UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede amministrativa: Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

CORSO DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

CURRICOLO MATEMATICA

CICLO XXXI

RATIONALITY OF DARMON POINTS OVER GENUS FIELDS OF NONMAXIMAL ORDERS

Coordinatore d'indirizzo: Prof. Martino BARDI

Supervisore: Prof. Matteo LONGO

Dottorando: Yan HU

Abstract

Stark-Heegner points, also known as Darmon points, were introduced by H. Darmon in [11], as certain local points on rational elliptic curves, conjecturally defined over abelian extensions of real quadratic fields. The rationality conjecture for these points is only known in the unramified case, namely, when these points are specializations of global points defined over the strict Hilbert class field H_F^+ of the real quadratic field F and twisted by (unramified) quadratic characters of $\mathrm{Gal}(H_F^+/F)$. We extend these results to the situation of ramified quadratic characters; we show that Darmon points of conductor $c \geq 1$ twisted by quadratic characters of $G_c^+ = \mathrm{Gal}(H_c^+/F)$, where H_c^+ is the strict ring class field of F of conductor c, come from rational points on the elliptic curve defined over H_c^+.

Riassunto

I punti di Stark-Heegner, noti anche come punti di Darmon, furono introdotti da H. Darmon in [11], come certi punti locali su curve ellittiche razionali, congettualmente definiti su estensioni abeliane di campi quadratici reali. La congettura sulla razionalità di questi punti è nota solo nel caso non ramificato, vale a dire, quando questi punti sono specializzazioni di punti globali definiti sull'Hilbert class field stretto H_F^+ del campo quadratico reale F e twistati tramite caratteri quadratici (non ramificati) di $\mathrm{Gal}(H_F^+/F)$. Noi estendiamo questi risultati al caso di caratteri quadratici ramificati, e mostriamo che i punti di Darmon di conduttore $c \geq 1$ twistati per caratteri quadratici di $G_c^+ = \mathrm{Gal}(H_c^+/F)$, dove H_c^+ è il ring class field stretto di F di conduttore c, provengono da punti razionali sulla curva ellittica definiti su H_c^+.

Acknowledgements

First and foremost, I must express my great thanks to my supervisor Prof. Matteo Longo for his for his immense support and encouragement without which this thesis would not have been possible. Prof. Longo is a great and helpful supervisor. He is always being patient to me when I was very slow in my progress and tolerate my dullness and fault. He makes me a better mathematicians and leads me to the right direction in mathematics.

I would like to thank Prof. Francesco Baldassarri and Prof. Bruno Chiarellotto. I have learnt a lot of knowledge from them. I would also like to thank all the members of the Number Theory and Arithmetic Geometry groups at Padova for creating a vibrant atmosphere. I have benefited tremendously from the various activities and discussions within the group. I am also very thankful to other professors and other staffs in the department.

I would like to thank Dr. Velibor Bojkovic, Dr.Guhanvenkat Harikumar, Dr. Genaro Hernandez Mada and Dr. Maria Rosaria Pati. They help me a lot in mathematics.

I would like to thank my friends in Padova. They are all helpful, friendly to me. They support me during my Ph.D period. I think Padova as my home because of them. Here I need to express my thanks to the people: Roberto BRAMATI, Sebastiano DON, Simone GIOVANNINI, Paolo LUZZINI, Roman PUKHTAIEVYCH, Marco TARANTINO, Alekos CECCHIN, Marco PICCIRILLI, Pietro GATTI, Davide BARCO, Federico CAMPANINI, Maria Teresa CHIRI, Giacomo GRAZIANI, Giovanna Giulia LE GROS, Federico VENTURELLI, Elena BACHINI, Guillermo PELINO, Luisa ANDREIS, Veronica Dal SASSO, Carlo MARTINUCCI, Laura COSSU, Frances ODUMODU, Francesco FERRARESSO, Daniele TOVAZZI, Dinh TRAN, Muhammad Hassan Raza KHAN, Pallavi KALIYAR, MD Masoom RABBANI.

I also would like to thank some Chinese friends I made during my period in Padova: Luming ZHAO, Meng ZHENG, Xue LI, Xiaohuan SUN, Qianqian LI, Bin ZHU, Bili ZHONG, Han DENG, Chuanyu SUN.

Finally, I thank my parents Mingzhu HU and Xiaodan LI for their support.

Introduction

Darmon points

The theory of complex multiplication gives a collection of points defined over class fields of imaginary quadratic fields. Birch related these points to the arithmetic of elliptic curves which plays an important role in Number Theory. Particularly, the work of Gross-Zagier [25] and the work of Gross-Kohnen-Zagier [24] depend on the properties of these points. H. Darmon extended Birch's idea to the case when the base field is not an imaginary quadratic field. In his fundamental paper [11], Darmon describes a conjectural p-adic analytic construction of global points on elliptic curves, points which are defined over the ring class fields of real quadratic fields, which are non-torsion when the central critical value of the first derivative of the complex L-function of the elliptic curve over the real quadratic field does not vanish. These points are called Stark-Heegner points or Darmon points. Note that the absence of a theory of complex multiplication in the real quadratic case, available in the imaginary quadratic case, makes the construction of global points on elliptic curves over real quadratic fields and their abelian extensions a rather challenging problem. The idea of Darmon was that the points are defined by locally analytic method, and conjecture that these come from global points. Following [11], many authors proposed similar constructions in different situations, including the cases of modular and Shimura curves, and the higher weight analogue of Stark-Heegner, or Darmon cycles; with no attempt to be complete, see for instance [14], [19], [36], [37], [54], [20], [47], [30], [29], [28], [27], and [26].

Let E be a rational elliptic curve of conductor $N = Mp$, with $p \nmid M$ an odd prime number and $M \geq 1$ and integer. Fix also a real quadratic field F, the arithmetic setting of the original construction in [11] should satisfy the following Heegner assumption:

1. The prime p is inert in F;
2. All primes $\ell \mid M$ are split in F.

Under these assumptions, the central critical value $L(E/F, 1)$ of the complex L-function of E over F vanishes. Darmon points are local points P_c for E defined over finite extension of F_p, the completion of F at the unique prime above p; their definition and the main properties are recalled in Chapter 3 below. The definition of these points depends on the choice of an auxiliary integer $c \geqslant 1$ which c is prime to p, called the conductor of a Darmon point P_c. The rationality conjecture predicts that these points P_c are localizations of global points $\mathbf{P}_c$ which are defined over the strict ring class field H_c^+ of F of conductor c.

The rationality conjectures for Darmon points are the most important open problems in the theory of Darmon points and for now only partial results are known toward the rationality conjectures for Darmon points, or more generally cycles. The first result on the rationality of Darmon points is obtained by Bertolini and Darmon in the paper [4], where they show that a certain linear combination of these points with coefficients given by values of genus characters of the real quadratic field F comes from a global point defined over the Hilbert class field of F. Instead of directly comparing the constructions of the two points, the main idea behind the proof of these results is to use a factorization formula for p-adic L-functions to compare the localization of Heegner points and Darmon points. The first step is the comparison between the Darmon point and the p-adic L-function. More precisely, the proof consists in relating Darmon points to the p-adic L-function interpolating central critical values of the complex L-functions over F attached to the arithmetic specializations of the Hida family passing through the modular form attached to E. The second step consists in expressing this p-adic L-function in terms of a product of two Mazur-Kitagawa p-adic L-functions, which are known to be related to Heegner points by the main result of [3]. A similar strategy has been adopted by [21], [49], [38], [39] obtaining similar results.

All known results in the direction of the conjectures in [11] involve linear combination of Darmon points twisted by genus characters, which are quadratic unramified characters of $\mathrm{Gal}(H_F^+/F)$, where H_F^+ is the (strict) Hilbert class field of F. The goal of this paper is to prove a similar rationality result for more general quadratic characters, namely, quadratic characters of ring class fields of F, so we allow for ramification.

In the remaining part of the introduction we briefly state our main result and the main differences with the case of genus characters treated up to now.

The Main Result

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $F/\mathbb{Q}$ be a real quadratic field $F = \mathbb{Q}(\sqrt{D})$ of discriminant $D = D_F > 0$, prime to N. We assume that $N = Mp$ with $p \nmid M$ and satisfies Heegner assumption:

1. The prime p is inert in F;
2. All primes $\ell \mid M$ are split in F.

Fix an integer c prime to $D \cdot N$ and a quadratic character

$$\chi : G_c^+ = \mathrm{Gal}(H_c^+/F) \to \{\pm 1\},$$

where, as above, H_c^+ denotes the strict class field of F of conductor c. Let $\mathcal{O}_c$ be the order in F of conductor c. Recall that G_c^+ is isomorphic to the group of strict equivalence classes of projective $\mathcal{O}_c^+$-modules, which we denote $\mathrm{Pic}^+(\mathcal{O}_c)$, where two such modules are strictly equivalent if they are the same up to an element of F of positive norm. We assume that χ is primitive, meaning that it does not factor through any G_f^+ with f a proper divisor of c.

Fix embeddings $F \hookrightarrow \bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ throughout. Let $P_c \in E(F_p)$ be a Darmon point of conductor c (see Chapter 3 below for the precise definition of these points) where, as above, F_p is the completion of F at the unique prime of F above p. It follows from their construction that Darmon points of conductor c are in bijection with equivalence classes of quadratic forms of discriminant Dc^2, and this can be used to define a Galois action $P_c \mapsto P_c^\sigma$ on Darmon points, where P_c is a fixed Darmon point of conductor c and $\sigma \in G_c^+$. We may then form the point

$$P_\chi = \sum_{\sigma \in G_c^+} \chi^{-1}(\sigma) P_c^\sigma \tag{1}$$

which lives in $E(F_p)$. Finally, let $\log_E : E(\mathbb{C}_p) \to \mathbb{C}_p$ denote the formal group logarithm of E. Note that, since p is inert in F, it splits completely in H_c^+, and therefore for any point $Q \in E(H_c^+)$ the localization of Q at any of the primes in H_c^+ dividing p lives in $E(F_p)$. Our main result is the following:

Theorem 1. *Assume that c is odd and coprime to DN. Let χ be a primitive quadratic character of G_c^+. Then there exists a point $\mathbf{P}_\chi$ in $E(H_c^+)$ and a rational number $n \in \mathbb{Q}^\times$ such that*

$$\log_E(P_\chi) = n \cdot \log_E(\mathbf{P}_\chi).$$

Moreover, the point $\mathbf{P}_\chi$ is of infinite order if and only if $L'(E/F, \chi, 1) \neq 0$.

If $c = 1$, this is essentially the main result of [4]. To be more precise, the work [4] needed to assume E had two primes of multiplicative reduction because of this assumption in [3]. However, this assumption has been removed by very recent work of Mok [43], which we also apply here.

The proof in the general case follows a similar line to that in [4]. However, some modifications are in order. The first difference is that the genus theory of non-maximal orders is more complicated than the usual genus theory, and the arguments need to be adapted accordingly. More importantly, one of the main ingredients in the proof of the rationality result in [4] is a formula of Popa [46] for the central critical value of the L-function over F of the specializations at arithmetic points of the Hida family passing through the modular form associated with the elliptic curve E. However, this formula does not allow treat L-functions twisted by ramified characters. Instead, we recast an L-value formula from [41] which allows for ramification, expressed in terms of periods of Gross-Prasad test vectors, in a more classical framework to get our result.

Contents

Chapter 1

Preliminaries

In this chapter we provide a brief introduction to the objects that will be used in the thesis.

1.1 Hecke operators

Let $\mathcal{H}$ be the Poincaré upper half-plane: $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. Let N be a positive integer. The principal congruence subgroup of level N is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Definition 1.1.1. A subgroup Γ of $\mathbf{SL}_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a congruence subgroup of level N.

For any positive integer N, the group

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \text{ such that } N \text{ divides } c \right\}$$

is called the Hecke congruence group of level N. Denote by $S_2(N) := S_2(\Gamma_0(N))$ the space of cusp forms of weight 2 on $\Gamma_0(N)$.

The vector space $S_2(N)$ is equipped with a non-degenerate Hermitian inner product

$$\langle f_1, f_2 \rangle = \int_{\mathcal{H}/\Gamma_0(N)} f_1(\tau) f_2(\bar{\tau}) dx dy,$$

known as the Petersson norm. It is also equipped with an action of certain Hecke operators T_p indexed by rational primes p and defined by the rules

$$T_p(f) := \begin{cases} \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) + pf(p\tau) & p \nmid N, \\ \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) & p \mid N. \end{cases}$$

Let $a_n := a_n(f)$ be the Fourier coefficient of f. These operators act linearly on $S_2(N)$ and their effect on the q-expansions at ∞ is given by the following formula:

$$T_p(f) := \begin{cases} \sum_{p|n} a_n q^{n/p} + p \sum a_n q^{pn} & p \nmid N, \\ \sum_{p|n} a_n q^{n/p} & p \mid N. \end{cases}$$

It is convenient to extend the definition of the Hecke operators to operators T_n indexed by arbitrary positive integers n by equating the coefficient of n^{-s} in the identity of formal Dirichlet series:

$$\sum_{n=1}^{\infty} T_n n^{-s} := \prod_{p\nmid N}(1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - T_p p^{-s})^{-1}.$$

1.2 Atkin-Lehner theory

Let $\mathbb{T}$ be the commutative subalgebra of $\mathrm{End}_{\mathbb{C}}(S_2(N))$ generated over $\mathbb{Z}$ by the Hecke operators T_n and let $\mathbb{T}^0$ denote the subalgebra generated only by those operators T_n with $(n, N) = 1$.

The space $S_2(N)$ does not decompose in general into a direct sum of the one-dimensional eigenspaces S_λ, where $\lambda : \mathbb{T} \to \mathbb{C}$ is $\mathbb{C}$-algebra homomorphism. However, there is a distinguished subspace of $S_2(N)$, the so-called space of newforms, which decomposes as a direct sum of one-dimensional eigenspaces under both the actions of $\mathbb{T}$ and $\mathbb{T}^0$. A modular form in $S_2(N)$ is said to be an oldform if it is a linear combination of functions of the form $f(d'z)$, with $f \in S^2(N/d)$ and $d' \mid d > 1$. The new subspace of $S_2(N)$, denoted $S_2^{\mathrm{new}}(N)$, is the orthogonal complement of the space $S_2^{\mathrm{old}}(N)$ of oldforms with respect to the Petersson norm.

Theorem 1.2.1. *(Atkin-Lehner). Let $f \in S_2^{\mathrm{new}}(N)$ be a be a simultaneous eigenform for the action of $\mathbb{T}^0$. Let S be any finite set of prime numbers and $g \in S_2(N)$ an* *eigenform for T_p for all $p \notin S$. If $a_p(f) = a_p(g)$ for all $p \notin S$, then $g = \lambda f$ for some $\lambda \in \mathbb{C}$.*

Proof. See [2]. □

The simultaneous eigenvector f satisfying the further condition $a_1(f) = 1$ is called the normalised newform of level N.

1.3 L-series

We can define the L-series attached to a newform f of level N:

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

where $a_n(f)$ is the Fourier coefficients of f.

We can also show that the L-series of a Hecke eigenform has a Euler product:

Theorem 1.3.1. *If f is a normalized Hecke eigenform, then*

$$L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1},$$

where a_n is the Fourier coefficient.

Proof. See the proof of Theorem 1.4.4 in [6]. □

Now we can define twisted L-functions $L(s, f, \chi)$ associated with f and indexed by the primitive Dirichlet character χ:

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

Next let us consider the L-series of f over field F associated with quadratic Dirichlet character attached to F. The L-series is defined by

$$L(f/F, s) = L(f, s) \cdot L(f, \chi, s),$$

where χ is the quadratic Dirichlet character attached to F and $L(f,\chi,s)$ is the twisted L-series. The $L(f/F,s) = L(f,s)\cdot L(f,\chi,s)$ factors into an Euler product:

$$L(f/F,s) = \prod_{p|N}(1 - a_{\mathbb{N}(p)}\mathbb{N}(p)^{-s})^{-1}\prod_{p\nmid N}(1 - a_{\mathbb{N}(p)}\mathbb{N}(p)^{-s} + \mathbb{N}(p)^{k-1-2s})^{-1},$$

where $\mathbb{N}(p)$ is the norm map, the product being taken this time over all the finite places p of F.

Now let us introduce the definition of discriminant.

Definition 1.3.2. Let F be a number field and $\alpha_1,\ldots,\alpha_n$ be a basis for $F/\mathbb{Q}$. Let $\sigma_1,\ldots,\sigma_n\colon F\to\mathbb{C}$ be all embeddings. The discriminant of F is defined as:

$$\Delta_F = \mathtt{det}\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n)\end{pmatrix}^2.$$

In particular, let $F = \mathbb{Q}(\sqrt{D})$ be a quadratic field, D is square free. The quadratic discriminant of F is

$$\Delta_F = \begin{cases} D & D\equiv 1 \pmod 4; \\ 4D & D\equiv 2,3 \pmod 4.\end{cases}$$

The discriminant defined above is also called fundamental discriminant. A discriminant of a quadratic field is said to be a prime discriminant if it has only one prime factor, so it must be one of the following type:

$$-4, \pm 8, \pm p\equiv 1 \pmod 4.$$

The product of coprime discriminants is again a discriminant. Every discriminant D can be written uniquely as a product of prime discriminants $D = P_1\cdots P_t$. For the discriminant Dc^2, c is odd, we can write $\Delta_1 = D_1 d$ and $\Delta_2 = D_2 d$ for some $d = \pm c = \prod_{j=1}^{s}\ell_j^*$ where $\ell_j^* = (-1)^{(\ell_j-1)/2}\ell_j$ with $\ell_j \mid c$ and $D = D_1\cdot D_2$ a factorization into coprime discriminants, allowing $D_1 = D$ or $D_2 = D$. For any such decomposition

$Dc^2 = \Delta_1 \cdot \Delta_2$, we define a character $\chi_{\Delta_1\Delta_2}$ on ideals by setting

$$\chi_{\Delta_1\Delta_2}(\mathfrak{p}) = \begin{cases} \chi_{\Delta_1}(\mathbb{N}(\mathfrak{p})) & \mathfrak{p} \nmid \Delta_1 \\ \chi_{\Delta_2}(\mathbb{N}(\mathfrak{p})) & \mathfrak{p} \nmid \Delta_2 \\ \chi_{\ell_j^*}(\mathbb{N}(\mathfrak{p})) & \mathfrak{p} \mid c \text{ and } \mathfrak{p} \nmid \ell_j \end{cases}$$

($\chi_m(n) = \left(\frac{m}{n}\right)$ is the Kronecker symbol). We can extend it to all fractional ideals by multiplicativity. More details about genus character can be found in [9].

Let χ be the character of G_c^+, then we have the twisted L-function:

$$L(f/F, \chi, s) = \prod_{p|N}(1 - \chi(p)a_{\mathbb{N}(p)}\mathbb{N}(p)^{-s})^{-1} \prod_{p\nmid N}(1 - \chi(p)a_{\mathbb{N}(p)}\mathbb{N}(p)^{-s} + \chi(p)^2\mathbb{N}(p)^{k-1-2s})^{-1},$$

where $\mathbb{N}(p)$ is the norm map, the product being taken this time over all the finite places p of F.

1.4 Modular curves and modular spaces

Let Γ be the subgroup of the $\mathbf{SL}_2(\mathbb{Z})$. The modular curve for such a Γ is defined as the quotient space of orbits under Γ,

$$Y_\Gamma = \mathcal{H}/\Gamma(N),$$

the action of Γ on $\mathcal{H}$ is the usual Möbius transformation. The modular curves for $\Gamma_0(N)$ is denoted $Y_{\Gamma_0(N)} = \mathcal{H}/\Gamma_0(N)$. The quotient $\mathcal{H}/\Gamma(N)$ inherits from the complex structure on $\mathcal{H}$ the structure of a non-compact Riemann surface. To compactify the modular curve Y_Γ, define $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and take the extended quotient

$$X(\Gamma) = \mathcal{H}^*/\Gamma.$$

The quotient $\mathcal{H}^*/\Gamma_0(N)$ can even be identified with the set of complex points of an algebraic curve defined over $\mathbb{Q}$, denoted by $X_0(N)$. This algebraic curve structure arises from the interpretation of $\mathcal{H}/\Gamma_0(N)$ as classifying isomorphism classes of elliptic curves with a distinguished cyclic subgroup of order N, which we shall explain now.

If $\gamma \in \Gamma_0(N)$ and $\tau \in \mathcal{H}/\Gamma_0(N)$, then the subgroup $\{\langle \frac{1}{N} \rangle\} \subset \frac{\mathbb{C}}{\mathbb{Z}+\mathbb{Z}\tau}$ remains invariant under the action of γ. Thus $\mathcal{H}/\Gamma_0(N)$ is a moduli space for the problem of determining equivalence classes of pairs (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N. There is a 1-1 correspondence between finite subgroups $\Phi \subset E$ and isogenies $\phi : E \to E'$ given by the association $\Phi \leftrightarrow \ker\phi$. Thus the point of $\mathcal{H}/\Gamma_0(N)$ can also be viewed as classifying triples (E, E', ϕ), where $\phi : E \to E'$ is an isogeny whose kernel is cyclic of order N. More details are discussed in C.13 of [52].

The following theorem of Eichler and Shimura establishes a relationship between these two L-series.

Theorem 1.4.1. *Let f be a normalised eigenform whose Fourier coefficients $a_n(f)$ are integers. Then there exists an elliptic curve E_f over $\mathbb{Q}$ such that*

$$L(E_f, s) = L(f, s).$$

Proof. See the proof of Theorem 2.10 in [12]. □

Let $J_0(N)$ denote the Jacobian variety of $X_0(N)$. The modular curve $X_0(N)$ is embedded in its Jacobian by sending a point P to the class of the degree 0 divisor $(P) - (i\infty)$. Let

$$\Phi_N : X_0(N) \to E_f$$

be the modular parametrisation obtained by composing the embedding $X_0(N) \to J_0(N)$ with the natural projection $J_0(N) \to E_f$ arising from the Eichler-Shimura construction.

1.5 Complex multiplication

Let $K = \mathbb{Q}(\omega_D)$ be a quadratic imaginary subfield of $\mathbb{C}$, where $D < 0$ is the discriminant of K and

$$\omega_D = \begin{cases} \frac{1+\sqrt{D}}{2} & if \quad D \equiv 1 (mod\ 4), \\ \frac{\sqrt{D}}{2} & \text{otherwise.} \end{cases} \tag{1.5.1}$$

Definition 1.5.1. Let $\mathcal{K}$ be a number field. An order $\mathcal{O}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ that is finitely generated as $\mathbb{Z}$-module and satisfies $\mathcal{O} \otimes \mathbb{Q} = \mathcal{K}$.

Every order is contained in the maximal order $\mathcal{O}_K = \mathbb{Z}[\omega_D]$ and is uniquely determined by its conductor c, a positive non-zero integer such that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}c\omega_D$. (3.1 [12]).

Theorem 1.5.2. *Let Λ be a lattice in $\mathbb{C}$ and $E = \mathbb{C}/\Lambda$ be an elliptic curve over $\mathbb{C}$. Then one of the following is true:*

(**i**) *End(E)$\cong \mathbb{Z}$.*

(**ii**) *End(E) is isomorphic to an order in a quadratic imaginary field K.*

Proof. See the proof of Theorem 5.5 in [52]. □

Definition 1.5.3. An elliptic curve $E/\mathbb{C}$ is said to have complex multiplication if its endomorphism ring is isomorphic to an order in quadratic imaginary field. More precisely, given such an order $\mathcal{O}$, one says that E has complex multiplication by $\mathcal{O}$ if End(E)$\simeq \mathcal{O}$.

If E has complex multiplication by $\mathcal{O}$, the corresponding period lattice of E is a projective $\mathcal{O}$-module of rank 1. If $\Lambda \subset \mathbb{C}$ is a projective $\mathcal{O}$-module of rank 1, the corresponding elliptic curve E has complex multiplication by $\mathcal{O}$. Thus, there is a bijection

$$\left\{ \begin{array}{c} E/\mathbb{C} \text{ with CM by } \mathcal{O}, \\ \text{up to isomorphism.} \end{array} \right\} \overset{\simeq}{\rightarrow} \left\{ \begin{array}{c} \text{Rank one projective } \mathcal{O}\text{-modules,} \\ \text{up to isomorphism.} \end{array} \right\}$$

The set on the right is called the Picard group of $\mathcal{O}$ and is donated Pic($\mathcal{O}$).

Theorem 1.5.4. *There exists an abelian extension H_c of K which is unramified outside of the primes dividing c, and whose Galois group is naturally identified, via the Artin map, with Pic($\mathcal{O}$).*

Remark 1.5.5. If $\mathfrak{p}$ is a prime ideal of K which is prime to c, we denote by $\pi_\mathfrak{p}$ a uniformiser of $K_\mathfrak{p}$, and by[$\mathfrak{p}$] the class in Pic($\mathcal{O}$) attached to the finite idèle $\iota_\mathfrak{p}(\pi_\mathfrak{p})$. The Artin reciprocity law map

$$\text{rec: Pic}(\mathcal{O}) \rightarrow \text{Gal}(H_c/K)$$

sends the element [$\mathfrak{p}$] to the inverse $\sigma_\mathfrak{p}^{-1}$ of the Frobenius element $\sigma_\mathfrak{p}$ at $\mathfrak{p}$.

Remark 1.5.6. The theorem above is a special case of the main theorem of the class field theory. For more details, one can see the Chapter VII, Theorem 5.1 in [7].

The extension H_c whose existence is guaranteed by the theorem is called the ring class field of K attached to $\mathcal{O}$.

1.6 Heegner points on $X_0(N)$

A non-cuspidal point on the curve $X_0(N)$ over $\mathbb{Q}$ is given by a pair of (E, E') of elliptic curves over $\mathbb{Q}$ and an isogeny $\phi : E \to E'$. We represent the point x by the diagram $(\phi : E \to E')$.

The ring End(x) associated to the point x is the subring of pairs (α, β) in End$(E)\times$ End(E') which are defined over $\mathbb{Q}$ and give a commutative square

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \alpha\downarrow & & \downarrow\beta \\ E & \xrightarrow[\phi]{} & E'. \end{array}$$

The ring End(x) is isomorphic to either $\mathbb{Z}$ or an order $\mathcal{O}$ in K.

Assume End(x)=$\mathcal{O}$ and let $\mathcal{O}_K$ be the ring of integers of K. The conductor c of $\mathcal{O}$ is defined as the index of $\mathcal{O}$ in $\mathcal{O}_K$. Then $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$ and the discriminants of $\mathcal{O}_K$ and $\mathcal{O}$ are d_K and $D = d_K c^2$. x is a Heegner point if End(x)=$\mathcal{O}$ and the conductor c of $\mathcal{O}$ is relatively prime to N.

Heegner points exist when all prime factors p of N are either split or ramified in K and every prime p with p^2 dividing N is ramified in K.

Remark 1.6.1. The article [23], the seminal article [25] and the follow-up article [24] provide lots of information on Heegner points and their connections with special values of the associated Rankin L-series.

Chapter 2

The p-adic upper half plane

In this chapter, we want to recall some basic theory of the p-adic upper half plane.

Let p be a prime, let $|.|_p$ denote the usual normalised p-adic absolute value on $\mathbb{Q}$, and let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to this absolute value. Let $\bar{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$; the field obtained by completing $\bar{\mathbb{Q}}_p$ with respect to the p-adic valuation is a complete algebraically closed field which is denoted by $\mathbb{C}_p$. Let G be the group $\mathbf{GL}_2(\mathbb{Q}_p)$ and $\mathbb{Z}_p$ denote the ring of integers in $\mathbb{Q}_p$. We will also use the additive valuation

$$v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$$

normalized so that $v_p(p) = 1$.

Let $V = \mathbb{Q}_p^2$ be a fixed two dimensional vector space, viewed as a space of row vectors, on which G acts from the left by the formula

$$g.(x, y) = (ax + by, cx + dy), \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, (x, y) \in \mathbb{Q}_p^2.$$

The homogeneous coordinates $(x, y) \in \mathbb{Q}_p^2$ are called unimodular if both coordinates are integral, but at least one is not divisible by p.

2.1 The p-adic upper half plane

The p-adic upper half plane is defined set theoretically to be

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

To construct $\mathcal{H}_p$, we need to describe an admissible covering that defines its rigid structure. Now we will introduce an easy form of Grothendieck topology which is called a G-topology.

Definition 2.1.1. Let X be a set. A G-topology T on X is given by the following data and requirements:

1. A family $\mathcal{F}$ of subsets of X with the properties: $\emptyset$, $X \in \mathcal{F}$ and if U,$V \in \mathcal{F}$, then $U \cap V \in \mathcal{F}$.

2. For each $U \in \mathcal{F}$ a set $\mathrm{Cov}(U)$ of coverings of U by elements of $\mathcal{F}$.

$\mathrm{Cov}(U)$ requires the following properties:

3. $\{U\} \in \mathrm{Cov}(U)$.

4. For V,$U \in \mathcal{F}$ with $V \subset U$ and $\mathcal{U} \in \mathrm{Cov}(U)$ the covering $\mathcal{U} \cap V := \{U' \cap V \mid U' \in \mathcal{U}\}$ belongs to $\mathrm{Cov}(V)$.

5. Let $U \in \mathcal{F}$, $\{U_i\}_{i\in I} \in \mathrm{Cov}(U)$ and $\mathcal{U}_i \in \mathrm{Cov}(U_i)$, then $\cup_{i\in I}\mathcal{U}_i := \{U' \mid U'$ belongs to some $\mathcal{U}_i\}$ is an element of $\mathrm{Cov}(U)$.

The $U \in \mathcal{F}$ are called admissible sets or T-open and the elements of $\mathrm{Cov}(U)$ are called admissible coverings or T-coverings.

Given $x \in \mathbb{P}^1(\mathbb{C}_p)$, we may choose homogeneous coordinates $x = [x_0, x_1]$ for x that are unimodular. For a real number $r > 0$, let

$$W(x, r) = \{y \in \mathbb{P}^1(\mathbb{C}_p) : v_p(y_0x_1 - y_1x_0) \geq r\},$$

where we always take a unimodular representative $[y_0, y_1]$ of y. Also define

$$W^-(x, r) = \{y \in \mathbb{P}^1(\mathbb{C}_p) : v_p(y_0x_1 - y_1x_0) > r\}.$$

Lemma 2.1.2. *Let x and x' be two elements of $\mathbb{P}^1(\mathbb{Q}_p)$, and let n be a positive integer. Then $W(x, n) \cap W(x', n) \neq \emptyset$ if and only if $[x_0, x_1] \equiv \lambda[x'_0, x'_1]$ (mod p^n) for some unit $\lambda \in \mathbb{Z}_p^*$*

Proof. See the proof of Lemma 1.2.1 in [15]. □

Remark 2.1.3. For each integer $n > 0$, let $\mathcal{P}_n$ be a set of representatives for the points of $\mathbb{P}^1(\mathbb{Q}_p)$ modulo p^n. Let $\mathcal{H}_n$ be the set

$$\mathcal{H}_n := \mathbb{P}^1(\mathbb{C}_p) \setminus \bigcup_{x \in \mathcal{P}_n} W(x, n)$$

Let $\mathcal{H}_n^- \subset \mathcal{H}_n$ be the set

$$\mathcal{H}_n^- := \mathbb{P}^1(\mathbb{C}_p) \setminus \bigcup_{x \in \mathcal{P}_n} W^-(x, n-1)$$

Then

$$\mathcal{H}_p = \bigcup_n \mathcal{H}_n = \bigcup_n \mathcal{H}_n^-.$$

Proposition 2.1.4. *$\mathcal{H}_p$ is an admissible open subdomain of $\mathbb{P}^1(\mathbb{Q}_p)$ and the coverings of $\mathcal{H}_p$ by the families $\{\mathcal{H}_n\}_{n=1}^{\infty}$ and $\{\mathcal{H}_n^-\}_{n=1}^{\infty}$ are admissible coverings.*

Proof. See the discussion following lemma 3 in [48] □

2.2 The p-adic uniformisation

The role of holomorphic functions on $\mathcal{H}$ is played by the rigid analytic functions on $\mathcal{H}_p$. These are functions that admit nice expressions when restricted to certain distinguished subsets of $\mathcal{H}_p$, called affinoids.

Let

$$\text{red: } \mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$$

be the natural map given by reduction modulo the maximal ideal of the ring of integers of $\mathbb{C}_p$.

The set

$$\begin{aligned}\mathcal{A} :&= \text{red}^{-1}(\mathbb{P}^1(\bar{\mathbb{F}}_p) - \mathbb{P}^1(\mathbb{F}_p)) \\ &= \{\tau \in \mathcal{H}_p \text{ such that } \mid \tau - t \mid \geq 1, \text{for } t = 0, ..., p-1, \text{and } \mid \tau \mid \leq 1\}\end{aligned}$$

is contained in $\mathcal{H}_p$ since red $(\mathbb{P}^1(\mathbb{Q}_p)) \subset \mathbb{P}^1(\mathbb{F}_p)$. It is an example of a standard affinoid in $\mathcal{H}_p$. We can also define the annuli

$$W_t = \{\tau \text{ such that } \tfrac{1}{p} <\mid \tau - t \mid < 1\},\ t = 0, ...p-1,$$
$$W_\infty = \{\tau \text{ such that } 1 <\mid \tau \mid < p\}.$$

Two lattices Λ_1 and Λ_2 are homothety classes in $\mathbb{Q}_p^2$ if there is a scalar $a \in \mathbb{Z}_p$ so that $\Lambda_1 = a\Lambda_2$.

Definition 2.2.1. Let $\mathcal{T}$ be the graph whose vertices are homothety classes $[\Lambda]$ of $\mathbb{Z}_p$-lattices $\Lambda \subset \mathbb{Q}_p^2$, where two vertices x and y are joined by an edge if $x = [\Lambda_1]$ and $y = [\Lambda_2]$ with

$$p\Lambda_1 \subsetneq \Lambda_2 \subsetneq \Lambda_1.$$

Proposition 2.2.2. *The graph $\mathcal{T}$ is a homogeneous tree of degree p+1.*

Proof. See the proof of Proposition 1.3.2 in [15] □

Let Λ be the $\mathbb{Z}_p$-lattice generated by x_1 and x_2, i.e. $\Lambda = \langle x_1, x_2 \rangle = \mathbb{Z}_p x_1 + \mathbb{Z}_p x_2$. The group G acts on $\mathcal{T}$ as follows:

$$\gamma.l = [\gamma.\Lambda := \langle \gamma x_1, \gamma x_2 \rangle],\ \ l = [\Lambda] \text{ and } \gamma \in G.$$

Here we view x_i as column vectors in $\mathbb{Q}_p$ and γx_i is the usual matrix multiplication. For $\lambda \in \mathbb{Q}_p^\times$, we know that $\gamma.\lambda\Lambda = \lambda\gamma.\Lambda$ and hence two lattices Λ and Λ' satisfies $\Lambda \sim \Lambda' \Rightarrow \gamma.\Lambda \sim \Lambda'$. The action is well-defined.

The tree space $\mathcal{T}$ is treated as a combinatorial object: a collection $\mathcal{T}_0$ of vertices indexed by homothety classes of $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$ and a collection $\mathcal{T}_1$ of edges consisting of pairs of adjacent vertices. An ordered edge is an ordered pair e=(v_1,v_2) of adjacent vertices. Then we can denote by $s(e)$:=v_1 and $t(v)$:=v_2 the source and target of e respectively. Write $\mathcal{E}(\mathcal{T})$ be the set of ordered edges of $\mathcal{T}$ and write $\mathcal{V}(\mathcal{T})$ be the set of vertices of $\mathcal{T}$.

Let $v_0 \in \mathcal{T}_0$ be the distinguished vertex of $\mathcal{T}$ attached to the homothety class of the standard lattice $\mathbb{Z}_p^2 \subset \mathbb{Q}_p^2$. The edges having v_0 as endpoint correspond to index p sublattices of $\mathbb{Z}_p^2$ and thus are in canonical bijection with $\mathbb{P}^1(\mathbb{F}_p)$. Label these edges as e_0,..., e_{p-1}, $e_\infty \in \mathcal{T}_1$.

Proposition 2.2.3. *There is a unique map*

$$r\colon \mathcal{H}_p \to \mathcal{T} = \mathcal{T}_0 \cup \mathcal{T}_1$$

satisfying the following properties:

1. *$r(\tau)=v_0$ if and only if $\tau \in \mathcal{A}$;*
2. *$r(\tau)=e_t$ if and only if $\tau \in W_t$;*
3. *r is G-equivariant, i.e.,*

$$r(\gamma\tau)=\gamma r(\tau), \quad \text{for all } \gamma \in G.$$

Proof. The proof of this proposition is explained in Proposition 5.1 of [12]. □

If $e = \{v_1, v_2\}$ is an edge of $\mathcal{T}$, it is convenient to denote by $]e[\subset \mathcal{T}$ the singleton $\{e\}$ and call it the open edge attached to e. The subset $[e]:=\{e, v_1, v_2\}$ of $\mathcal{T}$ is called the closed edge attached to e. The sets $\mathcal{A}_{[e]} := r^{-1}([e])$ and $W_{]e[} := r^{-1}(]e[)$ are called the standard affinoid and the standard annulus attached to e respectively. Note that $\mathcal{A}_{[e]}$ is a union of two translates by G of the standard affinoid $\mathcal{A}$ glued along the annulus $W_{]e[}$. The collection of affinoids $\mathcal{A}_{[e]}$, as e ranges over $\mathcal{T}_1$, gives a covering of $\mathcal{H}_p$ by standard affinoids whose pairwise intersections are either empty or of the form $\mathcal{A}_v := r^{-1}(v)$ with $v \in \mathcal{V}(\mathcal{T})$.

Fix an affinoid $\mathcal{A}_0 \subset \mathcal{H}_p$. A rational function having poles outside $\mathcal{A}_0$ attains its supremum on $\mathcal{A}_0$ (with respect to the p-adic metric). Hence the space of such functions can be equipped with the sup norm.

Definition 2.2.4. A $\mathbb{C}_p$-valued function f on $\mathcal{H}_p$ is said to be rigid-analytic if, for each edge e of $\mathcal{T}$, the restriction of f to the affinoid $\mathcal{A}_{[e]}$ is a uniform limit, with respect to the sup norm, of rational functions on $\mathbb{P}^1(\mathbb{C}_p)$ having poles outside $\mathcal{A}_{[e]}$.

Remark 2.2.5. Let Γ be a discrete subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$. The quotient $\mathcal{H}_p/\Gamma$ is equipped with the structure of a rigid analytic curve over $\mathbb{Q}_p$ and can be identified with the rigid analytification of an algebraic curve X over $\mathbb{Q}_p$ [17]. Not every curve over $\mathbb{Q}_p$ can be expressed as such a quotient. In fact, it can be shown that if $X = \mathcal{H}_p/\Gamma$ where Γ acts on $\mathcal{T}$ without fixed points, then it has a model over $\mathbb{Z}_p$ whose special fiber is a union of projective lines over $\mathbb{F}_p$ intersecting transversally at ordinary double points. The converse to this statement is a p-adic analogue of the classical complex uniformisation theorem.

2.3 p-adic measures

Let $\Gamma \subset \mathbf{SL}_2(\mathbb{Q}_p)$ be a discrete subgroup as in the previous section.

Definition 2.3.1. A form of weight k on $\mathcal{H}_p/\Gamma$ is a rigid analytic function f on $\mathcal{H}_p$ such that

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \qquad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Denote by $S_k(\Gamma)$ the $\mathbb{C}_p$-vector space of rigid analytic modular forms of weight k with respect to Γ. The space $S_2(\Gamma)$ can be identified with the space of rigid analytic differential forms on the quotient $\mathcal{H}_p/\Gamma$. In particular, the dimension of $S_2(\Gamma)$ over $\mathbb{C}_p$ is equal to the genus of this curve.

The set $\mathbb{P}^1(\mathbb{Q}_p)$ is endowed with its p-adic topology in which the open balls of the form

$$B(a, r) = \{t \text{ such that } |t - a| < p^{-r}\},\ a \in \mathbb{Q}_p,$$
$$B(\infty, r) = \{t \text{ such that } |t| > p^r\}$$

form a basis. These open balls are also compact, and any compact open subset of $\mathbb{P}^1(\mathbb{Q}_p)$ is a finite disjoint union of open balls of the form above.

Definition 2.3.2. A p-adic distribution on $\mathbb{P}^1(\mathbb{Q}_p)$ is a finitely additive function

$$\mu\colon \{\text{compact open } U \subset \mathbb{P}^1(\mathbb{Q}_p)\} \longrightarrow \mathbb{C}_p$$

satisfying $\mu(\mathbb{P}^1(\mathbb{Q}_p)) = 0$.

If μ is any p-adic distribution on $\mathbb{P}^1(\mathbb{Q}_p)$, and g is a locally constant function on $\mathbb{P}^1(\mathbb{Q}_p)$, then the integral $\int_{\mathbb{P}^1(\mathbb{Q}_p)} g(t)d\mu(t)$ can be defined as a finite Riemann sum. More precisely, letting

$$\mathbb{P}^1(\mathbb{Q}_p) = U_1 \cup \cdots \cup U_m$$

be a decomposition of $\mathbb{P}_1(\mathbb{Q}_p)$ as a disjoint union of open balls such that g is constant on each U_j, one defines

$$\int_{\mathbb{P}_1(\mathbb{Q}_p)} gd\mu := \sum_{j=1}^{m} g(t_j)\mu(U_j)$$

where t_j is any sample point in U_j. The distribution relation satisfied by μ ensures that this expression does not depend on the decomposition.

Definition 2.3.3. A p-adic measure is a bounded distribution, i.e., a distribution for which there is a constant C satisfying

$$|\mu(U)|_p < C, \text{ for all compact open } U \subset \mathbb{P}^1(\mathbb{Q}_p).$$

If λ is any continuous function on $\mathbb{P}^1(\mathbb{Q}_p)$, then the integral of λ against μ can be defined by the rule

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} \lambda(t)d\mu(t) = \lim_{\mathcal{C}=\{U_\alpha\}} \sum_{\alpha} \lambda(t_\alpha)\mu(U_\alpha),$$

where the limit is taken over increasingly fine covers $\{U_\alpha\}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by disjoint compact open subsets U_α, and t_α is a sample point in U_α.

Remark 2.3.4. In [33], it is shown that the integral is well-defined.

The following lemma shows that the connection between measures and rigid analytic function on $\mathcal{H}_p$.

Lemma 2.3.5. *Let μ be a measure on $\mathbb{P}^1(\mathbb{Q}_p)$.*

(1) *The function f defined by*

$$f_\mu(z) = \int_{\mathbb{P}^1(\mathbb{Q}_p)} (\frac{1}{z-t})d\mu(t)$$

is a rigid analytic function on $\mathcal{H}_p$.

(2) *If μ is a Γ-invariant measure on $\mathbb{P}^1(\mathbb{Q}_p)$, i.e.,$\gamma\mu(t) = \mu(\gamma t) = \mu(t)$, then f_μ belongs to $S_2(\Gamma)$.*

Proof. See the proof of Lemma 5.8 in [12]. □

Denote by $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma$ the space of all Γ-invariant measures on $\mathbb{P}^1(\mathbb{Q}_p)$.

Theorem 2.3.6. *(Schneider, Teitelbaum) The assignment $\mu \mapsto f_\mu$ is an isomorphism from Meas$(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{C}_p)^\Gamma$ to $S_2(\Gamma)$.*

Proof. See the proof of Theorem 5.9 in [12]. □

Definition 2.3.7. A harmonic cocycle on $\mathcal{T}$ is a function c: $\mathcal{E}(\mathcal{T}) \to \mathbb{C}_p$ satisfying

1. $c(e) = -c(\bar{e})$, for all $e \in \mathcal{E}(\mathcal{T})$;
2. $\sum_{s=(e)} c(e) = 0$ and $\sum_{t(e)=v} c(e) = 0$, for all $v \in \mathcal{T}_0$.

A harmonic cocycle c gives rise to a distribution μ_c on $\mathbb{P}^1(\mathbb{Q}_p)$ by the rule

$$\mu_c(U_c) = c(e).$$

Conversely, c can be recovered from the associated distribution by the rule above. Under this bijection, the Γ-invariant distributions correspond to Γ-invariant harmonic cocycles on $\mathcal{T}$.

2.4 p-adic line integrals

Let f be a rigid analytic function on $\mathcal{H}_p$. We need to define a notation of p-adic line integral attached to such a function. This line integral should be an expression of the form $\int_{\tau_1}^{\tau_2} f(z)dz \in \mathbb{C}_p$ and it should be linear and satisfy:

$$\int_{\tau_1}^{\tau_2} f(z)dz + \int_{\tau_2}^{\tau_3} f(z)dz = \int_{\tau_1}^{\tau_3} f(z)dz, \ \forall \tau_1, \tau_2, \tau_3 \in \mathcal{H}_p.$$

If $f(z)dz = dF$ is an exact differential on $\mathcal{H}$, one defines

$$\int_{\tau_1}^{\tau_2} f(z)dz = F(\tau_1) - F(\tau_2). \tag{2.4.1}$$

The equation $dF = f(z)dz$ is sufficient to define F up to a locally constant function in the complex setting. In the p-adic topology, there are plenty of locally constant functions which are not constant, because $\mathcal{H}_p$ is totally disconnected. This leads to an ambiguity in the choice of F, which is remedied by working with the rigid analytic topology in which all locally constant functions are constant.

However, in general there need not exist a rigid analytic F on $\mathcal{H}_p$ such that $dF = f(z)dz$. One may try to remedy this situation by singling out an antiderivative of certain rational functions. The p-adic logarithm defined on the open disc in $\mathbb{C}_p$ of radius 1 centered at 1 by the power series

$$\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$$

is singled out by the property of being a homomorphism from this open disc to $\mathbb{C}_p$. Choose an extension of the p-adic logarithm to all of $\mathbb{C}_p^\times$

$$\log\colon \mathbb{C}_p^\times \to \mathbb{C}_p$$

by fixing some element $\pi \in \mathbb{C}_p$ satisfying $\mid \pi \mid_p < 1$ and let $\log(\pi)$=0 (it is a homomorphism on $\mathbb{C}_p^\times$). The standard choice is obtained by taking $\pi = p$.

Having fixed a choice of p-adic logarithm, for each rational differential $f(z)dz$ on $\mathbb{P}^1(\mathbb{C}_p)$, a formal antiderivative of the form

$$F(z) = R(z) + \sum_{j=1}^{t} \lambda_j \log(z - z_j),$$

where R is a rational function, the $\lambda_j's$ belong to $\mathbb{C}_p$, and the z_j are the poles of $f(z)dz$. This antiderivative is unique up to an additive constant, and hence the equation 2.4.1 can be used to fix a well-defined line integral attached to $f(z)dz$.

Definition 2.4.1. Let f be a rigid analytic function on $\mathcal{H}_p$. Assume that its associated boundary distribution μ_f is a measure. Choose a branch $\log\colon \mathbb{C}_p^\times \to \mathbb{C}_p$ of the p-adic logarithm. Then the p-adic line integral associated to this choice is defined to be

$$\int_{\tau_1}^{\tau_2} f(z)dz := \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f(t), \quad \tau_1, \tau_2 \in \mathcal{H}_p. \tag{2.4.2}$$

Note that the integral is a locally analytic $\mathbb{C}_p$-valued function on $\mathbb{P}^1(\mathbb{Q}_p)$, so that the integral converges in $\mathbb{C}_p$. The equation 2.4.2 can be justified by the following computation relying on the Lemma 2.3.5:

$$\int_{\tau_1}^{\tau_2} f(z)dz = \int_{\tau_1}^{\tau_2} \int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{dz}{z-t}\right) d\mu_f(t) = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f(t).$$

Because the p-adic measure μ_f comes from a harmonic cocycle taking value in $\mathbb{Z}$ and not just $\mathbb{Z}_p$, it is possible to define the multiplicative refinement of the p-adic line integral by formally exponentiating the expression in 2.4.2

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} f(z)dz := \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f(t) \in \mathbb{C}_p^\times,$$

where

$$\times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} g(t)d\mu_f(t) := \lim_{\mathfrak{C}} \prod_{U_\alpha \in \mathfrak{C}} g(t_\alpha)^{\mu(U_\alpha)}$$

the limit is taken over increasingly fine covers $\mathcal{C}=\{ U_\alpha \}_\alpha$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by disjoint compact open subsets, with $t_\alpha \in U_\alpha$. This limit exists if $\log g$ is locally analytic and g takes values in a compact subset of $\mathbb{C}_p^\times$.

Remark 2.4.2. The multiplicative integral has the advantage over its more classical additive counterpart that it does not rely on a choice of p-adic logarithm and carries more information. The two integrals are related by the formula

$$\int_{\tau_1}^{\tau_2} f(z)dz = \log(\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} f(z)dz).$$

Chapter 3

Darmon points

This chapter reviews the definition of Darmon points given in [11]. Let the notation be as in the introduction: $E/\mathbb{Q}$ is an elliptic curve of conductor $N = Mp$ with $p \nmid M$ and $F/\mathbb{Q}$ is a real quadratic field of discriminant $D = D_F$ such that all primes dividing M are split in F and p is inert in F.

3.1 Modular symbol

For any field L, let $P_{k-2}(L)$ be the space of homogeneous polynomials in 2 variables of degree $k-2$, and let $V_{k-2}(L)$ be its L-linear dual. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(L)$ act from the right on $P(x,y) \in P_{k-2}(L)$ by the formula

$$(P \mid \gamma)(x,y) = P(ax+by, cx+dy)$$

and we equip $V_{k-2}(L)$ with the dual action.

Definition 3.1.1. Let G be an abelian group. An G-valued modular symbol is a function

$$\begin{aligned} I\colon \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) &\to G \\ (x,y) &\mapsto I\{x \to y\} \end{aligned}$$

satisfying

1. $I\{\ x \to y\ \} = -I\{\ y \to x\ \}$, for all $x,\ y \in \mathbb{P}^1(\mathbb{Q})$.
2. $I\{\ x \to y\ \} + I\{\ y \to z\ \} = I\{\ x \to z\ \}$, for all $x,\ y,\ z \in \mathbb{P}^1(\mathbb{Q})$.

Denote by $\mathrm{MS}(G)$ the group of G-valued modular symbols. The group $\mathbf{GL}_2(\mathbb{Q})$ acts from the left by fractional linear transformations on $\mathbb{P}^1(\mathbb{Q})$, and if G is equipped with a left $\mathbf{GL}_2(\mathbb{Q})$-action, then $\mathrm{MS}(G)$ inherits a right $\mathbf{GL}_2(\mathbb{Q})$-action by the rule

$$(I \mid \gamma)\{x \to y\} := \gamma.I\{\gamma^{-1}x \to \gamma^{-1}y\}.$$

For any positive integer M, the group

$$\Gamma_0(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \text{ such that } M \text{ divides } c \right\}$$

is called the Hecke congruence group of level M. Denote by $S_k(M) := S_k(\Gamma_0(M))$ the space of cusp forms of weight k on $\Gamma_0(M)$. Denote by $\mathrm{MS}_{\Gamma_0}(G)$ the space of $\Gamma_0(M)$-invariant modular symbol.

Given $f \in S_k(M)$, we may attach to f the standard modular symbol $\tilde{I}_f \in \mathrm{MS}_{\Gamma_0}(V_{k-2}(\mathbb{C}))$, explicitly, for $r, s \in \mathbb{P}^1(\mathbb{Q})$ and $P(x,y) \in P_{k-2}(\mathbb{C})$ an homogeneous polynomial of degree $k-2$, put

$$\tilde{I}_f\{r \to s\}(P(x,y)) = 2\pi i \int_r^s f(z)P(z,1)dz.$$

Remark 3.1.2. The integral is along any path in $\mathcal{H}$ between r and s which is discussed in [35]. According to the cuspidality of f, the integral converges. The details about the convergence of the integral are discussed in [12].

Remark 3.1.3. We can check that

$$\begin{aligned}
(\tilde{I}_f \mid \gamma)(P(x,y)) &= \gamma.\tilde{I}_f\{\gamma^{-1}r \to \gamma^{-1}s\}(P(x,y)) \\
&= 2\pi i \int_r^s f(z)P(z,1)dz \\
&= 2\pi i \int_{\gamma.r}^{\gamma.s} f(\gamma^{-1}z)P(\gamma^{-1}z,1)d\gamma^{-1}z \\
&= \tilde{I}_f\{\gamma.r \to \gamma.s\}((P \mid \gamma^{-1})(x,y)).
\end{aligned}$$

In [12], it is defined an action of the Hecke operators T_p, for $p \nmid M$, by

$$T_p(I)\{x \to y\} = I\{px \to py\} + \sum_{j=0}^{p-1} I\{\frac{x+j}{p} \to \frac{y+j}{p}\}.$$

Let Λ_E denote the so-called Neron lattice of E, generated by the periods of a Neron differential on E. Let t_E be the greatest common divisor of the integer $p+1-a_p(E)$, where p ranges over all primes which are congruent to 1 modulo M.

Theorem 3.1.4. *The modular symbol m_f attached to f_E takes values in a lattice Λ, which is contained in $\frac{1}{t_E}\Lambda_E$ with finite index.*

Proof. See the proof of Theorem 2.20 in [12]. □

The matrix $\omega_\infty = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ normalises Γ_0 and induces an involution on the space $\mathrm{MS}_{\Gamma_0(M)}(V_{k-2}(\mathbb{C}))$. Let $\tilde{I}_f^+$ and $\tilde{I}_f^-$ denote the plus and minus eigencomponents of I_f for the involution. Suppose that f is a normalized eigenform and let K_f be the field generated over $\mathbb{Q}$ by the Fourier coefficients of f. Thus we have the following proposition:

Proposition 3.1.5. *There exists complex periods Ω_f^+ and Ω_f^- with the property that the modular symbols*

$$I_f^+ := (\Omega_f^+)^{-1}\tilde{I}_f^+, \quad I_f^- := (\Omega_f^-)^{-1}\tilde{I}_f^-$$

belong to $MS_{\Gamma_0(M)}(V_{k-2}(K_f))$. These periods can be chosen to satisfy

$$\Omega_f^+\Omega_f^- = \langle f, f\rangle,$$

where $\langle f, f\rangle$ is the Petersson scalar product of f with itself.

Proof. The proof is explained in Section 1.1 of [34] and [40]. □

Choose a sign at infinity $\omega_\infty \in \{+1, -1\}$, and set

$$\Omega_f := \begin{cases} \Omega_f^+ & \omega_\infty = +1; \\ \Omega_f^- & \omega_\infty = -1; \end{cases}$$

$$I_f := \begin{cases} I_f^+ & \omega_\infty = +1; \\ I_f^- & \omega_\infty = -1. \end{cases}$$

Let H_c^1 denote compactly supported cohomology.

By Proposition 4.2 of [1], we can get

$$\mathrm{MS}_{\Gamma_0(M)}(V_{k-2}) \cong H_c^1(\Gamma_0(M), V_{k-2}).$$

Moreover we have a natural map $H_c^1(\Gamma_0(M), V_{k-2}) \to H^1(\Gamma_0(M), V_{k-2})$, which sends a modular symbol I to the 1-cocycle: $\gamma \mapsto I\{\gamma.x \to x\}$.

3.2 Double integrals

Let f be the newform of level N attached to E by modularity. Let $M_2(\mathbb{Z}[1/p])$ denote the ring of 2×2 matrices with entries in $\mathbb{Z}[1/p]$, and let $R \subset M_2(\mathbb{Z}[1/p])$ denote the subring of matrices which are upper-triangular modulo M. Define the group

$$\Gamma = \{\gamma \in R^\times \mid \det(\gamma) = 1\},$$

which acts on $\mathcal{H}_p$ by Möbius transformations. Let $\mathbb{P}$ denote a subset of $\mathbb{P}^1(\mathbb{Q})$. The following proposition is key to the definition of Darmon points.

Proposition 3.2.1. *There exists a unique system of $\mathbb{Z}$-valued measure on $\mathbb{P}^1(\mathbb{Q}_p)$, indexed by r, $s \in \mathbb{P}$ and denoted $\mu_f\{r \to s\}$, satisfying the following properties.*

1. *For all $r, s \in \mathbb{P}$,*

$$\mu_f\{r \to s\}(\mathbb{P}^1(\mathbb{Q}_p)) = 0, \quad \mu_f\{r \to s\}(\mathbb{Z}_p) = I_f\{r \to s\}.$$

2. *For all $\gamma \in \Gamma$, and all compact open $U \subset \mathbb{P}^1(\mathbb{Q}_p)$,*

$$\mu_f\{\gamma.r \to \gamma.s\}(\gamma.U) = \mu_f\{r \to s\}(U).$$

Proof. See the proof of Proposition 2.6 of [13]. □

The measures μ_f can be used to define a double multiplicative integral attached to τ_1, $\tau_2 \in \mathcal{H}_p$ and $x, y \in \mathbb{P}$, by setting

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega_f := \times\!\!\!\!\!\!\int_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{x \to y\}(t) \in \mathbb{C}_p.$$

The following lemma shows the properties of the multiplicative integral defined above:

Lemma 3.2.2. *The double multiplicative integral defined above satisfies the following properties:*

1. $\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_3}\int_x^y \omega_f = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega_f \times \times\!\!\!\!\!\!\int_{\tau_2}^{\tau_3}\int_x^y \omega_f$
2. $\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_{x_1}^{x_3} \omega_f = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_{x_1}^{x_2} \omega_f \times \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_{x_2}^{x_3} \omega_f$
3. $\times\!\!\!\!\!\!\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma x}^{\gamma y} \omega_f = (\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega_f)^{\omega^{|\gamma|}\omega_\infty^{sgn(\gamma)}}$, for all $\gamma \in R^\times$.

Proof. See the proof of Lemma 1.10 in [11] where more details are discussed. □

Let $q \in p\mathbb{Z}_p$ be the Tate period attached to E, and write

$$\Phi_{Tate}:\mathbb{C}_p^\times/q^{\mathbb{Z}} \to E(\mathbb{C}_p)$$

for the Tate uniformisation. See [53] for details.

Let $\log_q:\mathbb{C}_p^\times \to \mathbb{C}_p$ denote the branch of the p-adic logarithm satisfying $\log_q(q)=0$, and define a homomorphism

$$\log_E:E(\mathbb{C}_p) \to \mathbb{C}_p$$

by the rule

$$\log_E(P):=\log_q(\Phi_{Tate}^{-1}(P)).$$

Define the additive version of the double multiplicative integral to be

$$\int_{\tau_1}^{\tau_2}\int_r^s \omega_f := \log_q(\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_r^s \omega_f). \tag{3.2.1}$$

3.3 Indefinite integrals

We introduce the notion of indefinite integral. The following result justifies the choice of branch of p-adic logarithm that was made in 3.2.1.

Proposition 3.3.1. *There is a unique function from $\mathcal{H}_p \times \mathbb{P} \times \mathbb{P}$ to $\mathbb{C}_p$, denoted*

$$(\tau, r, s) \mapsto \int^{\tau} \int_{x}^{y} \omega_f$$

satisfying

1. *For all $\gamma \in \Gamma$,*
$$\int^{\gamma\tau} \int_{\gamma x}^{\gamma y} \omega_f = \int^{\tau} \int_{x}^{y} \omega_f.$$
2. *For all τ_1, $\tau_2 \in \mathcal{H}$,*
$$\int^{\tau_2} \int_{x}^{y} \omega_f - \int^{\tau_1} \int_{x}^{y} \omega_f = \int_{\tau_1}^{\tau_2} \int_{x}^{y} \omega_f.$$
3. *For all x, y, $z \in \mathbb{P}$,*
$$\int^{\tau} \int_{x}^{y} \omega_f + \int^{\tau} \int_{y}^{z} \omega_f = \int^{\tau} \int_{x}^{z} \omega_f.$$

Proof. The proof of this proposition is explained in [11]. □

The function characterised indirectly in the proposition above is called the indefinite integral attached to f.

Remark 3.3.2. It is the existence of the indefinite integral that relies crucially on the branch of p-adic logarithm chosen. The uniqueness of the indefinite integral is also discussed in [4].

The double multiplicative integral gives rise to a 1-cocycle $\tilde{c}_{f,\tau}(\gamma) \in Z^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ by the rule

$$\tilde{c}_{f,\tau}(\gamma)\{x \to y\} = \times\!\!\!\!\!\!\int_{\tau}^{\gamma\tau} \int_{x}^{y} \omega.$$

The natural image c_f of $\tilde{c}_{f,\tau}$ in $H^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ is independent of the choice of τ.

The $\mathbb{C}_p$-valued 2-cocycle $\tilde{d}_{\tau,x} \in \mathbb{Z}^2(\Gamma, \mathbb{C}_p^\times)$ is defined by setting

$$\tilde{d}_{\tau,x}(\alpha, \beta) := \tilde{c}_{f,\tau}(\alpha^{-1})\{x \to \beta x\} = \times\!\!\!\!\!\!\int_{\tau}^{\alpha^{-1}\tau} \int_{x}^{\beta x} \omega.$$

The natural image d of $\tilde{d}_{\tau,x}$ in $H^2(\Gamma, \mathbb{C}_p^\times)$ does not depend on the choice of τ and x.

Recall that $\mathcal{M}(\mathbb{C}_p)$ denotes the left Γ-module of $\mathbb{C}_p$-valued modular symbol on $\mathbb{P}^1(\mathbb{Q})$ and $\mathcal{F}$ denote the $\mathbb{C}_p$-valued functions on $\mathbb{P}^1(\mathbb{Q})$.

The map Δ: $\mathcal{F} \to \mathcal{M}(\mathbb{C}_p)$ defined by

$$(\Delta f)\{x \to y\} := f(y) - f(x)$$

is surjective and has as kernel the space of constant functions. Taking the cohomology of the short exact sequence of $\mathbb{C}_p[\Gamma]$-modules

$$0 \to \mathbb{C}_p \to \mathcal{F} \stackrel{\Delta}{\to} \mathcal{M}(\mathbb{C}_p) \to 0$$

yields a long exact sequence in cohomology:

$$H^1(\Gamma, \mathcal{F}) \to H^1(\Gamma, \mathcal{M}(\mathbb{C}_p)) \stackrel{\delta}{\to} H^2(\Gamma, \mathbb{C}_p) \to H^2(\Gamma, \mathcal{F})$$

All the cohomology groups appearing in the exact sequence are endowed with a natural action of the Hecke operators T_l with $l \nmid N$, defined as in [51]. These groups are equipped with the Atkin-Lehner involution W_∞ at ∞, defined using the matrix $a_\infty = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ which belongs to the normalisers of the groups $\Gamma_0(N)$, $\Gamma_0(M)$, $\Gamma_0'(M)(:= a_p\Gamma_0(M)a_p^{-1}$, a_p is the matrix used to define the Atkin-Lehner involution W_p) and Γ in $R^\times$. On modular symbols W_∞ is defined by the rule

$$(W_\infty m)\{x \to y\} = m\{a_\infty x \to a_\infty y\} = m\{-x \to -y\},$$

and on $H^1(\Gamma, \mathcal{M}(\mathbb{C}_p))$ by the rule

$$(W_\infty c)(\gamma)\{x \to y\} = c(\gamma^{a_\infty})\{-x \to -y\}.$$

Let $q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}$ be the discrete subgroup of $\mathbb{C}_p^\times$. We have the following theorem:

Theorem 3.3.3. *There exists a lattice $\Lambda_p \subset \mathbb{C}_p^\times$ commensurable with $q^{\mathbb{Z}}$ and such that the natural images of d in $H^2(\Gamma, \mathbb{C}_p^\times/\Lambda_p)$ and of c in $H^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times/\Lambda_p))$ are trivial.*

Proof. See the proof of Theorem 5.2 in [5]. □

We can define an modular symbol $m_\tau \in C^0(\Gamma, \mathcal{M}(\mathbb{C}_p^\times/q^{\mathbb{Z}}))$ and a 1-cochain $\xi_{\tau,x} \in C^1(\Gamma, \mathbb{C}_p^\times/q^{\mathbb{Z}})$ by the rules

$$\tilde{c}_\tau = dm_\tau, \quad \tilde{d}_{\tau,x} = d\xi_{\tau,x}.$$

It is useful to adopt the notation

$$⨍^\tau \int_x^y \omega_f := m_\tau\{x \to y\} \in \mathbb{C}_p^\times/q^{\mathbb{Z}},$$

Proposition 3.3.4. *The indefinite multiplicative integral* $\times\!\!\!\!\!\!\int^{\tau} \int_x^y \omega_f$ *satisfies the following properties:*

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega = \times\!\!\!\!\!\!\int^{\tau_2} \int_x^y \omega \div \times\!\!\!\!\!\!\int^{\tau_1} \int_x^y \omega, \pmod{q^{\mathbb{Z}}}$$

$$\times\!\!\!\!\!\!\int^{\tau} \int_{x_1}^{x_3} \omega = \times\!\!\!\!\!\!\int^{\tau} \int_{x_1}^{x_2} \omega \times \times\!\!\!\!\!\!\int^{\tau} \int_{x_2}^{x_3} \omega, \pmod{q^{\mathbb{Z}}}$$

$$\times\!\!\!\!\!\!\int^{\gamma\tau} \int_{\gamma x}^{\gamma y} \omega = (\times\!\!\!\!\!\!\int^{\tau} \int_x^y \omega)^{\omega^{|\gamma|}\omega_\infty^{sgn(\gamma)}}, \pmod{q^{\mathbb{Z}}}$$

for all $\gamma \in R^\times$.

Proof. See the proof of Lemma 3.7 in [11]. □

Note that $\log_q(q^{\mathbb{Z}})$=0, and we can write

$$\int^{\tau} \int_x^y \omega_f = \log_q(\times\!\!\!\!\!\!\int^{\tau} \int_x^y \omega_f).$$

3.4 Darmon points

We now define Darmon points using indefinite integrals above. Since p is inert in F, the set $\mathcal{H}_p \cap F$ is non-empty. The order associated to $\tau \in \mathcal{H}_p \cap F$ is defined to be

$$\mathcal{O}_\tau = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R \text{ such that } a\tau + b = c\tau^2 + d\tau \right\}.$$

Via the map $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto c\tau + d$, $\mathcal{O}_\tau$ is identified with a $\mathbb{Z}[1/p]$-order of F. Given $\tau \in \mathcal{H}_p \cap F$, let γ_τ=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ denote the unique generator for the stabiliser of τ in Γ satisfying c$\tau + d$ >1 (with respect to the chosen embedding $F \subset \bar{\mathbb{Q}}$). Let Φ_{Tate}: $\mathbb{C}_p/q^{\mathbb{Z}} \to E(\mathbb{C}_p)$ denote the Tate uniformisation of E at p. We associate to τ a multiplicative and an additive period by choosing any base point $x \in \mathbb{P}^1(\mathbb{Q}_p)$ and setting

$$J_\tau^\times := \times\!\!\!\!\!\!\int^{\tau} \int_x^{\gamma_\tau x} \omega_f \in \mathbb{C}_p, \qquad J_\tau := \log_q(J_\tau^\times) = \int^{\tau} \int_x^{\gamma_\tau x} \omega_f.$$

The image of $J_\tau^\times$ under Φ_{Tate} is well-defined in $E(\mathbb{C}_p)\otimes\mathbb{Q}$, and is called the Darmon point attached to τ and f:

$$P_\tau := \Phi_{\mathrm{Tate}}(J_\tau^\times); \quad \log_E(P_\tau) = J_\tau.$$

3.5 Shimura reciprocity law

Fix an integer c prime to $D \cdot N$ and let $\mathcal{O}_c$ be the order of F of conductor c. Let $\mathcal{Q}_{Dc^2}$ denote the set of primitive binary quadratic forms $Ax^2 + Bxy + Cy^2$ of discriminant Dc^2. The group $\mathbf{SL}_2(\mathbb{Z})$ acts from the right on the set $\mathcal{Q}_{Dc^2}$ via the formula

$$(Q \mid \gamma)(x,y) = Q(ax+by, cx+dy), \quad Q \in \mathcal{Q}_{Dc^2} \text{ and } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}). \tag{3.5.1}$$

The set of $\mathbf{SL}_2(\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms of discriminant Dc^2 is equipped with the group structure given by Gaussian composition law. If H_c^+ is the strict ring class field of F of conductor c, then its Galois group $G_c^+ = \mathrm{Gal}(H_c^+/F)$ is isomorphic to the group $\mathcal{Q}_{Dc^2}/\mathbf{SL}_2(\mathbb{Z})$ via global class field theory([9], Theorem 14.19).

The modified Heegner hypothesis implies that there exists an element $\delta \in \mathbb{Z}$ satisfying

$$\delta^2 \equiv D \pmod{4M}.$$

Fix such a δ and let $\mathcal{F}_{Dc^2}$ denote the subset of $\mathcal{Q}_{Dc^2}$ consisting of forms $Q(x,y) = Ax^2 + Bxy + Cy^2$ such that

$$M \mid A \quad \text{and} \quad B \equiv \delta \pmod{2M}.$$

The group $\Gamma_0(M)$ acts on the set $\mathcal{F}_{Dc^2}$ by the formula 3.5.1. The natural map

$$\mathcal{F}_{Dc^2}/\Gamma_0(M) \to G_c^+ \cong \mathcal{Q}_{Dc^2}/\mathbf{SL}_2(\mathbb{Z})$$

obtained by sending the class of the quadratic form $Q = Ax^2 + Bxy + Cy^2$ to its corresponding $\mathbf{SL}_2(\mathbb{Z})$-equivalence class is seen to be a bijection and hence $\mathcal{F}_{Dc^2}/\Gamma_0(M)$

is endowed with the structure of a principal homogeneous space under G_c^+. If $Q \in \mathcal{F}_{Dc^2}/\Gamma_0(M)$ and $\sigma \in G_c^+$, write Q^σ for the image of Q by σ.

Define

$$\mathcal{H}_p^{Dc^2} = \{\tau \in \mathcal{H}_p \cap F \mid \mathcal{O}_\tau = \mathcal{O}_c\}.$$

Given $Q = Ax^2 + Bxy + Cy^2 \in \mathcal{F}_{Dc^2}$, let

$$\tau_Q := \frac{-B + c\sqrt{D}}{2A}$$

be a fixed root of the quadratic polynomial $Q(x,1)$. Note that τ_Q belongs to $\mathcal{H}_p^{Dc^2}$, and that its image in $\Gamma \setminus \mathcal{H}_p^{Dc^2}$ is well-defined. Given $\sigma \in G_c^+$, write $\tau_Q^\sigma \in \mathcal{H}_p^{Dc^2}$ for the root of any quadratic form in the $\Gamma_0(M)$-equivalence class of τ_{Q^σ}.

Let P be a point in $E(H_c^+)$. Since p is inert in F, it splits completely in H_c^+, and therefore, after fixing a prime of H_c^+ above p, the point P localizes to a point in $E(F_p)$, where F_p is the completion of F at unique prime above p.

Denote by $\tau_p \in \mathrm{Gal}(H_c^+/\mathbb{Q})$ the Frobenius element at p. Since the prime p is inert in F, the element τ_p, which is only defined up to conjugation, corresponds to a reflection in the dihedral group $\mathrm{Gal}(H_c^+/\mathbb{Q})$. This reflection corresponds to the involution in $\mathrm{Gal}(F_p/\mathbb{Q}_p)$ after fixing an embedding $H_c^+ \to F_p$. Proposition 5.10 of [11] asserts there exists an $\sigma_\tau \in G_c^+$ satisfying

$$\tau_p(J_\tau) = -\omega_M J_{\tau^{\sigma_\tau}} \tag{3.5.2}$$

and

$$\tau_p(P_\tau) = \omega_N P_{\tau^{\sigma_\tau}}$$

where ω_M and ω_N are the signs of the Atkin-Lehner involution W_M and W_N, respectively, acting on f.

τ_p does not commute with Φ_{Tate} in general, but rather satisfies

$$\tau_p \Phi_{\mathrm{Tate}} \tau_p = a_p \Phi_{\mathrm{Tate}} = -\omega_p \Phi_{\mathrm{Tate}}.$$

Conjecture 3.5.1. The Darmon point $P_{\tau Q}$ is the localization of a global point P_c, defined over H_c^+, and the Galois action on this point is described by the following Shimura reciprocity law: if $P_c \in E(H_c^+)$ localizes to $P_{\tau_Q} \in E(F_p)$ then P_c^σ localizes to $P_{\tau_q^\sigma}$.

Chapter 4

Hida theory

4.1 Hida families

This chapter gives the definition of the indefinite integral and of Darmon points in terms of periods attached to Hida families.

Definition 4.1.1. A profinite group is a topological group G which is Hausdorff and compact, and which admits a basis of neighbourhoods of $1 \in G$ consisting of normal subgroups.

The Iwasawa algebra, usually denoted by Λ, is the complete group algebra $\mathbb{Z}_p[[G]]$ of a profinite group G, which is noncanonically isomorphic to $\mathbb{Z}_p$. More details about Iwasawa algebras and Iwasawa modules can be found in Chapter V of [45].

Let

$$\tilde{\Lambda} := \mathbb{Z}_p[[\mathbb{Z}_p^\times]], \quad \Lambda = \mathbb{Z}_p[[(1+p\mathbb{Z}_p)^\times]]$$

denote the usual Iwasawa algebras, and let

$$\mathcal{X} = \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

be the space of continuous p-adic characters of $\mathbb{Z}_p$, equipped with its natural p-adic topology. Elements of $\mathcal{X}$ can also be viewed as continuous algebra homomorphisms from $\tilde{\Lambda}$ to $\mathbb{Z}_p$. The set $\mathbb{Z}$ embeds naturally in $\mathcal{X}$ by the rule

$$k \mapsto x_k, \text{ with } x_k(t) = t^{k-2} \text{ for } t \in \mathbb{Z}_p^\times.$$

Note that with these conventions, the element 2 corresponds to the augmentation map on $\tilde{\Lambda}$ and Λ.

If $U \subset \mathcal{X}$ is an open subset of $\mathcal{X}$, then $\mathcal{A}(U)$ denote the collection of analytic functions on U, i.e, the collection of functions which can be expressed as a power series on each intersection $U \cap (\{a\} \times \mathbb{Z}_p)$, $a \in \mathbb{Z}/(p-1)\mathbb{Z}$. Assume that U is contained in the residue disk of 2, then $\mathcal{A}(U)$ is simply the ring of power series that converge on an open set of $\mathbb{Z}_p$.

A Hida family is a formal q-expansion

$$f_\infty = \sum_{n=1}^{\infty} a_n(k) q^n, \quad a_n(k) \in \mathcal{A}(U),$$

satisfying the following properties. Let $\mathbb{Z}^{\geqslant 2}$ denote the set of integers which are $\geqslant 2$:

1. If k belongs to $U \cap \mathbb{Z}^{\geqslant 2}$, the q-expansion

$$f_k := \sum_{n=1}^{\infty} a_n(k) q^n$$

is a normalised eigenform of weight k on $\Gamma_0(N)$. It is new at the primes dividing $M = N/p$. It is referred to as the weight k specialisation of f_∞. More precisely, if $k \in U \cap \mathbb{Z}^{>2}$, the modular form f_k arises from a normalised newform on $\Gamma_0(M)$, denoted $f_k^\sharp = \sum_n a_n(f_k^\sharp) q^n$. If $(p,n) = 1$, then $a_n(f_k^\sharp) = a_n(f_k)$. Letting

$$1 - a_p(f_k^\sharp) p^{-s} + p^{k-1-2s} = (1 - \alpha_p(k) p^{-s})(1 - \beta_p(k) p^{-s})$$

denote the Euler factor at p that appears in the L-series of $f_k^\sharp$, we may order the roots $\alpha_p(k)$ and $\beta_p(k)$ in such a way that

$$\alpha_p(k) = a_p(f_k), \quad \beta_p(k) = p^{k-1} a_p(f_k)^{-1}.$$

With this convention, we have

$$f_k(z) = f_k^\sharp(z) - \beta_p(k) f_k^\sharp(pz).$$

2. For $k = 2$, let $f_2 = f$.

The field F_{f_k} generated by the Fourier coefficient of the normalised eigenform f_k is a finite extension of $\mathbb{Q}$. For each $k \in U \cap \mathbb{Z}^{\geq 2}$, we choose the Shimura periods $\Omega_k^+ := \Omega_{f_k}^+$

and $\Omega_k^- := \Omega_{f_k}^-$ as in 3.1.5, requiring that

$$\Omega_2^+\Omega_2^- = \langle f, f\rangle, \quad \Omega_k^+\Omega_k^- = \langle f_k^\sharp, f_k^\sharp\rangle \ (k > 2).$$

Thanks to these periods we may talk about the $V_k(\mathbb{C}_p)$-valued modular symbols $I_{f_k}^+$ and $I_{f_k}^-$ associated to each f_k.

4.2 Periods attached to Hida families

Let $L_*{=}\mathbb{Z}_p^2$ denote the standard $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$, and let $L_*^{'}$ denote its set of primitive vectors, i.e, the vectors in L_* which are not divisible by p. Let $\mathbb{D}$ denote the space of compactly supported $\mathbb{Q}_p$-valued measures on $\mathcal{W}{:=}\mathbb{Q}_p^2$-$\{(0,0)\}$, and let $\mathbb{D}_*$ denote the subspace of measures that are supported on $L_*^{'}$. The group $\mathbb{Z}_p^\times$ acts on $\mathcal{W}$ and $L_*^{'}$ by the rule: $\lambda(x,y) = (\lambda x, \lambda y)$, for $\lambda \in \Lambda$, which defines the Λ and $\tilde{\Lambda}$ module structure on $\mathbb{D}$ and $\mathbb{D}_*$. The module $\mathbb{D}$ is also equipped with a right $\tilde{\Lambda}$-linear action of $\mathbf{GL}_2(\mathbb{Q}_p)$ defined by the rule

$$\int_{\mathcal{W}} F d(\gamma|\mu) = \int_{\gamma^{-1}\mathcal{W}} (F|\gamma) d\mu$$

where $\mathbf{GL}_2(\mathbb{Q}_p)$ operates on the continuous functions on $\mathcal{W}$ by the rule:

$$(F|\gamma) := F(ax+by, cx+dy), \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Let $\Gamma_0(p\mathbb{Z}_p)$ be the group of matrices in $\mathbf{GL}_2(\mathbb{Z}_p)$ which are upper triangular modulo p. For all $k \in \mathbb{Z}^{\geq 2}$, there is a $\Gamma_0(p\mathbb{Z}_p)$-equivariant homomorphism

$$\rho_k : \mathbb{D}_* \to V_{k-2}(\mathbb{C}_p).$$

defined by

$$\rho_k(\mu)(P(x,y)) := \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P(x,y) d\mu(x,y).$$

which induces a $\Gamma_0(p\mathbb{Z}_p)$-equivariant map

$$\rho_k : \mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*) \to \mathrm{MS}_{\Gamma_0(N)}(V_k(\mathbb{C}_p)).$$

where the space $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$ is equipped with a natural action of the Hecke operators and of the operator U_p. Let $\mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)$ denote the largest submodule on which U_p acts invertibly and call this the ordinary subspace of $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$.

Recall the ring $\Lambda^\dagger \subset \Lambda$ of power series which converges in some neighbourhood of 2 $\in \mathcal{X}$, and set

$$\mathbb{D}_*^\dagger := \mathbb{D}_* \bigotimes_\Lambda \Lambda^\dagger.$$

Similar notations are adopted, with the obvious meanings, when $\mathbb{D}_*$ is replaced by $\mathbb{D}$. If

$$\mu = \lambda_1\mu_1 + \cdots + \lambda_t\mu_t, \quad \text{with } \lambda_i \in \Lambda^\dagger,\ \mu_i \in \mathbb{D}_*$$

is any element of $\mathbb{D}_*^\dagger$, then there exists a neighbourhood U_μ of $2 \in \mathcal{H}$ on which all the coefficients λ_i converge. We call such a region U_μ a neighbourhood of regularity for μ.

Given $k \in \mathbb{Z}$, a function F on $\mathcal{W}$ is said to be homogeneous of degree k, if $F(\lambda x, \lambda y)) = \lambda^k F(x, y)$ for all $\lambda \in \mathbb{Z}_p$. For any $k \in U_\mu \cap \mathbb{Z}^{\geq 2}$, and any homogeneous function $F(x, y)$ of degree $k-2$, one can integrate F against μ on any compact open region $X \subset \mathcal{W}$ by the rule

$$\int_X F d\mu := \lambda_1(k) \int_X F d\mu_1 + \cdots + \lambda_t(k) \int_X F d\mu_t.$$

The space $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$ is equipped with a natural action of the Hecke operators, including an operator U_p. More precisely, it is given by the formula

$$\int_X F d(U_p\mu)\{r \to s\} = \sum_{a=0}^{p-1} \int_{p^{-1}\gamma_a X} (F \mid p\gamma_a^{-1}) d\mu\{\gamma_a r \to \gamma_a s\}.$$

Proposition 6.1 of [22] shows the module $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$ is free of finite rank over Λ. Therefore the same is true of the $\Lambda^\dagger$-module

$$\mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger := \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*) \otimes_\Lambda \Lambda^\dagger.$$

Theorem 4.2.1. *There exists a $\mathbb{D}_*^\dagger$-valued modular symbol $\mu_* \in \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger$ such that*

1. $\rho_2(\mu_*) = I_f$;
2. *For all $k \in U_{\mu_*} \cap \mathbb{Z}^{\geq 2}$, there exists a scalar $\lambda(k) \in \mathbb{C}_p$ such that*

$$\rho_k(\mu_*)=\lambda(k)I_{f_k}.$$

Proof. This is Theorem 5.13 of [22] and the proof is explained in section 6 of that paper. □

Remark 4.2.2. Note that μ_* depends on the choice of sign $\pm$ and that there are two $\mathbb{D}_*^\dagger$-valued modular symbols, $\mu_*^\pm \in \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger$, such that $\rho_2(\mu_*^\pm) = I_f^\pm$ and for all integers $k \in U$, $k \geq 2$, there is $\lambda^\pm(k) \in \mathbb{C}_p$ such that $\rho_k(\mu_*^\pm) = \lambda^\pm(k)I_{f_k}^\pm$; also, U can be chosen so that $\lambda^\pm(k) \neq 0$ for all $k \in U$.

Proposition 4.2.3. *There is a neighbourhood U of $2 \in \mathcal{X}$, with $\lambda(k) \neq 0$, for all $k \in U \cap \mathbb{Z}^{\geq 2}$.*

Proof. See the proof of Proposition 1.7 in [3]. □

Define a collection of $\mathbb{D}^\dagger$-valued modular symbols μ_L indexed by the $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$. Recall the group defined as follows:

$$\Gamma=\left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}[1/p]) \text{ with } M|c, \det(\gamma) > 0\right\}.$$

Proposition 4.2.4. *There exists a unique collection $\{\mu_L\}$ of $\mathbb{D}^\dagger$-valued modular symbols, indexed by the $\mathbb{Z}_p$-lattices $L \subset \mathbb{Q}_p^2$ and satisfying:*

1. *$\mu_{L_*}=\mu_*$;*
2. *For all $\gamma \in \Gamma$, and all compact open $X \subset \mathcal{W}$,*

$$\int_{\gamma X}(F|\gamma^{-1})d\mu_{\gamma L}\{\gamma r \to \gamma s\} = \int_X F d\mu_L\{r \to s\}.$$

Proof. See the proof of Proposition 1.8 in [3]. □

Some properties of the measure μ_L are recorded in a sequence of lemmas.

Lemma 4.2.5. *Let L be a lattice and L' be its set of primitive. The distributions $\mu_L\{r \to s\}$ are supported on L', for all r,$s \in \mathbb{P}^1(\mathbb{Q})$.*

Proof. See the proof of Lemma 1.9 in [3]. □

Lemma 4.2.6. *Suppose that $L_2 \subset L_1$ is a sublattice of index p in L_1. Then for all $k \in U \cap \mathbb{Z}^{\geq 2}$, for all homogeneous functions F on $L_1^{'} \cap L_2^{'}$ of degree k-2, and for all r,$s \in \mathbb{P}_1(\mathbb{Q})$, we have*

$$\int_{L_1^{'} \cap L_2^{'}} F d\mu_{L_2}\{r \to s\} = a_p(k) \int_{L_1^{'} \cap L_2^{'}} F d\mu_{L_1}\{r \to s\}.$$

Proof. See the proof of Lemma 1.10 in [3]. □

4.3 Indefinite integrals revisited

The relevance of Hida families to Darmon points can be explained by the fact that the system of distribution-valued modular symbols $\mu_L\{r \to s\}$ can be used to give a direct formula for this indefinite integral.

When $\tau \in \mathcal{H}_p \cap F_p$, and hence is defined over a quadratic unramified extension of $\mathbb{Q}_p$. In that case, the function

$$(x, y) \mapsto x - \tau u$$

identifies $\mathbb{Q}_p^2$ with F_p. Let L_τ be the $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$ defined by

$$L_\tau = \{(x, y) \mid x - \tau y \in \mathcal{O}_F \otimes \mathbb{Z}_p\}.$$

Recall the notation in Chapter 3,

Theorem 4.3.1. *For all $\tau \in \mathcal{H}_p \cap F_p$, and for all r,$s \in \mathbb{P}$,*

$$\int^{\tau} \int_r^s \omega_f = \int_{L_\tau^{'}} \log(x - \tau y) d\mu_{L_\tau}\{r \to s\}(x, y),$$

where $\log : F_p^\times \to F_p$ *is any branch of the p-adic logarithm.*

Corollary 4.3.2. *The Darmon point P_{τ_Q} associated to*

$$Q \in \mathcal{F}_{Dc^2}/\Gamma_0(M)$$

satisfies

$$\log_E P_{\tau_Q} = J_\tau = \int_{(\mathbb{Z}_p^2)'} \log(x - \tau r) d\mu_*\{r \to \gamma_\tau r\}(x, y).$$

Proof. See the proof of Theorem 2.5 and Corollary 2.6 in [4]. □

Theorem 4.3.3. *If* $Q \in \mathcal{F}_{Dc^2}$, *then*

$$\log_E(P_{\tau_Q}) = \int_{(\mathbb{Z}_p^2)'} \log_E(x - \tau_Q y) d\mu_*^{\pm}\{r \to s\}(x, y).$$

Proof. This follows from 4.3.1 as in 4.3.2 noticing that the set

$$\{(x, y) \in \mathbb{Q}_p^2 \mid x - \tau_Q y \in \mathcal{O}_K \otimes \mathbb{Z}_p\}$$

coincides with $\mathbb{Z}_p^2$. □

Chapter 5

Automorphic forms

In this chapter, we will review some basic knowledge about automorphic forms.

5.1 Haar measure and Tamagawa measure

Definition 5.1.1. Let X be a topological space. The ring $\mathbb{B}(X)$ of Borel sets on X is the smallest collection of subsets of X such that:

(1) every open subset of X is in $\mathbb{B}(X)$,

(2) $\bigcup\limits_{i=1}^{\infty} A_i \in \mathbb{B}(X)$, whenever $A_i \in \mathbb{B}(X)$ for $i = 1, 2, \ldots,$

(3) $A \cap (X - B) \in \mathbb{B}(X)$ whenever $A, B \in \mathbb{B}(X)$.

Definition 5.1.2. Let G be a locally compact group. A left Haar measure, $d_L : \mathbb{B}(G) \to [0, \infty]$ is a measure, defined on the ring of Borel sets such that:

(1) no open set has measure 0,

(2) no compact set has measure ∞,

(3) $d_L(U) = \sup\{d_L(K) \mid K$ is compact, and $K \subset U\}$ for all open sets U,

(4) $d_L(A) = \inf\{d_L(U) \mid U$ is open, and $A \subset U\}$ for all $A \in \mathbb{B}(G)$,

and d_L satisfies the invariance property

$d_L(g.S) = d_L(S)$, $\forall g \in G, S \in \mathbb{B}(G)$.

A right Haar measure is defined in the same way, except that the action is from the right.

Theorem 5.1.3. *Let G be a locally compact group. Then there exists left (right) Haar measure $\mathbb{B}(G) \to [0, \infty]$, which is unique up to scalars.*

Proof. See 15.8 in [31]. □

Definition 5.1.4. A locally compact group G is unimodular if there is a nonzero constant C such that $d_R g = C d_L g$.

Theorem 5.1.5. *Let G be a locally compact abelian group. Then the set G^* of all continuous homomorphisms $g^* : G \to \mathbb{C}^\times$ with $\mid g^*(g) \mid = 1$ $(\forall g \in G)$ is a locally compact abelian group, called the Pontryagin dual of G, with the group law being*

$$(g_1^* \cdot g_2^*)(g) = g_1^*(g) \cdot g_2^*(g), \ (\forall g \in G, g_1^*, g_2^* \in G^*),$$

and the topology being the compact-open topology. Furthermore $(G^*)^* \cong G$.

Proof. See the section 24 in [31]. □

Let G be a commutative locally compact group, G^* its dual. For $g^* \in G^*$ a character of G, its value at a point g of G is written as $\langle g, g^* \rangle$. Let ϕ be a continuous function on G, integrable for a Haar measure $d_L g$, given on G. Then the function ϕ^* defined on G^* by

$$\phi^*(g^*) = \int_G \phi(g) \langle g, g^* \rangle d_L g$$

is called the Fourier transform of ϕ with respect to $d_L g$. By the theory of Fourier transforms, there is a Haar measure $d_L^* g$ on G^*, such that the function ϕ^* is integrable on G^*, and ϕ is given by

$$\phi(g) = \int_{G^*} \phi^*(g^*) \langle -g, g^* \rangle d_L^* g^*.$$

This measure d_L^* is called the dual measure to d_L. In particular, assume that G^* has been identified with G via some isomorphism of G onto G^*, then $d_L^* = m d_L$, with some $m \in \mathbb{R}_+^\times$ and there is a unique Haar measure on G such that $d_L^* = d_L$. In this case, when $G \cong G^*$, we call $d_L g$ the self-dual Haar measure on G.

Remark 5.1.6. For more information about Haar measure and topological groups, people can see [31] for details.

Let V be an algebraic variety of dimension n, defined over F. Let x^0 be a point of V and $x_1, \cdots, x_n$ be local coordinates on V at x^0. A differential n-form on V is defined in a neighbourhood of x^0 in V as follows:

$$\omega = f(x) dx_1 \cdots dx_n$$

where f is a rational function on V which is defined at x^0. The form ω is said to be defined over F if f and the coordinate functions x_i are defined over F.

Let v denote a prime of F. Let G be a connected algebraic group over F and F_v be the completion F at v. We shall use ω to construct measure ω_v on the local group G_{F_v} where G_{F_v} is the set of points of G with coordinates in F_v.

The rational function f can be written as a formal power series in $t_i = x_i - x_i^0$ with coefficients in F. If x_i^0 are in F_v then f is a power series in the x_i with coefficients in F_v which converges in some neighbourhood of the origin in F_v^n. Hence there is a neighbourhood U of x^0 in G_{F_v} such that $\varphi : x \mapsto (t_1 \ldots t_n)$ is a homeomorphism of U onto a neighbourhood $\varphi(U)$ of the origin in F_v^n and the power series above converges in $\varphi(U)$. In $\varphi(U)$, we have the positive measure $\mid f(t) \mid_v dt_1 \cdots dt_n$ (where $dt_1 \cdots dt_n$ is the product measure $\mu_v \times \cdots \times \mu_v$ on F_v^n); pull this back to U by means of φ and we have a positive measure ω_v on U. Explicitly, if g is a continuous real-valued function on G_{F_v} with compact support, then

$$\int_U g\omega_v = \int_{\varphi(U)} g(\varphi^{-1}(t)) \mid f(t) \mid_v dt_1 \cdots dt_n.$$

The measure $\omega_v$is independent of the choice of local coordinates x_i.

Let $G_{\mathfrak{o}_v}$ be the compact subgroups of G_{F_v}. If the product

$$\prod_{v \neq \infty} \omega_v(G_{\mathfrak{o}_v})$$

converges absolutely, we define the Tamagawa measure by

$$\tau = \prod_v \omega_v.$$

More details are explained in the Chapter 2 of [55] and Chapter 10 of [7].

5.2 The adèle group $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$

Denote by $\mathbb{A}_\mathbb{Q}$ the adèle ring of $\mathbb{Q}$. The center of $\mathbb{A}_\mathbb{Q}$ is denoted by $Z_\mathbb{A}$:

$$Z_\mathbb{A} = \left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} : t \in \mathbb{A}_\mathbb{Q}^\times \right\}.$$

The adèle group $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ is the restricted product (relative to the maximal compact subgroups $U_p = \mathbf{GL}_2(\mathbb{Z}_p)$)

$$\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}) = \mathbf{GL}_2(\mathbb{R}) \times \prod_p{}' \mathbf{GL}_2(\mathbb{Q}_p)$$

where restricted product (relative to the subgroups U_p) means that all but finitely many of the components in the product are in U_p. An element $g \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ will be denoted in the forms

$$g = \{g_v\}_{v \le \infty} = \{g_\infty, \cdots, g_p, \cdots\}$$

where $g_v \in \mathbf{GL}_2(\mathbb{Q}_v)$ for all $v \le \infty$ and $g_p \in U_p$ for all but finitely many primes p.

Given $g, g' \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$, we define multiplication of these elements as follows:

$$gg' = \{g_\infty g'_\infty, \cdots, g_p g'_p, \cdots\},$$

where $g_v \cdot g'_v$ simply denotes matrix multiplication in $\mathbf{GL}_2(\mathbb{Q}_v)$ for all $v \le \infty$.

5.3 The action of $\mathbf{GL}_2(\mathbb{Q})$ on $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$

The group $\mathbf{GL}_2(\mathbb{Q})$ may be diagonally embedded in $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ as follows:

$$i : \mathbf{GL}_2(\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{A}_\mathbb{Q}) \qquad \gamma \mapsto \{\gamma, \gamma, \cdots\}.$$

We also define the embedding at ∞ by the rule

$$i_\infty : \mathbf{GL}_2(\mathbb{R}) \to \mathbf{GL}_2(\mathbb{A}_\mathbb{Q}) \qquad \alpha \mapsto \left\{ \alpha, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \cdots, \right\}.$$

The group $i(\mathbf{GL}_2(\mathbb{Q}))$ acts from the left on $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ by matrix multiplication.

Definition 5.3.1. Let $L^2(\mathbf{GL}_2(\mathbb{Q}) \setminus \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}}))$ denote the Hilbert space of measurable function f on $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ such that

(1)$f(\gamma g) = f(g)$ for all $\gamma \in \mathbf{GL}_2(\mathbb{Q})$;

(2)$f(gz) = f(g)\chi(z)$ for all $z \in Z_{\mathbb{A}}$;

(3) $\int_{Z_{\mathbb{A}}\mathbf{GL}_2(\mathbb{Q})\setminus\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})} \mid f(g) \mid^2 dg < \infty.$

5.4 Adèlic automorphic forms

We regard automorphic forms as the $\mathbb{C}$-valued functions f on $\mathbf{GL}_2(\mathbb{Q}) \setminus \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ which satisfy additional conditions.

Definition 5.4.1. A $\mathbb{C}$-valued function f on $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ is said to be smooth if for every fixed $g_0 \in \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$, there exists an open set U of $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$, containing g_0, and a smooth function f_U^{∞}: $\mathbf{GL}_2(\mathbb{R}) \to \mathbb{C}$ such that $f(g) = f_U^{\infty}(g_{\infty})$ for all $g \in U$.

Definition 5.4.2. Let $O(2, \mathbb{R})$ be the orthogonal group. Write $K = O(2, \mathbb{R}) \prod_p \mathbf{GL}_2(\mathbb{Z}_p)$ which is a maximal compact subgroup of $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$. A function $f : \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{C}$ is said to be right K-finite if the set

$$\{f(gk) \mid k \in K\},$$

of all right translate of $f(g)$ generates a finite dimensional vector space.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ where $a, b, c, d \in \mathbb{A}_{\mathbb{Q}}$. Define a norm function by

$$|| g ||:= \prod_{v \leq \infty} max\{| a_v |_v, | b_v |_v, | c_v |_v, | d_v |_v, | a_v d_v - b_v c_v |_v^{-1}\}.$$

Definition 5.4.3. f is said to be moderate growth if there exists constants $n, c \geq 0$ such that

$$| f(g) |\leq c \, || g ||^n$$

for all $g \in \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$.

Let $\mathfrak{g} = \mathfrak{gl}(2, \mathbb{R})$. Let $U(\mathfrak{g})$ be the universal enveloping algebra of $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$.

Definition 5.4.4. Let $Z(\mathfrak{g})$ denote the center of $U(\mathfrak{g})$. A smooth function

$$f : \mathbf{GL}_2(\mathbb{Q}) \setminus \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}}) \to \mathbb{C}$$

is said to be $Z(\mathfrak{g})$-finite if the set $\{Df(g) \mid D \in Z(\mathfrak{g})\}$ generates a finite dimensional vector space.

Definition 5.4.5. A Hecke character of $\mathbb{A}_{\mathbb{Q}}^{\times}$ is defined to be a continuous homomorphism

$$\chi : \mathbb{Q}^{\times} \setminus \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{C}^{\times}.$$

A Hecke character is said to be unitary if all its values have absolute value 1.

A unitary Hecke character of $\mathbb{A}_{\mathbb{Q}}^{\times}$ is characterized by the following four properties:

(1) $\chi(gg') = \chi(g)\chi(g')$, $(\forall g, g' \in \mathbb{A}_{\mathbb{Q}}^{\times})$;

(2) $\chi(\gamma g) = \chi(g)$, $(\forall \gamma \in \mathbb{Q}^{\times}, \forall g \in \mathbb{A}_{\mathbb{Q}}^{\times})$;

(3) χ is continuous at $\{1, 1, 1, \cdots\}$;

(4) $| \chi(g) |= 1$, $\forall g \in G$.

Now we will give the definition of an automorphic form for the adèle group.

Definition 5.4.6. Fix a unitary Hecke character $\chi : \mathbb{Q}^{\times} \setminus \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{C}^{\times}$. A function f on $\mathbf{GL}_2(\mathbb{Q}) \setminus \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ is called an automorphic form with a central character χ if

(1) f is smooth.

(2) $f(zg) = \chi(z)f(g)$, $(\forall g \in \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}}), z \in \mathbb{A}_{\mathbb{Q}}^{\times})$.

(3) f is right K-finite, K is defined above.

(4) f is of moderate growth.

(5) f is $Z(\mathfrak{g})$-finite.

Definition 5.4.7. For each unitary Hecke character χ, let $\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}}), \chi)$ be the $\mathbb{C}$-vector space of all adèlic automorphic forms for $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ with central character χ.

Definition 5.4.8. An adèlic automorphic form f is called a cusp form if

$$\int_{\mathbb{Q}\setminus\mathbb{A}_{\mathbb{Q}}} f\left(\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} g\right) du = 0$$

for all $g \in \mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$. Here $u \in \mathbb{A}_{\mathbb{Q}}$ and du is the Haar measure on $\mathbb{A}_{\mathbb{Q}}$.

5.5 Automorphic representations

Definition 5.5.1. The ring of finite adèles over $\mathbb{Q}$, denoted $\mathbb{A}_f$, is defined as follows:

$$\mathbb{A}_f = \{(x_v) : x_v = 1 \text{ if } v = \infty\} \subset \mathbb{A}.$$

Fix a unitary Hecke character χ. Recall that a representation is determined by a vector space and linear actions on the vector space. We are going to define three actions, two of them using right translation by suitable elements and a third one will be a Lie algebra action. In this section, we will explain these actions and these following three actions form the foundation for the construction of automorphic representations:

Define an action $\pi_f : \mathbf{GL}_2(\mathbb{A}_f) \to \mathrm{GL}(\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi))$. For $\phi \in \mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$:

$$\pi_f(a_f).\phi(g) := \phi(ga_f),$$

for all $g \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$, $a_f \in \mathbf{GL}_2(\mathbb{A}_f)$. Here, $\pi_f(a_f).\phi$ denotes the action of a_f on the vector ϕ.

Define an action $\pi_{K_\infty} : K_\infty \to GL(\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi))$ as follows. The group $K_\infty = O(2, \mathbb{R})$ can be embedded in $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ If $k_\infty \in K_\infty$, then $\left\{ k_\infty, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \dots \right\}$ is an element of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$. Let $\phi \in \mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$ and define

$$\pi_{K_\infty}(k).\phi(g) := \phi(gk),\ g \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q}),$$

where $k = \left\{ k_\infty, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \dots \right\}$, with $k_\infty \in K_\infty$. Here $\pi_{K_\infty}(k).\phi$ denotes the action of k on the vector ϕ.

Before explaining the action of $U(\mathfrak{g})$, we need to introduce some definitions.

Definition 5.5.2. Let $\alpha \in \mathfrak{gl}_2(\mathbb{R})$ and $F : \mathbf{GL}_2(\mathbb{R}) \to \mathbb{C}$, a smooth function. The we define a differential operator D_α acting on F by the rule:

$$D_\alpha F(g) := \frac{\partial}{\partial t} F(g \cdot \exp(t\alpha)) \mid_{t=0} = \frac{\partial}{\partial t} F(g + t(g \cdot \alpha)) \mid_{t=0} .$$

Remark 5.5.3. Recall that $\exp(t\alpha) = I + \sum_{k=1}^{\infty} \frac{(t\alpha)^k}{k!}$, where I denotes the identity matrix on $\mathfrak{gl}_2(\mathbb{R})$. Since we are differentiating with respect to t and then setting $t = 0$, only the first two terms for $\exp(t\alpha)$ matter.

We may extend the action of $\mathfrak{gl}_2(\mathbb{R})$ on smooth functions $F : \mathbf{GL}_2(\mathbb{R}) \to \mathbb{C}$ to an action of the complexification $\mathfrak{gl}_2(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} = \mathfrak{gl}_2(\mathbb{C})$, as follows:

Definition 5.5.4. Let $\beta \in \mathfrak{gl}_2(\mathbb{R})$ and $F : \mathbf{GL}_2(\mathbb{R}) \to \mathbb{C}$, a smooth function. Then we define a differential operator $D_{i\beta}$ acting on F by the rule:

$$D_{i\beta}F(g) := iD_\beta F(g).$$

More generally, if $\alpha + i\beta \in \mathfrak{gl}_2(\mathbb{C})$, with $\alpha, \beta \in \mathfrak{gl}_2(\mathbb{R})$, then

$$D_{\alpha+i\beta} = D_\alpha + iD_\beta.$$

The differential operator $D_{\alpha+i\beta}$ generate an algebra of differential operators which is isomorphic to the universal enveloping algebra $U(\mathfrak{g})$(Chapter 4 in [18]).

Now we can define the action of $U(\mathfrak{g})$ by differential operators.

Let $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{C})$ and $D \in U(\mathfrak{g})$ be a differential operator as defined above. We may define an action $\pi_\mathfrak{g}$ of $U(\mathfrak{g})$ on the vector space $\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$ as follows. For $\phi \in \mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$ let

$$\pi_\mathfrak{g}(D).\phi(g) := D\phi(g), \quad g \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q}),$$

where $\pi_\mathfrak{g}(D).\phi$ denotes the action of D on $\phi(g)$, which is given by the differential operator D acting in the variable g_∞.

Remark 5.5.5. The action of the finite adèles by right translation commutes with the action of $O(2,\mathbb{R})$ and the action of the $U(\mathfrak{g})$. The action of $O(2,\mathbb{R})$ and the action of $U(\mathfrak{g})$ do not commute, but satisfy the relation $\pi_\mathfrak{g}(D_\alpha).\pi_{K_\infty}(k) = \pi_{K_\infty}(k).\pi_\mathfrak{g}(D_{k^{-1}\alpha k})$.

Remark 5.5.6. The action of the finite adèle by right translation defines a group representation of $\mathbf{GL}_2(\mathbb{A}_f)$. The action of $K_\infty = O(2,\mathbb{R})$ by right translation defines a group representation of K_∞. The action of $U(\mathfrak{g})$ does not define a group representation because $U(\mathfrak{g})$ is not a group.

The space $\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$ is preserved by these three actions. The details are discussed in [18].

Now we can define the following two important types of modules.

Definition 5.5.7. Let $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{C})$, $K_\infty = O(2, \mathbb{R})$, and $U(\mathfrak{g})$ denote the universal enveloping algebras. We define a $(\mathfrak{g}, K_\infty)$-module to be a complex vector space V with actions

$$\begin{aligned} \pi_{\mathfrak{g}} : U(\mathfrak{g}) \to \ & \mathrm{End}(V), \\ \pi_{K_\infty} : K_\infty \to \ & \mathrm{GL}(V), \end{aligned}$$

such that, for each $v \in V$, the subspace of V spanned by $\{\pi_{K_\infty}(k).v \mid k \in K_\infty\}$ is finite dimensional, and the actions $\pi_{\mathfrak{g}}$ and π_{K_∞} satisfy the relations

$$\pi_{\mathfrak{g}}(D_\alpha).\pi_{K_\infty}(k) = \pi_{K_\infty}(k).\pi_{\mathfrak{g}}(D_{k^{-1}\alpha k})$$

for $\alpha \in \mathfrak{g}$, D_α, and all $k \in K_\infty$. Further, we require that

$$\pi_{\mathfrak{g}}(D_\alpha).v = \lim_{t \to 0} \frac{1}{t}(\pi_{K_\infty}(\exp(t\alpha)).v - v)$$

for all $v \in V$ and α in the Lie algebra of K_∞, which is contained in $\mathfrak{g}$.

We shall denote the pair of actions $(\pi_{\mathfrak{g}}, \pi_{K_\infty})$ by π and shall also refer to the ordered pair (π, V) as a $(\mathfrak{g}, K_\infty)$-module.

Definition 5.5.8. Let $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{C})$ and let $K_\infty = O(2, \mathbb{R})$. Also let $\mathbf{GL}_2(\mathbb{A}_f)$ denote the finite adèles. We define a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module to be a complex vector space V with actions

$$\begin{aligned} \pi_{\mathfrak{g}} : U(\mathfrak{g}) \to & \mathrm{End}(V), \\ \pi_{K_\infty} : K_\infty \to & \mathrm{GL}(V), \\ \pi_f : \mathbf{GL}_2(\mathbb{A}_f) \to & \mathrm{GL}(V), \end{aligned}$$

such that V, $\pi_{\mathfrak{g}}$ and π_{K_∞} form a $(\mathfrak{g}, K_\infty)$-module, and in addition the relations

$$\begin{aligned} \pi_f(a_f) \cdot \pi_{\mathfrak{g}}(D_\alpha) &= \pi_{\mathfrak{g}}(D_\alpha) \cdot \pi_f(a_f), \\ \pi_f(a_f) \cdot \pi_{K_\infty}(k) &= \pi_{K_\infty}(k) \cdot \pi_f(a_f), \end{aligned}$$

are satisfied for all $\alpha \in \mathfrak{g}$, $D_\alpha \in U_{\mathfrak{g}}$, $k \in K_\infty$, and $a_f \in \mathbf{GL}_2(\mathbb{A}_f)$.

We let $\pi = (\pi_{\mathfrak{g}}, \pi_{K_\infty}), \pi_f)$, and refer to the ordered pair (π, V) as a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module.

Definition 5.5.9. Let the complex vector space V be a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module. We say the $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module is smooth if every vector $v \in V$ is fixed by some open compact subgroup of $\mathbf{GL}_2(\mathbb{A}_f)$ under the action

$$\pi_f : \mathbf{GL}_2(\mathbb{A}_f) \to \mathrm{GL}(V).$$

The $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module is said to be irreducible if it is non-zero and has no proper non-zero subspaces preserved by the actions $\pi_\mathfrak{g}$, π_{K_∞}, π_f.

Now we define a type of morphism between these modules.

Definition 5.5.10. Let V, V' be complex vector spaces which are two $(\mathfrak{g}, K_\infty)$-modules with associated actions:

$$\pi_\mathfrak{g} : U(\mathfrak{g}) \to \mathrm{End}(V), \quad \pi'_\mathfrak{g} : U(\mathfrak{g}) \to \mathrm{End}(V'),$$
$$\pi_{K_\infty} : K_\infty \to \mathrm{GL}(V), \quad \pi'_{K_\infty} : K_\infty \to \mathrm{GL}(V').$$

A linear map $L : V \to V'$ is said to be intertwining if

$$L \circ \pi_\mathfrak{g}(D) = \pi'_\mathfrak{g}(D) \circ L, \quad (\forall D \in U(\mathfrak{g})), \qquad L \circ \pi_{K_\infty}(k) = \pi'_{K_\infty}(k) \circ L, \quad (\forall k \in K_\infty).$$

If the linear map L is an isomorphism, then we say the two $(\mathfrak{g}, K_\infty)$-modules are isomorphic.

Definition 5.5.11. Let V, V' be complex vector spaces which are two $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-modules with associated actions:

$$\pi_\mathfrak{g} : U(\mathfrak{g}) \to \mathrm{End}(V), \quad \pi'_\mathfrak{g} : U(\mathfrak{g}) \to \mathrm{End}(V'),$$
$$\pi_{K_\infty} : K_\infty \to \mathrm{GL}(V), \quad \pi'_{K_\infty} : K_\infty \to \mathrm{GL}(V').$$
$$\pi_f : \mathbf{GL}_2(\mathbb{A}_f) \to \mathrm{GL}(V), \, \pi'_f : \mathbf{GL}_2(\mathbb{A}_f) \to \mathrm{GL}(V')$$

A linear map $L : V \to V'$ is said to be intertwining if

$$L \circ \pi_\mathfrak{g}(D) = \pi'_\mathfrak{g}(D) \circ L, \quad (\forall D \in U(\mathfrak{g})),$$
$$L \circ \pi_{K_\infty}(k) = \pi'_{K_\infty}(k) \circ L, \quad (\forall k \in K_\infty),$$
$$L \circ \pi_f(a_f) = \pi'_{\mathbb{A}_f}(a_f) \circ L, \quad (\forall a_f \in \mathbf{GL}_2(\mathbb{A}_f)).$$

If L is an isomorphism, then we say the two $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-modules are isomorphic. Sometimes these maps are called intertwining operators.

Let V be a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module with actions: $\pi_\mathfrak{g}$, π_{K_∞}, π_f, which is defined above.

Let $W' \subset W \subset V$ be vector subspaces of V. If W, W' are closed under the action of $\pi_\mathfrak{g}$, π_{K_∞}, π_f, then W/W' is equipped with a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module structure as follows. Let $w + W'$ denote a coset in W/W' with $w \in W$. Then for all $w \in W$, $D \in U(\mathfrak{g})$, $k \in K_\infty$ and $a_f \in \mathbf{GL}_2(\mathbb{A}_f)$, we may define

$$\pi_\mathfrak{g}(D).(w + W') := \pi_\mathfrak{g}(D).w + W',$$
$$\pi_{K_\infty}(k).(w + W') := \pi_{K_\infty}(k).w + W',$$
$$\pi_f(a_f).(w + W') := \pi_f(a_f).w + W'.$$

These actions define a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module which is called a subquotient of V.

Definition 5.5.12. Fix a unitary Hecke character $\chi : \mathbb{Q}^\times \setminus \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}$. An automorphic representation with central character χ is defined to be a smooth $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module which is isomorphic to a subquotient of the complex vector space of adèlic automorphic forms $\mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$.

Definition 5.5.13. Fix a unitary Hecke character $\chi : \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}$. Let $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{C})$ and $K_\infty = O(2, \mathbb{R})$. We define a cuspidal automorphic representation with central character χ to be a smooth $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module which is isomorphic to a subquotient of the complex vector space of all adèlic cusp form for $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ with central character χ.

Remark 5.5.14. The automorphic forms are a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-module and the subspace of cuspforms is a $(\mathfrak{g}, K_\infty) \times \mathbf{GL}_2(\mathbb{A}_f)$-submodule.

5.6 Local L-function theory and Whittaker functions

5.6.1 The Fourier expansion of a cusp form

Let (π, V_π) be a cuspidal automorphic representation. Let $\varphi \in V_\pi$ be a cusp form on $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ and $N(\mathbb{A}_\mathbb{Q}) = N_2(\mathbb{A}_\mathbb{Q}) = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{A}_\mathbb{Q} \right\}$ be the maximal unipotent subgroup of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$.

For each continuous additive character $\psi : \mathbb{Q} \setminus \mathbb{A}_\mathbb{Q} \to \mathbb{C}^\times$, we define a ψ-Fourier coefficient of φ by

$$W_{\varphi,\psi}(g) = \int_{\mathbb{Q}\setminus\mathbb{A}_\mathbb{Q}} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) \psi^{-1}(x)dx, \quad g \in \mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), x \in \mathbb{A}_\mathbb{Q}.$$

This function satisfies

$$W_{\varphi,\psi}\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = \psi(x)W_{\varphi,\psi}(g).$$

Since φ is automorphic, we have $\varphi(x+a) = \varphi(x)$, for $a \in \mathbb{Q}$. Thus φ is periodic under $\mathbb{Q}$, then we have the Fourier expansion of φ:

$$\varphi(g) = \sum_\psi W_{\varphi,\psi}(g).$$

If we fix a non-trivial character ψ of $\mathbb{Q} \setminus \mathbb{A}_\mathbb{Q}$, then the additive characters of the compact group $\mathbb{Q} \setminus \mathbb{A}_\mathbb{Q}$ correspond to the elements in $\mathbb{Q}$ by the map:

$$\gamma \mapsto \psi_\gamma,$$

where ψ_γ is the character of the form $\psi_\gamma(x) = \psi(\gamma x)$, $\gamma \in \mathbb{Q}$, so

$$\varphi(g) = \sum_{\gamma\in\mathbb{Q}} W_{\varphi,\psi_\gamma}(g).$$

Since φ is cuspidal, for $\gamma = 0$ we have

$$W_{\varphi,\psi_0}(g) = \int_{\mathbb{Q}\setminus\mathbb{A}_\mathbb{Q}} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) dx = 0$$

and since φ is automorphic, for $\gamma \neq 0$, we have

$$\begin{aligned} W_{\varphi,\psi_\gamma}(g) &= \int_{\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q}} \varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) \psi_\gamma^{-1}(x)dx \\ &= \int_{\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q}} \varphi\left(\begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) \psi_\gamma^{-1}(x)dx \\ &= \int_{\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q}} \varphi\left(\begin{pmatrix} 1 & \gamma x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix} g\right) \psi^{-1}(\gamma x)dx. \end{aligned}$$

We make the change of variable $x \mapsto \gamma^{-1}x$, then we have

$$W_{\varphi,\psi_\gamma}(g) = W_{\varphi,\psi}\left(\begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix} g\right),$$

which gives the Fourier expansion for $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$

$$\varphi(g) = \sum_{\gamma\in\mathbb{Q}^\times} W_\varphi\left(\begin{pmatrix} \gamma & 0 \\ 0 & 1 \end{pmatrix} g\right)$$

where we set $W_{\varphi,\psi} = W_\varphi$.

5.6.2 Whittaker models

Consider the functions $W = W_\varphi$ which appear in the Fourier expansion of the cusp forms $\varphi \in V_\pi$. These are smooth functions on $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ satisfying $W(ng) = \psi(n)W(g)$ for all $n \in N(\mathbb{A}_\mathbb{Q})$. Let

$$\mathcal{W}(\pi,\psi) = \{W_\varphi \mid \varphi \in V_\pi\}.$$

The group $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ acts on the space $\mathcal{W}(\pi,\psi)$ by right translation and the map

$$\varphi \mapsto W_\varphi \quad \text{intertwines} \quad V_\pi \xrightarrow{\sim} \mathcal{W}(\pi,\psi).$$

The space $\mathcal{W}(\pi,\psi)$ is called the Whittaker model of π.

The idea of a Whittaker model makes sense over a local field. Let $\mathbb{Q}_v$ be a local field and ψ_v be a non-trivial continuous additive character of $\mathbb{Q}_v$. Let $\mathcal{W}(\psi_v)$ denote the space of smooth functions $W : \mathbf{GL}_2(\mathbb{Q}_v) \to \mathbb{C}$ which satisfy $W(ng) = \psi_v(n)W(g)$

for all $n \in N(\mathbb{Q}_v)$, where $N(\mathbb{Q}_v)$ is the maximal unipotent subgroup of $\mathbf{GL}_2(\mathbb{Q}_v)$. This is the space of smooth Whittaker functions on $\mathbf{GL}_2(\mathbb{Q}_v)$ and $\mathbf{GL}_2(\mathbb{Q}_v)$ acts on it by right translation.

If (π_v, V_{π_v}) is a smooth irreducible admissible representation of $\mathbf{GL}_2(\mathbb{Q}_v)$, then an intertwing

$$V_{\pi_v} \to \mathcal{W}(\psi_v) \quad \text{denoted by} \quad \xi_v \mapsto W_{\xi_v}$$

gives a Whittaker model $\mathcal{W}(\pi_v, \psi_v)$ of π_v.

Fix a representation (π, V_{π_v}), we can define a non-trivial continuous Whittaker functional $\Lambda_v : V_{\pi_v} \to \mathbb{C}$ satisfying:

$$\Lambda_v(\pi_v(n)\xi_v) = \psi_v(n)\Lambda_v(\xi_v)$$

for all $n \in N(\mathbb{Q}_v)$ and $\xi_v \in V_{\pi_v}$.

A model $\xi_v \mapsto W_{\xi_v}$ gives a functional by

$$\Lambda_v(\xi_v) = W_{\xi_v}(e), \quad e \text{ is the identity of } \mathbf{GL}_2(\mathbb{Q}_v),$$

and a functional Λ_v gives a model by setting

$$W_{\xi_v}(g) = \Lambda_v(\pi_v(g)\xi_v), \quad g \in \mathbf{GL}_2(\mathbb{Q}_v).$$

The fundamental result on local Whittaker models is due to Gelfand and Kazhdan ($v < \infty$, [16]) and Shalika ($v \mid \infty$, [50]).

Theorem 5.6.1. *Given (π_v, V_{π_v}) an irreducible admissible smooth representation of $\mathbf{GL}_2(\mathbb{Q}_v)$, the space of continuous Whittaker functionals is at most one dimensional and π_v has at most one Whittaker model.*

Definition 5.6.2. A representation (π_v, V_{π_v}) having a Whittaker model is called generic.

Consider the smooth cuspidal representation (π, V_π). If we factor π into local components

$$\pi \simeq \otimes' \pi_v \text{ with } V_\pi \simeq \otimes' V_{\pi_v}$$

then any Whittaker functional Λ on V_π determines a family of Whittaker functionals Λ_v on the V_{π_v} by

$$\Lambda_v : V_{\pi_v} \hookrightarrow \otimes' V_{\pi_v} \xrightarrow{\sim} V_\pi \xrightarrow{\Lambda} \mathbb{C}$$

such that $\Lambda = \otimes \Lambda_v$.

The Theorem 5.6.1 has the following consequences.

Corollary 5.6.3. *If $\pi = \otimes' \pi_v$ is any irreducible admissible smooth representation of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ then the space of Whittaker functionals of V_π is at most one dimensional, that is, π has a unique Whittaker model.*

The V_π has a global Whittaker functional given by

$$\Lambda(\varphi) = W_\varphi(e) = \int_{N(\mathbb{Q})\backslash N(\mathbb{A}_\mathbb{Q})} \varphi(n)\psi^{-1}(n)dn.$$

Corollary 5.6.4. *If (π, V_π) is cuspidal with $\pi \simeq \otimes' \pi_v$ then π and each of its local components π_v are generic.*

5.6.3 Eulerian Integral Representations

Let (π, V_π) be a cuspidal representation of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ and $\chi : \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}^\times$ be a unitary idèle class character, that is a cuspidal automorphic representation of $\mathbf{GL}_1(\mathbb{A}_\mathbb{Q})$.

For $\varphi \in V_\pi$, we set

$$I(\varphi, \chi, s) = \int_{\mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times} \varphi \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \chi(a) \mid a \mid^{s-\frac{1}{2}} d^\times a.$$

Proposition 5.6.5. *(1) $I(\varphi, \chi, s)$ is absolutely convergent for all $s \in \mathbb{C}$, hence entire.*

(2) $I(\varphi, \chi, s)$ is bounded in vertical strips.

(3) $I(\varphi, \chi, s)$ satisfies the functional equation

$$I(\varphi, \chi, s) = I(\tilde{\varphi}, \chi^{-1}, 1 - s)$$

where $\tilde{\varphi}(g) = \varphi({}^t g^{-1})$.

Proof. See the discussion in Lecture 5 of [8]. □

The integrals, as φ varies over V_π, are analytic and we want to see that the integrals are Eulerian, i.e, admit an expansion as an Euler product. First we replace φ by its Fourier expansion:

$$\begin{aligned}
I(\varphi,\chi,s) &= \int_{\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times} \varphi\begin{pmatrix} a & 0 \\ 0 & 1\end{pmatrix}\chi(a)\mid a\mid^{s-\frac{1}{2}} d^\times a \\
&= \int_{\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times}\sum_{\gamma\in\mathbb{Q}^\times} W_\varphi\begin{pmatrix} \gamma a & 0 \\ 0 & 1\end{pmatrix}\chi(a)\mid a\mid^{s-\frac{1}{2}} d^\times a \\
&= \int_{\mathbb{A}_\mathbb{Q}^\times} W_\varphi\begin{pmatrix} a & 0 \\ 0 & 1\end{pmatrix}\chi(a)\mid a\mid^{s-\frac{1}{2}} d^\times a \qquad \mathrm{Re}(s)>1.
\end{aligned}$$

Since $\pi\simeq\otimes\pi_v$ and require $\varphi=\otimes_v^{'}\xi_v$, then from the uniqueness of the Whittaker model we have

$$W_\varphi(g)=\prod_v W_{\xi_v}(g_v).$$

Since $\chi(a)=\prod\chi_v(a_v)$ and $\mid a\mid=\prod\mid a_v\mid_v$, we have

$$\begin{aligned}
I(\varphi,\chi,s) &= \prod_v\int_{\mathbb{Q}_v^\times} W_{\xi_v}\begin{pmatrix} a_v & 0 \\ 0 & 1\end{pmatrix}\chi_v(a_v)\mid a_v\mid_v^{s-\frac{1}{2}} d^\times a_v \\
&= \prod_v \Psi_v(W_\xi,\chi_v,s) \quad Re(s)>1,
\end{aligned}$$

where we define

$$\Psi_v(W_{\xi_v},\chi_v,s)=\int_{\mathbb{Q}_v^\times} W_{\xi_v}\begin{pmatrix} a_v & 0 \\ 0 & 1\end{pmatrix}\chi_v(a_v)\mid a_v\mid_v^{s-\frac{1}{2}} d^\times a_v$$

as the local integral.

This gives a factorization of our global integral into a product of local integrals.

5.6.4 Local L-function: the Non-Archimedean Case

Let (π,V_π) be an irreducible admissible smooth unitary generic representation of $\mathbf{GL}_2(\mathbb{Q}_p)$ and $(\pi',V_{\pi'})$ be an irreducible admissible smooth unitary generic representation of $\mathbf{GL}_1(\mathbb{Q}_p)$.

A Schwartz-Bruhat function is a complex valued function on $\mathbb{Q}_p$, which is locally constant and has compact support. Let $\mathcal{S}(\mathbb{Q}_p)$ denote the vector space of Schwartz-Bruhat functions on $\mathbb{Q}_p$. The basic analytic properties of the Whittaker functions are given in the following proposition.

Proposition 5.6.6. *There is a finite set of finite functions, say $X(\pi)$, depending only on π, such that for every $W \in \mathcal{W}(\pi, \psi)$, there exist Schwartz-Bruhat functions $\phi_\chi \in \mathcal{S}(\mathbb{Q}_p)$ such that for $a \in \mathbb{Q}^\times$, we have*

$$W\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \sum_{\chi \in X(\pi)} \chi(a)\phi_\chi(a).$$

Proof. See the Proposition 2.2 in [32]. □

From the factorization of the global integrals, we have defined families of local integrals $\{\Psi(W, \chi, s)\}$, for $W \in \mathcal{W}(\pi, \varphi)$ and χ is Hecke character. Then we have the following basic result.

Proposition 5.6.7. *(1) Each local integral $\Psi_v(W, \chi, s)$ converges for $Re(s) > 1$.*

(2) Each $\Psi_v(W, \chi, s) \in \mathbb{C}(q^{-s})$ is a rational function of q^{-s} and hence extends meromorphically to all of $\mathbb{C}$.

(3) Each $\Psi_v(W, \chi, s)$ can be written with a common denominator determined by $X(\pi)$ and $X(\pi')$. Hence the family has bounded denominators.

Proof. See the Proposition 6.2 in [8]. □

Theorem 5.6.8. *The family of local integrals $I(\pi \times \pi') = \langle \Psi(W, \chi, s) \rangle$ is a $\mathbb{C}[q^s, q^{-s}]$-fractional ideal of $\mathbb{C}(q^{-s})$ containing the constant 1.*

Proof. See the discussion in Theorem 6.1 in [8]. □

Since the ring $\mathbb{C}[q^s, q^{-s}]$ is a principal ideal domain, the fractional ideal $I(\pi \times \pi')$ has a generator. Since $1 \in I(\pi \times \pi')$, we can take a generator having numerator 1 and normalized (up to units) to be of the form $P(q^{-s})$ when $P(X) \in \mathbb{C}[X]$ and $P(0) = 1$.

Definition 5.6.9. The local L-function $L(\pi \times \pi', s) = P^{-1}(q^{-s})$ is the normalized generator of the fractional ideal $I(\pi \times \pi')$ spanned by the local integrals. We set $L(\pi, s) = L(\pi \times 1, s)$ where χ is the trivial character of $\mathbf{GL}_1(\mathbb{Q}_p)$.

Remark 5.6.10. $L(\pi \times \pi', s)$ is the minimal inverse polynomial $P(q^{-s})^{-1}$ such that $\frac{\Psi(W,\chi,s)}{L(\pi\times\pi',s)} \in \mathbb{C}[q^s, q^{-s}]$ are polynomials in q^s and q^{-s} and so are entire for all choices $W \in \mathcal{W}(\pi, \psi)$ and χ.

Theorem 5.6.11. *There exists a rational function $\gamma(\pi \times \pi', \psi, s) \in \mathbb{C}(q^{-s})$ such that*

$$\Psi(\tilde{W}, \tilde{\chi}, 1-s) = \omega_{\pi'}(-1)^{n-1}\gamma(\pi \times \pi', \psi, s)\Psi(W, \chi, s)$$

for all $W \in \mathcal{W}(\pi, \psi)$ and χ and $\omega_{\pi'}$ is the central character.

We say that $\gamma(\pi \times \pi', \psi, s)$ is the local γ-factor. An equally important local factor is the local ϵ-factor

$$\epsilon(\pi \times \pi', \psi, s) = \frac{\gamma(\pi \times \pi', \psi, s)L(\pi \times \pi', s)}{L(\tilde{\pi} \times \tilde{\pi}', 1-s)}$$

with the local functional equation becomes

$$\frac{\Psi(\tilde{W}, \tilde{\chi}, 1-s)}{L(\tilde{\pi} \times \tilde{\pi}', 1-s)} = \omega_{\pi'}(-1)^{n-1}\epsilon(\pi \times \pi', \psi, s)\frac{\Psi(W, \chi, s)}{L(\pi \times \pi', s)}.$$

5.6.5 Local L-functions: the Archimedean Case

Let π be a representation of $\mathbf{GL}_2(\mathbb{R})$ associated with a representation ρ_π of the Weil group $W_\mathbb{R}$ of $\mathbb{R}$ and π' be a representation of $\mathbf{GL}_1(\mathbb{R})$ associated with a representation ρ'_π of the Weil group $W_\mathbb{R}$ of $\mathbb{R}$. Then we define the L-function for π and π' as follows:

$$L(\pi \times \pi', s) = L(\rho_\pi \otimes \rho'_\pi, s)$$
$$\epsilon(\pi \times \pi', \psi, s) = \epsilon(\rho_\pi \otimes \rho'_\pi, \psi, s)$$

and we set

$$\begin{aligned}\gamma(\pi \times \pi', \psi, s) &= \frac{\epsilon(\pi \times \pi', \psi, s)L(\tilde{\pi} \times \tilde{\pi}', 1-s)}{L(\pi \times \pi', s)} \\ &= \frac{\epsilon(\rho_\pi \otimes \rho'_\pi, \psi, s)L(\tilde{\rho_\pi} \otimes \tilde{\rho_\pi}', 1-s)}{L(\rho_\pi \otimes \rho'_\pi, s)}.\end{aligned}$$

Then we have the following propositions and the details are discussed in [8].

Proposition 5.6.12. *Let π be an irreducible admissible generic representation of $\mathbf{GL}_2(\mathbb{R})$ which is smooth of moderate growth. Then there is a finite set of finite functions $X(\pi)$*

depending only on π such that for every $W \in \mathcal{W}(\pi,\psi)$, there exist Schwartz functions $\phi_\chi \in \mathcal{S}(\mathbb{R}^2)$ such that for $a \in \mathbb{R}$ and $k \in \mathbb{R}$, we have

$$W\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} k\right) = \sum_{\chi \in X(\pi)} \chi(a)\phi_\chi(a,k).$$

Proposition 5.6.13. *Each local integral $\Psi_v(W,\chi,s)$ converges absolutely for $Re(s) \gg 0$ and if π and π' are both unitary, they converge absolutely for $Re(s) \geq 1$.*

Let $\mathcal{M}(\pi \times \pi') = \mathcal{M}(\rho_\pi \otimes \rho'_\pi)$ be the space of all meromorphic functions $\phi(s)$ satisfying:

If $P(s) \in \mathbb{C}[s]$ is a polynomial such that $P(s)L(\pi \times \pi', s)$ is holomorphic in the vertical strip $S[a,b] = \{s \mid a \leq Re(s) \leq b\}$, then $P(s)\phi(s)$ is holomorphic and bounded in $S[a,b]$.

Theorem 5.6.14. *The integrals $\Psi_v(W,\chi,s)$ extend to meromorphic functions of s and $\Psi_j(W,\chi,s) \in \mathcal{M}(\pi \times \pi')$. In particular, $\frac{\Psi_j(W,\chi,s)}{L(\pi\times\pi',s)}$ are entire.*

Theorem 5.6.15. *We have the local functional equation*

$$\Psi(\tilde{W}, \tilde{\chi}, 1-s) = \omega_{\pi'}(-1)^{n-1}\gamma(\pi \times \pi', \psi, s)\Psi(W,\chi,s)$$

with $\gamma(\pi \times \pi', \psi, s) = \gamma(\rho_\pi \otimes \rho'_\pi, \psi, s)$ and $\omega_{\pi'}$ central character.

5.7 Global L-function

Let us consider the global setting. Let Σ be the set of all places of $\mathbb{Q}$. Take $\psi : \mathbb{Q}\backslash\mathbb{A}_\mathbb{Q} \to \mathbb{C}^\times$ a non-trivial continuous additive character.

Let (π, V_π) be a cuspidal representation of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$, which then decomposes as $\pi \backsimeq \otimes'\pi_v$. Let $(\pi', V_{\pi'})$ be a cuspidal representation of $\mathbf{GL}_1(\mathbb{A}_\mathbb{Q})$, which then decomposes as $\pi' \backsimeq \otimes'\pi'_v$.

For each place $v \in \Sigma$, we have defined local L-factors and ϵ-factors:

$$L(\pi_v \otimes \pi'_v, s) \quad \text{and} \quad \epsilon(\pi_v \otimes \pi'_v, \psi_v, s).$$

Then we define the global L-function and ϵ-factor as Euler products.

Definition 5.7.1. The global L-function and ϵ-factor for π and π' are

$$L(\pi \otimes \pi', s) = \prod_{v \in \Sigma} (\pi_v \otimes \pi'_v, s)$$

and

$$\epsilon(\pi \otimes \pi', s) = \prod_{v \in \Sigma} \epsilon(\pi_v \otimes \pi'_v, \psi_v, s).$$

The product defining the L-function is absolutely convergent for $\mathrm{Re}(s) \gg 0$ and the ϵ-factor is independent from the choice of ψ. More details are discussed in Lecture 9 of [8].

The following theorem shows that these L-functions have nice analytic properties.

Theorem 5.7.2. *If π is a cuspidal representation of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ and π' is a cuspidal representation of $\mathbf{GL}_1(\mathbb{A}_\mathbb{Q})$, then the global L-functions $L(\pi \otimes \pi', s)$ are nice in the sense that*

(i) $L(\pi \otimes \pi', s)$ converges for $\mathrm{Re} \gg 0$ and extends to an entire function of s;

(ii) this extension is bounded in vertical strips of finite width;

(iii) it satisfies the functional equation

$$L(\pi \otimes \pi', s) = \epsilon(\pi \otimes \pi', s) L(\tilde{\pi} \otimes \tilde{\pi}', 1 - s).$$

Proof. See the Lecture 9 of [8]. □

Chapter 6

Complex L-functions of real quadratic fields

We recast the special value formula in [41], restricted to the setting of the thesis, in a form convenient for our purpose.

Let $f \in S_k(\Gamma_0(M))$ be a even weight $k \geq 2$ newform for $\Gamma_0(M)$. Let $F/\mathbb{Q}$ be a real quadratic field of discriminant $D > 0$, prime to M, and let χ_D be the associated quadratic Dirichlet character. We also denote by the same symbol $\chi_D : \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{C}^{\times}$ the associated Hecke character, where $\mathbb{A}_{\mathbb{Q}}$ is the adèle ring of $\mathbb{Q}$. Assume that all primes $\ell \mid M$ are split in F.

Let c be an integer prime to $D \cdot M$ and let H_c^+ be the strict ring class field of F of conductor c. Let G_c^+=Gal(H_c^+/F). A character χ is primitive if it does not factor through G_f^+ for a proper divisor $f \mid c$. Let $\chi : G_c^+ \to \mathbb{C}^{\times}$ be a primitive character. We will denote by the same symbol $\chi : \mathbb{A}_F^{\times} \to \mathbb{C}^{\times}$ the associated Hecke character, where $\mathbb{A}_F$ is the adèle ring of F.

6.1 Quaternion algebra

A quaternion algebra over a field F is a 4-dimensional central simple algebra over F. Any quaternion algebra over a field F of characteristic $\neq$2 is isomorphic to an algebra of the form

$$\left(\frac{a,b}{F}\right) := F \oplus Fi \oplus Fj \oplus Fk, \text{ where } i^2 = a, j^2 = b, ij = -ji = k,$$

for some $a, b \in F^\times$. A quaternion algebra B over F is said to be split if it is isomorphic to the ring $M_2(F)$ of 2×2 matrices with entries in F. More generally, if K is an extension field of F, then B is said to be split over K if $B \otimes_F K$ is a split quaternion algebra over K.

For any place v of F, let F_v denote the completion of F at v and let $B_v := B \otimes_F F_v$. B is said to be split at v if B_v is a split quaternion algebra. Otherwise B is said to be ramified at v.

Let Z be a finitely generated subring of F.

Definition 6.1.1. A Z-order in B is a subring of B which is free of rank 4 as a Z-module. A maximal Z-order is a Z-order which is properly contained in no larger Z-order. An Eichler Z-order is the intersection of two maximal Z-orders.

6.2 Optimal embedding theory

Let us denote by $\mathcal{B} = \mathrm{M}_2(\mathbb{Q})$ the split algebra over $\mathbb{Q}$ and denote by R_0 the order in $\mathcal{B}$ consisting of matrices in $\mathrm{M}_2(\mathbb{Z})$ which are upper triangular modulo M. Let $\mathcal{O}_F$ be the ring of integer of F and $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_F$ be the order of F of conductor c. Let $\mathrm{Emb}(\mathcal{O}_c, R_0)$ be the set of optimal embedding $\psi : F \to \mathcal{B}$ of $\mathcal{O}_c$ into R_0 ($\psi(\mathcal{O}_c) = R_0 \cap \psi(F)$). For every prime $\ell \mid M$, equip R_0 and $\mathcal{O}_c$ with local orientations at ℓ, i.e., ring homomorphisms

$$\mathfrak{D}_\ell : R_0 \to \mathbb{F}_\ell, \ \mathfrak{o}_\ell : \mathcal{O}_c \to \mathbb{F}_\ell.$$

Two embeddings $\psi, \psi' \in \mathrm{Emb}(\mathcal{O}_c, R_0)$ are said to have the same orientation at a prime $\ell \mid M$ if $\mathfrak{D} \circ (\psi \mid_{\mathcal{O}_c}) = \mathfrak{D}_\ell \circ (\psi' \mid_{\mathcal{O}_c})$ and otherwise are said to have opposite orientation at ℓ. $\psi \in \mathrm{Emb}(\mathcal{O}_c, R_0)$ is an oriented optimal embedding if

$$\mathfrak{D}_\ell \circ (\psi \mid_{\mathcal{O}_c}) = \mathfrak{o}_\ell$$

for all primes $\ell \mid M$. The set of all such oriented optimal embeddings will be denoted by $\mathcal{E}(\mathcal{O}_c, R_0)$. The action of $\Gamma_0(M)$ on $\mathrm{Emb}(\mathcal{O}_c, R_0)$ from the right by conjugation restricts to an action on $\mathcal{E}(\mathcal{O}_c, R_0)$. If $\psi \in \mathcal{E}(\mathcal{O}_c, R_0)$ then $\psi^* := \omega_\infty \psi \omega_\infty^{-1}$ belongs to $\mathcal{E}(\mathcal{O}_c, R_0)$, where $\omega_\infty = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and ψ and ψ^* have the same orientation at all $\ell \mid M$. If ℓ is a prime dividing M then ψ and $\omega_\ell \psi \omega_l^{-1}$, where $\omega_\ell = \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}$, have opposite orientations at ℓ and the same orientation at all primes dividing M/ℓ.

Let $\mathfrak{a} \subset \mathcal{O}_c$ be an ideal representing a class $[\mathfrak{a}] \in \mathrm{Pic}^+(\mathcal{O}_c)$ and let $\psi \in \mathrm{Emb}(\mathcal{O}_c, R_0)$. The left R_0-ideal $R_0\psi(\mathfrak{a})$ is principal; let $a \in R_0$ be a generator of this ideal with positive reduced norm, which is unique up to elements in $\Gamma_0(M)$. The right action of $\psi(\mathcal{O}_c)$ on $R_0\psi(\mathfrak{a})$ shows that $\psi(\mathcal{O}_c)$ is contained in the right order of $R_0\psi(\mathfrak{a})$, which is equal to $a^{-1}R_0 a$. This defines an action of $\mathrm{Pic}^+(\mathcal{O}_c)$ on conjugacy classes of oriented embeddings given by

$$[\mathfrak{a}] \cdot [\psi] = [a\psi a^{-1}]$$

in $\mathrm{Emb}(\mathcal{O}_c, R_0)/\Gamma_0(M)$. The principal ideal $(\sqrt{D})$ is a proper $\mathcal{O}_c$-ideal of F; denote $\mathfrak{D}$ its class in $\mathrm{Pic}^+(\mathcal{O}_c)$ and define $\sigma_F := \mathrm{rec}(\mathfrak{D}) \in G_c^+$, where rec is the arithmetically normalized reciprocity map of class field theory. If $\mathfrak{a} = (\sqrt{D})$ then we can take $a = \omega_\infty \psi(\sqrt{d_D})$ in the above discussion, which shows that

$$\mathfrak{D} \cdot [\psi] = [\omega_\infty \psi \omega_\infty^{-1}] = [\psi^*].$$

Using the reciprocity map of class field theory, for all $\sigma \in G_c^+$ and $[\psi] \in \mathrm{Emb}(\mathcal{O}_c, R_0)/\Gamma_0(M)$ define

$$\sigma \cdot [\psi] := \mathrm{rec}^{-1}(\sigma)[\psi].$$

In particular, $\sigma_F \cdot [\psi] = [\psi^*]$ for all $\psi \in \mathrm{Emb}(\mathcal{O}_c, R_0)$.

If ψ is an oriented optimal embedding then the Eichler order $a^{-1}R_0 a$ inherits an orientation from the one of R_0 and it can be checked that we get an induced action of $\mathrm{Pic}^+(\mathcal{O}_c)$ (and G_c^+) on the set $\mathcal{E}(\mathcal{O}_c, R)/\Gamma_0(M)$, and this action is free and transitive. To describe a (non-canonical) bijection between $\mathcal{E}(\mathcal{O}_c, R)/\Gamma_0(M)$ and G_c^+, fix once and for all an auxiliary embedding $\psi_0 \in \mathcal{E}(\mathcal{O}_c, R)$; then $\sigma \mapsto \sigma[\psi_0]$ defines a bijection

$$E : G_c^+ \to \mathcal{E}(\mathcal{O}_c, R_0)/\Gamma_0(M)$$

whose inverse

$$G = E^{-1} : \mathcal{E}(\mathcal{O}_c, R_0)/\Gamma_0(M) \to G_c^+$$

satisfies the relation $G([\psi^*]) = \sigma_F G([\psi])$ for all $\psi \in \mathcal{E}(\mathcal{O}_c, R_0)$. Choose for every $\sigma \in G_c^+$ an embedding $\psi_\sigma \in E(\sigma)$, so that the family $\{\psi_\sigma\}_{\sigma \in G_c^+}$ is a set of representatives of the $\Gamma_0(M)$-conjugacy classes of oriented optimal embeddings of $\mathcal{O}_c$ into R_0. If $\gamma, \gamma' \in R_0$ write $\gamma \backsim \gamma'$ to indicate that γ and γ' are in the same $\Gamma_0(M)$-conjugacy class, and adopt a similar notation for (oriented) optimal embeddings of $\mathcal{O}_c$ into R_0. For all $\sigma, \sigma' \in G_c^+$, one has $\sigma\psi_{\sigma'} \backsim \psi_{\sigma\sigma'}$ and $\psi_\sigma^* \backsim \psi_{\sigma_F \sigma}$ for all $\sigma \in G_c^+$.

Finally, note that the set $\mathcal{E}(\mathcal{O}_c, R_0)/\Gamma_0(M)$ is in bijection with $\mathcal{F}_{Dc^2}/\Gamma_0(M)$, since both sets are in bijection with G_c^+; explicitly, to the class of the oriented optimal embedding ψ corresponds the class of the quadratic form

$$Q_\psi(x, y) = Cx^2 - 2Axy - BY^2$$

with $\psi(\sqrt{D}c) = \begin{pmatrix} A & B \\ C & -A \end{pmatrix}$.

Remark 6.2.1. For more details, see the section 4.2 of [37].

6.3 Adèlic ring class groups

In this section, we want to view the ring class group G_c^+ adelically. We also want to describe the relation with the ray class groups. In this section only, we allow F to be any arbitrary quadratic field of discriminant D and do not require c to be coprime to D.

6.3.1 Ideal class groups

Let $\mathcal{O}$ be a Dedekind domain.

Definition 6.3.1. A fractional ideal of F is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of F.

For instance, an element $a \in F^\times$ defines the fractional principal ideal $(a) = a\mathcal{O}$.

Proposition 6.3.2. *The fractional ideals form an abelian group, the ideal group J_F of F. The identity element is $(1) = \mathcal{O}$, and the inverse of $\mathfrak{a}$ is*

$$\mathfrak{a}^{-1} = \{x \in F | x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Proof. This follows from the Proposition 3.8 in [44]. □

The fractional principal ideals $(a) = a\mathcal{O}, a \in F^\times$, form a subgroup of the group of ideals J_F, which will be denoted P_F. The quotient group

$$Cl_F = J_F/P_F$$

is called the ideal class group of F.

6.3.2 Adèlic ring class groups

Let $\mathbb{A}_F^\times$ denote the idèle group of F.

The idèle class group I_F of an algebraic number field F is the topological union of the groups

$$\mathbb{A}_F^S = \prod_{\mathfrak{p} \in S} F_\mathfrak{p}^\times \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p},$$

where $F_\mathfrak{p}$ is completion with respect to $\mathfrak{p}$, $U_\mathfrak{p} = \mathcal{O}_{F_\mathfrak{p}}^\times$ for $\mathfrak{p}$ finite, $U_\mathfrak{p} = \mathbb{R}_+^\times$ for $\mathfrak{p}$ infinite real and S runs over all the finite set of places. Thus one has

$$\mathbb{A}_F^\times = \cup_S \mathbb{A}_F^S.$$

Define the diagonal embedding

$$F^\times \to \mathbb{A}_F^\times,$$

which associate to $a \in F^\times$ the idèle $\alpha \in \mathbb{A}_F^\times$ whose $\mathfrak{p}$-th component is the element $a \in F_p$. We call the elements of $F^\times$ in $\mathbb{A}_F^\times$ principal idèles. The intersection

$$F^S = F^\times \cap \mathbb{A}_F^S$$

consists of the numbers $a \in F^\times$ which are unites at all primes $\mathfrak{p} \notin S$, $\mathfrak{p} \nmid \infty$ and which are positive in $F_\mathfrak{p} = \mathbb{R}$ for all real infinite places $\mathfrak{p} \notin S$.

Definition 6.3.3. The element of the subgroup $F^\times$ of I_F are called principal idèle and the quotient group

$$C_F = \mathbb{A}_F^\times / F^\times$$

is called the idèle class group of F.

There is a surjective homomorphism between the idèle class group and the ideal class group Cl_F induced by :

$$\mathbb{A}_F^\times \longrightarrow J_F, \quad \alpha \mapsto (\alpha) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}.$$

Its kernel is

$$\mathbb{A}_F^{S_\infty} = \prod_{p|\infty} F_\mathfrak{p}^\times \times \prod_{p\nmid\infty} U_\mathfrak{p}.$$

Given a number field F, a module in F is a formal product

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$$

over all primes $\mathfrak{p}$, finite or infinite, of F, where the exponent must satisfy:

(1) $n_\mathfrak{p} \geqslant 0$, and at most finitely many are nonzero.

(2) $n_\mathfrak{p} = 0$ wherever $\mathfrak{p}$ is a complex infinite prime.

(3) $n_\mathfrak{p} \leqslant 1$ wherever $\mathfrak{p}$ is a real infinite prime.

A module $\mathfrak{m}$ may be written $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_F$-ideal and $\mathfrak{m}_\infty$ is a product of real infinite primes of F. More details are discussed in Section (8, A) of [10].

For every place $\mathfrak{p}$ of F we put $U_\mathfrak{p}^{(0)} = U_\mathfrak{p}$, and

$$U_\mathfrak{p}^{(n_\mathfrak{p})} = \begin{cases} 1 + \mathfrak{p}^{n_\mathfrak{p}} & \mathfrak{p} \nmid \infty \\ \mathbb{R}_+^\times \subset F_\mathfrak{p}^\times & \mathfrak{p} \text{ is real} \\ \mathbb{C}^\times = F_\mathfrak{p}^\times & \mathfrak{p} \text{ is complex} \end{cases} \tag{6.3.1}$$

for $n_\mathfrak{p} > 0$. Given $\alpha_\mathfrak{p} \in F_\mathfrak{p}^\times$ we write

$$\alpha_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^{n_\mathfrak{p}} \Longleftrightarrow \alpha_\mathfrak{p} \in U_\mathfrak{p}^{(n_\mathfrak{p})}.$$

For a finite prime $\mathfrak{p}$ and $n_\mathfrak{p} > 0$ this means the usual congruence; for a real place, it symbolizes positivity, and for a complex place it is the empty condition.

Definition 6.3.4. The group

$$C_F^\mathfrak{m} = \mathbb{A}_{F,\mathfrak{m}} F^\times / F^\times,$$

formed from the idèle group

$$\mathbb{A}_{F,\mathfrak{m}} = \prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})}$$

is called the congruence subgroup mod $\mathfrak{m}$, and the quotient group $C_F/C_F^\mathfrak{m}$ is called the ray class group mod $\mathfrak{m}$.

The ray class groups can be given the following ideal-theoretic description. Let $c \in \mathbb{N}$ and $\mathfrak{m} = \mathfrak{m}_f \mathfrak{m}_\infty$ where $\mathfrak{m}_f = c\mathcal{O}_F$ and $\mathfrak{m}_\infty$ a subset of the real places F. For a real place v, let σ_v be the associated embedding of F into $\mathbb{R}$. Let $J_\mathfrak{m}$ be the group of fractional ideals of $\mathcal{O}_F$ which are prime to $\mathfrak{m}_f$. Let $F_\mathfrak{m}^1$ be the subset of $F^\times$ consisting of x such that $\sigma_v(x) > 0$ for each $v \in \mathfrak{m}_\infty$ and $v_\mathfrak{p}(x-1) \geq v_\mathfrak{p}(c)$ for $\mathfrak{p} \mid \mathfrak{m}_f$, and $P_\mathfrak{m}^1$ denote the set of principal ideals generated by elements of $F_\mathfrak{m}^1$. Then we get the group $Cl_\mathfrak{m}(F) = J_\mathfrak{m}/P_\mathfrak{m}^1$ and

Proposition 6.3.5. *([44],Chapter VI, Prop 1.9) The homomorphism*

$$(\quad) : I_F \to J_F,\ \alpha \mapsto (\alpha) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

induces an isomorphism

$$C_F/C_F^\mathfrak{m} \cong Cl_\mathfrak{m}(F).$$

Let $F_\mathfrak{m}^\mathbb{Z}$ be the set of $x \in F^\times$ such that $\sigma_v(x) > 0$ for each $v \in \mathfrak{m}_\infty$ and for each $\mathfrak{p} \mid \mathfrak{m}_f$ there exists $a \in \mathbb{Z}$ coprime to c such that $v_\mathfrak{p}(x-a) \geq v_\mathfrak{p}(c)$. Let $P_\mathfrak{m}^\mathbb{Z}$ be the set of principal ideals in F generated by elements of $F_\mathfrak{m}^\mathbb{Z}$. Then the ring class group mod $\mathfrak{m}$ of F is $G_\mathfrak{m}(F) = J_\mathfrak{m}/P_\mathfrak{m}^\mathbb{Z}$. Note we can write

$$F_\mathfrak{m}^\mathbb{Z} = \bigsqcup_{a \in (\mathbb{Z}/c\mathbb{Z})^\times} a F_\mathfrak{m}^1.$$

Hence $G_{\mathfrak{m}}(F)/(\mathbb{Z}/c\mathbb{Z})^\times \simeq Cl_{\mathfrak{m}}(F)$. (The map from $(\mathbb{Z}/c\mathbb{Z})^\times$ to $G_{\mathfrak{m}}(F)$ is not necessarily injective.)

Via the usual correspondence between ideals and idèles, $J_{\mathfrak{m}}$ is identified with $\hat{F}_{\mathfrak{m}}^\times/\hat{\mathcal{O}}_F^\times$, where $\hat{F}_{\mathfrak{m}}^\times$ consists of finite idèles (α_v) such that $\alpha_v \in \mathcal{O}_{F,v}^\times$ for all $v \mid \mathfrak{m}_f$ and $\hat{\mathcal{O}}_F^\times = \prod_{v<\infty} \mathcal{O}_{F,v}^\times$. For $v < \infty$, we put $W_v = \mathcal{O}_{F,v}^\times$ unless $v \mid \mathfrak{m}_f$, in which case $W_v = 1 + \mathfrak{m}_f \mathcal{O}_{F,v}$. For $v \mid \infty$, we put $W_v = F_v^\times$ unless $v \mid \mathfrak{m}_\infty$, in which case $W_v = \mathbb{R}_{>0}$. Define

$$W = \prod W_v \quad \text{and} \quad \mathbb{A}_{F,\mathfrak{m}}^1 = {\prod}'_{v\nmid\mathfrak{m}} F_v^\times \times \prod_{v\mid\mathfrak{m}} W_v,$$

then we also can write

$$F_{\mathfrak{m}}^1 = F^\times \cap \mathbb{A}_{F,\mathfrak{m}}^1 \quad \text{and} \quad J_{\mathfrak{m}} \simeq \mathbb{A}_{F,\mathfrak{m}}^1/W,$$

so $Cl_{\mathfrak{m}}(F) = F_m^1 \setminus \mathbb{A}_{F,\mathfrak{m}}^1/W = F^\times \setminus \mathbb{A}_F^\times/W$.

For the ring class group, again we can realize it as a quotient of the idèles class group $F^\times \setminus \mathbb{A}_F^\times$, but now it will be a quotient by a subgroup $U = \prod U_\ell \times U_\infty$ which is a product over rational primes, rather than primes of F. As usual, for a rational prime $\ell < \infty$, write $\mathcal{O}_{F,\ell}$ for $\mathcal{O}_{F,\ell} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which is isomorphic to $\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$ if ℓ splits in F and otherwise is $\mathcal{O}_{F,v}$ if v is the unique prime of F above ℓ. Now set $U_\ell = \mathcal{O}_{F,\ell}^\times$ if $\ell \nmid c$ and $U_\ell = (\mathbb{Z}_\ell + c\mathcal{O}_{F,\ell})^\times$ if $\ell \mid c$. We can uniformly write $U_\ell = \mathcal{O}_{c,\ell}^\times$ for $\ell < \infty$, where $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_F$ and $\mathcal{O}_{c,\ell} = \mathcal{O}_c \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. For later use, we will write $\hat{\mathcal{O}}_c^\times = \prod U_\ell$. Note this is not the same as $\prod_{v<\infty} \mathcal{O}_{c,v}^\times$, where v runs over primes of F in the case that c is divisible by primes which split in F. Put $U_\infty = W_\infty = \prod_{v\mid\infty} W_\infty$ and $\mathbb{A}_{F,\mathfrak{m}}^{\mathbb{Z}} = {\prod}'_{v\nmid\mathfrak{m}} F_v^\times \times \prod_{v\mid\mathfrak{m}} U_v$, then $F_{\mathfrak{m}}^{\mathbb{Z}} = \mathbb{A}_{F,\mathfrak{m}}^{\mathbb{Z}} \cap F^\times$ and we see the ring class group is

$$G_{\mathfrak{m}}(F) = F_{\mathfrak{m}}^{\mathbb{Z}} \setminus \mathbb{A}_{F,\mathfrak{m}}^{\mathbb{Z}}/U = F^\times \setminus \mathbb{A}_F^\times/U.$$

In our case of interest, namely F is real quadratic and $\mathfrak{m}_\infty$ contains both real places of F, we write $U_\infty = F_\infty^+$. Thus we can write our strict ring class group as

$$G_c^+ = F^\times \setminus \mathbb{A}_F^\times/\hat{\mathcal{O}}_c^\times F_\infty^+. \tag{6.3.2}$$

6.4 Special value formulas

We return to our case. Let $F/\mathbb{Q}$ be a real quadratic field of discriminant D and f be a weight k newform for $\Gamma_0(M)$. Let c be an integer coprime with DM and $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_F$.

Let H_c be the corresponding ring class field and h_c be the degree of H_c/F, which coincides with the cardinality of $\mathrm{Pic}(\mathcal{O}_c)$. Let h_c^+ be the cardinality of G_c^+, then h_c^+/h_c is equal to 1 or 2. Fix ideals $\mathfrak{a}_\sigma$ for all $\sigma \in G_c$=Gal(H_c/F) in such a way that $\Sigma_c = \{\mathfrak{a}_\sigma \mid \sigma \in G_c\}$ is a complete system of representatives for $\mathrm{Pic}(\mathcal{O}_c)$. Clearly $\Sigma_c^+ = \Sigma_c$ is also a system of representatives for $\mathrm{Pic}^+(\mathcal{O}_c)$ if $h_c^+ = h_c$, while if $h_c^+ \neq h_c$ the set Σ_c^+ of representatives of $\mathrm{Pic}^+(\mathcal{O}_c)$ can be written as $\Sigma_c \cap \Sigma_c^{'}$ with $\Sigma_c^{'} = \{\mathfrak{d}a_\sigma \mid \sigma \in G_c\}$ and $\mathfrak{d} = (\sqrt{D})$. Let $\epsilon_c > 1$ is the smallest totally positive power of a fundamental unit in $\mathcal{O}_c^\times$ and for all $\sigma \in G_c^+$ define $\gamma_\sigma = \psi_\sigma(\epsilon_c)$. Finally, define

$$\alpha = \prod_{\ell | c, (\frac{D}{\ell})=-1} \ell, \tag{6.4.1}$$

where ℓ runs over all rational primes dividing c which are inert in F.

Denote by π_f and π_χ the automorphic representations of $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ attached to f and χ, respectively.

Theorem 6.4.1. *Let c be an integer such that $(c, DM) = 1$. Let χ be a character of G_c^+ such that the absolute norm of the conductor of χ is $c(\chi) = c^2$. For any choice of the base point $\tau_0 \in \mathcal{H}$, we have*

$$L(\pi_f \otimes \pi_\chi, 1/2) = \frac{4}{\alpha^2 \cdot (Dc^2)^{(k-1)/2}} \mid \sum_{\sigma \in G_c^+} \chi^{-1}(\sigma) \int_{\tau_0}^{\gamma_\sigma(\tau_0)} f(z) Q_{\psi_\sigma}(z,1)^{(k-2)/2} dz \mid^2 .$$

When c=1, this is the positive weight case of Theorem 6.3.1 in [46], which also treats weight 0 Maass forms.

Proof. Write $\pi := \pi_f = \otimes_v^{'} \pi_v$, where v runs over all places of $\mathbb{Q}$, and let $n_\ell(\pi)$ be the conductor of π_ℓ for each prime number ℓ. Define

$$U_f(M) = \prod_\ell U_\ell(M), \quad U_\ell(M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}_\ell) : c \equiv 0 \bmod M \right\}.$$

We associate to f the automorphic form $\varphi_\pi = \varphi_f \in \mathcal{A}(\mathbf{GL}_2(\mathbb{A}_\mathbb{Q}), \chi)$ given by

$$\varphi_\pi : Z(\mathbb{A})\mathbf{GL}_2(\mathbb{Q}) \setminus \mathbf{GL}_2(\mathbb{A}_\mathbb{Q})/U_f(M) \to \mathbb{C}$$
$$\varphi_\pi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2j(g;i)^k f\left(\frac{ai+b}{ci+d}\right),$$

for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})^+$, where we write $j(g;i)$ $=\det(g)^{1/2}(ci+d)^{-1}$ for the automorphy factor. Then φ_π is $R_{0,\ell}$-invariant for each finite prime ℓ. The scaling factor of 2 is present so that the archimedean zeta integral of φ_π gives the archimedean L-factor.

For $\phi \in \pi$, let

$$(\phi, \phi) = \int_{Z(\mathbb{A}_\mathbb{Q})\mathbf{GL}_2(\mathbb{Q})\backslash\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})} \phi(t)\overline{\phi(t)}dt$$

be the Petersson norm of ϕ, where we take as measures on the groups $\mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ and $Z(\mathbb{A}_\mathbb{Q})$ the products of the local Tamagawa measures. Here, as usual, we take the quotient measure on the quotient, giving $\mathbf{GL}_2(\mathbb{Q}) \subset \mathbf{GL}_2(\mathbb{A}_\mathbb{Q})$ the counting measure.

Denote by π_F the base change of π to F. Let $L(\pi_F \otimes \chi, s)$ be the L-function of π_F twisted by χ, which equals the Rankin-Selberg L-function $L(\pi_f \otimes \pi_\chi, s)$. Since F splits at each prime ℓ where π is ramified and at ∞, $\epsilon(\pi_{F,v} \otimes \chi_v, 1/2) = +1$ for all places v of $\mathbb{Q}$. Then, in our setting, the main result in [[41], Theorem 4.2] states that

$$\frac{\mid P_\chi(\varphi) \mid^2}{(\varphi,\varphi)} = \frac{L(\pi_F \otimes \chi, 1/2)}{(\varphi_\pi', \varphi_\pi')} \cdot \frac{4}{\sqrt{Dc(\chi)}} \cdot \prod_{\ell \mid c} \left(\frac{\ell}{\ell - \chi_D(\ell)} \right)^2, \tag{6.4.2}$$

where $\varphi \in \pi$ is a suitable test vector,

$$P_\chi(\varphi) = \int_{F^\times \mathbb{A}_\mathbb{Q}^\times \backslash \mathbb{A}_F^\times} \varphi(t)\chi^{-1}(t)dt,$$

and φ_π' (denoted φ_π in loc. cit) is a vector in π differing from φ_π only at ∞. We describe φ and φ_π' precisely below. Similar to before, we take the products of local Tamagawa measures on $\mathbb{A}_F^\times$ and $\mathbb{A}_\mathbb{Q}^\times$, and give $F^\times$ the counting measure.

First we describe the choice of the test vector φ, which we only need to specify up to scalars, as the left-hand side above is invariant under scalar multiplication. We will take $\varphi = \otimes_v' \varphi_v$, where v runs over all places of $\mathbb{Q}$. For ℓ a finite prime of $\mathbb{Q}$, let $c(\chi_\ell)$ denote the smallest n such that χ_ℓ is trivial on $(\mathbb{Z}_\ell + \ell^n \mathcal{O}_{F,\ell})^\times$. Since χ is a character of G_c^+, we have $c(\chi_\ell) \leq v_\ell(c)$ for all ℓ. In particular, χ_ℓ is trivial on $\mathbb{Z}_\ell^\times$, so $c(\chi_\ell)$ is the smallest n such that χ_ℓ is trivial on $(1 + \ell^n \mathcal{O}_{F,\ell})^\times$, and thus agrees with the usual definition of the conductor of χ_ℓ when ℓ is inert in F. Similarly, if ℓ is ramified in F, say $\ell = \mathfrak{p}^2$, then $c(\chi_\ell)$ is twice the conductor of $\chi_\ell = \chi_\mathfrak{p}$:

$$F_{\mathfrak{p}}^{\times} \to \mathbb{C}^{\times},$$

though this case does not occur by our assumption $(c, D) = 1$. If $\ell = \mathfrak{p}_1\mathfrak{p}_2$ is split in F, then we can write $\chi_\ell = \chi_{\mathfrak{p}_1} \otimes \chi_{\mathfrak{p}_2}$ with $\chi_{\mathfrak{p}_1}$, $\chi_{\mathfrak{p}_2}$ characters of $\mathbb{Q}_\ell^{\times}$, which are inverses of each other on $\mathbb{Z}_\ell^{\times}$ as χ_ℓ is trivial on $\mathbb{Z}_\ell^{\times}$. Hence $\chi_{\mathfrak{p}_1}$ and $\chi_{\mathfrak{p}_2}$ have the same conductor, which is $c(\chi_\ell)$. Consequently, $c(\chi)$, the absolute norm of the conductor of χ, is

$$c(\chi) = \mathrm{Norm}\left(\prod_{\ell} \ell^{c(\chi_\ell)}\right) = \prod_{\ell} \ell^{2c(\chi_\ell)}, \tag{6.4.3}$$

where ℓ runs over all the primes of F but not the rational primes.

Note that since $(c, M) = 1$, we have $c(\chi_\ell) = 0$ whenever π_ℓ is ramified, i.e., the conductor $c(\pi_\ell) > 0$. If $c(\chi_\ell) = 0$, let $R_{\chi,\ell}$ be an Eichler order of reduced discriminant $\ell^{c(\pi_\ell)}$ in $\mathrm{M}_2(\mathbb{Q}_\ell)$ containing $\mathcal{O}_{F,\ell}$. If $c(\chi_\ell) > 0$, so π_ℓ is unramified, let $R_{\chi,\ell}$ be a maximal order of $\mathrm{M}_2(\mathbb{Q}_\ell)$ which optimally contains $\mathbb{Z}_\ell + \ell^{c(\chi_\ell)}\mathcal{O}_{F,\ell}$. In either case, $R_{\chi,\ell}$ is unique up to conjugacy and pointwise fixes a 1-dimensional subspace of π_ℓ. For $\ell < \infty$, take $\varphi_\ell \in \pi_\ell^{R_{\chi,\ell}}$ nonzero, normalized in such a way that $\otimes' \varphi_\ell$ converges. For instance, we can take $\varphi_\ell = \varphi_{\pi,\ell}$ at almost all ℓ. Each φ_ℓ is a local Gross-Prasad test vector [[41], Section 4.1], and our assumptions imply that the local Gross-Prasad test vectors φ_ℓ are (up to scalars) translates of the new vectors $\varphi_{\pi,\ell}$. (Gross-Prasad test vectors are not translates of new vectors in general.)

Embed F into $\mathrm{M}_2(\mathbb{Q})$ as follows. Consider a quadratic form

$$Q(x, y) = -\frac{C}{2}x^2 + Axy + \frac{B}{2}y^2 \in \mathcal{F}_{Dc^2}.$$

This means Q is primitive of discriminant $Dc^2 = A^2 + BC$, $2 \mid B$ and $2M \mid C$, which implies $A^2 \equiv Dc^2 \bmod 4$. Take the embedding of F into $\mathrm{M}_2(\mathbb{Q})$ induced by

$$\sqrt{D}c \mapsto \begin{pmatrix} A & B \\ C & -A \end{pmatrix}.$$

Then $\mathcal{O}_c = R_0 \cap F$, and

$$F_\infty^{\times} = \left\{ g(x, y) := \begin{pmatrix} x + A & By \\ Cy & x - Ay \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R}) \right\}.$$

For a prime $\ell \nmid c$, we have $\mathcal{O}_{c,\ell} = \mathcal{O}_{F,\ell} \subset R_{0,\ell}$. Thus we may take $R_{\chi,\ell} = R_{0,\ell}$ for $\ell \nmid c$ such that χ_ℓ is unramified, in particular, for $\ell \nmid cD$. When χ_ℓ is ramified, we may take $R_{\chi,\ell} = R_{0,\ell}$ if and only if $c(\chi_\ell) = v_\ell(c)$. By assumption,

$$c(\chi) = \prod_\ell \ell^{2c(\chi_\ell)} = c^2,$$

so we may take $R_{\chi,\ell} = R_{0,\ell}$ at each finite place ℓ. Thus we may and will take φ_ℓ to be $\varphi_{\pi,\ell}$ at each ℓ.

Now we describe φ_∞. Note we can identify $F_\infty^\times/\mathbb{Q}_\infty^\times$ with $F_\infty^1/\{\pm 1\}$, where

$$F_\infty^1 = F_\infty^{1,+} \cup F_\infty^{1,-},\ F_\infty^{1,\pm} = \{g(x,y) \in F_\infty^\times : \det g(x,y) = x^2 - Dc^2y^2 = \pm 1\}.$$

Let

$$\gamma_\infty = \begin{pmatrix} A + \sqrt{D}c & A - \sqrt{D}c \\ C & C \end{pmatrix}.$$

Then

$$\gamma_\infty^{-1} \begin{pmatrix} A & B \\ C & -A \end{pmatrix} \gamma_\infty = \begin{pmatrix} \sqrt{D}c & 0 \\ 0 & -\sqrt{D}c \end{pmatrix}.$$

So

$$\gamma_\infty^{-1} F_\infty^1 \gamma_\infty = \left\{ \begin{pmatrix} x + y\sqrt{D}c & 0 \\ 0 & x - y\sqrt{D}c \end{pmatrix} : x^2 - Dc^2y^2 = \pm 1 \right\}.$$

The maximal compact subgroup of F_∞^1 is

$$\Gamma_F = \gamma_\infty \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \gamma_\infty^{-1} = \{\pm I, \pm g(0, -(\sqrt{D}c)^{-1})\},$$

where one reads the $\pm$ signs independently. Let $U_\infty = \gamma_\infty \mathrm{O}(2) \gamma_\infty^{-1}$, where $\mathrm{O}(2)$ denotes the standard maximal compact subgroup of $\mathbf{GL}_2(\mathbb{R})$. Then $U_\infty \supset \Gamma_F$, and the archimedean test vector in [[41], Section 4.1] is the unique up to scalars nonzero vector φ_∞ lying in the minimal U_∞-type such that Γ_F acts by χ_∞ on φ_∞. Specifically, we can take

$$\varphi_\infty = \pi_\infty(\gamma_\infty)(\varphi_{\infty,k} \pm \varphi_{\infty,-k}), \tag{6.4.4}$$

where $\varphi_{\infty,\pm k} = \frac{1}{2}\pi_\infty \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix} \varphi_\pi$ is a vector of weight $\pm k$ in π_∞, and the $\pm$ sign in 6.4.4 matches the sign of $\chi_\infty \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. This completely describes the test vector φ chosen in [41].

For our purposes, we would like to work with a different archimedean component than φ_∞, corresponding to (a translate of) φ_π. Let φ^- be the pure tensor in π which agrees with φ at all finite places, and is defined like φ_∞ at infinity except using the opposite sign in the sum 6.4.4. Then necessarily any χ_∞-equivariant linear function on π_∞ kills φ^-_∞, so $P_\chi(\varphi^-) = 0$. Hence $P_\chi(\varphi) = P_\chi(\varphi')$ where $\varphi' = \varphi + \varphi^-$, and we can write $\varphi' = \otimes\varphi'_v$, where $\varphi'_\ell = \varphi_\ell$ for finite primes ℓ and $\varphi'_\infty = \pi_\infty(\gamma_\infty)\varphi_\pi$, i.e., $\varphi'(x) = \varphi_\pi(x\gamma_\infty)$.

Finally, we describe the vector φ'_π appearing in 6.4.2. It is defined to a factorizable function in π whose associated local Whittaker functions are new vectors whose zeta functions are the local L-factors of π at finite places, and at infinity is the vector in the minimal O(2)-type that transforms by χ_∞ under $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ such that the associated Whittaker function (restricted to first diagonal component) at infinity is

$$W_\infty(t) = 2\chi_\infty \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \mid t \mid^{k/2} e^{-2\pi|t|}.$$

(This normalization gives $L_\infty(s,\pi) = \int_0^\infty W_\infty(t) \mid t \mid^{s-1/2} d^\times t$.) Thus φ'_π agrees with φ_π at all finite places and $\varphi'_{\pi,\infty} = 2(\varphi_{\infty,k} \pm \varphi_{\infty,-k})$, where the $\pm$ sign matches that in 6.4.4.

Hence $\varphi = \frac{1}{2}\pi(\gamma_\infty)\varphi'_\pi$, so by invariance of the inner product we have $(\varphi,\varphi) = \frac{1}{4}(\varphi'_\pi, \varphi'_\pi)$, and 6.4.2 becomes

$$\mid P_\chi(\varphi') \mid^2 = \mid P_\chi(\varphi) \mid^2 = L(\pi_F \otimes \chi, 1/2) \cdot \frac{1}{\sqrt{D}c} \cdot \prod_{\ell \mid c} \left(\frac{\ell}{\ell - \chi_D(\ell)} \right)^2. \tag{6.4.5}$$

Now we want to rewrite $P_\chi(\varphi')$. Recall that $\epsilon_c > 1$ is the smallest totally positive power of a fundamental unit in $\mathcal{O}_c^\times$. From 6.3.2, we obtain the isomorphism

$$\mathbb{A}_\mathbb{Q}^\times F^\times \setminus \mathbb{A}_F^\times / \hat{\mathcal{O}}_c^\times \simeq G_c^+ \cdot (F_\infty^+ / \langle \epsilon_c \rangle \mathbb{Q}_\infty^+) \simeq G_c^+ \cdot (F_\infty^{1,+} / \langle \pm\epsilon_c \rangle).$$

We may identify

$$F_\infty^{1,+}/\langle \pm\epsilon_c\rangle = \left\{ \begin{pmatrix} x+Ay & By \\ Cy & x-Ay \end{pmatrix} \in \mathbf{SL}_2(\mathbb{R}) : 1 \le x + y\sqrt{D}c < \epsilon_c \right\},$$

and the orbit of $\gamma_\infty i$ in the upper half plane by this set is the geodesic segment connecting $\gamma_\infty i$ to $\epsilon_c\gamma_\infty i$, i.e., the image under γ_∞ of $\{iy : 1 \le y \le \epsilon_c^2\} \subset \mathcal{H}$. Let us call this arc Υ.

Since

$$\mathbb{A}_\mathbb{Q}^\times \subset F^\times \hat{\mathcal{O}}_c^\times F_\infty^+ \quad \text{and} \quad G_c^+ \simeq F^\times \setminus \mathbb{A}_F^\times / \hat{\mathcal{O}}_c^\times F_\infty^+,$$

where $F_\infty^+ = (\mathbb{R}_{>0})^2$, we see that χ is trivial on $\mathbb{A}_\mathbb{Q}^\times \hat{\mathcal{O}}_c^\times F_\infty^+$. The Tamagawa measure gives that

$$\mathrm{vol}(F^\times \mathbb{A}_\mathbb{Q}^\times \setminus \mathbb{A}_F^\times) = 2L(1,\eta) = 4h_F \log\epsilon_F \mathrm{vol}(\hat{\mathcal{O}}^\times),$$

where η is the quadratic character of $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$ attached to $F/\mathbb{Q}$ and ϵ_F is the fundamental unit of F. This implies that

$$\mathrm{vol}(\mathbb{A}_\mathbb{Q}^\times F^\times \setminus \mathbb{A}_F^\times / \hat{\mathcal{O}}_c^\times) = 2h_c^+ \mathrm{len}(\Upsilon),$$

where len(Υ)=2logϵ_c is the length of Υ with respect to the usual hyperbolic distance. Thus we compute

$$\begin{aligned} P_\chi(\varphi') &= 2\mathrm{vol}(\hat{\mathcal{O}}_c^\times) \sum_{t \in G_c^+} \chi^{-1}(t) \int_{F_\infty^{1,+}/\langle\pm\epsilon_c\rangle} \varphi_\pi(tg\gamma_\infty) dg \\ &= 4\mathrm{vol}(\hat{\mathcal{O}}_c^\times) \sum_{t \in G_c^+} \chi^{-1}(t) \int_1^{\epsilon_c} j(t\gamma_\infty \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}; i)^k f(t\gamma_\infty \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \cdot i) d^\times u \\ &= 2\mathrm{vol}(\hat{\mathcal{O}}_c^\times) \sum_{t \in G_c^+} \chi^{-1}(t) \int_1^{\epsilon_c^2} j(t\gamma_\infty \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}; i)^k f(t\gamma_\infty \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \cdot i) d^\times y, \end{aligned}$$

where we use that f has trivial central character and the substitution $y = u^2$ at the last step.

For ℓ a rational prime dividing c, note that

$$\mathcal{O}_{F,\ell}^\times / \mathcal{O}_{c,\ell}^\times \simeq \mathbb{Z}_\ell^\times / (1 + c\mathbb{Z}_\ell)$$

when ℓ splits in F and

$$\mathcal{O}_{F,\ell}^{\times}/\mathcal{O}_{c,\ell}^{\times} \simeq (\mathcal{O}_{F,\ell}^{\times}/(1+c\mathcal{O}_{F,\ell}))/(\mathbb{Z}_{\ell}^{\times}/(1+c\mathbb{Z}_{\ell}))$$

when ℓ is inert in F. Hence, with our choice of measures,

$$\mathrm{vol}(\hat{\mathcal{O}}_c^{\times}) = \mathrm{vol}(\hat{\mathcal{O}}_F^{\times})\prod_{\ell\mid c}[\mathcal{O}_{F,\ell}^{\times}:\mathcal{O}_{c,\ell}^{\times}]^{-1} = \frac{1}{\sqrt{D}}\prod_{\ell\mid c,(\frac{D}{\ell})=1}\frac{1}{(\ell-1)\ell^{v_\ell(c)-1}}\cdot\prod_{\ell\mid c,(\frac{D}{\ell})=-1}\frac{1}{(\ell+1)\ell^{v_\ell(c)}},$$

where ℓ runs over rational primes.

The next task is then to rewrite the integral appearing in the right-hand side of the above formula. Let $z = \gamma_\infty iy$. Then

$$z = \frac{A}{C} + \frac{\sqrt{D}c}{C}\left(1 - \frac{2}{1+iy}\right).$$

Since

$$\frac{2iy}{(1+iy)^2} = \frac{2}{1+iy} - \frac{1}{2}\left(\frac{2}{1+iy}\right)^2 = \frac{BC + 2ACz - C^2z^2}{2Dc^2},$$

we have

$$j\left(\gamma_\infty\begin{pmatrix} y & 0\\ 0 & 1\end{pmatrix}; i\right)^{-2} = \frac{C(1+iy)^2}{2\sqrt{D}cy} = \frac{2i\sqrt{D}c}{-Cz^2+2Az+B} = \frac{i\sqrt{D}c}{Q(z,1)},$$

and

$$dz = \frac{2iy\sqrt{D}c}{C(1+iy)^2}d^\times y \ \text{ i.e. } \ d^\times y = \frac{2\sqrt{D}c}{-Cz^2+2Az+B}dz = \frac{\sqrt{D}c}{Q(z,1)}dz.$$

Making the change of variable $z = \gamma_\infty iy$, the above expression can be rewritten as

$$P_\chi(\varphi') = \frac{2\mathrm{vol}(\hat{\mathcal{O}}_c^{\times})}{i^{k/2}\cdot(\sqrt{D}c)^{(k-2)/2}}\cdot\sum_{t\in G_c^+}\chi^{-1}(t)\int_\Upsilon f(tz)\cdot Q(z,1)^{(k-2)/2}dz.$$

After another change of variable $z' = tz$, the above integral becomes

$$\begin{aligned}\int_{t\Upsilon} f(z')\cdot Q(t^{-1}z',1)^{(k-2)/2}dz' &= \int_{t\Upsilon} f(z')\cdot(Q\mid t^{-1})(z',1)^{(k-2)/2}dz'\\ &= \int_{\tau_t}^{(t\epsilon_c t^{-1})\tau_t} f(z')\cdot(Q\mid t^{-1})(z',1)^{(k-2)/2}dz'\end{aligned}$$

where $\tau_t = t\gamma_\infty i$. Now, as long as t varies in G_c^+, the quadratic forms $Q\mid t^{-1}$ are representatives for the classes in $\mathcal{F}_{Dc^2}/\Gamma_0(M)$, as discussed in 6.2. Moreover, since Υ is closed in $\mathcal{H}/\Gamma_0(N)$, this integral does not depend on the choice of base point. Plugging this into 6.4.5 gives the asserted formula. □

6.5 Genus fields attached to orders

From now on, we assume that c is odd. The genus field attached to the order $\mathcal{O}_c$ of discriminant Dc^2 is the finite abelian extension of $\mathbb{Q}$, with Galois group isomorphic to copies of $\mathbb{Z}/2\mathbb{Z}$, contained in the strict class field H_c^+ of F of conductor c and generated by the quadratic extensions $\mathbb{Q}(\sqrt{D_i})$ and $\mathbb{Q}(\sqrt{\ell^*})$ where $D = \prod_i D_i$ is any possible factorization of D into primary discriminants, $\ell \mid c$ is a prime number and $\ell^* = (-1)^{(\ell-1)/2}\ell$. See [[9], pp. 242-244] for details.

Assume a quadratic character $\chi : G_c^+ \to \{\pm 1\}$ is primitive. By 6.4.3, this means $c(\chi) = c^2$. Then χ cuts out a quadratic extension H_χ/F which is biquadratic over $\mathbb{Q}$. Each quadratic extension of $\mathbb{Q}$ contained in the genus field of the order $\mathcal{O}_c$ is of the form $\mathbb{Q}(\sqrt{\Delta})$ for some $\Delta = D' \cdot \prod_{j=1}^{s} \ell_j^*$, with $\ell_j \mid c$ and D' a fundamental discriminant dividing D. Write $H_\chi = \mathbb{Q}(\sqrt{\Delta_1}, \sqrt{\Delta_2})$, with $\Delta_i = D_i \cdot \prod_{j=1}^{s_i} \ell_{i,j}^*$ for $i = 1, 2$ as above (so $\ell_{i,j}$ are primes dividing c), and let $K_1 = \mathbb{Q}(\sqrt{\Delta_1})$ and $K_2 = \mathbb{Q}(\sqrt{\Delta_2})$. Since the third quadratic extension contained in H_χ is the quadratic extension is $\mathbb{Q}(\sqrt{D})$, we have $\Delta_1 \cdot \Delta_2 = D \cdot x^2$ for some $x \in \mathbb{Q}^\times$. We can write $\Delta_1 = D_1 d$ and $\Delta_2 = D_2 d$ for some $d = \prod_{j=1}^{s} \ell_j^*$ with $\ell_i \mid c$ primes and $D = D_1 \cdot D_2$ a factorization into fundamental discriminants, allowing $D_1 = D$ or $D_2 = D$. If $d \neq \pm c$, then χ factors through the extension $H_d^+ \neq H_c^+$ by the genus theory of the order of conductor Dd^2, and therefore χ is not a primitive character of H_c^+. So $d = \pm c$. Therefore, we conclude that $K_1 = \mathbb{Q}(\sqrt{D_1 d})$ and $K_2 = \mathbb{Q}(\sqrt{D_2 d})$ of $\mathbb{Q}$ satisfy the following properties:

- $D_1 \cdot D_2 = D$, where D_1 and D_2 are two coprime fundamental discriminants (possibly equal to 1).
- $d = \pm c$ and d is a fundamental discriminant.

Let $\chi_{D_1 d}$ and $\chi_{D_2 d}$ be the quadratic characters attached to the extensions K_1 and K_2 respectively; thus $\chi_{D_1 d}(x) = \left(\dfrac{D_1 d}{x}\right)$ and $\chi_{D_2 d}(x) = \left(\dfrac{D_2 d}{x}\right)$. Let χ_D be the quadratic character attached to the extension $F/\mathbb{Q}$; thus $\chi_D(x) = \left(\dfrac{D}{x}\right)$. In particular, for all $\ell \nmid c$ we have

$$\chi_D(\ell) = \chi_{D_1 d}(\ell) \cdot \chi_{D_2 d}(\ell).$$

Say that χ has sign $+1$ if H_χ/F is totally real, and sign -1 otherwise. If χ has sign

$\omega_\infty \in \{\pm 1\}$, put $I_f = I_f^{\omega_\infty}$ and $\Omega_f = \Omega_f^{\omega_\infty}$. Define

$$\mathbb{L}(f,\chi) := \sum_{\sigma \in G_c^+} \chi^{-1}(\sigma) I_f\{\tau_0 \to \gamma_{\psi_\sigma}(\tau_0)\}(Q_{\psi_\sigma}(x,y)^{(k-2)/2}).$$

Lemma 6.5.1. $\overline{\mathbb{L}(f,\chi)} = \omega_\infty \cdot \mathbb{L}(f,\chi)$.

Proof. This follows from the discussion in [[46],§6.1]. Define

$$\Theta_\psi := I_f\{\tau_0 \to \gamma_\psi(\tau_0)\}(Q_\psi(x,y)^{(k-2)/2}),$$

which is independent of the choice of τ_0 and the $\Gamma_0(M)$-conjugacy class of ψ. Let $z \to \bar{z}$ denote complex conjugation. A direct computation shows that $\bar{\Theta}_\psi = \Theta_{\psi^*}$ where $\psi^* = \omega_\infty \psi \omega_\infty^{-1}$. From the discussion in 6.2, we have $\sigma_F \cdot [\psi] = [\psi^*]$, and it follows that $\bar{\Theta}_\psi = \Theta_{\sigma_F \psi}$. Taking sums over a set of representatives of optimal embeddings shows that $\overline{\mathbb{L}(f,\chi)} = \chi(\sigma_F) \cdot \mathbb{L}(f,\chi)$. Let H_χ be the field cut out by χ. The description of a system of representatives Σ_c and Σ_c^+ of $\mathrm{Gal}(H_c/F)$ and $\mathrm{Gal}(H_c^+/F)$ in 6.4 shows that if $\chi(\sigma_F) = 1$ then H_χ is contained in H_c, and therefore H_χ is totally real. On the other hand, if $\chi(\sigma_F) = -1$, then H_χ cannot be contained in H_c, and therefore it is not totally real, so it is the product of two imaginary extensions. By the definition of the sign of χ, this means that $\mathbb{L}(f,\chi)$ is a real number when χ is even, and is a purely imaginary complex number when χ is odd, and the result follows. □

Using the relation

$$L(\pi_g \times \pi_\chi, 1/2) = \tfrac{4}{(2\pi)^k} \left(\left(\frac{k-2}{2}\right)!\right)^2 L(f/F,\chi,k/2),$$

it follows from Lemma 6.5.1 that Theorem 6.4.1 can be rewritten in the following form:

$$L(f/F,\chi,k/2) = \frac{(2\pi i)^{k-2} \cdot \Omega_f^2 \cdot \omega_\infty}{\left(\left(\frac{k-2}{2}\right)!\right)^2 \cdot \alpha^2 \cdot (Dc^2)^{(k-1)/2}} \cdot \mathbb{L}(f,\chi)^2. \tag{6.5.1}$$

Remark 6.5.2. By the lemma, the sign ω_∞ should also appear in equation (28) of [4], as the left hand side of that equation is not positive when χ is odd. However, the main result in [4] still follows as this sign will cancel out with a sign arising from Gauss sums as in our argument in next chapter.

Chapter 7

p-adic L-functions

Recall the notation introduced in Chapter 4: f_∞ is the Hida family passing through the weight two modular form f of level $N = Mp$ associated to the elliptic curve E by modularity; U is a connected neighbourhood of 2 in the weight space $\mathcal{X}$. $\mu_*^\pm$ is a measure-valued modular symbol satisfying the property that for all integers $k \in U, k \geq 2$, there is $\lambda^\pm(k) \in \mathbb{C}_p^\times$ such that $\rho_k(\mu_*^\pm) = \lambda^\pm(k) I_{f_k}^\pm$ and $\lambda^\pm(2) = 1$.

Let $I_{f_k^\sharp}$ be the modular symbol attached to $f_k^\sharp$ via the choice of complex period Ω_k, which are introduced in section 4.1. The modular symbol satisfies the relation

$$I_{f_k}\{r \to s\}(P) = I_{f_k^\sharp}\{r \to s\}(P) - p^{k-2} a_p(k)^{-1} I_{f_k^\sharp}\{r/p \to s/p\}(P(x, y/p)).$$

7.1 The Mazur-Kitagawa p-adic L-function

Let χ:$(\mathbb{Z}/m\mathbb{Z})^\times \to \{\pm 1\}$ be a primitive quadratic Dirichlet character of conductor m with χ(-1)=$(-1)^{(k-2)/2}\omega_\infty$, and let

$$\tau(\chi) := \sum_{a=1}^{m} \chi(a) e^{2\pi i a/m}$$

denote the Gauss sum attached to χ. For each $k \in U \cap \mathbb{Z}^{\geq 2}$, $1 \leq j \leq k-1$ with j odd and let $\Omega_{f_k} = \Omega_{f_k}^{\omega_\infty}, \lambda(k) = \lambda^{\omega_\infty}(k), \mu_* = \mu_*^{\omega_\infty}$. The expression

$$L^{alg}(f_k, \chi, j) := \frac{(j-1)!\tau(\chi)}{(-2\pi i)^{j-1}\Omega_{f_k}} L(f_k, \chi, j)$$

belongs to K_{f_k}; it is called the algebraic part of the special value $L(f_k, \chi, j)$.

One defines $L^{alg}(f_k^\sharp, \chi, j)$ similarly, by replacing f_k by $f_k^\sharp$ in the definition above. We have

$$L^{alg}(f_k, \chi, j) = (1 - \chi(p)a_p(k)^{-1}p^{k-1-j})L^{alg}(f_k^\sharp, \chi, j).$$

We use the measure $\mu_*\{r \to s\}$ to define the Mazur-Kitagawa two variable p-adic L-function attached to f and a Dirichlet character χ:

Definition 7.1.1. Let χ be a primitive quadratic Dirichlet character of conductor m satisfying $\chi(-1)=(-1)^{(k-2)/2}\omega_\infty$. The Mazur-Kitagawa two-variable p-adic L-function attached to χ is the function of $(k, s) \in U \times \mathcal{H}$ defined by the rule:

$$L_p(f_\infty, \chi, k, s) = \sum_{a=1}^{m} \chi(pa) \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} (x - \frac{pa}{m}y)^{s-1} y^{k-s-1} d\mu_*\{\infty \to \frac{pa}{m}\}.$$

This function satisfies the following interpolation property with respect to special values of the classical L-function $L^{alg}(f_k, \chi, j)$.

Theorem 7.1.2. *Suppose that $k \in U \cap \mathbb{Z}^{\geqslant 2}$, and that $1 \leqslant j \leqslant k-1$ satisfies $\chi(-1) = (-1)^{j-1}\omega_\infty$. Then*

$$L_p(f_\infty, \chi, k, j) = \lambda(k)(1 - \chi(p)a_p(k)^{-1}p^{j-1})L^{alg}(f_k, \chi, j).$$

Proof. See Theorem 1.12 of [3]. □

Corollary 7.1.3. *Suppose that $\chi(-1) = (-1)^{k/2-1}\omega_\infty$. Then for all $k \in U \cap \mathbb{Z}^{\geq 2}$,*

$$L_p(f_\infty, \chi, k, j) = \lambda(k)(1 - \chi(p)a_p(k)^{-1}p^{j-1})(1 - \chi(p)a_p(k)^{-1}p^{k-1-j})L^{alg}(f_k^\sharp, \chi, j).$$

In particular, when $j = k/2$, one obtains

$$L_p(f_\infty, \chi, k, k/2) = \lambda(k)(1 - \chi(p)a_p(k)^{-1}p^{(k-2)/2})^2 L^{alg}(f_k^\sharp, \chi, k/2). \tag{7.1.1}$$

7.2 p-adic L-functions attached to real quadratic fields

Given $Q = Ax^2 + Bxy + Cy^2 \in \mathcal{F}_{Dc^2}$, let $\tau = \tau_Q$ and $\overline{\tau}$ be the root of the quadratic polynomial $Q(x, 1)$. For any $\kappa \in U$, define

$$Q(x, y)^{(\kappa-2)/2} = \exp_p(\frac{\kappa - 2}{2} \log_q(\langle Q(x, y)\rangle))$$

where $\exp_p$ is the p-adic exponential and for $x \in \mathbb{Q}_p$, we let $\langle x\rangle$ denote the principal unit of x, satisfying $x = p^{v_p(x)}\zeta\langle x\rangle$ for a $(p-1)$-th root of unity ζ. Recall the Hida family f_∞ introduced in Section 4.1.

Definition 7.2.1. Let $Q \in \mathcal{F}_{Dc^2}$ and let γ_{τ_Q} be the generator of the stabilizer of the root τ_Q of $Q(z, 1)$, chosen as in Section 3.4.

1. Let $r \in \mathbb{P}^1(\mathbb{Q})$. The partial square root p-adic L-function attached to f_∞, a choice of sign $\pm$ and Q is the function of $\kappa \in U$ defined by

$$\mathcal{L}_p^{\pm}(f_\infty/F, Q, \kappa) = \int_{(\mathbb{Z}_p^2)'} Q(x, y)^{\frac{(\kappa-2)}{2}} d\mu_*^{\pm}\{r \to \gamma_{\tau_Q}(r)\}(x, y).$$

2. Let χ be a character of G_c^+. The square root p-adic L-function attached to f_∞, a choice of sign $\pm$ and χ is the function of $\kappa \in U$ defined by

$$\mathcal{L}_p^{\pm}(f_\infty/F, \chi, \kappa) := \sum_{\sigma\in G_c^+} \chi^{-1}(\sigma)\mathcal{L}_p^{\pm}(f_\infty/F, Q^\sigma, \kappa).$$

3. The p-adic L-function attached to f_∞, the sign $\pm$ and χ is the function of $\kappa \in U$ defined by

$$L_p^{\pm}(f_\infty/F, \chi, \kappa) = \mathcal{L}_p^{\pm}(f_\infty/F, \chi, \kappa)^2.$$

Let $\chi : G_c^+ \to \{\pm1\}$ be a quadratic ring class character. Let ϵ be the sign of χ and set $\omega_\infty = \epsilon$. Denote $\mu_* = \mu_*^{\omega_\infty}$, $\Omega_{f_k} = \Omega_{f_k}^{\omega_\infty}$, $\lambda(k) = \lambda^{\omega_\infty}(k)$ and $L_p(f_\infty/F, \chi, k) = L_p^{\omega_\infty}(f_\infty/F, \chi, k)$. Recall the newform $f_k^\sharp$ whose p-stabilization is the weight k specialization of the Hida family f_∞ introduced in the section 4.1. Define the algebraic part of the central value of the L-function of the newform $f_k^\sharp$ twisted by χ to be

$$L^{alg}(f_k^\sharp/F, \chi, k/2) = \frac{(\frac{k}{2} - 1)!^2\sqrt{D}c}{(2\pi i)^{k-2}\Omega^2_{f_k^\sharp}} L(f_k^\sharp/F, \chi, k/2).$$

Proposition 7.2.2. *For all $k \in U \cap \mathbb{Z}^{\geq 2}$, for all $P \in P_k(\mathbb{C}_p)$ and for all $r, s \in \mathbb{P}$,*

$$\int_{(\mathbb{Z}_p^2)'} P(x,y) d\mu_*\{r \to s\}(x,y) = \lambda(k)(1 - a_p(k)^{-2}p^{k-2}) I_{f_k^\sharp}\{r \to s\}(P).$$

Proof. See the proof of Proposition 2.4 in [4]. □

Theorem 7.2.3. *For all integers $k \in U$, $k \geq 2$, we have*

$$L_p(f_\infty/F, \chi, k) = \lambda(k)^2 \cdot \alpha^2 (1 - a_p(k)^{-2}p^{k-2})^2 \cdot (Dc^2)^{\frac{k-2}{2}} \cdot L^{alg}(f_k^\sharp/F, \chi, k/2).$$

where $\alpha = 2 \prod_{\ell | c, (\frac{D}{\ell}) = -1} \ell$

Proof. By Definition 7.2.1 and Proposition 7.2.2

$$\begin{aligned} \mathcal{L}_p(f_\infty/F, Q, k) &= \int_{(\mathbb{Z}_p^2)'} Q(x,y)^{\frac{(k-2)}{2}} d\mu_*\{r \to \gamma_{\tau_Q}(r)\}(x,y) \\ &= \lambda(k)(1 - a_p(k)^{-2}p^{k-2}) I_{f_k^\sharp}\{r \to \gamma_{\tau_Q}(r)\}(Q^{(k-2)/2}). \end{aligned}$$

We get, in the notation of Section 6.5,

$$L_p(f_\infty/F, \chi, k) = \lambda(k)^2 \cdot (1 - a_p(k)^{-2}p^{k-2})^2 \cdot \mathbb{L}(f_k^\sharp, \chi)^2.$$

Then using 6.5.1 gives the result. □

7.3 A factorization formula for genus characters

Let $\chi : G_c^+ \to \{\pm 1\}$ be a primitive character, and let $\chi_{D_1 d} : \mathbb{Q}(\sqrt{D_1 d}) \to \{\pm 1\}$ and $\chi_{D_2 d} : \mathbb{Q}(\sqrt{D_2 d}) \to \{\pm 1\}$ be the associated quadratic Dirichlet characters.

Theorem 7.3.1. *The following equality*

$$L_p(f_\infty/F, \chi, \kappa) = \alpha^2 \cdot (Dc^2)^{\frac{\kappa-2}{2}} \cdot L_p(f_\infty, \chi_{D_1 d}, \kappa, \kappa/2) \cdot L_p(f_\infty, \chi_{D_2 d}, \kappa, \kappa/2)$$

holds for all $\kappa \in U$, where $\alpha = \prod_{\ell | c, (\frac{D}{\ell}) = -1} \ell.$

Proof. Let $\chi_{D_i d}$ denote the quadratic characters associated with the extension $\mathbb{Q}(\sqrt{D_i d})$. Since p is inert in F, we have $\chi_D(p) = -1$, and since $\chi_D(\ell) = \chi_{D_1 d}(\ell) \cdot \chi_{D_2 d}(\ell)$, we get

$$\chi_{D_1 d}(p) = -\chi_{D_2 d}(p).$$

It follows that Euler factor $(1 - a_p(k)^{-2}p^{k-2})^2$ appearing in Theorem 7.2.3 is equal to the product of the two Euler factors

$$(1 - \chi_{D_1d}(p)a_p(k)^{-1}p^{(k-2)/2})^2 \text{ and } (1 - \chi_{D_2d}(p)a_p(k)^{-1}p^{(k-2)/2})^2$$

appearing in the 7.1.1 above. By comparison of Euler factors, we see that for all even integers $k \geq 4$ in U we have

$$L(f_k^\sharp/F, \chi, s) = L(f_k^\sharp, \chi_{D_1d}, s) \cdot L(f_k^\sharp, \chi_{D_2d}, s). \tag{7.3.1}$$

Therefore, from Theorem 7.2.3 and the factorization formula 7.3.1, it follows that for all even integers $k \geq 4$ in U the following formula holds:

$$L_p(f_\infty/F, \chi, k) = \left(\frac{\alpha^2 \cdot \sqrt{D}c \cdot (Dc^2)^{(k-2)/2} \cdot \omega_\infty}{\tau(\chi_{D_1d}) \cdot \tau(\chi_{D_2d})}\right) \cdot L_p(f_\infty, \chi_{D_1d}, k, k/2) \cdot L_p(f_\infty, \chi_{D_2d}, k, k/2). \tag{7.3.2}$$

Since D_id are fundamental discriminants, $\tau(\chi_{D_id}) = \sqrt{D_id}$ (interpreting $\sqrt{x}$ as $i\sqrt{\mid x \mid}$ for $x < 0$), so

$$\frac{\sqrt{D}c}{\tau(\chi_{D_1d}) \cdot \tau(\chi_{D_2d})} = \omega_\infty,$$

and the formula in the statement holds for all even integers $k \geq 4$ in U. Since $\mathbb{Z} \cap U$ is a dense subset of U, and the two sides of equation 7.3.2 are continuous functions in U, they coincide on U. □

Chapter 8

The Main Result

Let the notation be as in the introduction: $E/\mathbb{Q}$ is an elliptic curve of conductor $N = Mp$ with $p \nmid M$, $p \neq 2$ and $F/\mathbb{Q}$ a real quadratic field of discriminant $D = D_F$ such that all primes dividing M are split in F and p is inert in F. Finally, $c \in \mathbb{Z}$ is a positive integer prime to ND and $\chi : G_c^+ \to \{\pm 1\}$ is a primitive quadratic character of the strict ring class field of conductor c of F. Let ω_∞ be the sign of χ and as above put $\mathcal{L}_p(f_\infty/F, Q, \kappa) = \mathcal{L}_p^{\omega_\infty}(f_\infty/F, Q, \kappa)$, $\mathcal{L}_p(f_\infty/F, \chi, \kappa) = \mathcal{L}_p^{\omega_\infty}(f_\infty/F, \chi, \kappa)$ and $L_p(f_\infty/F, \chi, \kappa) = L_p^{\omega_\infty}(f_\infty/F, \chi, \kappa)$.

We begin by observing that $\mathcal{L}_p(f_\infty/F, Q, 2) = 0$, since its value is $\mu_f\{r \to \gamma_{\tau_Q}(r)\}(\mathbb{P}^1(\mathbb{Q}_p))$, and the total measure of μ_f is zero. For the next result, let ω_M be the sign of the Atkin-Lehner involution acting on f. Also, let $\log_E$: $E(\mathbb{C}_p) \to \mathbb{C}$ denote the logarithmic map on $E(\mathbb{C}_p)$ induced from the Tate uniformization and the choice of the branch $\log_q$ of the logarithm fixed above.

Theorem 2. *For all quadratic characters $\chi : G_c^+ \to \{\pm 1\}$ we have*

$$\frac{d}{d\kappa}\mathcal{L}_p(f_\infty/F, \chi, \kappa)_{\kappa=2} = \frac{1}{2}(1 - \chi_{D_1 d}(-M)\omega_M)\log_E(P_\chi).$$

where P_χ is defined as in 1.

Proof. We have

$$\begin{aligned}\frac{d}{d\kappa}\mathcal{L}_Q(f_\infty/F, \chi, \kappa)_{\kappa=2} &= \frac{1}{2}\int_{(\mathbb{Z}_p^2)'}(\log_q(x - \tau_Q y) + \log_q(x - \bar{\tau}_Q y))d\mu_*\{r \to \gamma_{\tau_Q}(r)\} \\ &= \frac{1}{2}(\log_E(P_{\tau_Q}) + \log_E(\tau_p P_{\tau_Q})).\end{aligned}$$

By [3.5.2], $\tau_p(J_{\tau_Q}) = -\omega_M J_{\tau_Q}^{\sigma\tau_Q}$ and by [[4], Proposition 1.8], we know that $\chi(\sigma) = \chi_{D_1d}(-M)$, so the result follows summing over all Q. $\square$

Theorem 3. *Let χ be a primitive quadratic character of G_c^+ with associated Dirichlet characters χ_{D_1d} and χ_{D_2d}. Suppose that $\chi_{D_1d}(-M) = -\omega_M$. Then:*

(1) There is a point $\mathbf{P}_\chi$ in $E(H_\chi)^\chi$ and $n \in \mathbb{Q}^\times$ such that $\log_E(P_\chi) = n \cdot \log_E(\mathbf{P}_\chi)$.

(2) The point $\mathbf{P}_\chi$ is of infinite order if and only if $L'(E/F, \chi, 1) \neq 0$.

Proof. By Theorem 2 we have

$$\frac{1}{2}\frac{d^2}{d\kappa^2}L_p(f_\infty/F, \chi, \kappa)_{\kappa=2} = \log_E^2(P_\chi).$$

On the other hand, by the factorization of Theorem 7.3.1 we have

$$L_p(f_\infty/F, \chi, \kappa) = \alpha^2 \cdot (Dc^2)^{(\kappa-2)/2} \cdot L_p(f_\infty, \chi_{D_1d}, \kappa, \kappa/2) \cdot L_p(f_\infty, \chi_{D_2d}, \kappa, \kappa/2),$$

where the integer $\alpha = \prod_{\ell | c, (\frac{D}{\ell})=-1} \ell$. Let $\text{sign}(E, \chi_{D_id}) = -\omega_N \chi_{D_id}(-N)$, where ω_N is the sign of the Atkin-Lehner involution at N. This is the sign of the functional equation of the complex L-series $L(E, \chi_{D_id}, s)$. Since

$$\chi_{D_1d}(-N) \cdot \chi_{D_2d}(-N) = \chi_D(-N) = -1,$$

we may order the characters χ_{D_1d} and χ_{D_2d} in such a way that $\text{sign}(E, \chi_{D_1d}) = -1$ and $\text{sign}(E, \chi_{D_2d}) = +1$. So $\chi_{D_1d}(-N) = \omega_N$ and since $\chi_{D_1d}(-M) = -\omega_M$ it follows that $\chi_{D_1d}(p) = -\omega_p = a_p$. So the Mazur-Kitagawa p-adic L-function $L_p(f, \chi_{D_1d}, \kappa, s)$ has an exceptional zero at $(\kappa, s) = (2, 1)$ and its order of vanishing is at least 2. We may apply [[3], Theorem 5.4], [[42], Sec. 6] and [[43], Theorem 3.1], which show that there is a global point $\mathbf{P}_{\chi_{D_1d}} \in E(\mathbb{Q}\sqrt{D_1c})$ and a rational number $\ell_1 \in \mathbb{Q}^\times$ such that

$$\frac{d^2}{d\kappa^2}L_p(f_\infty, \chi_{D_1d}, \kappa, \kappa/2)_{\kappa=2} = \ell_1 \log_E^2(\mathbf{P}_{\chi_{D_1d}})$$

and this point is of infinite order if and only if $L'(E, \chi_{D_1d}, 1) \neq 0$. Moreover, $\ell_1 \equiv L^{alg}(f, \psi, 1) \bmod ((\mathbb{Q}^\times)^2)$ for any primitive Dirichlet character ψ for which $L(f, \psi, 1) \neq 0$ and such that $\psi(\ell) = \chi_{D_1d}(\ell)$ for all $\ell \mid M$ and $\psi(p) = -\chi_{D_1d}(p)$. Now

$$\ell_2 = \frac{1}{2}L_p(f_\infty, \chi_{D_2d}, 2, 1) = L^{alg}(E, \chi_{D_2d}, 1)$$

is a rational number which is non-zero if and only if $L(E, \chi_{D_2 d}, 1) \neq 0$. In this case, $\ell_1 \ell_2$ is a square: choose $t \in \mathbb{Q}^\times$ such that $t^2 = \ell_1 \ell_2$ if $\ell_2 \neq 0$ and $t = 1$ otherwise, and let $\mathbf{P}_\chi = \mathbf{P}_{\chi_{D_1 d}}$ in the first case and 0 otherwise. Now the first part of the theorem follows setting $n = \alpha \cdot t$. Finally, for the second part note that $L(E, \chi_{D_2 d}, 1) \neq 0$ if and only if $L'(E/F, \chi, 1) = 0$ thanks to the factorization 7.3.1. $\square$

Bibliography

[1] A. Ash and G. Stevens, *Modular forms in characteristic l and special values of their l-functions*, Duke Math. J **53** (1986), no. 3, 849–868.

[2] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR 0268123

[3] M. Bertolini and H. Darmon, *Hida families and rational points on elliptic curves*, Invent. Math. **168** (2007), no. 2, 371–431. MR 2289868

[4] ______, *The rationality of Stark-Heegner points over genus fields of real quadratic fields*, Annals of mathematics (2009), 343–370.

[5] M. Bertolini, H. Darmon, and P. Green, *Periods and points attached to quadratic algebras*, Heegner points and Rankin L-series **49** (2004), 323–367.

[6] D. Bump, *Automorphic forms and representations*, vol. 55, Cambridge University Press, 1998.

[7] J. Cassels and A. Frölich, *Algebraic number theory: proceedings of an instructional conference*, Academic Pr, 1967.

[8] J. Cogdell, *Lectures on l-functions, converse theorems, and functoriality for gl (n)*, Lectures in Automorphic L-functions (2004), 3–96.

[9] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer Science & Business Media, 2012.

[10] D.A. Cox, *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, vol. 34, John Wiley & Sons, 2011.

[11] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Ann. of Math. (2) **154** (2001), no. 3, 589–639. MR 1884617

[12] ______, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. MR 2020572

[13] H. Darmon and S. Dasgupta, *Elliptic units for real quadratic fields*, Annals of mathematics **163** (2006), no. 1, 301–346.

[14] S. Dasgupta, *Stark-Heegner points on modular Jacobians*, Ann. Sci. École Norm. Sup. (4) **38** (2005), no. 3, 427–469. MR 2166341

[15] S. Dasgupta and J. Teitelbaum, *The p-adic upper half plane*, This volume (2007).

[16] IM Gelfand and D. Kazhdan, *Representations of the group gl (n, k) where k is a local field*, Lie groups and their representations (Proc. Summer School, Bolyai János Math. Soc., Budapest, 1971) (1975), 95–118.

[17] L. Gerritzen and M. Van der Put, *Schottky groups and mumford curves*, vol. 817, Springer, 2006.

[18] D. Goldfeld and J. Hundley, *Automorphic representations and l-functions for the general linear group*, vol. 1, Cambridge University Press, 2011.

[19] M. Greenberg, *Stark-Heegner points and the cohomology of quaternionic Shimura varieties*, Duke Math. J. **147** (2009), no. 3, 541–575. MR 2510743

[20] M. Greenberg and M.A. Seveso, *p-adic families of cohomological modular forms for indefinite quaternion algebras and the Jacquet-Langlands correspondence*, Canad. J. Math. **68** (2016), no. 5, 961–998. MR 3536925

[21] M. Greenberg, M.A. Seveso, and S. Shahabi, *Modular p-adic L-functions attached to real quadratic fields and arithmetic applications*, J. Reine Angew. Math. **721** (2016), 167–231. MR 3574881

[22] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), no. 2, 407–447. MR 1198816 (93m:11054)

[23] B. Gross, *Heegner points on* $x_0(n)$, 1984, pp. 87–106.

[24] B. Gross, W. Kohnen, and D. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), no. 1-4, 497–562. MR 909238

[25] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 833192 (87j:11057)

[26] X. Guitart and M. Masdeu, *Computation of ATR Darmon points on nongeometrically modular elliptic curves*, Exp. Math. **22** (2013), no. 1, 85–98. MR 3038785

[27] ———, *Overconvergent cohomology and quaternionic Darmon points*, J. Lond. Math. Soc. (2) **90** (2014), no. 2, 495–524. MR 3263962

[28] ———, *Elementary matrix decomposition and the computation of Darmon points with higher conductor*, Math. Comp. **84** (2015), no. 292, 875–893. MR 3290967

[29] ———, *A p-adic construction of ATR points on* $\mathbb{Q}$*-curves*, Publ. Mat. **59** (2015), no. 2, 511–545. MR 3374616

[30] X. Guitart, M. Masdeu, and Mehmet H. ¸Sengün, *Darmon points on elliptic curves over number fields of arbitrary signature*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 2, 484–518. MR 3384519

[31] E. Hewitt and K.A. Ross, *Abstract harmonic analysis: Volume i structure of topological groups integration theory group representations*, vol. 115, Springer Science & Business Media, 2012.

[32] H. Jacquet, I.I. Piatetski-Shapiro, and J. Shalika, *Automorphic forms on gl (3) i*, Annals of Mathematics **109** (1979), no. 1, 169–212.

[33] N. Koblitz, *P-adic numbers*, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer, 1977, pp. 1–20.

[34] W. Kohnen and D. Zagier, *Modular forms with rational periods*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 197–249. MR 803368

[35] S. Lang, *Introduction to modular forms*, vol. 222, Springer Science & Business Media, 2012.

[36] M. Longo, V. Rotger, and S. Vigni, *On rigid analytic uniformizations of Jacobians of Shimura curves*, Amer. J. Math. **134** (2012), no. 5, 1197–1246. MR 2975234

[37] ______, *Special values of L-functions and the arithmetic of Darmon points*, J. Reine Angew. Math. **684** (2013), 199–244. MR 3181561

[38] M. Longo and S. Vigni, *The rationality of quaternionic Darmon points over genus fields of real quadratic fields*, Int. Math. Res. Not. IMRN (2014), no. 13, 3632–3691. MR 3229764

[39] ______, *Quaternionic Darmon points on abelian varieties*, Riv. Math. Univ. Parma (N.S.) **7** (2016), no. 1, 39–70. MR 3675402

[40] J.I. Manin, *Periods of parabolic forms and p-adic hecke series*, Selected Papers Of Yu I Manin, World Scientific, 1996, pp. 268–290.

[41] K. Martin and D. Whitehouse, *Central L-values and toric periods for* GL(2), Int. Math. Res. Not. IMRN (2009), no. 1, Art. ID rnn127, 141–191. MR 2471298

[42] C.P. Mok, *Heegner points and p-adic l-functions for elliptic curves over certain totally real fields*, Commentarii Mathematici Helvetici **86** (2011), no. 4, 867–945.

[43] ______, *On a theorem of bertolini-darmon about rationality of stark-heegner points over genus fields of real quadratic fields*, arXiv preprint arXiv:1801.09285 (2018).

[44] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859 (2000m:11104)

[45] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, vol. 323, Springer Science & Business Media, 2013.

[46] A.A. Popa, *Central values of rankin l-series over real quadratic fields*, Compositio Mathematica **142** (2006), no. 4, 811–866.

[47] V. Rotger and M.A. Seveso, *$\mathscr{L}$-invariants and Darmon cycles attached to modular forms*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 6, 1955–1999. MR 2984593

[48] P. Schneider and U. Stuhler, *The cohomology of p-adic symmetric spaces*, Inventiones mathematicae **105** (1991), no. 1, 47–122.

[49] M.A. Seveso, *p-adic L-functions and the rationality of Darmon cycles*, Canad. J. Math. **64** (2012), no. 5, 1122–1181. MR 2979580

[50] J.A. Shalika, *The multiplicity one theorem for gln*, Annals of mathematics (1974), 171–193.

[51] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, vol. 1, Princeton university press, 1971.

[52] J.H. Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[53] ———, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 2013.

[54] M. Trifković, *Stark-Heegner points on elliptic curves defined over imaginary quadratic fields*, Duke Math. J. **135** (2006), no. 3, 415–453. MR 2272972

[55] A. Weil, *Adeles and algebraic groups*, vol. 23, Springer Science & Business Media, 2012.