the proof. □

5.3 Computing tangent spaces

Recall that the tangent space to a deformation functor $D : \mathcal{C}_{\mathbb{Q}_p} \to \mathrm{Set}$ is defined as its value on the ring of dual numbers $\mathbb{Q}_p[\epsilon] \in \mathcal{C}_{\mathbb{Q}_p}$. Henceforth, we will also use the notation

$$t_D := D(\mathbb{Q}_p[\epsilon]).$$

Lemma 5.3.1. *Let V be the free $\mathbb{Q}_p$-module of rank 2 with its G_F-action given by ρ_η. Let t_{ρ_η} be the tangent space to D_{ρ_η}. Then t_{ρ_η} is isomorphic to $H^1(G_F, \mathrm{End}(V))$.*

Proof. This is Proposition 1 on page 284 of [CSS13], which provides us with the explicit bijection

$$H^1(G_F, \mathrm{End}(V)) \to t_{\rho_\eta}$$

by mapping Θ to the lift $(1 + \epsilon\Theta)\rho_\eta \in D_{\rho_\eta}(\mathbb{Q}_p[\epsilon])$. Checking this is just a calculation and we leave it to the curious reader to verify. □

We stress here that the action of G_F on $\mathrm{End}(V)$ is given by $gM = \rho_\eta(g)^{-1} M \rho_\eta(g)$ for any $g \in G_F$ and $M \in \mathrm{End}(V) \cong M_2(\mathbb{Q}_p)$. This G_F-module is also often written as $\mathrm{ad}(\rho_\eta)$, the *adjoint representation*. We will do so henceforth.

Lemma 5.3.2. *There is a well-defined map of G_F-modules*

$$\varphi_1 : \mathrm{ad}(\rho_\eta) \to \mathbb{Q}_p(\chi) : \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mapsto z.$$

Proof. Since this is clearly a group homomorphism, it suffices to verify the Galois-equivariance. To this end, we compute that

$$\begin{aligned} \begin{pmatrix} 1 & -\eta \\ 0 & \chi \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & \chi\eta \\ 0 & \chi \end{pmatrix} &= \begin{pmatrix} 1 & -\eta \\ 0 & \chi \end{pmatrix} \begin{pmatrix} x & x\chi\eta + y\chi \\ z & z\chi\eta + w\chi \end{pmatrix} \\ &= \begin{pmatrix} x - z\eta & x\chi\eta + y\chi - z\chi\eta^2 - w\chi\eta \\ z\chi & z\eta + w \end{pmatrix}. \end{aligned}$$

This shows that conjugation indeed induces multiplication by χ on the bottom-left entry, completing the proof. □

Now let $W_1 = \ker(\varphi_1)$; in other words, we have a short exact sequence

$$0 \to W_1 \to \mathrm{ad}(\rho_\eta) \to \mathbb{Q}_p(\chi) \to 0.$$

We proceed to refine W_1 slightly.

Lemma 5.3.3. *There is a well-defined map of G_F-modules*

$$\varphi_2 : W_1 \to \mathbb{Q}_p \oplus \mathbb{Q}_p : \begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \mapsto (x, w).$$

Proof. Once again, we are left to verify Galois equivariance. This becomes apparent from the following specialisation of the computation from the proof of Lemma 5.3.2 above;

$$\begin{pmatrix} 1 & -\eta \\ 0 & \chi \end{pmatrix} \begin{pmatrix} x & y \\ 0 & w \end{pmatrix} \begin{pmatrix} 1 & \chi\eta \\ 0 & \chi \end{pmatrix} = \begin{pmatrix} x & x\chi\eta + y\chi - w\chi\eta \\ 0 & w \end{pmatrix},$$

obtained by setting $z = 0$. Indeed, we see that x and w remain untouched by the Galois action, as desired. □

We now define $W_2 = \ker(\varphi_2)$, so that we have a short exact sequence

$$0 \to W_2 \to W_1 \to \mathbb{Q}_p \oplus \mathbb{Q}_p \to 0.$$

The following result completes the filtration and allows us to start computing cohomology groups using long exact sequences.

Lemma 5.3.4. *There is a well-defined map of G_F-modules*

$$W_2 \to \mathbb{Q}_p(\chi) : \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \mapsto y.$$

Proof. Indeed, we copy the computation from before once more to find

$$\begin{pmatrix} 1 & -\eta \\ 0 & \chi \end{pmatrix} \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & \chi\eta \\ 0 & \chi \end{pmatrix} = \begin{pmatrix} 1 & -\eta \\ 0 & \chi \end{pmatrix} \begin{pmatrix} 0 & y\chi \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & y\chi \\ 0 & 0 \end{pmatrix},$$

which completes the proof. □

Proposition 5.3.5. *The group $H^1(G_F, W_1)$ is 3-dimensional. On the other hand, it holds that $H^2(G_F, W_1) = 0$.*

Proof. Since $\chi \neq \mathbb{1}$, it is clear that

$$H^0(G_F, \mathbb{Q}_p(\chi)) = 0 \quad \text{and} \quad H^0(G_F, \mathbb{Q}_p \oplus \mathbb{Q}_p) = \mathbb{Q}_p \oplus \mathbb{Q}_p.$$

Further, one may observe that

$$\begin{aligned} H^0(G_F, W_1) = W_1^{G_F} &= \left\{ M \in W_1 \mid \rho^{-1} M \rho = M \right\} \\ &= W_1 \cap \left\{ M \in M_2(\mathbb{Q}_p) \mid M\rho = \rho M \right\} = \langle \mathrm{id} \rangle \cong \mathbb{Q}_p, \end{aligned}$$

since in the proof of Proposition 5.2.2, we showed that only scalar matrices commute with the image of ρ_η for $\eta \neq 0 \in H^1(G_F, \mathbb{Q}_p(\chi))$. Finally, we recall Lemma 5.1.7, which states that $H^2(G_F, \mathbb{Q}_p(\chi)) = 0$. Combining all of this, the long exact sequence associated with the short exact sequence defining W_2 becomes

$$0 \to \mathbb{Q}_p \to \mathbb{Q}_p \oplus \mathbb{Q}_p \to H^1(G_F, \mathbb{Q}_p(\chi)) \to H^1(G_F, W_1) \to H^1(G_F, \mathbb{Q}_p \oplus \mathbb{Q}_p) \to 0.$$

We now find that

$$\dim\, H^1(G_F, W_1) + 2 = 1 + \dim\, H^1(G_F, \mathbb{Q}_p(\chi)) + \dim\, H^1(G_F, \mathbb{Q}_p \oplus \mathbb{Q}_p).$$

Applying Corollary 5.1.5 and Corollary 5.1.6, we conclude that

$$\dim\, (H^1(G_F, W_1)) = 1 + 2 + 2 - 2 = 3,$$

completing the proof of the first claim. For the second, we look slightly further along in the long exact sequence, to find

$$\ldots \to H^2(G_F, \mathbb{Q}_p(\chi)) \to H^2(G_F, W_1) \to H^2(G_F, \mathbb{Q}_p \oplus \mathbb{Q}_p) \to \ldots$$

Now again, by Lemma 5.1.7, the first and last terms here must vanish, and as such, so will $H^2(G_F, W_1)$. □

Theorem 5.3.6. *The tangent space t_{ρ_η} is 5-dimensional.*

Proof. Using the isomorphism

$$t_{\rho_\eta} \cong H^1(G_F, \mathrm{ad}(\rho_\eta))$$

from Lemma 5.3.1, we reduce to computing the dimension of the latter cohomology group. We now use the long exact sequence associated with the short exact sequence defining W_1. Recalling that

$$H^0(G_F, \mathbb{Q}_p(\chi)) = 0 \quad \text{and} \quad H^2(G_F, W_1) = 0$$

by Proposition 5.3.5 above, we conclude that part of this sequence reads

$$0 \to H^1(G_F, W_1) \to H^1(G_F, \mathrm{ad}(\rho_\eta)) \to H^1(G_F, \mathbb{Q}_p(\chi)) \to 0.$$

In particular, by Corollary 5.1.6 and Proposition 5.3.5, we find that

$$\dim\, H^1(G_F, \mathrm{ad}(\rho_\eta)) = \dim\, H^1(G_F, W_1) + \dim\, H^1(G_F, \mathbb{Q}_p(\chi)) = 5,$$

completing the proof. □

With this in hand, we will next concern ourselves with the tangent spaces associated with the two other deformation functors we introduced;

$$t_{\rho_\eta}^{\mathrm{fil}} := D_{\rho_\eta}^{\mathrm{fil}}(\mathbb{Q}_p[\epsilon]) \quad \text{and} \quad t_{\rho_\eta}^{\mathrm{no}} := D_{\rho_\eta}^{\mathrm{no}}(\mathbb{Q}_p[\epsilon]).$$

Lemma 5.3.7. *The space $t^{\mathrm{fil}}_{\rho_\eta}$ is isomorphic to $H^1(G_F, \mathrm{ad}(\rho_\eta)) \oplus \mathbb{Q}_p^2$.*

Proof. By its definition and using Proposition 5.2.7, we have

$$t^{\mathrm{fil}}_{\rho_\eta} = \mathrm{Hom}(R^{\mathrm{fil}}_{\rho_\eta}, \mathbb{Q}_p[\epsilon]) = \mathrm{Hom}(R_{\rho_\eta}[\![X, Y]\!], \mathbb{Q}_p[\epsilon]).$$

Now observe that we may choose the images of X and Y arbitrarily and independently in the maximal ideal $\mathbb{Q}_p\epsilon$ and can thus be specified with two additional numbers. We then obtain the isomorphism

$$\mathrm{Hom}(R_{\rho_\eta}[\![X, Y]\!], \mathbb{Q}_p[\epsilon]) \cong \mathrm{Hom}(R_{\rho_\eta}, \mathbb{Q}_p[\epsilon]) \oplus \mathbb{Q}_p^2.$$

Finally, using Lemma 5.3.1, we find that

$$\mathrm{Hom}(R_{\rho_\eta}, \mathbb{Q}_p[\epsilon]) \cong D_{\rho_\eta}(\mathbb{Q}_p[\epsilon]) \cong t_{\rho_\eta} \cong H^1(G_F, \mathrm{ad}(\rho_\eta)).$$

This proves the result. □

Proposition 5.3.8. *A triple $(\Theta, \lambda_1, \lambda_2) \in H^1(G_F, \mathrm{ad}(\rho_\eta)) \oplus \mathbb{Q}_p^2$ corresponds to a nearly ordinary deformation of ρ_η if and only if*

$$c|_{G_{\mathfrak{p}_1}} = \lambda_1(1-\chi) \quad \textit{and} \quad \chi b|_{G_{\mathfrak{p}_2}} = \lambda_2(\chi - 1), \quad \textit{where} \quad \Theta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Proof. By its definition and using Proposition 5.2.9, we have

$$t^{\mathrm{no}}_{\rho_\eta} = \mathrm{Hom}(R^{\mathrm{no}}_{\rho_\eta}, \mathbb{Q}_p[\epsilon]) = \mathrm{Hom}(R_{\rho_\eta}[\![X, Y]\!]/I, \mathbb{Q}_p[\epsilon]),$$

where $I = I_1 + I_2$ as in the proof of Proposition 5.2.9. In other words, the tangent space $t^{\mathrm{no}}_{\rho_\eta}$ is identified with those elements from $\mathrm{Hom}(R_{\rho_\eta}[\![X, Y]\!], \mathbb{Q}_p[\epsilon])$ for which all images of expressions generating the ideal I vanish inside $\mathbb{Q}_p[\epsilon]$. If

$$\rho^{\mathrm{univ}} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

then the ideal I is generated by the expressions

$$\begin{aligned} \gamma(x) + (\delta(x) - \alpha(x))X - \beta(x)X^2 \quad & \text{for all } x \in G_{\mathfrak{p}_1}; \\ \beta(y) + (\alpha(y) - \delta(y))Y - \gamma(y)Y^2 \quad & \text{for all } y \in G_{\mathfrak{p}_2}. \end{aligned}$$

Now let $\varphi \in \mathrm{Hom}(R_{\rho_\eta}[\![X, Y]\!], \mathbb{Q}_p[\epsilon])$. By Lemma 5.3.7 above, there is a unique triple $(\Theta, \lambda_1, \lambda_2) \in H^1(G_F, \mathrm{ad}(\rho_\eta)) \oplus \mathbb{Q}_p^2$ such that

$$\varphi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (1 + \epsilon\Theta)\rho_\eta = \begin{pmatrix} 1 + a\epsilon & \chi\eta + \chi[\eta a + b]\epsilon \\ c\epsilon & \chi + \chi[\eta c + d]\epsilon \end{pmatrix}$$

and such that $\varphi(X) = \lambda_1\epsilon$ and $\varphi(Y) = \lambda_2\epsilon$. We can now compute the constraints posed by the vanishing on I, using that $\epsilon^2 = 0$ to simplify our expressions, to be

$$c = \lambda_1(1-\chi) \quad \text{on } G_{\mathfrak{p}_1} \quad \text{and} \quad \chi\eta + \chi[\eta a + b]\epsilon + \lambda_2(1-\chi)\epsilon = 0 \quad \text{on } G_{\mathfrak{p}_2}.$$

However, η is chosen to be trivial on $G_{\mathfrak{p}_2}$, and as such, we obtain the two expressions that we were to prove. □

Lemma 5.3.9. *There is a well-defined surjective homomorphism*

$$f : H^1(G_F, \mathrm{ad}(\rho_\eta)) \to H^1(G_{\mathfrak{p}_1}, \mathbb{Q}_p(\chi)) \oplus H^1(G_{\mathfrak{p}_2}, \mathbb{Q}_p(\chi))$$

given by, adopting the usual notation for the components of Θ*,*

$$(\Theta, \lambda_1, \lambda_2) \mapsto \big(c|_{G_{\mathfrak{p}_1}}, b|_{G_{\mathfrak{p}_2}}\big).$$

Proof. The proof of Theorem 5.3.6 showed the existence of a surjective map

$$H^1(G_F, \mathrm{ad}(\rho_\eta)) \to H^1(G_F, \mathbb{Q}_p(\chi))$$

which is easily seen to be given by mapping $\Theta \in H^1(G_F, \mathrm{ad}(\rho_\eta))$ to $c \in H^1(G_F, \mathbb{Q}_p(\chi))$. On the other hand, when restricting to $G_{\mathfrak{p}_2}$, by virtue of $\eta|_{G_{\mathfrak{p}_2}} = 0$, the representation ρ_η reduces to $\mathbb{1} \oplus \chi$. Using Lemma 5.2.1, it follows that also $b|_{G_{\mathfrak{p}_2}} \in H^1(G_{\mathfrak{p}_2}, \mathbb{Q}_p(\chi))$. Combining these two maps yields f. For its surjectivity, it suffices to show that f its not trivial on the second component. However, the map restricted to the submodule $H^1(G_F, W_2)$ of $H^1(G_F, \mathrm{ad}(\rho_\eta))$ is clearly surjective, completing the proof. □

Proposition 5.3.10. *The tangent space* $t^{\mathrm{no}}_{\rho_\eta}$ *is in bijection with* $\ker(f)$.

Proof. For $i \in \{1, 2\}$, fix $x_i \in G_{\mathfrak{p}_i} \setminus G_L$. Given $\Theta \in \ker(f)$, we may construct a nearly ordinary triple $(\Theta, \lambda_1, \lambda_2)$ using the association

$$\Theta \mapsto \big(\Theta, c(x_1)/2, b(x_2)/2\big).$$

This is in fact nearly ordinary, because by virtue of Θ being in the kernel of f, the cocycles $c|_{\mathfrak{p}_1}$ and $b|_{\mathfrak{p}_2}$ are coboundaries and as such, are given by $c|_{\mathfrak{p}_1} = \mu_1(1-\chi)$ and $\chi b|_{\mathfrak{p}_2} = \mu_2(\chi - 1)$ for certain $\mu_1, \mu_2 \in \mathbb{Q}_p$. Using that $\chi(x_i) = -1$ by construction, evaluating yields that $\mu_1 = c(x_1)/2$ and $\mu_2 = b(x_2)/2$ are uniquely determined. Comparing with Proposition 5.3.8, this shows that the triple is indeed nearly ordinary. Conversely, to any nearly ordinary triple we may associate its first component Θ, since by Proposition 5.3.8, for nearly ordinary triples, $c|_{\mathfrak{p}_1}$ and $b|_{\mathfrak{p}_2}$ must be coboundaries, and thus Θ must in fact be inside $\ker(f)$. Since these operations are evidently inverse, this establishes the proposition. □

Corollary 5.3.11. *The tangent space $t_{\rho_\eta}^{\mathrm{no}}$ is 3-dimensional.*

Proof. Using Lemma 5.3.9 and Proposition 5.3.10 above, we have identified this tangent space as the kernel of the surjective map

$$f : t_{\rho_\eta} \to H^1(G_{\mathfrak{p}_1}, \mathbb{Q}_p(\chi)) \oplus H^1(G_{\mathfrak{p}_2}, \mathbb{Q}_p(\chi))$$

Using Theorem 5.3.6 and Corollary 5.1.6, we may now conclude that

$$\dim t_{\rho_\eta}^{\mathrm{no}} = 5 - 2 = 3;$$

as claimed. □

5.4 Representations on Hecke algebras

Let $\mathbb{T}^{\mathrm{no}} := h_{\mathbf{1},\mathbf{0}}^{\mathrm{n.o.}}(K(p^\infty), \mathbb{Q}_p)$ denote the nearly ordinary Hecke algebra as defined in [Hid89a] and sketched in Appendix A.5. We recall that this inherently adèlic object is generated by Hecke operators $T_{\mathfrak{l}}$ for prime ideals $\mathfrak{l} \subset \mathcal{O}_F$ with $\mathfrak{l} \nmid p$, and operators U_{π_i} for $i \in \{1, 2\}$ as π_i ranges over the uniformisers of $\mathcal{O}_{F,\mathfrak{p}_i}$. Let $E_{1,\chi}$ denote the parallel weight $(1, 1)$ Hilbert Eisenstein series as defined in Appendix A.2 and let

$$f := (1 - V_{\mathfrak{p}_1})(1 + V_{\mathfrak{p}_2})E_{1,\chi} = E_{1,\chi}^{(p)}$$

be the appropriate p-stabilisation that is core to all our arguments. A priori there are four ways to p-stabilise $E_{1,\chi}$, corresponding with the signs $(+,+)$, $(+,-)$, $(-,+)$ and $(-,-)$. The choices $(-,+)$ and $(+,-)$ yield equivalent theories, but with the roles of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ reversed. However, the other two choices will not work for our purposes for two reasons. First and foremost, from the proof of Lemma A.3.3, one easily deduces that these two other choices do not yield a p-adic cusp form, and therefore we have no hope of deforming it as one.

The second reason is more subtle, and it will manifest itself throughout this section. If we choose the same sign twice, then associated with this p-stabilisation is a nearly ordinary deformation problem in which we would insist both $G_{\mathfrak{p}_1}$ and $G_{\mathfrak{p}_2}$ to fix a lift of *the same* line among $\langle e_1 \rangle$ or $\langle e_2 \rangle$. This is because the sign of the p-stabilisation is connected to the quotient character of the associated nearly ordinary Galois representation we are deforming. This character is χ for the line $\langle e_1 \rangle$ and $\mathbb{1}$ for $\langle e_2 \rangle$. Evaluated at $\mathfrak{p}_i$ for $i \in \{1, 2\}$, these characters yield -1 and 1 respectively. In this sense, our choice of p-stabilisation matches our Definition 5.2.8 of a nearly ordinary deformation.

There are again two reasons for why it is important to work with a deformation problem in which the stable lines for the decomposition groups are lifts of different lines. The first is that it enables us to carry out the strategy that we will follow in this section; in particular, in the proof of Proposition 5.4.10 we will use that the nearly ordinary condition affects the lower left entry for one of the decomposition groups, and the upper right entry for the other, cutting out a 1-dimensional subspace of the 2-dimensional space $H^1(G_F, \mathbb{Q}_p(\chi))$. Without this information, it is not obvious how to proceed.

The second reason for this importance is again rather subtle and will only manifest itself in Chapter 6. To prove Theorem B, we will have to take the diagonal restriction of an infinitesimal cuspidal p-adic family of modular forms with respect to the ideal $\mathcal{D}_F^{-1}\mathfrak{q}_1$. However, as explained in Remark A.3.6, its $\epsilon = 0$ specialisation will *not* vanish. In view of Lemma 2.1 in [DPV21], which requires this vanishing to ensure that the derivative of such a family is still an overconvergent modular form, this fact might jeopardise our strategy. However, we remedy this issue by choosing in Section 6.2 a deformation in the so-called *anti-parallel* weight direction, which ensures that the weight of the diagonal restriction of our family remains constant. Then we may still use Lemma 2.1 in [DPV21] to conclude that our derivative is an overconvergent modular form by subtracting a constant family; we use this trick in the proof of Proposition 6.3.1. The weight character for nearly ordinary modular forms can be computed from the two quotient characters. If we had been working with a deformation problem in which both decomposition groups would have fixed lines lifting the same line, then the two quotient characters would have been equal and we would not have had the freedom required to write down a deformation with the properties that we need.

The modular form $f = E_{1,\chi}^{(p)}$ defines a morphism $\mathbb{T}^{\mathrm{no}} \to \mathbb{Q}_p$ by sending a Hecke operator to its f-eigenvalue. Let $\mathbb{T}$ be the nilreduction of the completion of the localisation of $\mathbb{T}^{\mathrm{no}}$ at the prime ideal $\mathfrak{m}_f$ given by the kernel of this morphism. Let $\mathbb{K}$ be its ring of fractions, which is a product of fields. Then Hida proved the following in [Hid89a].

Theorem 5.4.1. *There exists a unique semisimple Galois representation $\pi : G_F \to \mathrm{GL}_2(\mathbb{K})$ with the following properties:*

- *π is continuous, odd and unramified outside p;*
- *For each prime $\mathfrak{l} \nmid p$, it holds that*

$$\det(1 - \pi(\mathrm{Frob}_\mathfrak{l})X) = 1 - T_\mathfrak{l} X + \langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l}) X^2;$$

- *For $i \in \{1,2\}$ there exist characters $\epsilon_i, \delta_i : G_{\mathfrak{p}_i} \to \mathbb{T}^\times$ such that, up to equivalence, when restricted to $G_{\mathfrak{p}_i}$, the representation π is of the form*

$$\pi(\sigma) = \begin{pmatrix} \epsilon_i(\sigma) & * \\ 0 & \delta_i(\sigma) \end{pmatrix} \quad \text{for} \quad \sigma \in G_{\mathfrak{p}_i}.$$

- *If we identify $G_{\mathfrak{p}_i}^{\mathrm{ab}} \cong F_{\mathfrak{p}_i}^\times$ through the arithmetic local reciprocity map, then we have the identity $\delta_i(x) = U_x$ for all $x \in F_{\mathfrak{p}_i}^\times$.*

To obtain from this a deformation of ρ_η, we are to refine this representation in two ways. First, we must find a stable lattice inside $\mathbb{K}^2$ so that we obtain a representation $G_F \to \mathrm{GL}_2(\mathbb{T})$ instead, which we may then reduce modulo its maximal ideal $\mathfrak{m}_f$. Secondly, we must insist that this reduction equals ρ_η. Let us achieve these two results in succession. The former will turn out to consume most of the work. The techniques used in this section reflect strongly those employed in Section 4 of [DKV18], but again see also the works [Poz19, BDP22, BD16, BDS20, BC06].

Lemma 5.4.2. *There exist an element $\gamma \in G_F$ and a basis of $\{e_1, e_2\}$ of $\mathbb{K}^2$ such that $\chi(\gamma) = -1$ and in addition,*

$$\pi(\gamma) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

where $\lambda_1 \equiv 1 \mod \mathfrak{m}_f$ and $\lambda_2 \equiv -1 \mod \mathfrak{m}_f$, and such that the unique lines fixed by the subgroup $G_{\mathfrak{p}_i}$ for $i \in \{1,2\}$, can be written as $\langle e_1 + y_i e_2 \rangle$ where $y_i \in \mathbb{K}^\times$.

Proof. This is the content of Lemma 4.3, Equation 64 in Section 4.2 and Lemma 4.6 in [DKV18]. The fact that there must be a unique fixed line comes down to the fact that π is irreducible, and the statement about the lines being in general position is not deep considering $\mathbb{K}$ is a product of fields, and as such, almost all lines are of that form. □

In any basis as in the lemma above, write

$$\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

for certain functions $a, b, c, d : G_F \to \mathbb{K}$.

Lemma 5.4.3. *The functions a and d take values in $\mathbb{T}$. In fact, it holds that $a \equiv \mathbb{1} \mod \mathfrak{m}_f$ and $d \equiv \chi \mod \mathfrak{m}_f$.*

Proof. For any prime $\mathfrak{l} \nmid p$, using Theorem 5.4.1, we have that

$$a(\mathrm{Frob}_\mathfrak{l}) + d(\mathrm{Frob}_\mathfrak{l}) = \mathrm{Tr}(\pi(\mathrm{Frob}_\mathfrak{l})) = T_\mathfrak{l} \in \mathbb{T}.$$

In other words, the continuous map $\mathrm{Tr}(\pi) : G_F \to \mathbb{K}$ takes on integral values for every element $\mathrm{Frob}_\mathfrak{l}$ for $\mathfrak{l} \nmid p$. By Chebotarev's Density Theorem, these Galois elements are dense inside G_F, and as such, by continuity the result follows for all of G_F. We may then observe that also

$$\lambda_1 a(\mathrm{Frob}_\mathfrak{l}) + \lambda_2 d(\mathrm{Frob}_\mathfrak{l}) = \mathrm{Tr}(\pi(\gamma \mathrm{Frob}_\mathfrak{l})) \in \mathbb{T}.$$

Combining these two expressions and using that $\lambda_1 - \lambda_2 \in \mathbb{T}^\times$ then yields that a and d both must have integral image themselves, completing the proof of the first claim. To see the second, we observe that $T_\mathfrak{l} \equiv 1 + \chi(\mathfrak{l}) \mod \mathfrak{m}_f$ because $f = E^{(p)}_{1,\chi}$ has eigenvalue $1 + \chi(\mathfrak{l})$ for the operator $T_\mathfrak{l}$. Again, by continuity, this implies that for any $\sigma \in G_F$, it holds that

$$a(\sigma) + d(\sigma) = \mathrm{Tr}(\pi(\sigma)) \equiv 1 + \chi(\sigma) \mod \mathfrak{m}_f$$

and as such, it also holds that

$$a(\sigma) - d(\sigma) \equiv \lambda_1 a(\sigma) + \lambda_2 d(\sigma) = \mathrm{Tr}(\pi(\gamma\sigma)) \equiv 1 - \chi(\sigma) \mod \mathfrak{m}_f.$$

Combining these two equations shows the claim from the lemma. □

Lemma 5.4.4. *For any $\sigma, \tau \in G_F$, it holds that $b(\sigma)c(\tau) \in \mathfrak{m}_f$.*

Proof. This follows from the fact that π is a homomorphism;

$$\begin{pmatrix} a(\sigma\tau) & b(\sigma\tau) \\ c(\sigma\tau) & d(\sigma\tau) \end{pmatrix} = \pi(\sigma\tau) = \pi(\sigma)\pi(\tau) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} a(\tau) & b(\tau) \\ c(\tau) & d(\tau) \end{pmatrix}.$$

Comparing the top left entry then yields the equality

$$a(\sigma\tau) = a(\sigma)a(\tau) + b(\sigma)c(\tau).$$

By the above, all values of a must be contained in $1 + \mathfrak{m}_f\mathbb{T}$, and as such, the expression $b(\sigma)c(\tau)$ must be inside of $\mathfrak{m}_f$ for all $\sigma, \tau \in G_F$. □

Definition 5.4.5. Let B denote the $\mathbb{T}$-submodule of $\mathbb{K}$ generated by all elements of the form $b(\sigma)$ for $\sigma \in G_F$, and C the analogous submodule using the elements $c(\sigma)$.

Lemma 5.4.6. *There are well-defined injective maps*

$$j_B : \mathrm{Hom}_{\mathbb{T}}(B/\mathfrak{m}_f B, \mathbb{T}/\mathfrak{m}_f) \to H^1(G_F, \mathbb{Q}_p(\chi)) : \phi \mapsto \chi \cdot (\phi \circ b);$$
$$j_C : \mathrm{Hom}_{\mathbb{T}}(C/\mathfrak{m}_f C, \mathbb{T}/\mathfrak{m}_f) \to H^1(G_F, \mathbb{Q}_p(\chi)) : \psi \mapsto \psi \circ c.$$

Proof. To show that the maps are well-defined, we write out the equations for the off-diagonal entries we obtain when we require π to be a homomorphism. These yield respectively that

$$b(\sigma\tau) = d(\tau)b(\sigma) + a(\sigma)b(\tau) \quad \text{and} \quad c(\sigma\tau) = a(\tau)c(\sigma) + d(\sigma)c(\tau).$$

We may now write out, using that a and d take values in $\mathbb{T}$ and as such commute with the application of ϕ by its assumed $\mathbb{T}$-linearity,

$$\begin{aligned}(\chi \cdot (\phi \circ b))(\sigma\tau) &= \chi(\sigma\tau)\phi(b(\sigma\tau)) \\ &= \chi(\sigma\tau)\big(d(\tau)\phi(b(\sigma)) + a(\sigma)\phi(b(\tau))\big) \\ &\equiv \chi(\sigma\tau)\big(\chi(\tau)\phi(b(\sigma)) + \phi(b(\tau))\big) \mod \mathfrak{m}_f \\ &= (\chi \cdot (\phi \circ b))(\sigma) + \chi(\sigma)(\chi \cdot (\phi \circ b))(\tau),\end{aligned}$$

showing well-definedness. A very similar calculation shows that $\psi \circ c \in Z^1(G_F, \mathbb{Q}_p(\chi))$. It remains to show that, if the result is a coboundary, then ϕ must have been identically zero, again because the proof for j_C will be very similar. So let us suppose that for some $\lambda \in \mathbb{T}/\mathfrak{m}_f$, it holds that $\chi \cdot (\phi \circ b) = \lambda(1 - \chi)$. In particular, this means that $G_L \subset \ker(\chi \cdot (\phi \circ b))$, or equivalently, $G_L \subset \ker(\phi \circ b)$. Any other element of G_F can be written as $\gamma\tau$ for some $\tau \in G_L$. Using that $b(\gamma) = 0$, as can be read off from the matrix $\pi(\gamma)$, we compute that

$$(\phi \circ b)(\gamma\tau) = d(\tau)(\phi \circ b)(\gamma) + a(\gamma)(\phi \circ b)(\tau) \equiv d(\tau) \cdot \phi(0) + 1 \cdot 0 = 0 \mod \mathfrak{m}_f,$$

showing that $\phi \circ b$ is trivial everywhere. Since ϕ is defined on the module generated by all the images of b, it must be trivial itself. □

We continue to exploit the knowledge that π is nearly ordinary to obtain certain local information about the entries b and c, which we will later use to deduce further global properties of the modules B and C. It is quite remarkable how a subtle dance between global properties and information about local restrictions turns out to provide us with all the conclusions that we need.

Lemma 5.4.7. *It holds that* $\epsilon_1 \equiv \mathbb{1} \mod \mathfrak{m}_f$ *and* $\delta_1 \equiv \chi \mod \mathfrak{m}_f$. *Similarly, it holds that* $\epsilon_2 \equiv \chi \mod \mathfrak{m}_f$ *and* $\delta_2 \equiv \mathbb{1} \mod \mathfrak{m}_f$.

Proof. We have seen before that $\mathrm{Tr}(\pi(\sigma)) \equiv 1 + \chi(\sigma) \mod \mathfrak{m}_f$ for all $\sigma \in G_F$, so if we have shown the above claims for δ_1 and δ_2, the results for ϵ_1 and ϵ_2 follow. To determine δ_1, we recall from Theorem 5.4.1 that $\delta_1(x) = U_x$ for all $x \in G_{\mathfrak{p}_i}^{\mathrm{ab}} \cong F_{\mathfrak{p}_i}^\times$. By construction, the p-stabilisation $f = E_{1,\chi}^{(p)} = (1 - V_{\mathfrak{p}_1})(1 + V_{\mathfrak{p}_2})E_{1,\chi}$ is a U_{π_1}-eigenvector with eigenvalue -1 for all uniformisers π_1 inside $F_{\mathfrak{p}_i}^\times$. Therefore, $U_{\pi_1} \equiv -1 = \chi(\mathfrak{p}_1) \mod \mathfrak{m}_f$ and so $\delta_1 \equiv \chi \mod \mathfrak{m}_f$; the proof for δ_2 is similar. □

Proposition 5.4.8. *The map* $c \mod \mathfrak{m}_f C$ *is a coboundary when restricted to* $G_{\mathfrak{p}_1}$. *Similarly, the map* $\chi \cdot b \mod \mathfrak{m}_f B$ *is a coboundary when restricted to* $G_{\mathfrak{p}_2}$.

Proof. We only show the claim about $c \mod \mathfrak{m}_f C$, for the result for $\chi \cdot b \mod \mathfrak{m}_f B$ can be proved analogously. Let

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

be the change of basis matrix that changes π into the upper triangular form from Theorem 5.4.1 on $G_{\mathfrak{p}_1}$. Then it must satisfy for all $\sigma \in G_{\mathfrak{p}_1}$,

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \epsilon_1(\sigma) & * \\ 0 & \delta_1(\sigma) \end{pmatrix}.$$

By Lemma 4.6 in [DKV18], we may assume that $x, z \in \mathbb{K}^\times$. Comparing the bottom left entries, we obtain that

$$xc(\sigma) + zd(\sigma) = z\epsilon_1(\sigma), \quad \text{or equivalently,} \quad c(\sigma) = \frac{z}{x}\big(\epsilon_1(\sigma) - d(\sigma)\big).$$

Choose any $\tau \in G_{\mathfrak{p}_1}$ such that $\chi(\tau) = -1$. Using Lemma 5.4.7 above in combination with Lemma 5.4.3, we find that $\epsilon_1(\tau) \equiv 1 \not\equiv -1 \equiv d(\tau) \mod \mathfrak{m}_f$, and as a result, it follows that $\epsilon_1(\tau) - d(\tau) \notin \mathfrak{m}_f$. In other words, it belongs to $\mathbb{T}^\times$. This shows that

$$\frac{z}{x} = c(\tau) \cdot \big(\epsilon_1(\tau) - d(\tau)\big)^{-1} \in C,$$

since C was the $\mathbb{T}$-module *generated* by the images of c. Therefore

$$c(\sigma) \equiv \frac{z}{x}\big(\epsilon_1(\sigma) - d(\sigma)\big) \equiv \frac{z}{x}\big(1 - \chi(\sigma)\big) \mod \mathfrak{m}_f C,$$

which shows that c is a coboundary $\mod \mathfrak{m}_f C$ on $G_{\mathfrak{p}_1}$. □

Corollary 5.4.9. *The map* $c \mod \mathfrak{m}_f C$ *is* not *a coboundary when restricted to* $G_{\mathfrak{p}_2}$. *Similarly, the map* $\chi \cdot b \mod \mathfrak{m}_f B$ *is* not *a coboundary when restricted to* $G_{\mathfrak{p}_1}$.

Proof. Again, we only show the claim about $c \mod \mathfrak{m}_f C$, for the result for $\chi \cdot b \mod \mathfrak{m}_f B$ can be proved analogously. Let us therefore suppose that c is a coboundary when restricted to both $G_{\mathfrak{p}_1}$ and $G_{\mathfrak{p}_2}$. We claim that c is then a coboundary globally.

To see this, first note that $c \in H^1(G_F, C/\mathfrak{m}_f C)$ if the action of G_F on $C/\mathfrak{m}_f C$ is through the character χ. Indeed, by Lemma 5.4.3,

$$c(\sigma\tau) = a(\tau)c(\sigma) + d(\sigma)c(\tau) \equiv c(\sigma) + \chi(\sigma)c(\tau) \mod \mathfrak{m}_f C.$$

Through a proof similar to that of Corollary 5.1.6, we may now conclude that the natural restriction maps

$$H^1(G_F, C/\mathfrak{m}_f C) \xrightarrow{\sim} H^1(G_{\mathfrak{p}_1}, C/\mathfrak{m}_f C) \oplus H^1(G_{\mathfrak{p}_2}, C/\mathfrak{m}_f C)$$

induce an isomorphism; here we have implicitly used that $C/\mathfrak{m}_f C$ is a finitely generated module over $\mathbb{T}/\mathfrak{m}_f\mathbb{T} \cong \mathbb{Q}_p$, as shown in Lemme 4 in [BC06]. Any cocycle that is a coboundary at the two places above p of F, must thus have been globally trivial to begin with. It follows that there exists some $\lambda \in C/\mathfrak{m}_f C$ such that $c(\sigma) \equiv \lambda \cdot (1 - \chi(\sigma)) \mod \mathfrak{m}_f C$. In particular, it follows that $0 = c(\gamma) \equiv 2\lambda \mod \mathfrak{m}_f C$, and as such, it follows that $\lambda \equiv 0 \mod \mathfrak{m}_f C$ and hence $C/\mathfrak{m}_f C = 0$. By Nakayama's Lemma, it follows from this that $C = 0$ globally, and as such, c must be the zero-cocycle. However, π is irreducible; this is a contradiction and this completes the proof. □

Proposition 5.4.10. *Both* B *and* C *are free* $\mathbb{T}$*-modules of rank 1.*

Proof. Using the same argument as Lemme 4 in [BC06], it follows that both B and C are $\mathbb{T}$-modules of finite type. We claim that it suffices to show that the images of the maps j_B and j_C are 1-dimensional inside $H^1(G_F, \mathbb{Q}_p(\chi))$. Indeed, if this is true, by the injectivity established by Lemma 5.4.6, using that $\mathbb{T}/\mathfrak{m}_f\mathbb{T} \cong \mathbb{Q}_p$, it would follow that the space $\mathrm{Hom}_{\mathbb{T}}(B/\mathfrak{m}_f B, \mathbb{Q}_p)$ is 1-dimensional. In other words, $B/\mathfrak{m}_f B$ is generated by a single element. Using Nakayama's Lemma, the same must then hold for B itself, completing the proof. Of course, the proof for C is analogous. Now, Proposition and Corollary 5.4.9 combine to imply that both b and c will be locally trivial at precisely one of the two places above p. These constraints cut out a 1-dimensional subspace $H^1(G_{\mathfrak{p}_i}, \mathbb{Q}_p(\chi)) \subset H^1(G_F, \mathbb{Q}_p(\chi))$; this proves the proposition. □

Corollary 5.4.11. *There exists a basis of $\mathbb{K}^2$ such that the image of π takes values in $\mathbb{T}^2$ and is upper triangular* $\bmod \mathfrak{m}_f$. *The $\mathbb{T}$-module spanned by these basis vectors is G_F-stable.*

Proof. By Proposition 5.4.10 above, we can find an element $b_0 \in B$ generating the $\mathbb{T}$-module B. Now consider the basis $\{b_0 e_1, e_2\}$, in which π looks like

$$\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma)b_0^{-1} \\ c(\sigma)b_0 & d(\sigma) \end{pmatrix}.$$

Since $B = \mathbb{T} \cdot b_0$, it follows that $b(\sigma)b_0^{-1} \in \mathbb{T}$ for all $\sigma \in G_F$. By Lemma 5.4.4, it further follows that $c(\sigma)b_0 \in \mathfrak{m}_f$ for all $\sigma \in G_F$. This means that π takes values in $\mathbb{T}^2$, and as such, it stabilises the lattice $M = \langle b_0 e_1, e_2 \rangle$. □

We now rescale our original choice of basis vectors as in the corollary above, to avoid having to continue to take b_0 with us in all our future calculations.

Proposition 5.4.12. *The representation π in the basis above is, up to a scalar unit multiple of one of the basis vectors, a lift of ρ_η.*

Proof. From Lemma 5.4.3 and the corollary above, we know that

$$a \equiv \mathbb{1} \mod \mathfrak{m}_f, \quad d \equiv \chi \mod \mathfrak{m}_f \quad \text{and} \quad c \equiv 0 \mod \mathfrak{m}_f,$$

so it suffices to show that $b(\sigma) \equiv \lambda \cdot \eta \mod \mathfrak{m}_f$ for some $\lambda \in \mathbb{Q}_p^\times$. Recall that η is characterised up to such a scalar λ by being a generator for the 1-dimensional subspace of $H^1(G_F, \mathbb{Q}_p(\chi))$ of cocycles that vanish on the decomposition group $G_{\mathfrak{p}_2} \subset G_F$. This means that it suffices to show that $b(\sigma) \in \mathfrak{m}_f$ for all $\sigma \in G_{\mathfrak{p}_2}$ to complete the proof. However, we already assume that $b \mod \mathfrak{m}_f$ is a coboundary when restricted to $G_{\mathfrak{p}_2}$, and similarly to before, evaluating at γ then yields that $b \mod \mathfrak{m}_f$ must vanish on all of $G_{\mathfrak{p}_2}$. As a result, it must be a scalar multiple of η. Since $b \mod \mathfrak{m}_f$ cannot be trivial when restricted to $G_{\mathfrak{p}_1}$, as a result of Corollary 5.4.9, it follows that $b \mod \mathfrak{m}_f$ is even a non-zero scalar multiple of η. As such, we may scale the basis by a further unit to ensure equality, completing the proof. □

Finally, to conclude that π in any basis that satisfies the conclusion from Proposition 5.4.12 is actually a *deformation* of ρ_η when it comes to the specific nearly ordinary deformation problem at hand, it remains to identify free direct summands of rank 1 inside $\mathbb{T}^2$ on which suitable restrictions of π act scalar. We are given the existence of such lines in $\mathbb{K}^2$,

and to obtain the necessary lines in $\mathbb{T}^2$, we follow the general reasoning in the proof of Proposition 2.3.1 in [Poz19].

Theorem 5.4.13. *Consider π from Theorem 5.4.1 in any basis satisfying the conclusion from Proposition 5.4.12. Then π defines a nearly ordinary deformation of ρ_η.*

Proof. It suffices to exhibit for $i \in \{1,2\}$ a free direct summand L_i of rank 1 inside $\mathbb{T}^2$ which is stable under the restriction $\pi|_{G_{\mathfrak{p}_i}}$ and which lifts e_i. We demonstrate how to obtain L_1; the construction of L_2 is analogous. Recall that we can find matrices satisfying

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} \epsilon_1(\sigma) & * \\ 0 & \delta_1(\sigma) \end{pmatrix},$$

with $x, z \in \mathbb{K}^\times$, yielding the equalities

$$b(\sigma) = \frac{x}{z}\big(\epsilon_1(\sigma) - a(\sigma)\big) \quad \text{and} \quad c(\sigma) = \frac{z}{x}\big(\epsilon_1(\sigma) - d(\sigma)\big).$$

After this change of basis, the stable line for the image of π will be generated by

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} e_1 = \begin{pmatrix} x \\ z \end{pmatrix}.$$

If $\epsilon_1 \equiv \chi \mod \mathfrak{m}_f$, we would find using identical reasoning as in the proof of Lemma 5.4 that $b \mod \mathfrak{m}_f$ must be a coboundary on $G_{\mathfrak{p}_1}$, contradicting that c is already a coboundary there in view of Corollary 5.4.9. As such, it follows that $\epsilon_1 \equiv 1 \mod \mathfrak{m}_f$ and again choosing some $\tau \in G_{\mathfrak{p}_1} \setminus G_L$, we find that

$$\frac{z_1}{x_1} = c(\tau)\big(\epsilon_1(\tau) - d(\tau)\big)^{-1} \in \mathfrak{m}_f.$$

where we used that c takes values in $\mathfrak{m}_f$. We thus set

$$L_1 = \left\langle \begin{pmatrix} 1 \\ z/x \end{pmatrix} \right\rangle.$$

Indeed, this line is fixed by π and as $z/x \in \mathfrak{m}_f$, the line L_1 reduces to $\langle e_1 \rangle$. This completes the proof. □

5.5 A modularity theorem

The goal of this section will be to prove an isomorphism $R^{\mathrm{no}}_{\rho_\eta} \cong \mathbb{T}$. We have already constructed the map; indeed, Theorem 5.4.13 claims that there exists a nearly ordinary deformation π of ρ_η to $\mathbb{T}$ satisfying various properties. By the universal property of $R^{\mathrm{no}}_{\rho_\eta}$, this induces a map

$$\mathcal{T} : R^{\mathrm{no}}_{\rho_\eta} \to \mathbb{T}$$

that induces this deformation from ρ^{univ}.

Lemma 5.5.1. *The map $\mathcal{T} : R^{\mathrm{no}}_{\rho_\eta} \to \mathbb{T}$ is surjective.*

Proof. Let $\Lambda = \mathbb{Q}_p[\![X, Y, Z]\!]$ be as defined in Section 2.2 and 3.1 in [BDS20]. Both $R^{\mathrm{no}}_{\rho_\eta}$ and $\mathbb{T}$ carry a natural Λ-algebra structure and the map $\mathcal{T}$ defined above is generally Λ-linear. Since $\mathbb{T}$ is generated over Λ by the operators $T_\mathfrak{l}$, $\langle \mathfrak{l} \rangle$ and U_x for $x \in \mathcal{O}_F \otimes \mathbb{Z}_p$, it suffices to show that these are contained in the image of $\mathcal{T}$. We use the defining relation that $\pi = \mathcal{T} \circ \rho^{\mathrm{univ}}$ to show for $\mathfrak{l} \nmid p$ that

$$\mathcal{T}\big(\mathrm{Tr}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\mathfrak{l}))\big) = \mathrm{Tr}\big(\mathcal{T}(\rho^{\mathrm{univ}}(\mathrm{Frob}_\mathfrak{l}))\big) = \mathrm{Tr}(\pi(\mathrm{Frob}_\mathfrak{l})) = T_\mathfrak{l}.$$

Similarly,

$$\mathcal{T}\big(\det(\rho^{\mathrm{univ}}(\mathrm{Frob}_\mathfrak{l}))\big) = \det(\pi(\mathrm{Frob}_\mathfrak{l})) = \langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l}).$$

It now suffices to consider the operators U_x for $x \in F \otimes \mathbb{Z}_p \cong F_{\mathfrak{p}_1} \times F_{\mathfrak{p}_2}$. Use the stable lines for ρ^{univ} and π to construct bases. If we then let Δ denote the bottom right entry of ρ^{univ}, we then obtain for $x \in F^\times_{\mathfrak{p}_1}$ that $\mathcal{T}\big(\Delta(x)\big) = \delta_1(x) = U_x$. The top-left entry yields the same result for $x \in F^\times_{\mathfrak{p}_2}$, completing the proof. □

To show that the map $\mathcal{T} : R^{\mathrm{no}}_{\rho_\eta} \to \mathbb{T}$ must in fact be an isomorphism, we use some general results from commutative algebra. Namely, it turns out that we have now gathered enough data to proceed by commutative algebraic considerations.

Lemma 5.5.2. *Let k be a field and $(A, \mathfrak{m}_A)$ and $(B, \mathfrak{m}_B)$ be local k-algebras. Suppose that $\dim_k(\mathfrak{m}_A/\mathfrak{m}_A^2) = \dim(B) < \infty$ and that there is a surjective map of k-algebras $A \to B$. Then A and B are both regular local rings with the same finite Krull dimension.*

Proof. Write $\dim_k(\mathfrak{m}_A/\mathfrak{m}_A^2) = \dim(B) = d$. Using the surjective map $A \to B$, it follows that $\dim(A) \geq \dim(B) = d$. By Krull's Principal Ideal

Theorem, see the Stacks Project [00KD], it also holds that $\dim(A) \leq \dim_k(\mathfrak{m}_A/\mathfrak{m}_A^2) = d$. It follows that $\dim(A) = d$ and as such, A is regular. Similarly, the existence of the surjection implies that $\dim_k(\mathfrak{m}_B/\mathfrak{m}_B^2) \leq \dim_k(\mathfrak{m}_A/\mathfrak{m}_A^2) = d$. However, again by Krull's Principal Ideal Theorem, we know that also $\dim_k(\mathfrak{m}_B/\mathfrak{m}_B^2) \geq \dim(B) = d$. We conclude that also $\dim_k(\mathfrak{m}_B/\mathfrak{m}_B^2) = d$ and so, B must also be regular and of the same dimension as A. □

Proposition 5.5.3. *Let k be a field and let $(A, \mathfrak{m}_A)$ and $(B, \mathfrak{m}_B)$ be Noetherian regular local k-algebras with the same finite Krull dimension. Then every surjective map $f : A \to B$ must be an isomorphism.*

Proof. Because f is a map of local rings, it follows that $f(\mathfrak{m}_A) \subset \mathfrak{m}_B$ and as such, $f(\mathfrak{m}_A^n) \subset \mathfrak{m}_B^n$ for any integer $n \geq 1$. This means that for any integer $n \geq 1$, the morphism f descends to a map

$$f_n : A/\mathfrak{m}_A^n \to B/\mathfrak{m}_B^n.$$

We will show that each f_n is an isomorphism. Assuming this, it would follow that f itself must be an isomorphism. Indeed, if $f(a) = 0$ for some $a \in A$, then also $f_n(a) = 0$ for all $n \geq 1$ and as such, $a \in \mathfrak{m}_A^n$ for all $n \geq 1$. But by Krull's Intersection Theorem, see the Stacks Project [00IP], we may then conclude that $a = 0$, completing the proof.

It remains to show that each f_n is an isomorphism. We prove this with induction, starting with the observation that the map $A \to B/\mathfrak{m}_B \cong k$ is a surjective map to a field, so its kernel must be a maximal ideal of A. Since A is a local ring, it follows that this maximal ideal must be $\mathfrak{m}_A$ and as such, $f_1 : A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ must be an isomorphism.

Now suppose that for some $n \geq 1$, we have shown that f_n is an isomorphism. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{m}_A^n/\mathfrak{m}_A^{n+1} & \longrightarrow & A/\mathfrak{m}_A^{n+1} & \longrightarrow & A/\mathfrak{m}_A^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \\ 0 & \longrightarrow & \mathfrak{m}_B^n/\mathfrak{m}_B^{n+1} & \longrightarrow & B/\mathfrak{m}_B^{n+1} & \longrightarrow & B/\mathfrak{m}_B^n & \longrightarrow & 0 \end{array}$$

If we can show that the map $\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1} \to \mathfrak{m}_B^n/\mathfrak{m}_B^{n+1}$ is always an isomorphism of k-vector spaces, then by the five lemma we would conclude our induction step.

To this end, we let $b_1, \ldots, b_d \in \mathfrak{m}_B$ be a k-basis of the tangent space $\mathfrak{m}_B/\mathfrak{m}_B^2$. Because f is surjective, we can find $a_1, \ldots, a_d \in A$ such that $f(a_i) = b_i$ for all $1 \leq i \leq d$. Because f_1 was an isomorphism, we

know that even $a_1, \ldots, a_d \in \mathfrak{m}_A$. In fact, we claim that these elements form a basis for the tangent space $\mathfrak{m}_A/\mathfrak{m}_A^2$. Indeed, they are linearly independent over k, for if they were not, we would find non-zero $\lambda_i \in k$ such that

$$\sum_{i=1}^{d} \lambda_i a_i \in \mathfrak{m}_A^2 \overset{f(\cdot)}{\Longrightarrow} \sum_{i=1}^{d} \lambda_i b_i \in f(\mathfrak{m}_A^2) \subset \mathfrak{m}_B^2.$$

However, this contradicts the linear independence of the b_i. By the regularity assumption and the fact that A and B have the same dimension, their tangent spaces must also have the same dimension. This shows that the map $\mathfrak{m}_A/\mathfrak{m}_A^2 \to \mathfrak{m}_B/\mathfrak{m}_B^2$ induced by f is an isomorphism.

To finish the proof, we appeal to Lemma 10.106.1 in the Stacks Project [00NO], which implies that k-bases for $\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1}$ and $\mathfrak{m}_B^n/\mathfrak{m}_B^{n+1}$ are given by

$$\left\{ \prod_{i=1}^{d} a_i^{n_i} \;\middle|\; n_i \geq 0,\ \sum_{i=1}^{d} n_i = n \right\} \quad \text{and} \quad \left\{ \prod_{i=1}^{d} b_i^{m_i} \;\middle|\; m_i \geq 0,\ \sum_{i=1}^{d} m_i = n \right\}$$

respectively. Now we remark that

$$f\left(\prod_{i=1}^{d} a_i^{n_i} \right) = \prod_{i=1}^{d} b_i^{n_i}$$

to conclude that f takes one basis to another, thus inducing an isomorphism of k-vector spaces. This concludes the proof. □

Theorem 5.0.1. *The map $\mathcal{T} : R^{\mathrm{no}}_{\rho_\eta} \to \mathbb{T}$ is an isomorphism.*

Proof. Corollary 5.3.11 shows that $\dim(t^{\mathrm{no}}_{\rho_\eta}) = 3$ and from Proposition A.5.5, it follows that $\mathbb{T}$ is equidimensional of dimension 3. By Lemma 5.5.1, the map $\mathcal{T}$ is surjective. Now Lemma 5.5.2 implies that both $R^{\mathrm{no}}_{\rho_\eta}$ and $\mathbb{T}$ are regular of the same Krull dimension; namely 3. Because they are also Noetherian, Proposition 5.5.3 implies that the surjective map $\mathcal{T}$ must in fact be an isomorphism, completing the proof. □

CHAPTER 6

The p-adic analytic proof

The aim of this final chapter is to carry out **Step 3** of the proof of Theorem B as outlined in Section 2.4 by following in rough lines the following steps. First, using the results from Chapter 4, we rewrite the defining formula for the cross ratio of CM-values of the Θ-function into a more convenient form. Next, we will consider one particular infinitesimal deformation of the rigidified Galois representation ρ_η defined in Section 5.2 and supported by the main result from Chapter 5, we compute the morphism from the Hecke algebra that corresponds to it. From this, we determine the Fourier coefficients of the infinitesimal cuspidal family of p-adic modular forms centered around $E_{1,\chi}^{(p)}$ that corresponds to it. Finally, we take its diagonal restriction, take its derivative with respect to the weight parameter and apply the ordinary projection operator. We argue that the first Fourier coefficient of the result of this computation must vanish, and comparing its explicit description to 0 then will yield Theorem B. This approach mimics the strategies used in [DPV21, DPV23]. For notational convenience, thoughout this chapter, we will for $\nu \in F$ denote $\nu' := \sigma(\nu) \in F$; its Galois conjugate.

6.1 Rewriting the Θ-series

Recall that our main object of interest was defined as

$$\Theta(D_1, D_2) := \prod_{[c_1],[c_2]} \frac{\Theta\big([c_1]\cdot\tau_1, [c_1]\cdot\tau_1'; [c_2]\cdot\tau_2\big)}{\Theta\big([c_1]\cdot\tau_1, [c_1]\cdot\tau_1'; [c_2]\cdot\tau_2'\big)}$$

where by $[c_i]\cdot\tau_i$ for $[c_i] \in \mathrm{Pic}(K_i)$ we mean the fixed point in $\mathcal{H}_p$ for the embedding $[c_i]\cdot\alpha_i$. We remark here that the point $[c_i]\cdot\tau_i$ is only well defined up to multiplication by $R_q^\times$, but this does not change the value of the Θ-functions we are computing, since

$$\frac{\Theta(\tau_1, \tau_1'; \tau_2)}{\Theta(\tau_1, \tau_1'; \tau_2')} = \prod_{b \in R_q[1/p]_1^\times} [\tau_1, \tau_1', b\tau_2, b\tau_2'],$$

where we defined the cross-ratio as

$$[\tau_1, \tau_1', b\tau_2, b\tau_2'] = \frac{(\tau_1 - b\tau_2)(\tau_1' - b\tau_2')}{(\tau_1 - b\tau_2')(\tau_1' - b\tau_2)}.$$

Let $\overline{\alpha_1}$ denote the embedding α_1 precomposed with the non-trivial automorphism of K_i. Recall Section 4.4, in which we associated to every pair of embeddings $\mathcal{O}_i \to R_q$ for $i \in \{1,2\}$ an F-quadratic form refining the

quaternion norm on B_q. If $\det_F$ denotes that form for the pair (α_1, α_2), let $\det'_F$ denote that form for the pair $(\overline{\alpha_1}, \alpha_2)$. These two forms relate to each other through the following lemma.

Lemma 6.1.1. *The functions* $\det_F$ *and* $\det'_F$ *are* $\mathrm{Gal}(F/\mathbb{Q})$*-conjugates.*

Proof. This is immediate from Lemma 4.4.4. Indeed, there it was shown that the bilinear form associated with $\det_F$ was given by

$$B_q \times B_q \to F : (\gamma_1, \gamma_2) \mapsto \frac{\mathrm{tr}(\gamma_1\overline{\gamma_2})}{2} + \frac{\mathrm{tr}(A\gamma_1 B\overline{\gamma_2})}{2\sqrt{D}},$$

where $A = \alpha_1(\sqrt{D_1})$ and $B = \alpha_2(\sqrt{D_2})$. The effect of changing to $\overline{\alpha_1}$ is to replace A by $-A$, which clearly yields the Galois conjugate bilinear form in the formula above. □

Lemma 6.1.2. *For any* $b \in B_q$*, we have*

$$[\tau_1, \tau'_1, b\tau_2, b\tau'_2] = -\frac{\det_F(b)}{\det'_F(b)}.$$

Proof. Recall from Theorem 4.4.9 that

$$\det_F(b) = \mathrm{Nm}(b)\frac{(\tau_1 - b\tau_2)(\tau'_1 - b\tau'_2)}{(\tau_1 - \tau'_1)(b\tau_2 - b\tau'_2)}.$$

Similarly, using Lemma 6.1.1 and the final claim of Proposition 4.4.8, to obtain the value of $\det'_F(b)$ we swap τ_1 and τ'_1 to find

$$\det'_F(b) = \mathrm{Nm}(b)\frac{(\tau'_1 - b\tau_2)(\tau_1 - b\tau'_2)}{(\tau'_1 - \tau_1)(b\tau_2 - b\tau'_2)},$$

Since the denominators agree up to a sign, the result follows from dividing these two expressions. □

The following lemma will be used implicitly and without mention throughout the remainder of this section.

Lemma 6.1.3. *The maximal order* R_q *is stable under its involution.*

Proof. Let $b \in R_q$ be arbitrary. Then $\mathbb{Z}[b] \subset R_q$ must be a finitely generated $\mathbb{Z}$-module since R_q is. But $\mathbb{Z}[b]$ is a subring of a quadratic number field, and it is well known that such rings are finitely generated if and only if b is integral over $\mathbb{Z}$. In particular, its minimal polynomial in $\mathbb{Z}[X]$ must be monic. This minimal polynomial is given by $X^2 - \mathrm{tr}(b)X + \mathrm{Nm}(b) = 0$. It follows that in particular, $\mathrm{tr}(b)$ must be an integer and since $1 \in R_q$, it follows that also $\overline{b} = \mathrm{tr}(b) - b \in R_q$. □

We are now ready for the main result of this section.

Proposition 6.1.4. *The following equality holds true:*

$$\frac{2}{w_1 w_2}\log_p \Theta(D_1, D_2) = \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{2n}}} \log_p\left(\frac{\nu}{\nu'}\right)\cdot \rho(\nu\mathfrak{q}_1^{-1}\mathcal{D}_F).$$

Proof. We apply Lemma 6.1.2 to the expression defining $\Theta(D_1, D_2)$, ignoring the sign by pairing each quaternion with its negative. We obtain

$$\Theta(D_1, D_2) = \prod_{[c_1],[c_2]} \prod_{b\in R_q[1/p]_1^\times} \frac{\det_F[c_1, c_2](b)}{\det'_F[c_1, c_2](b)},$$

where the first product is taken over all $[c_i] \in \mathrm{Pic}(K_i)$ for $i \in \{1, 2\}$. Now let $b \in R_q[1/p]_1^\times$. In other words, $\mathrm{Nm}(b) = 1$ and there exists some *minimal* $k \geq 0$ such that $B := p^k b \in R_q$. This association induces a bijection

$$R_q[1/p]_1^\times \to \bigsqcup_{k=0}^{\infty} \left\{B \in R_q \mid p \nmid B,\ \mathrm{Nm}(B) = p^{2k}\right\}.$$

We define for any $n \geq 0$ the set

$$R_q(n) := \left\{B \in R_q \mid \ \mathrm{Nm}(B) = p^{2n}\right\}.$$

Now we observe the association $B \mapsto p^{n-k}B$ induces a bijection

$$\bigsqcup_{k=0}^{n} \left\{B \in R_q \mid p \nmid B,\ \mathrm{Nm}(B) = p^{2k}\right\} \xrightarrow{\sim} R_q(n).$$

By $\mathbb{Z}$-linearity, we find that

$$\frac{\det_F[c_1, c_2](p^{n-k}b)}{\det'_F[c_1, c_2](p^{n-k}b)} = \frac{\det_F[c_1, c_2](b)}{\det'_F[c_1, c_2](b)}.$$

As such, we may use the above bijections to write

$$\Theta(D_1, D_2) = \lim_{n\to\infty} \prod_{[c_1],[c_2]} \prod_{b\in R_q(n)} \frac{\det_F[c_1, c_2](b)}{\det'_F[c_1, c_2](b)}.$$

We now change the way in which we view these finite products over which we take the limit. Instead of ranging over all $b \in R_q(n)$ and recording its

associated $\det_F[c_1, c_2]$-value, we will range over each possible $\det_F[c_1, c_2]$-value and record how often it is reached by some $b \in R_q(n)$. Recalling that $b \in R_q(n)$ means that $\mathrm{Tr}(\det[c_1, c_2]_F(b)) = \mathrm{Nm}(b) = p^{2n}$ and that the values of $\det_F[c_1, c_2]$ are always totally positive, we may rewrite the above to

$$\Theta(D_1, D_2) = \lim_{n\to\infty} \prod_{\substack{\nu \gg 0, \\ \mathrm{tr}(\nu)=p^{2n}}} \left(\frac{\nu}{\nu'}\right)^{\#\{(b,[c_1],[c_2]) \mid \det_F[c_1,c_2](b)=\nu\}},$$

where $(b, [c_1], [c_2]) \in R_q(n) \times \mathrm{Pic}(K_1) \times \mathrm{Pic}(K_2)$. Now we invoke Theorem 4.0.2, using that $\#\left(\mathcal{O}_1^\times \mathcal{O}_2^\times\right) = w_1 w_2/2$, to find that

$$\#\{(b, [c_1], [c_2]) \mid \det_F[c_1, c_2](b) = \nu\} = \frac{w_1 w_2}{2} \rho(\nu \mathfrak{q}_1^{-1} \mathcal{D}_F),$$

where $\mathfrak{q}_1$ is the reflex prime induced by the two embeddings α_1 and α_2 and ρ counts the number of integral ideals of L with given norm in F. Applying the p-adic logarithm now yields the result. □

We continue this section by examining the closely associated quantity $\Theta_p(D_1, D_2)$. Recall that $\pi \in R_q$ denoted a quaternion with $\mathrm{Nm}(\pi) = p$. Then we have the following lemma.

Lemma 6.1.5. *Right multiplication by π induces a bijection between*

$$R_q[1/p]_1^\times := \left\{b \in R_q[1/p]^\times \mid \mathrm{Nm}(b) = 1\right\}$$

and the set

$$R_q[1/p]_p^\times := \left\{b \in R_q[1/p]^\times \mid \mathrm{Nm}(b) = p\right\}.$$

Proof. Is it clear that this map is well-defined and injective. For surjectivity, we remark that if $b \in R_q[1/p]^\times$ satisfies $\mathrm{Nm}(b) = p$, then

$$(b\overline{\pi}/p) \cdot \pi = b(\overline{\pi}\pi)/p = b,$$

with $b\overline{\pi}/p \in R_q[1/p]_1^\times$, completing the proof. □

Proposition 6.1.6. *The following equality holds true:*

$$\log_p \Theta_p(D_1, D_2) = \frac{w_1 w_2}{2} \lim_{n\to\infty} \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{2n+1}}} \log_p\left(\frac{\nu}{\nu'}\right) \cdot \rho(\nu \mathfrak{q}_1^{-1} \mathcal{D}_F),$$

Proof. Using Lemma 6.1.5 above, we rewrite

$$\begin{aligned}\frac{\Theta(\tau_1,\tau_1';\pi\tau_2)}{\Theta(\tau_1,\tau_1';\pi\tau_2')} &= \prod_{b\in R_q[1/p]_1^\times} \frac{\big(\tau_1-b(\pi\tau_2)\big)\big(\tau_1'-b(\pi\tau_2')\big)}{\big(\tau_1-b(\pi\tau_2')\big)\big(\tau_1'-b(\pi\tau_2)\big)}\\ &= \prod_{b\in R_q[1/p]_1^\times} \frac{\big(\tau_1-(b\pi)\tau_2\big)\big(\tau_1'-(b\pi)\tau_2'\big)}{\big(\tau_1-(b\pi)\tau_2'\big)\big(\tau_1'-(b\pi)\tau_2\big)}\\ &= \prod_{b\in R_q[1/p]_p^\times} \frac{(\tau_1-b\tau_2)(\tau_1'-b\tau_2')}{(\tau_1-b\tau_2')(\tau_1'-b\tau_2)}.\end{aligned}$$

One may now repeat the proof of Proposition 6.1.4 above verbatim to arrive at the desired conclusion. □

We conclude this section by proving that the formula from Theorem B correctly counts the factors of p on both sides of the equation. This is necessary to do separately, as our application of $\log_p$ forces us to forfeit any information regarding the number of factors of p on both sides, by virtue of $\log_p(p)=0$. Therefore, we are forced to count these factors by hand first. We need a small elementary lemma.

Lemma 6.1.7. *Let $\nu\in\mathcal{D}_F^{-1}$ be such that $\mathrm{tr}(\nu)=p^n$ for some positive integer n and suppose further that $v_{\mathfrak{p}_1}(\nu)\neq v_{\mathfrak{p}_2}(\nu)$ or that $v_p(\mathrm{Nm}(\nu))$ is odd. Then $p^n\mid\nu$.*

Proof. Let us write

$$\nu\sqrt{D}=\frac{x+p^n\sqrt{D}}{2},\quad \text{so that}\quad \mathrm{Nm}(\nu\sqrt{D})=\frac{x^2-p^{2n}D}{4}.$$

Write $x=p^k y$ where $p\nmid y$. If $k\geq n$, we are done. If not, we find that

$$\nu\sqrt{D}=p^k\frac{y+p^{n-k}\sqrt{D}}{2}\quad\text{and}\quad \mathrm{Nm}(\nu\sqrt{D})=p^{2k}\frac{y^2-p^{2n-2k}D}{4}.$$

If $v_{\mathfrak{p}_1}(\nu)\neq v_{\mathfrak{p}_2}(\nu)$, then the fraction $(y+p^{n-k}\sqrt{D})/2$ must still contain a factor of $\mathfrak{p}_i$ for some $i\in\{1,2\}$. As such, its norm must still be divisible by p. If $v_p(\mathrm{Nm}(\nu))$ is odd, the same conclusion follows. But this means that $p\mid y$; this is a contradiction. □

Proposition 6.1.8. *It holds that*

$$\frac{\pm 2}{w_1w_2}v_p\left(\frac{\Theta(D_1,D_2)}{\Theta_p(D_1,D_2)}\right)=\sum_{\substack{x^2<D\\ x^2\equiv D \bmod 4N}}\delta(x)v_p\left(F\left(\frac{D-x^2}{4N}\right)\right).$$

Proof. The proof of Theorem 6.1.4 showed that, before applying $\log_p$,

$$\Theta(D_1, D_2)^{\frac{\pm 2}{w_1 w_2}} = \lim_{n\to\infty} \prod_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{2n}}} \left(\frac{\nu}{\nu'}\right)^{\rho(\nu\mathfrak{q}_1^{-1}\mathcal{D}_F)}$$

and similarly for $\Theta_p(D_1, D_2)$ as a result of Proposition 6.1.6. We claim that the $\mathfrak{p}_1$-adic valuation of each term in the limit is constant. Indeed, only terms with $v_{\mathfrak{p}_1}(\nu) \neq v_{\mathfrak{p}_1}(\nu') = v_{\mathfrak{p}_2}(\nu)$ can contribute to the $\mathfrak{p}_1$-adic valuation of this expression. By Lemma 6.1.7, this means that only those ν lifted from trace 1 can contribute. This contribution is independent of n because $\rho(p^{2n}\nu\mathfrak{q}_1^{-1}\mathcal{D}_F) = \rho(\nu\mathfrak{q}_1^{-1}\mathcal{D}_F)$. We then conclude that

$$\begin{aligned}\frac{\pm 2}{w_1 w_2} v_{\mathfrak{p}_1}\left(\Theta(D_1, D_2)\right) &= \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=1}} \rho(\nu\mathfrak{q}_1^{-1}\mathcal{D}_F)\big(v_{\mathfrak{p}_1}(\nu) - v_{\mathfrak{p}_1}(\nu')\big) \\ &= \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{p}_1\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=1}} \rho(\nu\mathfrak{q}_1^{-1}\mathcal{D}_F) v_{\mathfrak{p}_1}(\nu) - \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{p}_1\mathfrak{q}_2)^+ \\ \mathrm{tr}(\nu)=1}} \rho(\nu\mathfrak{q}_2^{-1}\mathcal{D}_F) v_{\mathfrak{p}_1}(\nu).\end{aligned}$$

Note that for all contributing terms, we must have that $v_{\mathfrak{p}_1}(\nu)$ is even; indeed, otherwise $\mathfrak{p}_1$ is a special prime of $\nu\mathfrak{q}_1^{-1}\mathcal{D}_F$ and as such, its value under ρ would vanish.

On the other hand, we remark that either $v_{\mathfrak{p}_1}(\nu) = 0$ or $v_{\mathfrak{p}_2}(\nu) = 0$ for any $\nu \in \mathcal{D}_F^{-1}$ of trace 1. As such, it follows that $\rho(p^{2n+1}\nu\mathfrak{q}_1^{-1}\mathcal{D}_F) = 0$ for any $\nu \in \mathcal{D}_F^{-1}$ of trace 1; indeed, at least one of the $\mathfrak{p}_i$ for $i \in \{1, 2\}$ must be a special prime. Following the argument above, we conclude that $v_{\mathfrak{p}_1}(\Theta_p(D_1, D_2)) = 0$. For the $\mathfrak{p}_2$-adic valuation, an analogous argument applies.

By definition of the F-function, its value is only a power of p if the prime p divides the quantity $\mathrm{Nm}(\nu\sqrt{D})/N = (D - x^2)/4N$ an odd number of times. In other words, the corresponding element $\nu \in \mathcal{D}_F^{-1}$ of trace 1 must contain an even number of factors of one of the $\mathfrak{p}_i$ for $i \in \{1, 2\}$. These are the same $\nu \in \mathcal{D}_F^{-1}$ of trace 1 that we found earlier to contribute to the valuation of $\Theta(D_1, D_2)$. The agreement between the exponent in the definition of the F-value and the function ρ has been shown before in the proof of Theorem 3.2.5; the alternating sum matches up all terms and equality has been established. □

6.2 Extracting a_ν from $\tilde{\rho}$

In this section we will compute the p-adic modular form that is associated with a particular nearly ordinary deformation as considered in Chapter 5, of which we have proved its modularity in Theorem 5.0.1. We record its existence in the following lemma.

Lemma 6.2.1. *There exists a deformation $\widetilde{\rho} : G_F \to \mathbb{Q}_p[\epsilon]$ of the form*

$$\widetilde{\rho} = \left(1 + \epsilon \begin{pmatrix} \phi_p & b \\ 0 & -\phi_p \end{pmatrix}\right) \begin{pmatrix} 1 & \chi\eta \\ 0 & \chi \end{pmatrix},$$

where $\phi_p \in \mathrm{Hom}(G_F, \mathbb{Q}_p)$ denotes the p-adic cyclotomic character from in Proposition 5.1.5 and where $b : G_F \to \mathbb{Q}_p$ satisfies $b|_{G_{\mathfrak{p}_2}} = 0$.

Proof. First note that the vanishing of the lower-left entry forces both diagonal entries to be elements from $\mathrm{Hom}(G_F, \mathbb{Q}_p) = \langle \phi_p \rangle$ as a result of Lemma 5.3.3. We may choose them freely, as the proof of Proposition 5.3.5 shows that the map

$$H^1(G_F, W_1) \to H^1(G_F, \mathbb{Q}_p \oplus \mathbb{Q}_p)$$

is surjective. Finally, one verifies that we may always adjust the top-right entry by an element from $H^1(G_F, \mathbb{Q}_p(\chi))$. Since its restriction to $G_{\mathfrak{p}_2}$ is always in $H^1(G_{\mathfrak{p}_2}, \mathbb{Q}_p(\chi))$ as η vanishes there as a result of Lemma 5.2.1, by the isomorphism from Corollary 5.1.6 we can in particular make this restriction vanish. This completes the proof. □

By construction, the lines $\langle e_1 \rangle$ and $\langle e_2 \rangle$ are now fixed by $G_{\mathfrak{p}_1}$ and $G_{\mathfrak{p}_2}$ respectively under the action of $\widetilde{\rho}$. It follows that the quotient characters δ_i from Theorem 5.4.1 for this deformation are given by

$$\delta_1 = \chi - \chi\phi_p\epsilon \quad \text{and} \quad \delta_2 = 1 + \phi_p\epsilon.$$

Since $\det(\tilde{\rho})$ is constant, after identifying $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times \cong \mathcal{O}_{F_{\mathfrak{p}_1}}^\times \times \mathcal{O}_{F_{\mathfrak{p}_2}}^\times \cong I_{\mathfrak{p}_1} \times I_{\mathfrak{p}_2}$, it is a general fact that the weight character of the modular form associated with this Galois representation is given by $\delta_1 \times \delta_2$. In particular, the weight character for the diagonal restriction is the map

$$(\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \xrightarrow{\Delta} (\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \cong \mathcal{O}_{F_{\mathfrak{p}_1}}^\times \times \mathcal{O}_{F_{\mathfrak{p}_2}}^\times \to \mathbb{Q}_p[\epsilon],$$

where Δ here denotes the diagonal embedding. Using that χ is trivial on the inertia subgroups $I_{\mathfrak{p}_i} \subset G_{\mathfrak{p}_i}$ for $i \in \{1, 2\}$, as the extension L/F is unramified, we trace through the maps to find

$$x \mapsto (x, x) \mapsto \delta_1(x)\delta_2(x) = \big(1 - \log_p(x)\epsilon\big)\big(1 + \log_p(x)\epsilon\big) = 1.$$

In particular, the diagonal restriction is of *constant* weight. This shows that the above deformation describes an infinitesimal family of modular forms in the so-called *anti-parallel* weight direction. We will use this in the proof of Proposition 6.3.1 to allow us to conclude that the derivative with respect to the weight parameter of our family is in fact a modular object, even though the specialisation of this family does *not* vanish.

By its universal property, the deformation $\widetilde{\rho}$ comes from some map $R^{\mathrm{no}}_{\rho_\eta} \to \mathbb{Q}_p[\epsilon]$. By Theorem 5.0.1, the isomorphism yields a unique associated map $\varphi : \mathbb{T} \to \mathbb{Q}_p[\epsilon]$. The majority of this section will be dedicated to computing this morphism.

Recall that $\mathbb{T}$ is generated by the operators $T_\mathfrak{l}$ and $\langle \mathfrak{l} \rangle$ for all primes $\mathfrak{l}$ of F coprime to p, and the operators U_{π_1} and U_{π_2} where $\pi_1, \pi_2 \in \mathbb{A}_F^\times$ are local uniformisers at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively.

Theorem 5.4.1 dictates how we should deduce the images of the various Hecke operators from the associated representation. Indeed, it shows that $\varphi(T_\mathfrak{l})$ should correspond to the trace of $\widetilde{\rho}(\mathrm{Frob}_\mathfrak{l})$, whereas $\langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l})$ should correspond to its determinant. Finally, the images of the operators U_{π_i} are deduced from the values $\delta_i(\pi_i)$ for $i \in \{1, 2\}$. We will now determine these quantities in this order.

Lemma 6.2.2. *For any $\tau \in G_F$ it holds that*

$$\mathrm{Tr}(\tilde{\rho}(\tau)) = 1 + \chi(\tau) + (1 - \chi(\tau))\phi_p(\tau)\epsilon.$$

Proof. By writing out the definition of $\widetilde{\rho}(\tau)$, we find that

$$\mathrm{Tr}(\tilde{\rho}(\tau)) = 1 + \phi_p(\tau)\epsilon + \chi(\tau)(1 - \phi_p(\tau)\epsilon).$$

Rewriting then yields the result. □

Lemma 6.2.3. *Let $\varphi : \mathbb{T} \to \mathbb{Q}_p[\epsilon]$ be the morphism induced by the deformation $\tilde{\rho}$ and let $\mathfrak{l} \nmid p$ be a prime ideal of F. Then*

$$\varphi(T_\mathfrak{l}) = \begin{cases} 2 & \text{if } \chi(\mathfrak{l}) = 1; \\ 2\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon & \text{if } \chi(\mathfrak{l}) = -1. \end{cases}$$

Proof. We split cases, using that $\varphi(T_\mathfrak{l}) = \mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_\mathfrak{l}))$ as long as $\mathfrak{l} \nmid p$. If $\chi(\mathrm{Frob}_\mathfrak{l}) = 1$, then Lemma 6.2.2 yields the claim.

If $\chi(\mathrm{Frob}_\mathfrak{l}) = -1$, however, Lemma 6.2.2 then yields that

$$\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_\mathfrak{l})) = 2\phi_p(\mathrm{Frob}_\mathfrak{l})\epsilon.$$

We complete the proof by remarking that by definition, $\mathrm{Frob}_\mathfrak{l}$ will raise the topological generator ζ_{p^∞} of the extension $F(\zeta_{p^\infty})/F$ to the power $\mathrm{Nm}(\mathfrak{l})$, so the result follows by tracing through the definition of ϕ_p. □

We continue with the images of the diamond operators.

Lemma 6.2.4. *For any prime ideal $\mathfrak{l} \nmid p$ of F, it holds that*

$$\varphi(\langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l})) = \chi(\mathrm{Frob}_{\mathfrak{l}}).$$

Proof. Recall that the image of $\mathrm{Frob}_{\mathfrak{l}}$ has determinant $\varphi(\langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l}))$. In our case, the determinant is kept constant, so this is $\chi(\mathrm{Frob}_{\mathfrak{l}})$. □

Finally, we determine the images of the operators U_{π_i} for π_i a uniformiser of $\mathcal{O}_{F_{\mathfrak{p}_i}}$ for $i \in \{1, 2\}$.

Lemma 6.2.5. *Let π_i for $i \in \{1, 2\}$ be a uniformiser of $\mathcal{O}_{F_{\mathfrak{p}_i}}$. Then*

$$\varphi(U_{\pi_1}) = -1 + \log_p(\pi_1)\epsilon \quad \textit{and} \quad \varphi(U_{\pi_2}) = 1 + \log_p(\pi_2)\epsilon.$$

Proof. Since the images of the operators U_{π_i} for $i \in \{1, 2\}$ agree with the images of the elements π_i under the map δ_i, suppressing the local reciprocity map, this follows from combining the earlier found expressions

$$\delta_1 = \chi - \chi\phi_p\epsilon \quad \text{and} \quad \delta_2 = 1 + \phi_p\epsilon$$

with the definition of the map ϕ_p, with the p-adic logarithm extended to all of $\mathbb{Q}_p^\times$ through the Iwasawa branch, as $\chi(\pi_i) = -1$ because the primes $\mathfrak{p}_i$ for $i \in \{1, 2\}$ are inert in the extension L/F. □

Proposition 6.2.6. *Let $\varphi : \mathbb{T} \to \mathbb{Q}_p[\epsilon]$ be the morphism induced by the deformation $\tilde{\rho}$, let $\mathfrak{l} \nmid p$ be a prime ideal of F and $n \geq 0$ an integer. Then*

$$\varphi(T_{\mathfrak{l}^n}) = \begin{cases} n+1 & \textit{if } \chi(\mathfrak{l}) = 1; \\ (n+1)\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon & \textit{if } \chi(\mathfrak{l}) = -1 \textit{ and } n \textit{ is odd;} \\ 1 & \textit{if } \chi(\mathfrak{l}) = -1 \textit{ and } n \textit{ is even.} \end{cases}$$

Further, for π_i for $i \in \{1, 2\}$ a uniformiser of $\mathcal{O}_{F_{\mathfrak{p}_i}}$, it holds that

$$\varphi(U_{\pi_1^n}) = (-1)^n(1 - n\log_p(\pi_1)\epsilon);$$
$$\varphi(U_{\pi_2^n}) = 1 + n\log_p(\pi_2)\epsilon.$$

Proof. We remind the reader of the essential recursion relation

$$T_{\mathfrak{l}^{n+1}} = T_{\mathfrak{l}^n}T_{\mathfrak{l}} - \langle \mathfrak{l} \rangle \mathrm{Nm}(\mathfrak{l})T_{\mathfrak{l}^{n-1}}$$

for $\mathfrak{l} \nmid p$, whereas $U_{\pi^n} = U_\pi^n$ for the adèles above p.

- If $\chi(\mathrm{Frob}_\mathfrak{l}) = 1$, then $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_\mathfrak{l})) = 2$ by Lemma 6.2.3. Further using Lemma 6.2.4, we obtain the recursion

$$T(n+1) = 2T(n) - T(n-1) \quad \text{with} \quad T(0) = 1, \quad T(1) = 2.$$

  This is easily solved and yields $T(n) = n + 1$ for all $n \geq 0$.

- If on the other hand $\chi(\mathfrak{l}) = -1$, then $\mathrm{Tr}(\tilde{\rho}(\mathrm{Frob}_\mathfrak{l})) = 2\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon$ by Lemma 6.2.3. Again by Lemma 6.2.4, we obtain the recursion

$$L(n+1) = 2\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon \cdot L(n) + L(n-1)$$

  with $L(0) = 1$ and $L(1) = 2\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon$. One deduces

$$L(2n) = 1 \quad \text{and} \quad L(2n-1) = 2n\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon \quad \text{for all } n \geq 1.$$

- In the final case, we raise the expressions from Lemma 6.2.5 to the appropriate exponent to find

$$\varphi(U_{\pi_1^n}) = (-1 + \log_p(\pi_1)\epsilon)^n = (-1)^n(1 - n\log_p(\pi_1)\epsilon).$$

Similarly, we obtain $\varphi(U_{\pi_2^n})$, completing the proof. □

Remark 6.2.7. By considering the quotient of two uniformisers at a given place, it is not difficult to convince oneself that for any idèles α_1, α_2 supported only at $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively, it holds that

$$\varphi(U_{\alpha_1}) = (-1)^{v_{\mathfrak{p}_1}(\alpha_1)}(1 - \log_p(\alpha_1)\epsilon) \quad \text{and} \quad \varphi(U_{\alpha_2}) = 1 + \log_p(\alpha_2)\epsilon.$$

This extends the formulae for π_1^n and π_2^n above.

Corollary 6.2.8. *Let $\mathfrak{l} \nmid p$ be a prime ideal of F and let $n \in \mathbb{N}$. Recalling $\rho(I) := \#\{J \subset \mathcal{O}_L \mid \mathrm{Nm}_F^L(J) = I\}$ for $I \subset \mathcal{O}_F$, we have that*

$$\varphi(T_{\mathfrak{l}^n}) = \rho(\mathfrak{l}^n) + \frac{1}{2}(n+1)\big(1 - \chi(\mathfrak{l}^n)\big)\log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon.$$

Proof. Indeed, we have seen before in Chapter 3 that

$$\rho(\mathfrak{l}^n) = \begin{cases} n+1 & \text{if } \chi(\mathfrak{l}) = 1; \\ 0 & \text{if } \chi(\mathfrak{l}) = -1 \text{ and } n \text{ is odd}; \\ 1 & \text{if } \chi(\mathfrak{l}) = -1 \text{ and } n \text{ is even}. \end{cases}$$

These quantities match the integral parts of $\varphi(T_{\mathfrak{l}^n})$ from Proposition 6.2.6 above. As for the infinitesimal part, we remark that we get no contribution if and only if $\chi(\mathfrak{l}^n) = 1$, and as such, the expression $1 - \chi(\mathfrak{l}^n)$ is twice the indicator function for the case $\chi(\mathfrak{l}) = -1$ and n is odd. Combining these two parts yields the corollary. □

The appearance of the ρ-function in the integral part should not be surprising, as this simply corresponds to the Eisenstein series we are deforming; compare with Proposition A.2.9 and Lemma A.2.10.

Because we have well-defined operators $T_{\mathfrak{l}^n}$ for any integral ideal $\mathfrak{l} \nmid p$, we may by multiplying these expressions together extend this to a well-defined notion of an operator T_J for any integral ideal $J \subset \mathcal{O}_F$ coprime to p. Using this notion, we arrive at the following Corollary from the above computations.

Corollary 6.2.9. *Let $J \subset \mathcal{O}_F$ be any ideal coprime to p. Then*

$$\varphi(T_J) = \rho(J) + \frac{1}{2} \sum_{\mathfrak{l}^n \| J} \Big((n+1)\big(1 - \chi(\mathfrak{l}^n)\big)\rho(J/\mathfrak{l}^n) \Big) \log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon.$$

Proof. By definition

$$T_J = \prod_{\mathfrak{l}^n \| J} T_{\mathfrak{l}^n}.$$

One may write out, keeping in mind that $\epsilon^2 = 0$, that

$$\begin{aligned} \varphi(T_J) &= \prod_{\mathfrak{l}^n \| J} \Big(\rho(\mathfrak{l}^n) + \frac{1}{2}(n+1)\big(1 - \chi(\mathfrak{l}^n)\big) \log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon \Big) \\ &= \prod_{\mathfrak{l}^n \| J} \rho(\mathfrak{l}^n) + \frac{1}{2} \sum_{\mathfrak{l}^n \| J} (n+1)\big(1 - \chi(\mathfrak{l}^n)\big) \log_p(\mathrm{Nm}(\mathfrak{l}))\epsilon \prod_{\mathfrak{t}^m \| J/\mathfrak{l}^n} \rho(\mathfrak{t}^m). \end{aligned}$$

The corollary now follows from the multiplicativity of ρ. □

For any integral ideal J coprime to p, we define $\mathcal{F}(J) \in \mathbb{N}$ by

$$\log_p(\mathcal{F}(J)) := \frac{1}{2} \sum_{\mathfrak{l}^n \| J} \Big((n+1)\big(1 - \chi(\mathfrak{l}^n)\big)\rho(J/\mathfrak{l}^n) \Big) \log_p(\mathrm{Nm}(\mathfrak{l})).$$

This quantity has the following crucial property. As in Chapter 3, we will refer to those prime powers $\mathfrak{l}^n \| J$ with $\chi(\mathfrak{l}^n) = -1$, as the *special primes* of the ideal J. Note that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ can also be special primes, if we relax the condition that J be coprime to p, as we will soon do.

Proposition 6.2.10. *Let $J \subset \mathcal{O}_F$ be any integral ideal coprime to p. Then*

$$\varphi(T_J) = \rho(J) + \log_p(\mathcal{F}(J))\epsilon.$$

In addition, $\mathcal{F}(J)$ is a power of a single rational prime. If J is a primitive ideal, then it even holds that $\mathcal{F}(J) = F(\mathrm{Nm}(J))^2$, where F is as in our main results, Theorem A and Theorem B.

Proof. The first claim follows from Corollary 6.2.9 and the definition of $\mathcal{F}(J)$. For the second, we note that the only summands in the expression defining $\mathcal{F}(J)$ that could possibly contribute are those for the special primes of J. If there are no such primes, then $\mathcal{F}(J) = 1$. If there is more than special prime, one of which being $\mathfrak{l}^n$, then its contribution will also vanish. Namely, in that case it holds that $\rho(J/\mathfrak{l}^n) = 0$, as the existence of a special prime obstructs an ideal from being a norm from the field L. We conclude that $\mathcal{F}(J) = 1$ in that case too. Only the case in which there is a unique special prime remains, proving that $\mathcal{F}(J)$ is a power of the underlying rational prime ℓ, as claimed. Finally, our primitivity assumption forces all primes dividing J to split in $F/\mathbb{Q}$ and to all lie above different rational primes, and as such, the prime factorisation of J in F matches the prime factorisation of its norm in $\mathbb{Q}$. From the proof of Proposition 3.2.5 in Chapter 3, it follows that the exact exponent of ℓ occuring in the expression of Giampietro's F can also be written as $(n+1)\rho(J/\mathfrak{l}^n)/2$, proving the claimed equality. □

By Theorem 5.0.1, the morphism $\varphi : \mathbb{T} \to \mathbb{Q}_p[\epsilon]$ computed above will correspond to a cuspidal family of p-adic Hilbert modular forms, which we will denote by $E_{1,\chi}^{(p)}(\epsilon)$. In the next section, we will be interested in the first derivative with respect to ϵ of the diagonal restriction of this family with respect to the ideal $t_\lambda = \mathcal{D}_F^{-1}\mathfrak{q}_1$. To simplify notation, we will thus set $a_\nu := a_p(\mathcal{D}_F\mathfrak{q}_1^{-1}\nu)$, as these will be the relevant coefficients to compute the desired diagonal restriction, see in Appendix A.2.

For notational convenience, for any ideal $J \subset \mathcal{O}_F$, we let $\widetilde{J}$ denote its *p-deprivation*; in other words, $\widetilde{J}$ denotes the ideal J with all factors of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ removed. Finally, we introduce the notation J_ν for the ideal $\nu\mathcal{D}_F\mathfrak{q}_1^{-1}$. We now state the main result of this section.

Theorem 6.2.11. *For any $\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+$, it holds that*

$$a_\nu = (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\rho(\widetilde{J_\nu}) + \log_p(\mathcal{F}(\widetilde{J_\nu}))\epsilon - \rho(\widetilde{J_\nu})\log_p(\nu/\nu')\epsilon\big).$$

Proof. Using the same argument as in Theorem 3.13 in [DPV23], we may use the relations proved by Hida for classical forms also in this setting. By the results of Section 1 in [Hid91] and Proposition A.4.4, for any $\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+$, we must consider the idèle $\alpha = \nu d\varpi_{\mathfrak{q}_1}^{-1}$, where $\varpi_{\mathfrak{q}_1}$ is any idèle that equals 1 everywhere away from $\mathfrak{q}_1$, where it is a uniformiser, and where $d \in \mathbb{A}_F^\times$ is such that it generates the ideal $\mathcal{D}_F$ and is trivial at p. Let $\widetilde{\nu}$ denote the idèle that is equal to ν everywhere away from p, where it is equal to 1. Then $\nu = \widetilde{\nu}\nu_{\mathfrak{p}_1}\nu_{\mathfrak{p}_2}$ and we note that α generates

the ideal J_ν, so that $\widetilde{J_\nu}$ is generated by the idèle $\widetilde{\nu} d\varpi_{\mathfrak{q}_1}^{-1}$. Using Remark 6.2.7, we compute that

$$\begin{aligned}
\varphi(T_\alpha) &= \varphi(T_{\widetilde{\nu} d\varpi_{\mathfrak{q}_1}^{-1}})\varphi(U_{\nu_{\mathfrak{p}_1}})\varphi(U_{\nu_{\mathfrak{p}_2}}) \\
&= \varphi(T_{\widetilde{J_\nu}}) \cdot (-1)^{v_{\mathfrak{p}_1}(\nu_{\mathfrak{p}_1})}(1 - \log_p(\nu_{\mathfrak{p}_1})\epsilon) \cdot (1 + \log_p(\nu_{\mathfrak{p}_2})\epsilon) \\
&= (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\rho(\widetilde{J_\nu}) + \log_p(\mathcal{F}(\widetilde{J}_\nu))\epsilon\big)(1 - \log_p(\nu_{\mathfrak{p}_1})\epsilon)(1 + \log_p(\nu'_{\mathfrak{p}_1})\epsilon) \\
&= (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\rho(\widetilde{J_\nu}) + \log_p(\mathcal{F}(\widetilde{J}_\nu))\epsilon\big)\big(1 - \log_p(\nu_{\mathfrak{p}_1}/\nu'_{\mathfrak{p}_1})\epsilon\big) \\
&= (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\rho(\widetilde{J_\nu}) + \log_p(\mathcal{F}(\widetilde{J}_\nu))\epsilon - \rho(\widetilde{J_\nu})\log_p(\nu/\nu')\epsilon\big);
\end{aligned}$$

this is the statement of the theorem. We used here that $v_{\mathfrak{p}_2}$ can be identified with $v'_{\mathfrak{p}_1}$, since under the isomorphism $\mathcal{O}_F \otimes \mathbb{Z}_p \cong \mathcal{O}_{F_{\mathfrak{p}_1}} \times \mathcal{O}_{F_{\mathfrak{p}_2}}$, the element ν is sent to (ν, ν'). □

6.3 Proof of Theorem B

In Theorem 6.2.11, we computed the relevant Fourier coefficients for the diagonal restriction with respect to the ideal $\mathcal{D}_F^{-1}\mathfrak{q}_1$ of the cuspidal family of p-adic Hilbert modular forms $E_{1,\chi}^{(p)}(\epsilon)$ associated with the morphism $\varphi : \mathbb{T} \to \mathbb{Q}_p[\epsilon]$ induced by the deformation $\widetilde{\rho}$ defined in Lemma 6.2.1. Taking its derivative with respect to the parameter ϵ amounts to considering only the ϵ-part. Let Δ denote the diagonal restriction operator for the ideal $\mathcal{D}_F^{-1}\mathfrak{q}_1$. As $E_{1,\chi}^{(p)}(\epsilon)$ is p-adically a cusp form by Lemma A.3.3, we have

$$\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon) = \sum_{n=1}^{\infty}\Big(\sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=n}} \frac{d}{d\epsilon}a_\nu\Big)\mathbf{q}^n.$$

By Theorem 6.2.11 and the equation above, this yields for any $n \in \mathbb{N}$,

$$a_n\left(\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon)\right) = \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=n}} (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\log_p \mathcal{F}(\widetilde{J_\nu}) - \rho(\widetilde{J_\nu})\log_p(\nu/\nu')\big).$$

Proposition 6.3.1. *The object $\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon)$ is an overconvergent p-adic modular form of weight 2. Its ordinary projection $e^{\mathrm{ord}}\left(\Delta\frac{d}{d\epsilon}E_{1,\chi}^{(p)}(\epsilon)\right)$ is a classical modular form in $\mathcal{S}_2(\Gamma_0(N))$.*

Proof. We have seen before that the weight character for $\Delta E_{1,\chi}^{(p)}(\epsilon)$ is constant, and because for the $\epsilon = 0$-specialisation its weight is $1+1 = 2$,

the result will be of constant weight 2. Its specialisation does not vanish, but by subtracting a constant family, Lemma 2.1 in [DPV21] yields that its derivative is still an overconvergent p-adic modular form of weight 2. By Coleman's Classicality Theorem, which can be found as Theorem 6.1 in [Col96], its ordinary projection is of slope $0 < 1$ and hence classical. Further, it is a cusp form because $E_{1,\chi}^{(p)}$ is a p-adic cusp form by Lemma A.3.3. For the level, since we used the ideal $\mathcal{D}_F\mathfrak{q}_1^{-1}$, the tame level of our diagonal restriction will be q. The level of its ordinary projection is then obtained by multiplying its tame level by p. Combining all of this, we obtain an object in $\mathcal{S}_2(\Gamma_0(N))$, as claimed. □

If we apply the operator e^{ord} from Appendix A.5, we obtain

$$\begin{aligned} a_1\left(e^{\mathrm{ord}}\left(\frac{d}{d\epsilon}\Delta E_{1,\chi}^{(p)}(\epsilon)\right)\right) &= \lim_{n\to\infty} a_{p^{n!}}\left(\frac{d}{d\epsilon}\Delta E_{1,\chi}^{(p)}(\epsilon)\right) \\ &= \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!}}} (-1)^{v_{\mathfrak{p}_1}(\nu)}\big(\log_p \mathcal{F}(\widetilde{J_\nu}) - \rho(\widetilde{J_\nu})\log_p(\nu/\nu')\big). \end{aligned}$$

We analyse the two terms occuring in this expression separately. Define

$$A := \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!}}} (-1)^{v_{\mathfrak{p}_1}(\nu)}\rho(\widetilde{J_\nu})\log_p(\nu/\nu')$$

and

$$B := \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!}}} (-1)^{v_{\mathfrak{p}_1}(\nu)}\log_p(\mathcal{F}(\widetilde{J_\nu})).$$

For the sake of brevity, we extend the definition of v_p to F by setting it equal to $v_{\mathfrak{p}_1} \times v_{\mathfrak{p}_2}$ there; this will save some space in what is to come.

Proposition 6.3.2. *It holds that*

$$A = \frac{2}{w_1 w_2}\log_p\left(\Theta(D_1, D_2)\right) - \frac{2}{w_1 w_2}\log_p\left(\Theta_p(D_1, D_2)\right).$$

Proof. We note that since $\chi(J_\nu) = \chi(\mathcal{D}_F)\chi(\mathfrak{q}_1) = (-1)^2 = 1$, the parities of $v_{\mathfrak{p}_1}(J_\nu)$ and $v_{\mathfrak{p}_2}(J_\nu)$ being different would imply that $\chi(\widetilde{J_\nu}) = -1$, and as such, $\rho(\widetilde{J_\nu}) = 0$ by Corollary A.2.11. Hence we may write

$$A = \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!} \\ v_p(\nu)\equiv(0,0)}} \rho(\widetilde{J_\nu})\log_p(\nu/\nu') - \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!} \\ v_p(\nu)\equiv(1,1)}} \rho(\widetilde{J_\nu})\log_p(\nu/\nu'),$$

both congruences being modulo 2. For the first term, one may observe that $\rho(\widetilde{J_\nu}) = \rho(J_\nu)$. In fact, $\rho(J_\nu) = 0$ unless $v_p(\nu) \equiv (0,0) \mod 2$, and as a result, we may even write the first term as

$$\lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!}}} \rho(J_\nu)\log_p(\nu/\nu') = \frac{2}{w_1 w_2}\log_p\left(\Theta(D_1,D_2)\right),$$

where we appealed to Proposition 6.1.4 and the fact that the limit exists when taken over all $\mathrm{tr}(\nu) = p^{2n}$; as such, the limit taken over $\mathrm{tr}(\nu) = p^{n!}$ exists too and equals the same value, as $n!$ is even for $n \geq 2$. For the second term, one may observe that $p \mid \nu$, and as such, we may make the substitution $\nu \leftrightarrow p\nu$, further using that $\rho(\widetilde{J_\nu}) = \rho(J_{p\nu})$, to obtain

$$\lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!} \\ v_p(\nu)\equiv(1,1)}} \rho(\widetilde{J_\nu})\log_p(\nu/\nu') = \lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=p^{n!-1}}} \rho(J_\nu)\log_p(\nu/\nu'),$$

where we were allowed to omit the bottom subscript for the same reason as before. We conclude by Proposition 6.1.6. □

Proposition 6.3.3. *It holds that*

$$B = \sum_{\mathrm{Nm}(\mathfrak{a})=N} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}a)^+ \\ \mathrm{tr}(\nu)=1}} \delta(\mathfrak{a})\log_p(F(\mathrm{Nm}(J_\nu)/p)).$$

Proof. First note that, by Lemma 6.2.10, it holds that $\mathcal{F}(\widetilde{J_\nu}) = 1$ as soon as $\chi(\widetilde{J_\nu}) = 1$, because this implies that the number of special primes is even, and thus in particular not one. Since $\chi(J_\nu) = 1$, it follows that one of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ must be special to get a non-zero contribution to the sum. Since ν contains the full p-part of J_ν, this implies that $v_p(\mathrm{Nm}(\nu))$ must be odd. By Lemma 6.1.7, it follows that $p^{n!} \mid \nu$ if $\mathrm{tr}(\nu) = p^{n!}$. It follows that all contributing summands to the n-th term in the limit are lifted from those ν of unit trace. In fact, since $\widetilde{J_{p^{n!}\nu}} = \widetilde{J_\nu}$ and $v_{\mathfrak{p}_1}(J_{p^{n!}\nu}) \equiv v_{\mathfrak{p}_1}(J_\nu) \mod 2$ for $n \geq 2$, each summand induced by some ν of unit trace is independent of n. The limit thus equals its first term;

$$B = \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=1 \\ v_p(\mathrm{Nm}(\nu)) \text{ odd}}} (-1)^{v_{\mathfrak{p}_1}(J_\nu)}\log_p(\mathcal{F}(\widetilde{J_\nu})).$$

Note that the ideal $\widetilde{J_\nu}$ is always primitive by Lemma 3.2.1. As it is prime to p by definition, it follows from Proposition 6.2.10 that $\mathcal{F}(\widetilde{J_\nu}) = F(\mathrm{Nm}(\widetilde{J_\nu}))^2$ in all cases. Because the number of factors of p in $\mathrm{Nm}(J_\nu)$ is odd for all the terms contributing to the sum, $\mathrm{Nm}(J_\nu)/p$ will have an even number, as does $\mathrm{Nm}(\widetilde{J_\nu})$. As a result, the F-values of these integers must be the same. We conclude that

$$B = 2 \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=1 \\ v_p(\mathrm{Nm}(\nu)) \text{ odd}}} (-1)^{v_{\mathfrak{p}_1}(J_\nu)} \log_p(F(\mathrm{Nm}(J_\nu)/p)).$$

Note that we may omit any congruence conditions on $v_p(\mathrm{Nm}(\nu))$, as in the case of the number of factors of p dividing $\mathrm{Nm}(J_\nu)$ being even, dividing by p makes p a special prime of $\mathrm{Nm}(J_\nu)/p$. As such, its F-value must be a power of p, of which the p-adic logarithm vanishes. Since contributing ν must contain a factor of $\mathfrak{p}_1$ or $\mathfrak{p}_1'$, we have proved that

$$B = 2 \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{p}_1\mathfrak{q}_1)^+ \\ \text{and } \nu \in (\mathcal{D}_F^{-1}\mathfrak{p}_2\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=1}} (-1)^{v_{\mathfrak{p}_1}(J_\nu)} \log_p(F(\mathrm{Nm}(J_\nu)/p)).$$

Adding in those $\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_2)^+$ is the same as adding a term for the Galois-conjugate of every $\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+$. For every non-zero term in the sum, we have that $v_{\mathfrak{p}_1}(J_{\nu'}) \not\equiv v_{\mathfrak{p}_1}(J_\nu) \mod 2$ and $\mathrm{Nm}(J_{\nu'}) = \mathrm{Nm}(J_\nu)$. In other words, the summands for ν and ν' would agree up to a sign. Finally, $\delta(\mathfrak{a})$ measures this sign together with $(-1)^{v_{\mathfrak{p}_1}(\nu)}$. □

To complete the proof, we will only need one more result about the ordinary projection that we have now computed. Namely, we will show that its first Fourier coefficient must always vanish.

Lemma 6.3.4. *The form* $e^{\mathrm{ord}}\left(\Delta \frac{d}{d\epsilon} E_{1,\chi}^{(p)}(\epsilon)\right)$ *is a* U_p*-eigenvector with eigenvalue* -1.

Proof. By definition of the U_p operator, we should check that $a_{pm} = -a_m$ for all $m \in \mathbb{N}$. The coefficient for a_m can be split up into the two terms

$$\lim_{n\to\infty} \sum_{\substack{\nu \in (\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=m\cdot p^{n!}}} (-1)^{v_{\mathfrak{p}_1}(\nu)} \rho(\widetilde{J_\nu}) \log_p(\nu/\nu')$$

and

$$\lim_{n\to\infty} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}\mathfrak{q}_1)^+ \\ \mathrm{tr}(\nu)=m\cdot p^{n!}}} (-1)^{v_{\mathfrak{p}_1}(\nu)} \log_p(\mathcal{F}(\widetilde{J_\nu})).$$

For the former, one may trace through the proof of Proposition 6.3.2 to find that the limit is only dependent on the parity of the numbers $v_p(m) + n!$ for $n \geq 2$, the difference being a sign when we move from m to pm, caused by the factor $(-1)^{v_{\mathfrak{p}_1}(\nu)}$. For the latter, the proof of Proposition 6.3.3 reduces the contributions to those ν of trace $m/p^{v_p(m)}$, once again the only difference being the sign $(-1)^{v_{\mathfrak{p}_1}(\nu)}$ dependent on the parity of $v_p(m)$. We leave the details to the reader. □

Corollary 6.3.5. *For $N \in \{6, 10, 22\}$, it holds that*

$$e^{\mathrm{ord}}\left(\Delta \frac{d}{d\epsilon} E_{1,\chi}^{(p)}(\epsilon)\right) = 0.$$

Proof. For $N \in \{6, 10\}$, one checks that $\mathcal{S}_2(\Gamma_0(N)) = 0$ so the result follows from Proposition 6.3.1. It remains to analyse the case that $N = 22$, when the space $\mathcal{S}_2(\Gamma_0(22))$ is 2-dimensional and spanned by two oldforms. Recall that we assumed $q \in \{2, 3, 5, 7, 13\}$, so we need only check the case that $p = 11$ and $q = 2$. It is easy to check that the operator U_{11} acts trivially on $\mathcal{S}_2(\Gamma_0(22))$, so by Lemma 6.3.4, the result follows. □

Proof. (of Theorem B) We conclude from Corollary 6.3.5 that $A+B = 0$. Using Proposition 6.3.2 and Proposition 6.3.3, this shows that

$$\frac{2}{w_1 w_2} \log_p\left(\frac{\Theta(D_1, D_2)}{\Theta_p(D_1, D_2)}\right) = \sum_{\mathrm{Nm}(a)=N} \sum_{\substack{\nu\in(\mathcal{D}_F^{-1}a)^+ \\ \mathrm{tr}(\nu)=1}} \delta(a) \log_p(F(\mathrm{Nm}(J_\nu)/p)).$$

Finally, for $\nu = (x + \sqrt{D})/2\sqrt{D}$, it holds that

$$\mathrm{Nm}(J_\nu)/p = \frac{D - x^2}{4N}.$$

This proves Theorem B up to an element from $\pm p^{\mathbb{Z}}$, as this is the kernel of $\log_p$. We conclude by Proposition 6.1.8 that the factors of p on both sides match up too, which reduces our ambiguity to a mere sign. This is permitted by Theorem B and concludes the proof. □

APPENDIX A

Various types of modular forms

This appendix assumes the reader to be familiar with the theory of classical *modular forms*. A comprehensive introduction to classical modular forms can be found in [DS05]. We will start by briefly recalling their automorphic perspective and we will subsequently generalise this treatment to more general types of modular forms in the sections that follow. First, we change the ground field from $\mathbb{Q}$ to a real quadratic field F and then we describe an adèlic approach to Hilbert modular forms. Finally, we will leave the archimedean setting and consider p-adic modular forms instead, briefly introducing Hida families, as we will need them for our methods in Chapter 6.

A.1 Adelic modular forms

In order to motivate some of the later sections, we take a moment to illustrate the way in which the classical modular forms can be reinterpreted in an adèlic language. We closely follow the treatment and notation from [Dei12]. Throughout this section, let

$$\mathrm{SO}(2) := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R},\ a^2 + b^2 = 1 \right\};$$

this is the stabiliser of $i \in \mathbb{C}$ under the action of $\mathrm{SL}_2(\mathbb{R})$. Further, for notational convenience, for any commutative ring R we denote

$$G_R := \mathrm{GL}_2(R) \quad \text{and} \quad G^1_R := \mathrm{SL}_2(R).$$

One may choose a *Haar measure* on the group $G^1_{\mathbb{R}}$ and if $\Gamma \subset G^1_{\mathbb{R}}$ is a discrete subgroup, we obtain a natural Haar measure on the quotient space $\Gamma \setminus G^1_{\mathbb{R}}$. We use this to define the space

$$L^2(\Gamma \setminus G^1_{\mathbb{R}}) := \left\{ f : \Gamma \setminus G^1_{\mathbb{R}} \to \mathbb{C} \text{ such that } \int_{\Gamma \setminus G^1_{\mathbb{R}}} |f(x)|^2 dx < \infty \right\}.$$

The map

$$\mathbb{C} \to M_2(\mathbb{Q}) : a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

restricts to an isomorphism of groups

$$\{z \in \mathbb{C} : |z| = 1\} =: \mathbb{T} \xrightarrow{\sim} \mathrm{SO}(2).$$

Therefore, for any $k \in \mathbb{Z}$ we can define the character

$$\epsilon_k : \mathrm{SO}(2) \to \mathbb{T} \quad \text{induced by the map} \quad \mathbb{T} \xrightarrow{(-)^k} \mathbb{T}.$$

We may now define the subspace

$$L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_k] := \{f \in L^2(\Gamma \setminus G^1_{\mathbb{R}}) \mid f(xu) = \epsilon_k(u)f(x),\ \forall u \in \mathrm{SO}(2)\}.$$

Let $|_k$ denote the usual slash operator, and for brevity, we will denote

$$j_\alpha(z) := cz + d \quad \text{for any} \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Let $\mathcal{S}_k(\Gamma)$ denote the space of weight k cuspforms for Γ. The following is Proposition 3.3.4 in [Dei12].

Proposition A.1.1. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and $k \in \mathbb{Z}$. Given $f \in \mathcal{S}_k(\Gamma)$, define the map*

$$\phi_f : G^1_{\mathbb{R}} \to \mathbb{C} \quad \textit{through} \quad \phi_f(\alpha) = (f|_k\alpha)(i).$$

This association induces an (isometric) injection

$$\mathcal{S}_k(\Gamma) \hookrightarrow L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_{-k}].$$

Proof. We content ourselves for now with verifying that indeed it holds that $\phi_f \in L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_{-k}]$. To this end, we compute for $\gamma \in \Gamma$ that

$$\phi_f(\gamma\alpha) = (f|_k\gamma\alpha)(i) = ((f|_k\gamma)|_k\alpha)(i) = (f|_k\alpha)(i) = \phi_f(\alpha),$$

using the Γ-invariance of f. This shows that $\phi_f : \Gamma \setminus G^1_{\mathbb{R}} \to \mathbb{C}$ is well-defined. Square-integrability follows from the vanishing of f at all cusps, so its remains to verify that ϕ_f lands in the required ϵ_{-k}-eigenspace. Indeed, we compute for $u \in \mathrm{SO}(2)$ that

$$\phi_f(xu) = ((f|_kx)|_ku)(i) = j_u(i)^{-k}(f|_kx)(ui) = \epsilon_{-k}(u)\phi_f(x),$$

where we used that $j_u(i)^{-k} = \epsilon_{-k}(u)$ by definition and that $ui = i$. This completes the proof sketch. □

The proposition above allows us to view classical modular forms as elements of the space $L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_{-k}]$; in particular is shows that the *weight* is perhaps more naturally viewed as a character, as opposed to a positive integer as the classical theory seems to suggest. In fact, we have a natural eigenspace decomposition

$$L^2(\Gamma \setminus G^1_{\mathbb{R}}) = \bigoplus_{k \in \mathbb{Z}} L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_k].$$

It is in this sense that studying the space $L^2(\Gamma \setminus G^1_{\mathbb{R}})$ is akin to studying all classical modular forms of all possible weights at once. We can refine the above result if we let $\mathbb{A}$ denote the $\mathbb{Q}$-adèles, $\mathbb{A}^{\text{fin}}$ the finite $\mathbb{Q}$-adèles, and further set

$$Z_{\mathbb{R}} := \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{R}^\times \right\}.$$

Let $\widehat{\mathbb{Z}}$ denote the ring of profinite integers. The following statement is now purely group-theoretic, see Proposition 7.2.4 in [Dei12].

Lemma A.1.2. *Let Γ be a congruence subgroup and let K_Γ be the closure of Γ in $G_{\widehat{\mathbb{Z}}}$. Then the map*

$$\Gamma \setminus G^1_{\mathbb{R}} \xrightarrow{\sim} G_{\mathbb{Q}} \setminus G^1_{\mathbb{A}} \, / K_\Gamma$$

given by $\Gamma x \mapsto G_{\mathbb{Q}}(1,x)K_\Gamma$ is a $G^1_{\mathbb{R}}$-equivariant isomorphism, where we wrote $(1,x) \in G_{\mathbb{A}^{\text{fin}}} \times G_{\mathbb{R}} = G_{\mathbb{A}}$.

This has the following consequence, which allows us to view classical modular forms as adèlic objects, using Proposition A.1.1. This is Theorem 7.2.5 in [Dei12].

Theorem A.1.3. *Let Γ be a congruence subgroup and let K_Γ be the closure of Γ in $G_{\widehat{\mathbb{Z}}}$. Then restriction induces a (unitary) $G^1_{\mathbb{R}}$-equivariant isomorphism*

$$L^2(G_{\mathbb{Q}} Z_{\mathbb{R}} \setminus G_{\mathbb{A}} \, / K_\Gamma) \xrightarrow{\sim} L^2(\Gamma \setminus G^1_{\mathbb{R}}).$$

The elements from $L^2(G_{\mathbb{Q}} Z_{\mathbb{R}} \setminus G_{\mathbb{A}})$ are called *automorphic forms*. Through the arrows

$$\mathcal{S}_k(\Gamma) \hookrightarrow L^2(\Gamma \setminus G^1_{\mathbb{R}})[\epsilon_{-k}] \hookrightarrow L^2(\Gamma \setminus G^1_{\mathbb{R}}) \xrightarrow{\sim} L^2(G_{\mathbb{Q}} Z_{\mathbb{R}} \setminus G_{\mathbb{A}} \, / K_\Gamma),$$

we have now realised classical modular forms as special cases of the more general concept of an automorphic form. The class of automorphic forms is more broad however, for it also includes objects like Maaß-waveforms, as explained in Section 2.8 in [Dei12]. We opt to not dive deeper into this theory here, however, thus concluding this section.

A.2 Classical Hilbert modular forms

Throughout this section, we fix an embedding $F \subset \mathbb{R}$, and for $\nu \in F$, we let $\nu' = \sigma(\nu) \in F$ denote its Galois conjugate. It is our aim to sketch a theory of modular forms, but now with the base field F instead of $\mathbb{Q}$. We follow the notation from Chapter 2 in [DDP11].

Definition A.2.1. For $z = (z_1, z_2) \in \mathbb{C} \times \mathbb{C}$ and $\mathbf{k} = (k_1, k_2) \in \mathbb{Z}^2$, define for $a, b \in F$ the quantity

$$(az + b)^{\mathbf{k}} := (az_1 + b)^{k_1}(a'z_2 + b')^{k_2}.$$

We will also write

$$\mathrm{GL}_2^+(F) := \{A \in \mathrm{GL}_2(F) \mid \det(A) \gg 0\}.$$

Definition A.2.2. Let $\gamma \in \mathrm{GL}_2^+(F)$ and $z = (z_1, z_2) \in \mathcal{H} \times \mathcal{H}$. We set

$$\gamma \cdot z := \left(\frac{az_1 + b}{cz_1 + d}, \frac{a'z_2 + b'}{c'z_2 + d'}\right) \quad \text{if} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

A fundamental domain for this group action, roughly speaking, is the union of $h_F := \#\mathrm{Pic}(F)$ different open subsets of the product $\mathcal{H} \times \mathcal{H}$. This explains in part why the class numbers h_F and, more precisely, $h_F^+ := \#\mathrm{Pic}(F)^+$, will appear centrally in the theory.

Definition A.2.3. The action of $\gamma \in \mathrm{GL}_2^+(F)$ defined above induces the *weight* $\mathbf{k} = (k_1, k_2) \in \mathbb{Z}^2$ action on the space of functions $\mathcal{H} \times \mathcal{H} \to \mathbb{C}$.

$$f|_{\mathbf{k}}\gamma(z) := \det(\gamma)^{k_1/2}\det(\gamma')^{k_2/2}(cz + d)^{-\mathbf{k}} f(\gamma z).$$

Definition A.2.4. For each class $\lambda \in \mathrm{Pic}(F)^+$, we fix a representative ideal $t_\lambda \subset \mathcal{O}_F$ with $[t_\lambda] = \lambda$. We use it to define the groups Γ_λ as

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(F) : a, d \in \mathcal{O}_F,\ b \in t_\lambda^{-1}\mathcal{D}_F^{-1},\ c \in t_\lambda \mathcal{D}_F,\ ad - bc \in \mathcal{O}_F^\times \right\}.$$

Definition A.2.5. A weight $\mathbf{k} \in \mathbb{Z}^2$ *classical Hilbert modular form* is an h_F^+-tuple of holomorphic functions

$$f_\lambda : \mathcal{H} \times \mathcal{H} \to \mathbb{C},$$

where $\lambda \in \mathrm{Pic}(F)^+$, such that $f_\lambda|_{\mathbf{k}}\gamma = f_\lambda$ for all $\gamma \in \Gamma_\lambda$.

This means that f_λ for any $\lambda \in \mathrm{Pic}(F)^+$ has a Fourier expansion

$$f_\lambda(z_1, z_2) = a_\lambda(0) + \sum_{\nu \in t_\lambda^+} a_\lambda(\nu) e^{2\pi i(z_1\nu + z_2\nu')}.$$

Definition A.2.6. The coefficients $a_\lambda(\nu)$ are called the *unnormalised Fourier coefficients* of f. They may be normalised to eradicate the initial choices of the representative ideals t_λ by setting for each integral ideal $\mathfrak{m} \subset \mathcal{O}_F$,

$$a(\mathfrak{m}, f) := a_\lambda(\nu)\mathrm{Nm}(t_\lambda)^{-(k_1+k_2)/2}\nu^{(k_1-k_2)/2},$$

where $\lambda = -[\mathfrak{m}] \in \mathrm{Pic}(F)^+$ and $\nu \in t_\lambda^+$ is such that $\mathfrak{m}t_\lambda = (\nu)$.

Lemma A.2.7. *The normalised Fourier coefficients $a(\mathfrak{m}, f)$ are well-defined for any $\mathfrak{m} \subset \mathcal{O}_F$.*

Proof. The only choice we make during their construction is that of the element $\nu \in t_\lambda^+$ generating the ideal $\mathfrak{m}t_\lambda$. Let $\epsilon \in \mathcal{O}_F^{\times,+}$ denote a totally positive unit and let $\mu = \epsilon\nu$ be any other such choice. Then we must show that $a_\lambda(\nu) = a_\lambda(\mu)\epsilon^{(k_1-k_2)/2}$. Indeed, we compute that

$$f(z_1, z_2) = f|_{\mathbf{k}} \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} (z_1, z_2) = \epsilon^{k_1/2}(\epsilon')^{k_2/2} f(\epsilon z_1, \epsilon' z_2).$$

Now note that $\epsilon^{k_1/2}(\epsilon')^{k_2/2} = \epsilon^{(k_1-k_2)/2}$, as $\epsilon \gg 0$ implies that $\epsilon\epsilon' = \mathrm{Nm}(\epsilon) = 1$. Now comparing the coefficient in front of $e^{2\pi i(z_1\mu + z_2\mu')} = e^{2\pi i(z_1\epsilon\nu + z_2\epsilon'\nu')}$ on both sides yields the claimed equality. □

Remark A.2.8. The observant reader might have noticed the striking absence of any conditions regarding holomorphicity at the cusps in Definition A.2.5. Rather remarkably, such conditions are automatically satisfied for holomorphic functions satisfying the transformation properties given above. This is called *Koecher's principle* and can be found for instance as Theorem 1.20 in [Bru08].

To introduce the most vital example for the purposes of this thesis, we must first define the complex L-function

$$L(\chi, s) := \sum_{\mathfrak{a} \subset \mathcal{O}_F} \chi(\mathfrak{a})\mathrm{Nm}(\mathfrak{a})^{-s},$$

which converges as soon as $\mathrm{Re}(s) > 1$ and allows a holomorphic continuation to all of $\mathbb{C}$. The following is a special case of the much more general Proposition 2.1 in [DDP11].

Proposition A.2.9. *There exists a parallel weight $\mathbf{k} = \mathbf{1} = (1, 1)$ Hilbert modular form $E_{1,\chi}$ with normalised Fourier coefficients*

$$a_\lambda(0, E_{1,\chi}) = \frac{1 + \chi(\lambda)}{4} L(\chi, 0),$$

and for $\mathfrak{m} \subset \mathcal{O}_F$,

$$a(\mathfrak{m}, E_{1,\chi}) = \sum_{I|\mathfrak{m}} \chi(I).$$

Using the following lemma, we may rewrite these coefficients in a more concrete way.

Lemma A.2.10. *For any ideal $\mathfrak{m} \subset \mathcal{O}_F$, it holds that*

$$\sum_{I|\mathfrak{m}} \chi(I) = \rho(\mathfrak{m}) \geq 0.$$

Proof. Because both χ and ρ are multiplicative, we can rewrite

$$\sum_{I|\mathfrak{m}} \chi(I) = \prod_{\mathfrak{r}^k \| \mathfrak{m}} \sum_{i=0}^{k} \chi(\mathfrak{r}) \quad \text{and} \quad \rho(\mathfrak{m}) = \prod_{\mathfrak{r}^k \| \mathfrak{m}} \rho(\mathfrak{r}^k).$$

We thus complete the proof after showing that for every prime $\mathfrak{r} \subset \mathcal{O}_F$,

$$\sum_{i=0}^{k} \chi(\mathfrak{r}) = \rho(\mathfrak{r}^k) = \begin{cases} k+1 & \text{if } \chi(\mathfrak{r}) = 1; \\ 1 & \text{if } \chi(\mathfrak{r}) = -1 \text{ and } k \text{ is even}; \\ 0 & \text{if } \chi(\mathfrak{r}) = -1 \text{ and } k \text{ is odd}. \end{cases}$$

This is easily verified for the leftmost term, and counting ideals is easy after recalling that $\chi(\mathfrak{r})$ measures the splitting behaviour of $\mathfrak{r}$ in L/F. □

Corollary A.2.11. *Suppose that $\chi(\mathfrak{m}) = -1$. Then*

$$\rho(\mathfrak{m}) = 0, \quad \textit{and as such,} \quad (E_{1,\chi})_{[\mathfrak{m}]} = 0.$$

Proof. It is clear from Proposition A.2.9 that the constant term vanishes in this case, so consider now the higher Fourier coefficients.

Using the same product expansion as in the proof of Lemma A.2.10, it follows that the result must vanish if there exists some prime $\mathfrak{r}$ of $\mathcal{O}_F$ with $\chi(\mathfrak{r}) = -1$ dividing $\mathfrak{m}$ an odd number of times. Again by multiplicativity of χ, this is ensured if $\chi(\mathfrak{m}) = -1$, as we assume.

Alternatively, Proposition 4.1.5 in Chapter 4 shows that the image of the norm map Nm_F^L is contained in the kernel of χ, hence in particular $\mathfrak{m}$ is not a norm. □

Since χ is totally odd, it holds that $\chi(\mathcal{D}_F) = -1$; see also Proposition 4.0.3. Therefore, it follows from the above that

$$(E_{1,\chi})_{[\mathcal{D}_F^{-1}]} = 0.$$

This fact has historically come to be known as *Hecke's sign error*, as after missing a single minus sign in an otherwise impressive calculation, Hecke once mistakenly concluded the incorrect *non-vanishing* of the Hilbert Eisenstein series above. However, as unfortunate as this may have been for Hecke at the time, this fact was later exploited by Gross and Zagier in [GZ84], and lies at the foundation of their analytic proof of Theorem 1.2.1, as described in Section 1.6. To understand that method, we will need to introduce the following concept.

Definition A.2.12. The *diagonal restriction* of a weight $\mathbf{k} = (k_1, k_2) \in \mathbb{Z}^2$ Hilbert modular form $f : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ is defined as the map

$$\Delta f : \mathcal{H} \to \mathbb{C} \quad \text{given by} \quad \Delta f(z) = f(z, z);$$

one checks that this must be a classical modular form of weight $k_1 + k_2$.

From a more algebraic perspective, we may try to describe this operation on the level of q-expansions. To this end, we remark that setting $z_1 = z_2 = z$ in the expression $e^{2\pi i(z_1\nu + z_2\nu')}$ yields $e^{2\pi i z \mathrm{tr}(\nu)} = \mathbf{q}^{\mathrm{tr}(\nu)}$, where $\mathbf{q} = e^{2\pi i z}$ as usual. In other words, the diagonal restriction collects elements $\nu \in F$ of fixed trace and together these constitute the Fourier coefficients of the classical modular form.

Concretely, one chooses some fractional F-ideal $\mathfrak{m}$ with respect to which to compute the diagonal restriction, and one obtains for the Fourier coefficients

$$a_n(\Delta_{\mathfrak{m}} f) = \sum_{\substack{\nu \in \mathfrak{m}^+ \\ \mathrm{tr}(\nu) = n}} a(\nu \mathfrak{m}^{-1}, f).$$

For those primes $\mathfrak{l} \subset \mathcal{O}_F$ that satisfy $[\mathfrak{l}] = [0] \in \mathrm{Pic}(F)^+$, we may write $\mathfrak{l} = (\varpi)$ for some $\varpi \in \mathcal{O}_F^+$. Let $B \subset \Gamma_\lambda$ be a set of representatives with

$$\Gamma_\lambda \begin{pmatrix} 1 & 0 \\ 0 & \varpi \end{pmatrix} \Gamma_\lambda = \bigsqcup_{\gamma \in B} \Gamma_\lambda \gamma.$$

As explained in [MS15], one may then define the Hecke operator $T_{\mathfrak{l}}$ as

$$T_{\mathfrak{l}} f_\lambda := \varpi^{k_1/2-1} (\varpi')^{k_2/2-1} \sum_{\gamma \in B} f|_{\mathbf{k}} \gamma.$$

One can check that this definition is independent of the choice of ϖ. This definition displays strong similarities to its classical counterpart. One may further define diamond operators $\langle \mathfrak{l} \rangle$ to recursively set

$$T_{\mathfrak{l}^n} := T_{\mathfrak{l}^{n-1}} T_{\mathfrak{l}} - \langle \mathfrak{l} \rangle \varpi^{k_1 - 1} (\varpi')^{k_2 - 1} T_{\mathfrak{l}^{n-2}}.$$

However, the failure of the triviality of the narrow class group prevents us from using the above definition to define operators $T_{\mathfrak{l}^n}$ for each prime ideal $\mathfrak{l}$. This suggests that perhaps the theory is more easily set up in an adèlic or local language, as opposed to the global language considered hitherto. Together with the results from Section A.1, this more than justifies the ideas contained in the Section A.4, which, along with the section thereafter, forms the technical heart of this appendix.

A.3 p-stabilisations

We recall the notion of a p-stabilisation for a classical modular form.

Definition A.3.1. Let $f \in \mathcal{S}_k(\Gamma_0(N))$ for some positive integer N and let $p \nmid N$ be a prime number. Define its *Hecke polynomial* as

$$X^2 - a_p(f)X + p^{k-1} =: (X - \alpha)(X - \beta);$$

this is the characteristic polynomial of Frobenius at p for the Galois representation associated with the modular form f. We say that f is *regular* at p whenever $\alpha \neq \beta$.

From now on, we let $p \nmid N$ be such a regular prime and for any $f \in \mathcal{S}(\Gamma_0(N))$ we define

$$f_\alpha(z) := f(z) - \beta f(pz) \quad \text{and} \quad f_\beta(z) := f(z) - \alpha f(pz).$$

It is clear that these are both elements of $\mathcal{S}(\Gamma_0(Np))$ and they are called the two *p-stabilisations* of f. The following lemma explains this.

Lemma A.3.2. *Let $f \in \mathcal{S}(\Gamma_0(N))$ be a normalised eigenform. Then both f_α and f_β are normalised eigenforms of level Np, with U_p-eigenvalues α and β respectively.*

Proof. It is easy to check that both f_α and f_β remain T_ℓ-eigenvectors for each prime $\ell \neq p$ with the same eigenvalue. We thus reduce to analysing the operators T_p on $\mathcal{S}(\Gamma_0(N))$ and U_p on $\mathcal{S}(\Gamma_0(Np))$.

By symmetry, it suffices to show that $U_p f_\alpha = \alpha f_\alpha$. We prove this on the level of **q**-expansions. On the left hand side, the n-th Fourier coefficient is equal to

$$a_{np}(f_\alpha) = a_{np}(f) - \beta a_n(f)$$

whereas on the right hand side, it is equal to

$$\alpha a_n(f) - \alpha\beta a_{n/p}(f).$$

To prove equality, it thus suffices to show that

$$a_{np}(f) = (\alpha + \beta)a_n(f) - \alpha\beta a_{n/p}(f) = a_p(f)a_n(f) - p^{k-1}a_{n/p}.$$

Now use that f is a normalised eigenform and as such, coprime coefficients are multiplicative. Writing $n = p^k m$ with $p \nmid m$, we divide out by $a_m(f)$ to reduce to showing that

$$a_{p^{k+1}} = a_p(f)a_{p^k}(f) - p^{k-1}a_{p^{k-1}};$$

this is trivial for $k = 0$ and for positive k again ensured by the fact that f is a normalised eigenform and the well known recursive definition of the Hecke operators for prime powers. □

A p-stabilised modular form can be viewed as a p-adic modular form, see Section A.5. We mimic Definition A.3.1 and consider various ways to *p-stabilise* the object $E_{1,\chi}$. Let $V_{\mathfrak{p}_1}$ and $V_{\mathfrak{p}_2}$ be the level raising operators, denoted as $|_{\mathfrak{p}_i}$ in Section 2.6 in [DK20]. On the normalised Fourier coefficients of the Hilbert modular form f, these operators act through the rules

$$a_\lambda(0, V_{\mathfrak{p}_i} f) = a_{\lambda\mathfrak{p}_i}(0, f) \quad \text{and} \quad a(\mathfrak{m}, V_{\mathfrak{p}_i} f) = \begin{cases} a(\mathfrak{m}/\mathfrak{p}_i, f) & \text{if } \mathfrak{p}_i \mid \mathfrak{m}; \\ 0 & \text{otherwise.} \end{cases}$$

These operators refine the classical level raising operation $f(z) \mapsto f(pz)$ in the sense that for a Hilbert modular form f, it holds that

$$V_{\mathfrak{p}_1} V_{\mathfrak{p}_2} f(z_1, z_2) = V_{\mathfrak{p}_2} V_{\mathfrak{p}_1} f(z_1, z_2) = f(pz_1, pz_2).$$

We now specialise to the form $E_{1,\chi}$, whose associated Galois representation of G_F is given by $\rho = \mathbb{1} \oplus \chi$. For $i \in \{1, 2\}$ its Hecke polynomial, which is the characteristic polynomial of Frobenius, is then given by

$$X^2 + [\mathbb{1}(\mathfrak{p}_i) + \chi(\mathfrak{p}_i)]X + \mathbb{1}(\mathfrak{p}_i)\chi(\mathfrak{p}_i) = X^2 - 1,$$

as $\chi(\mathfrak{p}_i) = -1$. There are therefore four possible ways for us to *p-stabilise* the modular form $E_{1,\chi}$, given by

$$(1 \pm V_{\mathfrak{p}_1})(1 \pm V_{\mathfrak{p}_2}) E_{1,\chi}.$$

For the purposes of this thesis, we choose the stabilisation

$$E_{1,\chi}^{(p)} := (1 - V_{\mathfrak{p}_1})(1 + V_{\mathfrak{p}_2}) E_{1,\chi}$$

and fix it throughout this thesis. For a discussion explaining this choice conceptually, see the start of Section 5.4. However, we do note here that our choice for opposite signs for this p-stabilisation has the following consequence.

Lemma A.3.3. *The form $E_{1,\chi}^{(p)}$ is a p-adic Hilbert cusp form.*

Proof. It is noted above, and on page 461 of [DDP11] and Equation 10 in [DK20] it is shown, that the constant term of the result of applying level-raising operator at a certain class $\lambda \in \mathrm{Pic}(F)^+$ is the constant term at the class $\lambda\mathfrak{p}_i$. With Proposition 2.1 in [DDP11], or equivalently our Proposition A.2.9, we find that the constant term of $E_{1,\chi}^{(p)}$ at any class λ equals

$$\Big[\big(1+\chi(\lambda)\big)-\big(1-\chi(\lambda)\big)+\big(1-\chi(\lambda)\big)-\big(1+\chi(\lambda)\big)\Big]\frac{L_F(\chi,0)}{4}=0.$$

This shows that $E_{1,\chi}^{(p)}$ vanishes at all the cusps lying over ∞, and therefore it must be a p-adic cusp form. □

The following makes the form $E_{1,\chi}^{(p)}$ a bit more explicit.

Proposition A.3.4. *The normalised Fourier coefficients of the form $E_{1,\chi}^{(p)}$ are given by*

$$a\left(\mathfrak{m}, E_{1,\chi}^{(p)}\right) = (-1)^{v_{\mathfrak{p}_1}(\mathfrak{m})}\rho(\widetilde{\mathfrak{m}}),$$

*where $\widetilde{\mathfrak{m}}$ denotes the p-*depletion *of $\mathfrak{m} \subset \mathcal{O}_F$, obtained from $\mathfrak{m}$ by removing all factors of primes of F above p.*

Proof. By the rules above, we find for any nonzero integral ideal $\mathfrak{m} \subset \mathcal{O}_F$,

$$a(\mathfrak{m}, E_{1,\chi}^{(p)}) = a(\mathfrak{m}, E_{1,\chi}) - a(\mathfrak{m}/\mathfrak{p}_1, E_{1,\chi}) + a(\mathfrak{m}/\mathfrak{p}_2, E_{1,\chi}) - a(\mathfrak{m}/p, E_{1,\chi}),$$

where we adopt the convention $a(\mathfrak{n}, E_{1,\chi}) = 0$ if $\mathfrak{n}$ is a non-integral fractional ideal of F. Lemma A.2.9 and Lemma A.2.10 now combine to yield

$$a(\mathfrak{m}, E_{1,\chi}^{(p)}) = \rho(\mathfrak{m}) - \rho(\mathfrak{m}/\mathfrak{p}_1) + \rho(\mathfrak{m}/\mathfrak{p}_2) - \rho(\mathfrak{m}/p)$$

For the function ρ to be non-zero, the proof of Corollary A.2.11 shows that both the number of factors of both $\mathfrak{p}_i$ for $i \in \{1,2\}$ must be even. Therefore, at most one of these four terms can be non-zero. The sign of this term is determined by the parity of $v_{\mathfrak{p}_1}(\mathfrak{m})$. Finally, an even number of factors of $\mathfrak{p}_i$ for $i \in \{1,2\}$ does not change the outcome of the ρ-function; the result follows. □

Remark A.3.5. Suppose that the ideal $\mathfrak{m}$ is coprime to p, satisfies $\chi(\mathfrak{m}) = -1$ and is stable under the non-trivial automorphism σ of $F/\mathbb{Q}$. We then claim that the diagonal restriction of $E_{1,\chi}^{(p)}$ with respect to the ideal $\mathfrak{m}$ vanishes identically. This would follow if we can show that $a\left(\nu\mathfrak{m}, E_{1,\chi}^{(p)}\right) = -a\left(\nu'\mathfrak{m}, E_{1,\chi}^{(p)}\right)$ for all $\nu \in \mathfrak{m}^+$, for then the contributions of ν and $\nu' \in \sigma(\mathfrak{m}) = \mathfrak{m}$ to the appropriate Fourier coefficient would cancel out. To see this, first note that $\rho(\widetilde{\nu\mathfrak{m}^{-1}}) = \rho(\widetilde{\nu'\mathfrak{m}^{-1}})$ because these ideals are Galois conjugates. Second, the contribution of ν can only be non-zero if $\chi(\widetilde{\nu\mathfrak{m}^{-1}}) = 1$ by the proof of Lemma A.2.11, so the total number of factors of primes of F above p inside ν must be odd. Therefore $(-1)^{v_{\mathfrak{p}_1}(\nu)} = -(-1)^{v_{\mathfrak{p}_2}(\nu)} = -(-1)^{v_{\mathfrak{p}_1}(\nu')}$. We conclude using Proposition A.3.4.

Remark A.3.6. From the remark above, we conclude that the diagonal restriction of $E_{1,\chi}^{(p)}$ with respect to the ideal $\mathcal{D}_F^{-1}$ vanishes. However, it does *not* show that the diagonal restriction of $E_{1,\chi}^{(p)}$ with respect to the ideal $\mathcal{D}_F^{-1}\mathfrak{q}_1$ vanishes, and indeed it generally will not. The importance and subtleties caused by this observation are explained at the start of Section 5.4 and in the proof of Proposition 6.3.1.

A.4 Adelic Hilbert modular forms

We aim to redo most of the previous sections in an adèlic language from the automorphic perspective outlined in Section A.1. This theory was developed in the second half of the 20th century, and later refined by Hida over the scope of many papers, including but not limited to [Hid89b, Hid91, Hid89a]. These works also discuss p-adic modular forms, which will be the focus of the next section. We refer to Hida's work for a comprehensive introduction; here we only recall some definitions and focus on what we will need for our purposes. We shall closely adhere to the notation used in Section 2.1 in Fornea's thesis [For19].

We define the algebraic group

$$G_F := \mathrm{Res}_{F/\mathbb{Q}}\mathrm{GL}_{2,F},$$

where $\mathrm{Res}_{F/\mathbb{Q}}$ denotes the Weil-restriction of scalars. In view of Proposition A.1.1, we set $\mathbf{i} := (i, i) \in \mathcal{H} \times \mathcal{H}$ and let C_∞^+ be the stabiliser of $\mathbf{i}$ under the natural action of the group $G_F(\mathbb{R})^+$, which we recall denotes the subgroup of $G_F(\mathbb{R})$ of all matrices with totally positive determinant.

Further, we let $K \subset G_F(\mathbb{A}_F^{\mathrm{fin}})$ be a compact open subgroup, which will be the *level* of the modular object we will define momentarily. Note the similarities here with the case of $\mathbb{Q}$: the ring of finite adèles $\mathbb{A}_F^{\mathrm{fin}}$ can be written as $F\widehat{\mathcal{O}_F}$. The ring $\widehat{\mathcal{O}_F}$ may be compared to $\widehat{\mathbb{Z}}$ and the closure $K_\Gamma \subset \mathrm{SL}_2(\widehat{\mathbb{Z}})$ of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ describing the level of a classical modular form will indeed be a compact open subgroup. This is the group that appears in Theorem A.1.3.

Let $\mathbf{k} = (k_1, k_2) \in \mathbb{Z}^2$ and $\mathbf{w} = (w_1, w_2) \in \mathbb{Z}^2$ be such that $\mathbf{k} - 2\mathbf{w} = m\mathbf{1}$ for some integer m, where $\mathbf{1} = (1, 1)$.

Definition A.4.1. A *Hilbert modular form* of weight $(\mathbf{k}, \mathbf{w})$ is a function $f : G_F(\mathbb{A}_F) \to \mathbb{C}$ satisfying the following properties:

- For any $\alpha \in G_F(\mathbb{Q})$ and $u \in K \cdot C_\infty^+$, it holds that $f(\alpha x u) = f(x) j_{\mathbf{k},\mathbf{w}}(u_\infty, \mathbf{i})^{-1}$, where $u_\infty \in G_F(\mathbb{R})$. Here we wrote for
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ that } j_{\mathbf{k},\mathbf{w}}(A, z) := \det(A)^{-\mathbf{w}}(cz + d)^{\mathbf{k}},$$
adopting the notation $\det(A)^{-\mathbf{w}}$ and $(cz + d)^{\mathbf{k}}$ from Section A.2.
- For every $x \in G_F(\mathbb{A}_F^{\mathrm{fin}})$, define the function $f_x : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ given by $f_x(z) := f(xu_\infty) j_{\mathbf{k},\mathbf{w}}(u_\infty, \mathbf{i})$, where $u_\infty \in G_F(\mathbb{R})^+$ is such that $u_\infty \mathbf{i} = z \in \mathcal{H} \times \mathcal{H}$. Then f_x is holomorphic.

If in addition for all $x \in G_F(\mathbb{A})$ and all additive measures on $F \setminus \mathbb{A}_F$ it holds that
$$\int_{F \setminus \mathbb{A}_F} f\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} x\right) da = 0,$$
then we say that f is a *cuspform*.

We denote the space of cuspforms of weight $(\mathbf{k}, \mathbf{w})$ and level $K \subset G_F(\mathbb{A}_F^{\mathrm{fin}})$ by $\mathcal{S}_{\mathbf{k},\mathbf{w}}(K)$. Let $\mathfrak{m} \subset \mathcal{O}_F$ be an integral ideal. We then define the subgroups
$$U_0(\mathfrak{m}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_F(\widehat{\mathbb{Z}}) \;\middle|\; c \in \mathfrak{m}\widehat{\mathcal{O}_F} \right\};$$
$$V_1(\mathfrak{m}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_0(\mathfrak{m}) \;\middle|\; d - 1 \in \mathfrak{m}\widehat{\mathcal{O}_F} \right\};$$
$$V_{1,1}(\mathfrak{m}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in V_1(\mathfrak{m}) \;\middle|\; a - 1 \in \mathfrak{m}\widehat{\mathcal{O}_F} \right\};$$
$$U(\mathfrak{m}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in V_{1,1}(\mathfrak{m}) \;\middle|\; b \in \mathfrak{m}\widehat{\mathcal{O}_F} \right\}.$$

Definition A.4.2. Let p be a rational prime and $\mathfrak{m} \subset \mathcal{O}_F$ an ideal. Suppose that p and $\mathfrak{m}$ are coprime and let $K \subset G_F(\widehat{\mathbb{Z}})$ be a compact open subgroup satisfying $V_1(\mathfrak{m}) \subset K \subset U_0(\mathfrak{m})$. We then define for any positive integer n the subgroups

$$K(p^n) := K \cap V_{1,1}(p^n \mathcal{O}_F) \subset K.$$

We now describe the unique adèlic $\mathbf{q}$-expansion associated with Hilbert modular forms as defined above. Let $d_F \in \mathbb{A}_F^{\mathrm{fin},\times}$ be fixed such that $d_F \mathcal{O}_F = \mathcal{D}_F$ and let H_F denote the Hilbert class field of F. By the Principal Ideal Theorem, for each ideal $\mathfrak{a} \subset \mathcal{O}_F$, the ideal $\mathfrak{a}\mathcal{O}_{H_F}$ is principal. For each prime ideal $\mathfrak{r} \subset \mathcal{O}_F$, we may thus choose a generator $\{\mathfrak{r}\} \in \mathcal{O}_{H_F}$ of this ideal and we extend this definition multiplicatively to define $\{\mathfrak{a}\}$ for any ideal $\mathfrak{a} \subset \mathcal{O}_F$.

Let $\mathrm{Pic}(F, \mathfrak{m})^+$ denote the narrow ray class group of F with modulus $\mathfrak{m} \subset \mathcal{O}_F$. For each $\lambda \in \mathrm{Pic}(F, \mathfrak{m})^+$, we may fix $a_\lambda \in \mathbb{A}_F^{\mathrm{fin},\times}$ such that we have the decomposition

$$\mathbb{A}_F^\times = \bigsqcup_{\lambda \in \mathrm{Pic}(F,\mathfrak{m})^+} F^\times a_\lambda \det(V_{1,1}(\mathfrak{m})) F_\infty^{\times,+}.$$

By construction, we will have $[\mathfrak{a}_\lambda] := [a_\lambda \mathcal{O}_F] = \lambda \in \mathrm{Pic}(F)^+$. This induces a similar decomposition

$$G_F(\mathbb{A}) = \bigsqcup_{\lambda \in \mathrm{Pic}(F,\mathfrak{m})^+} G_F(\mathbb{Q}) t_\lambda V_{1,1}(\mathfrak{m}) G_F(\mathbb{R})^+, \text{ where } t_\lambda := \begin{pmatrix} a_\lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

We may decompose any $z \in \mathcal{H} \times \mathcal{H}$ as $z = x_\infty + \mathbf{i} y_\infty$ for uniquely determined $x_\infty \in \mathbb{R} \times \mathbb{R}$ and $y_\infty \in \mathbb{R}^+ \times \mathbb{R}^+$. Now let $f \in \mathcal{S}_{\mathbf{k},\mathbf{w}}(V_{1,1}(\mathfrak{m}))$ and define for any $\lambda \in \mathrm{Pic}(F, \mathfrak{m})^+$ the map

$$f_\lambda : \mathcal{H} \times \mathcal{H} \to \mathbb{C} : z \mapsto y_\infty^{-\mathbf{w}} f\left(t_\lambda \begin{pmatrix} y_\infty & x_\infty \\ 0 & 1 \end{pmatrix}\right).$$

Using the theory outlined in Section A.2, one shows that this function admits a Fourier expansion of the form

$$f_\lambda(z) = \sum_{\nu \in (\mathfrak{a}_\lambda \mathcal{D}_F^{-1})^+} a(\nu, f_\lambda) e^{2\pi i(\nu z_1 + \nu' z_2)}.$$

We are now ready to define the adèlic and p-adic $\mathbf{q}$-expansions of f. One may deduce from the decomposition above that any $y \in \mathbb{A}_F^{\mathrm{fin},\times} F_\infty^{\times,+}$

can be decomposed as $y = \nu a_\lambda^{-1} d_F u$ for some $\nu \in F^{\times,+}$ and $u \in \det(U(\mathfrak{m}))F_\infty^{\times,+}$. We then define the functions

$$a(-,f) : \mathbb{A}_F^{\mathrm{fin},\times} F_\infty^{\times,+} \to \mathbb{C} \quad \text{and} \quad a_p(-,f) : \mathbb{A}_F^{\mathrm{fin},\times} F_\infty^{\times,+} \to \overline{\mathbb{Q}}_p$$

to be zero outside of $\widehat{\mathcal{O}}_F F_\infty^{\times,+}$, and otherwise through the formulas

$$a(y,f) := a(\nu, f_\lambda)\{y^{\mathbf{w-1}}\}\nu^{\mathbf{1-w}}|a_i|_{\mathbb{A}_F}$$

and

$$a_p(y,f) := a(\nu, f_\lambda) y_p^{\mathbf{w-1}} \nu^{\mathbf{1-w}} a_{\lambda,p}^{\mathbf{1}} |a_\lambda^\infty|_{\mathbb{A}_F}.$$

If we now define the maps

$$e_F : \mathbb{C} \times \mathbb{C} : (z_1, z_2) \mapsto \exp(2\pi i(z_1 + z_2))$$

and

$$\chi_F : \mathbb{A}_F / F \to \mathbb{C}^\times : x \mapsto e_F(x_\infty),$$

the following is Theorem 1.1 in [Hid91].

Theorem A.4.3. *Each holomorphic Hilbert cuspform $f \in \mathcal{S}_{\mathbf{k},\mathbf{w}}(V_{1,1}(\mathfrak{m}))$ admits an adèlic* **q***-expansion of the form*

$$f\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = |y|_{\mathbb{A}_F} \sum_{\nu \in F^+} a(\nu y d_F, f)\{(\nu y d_F)^{\mathbf{1-w}}\}(\nu y_\infty)^{\mathbf{w-1}} e_F(\mathbf{i}\nu y_\infty)\chi_F(\nu x),$$

where $y \in \mathbb{A}_F^{\mathrm{fin},\times} F_\infty^{\times,+}$ and $x \in \mathbb{A}_F^\times$.

We now define Hecke operators acting on these objects, following Section 2.1.2 of [For19]. These act on the space $\mathcal{S}_{\mathbf{k},\mathbf{w}}(K)$, where $V_{1,1}(\mathfrak{m}) \subset K \subset U_0(\mathfrak{m})$ for some ideal $\mathfrak{m} \subset \mathcal{O}_F$. Choose a prime $\mathfrak{p}$ above p in F. Similar to before, we may for each ideal $\mathfrak{a} \subset \mathcal{O}_F$ define an element $\{\mathfrak{a}\}_p \in \mathcal{O}_{F,\mathfrak{p}}$ such that $\mathfrak{a}\mathcal{O}_{F,\mathfrak{p}} = \{\mathfrak{a}\}_p \mathcal{O}_{F,\mathfrak{p}}$. We will assume that $\{\mathfrak{a}\}_p = 1$ whenever $\mathfrak{a}$ is prime to $p\mathcal{O}_F$. This notion can be extended to all adèles by considering the ideal that it generates.

Let $\mathfrak{l} \subset \mathcal{O}_F$ be a prime ideal not dividing $\mathfrak{m}$ and let $\varpi \in \mathcal{O}_{F,\mathfrak{l}} \subset \mathbb{A}_F^\times$ be a local uniformiser. Then we define for $f \in \mathcal{S}_{\mathbf{k},\mathbf{w}}(K)$,

$$T_\mathfrak{l} f(x) := \{\varpi\}_p^{\mathbf{w-1}} \sum_{b \in B} f(xb),$$

where $B \subset G_F(\mathbb{A})$ is such that

$$V_{1,1}(\mathfrak{m}) \begin{pmatrix} \varpi & 0 \\ 0 & 1 \end{pmatrix} V_{1,1}(\mathfrak{m}) = \bigsqcup_{b \in B} V_{1,1}(\mathfrak{m}) b.$$

In addition, we define $\langle \mathfrak{l} \rangle f(x) = f(x\varpi)$. If $\mathfrak{l} \mid \mathfrak{m}$, we use the same definition, but now we will denote the resulting operators by U_ϖ and $\langle \varpi \rangle$ respectively, as they will depend on the precise choice of uniformiser ϖ at $\mathfrak{l}$. To capture this effect, for a local unit $a \in \prod_{\mathfrak{l}|\mathfrak{m}} \mathcal{O}_{F,\mathfrak{l}}^\times$, we define the operator $T(a,1)$ using the same definition above, but with ϖ replaced by a. Finally, we may extend the above definitions to define the operators $T_{\mathfrak{l}^n}$ and U_{ϖ^n} using the usual recursive relations.

To each element from $\mathbb{A}_F^\times$, we may now associate one or more Hecke operators as follows. Let $y \in \widehat{O}_F \cap \mathbb{A}_F^\times$. Then we can write

$$y = a \prod_{\mathfrak{l} \subset \mathcal{O}_F} \varpi_{\mathfrak{l}}^{e(\mathfrak{l})} u, \quad \text{where} \quad a \in \prod_{\mathfrak{l}|\mathfrak{m}} \mathcal{O}_{F,\mathfrak{l}}^\times \quad \text{and} \quad u \in \det V_{1,1}(\mathfrak{m}).$$

If we let $\mathfrak{n} \subset \mathcal{O}_F$ denote the ideal locally generated by the $\varpi_{\mathfrak{l}}^{e(\mathfrak{l})}$, when we define the Hecke operator

$$T_y := T(a,1) T_{\mathfrak{n}} \prod_{\mathfrak{l}|\mathfrak{m}} U_{\varpi_{\mathfrak{l}}}^{e(\mathfrak{l})}.$$

This associates with each adèle $y \in \widehat{O}_F \cap \mathbb{A}_F^\times$ uniquely a Hecke operator. The $\mathcal{O}_{F,\mathfrak{p}}$-subalgebra of $\mathrm{End}(\mathcal{S}_{\mathbf{k},\mathbf{w}}(K))$ generated by the operators described above is denoted $h_{\mathbf{k},\mathbf{w}}(K, \mathcal{O}_{F,\mathfrak{p}})$; the *Hecke algebra*. The following result can be shown to hold by construction.

Proposition A.4.4. *Let $f \in \mathcal{S}_{\mathbf{k},\mathbf{w}}(K)$ be a Hilbert modular eigenform, normalised such that $a(1,f) = 1$. Then the T_y-eigenvalue of f is given by the Fourier coefficient $a(y,f)$.*

A.5 p-adic modular forms and Hida families

In this thesis, we will not set up the theory of p-adic modular forms in great detail. For a very clear introduction to the topic and the notion of overconvergent modular forms, consult for example [Von21]. We will however recall a few concepts in the setting over $\mathbb{Q}$ that will illustrate our definitions in the setting from Section A.4 above.

Definition A.5.1. A p-adic modular form for $\mathrm{SL}_2(\mathbb{Z})$ is a power series $f(\mathbf{q}) \in \mathbb{Q}_p[\![\mathbf{q}]\!]$ with the property that there is a sequence $f_i \in \mathcal{M}_{k_i}(\mathrm{SL}_2(\mathbb{Z}))$ with rational Fourier coefficients such that

$$\lim_{i \to \infty} \inf_{n \in \mathbb{N}} \big(v_p(f(\mathbf{q}) - f_i(\mathbf{q})) \big) = \infty.$$

In other words, a p-adic modular form can be viewed as the p-adic limit of $\mathbf{q}$-expansions of classical modular forms. One can show that the weights k_i of the classical modular forms f_i must also converge to a limit p-adically, thus establishing a well-defined notion of the *weight* $k = \lim k_i$ of the p-adic modular form defined above. The reader should find it easy to generalise this notion to more general congruence subgroups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ with level $p \nmid N$.

Classical modular forms of weight $2k$ for Γ are in bijection with the global sections of the kth tensor power of the sheaf of holomorphic differentials on the modular curve X_Γ through an elementary argument. For $\Gamma = \Gamma_1(N)$, the curve $X_1(N)(\mathbb{C}) = \Gamma_1(N)\backslash\mathcal{H}$ parametrizes elliptic curves together with an N-torsion point. Let A_p denote the *Hasse-invariant* of an elliptic curve. Then one may define for $0 \leq r \leq 1$ the subsets

$$X_r(\mathbb{C}_p) := \{x \in X_1(N)(\mathbb{C}_p) \mid v_p(A_p(x)) \leq r\}.$$

Then $X_1(\mathbb{C}_p)^{\mathrm{ord}} := X_0(\mathbb{C}_p)$ denotes the *ordinary locus* of $X_1(N)(\mathbb{C}_p)$, corresponding to all elliptic curves with ordinary reduction at p. It was shown by Katz that p-adic modular forms as defined above biject with the holomorphic differentials on $X_1(\mathbb{C}_p)^{\mathrm{ord}}$. Those modular forms that extend to holomorphic differentials on $X_r(\mathbb{C}_p)$ for some $r > 0$ are called (r-)*overconvergent*.

Definition A.5.2. An overconvergent modular form is called *ordinary* if it is a U_p-eigenvector with eigenvalue a p-adic unit. Recall that, if $f = \sum a_n \mathbf{q}^n$ is a(n overconvergent) modular cuspform, then

$$U_p f := \sum_{n=1}^{\infty} a_{pn} \mathbf{q}^n.$$

Definition A.5.3. The *ordinary projection* operator is defined as

$$e^{\mathrm{ord}} := \lim_{n\to\infty} U_p^{n!}.$$

One checks that the image of e^{ord} is indeed always an ordinary overconvergent modular form, and

$$a_m(e^{\mathrm{ord}} f) = \lim_{n\to\infty} a_{m\cdot p^{n!}}(f).$$

We finally aim to generalise these notions to Hida's adèlic setting over the real quadratic field F. We will follow Section 2.2 in [For19]. Recall the notation from Section A.4 and let $V_{1,1}(\mathfrak{m}) \subset K \subset U_0(\mathfrak{m})$ be a compact

open subgroup. We mimic the idea of p-adic Hilbert modular forms being the limit of classical Hilbert modular forms, by first setting

$$\mathcal{S}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}) := \varinjlim_n S_{\mathbf{k},\mathbf{w}}(K(p^n),\mathcal{O}_{F,\mathfrak{p}}),$$

which is a module over the p-adic Hecke algebra

$$h_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}) := \varprojlim_n h_{\mathbf{k},\mathbf{w}}(K(p^n),\mathcal{O}_{F,\mathfrak{p}}).$$

This algebra contains operators of the form

$$\mathbf{T}_y := \varprojlim_n = T_y\{y\}^{\mathbf{1}-\mathbf{w}} y_p^{\mathbf{w}-\mathbf{1}}.$$

As before, the supremum of the p-adic valuation of the $a_p(-,f)$ defines a p-adic norm on the space $\mathcal{S}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}})$. The object of interest is now defined as its completion;

$$\overline{\mathcal{S}}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}),$$

much like Definition A.5.1.

Definition A.5.4. Let the *nearly ordinary* Hecke algebra be the largest subalgebra $h^{\text{n.o.}}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}) \subset h_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}})$ in which $\mathbf{T}_p$ is a p-adic unit. Define the (nearly) ordinary projection operator by $e^{\text{ord}} := \lim_{n\to\infty} \mathbf{T}_p^{n!}$ and we let the space of nearly ordinary p-adic cuspforms be

$$\overline{\mathcal{S}}^{\text{n.o.}}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}) := e^{\text{ord}}\overline{\mathcal{S}}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}}).$$

We will need the following result later to prove a modularity theorem, which is Theorem 2.4 in [Hid89b].

Proposition A.5.5. *The nearly ordinary Hecke algebra defined above, $h^{\text{n.o.}}_{\mathbf{k},\mathbf{w}}(K(p^\infty),\mathcal{O}_{F,\mathfrak{p}})$, is finite and torsion-free over a ring $\Lambda \cong \mathcal{O}_{F,\mathfrak{p}}[\![W_F]\!]$, where there is an isomorphism $W_F \cong \mathbb{Z}_p^3$.*

In formulating the above result, we implicitly used that Leopoldt's defect vanishes for F, which is known as $F/\mathbb{Q}$ is abelian. This concludes our brief mathematical promenade that took us from the well-known theory of classical modular forms to the depths of Hida's adèlic description of Hilbert modular forms; a language that we use in Chapter 6.

Bibliography

[BC91] Jean-François Boutot and Henri Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et de Drinfeld. *Astérisque*, (196-97):45–158, 1991.

[BC06] Joel Bellaïche and Gaetan Chenevier. Lissité de la courbe de Hecke de aux points Eisenstein critiques. *Journal of the Institute of Mathematics of Jussieu*, 5(2):333–349, 2006.

[BCG23] Nicolas Bergeron, Pierre Charollois, and Luis E. Garcia. Elliptic units for complex cubic fields. *arXiv preprint arXiv:2311.04110*, 2023.

[BD16] Joël Bellaïche and Mladen Dimitrov. On the eigencurve at classical weight 1 points. *Duke Mathematical Journal*, 165(2):245 – 266, 2016.

[BDP22] Adel Betina, Mladen Dimitrov, and Alice Pozzi. On the failure of Gorensteinness at weight 1 Eisenstein points of the eigencurve. *American Journal of Mathematics*, 144(1):227–265, 2022.

[BDS20] Adel Betina, Mladen Dimitrov, and Sheng-Chi Shih. Eisenstein points on the Hilbert cuspidal eigenvariety. *preprint*, 2020.

[Bet20] Adel Betina. Ramification of the eigencurve at classical RM points. *Canadian Journal of Mathematics*, 72(1):57–88, 2020.

[Bru08] Jan Hendrik Bruinier. Hilbert modular forms and their applications. In *The 1-2-3 of modular forms*, pages 105–179. Springer, 2008.

[Čer76] Ivan V. Čerednik. Uniformization of algebraic curves by discrete arithmetic subgroups of with compact quotients. *Mathematics of the USSR-Sbornik*, 29(1):55, 1976.

[Cla03] Pete L. Clark. *Rational points on Atkin-Lehner quotients of Shimura curves*. Harvard University, 2003.

[Col96] Robert F. Coleman. Classical and overconvergent modular forms. *Inventiones mathematicae*, 124:215–241, 1996.

[CSS13] Gary Cornell, Joseph H. Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem*. Springer Science & Business Media, 2013.

[Daa23] Michael A. Daas. CM-values of p-adic Θ-functions. *arXiv preprint arXiv:2309.17251*, 2023.

[DDP11] Samit Dasgupta, Henri Darmon, and Robert Pollack. Hilbert modular forms and the Gross-Stark conjecture. *Annals of mathematics*, pages 439–484, 2011.

[Dei12] Anton Deitmar. *Automorphic forms*. Springer Science & Business Media, 2012.

[Del71] Pierre Deligne. Travaux de shimura. In *Séminaire Bourbaki vol. 1970/71 Exposés 382–399*, pages 123–165. Springer, 1971.

[DGL23] Henri Darmon, Lennart Gehrmann, and Michael Lipnowski. Rigid meromorphic cocycles for orthogonal groups. 2023.

[DK20] Samit Dasgupta and Mahesh Kakde. On constant terms of Eisenstein series. *arXiv preprint arXiv:2010.00650*, 2020.

[DK23a] Samit Dasgupta and Mahesh Kakde. Brumer-Stark Units and Explicit Class Field Theory. *Duke Mathematical Journal*, 2023.

[DK23b] Samit Dasgupta and Mahesh Kakde. On the Brumer-Stark conjecture. *Annals of Mathematics*, 197(1):289–388, 2023.

[DKV18] Samit Dasgupta, Mahesh Kakde, and Kevin Ventullo. On the Gross-Stark Conjecture. *Annals of Mathematics*, 188(3):833–870, 2018.

[DPV21] Henri Darmon, Alice Pozzi, and Jan Vonk. Diagonal restrictions of p-adic Eisenstein families. *Mathematische Annalen*, 379(1):503–548, 2021.

[DPV23] Henri Darmon, Alice Pozzi, and Jan Vonk. The values of the Dedekind-Rademacher cocycle at real multiplication points. *J. Eur. Math. Soc.*, 2023.

[Dri76] Vladimir G. Drinfeld. Coverings of p-adic symmetric domains. *Funkcional. Anal. i Priložen*, 10:29–40, 1976.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[DT08] Henri Darmon and Gonzalo Tornaría. Stark-Heegner points and the Shimura correspondence. *Compositio Mathematica*,

144(5):1155–1175, 2008.

[DV21] Henri Darmon and Jan Vonk. Singular moduli for real quadratic fields: a rigid analytic approach. *Duke Mathematical Journal*, 170(1):23–93, 2021.

[Elk98] Noam D. Elkies. Shimura curve computations. In *International Algorithmic Number Theory Symposium*, pages 1–47. Springer, 1998.

[Err11] Eric Errthum. Singular moduli of Shimura curves. *Canadian Journal of Mathematics*, 63(4):826–861, 2011.

[For19] Michele Fornea. On twisted triple products and the arithmetic of elliptic curves. 2019.

[GD22] Sofia Giampietro and Henri Darmon. A p-adic approach to singular moduli on Shimura curves. *Involve, a Journal of Mathematics*, 15(2):345–365, 2022.

[Geh20] Lennart Gehrmann. On quaternionic rigid meromorphic cocyles. *Mathematical Research Letters*, 2020.

[GKZ87] Benedict H. Gross, Winfried Kohnen, and Don B. Zagier. Heegner points and derivatives of L-series. II. *Mathematische Annalen*, 278:497–562, 1987.

[GMX21] Xavier Guitart, Marc Masdeu, and Xavier Xarles. A quaternionic construction of p-adic singular moduli. *Research in the Mathematical Sciences*, 8:1–20, 2021.

[Gro86] Benedict H. Gross. Local heights on curves. In *Arithmetic geometry*, pages 327–339. Springer, 1986.

[Gro87] Benedict H. Gross. Heights and the special values of L-series. In *Conference Proceedings of the CMS*, volume 7, 1987.

[GvdP06] Lothar Gerritzen and Marius van der Put. *Schottky groups and Mumford curves*, volume 817. Springer, 2006.

[GZ84] Benedict H. Gross and Don B. Zagier. On singular moduli. *Journal für die reine und angewandte Mathematik*, 355:191–220, 1984.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Inventiones mathematicae*, 84:225–320, 1986.

[Hid89a] Haruzo Hida. Nearly ordinary hecke algebras and Galois representations of several variables. *Algebraic Analysis, Geometry and Number Theory*, pages 115–134, 1989.

[Hid89b] Haruzo Hida. On Nearly Ordinary Hecke Algebras for GL(2) over Totally Real Fields. In *Algebraic Number Theory—in honor of K. Iwasawa*, volume 17, pages 139–170. Mathemati-

cal Society of Japan, 1989.

[Hid91] Haruzo Hida. On p-adic L-functions of GL(2)×GL(2) over totally real fields. In *Annales de l'institut Fourier*, volume 41, pages 311–391, 1991.

[HY12] Benjamin J. Howard and Tonghai Yang. Singular moduli refined. *arXiv: Number Theory*, 2012.

[KRY04] Stephen S. Kudla, Michael Rapoport, and Tonghai Yang. Derivatives of Eisenstein series and Faltings heights. *Compositio Mathematica*, 140(4):887–951, 2004.

[LN19] Matteo Longo and Marc-Hubert Nicole. The p-adic variation of the Gross-Kohnen-Zagier theorem. *Forum Mathematicum*, 31, 06 2019.

[Lu11] Wei Lu. Introduction to Local and Global Euler Characteristic Formulas. *arXiv preprint arXiv:1112.4373*, 2011.

[Maz89] Barry Mazur. Deforming Galois representations. In *Galois Groups over $\mathbb{Q}$: Proceedings of a Workshop Held March 23–27, 1987*, pages 385–437. Springer, 1989.

[Mor70] Yasuo Morita. Ihara's conjectures and moduli space of abelian varieties. *Master's Thesis, Tokyo*, 1970.

[MS15] Richard A. Moy and Joel Specter. There exist non-CM Hilbert modular forms of partial weight 1. *International Mathematics Research Notices*, 2015(24):13047–13061, 2015.

[Ogg83] Andrew P. Ogg. Real points on shimura curves. *Arithmetic and Geometry: Papers Dedicated to I.R. Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic*, pages 277–307, 1983.

[Pad23] Oana Padurariu. Shimura curves admitting a smooth plane model. *arXiv preprint arXiv:2310.11767*, 2023.

[Phi15] Andrew Phillips. *Moduli of CM false elliptic curves*. PhD thesis, Boston College, 2015.

[Poz19] Alice Pozzi. *The eigencurve at weight one Eisenstein points*. PhD thesis, McGill University, 2019.

[Ric21] James Rickards. *Intersections of closed geodesics on Shimura curves*. PhD thesis, McGill University, 2021.

[Rom13] Matthieu Romagny. Models of curves. In *Arithmetic and geometry around Galois theory*, pages 149–170. Springer, 2013.

[Sch09] Jarad Schofer. *Borcherds forms and generalizations of singular moduli*. Walter de Gruyter GmbH & Co. KG, 2009.

[Shi67] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Annals of Mathematics*, pages 58–159,

1967.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[vdP92] Marius van der Put. Discrete groups, Mumford curves and theta functions. In *Annales de la Faculté des sciences de Toulouse: Mathématiques*, volume 1, pages 399–438, 1992.

[Vis89] Angelo Vistoli. Intersection theory on algebraic stacks and on their moduli spaces. *Inventiones mathematicae*, 97(3):613–670, 1989.

[Voi09] John Voight. Shimura curve computations. *Arithmetic geometry*, 8:103–113, 2009.

[Voi21] John Voight. *Quaternion algebras*. Springer Nature, 2021.

[Von21] Jan Vonk. Overconvergent modular forms and their explicit arithmetic. *Bulletin of the American Mathematical Society*, 58(3):313–356, 2021.

[Wer96] Annette Werner. Local heights on Mumford curves. *Mathematische Annalen*, 306:819–831, 1996.

[Wil70] Kenneth S. Williams. Integers of biquadratic fields. *Canadian Mathematical Bulletin*, 13(4):519–526, 1970.

[YZZ13] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang. *The Gross-Zagier Formula on Shimura Curves:(AMS-184)*, volume 184. Princeton University Press, 2013.

[Zha01] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Annals of mathematics*, 153(1):27–147, 2001.

Summary

In the 1980s, Gross and Zagier studied the differences between singular moduli, which are the CM-values of Klein's j-function. For example,

$$j\left(\frac{1+\sqrt{-43}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) = 2^{19} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 37 \cdot 433.$$

They proved that these numbers obey very predictable prime factorisations and that the primes that occur in these expressions are relatively small and inert in both CM-fields in question. These remarkable properties sparked a chain of investigations that fuelled many deep results and crucial ideas across various areas of mathematics over the decades that followed, which continue to inspire mathematicians to this day.

We prove a p-adic version of the work by Gross and Zagier on the differences between singular moduli by proving a set of conjectures by Sofia Giampietro and Henri Darmon, who investigated the factorisation of a rational invariant associated to a pair of CM-points on a genus zero Shimura curve, obtained as the ratio of the CM-values of p-adic Θ-functions. As did Gross and Zagier, we give two proofs; an algebraic proof using CM-theory, and more interestingly, also an analytic proof using p-adic infinitesimal deformations of an Hilbert Eisenstein series. Since there are no explicit formulae for its cuspidal p-adic deformations, we instead compute the Frobenius traces of an appropriate Galois deformation, and show their modularity via an $R = T$ theorem. This approach aims to bridge the gap between classical CM-theory and the more recent p-adic advances in the theory of real multiplication.

Chapter 1 serves to illustrate the context within which this thesis is best viewed and starts by introducing CM-theory from an adèlic perspective. We present the factorisation results by Gross and Zagier on the

differences between singular moduli and illustrate these through various examples. We reinterpret their results in the language of intersection numbers of pairs of embeddings and by means of numerous examples this viewpoint is made very concrete. We sketch both the algebraic and analytic proofs of these factorisation results; especially the analytic proof will serve as a great inspiration for the strategy followed in Chapter 6, albeit in a non-archimedean setting as opposed to an archimedean one.

Thereafter, in Chapter 2, we introduce a certain class of Shimura curves associated with indefinite rational quaternion algebras. After outlining some of their basic properties, we describe the conjectures by Giampietro and Darmon and stress the parallels with the results by Gross and Zagier. We then discuss how the p-adic uniformisation of Shimura curves can be used to approach these conjectures p-adically, and an equivalent non-archimedean statement is posed. We outline the general strategies for the proofs of these key results and we stress the similarities between our approach and recent advancements in the theory of real multiplication, among other recent developments.

In Chapter 3, we describe an approach that mirrors the ideas behind Gross and Zagier's original algebraic proof, exploiting the moduli interpretation of the Shimura curve and the theory of complex multiplication. We appeal to the main result of the PhD thesis of Andrew Phillips, which computes the degree of certain refinements of the moduli stack of false elliptic curves, following ideas of Howard and Yang. Using these results, the proof of Theorem A is rather straightforward.

The weight of this thesis is concentrated in our proof of Theorem B. For this, we follow the general strategy of the main arguments presented in work done by Darmon, Pozzi and Vonk. We study a p-stabilisation of the same Hilbert Eisenstein series as did Gross and Zagier. In this sense, our approach is a true p-adic transposition of their seminal work. This second proof can be divided into three distinct steps, which we will now outline and which will reflect the three chapters that take up the full treatment of this approach.

In Chapter 4, we start by recalling some background on genus theory, a study pioneered by Gauß. We prove the exactness of a key sequence using basic class field theory and group cohomology. Next, we prove the existence of and give various different expressions for a quadratic form refining the norm form on a quaternion algebra, which allows us to describe an algebraic construction that associates to a quaternion a certain ideal in a biquadratic field. Through this, we derive a bijection between quaternions and certain elements in a real quadratic field of fixed

trace. This allows us to rewrite the CM-values of p-adic Θ-functions in a meaningfully different way in Section 6.1.

Since, unlike as in the work of Gross and Zagier, the $\mathbf{q}$-expansion of a cuspidal p-adic family passing through the p-stabilised Hilbert Eisenstein series is not a-priori known, we obtain such a family by deforming a rigidification of the decomposable representation associated with this Eisenstein series. More precisely, we will consider all nearly ordinary deformations, which are all such deformations for which the decomposition groups at both primes above p each fix a distinct line. This approach requires us to prove the modularity of such deformations to justify constructing from this deformation the required family of modular forms.

Therefore, Chapter 5 proves an $R = T$ theorem, a famous instance of which occurred in the proof by Wiles of Fermat's Last Theorem. Here, R denotes the universal nearly ordinary deformation ring, and T denotes Hida's cuspidal nearly ordinary Hecke algebra. Using similar methods as in Pozzi's and Betina's theses, along with many other works, and using fundamental results from Hida, we construct a lift of the rigidified representation to the nearly ordinary Hecke algebra, though some additional care is required to circumvent the difficulties of some cohomology groups being 2-dimensional, rather than 1-dimensional. Comparing the dimensions of the Hecke algebra and the resulting deformation ring, the $R = T$ theorem follows purely by commutative algebra.

Finally, in Chapter 6, we consider one particular nearly ordinary deformation and explicitly compute the infinitesimal family of cuspidal deformations of the Hilbert Eisenstein series that corresponds to it. After taking its diagonal restriction, its derivative with respect to the weight parameter and applying the ordinary projection operator, we argue why the result must vanish identically. Ultimately, we conclude the proof of Theorem B by computing explicitly the Fourier coefficients of the mostly theoretically used ordinary projection and equating the first of these coefficients to zero.

Appendix A provides a brief introduction to various types of modular forms. It assumes the theory of classical modular forms and starts by outlining their automorphic perspective, and we will subsequently generalise this treatment to more general types of modular forms in the sections that follow. First, we change the ground field from $\mathbb{Q}$ to a real quadratic field. Then we combine our treatments and describe an adèlic approach to Hilbert modular forms and Hida families, as we will need them for our methods in Chapter 6, leaving the archimedean world and considering p-adic modular forms instead.

Samenvatting

In de jaren 1980 bestudeerden Gross en Zagier de verschillen tussen singuliere moduli; de CM-waarden van Klein's j-functie. Bijvoorbeeld,

$$j\left(\frac{1+\sqrt{-43}}{2}\right) - j\left(\frac{1+\sqrt{-163}}{2}\right) = 2^{19} \cdot 3^6 \cdot 5^3 \cdot 7^3 \cdot 37 \cdot 433.$$

Ze bewezen dat deze getallen voorspelbare priemfactorisaties genieten en dat de priemgetallen die in deze uitdrukkingen voorkomen relatief klein en inert zijn in beide CM-lichamen in kwestie. Deze opmerkelijke eigenschappen gaven de aanzet tot een lange reeks aan wiskundige expedities die in de daaropvolgende decennia leidden tot vele diepgaande resultaten en cruciale ideeën in verschillende gebieden van de wiskunde, die wiskundigen tot op de dag van vandaag blijven inspireren.

We bewijzen een p-adische versie van het werk van Gross en Zagier over de verschillen tussen singuliere moduli door een vermoeden van Sofia Giampietro en Henri Darmon te bewijzen, die de factorisatie onderzochten van een rationale invariant geassocieerd met een paar CM-punten op een genus nul Shimura kromme, verkregen als de kruisverhouding van de CM-waarden van p-adische Θ-functies. Net als Gross en Zagier geven we twee bewijzen; een algebraïsch bewijs met behulp van CM-theorie, en ook een interessanter analytisch bewijs met behulp van p-adische infinitesimale deformaties van Hilbert Eisenstein-reeksen. Aangezien er geen expliciete formules zijn voor dit soort cuspidale p-adische vervormingen, berekenen we deze middels de Frobenius-sporen van de geassocieerde Galoisdeformatie en tonen we hun modulariteit aan middels een $R = T$-stelling. Deze methode hoopt de kloof te overbruggen tussen de klassieke CM-theorie en de meer recente p-adische ontwikkelingen in de theorie van de reële vermenigvuldiging.

Hoofdstuk 1 behandelt de context waarin dit proefschrift geplaatst dient te worden. Het introduceert de nodige achtergrond over CM-theorie vanuit een adèlisch perspectief en de factorisatiestellingen van Gross en Zagier over de verschillen tussen singuliere moduli worden uitgelegd en toegelicht middels verschillende voorbeelden. We herinterpreteren hun resultaten in de taal van snijdingsgetallen van paren van embeddingen en illustreren dit perspectief met een veelvoud aan voorbeelden. Zowel de algebraïsche als de analytische bewijzen van deze factorisatieresultaten worden geschetst.

In Hoofdstuk 2 introduceren we vervolgens een bepaalde klasse van Shimura krommen geassocieerd met indefiniete rationale quaternionalgebra's. We schetsen enkele kerneigenschappen van deze krommen en beschrijven dan de vermoedens van Giampietro en Darmon met een focus op de parallellen met de resultaten van Gross en Zagier. Vervolgens bespreken we hoe de p-adische uniformisatie van Shimura krommen gebruikt kan worden om deze vermoedens p-adisch te benaderen, en we vertalen het vermoeden naar deze equivalente niet-archimedische context. We schetsen de algemene strategie voor het bewijs van deze kernresultaten en we behandelen de sterke overeenkomsten met recente vorderingen in de theorie van de reële vermenigvuldiging.

In Hoofdstuk 3 beschrijven we een bewijs dat de ideeën achter het oorspronkelijke algebraïsche bewijs van Gross en Zagier weerspiegelt, gebruikmakend van de moduli interpretatie van de Shimura kromme en de theorie van complexe vermenigvuldiging. We doen een beroep op het belangrijkste resultaat van het proefschrift van Andrew Phillips, die de graad van bepaalde verfijningen van de moduli stack van zogenaamde valse elliptische krommen berekende, gebruikmakend van ideeën van Howard en Yang. Met behulp van deze resultaten is het bewijs van Stelling A vrij eenvoudig.

De focus van deze scriptie ligt op ons bewijs van Stelling B. Hiervoor volgen we een algemene strategie uiteengezet in eerder werk van Darmon, Pozzi en Vonk. We bestuderen een p-stabilisatie van dezelfde Hilbert Eisenstein-reeks die gebruikt werd door Gross en Zagier. In die zin is ons werk een heus p-adisch analogon van hun werk. Dit tweede bewijs kan verdeeld worden in drie verschillende stappen, die we nu zullen behandelen en die de drie verschillende hoofdstukken reflecteren waaruit dit bewijs is opgebouwd.

In Hoofdstuk 4 herhalen we wat achtergrondinformatie over genustheorie, iets wat Gauß reeds lang geleden ontwikkeld heeft. Middels klasselichamentheorie en groepencohomologie bewijzen we de exactheid

van een uiterst belangrijke rij. Vervolgens bewijzen we het bestaan van een kwadratische vorm die de gebruikelijke normvorm op een quaternionenalgebra verfijnt, en we geven hiervoor verschillende expliciete formules. We gebruiken dit om een algebraïsche constructie op te zetten die een bepaalde quaternion associeert met een ideaal in een bikwadratisch lichaam. Hieruit leiden we een bijectie af tussen quaternionen en bepaalde elementen in een reëel kwadratisch lichaam met een vast spoor. Hierdoor kunnen we de CM-waarden van p-adische Θ-functies op een betekenisvolle manier herschrijven in Sectie 6.1, waar we deze resultaten nodig hebben.

Anders dan in het werk van Gross en Zagier, is de $\mathbf{q}$-expansie van een cuspidale p-adische familie die door de Hilbert Eisenstein-reeks gaat niet a-priori bekend. Daarom verkrijgen we zo'n familie door een rigidificatie van de ermee geassocieerde decomposeerbare representatie te vervormen. Om precies te zijn, zullen we alle bijna ordinaire deformaties beschouwen; dat zijn alle deformaties waarvoor de decompositiegroepen van de twee priemen boven p elk een aparte lijn vasthouden. Deze benadering vereist dat we de modulariteit van zulke deformaties bewijzen om te rechtvaardigen dat we hieruit de gezochte familie van modulaire vormen kunnen construeren.

Hoofdstuk 5 bewijst daarom een $R = T$-stelling, waarvan een beroemd voorbeeld voorkwam in het bewijs van Wiles van de laatste stelling van Fermat. Hier duidt R de universele bijna ordinaire deformatiering aan, en T Hida's cuspidale bijna ordinaire Hecke-algebra. Gebruikmakend van vergelijkbare methoden als in de proefschriften van Pozzi en Betina en vele andere bronnen, en door fundamentele resultaten van Hida te gebruiken, construeren we een lift van de gerigidificeerde representatie naar de bijna ordinaire Hecke-algebra, hoewel op sommige plekken extra zorg nodig is omdat sommige cohomologiegroepen 2-dimensionaal zijn, in plaats van 1-dimensionaal. Uit de vergelijking van de dimensies van de Hecke-algebra en de deformatiering volgt dan de gezochte $R = T$-stelling.

Tenslotte beschouwen we in Hoofdstuk 6 een specifieke bijna ordinaire deformatie en berekenen we expliciet de infinitesimale familie van deformaties van de Hilbert Eisenstein-reeks die ermee correspondeert. Na het nemen van de afgeleide naar de infinitesimale gewichtsparameter van zijn diagonale restrictie en het toepassen van de p-adische ordinaire projectieoperator, tonen we aan dat het resultaat identiek nul moet zijn. Uiteindelijk completeren we het bewijs van Stelling B door expliciet de Fouriercoëfficiënten van de meestal louter theoretisch gebruikte ordinaire projectie te berekenen en de eerste van deze gelijk aan nul te stellen.

Appendix A geeft een korte introductie tot verschillende typen van modulaire vormen. Het veronderstelt de theorie van klassieke modulaire vormen als bekend voor de lezer, en legt uit hoe ze gezien kunnen worden vanuit een meer automorf perspectief. In de daaropvolgende secties veralgemeniseren we deze behandeling naar meer algemene modulaire vormen. Eerst veranderen we het grondlichaam van $\mathbb{Q}$ in een reëel kwadratisch lichaam. Tenslotte combineren we deze behandelingen en beschrijven we een adèlische benadering van Hilbert modulaire vormen en Hida families, omdat we die nodig hebben voor onze methoden in Hoofdstuk 6. Hiervoor verlaten we de archimedische wereld en beschouwen in plaats daarvan p-adische modulaire vormen.

Acknowledgements

This thesis is the result of many years of arduous and continuous labour. However, I could not have done it without the wonderful people who have continued to support me throughout the years. I am deeply indebted to each and every single one of you.

First of all, I would like to thank my supervisor Jan Vonk. It was a privilege to do research under his supervision and to have numerous long and deep mathematical discussions about countless trivialities, problems, solutions, breakthroughs and successes. He has enabled me to travel to many beautiful places and meet many fascinating mathematicians. Without him, I would not be the mathematician I am today.

I would like to further extend my gratitude to everyone who has helped me work through some mathematical difficulties at any point during my research. In particular, I am indebted to Alex Braat, Wouter Rienks and John Voight for pointing me in the right direction on one or even multiple occasions. In addition, I would like to thank my office mates Charlotte Dombrowski, Margherita Pagano and Xiao Yang for welcoming me warmly on the days I would travel to Leiden. I would also like to thank Daan van Gent, Hendrik Lenstra and Peter Stevenhagen for many meaningful discussions.

I would like to conclude by profoundly thanking my parents and my siblings for allowing me to continue to live with you all for the duration of my research project, and providing a healthy and pleasant working environment for me at home, as well as a loving beacon of acceptance and support that I could always fall back on. In addition, I would like to thank my two closest friends, Rowdy de Groot and Tim Al, for their close personal support throughout the years. My gratitude also extends to Koen Doodeman, who helped sparked my love for number theory, and who designed the beautiful cover of this thesis. Finally, I would like to thank Miriam Ní Chobhthaigh for changing the way in which I view the world in countless ways, both mathematical and otherwise.

Thank you all.

Curriculum Vitae

Michael Alexander Daas is geboren op 30 augustus 1997 te Zaandijk en opgegroeid in Wormer, Noord-Holland. In 2015 behaalde hij cum laude zijn middelbareschooldiploma aan het St. Michaël College te Zaandam.

In datzelfde jaar begon hij zijn bachelorstudie aan de Universiteit van Amsterdam in zowel de natuurkunde als de wiskunde, welke hij beide in 2018 cum laude en met een dubbel honours-certificaat afrondde. Zijn bachelorscriptie droeg de titel "*An introductory approach to instantons and the ADHM-construction*", en was voltooid onder supervisie van Raf Bocklandt en Erik Verlinde.

Daaropvolgend startte hij zijn masterstudie in de wiskunde in de specialisatietrack Algebra en Meetkunde. Deze studie werd in 2020 cum laude afgerond na het inleveren van de masterscriptie "*The Symplectic Method for solving Diophantine Equations*" onder begeleiding van Sander Dahmen, werkzaam aan de Vrije Universiteit.

In september van dat jaar begon hij zijn promotietraject bij het mathematisch instituut aan de Universiteit Leiden, onder dagelijkse begeleiding van Jan Vonk. Dit manuscript is hiervan het resultaat. Naast het ontwikkelen van een professionele onderzoeksvaardigheid, heeft hij ook middels trainingen zijn presentatievaardigheden en communicatievaardigheden verder ontwikkeld.

Reeds sinds het laatste jaar van zijn bacheloropleiding is hij aan verscheidene universiteiten werkzaam geweest als student-assistent bij een pluraliteit aan wiskundevakken van uiteenlopende niveaus. Gedurende deze tijd is hij ook werkzaam geweest bij de wiskundeolympiade als begeleider van talentvolle middelbare scholieren. Tevens heeft hij herhaaldelijk een training georganiseerd om studenten voor te bereiden op een internationale wiskundewedstrijd, met goede resultaten tot gevolg.

Vanaf september 2024 zal hij voor twee jaar als postdoctoraal onderzoeker werken aan het Max-Planck-Institut für Mathematik in Bonn.