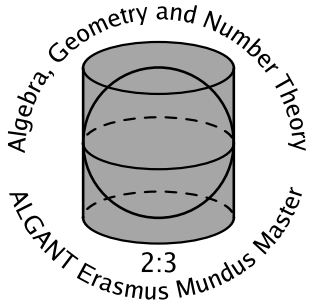
Rajneesh Kumar Singh

Anticyclotomic p-adic L-functions Attached To Elliptic Curves Over Imaginary Quadratic-Fields

Master's thesis, defended on August 15, 2007

Supervised By : Prof.Dr. Adrian Iovita &
Prof.Dr. Bas Edixhoven



Mathematisch Instituut
Universiteit Leiden

Contents

Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, let E have a good ordinary reduction at a prime p, $p \neq 2$ and let K be an imaginary quadratic field of discriminant D_K. Write K_∞/K for the anticyclotomic $\mathbb{Z}_p$-extension of K and set $G_\infty = \mathrm{Gal}(K_\infty/K)$. It will be assumed throughout that the discriminant of K is prime to N, so that K determines a factorisation

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

where N^+ (resp.N^-) is divisible only by primes different from p which are split (resp. inert) in K. Also we will assume that N^- is the square-free product of an odd number of primes.

Let us recall the definition of anticyclotomic extension of an imaginary quadratic number field K. It is known that if $\widetilde{K}_\infty$ is the compositum of all $\mathbb{Z}_p$-extensions of K (i.e. of Galois extensions F of K with $\mathrm{Gal}(F/K)$ topologically isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers) then $\mathrm{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Let K^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of K (i.e. unique $\mathbb{Z}_p$- extension of K in $K(\mu_{p^\infty})$, where μ_{p^∞} the group of all p power roots of 1). Then there exist a unique $\mathbb{Z}_p$-extension of K, K^{acyc}, such that $K^{acyc} \cap K^{cyc} = K$ and K^{acyc} is galois over $\mathbb{Q}$. This K^{acyc} is called the anticyclotomic extension of K.

In this thesis we study the works of Bertolini-Darmon [BD01] on how to attach an anticyclotomic p-adic L-function to the data consisting of such an elliptic curve E over $\mathbb{Q}$ and such a quadratic imaginary field K.

For an elliptic curve E defined over $\mathbb{Q}$ and a non-archimedean place p, the curve E is said to have good reduction at p if it extends to a smooth integral projective model over the ring of integers $\mathbb{Z}_p$ of $\mathbb{Q}_p$. In this case, reduction modulo p gives rise to an elliptic curve over the residue field $\mathbb{F}_p$. we set

$$a_p := p + 1 - \#E(\mathbb{F}_p).$$

The curve E is said to have split (resp. non-split) multiplicative reduction at p if there is a projective model of E over $\mathbb{Z}_p$ for which the corresponding reduced curve has a node

with tangent lines having slopes defined over $\mathbb{F}_p$ (resp. over the quadratic extension of $\mathbb{F}_p$ but not over $\mathbb{F}_p$). For more details see ([Si], Arithmetic of elliptic curves, Silverman). For $s \in \mathbb{C}$ define the $\mathbb{C}$-valued local L-function at p by setting $L(E/\mathbb{Q}_p, s)$ to be

$$\begin{array}{rl} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{if } E \text{ has good reduction at } p, \\ (1 - p^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } p, \\ (1 + p^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 1 & \text{otherwise.} \end{array}$$

And we complete the definition to the archimedean place ∞ by setting

$$L(E/\mathbb{R}, s) = (2\pi)^{-s}\Gamma(s).$$

Our strategy for attaching an anticyclotomic p-adic L-fuction to (E, K) will be as follows. Thanks to the deep work of Wiles et.al. it is now known that every elliptic curve over $\mathbb{Q}$ is modular, i.e. there exists a cuspidal eigenform f of weight 2 on $\Gamma_0(N)$ for some N (N can be choosen to be the conductor of E) such that

$$L(E/\mathbb{Q}, s) = L(f, s), \tag{0.1}$$

where

$$L(E/\mathbb{Q}, s) = \prod_{v \neq \infty} L(E/\mathbb{Q}_v, s). \tag{0.2}$$

The infinite product in this equation converges for $\mathrm{Re}(s) > \frac{3}{2}$.

Let χ be a Dirichlet character mod N. Since f is cusp form, it has Fourier series $f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$ and the corresponding L-function $L(f, s)$ is defined by

$$L(f, s) = \sum_{n \geq 1} a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^s \frac{dt}{t}. \tag{0.3}$$

The function $L(f, \chi, s)$ is defined by

$$L(f, \chi, s) = L(f_\chi, s)$$

where $f_\chi = f_\chi(z) = \sum_n \chi(n) a_n e^{2\pi i n z}$.
Let M be a fixed integer greater than 0 and prime to p. Set:

$$\begin{aligned} \mathbb{Z}_{p,M} &= \varprojlim_{\nu} \left(\frac{\mathbb{Z}}{p^\nu M\mathbb{Z}} \right) \\ &= \varprojlim_{\nu} \left(\frac{\mathbb{Z}}{p^\nu \mathbb{Z}} \times \frac{\mathbb{Z}}{M\mathbb{Z}} \right) \\ &= \mathbb{Z}_p \times \frac{\mathbb{Z}}{M\mathbb{Z}} \end{aligned}$$

$$\mathbb{Z}_{p,M}^* \quad = \quad \mathbb{Z}_p^* \times \left(\frac{\mathbb{Z}}{M\mathbb{Z}}\right)^* .$$

We will see in chapter I (section 1.9) using modular symbol and the eigenform f which has eigenvalue a_p for the Hecke operator T_p that we can define a measure $\mu_{f,\alpha}$ on $\mathbb{Z}_{p,M}^*$, where α is the p-adic unit root of the equation $X^2 - a_p X + p = 0$.
Let $\bar{\mathbb{Q}}$ be algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We fix an embedding

$$i : \bar{\mathbb{Q}} \longrightarrow \mathbb{C}_p$$

For $x \in \mathbb{Z}_p^*$ we can write uniquely,

$$x = \omega(x) \cdot < x > \tag{0.4}$$

where $\omega(x)$ is a root of unity and where

$$< x > \in 1 + p\mathbb{Z}_p \ . \tag{0.5}$$

Now the p-adic L-function for the cusp form f of weight 2 on $\Gamma_0(N)$ is defined by

$$L_p(f, \chi, s) = \int_{\mathbb{Z}_{p,M}^*} < x >^{s-1} \chi(x) \mu_{f,\alpha}(x).$$

This L-function $L_p(f, \chi, s)$ is the cyclotomic p-adic L-function attached to E. In chapter I our work is motivated to calculate $L(f, \chi, s), L_p(f, \chi, s)$. At the end of the first chapter we relate special values of the L-function with special values of the p-adic L-function.

In chapter II we study the basic notions regarding quaternion algebras over an arbitrary field. The main result of this chapter is that all quaternion algebras are simple central algebras, all simple central algebras of dimension 4 are quaternion algebras and if H is a quaternion algebra over field F then it is either isomorphic to $M_2(F)$ or it is a division algebra.

In chapter III we deal with quaternion algebras over local fields. The main result of this chapter is theorem 3.1.1 which gives a classification of quaternion algebras over local fields. Also we study the structure of $M_2(F)$ where F is a local field and a notion relating to Bruhat-Tits trees. Also we study here the zeta function for quaternion algebras over local fields.

In chapter IV our aim is to give a classification of quaternion algebras over global fields analogous to case of a local field. But due to lack of time we content ourselves by defining the concept of adeles and giving references where the classification results can be found.

The 5th chapter form the heart of this thesis. There we study how to attach an anticyclotomic p-adic L-function to an elliptic curve over an imaginary quadratic field K, so we need a measure on $G_\infty = \mathrm{Gal}(K_\infty/K)$.

Let B be the definite quaternion algebra over $\mathbb{Q}$ ramified exactly at the primes dividing N^-. That is to say, the algebra $B \otimes \mathbb{R}$ is isomorphic to Hamiltonian's real quaternions, and for each prime l the ring $B_l := B \otimes \mathbb{Q}_l$ is isomorphic to the matrix algebra $M_2(\mathbb{Q}_l)$ if l does not divide N^-, and to the quaternion division algebra over $\mathbb{Q}_l$ otherwise. The assumption on N^- ensures the existence of this quaternion algebra and it is unique up to isomorphism from the classification of quaternion algebras over global fields.

Let K be a quadratic algebra of discriminant prime to N which embeds in B. Since B is definite of discriminant N^-, the algebra K is an imaginary quadratic field in which all prime divisors of N^- are inert. Let $\mathcal{O}_K$ denote the ring of integers of K and let $\mathcal{O} = \mathcal{O}_K[1/p]$ be the maximal $\mathbb{Z}[1/p]$-order in K. Let R be an Eichler $\mathbb{Z}[\frac{1}{p}]$-order of level N^+.

Fix an embedding

$$\Psi : K \longrightarrow B \text{ satisfying } \Psi(K) \cap R = \Psi(\mathcal{O}).$$

Such a Ψ exists because all the primes dividing N^+ are split in K. Since $p \nmid N^-$, $B \otimes \mathbb{Q}_p = M_2(\mathbb{Q}_p)$. Now Ψ induces a map from

$$K_p{}^* = (K \otimes \mathbb{Q}_p)^* \hookrightarrow B_p^* = (B \otimes \mathbb{Q}_p)^* = GL_2(\mathbb{Q}_p)$$

since $\mathbb{Q}_p{}^* \subset K_p{}^*$ and $\mathbb{Q}_p{}^*$ is embedded in $GL_2(\mathbb{Q}_p)$ by

$$\mathrm{a} \to \begin{pmatrix} \mathrm{a} & 0 \\ 0 & \mathrm{a} \end{pmatrix}.$$

Hence this yields an action of $K_p{}^*/\mathbb{Q}_p{}^*$ on the Bruhat-Tits tree $\mathcal{T}$ of $PGL_2(\mathbb{Q}_p)$.
Since K is unramified at p, we only have to deal with two cases, one when p remains inert in K, another when p splits in K. In the first case we know from global class field theory $G_\infty = \mathrm{Gal}(K_\infty/K) = (K_p{}^*/\mathbb{Q}_p{}^*)/(\mu_{p^2-1}/\mu_{p-1})$. In the first case our aim is to define a measure on $K_p{}^*/\mathbb{Q}_p{}^*$ which is isomorphic to $\mathbb{Z}_p \times \frac{\mathbb{Z}}{M\mathbb{Z}}$ with $M = p+1$. For that we consider a modular form f of weight 2 defined on a quaternion algebra B of level $\hat{R}^*$, i.e. f is a function from $B^* \backslash \hat{B}^* / \hat{R}^*$ taking values in $\mathbb{Z}_p$. We use then the following theorem which is a consequence of the strong approximation theorem to simplify the definition of modular forms on quaternion algebra :

Theorem 0.0.1 *.Let p be a prime at which the quaternion algebra B is split. Then the natural map*

$$R^* \backslash B_p^* / R_p^* \longrightarrow B^* \backslash \hat{B}^* / \hat{R}^*$$

which sends the class represented by b_p to the class of the idele $(...1, b_p, 1, ...)$ is a bijection.

For more details see (Vi80, chapter III , section 3 and 4).

In our case $B^*\backslash\hat{B}^*/\hat{R}^* \cong R^*\backslash B_p^*/(\mathbb{Q}_p^* GL_2(\mathbb{Z}_p)) \cong \Gamma\backslash GL_2(\mathbb{Q}_p)/(\mathbb{Q}_p^* GL_2(\mathbb{Z}_p)) = \Gamma\backslash\mathcal{V}(\mathcal{T})$, where $\Gamma = R^*$ and $\mathcal{V}(\mathcal{T})$ the set of vertices of the Bruhat-Tits tree. That is the modular form f on a quaternion algebra B of weight 2 and level $\hat{R}^*$ that is a $\mathbb{Z}_p$-valued function on $\mathcal{V}(\mathcal{T})$, which is Γ-invariant.

Denote by $\mathcal{M}_2(B)$ the space of such modular forms. It is a free $\mathbb{Z}_p$-module of finite rank.

From the Jacquet-Langlands theorem there exist an eigenform belonging $\mathcal{M}_2(B)$ denoted by f by abuse of notations for all $T_l,\ \ l \not| N$ such that $f_{|T_l} = a_l.f$ (a_l are the ones for f_E). Using this eigenform we define a measure on ${K_p}^*/{\mathbb{Q}_p}^*$.

In the second case when p splits in K, from global class field theory we know that

$$\left({K_p}^*/\mu_{p-1}{\mathbb{Q}_p}^*\right)/{u_p}^{\mathbb{Z}} \cong G_\infty = \mathrm{Gal}(K_\infty/K)$$

where u_p is the generator of p-units of $\mathcal{O}_K\left[\frac{1}{p}\right]$ of norm 1. Analogously to the previous case we define a measure on $\left({K_p}^*/{\mathbb{Q}_p}^*\right)/{u_p}^{\mathbb{Z}}$ which is isomorphic to $\mathbb{Z}_p \times \frac{\mathbb{Z}}{M\mathbb{Z}}$ with $M = p-1$. Again we relate special values of the p-adic L-function in terms of the classical L-function.

The motivation behind attaching a p-adic L-functions is this: we have a complex L-functions attached to E and it is defined by an Euler product. While studying p-adic L-functions in general we see that values taken by these functions on special points in the common domain of the corresponding classical L-functions differ by a scalar multiple. Hence we expect p-adic L-function should also have arithmetic information.
This is also well understood conjecturally in the form of "**Main conjectures** ". As it is well known from section 2 of [BD01], we attach to the data $(E,\ K,\ p)$ an anticyclotomic p-adic L-function $L_p(E,K)$ which belongs to the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[G_\infty]]$. To an elliptic curve E over a number field F, we can attach a Selmer group. Take its p-primary part and call is $S(F)$. Take direct limit

$$\varinjlim_{\substack{K \subset F \subset K^{acyc} \\ F/K \ \text{finite}}} S(F) =: S(K^{acyc}).$$

Now take its Pontryagin dual

$$X := Hom\left(S(K^{acyc}), \mathbb{Q}_p/\mathbb{Z}_p\right).$$

It is known that X is a compact Λ- module. This comes from a deep theorem of **Kato**. There is a nice structure theorem for modules like these and we can attach a characteristic power series $\mathcal{C}$, which is well defined up to units in Λ. The **Main conjecture** says that the characteristic power series $\mathcal{C}$ divides the p-adic L-function which is proved under a mild technical assumption by Bertolini-Darmon in section 2 of [BD01].

1 Modular Symbols, Measures and L-Functions

1.1 Elementary Notions

Throughout this section we will deal with non co-compact arithmetic subgroups of $SL_2(\mathbb{R})$. Γ denote a congruence subgroup, i.e. a subgroup of $SL_2(\mathbb{Z})$ which contains the homogeneous principal congruence subgroup

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\bmod N) \right\}$$

for some positive integer N. For example $SL_2(\mathbb{Z})$ is the full congruence group of level 1, and the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} (\bmod N) \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} (\bmod N) \right\}$$

where "*" means "unspecified " and satisfying

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}).$$

Let us denote by $\mathcal{H}$ the upper half plane:

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

Let $GL_2(\mathbb{R})^+$ denote the subgroup of $GL_2(\mathbb{R})$ of matrices with positive determinant. If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ belongs to $GL_2(\mathbb{R})^+$, set:

$$\rho(A)(z) = \frac{\det(A)^{\frac{1}{2}}}{cz + d}. \tag{1.1}$$

In particular if $A \in \mathbb{SL}_2(\mathbb{Z})$, then $\rho(A)(z) = (cz + d)^{-1}$.

We have an action of $GL_2(\mathbb{R})$ on the Riemann Sphere $\mathbb{C} \cup \{\infty\}$ via

$$A(z) = \frac{az+b}{cz+d},$$

where

$$\begin{aligned} A(\infty) &= \frac{a}{c} \text{ if } c \neq 0 \\ &= \infty \text{ if } c = 0 \end{aligned}$$

This formula implies that $GL_2(\mathbb{R})^+$ acts on the upper half plane $\mathcal{H}$.

Definition 1.1.1 . *Let k be an integer. A meromorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is **weakly modular of weight** k and level 1 if*

$$f(A(z)) = (cz+d)^k f(z) \text{ for } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \text{ and } z \in \mathcal{H}.$$

Since $SL_2(\mathbb{Z})$ contains the translation matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : z \longmapsto z+1,$$

for which the factor $cz+d$ is simply 1, we have that $f(z+1) = f(z)$ for every weakly modular function $f : \mathcal{H} \longrightarrow \mathbb{C}$. That is, weakly modular functions are $\mathbb{Z}$-periodic. Let $D = \{\mathrm{q} \in \mathbb{C} : |\mathrm{q}| < 1\}$ be the open complex disk, let $D' = D - 0$, and recall from complex analysis that the $\mathbb{Z}$-periodic holomorphic map $z \mapsto e^{2\pi i z} = \mathrm{q}$ takes $\mathcal{H}$ to D'. Thus, corresponding to f, the function $g : D' \to \mathbb{C}$ where $g(\mathrm{q}) = f(\log(\mathrm{q})/(2\pi i))$ is well defined even though the logarithm is only determined up to $2\pi i\mathbb{Z}$, and $f(z) = g(e^{2\pi i z})$. If f is holomorphic on the upper half plane then the composition is holomorphic on the punctured disk since the logarithm can be defined holomorphically about each point, and so g has a Laurent expansion $g(\mathrm{q}) = \sum_{n\in\mathbb{Z}} a_n \mathrm{q}^n$ for $\mathrm{q} \in D'$. The relation $|\mathrm{q}| = e^{-2\pi \mathrm{Im}(z)}$ shows that $\mathrm{q} \to 0$ as $\mathrm{Im}(z) \to \infty$. Define f to be holomorphic at ∞ if g extends holomorphically to the puncture point $\mathrm{q} = 0$, i.e., the Laurent series sums over $n \in \mathbb{N}$. This means that f has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n(f)\mathrm{q}^n, \ \mathrm{q} = e^{2\pi i z}.$$

Since $\mathrm{q} \to 0$ if and only if $\mathrm{Im}(z) \to \infty$, showing that a weakly modular holomorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ doesn't require computing its Fourier expansion, only showing that $\lim_{\mathrm{Im}(z)\to\infty} f(z)$ exists or even just that $f(z)$ is bounded as $\mathrm{Im}(z) \to \infty$. For more details see([DS] chapter I).

Definition 1.1.2 *: Let k be an integer and $f : \mathcal{H} \longrightarrow \mathbb{C}$ be a meromorphic function, then we say f is modular form of weight k and level 1 if*
(1) *f is weakly modular of weight k,*
(2) *f is holomorphic on $\mathcal{H}$,*
(3) *f is holomorphic at ∞.*

The set of modular forms of weight k and level 1 is denoted $\mathcal{M}_k(SL_2(\mathbb{Z}))$.

Let k be a positive integer. For any complex valued function f on $\mathcal{H}$, we define the action of an element A of $GL_2(\mathbb{R})^+$ by

$$\left(f_{|[A]_k}\right)(z) = (\rho(A)(z))^k f(Az).$$

This is a right action of $GL_2(\mathbb{R})^+$ on the set of $\mathbb{C}$-valued function on $\mathcal{H}$:

$$f_{|[AB]_k} = \left(f_{|[A]_k}\right)_{|[B]_k}.$$

For a congruence group Γ, a Γ-equivalence class of points in $\mathbb{Q} \cup \{\infty\}$ is called a cusp of Γ.

Definition 1.1.3 *: A complex valued function f(z) is called a Γ -automorphic form of weight k if it satisfies the following conditions :*
(1)$f_{|[A]_k} \equiv f$, *i.e.*

$$f(A(z)) = (cz+d)^k f(z)$$

for all $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$,
(2) *f is holomorphic on $\mathcal{H}$; and*
(3) *f is holomorphic at every cusp of Γ.*

The space of such functions will be denoted by $\mathcal{M}_k(\Gamma)$.

For congruence subgroups, elements of $\mathcal{M}_k(\Gamma)$ are often called modular forms(or modular forms of level N if $\Gamma = \Gamma(N)$). If χ is a Dirichlet character modulo N (a character of $(\mathbb{Z}/N\mathbb{Z})^*$ extended in the obvious way to $\mathbb{Z}$), and $f(z)$ satisfies (in place of (1) in definition 1.1.3)

$$f(A(z)) = \chi(d)^{-1}(cz+d)^k f(z),$$

for all $A \in \Gamma_0(N)$, then f is an automorphic form of weight k and character χ. The space of all such function is denoted by $\mathcal{M}_k(N,\chi)$. For more details see ([G], chapter I)

If Γ is the conguence group $\Gamma_0(N)$, the Fourier expansion at ∞ of any f in $\mathcal{M}_k(\Gamma)$ will be of the form

$$f(z) = \sum_{n=0}^{\infty} a_n(f)\mathrm{q}^n, \ \mathrm{q} = e^{2\pi i z}.$$

Definition 1.1.4 *: A Γ-automorphic form is a cusp form if it vanishes at every cusp of Γ, i.e., its zeroth Fourier coefficients at each cusp is zero.*

The space of Γ -cusp forms of weight k and character χ will be denoted $\mathcal{S}_k(\Gamma,\chi)$.

For every $\gamma \in GL_2(\mathbb{Q})^+$, we can write $\gamma = \alpha\gamma'$, where $\alpha \in SL_2(\mathbb{Z})$ and $\gamma' = \mathrm{r}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ with $\mathrm{r} \in \mathbb{Q}^+$ and $a, b, d \in \mathbb{Z}$ relatively prime. Using this, we will show that for a given $f \in \mathcal{M}_k(\Gamma)$ for some congruence subgroup Γ and given such a $\gamma = \alpha\gamma'$, if the Fourier expansion for $f_{|_{[\alpha]_k}}$ has constant term 0, then the same holds for $f_{|_{[\gamma]_k}}$ too.

Since $\alpha \in SL_2(\mathbb{Z})$, then $\alpha^{-1}\Gamma\alpha$ is also a congruence subgroup. So $\alpha^{-1}\Gamma\alpha$ contains a matrix $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ for some minimal $h \in \mathbb{Z}^+$. This implies that $f_{|[\alpha]_k}$ has a Fourier expansion, so $f_{|[\gamma]_k}$ has one too. The Fourier expansion for $f_{|[\alpha]_k}$ is :

$$f_{|[\alpha]_k}(z) = \sum_{n=0}^{\infty} a_n(f_{|[\alpha]_k})\mathrm{q}^n,\ \mathrm{q} = e^{2\pi iz/h}\ .$$

Now,

$$\gamma^{-1}\Gamma\gamma = \frac{1}{ad}\begin{bmatrix} d & -b \\ 0 & a \end{bmatrix}\alpha^{-1}\Gamma\alpha\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

contains a matrix $\begin{bmatrix} 1 & dh \\ 0 & 1 \end{bmatrix}$. This implies that $f_{|[\gamma]_k}$ has Fourier expansion

$$f_{|[\gamma]_k}(z) = \sum_{n=0}^{\infty} a_n(f_{|[\gamma]_k})\mathrm{q}^n,\ \mathrm{q} = e^{2\pi iz/dh}\ .$$

From the above calculation, we get that if the Fourier expansion for $f_{|[\alpha]_k}$ has constant term 0 , then $f_{|[\gamma]_\mathrm{k}}$ does so too. Thus we are done. For more details see ([DS] chapter I, page 24)

Now we are going to introduce the *double coset operator* to understand Hecke operators. For more details for next section see ([DS] chapter V).

1.2 The Double Coset Operator

Let Γ_1 and Γ_2 be congruence subgroup of $SL_2(\mathbb{Z})$. Then Γ_1 and Γ_2 are subgroups of $GL_2(\mathbb{Q})^+$. For each $\alpha \in GL_2(\mathbb{Q})^+$, the set

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a double coset in $GL_2(\mathbb{Q})^+$.

Lemma 1.2.1 *: Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let α be an element of $GL_2(\mathbb{Q})^+$. Then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ is again a congruence subgroup of $SL_2(\mathbb{Z})$.*

Proof : There exists an $N' \in \mathbb{Z}^+$ satisfying the conditions $\Gamma(N') \subset \Gamma$, $N'\alpha \in M_2(\mathbb{Z})$, $N'\alpha^{-1} \in M_2(\mathbb{Z})$. Set $N = N'^3$. The calculation

$$\alpha\Gamma(N)\alpha^{-1} \subset \alpha\left(\mathrm{I} + N'^3 M_2(\mathbb{Z})\right)\alpha^{-1} = \mathrm{I} + N'.N'\alpha.M_2(\mathbb{Z}).N'\alpha^{-1} \subset \mathrm{I} + N'M_2(\mathbb{Z})$$

and the observation that $\alpha\Gamma(N)\alpha^{-1}$ consists of determinant-1 matrices combine to show that $\alpha\Gamma(N)\alpha^{-1} \subset \Gamma(N')$. Thus $\Gamma(N) \subset \alpha^{-1}\Gamma(N')\alpha \subset \alpha^{-1}\Gamma\alpha$, and after intersecting with $SL_2(\mathbb{Z})$, we get the result. □

Using this lemma we can say that if $\alpha \in GL_2(\mathbb{Q})^+$ and $f \in \mathcal{M}_k(\Gamma(N))$ for some $N \in \mathbb{Z}^+$, then $f_{|[\alpha]_k}$ belongs to $\mathcal{M}_k(\Gamma(N'))$ for some $N' \in \mathbb{Z}^+$. The analogous statement holds for cusp forms.
Now fix an integer $k \geq 2$ and let $N \geq 1$. Let $\mathcal{S}(N, \chi, k)$ denote the space of holomorphic cusp forms of weight k with character χ on $\Gamma_0(N)$, where χ is a Dirichlet charcter on $\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*$.
Let

$$\mathcal{S}_k = \sum_{N,\chi} \mathcal{S}(N, \chi, k)$$

denote the space of all cusp forms of weight k which are on $\Gamma_1(N)$.
Then,

$$\mathcal{S}_k = \sum_{N,\chi} \mathcal{S}(N, \chi, k) \subset \sum_{N} \mathcal{S}_k(\Gamma(N)) = \mathcal{S}'_k.$$

We proved earlier that $GL_2(\mathbb{Q})^+$ acts on the space $\sum_N \mathcal{S}_k(\Gamma(N))$ by the formula :

$$\left(f_{|A}\right)(z) = (\rho(A)(z))^k . f(A(z))$$

Lemma 1.2.2 *: Let Γ_1 and Γ_2 be congruence subgroup of $SL_2(\mathbb{Z})$, and let α be an element of $GL_2(\mathbb{Q})^+$. Set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, a subgroup of Γ_2. Then left multiplication by α,*

$$\Gamma_2 \longrightarrow \Gamma_1\alpha\Gamma_2 \text{ given by } \gamma_2 \mapsto \alpha\gamma_2$$

induces a natural bijection from the coset space $\Gamma_3 \setminus \Gamma_2$ to the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$.

Proof : The map $\Gamma_2 \longrightarrow \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ taking γ_2 to $\Gamma_1\alpha\gamma_2$ is clearly surjective. The images of the elements γ_2, γ'_2 are in the same orbit when $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma'_2$, that is $\gamma'_2\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha$ and of course $\gamma'_2\gamma_2^{-1} \in \Gamma_2$. So from the definition $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, $\Gamma_3 \setminus \Gamma_2 \longrightarrow \Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ is a bijection from cosets $\Gamma_3\gamma_2$ to orbits $\Gamma_1\alpha\gamma_2$. □

From Lemma 1.2.1 $\alpha^{-1}\Gamma_1\alpha \cap SL_2(\mathbb{Z})$ is a congruence subgroup of $SL_2(\mathbb{Z})$. So its index in $SL_2(\mathbb{Z})$ is finite, hence the coset space $\Gamma_3 \setminus \Gamma_2$ is finite and so is the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$. Due to finiteness of the orbit space, the double coset space $\Gamma_1\alpha\Gamma_2$ can act on the modular forms.

Definition 1.2.3 *: For congruence subgroups Γ_1 and Γ_2 of $SL_2(\mathbb{Z})$ and $\alpha \in GL_2(\mathbb{Q})^+$, the weight-$k$ $\Gamma_1\alpha\Gamma_2$ operator takes function $f \in \mathcal{M}_k(\Gamma_1)$ to*

$$f_{|[\Gamma_1\alpha\Gamma_2]_k} = \sum_j f_{|[\beta_j]_k}$$

where $\{\beta_j\}$ are orbit representatives, that is $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ is a disjoint union.

The double coset operator is well defined, that is, it is independent of how the β_j's are chosen: assume that if β and β' represent the same orbit in $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$, that is, $\Gamma_1\beta = \Gamma_1\beta'$. Let $\beta = \gamma_1\alpha\gamma_2$ and $\beta' = \gamma_1'\alpha\gamma_2'$, or equivalently $\alpha\gamma_2 \in \Gamma_1\alpha\gamma_2'$. Since f is weight-k invariant under Γ_1, it easily follows that $f_{|[\beta]_k} = f_{|[\beta']_k}$.

Now we want to show that the weight-k $\Gamma_1\alpha\Gamma_2$ operator takes modular forms with respect to Γ_1 to modular forms with respect to Γ_2, i.e.

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \longrightarrow \mathcal{M}_k(\Gamma_2)$$

That is, we have to show for each $f \in \mathcal{M}_k(\Gamma_1)$, the transformed $f_{|[\Gamma_1\alpha\Gamma_2]_k}$ is Γ_2- invariant and is holomorphic at the cusps. Firs we will show that it is invariant under Γ_2.
We know that any $\gamma_2 \in \Gamma_2$ permutes the orbit space $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$ by right multiplication. We have a map

$$\gamma_2 : \Gamma_1 \setminus \Gamma_1\alpha\Gamma_2 \longrightarrow \Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$$

given by $\Gamma_1\beta \mapsto \Gamma_1\beta\gamma_2$. This map is well defined and bijective. So if $\{\beta_j\}$ is set of orbit representatives for $\Gamma_1 \setminus \Gamma_1\alpha\Gamma_2$, then $\{\beta_j\}\,\gamma_2$ is a set of orbit representatives as well. Thus

$$\left(f_{|[\Gamma_1\alpha\Gamma_2]_k}\right)_{|[\gamma_2]_k} = \sum_j f_{|[\beta_j\gamma_2]_k} = f_{|[\Gamma_1\alpha\Gamma_2]_k}.$$

So $f_{|[\Gamma_1\alpha\Gamma_2]_k}$ is weight k-invariant under Γ_2.

We have to show now that the transformed $f_{|[\Gamma_1\alpha\Gamma_2]_k}$ is holomorphic at the Γ_2-cusps. We know that for any $f \in \mathcal{M}_k(\Gamma_1)$ and for any $\gamma \in GL_2(\mathbb{Q})^+$, the function $g = f_{|[\gamma]_k}$ is holomorphic at infinity, i.e., it has a Fourier expansion

$$g(z) = \sum_{n\geq 0} a_n(g) e^{2\pi i n z/h}$$

for some period $h \in \mathbb{Z}^+$. If functions $g_1, g_2, g_3, ...g_d : \mathcal{H} \to \mathbb{C}$ are holomorphic at infinity, that is, if each has a Fourier expansion, then so does their sum (we can prove

this very easily by using the l.c.m of their periods). For any $\delta \in SL_2(\mathbb{Z})$, the functions $\left(f_{|[\Gamma_1\alpha\Gamma_2]_k}\right)_{|[\delta]_k}$ is a sum of functions $g_j = f_{|}[\gamma_j]_k$ with $\gamma_j = \beta_j\delta \in GL_2(\mathbb{Q})^+$. So it is holomorphic at infinity. Since δ is arbitrary, it is holomorphic at the cusps. We have proved our claim.
Similarly, it holds for cusp forms that

$$[\Gamma_1\alpha\Gamma_2]_k : \mathcal{S}_k(\Gamma_1) \longrightarrow \mathcal{S}_k(\Gamma_2)$$

is a well defined operator and that it takes cusp forms to cusp forms.

The operator $T_p = \Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma$ is known the Hecke operator with repect to the congruence subgroup Γ.

Our main goal in this chapter is to construct p-adic L-fuctions associated with modular forms of weight 2 and trivial characters. So from now we only consider modulars form is of weight 2 and let χ to be the trivial character denoted by ϵ. That is,

$$\epsilon : \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right) \longrightarrow \mathbb{C}$$

where

$$\begin{aligned} \epsilon(a) &= 1 \text{ if } (a, N) = 1 \\ &= 0 \text{ otherwise.} \end{aligned}$$

Now we are going to define the concept of modular integral.

1.3 Modular Integrals

Fix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})^+$. As we know $GL_2(\mathbb{R})^+$ acts on the Riemann z-sphere $\mathbb{C} \cup \{\infty\}$ via

$$A(z) = \frac{az + b}{cz + d}.$$

Differentiating the functions on both sides of the above equation, we get

$$\begin{aligned} d(A(z)) &= \frac{\det(A)}{(cz + d)^{-2}} dz \\ &= (\rho(A(z)))^2 dz. \end{aligned}$$

Note that the "d" in dz and "d" in $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ are not be confused.

For $f \in \mathcal{S}_2'$,

$$(f_{|A})(z)dz = f(A(z))d(A(z))$$

So we get that the differential is invariant under the operator $GL_2(\mathbb{Q})^+$.

Let $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ and define a map

$$\phi : \mathcal{S}_2' \times \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{C}$$

by

$$\begin{aligned} \phi(f, r) &= 2\pi i \int_{\infty}^{r} f(z)dz \\ &= \begin{cases} 2\pi \int_0^{\infty} f(r+it)dt & \text{if } r \in \mathbb{Q} \\ 0 \text{ if } r = \infty \end{cases} \end{aligned}$$

We are going to adopt the convention that if one argument is to be kept constant in a discussion, it may be in the position of subscript in our notation. Thus, $\phi(f, r) = \phi_f(r)$. Clearly,
(a) ϕ is linear in f for any $r \in \mathbb{P}^1(\mathbb{Q})$
(b)$\phi(f_{|\mathrm{A}}, r) = \phi_f(\mathrm{A}(r)) - \phi_f(\mathrm{A}(\infty))$ for $A \in GL_2(\mathbb{Q})^+$.
By a modular integral we shall mean a mapping

$$\phi : \mathcal{S}_2' \times \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{C}$$

satisfying axioms (a) and (b).

1.4 The Module of Values

Let $A_j \in SL_2(\mathbb{Z})$ be coset representatives for $\Gamma_0(N)$, so that

$$SL_2(\mathbb{Z}) = \coprod_{j \in I} \Gamma_0(N).A_j$$

where I is a finite set, because we know that

$$[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + \frac{1}{p}).$$

For fixed $f \in \mathcal{S}_2(\Gamma_0(N), \epsilon)$, let $L_f \subseteq \mathbb{C}$ denote the $\mathbb{Z}$-module generated by the image of $\mathbb{P}^1(\mathbb{Q})$ under the mapping ϕ_f.

Proposition 1.4.1 *: The $\mathbb{Z}$-module L_f is the $\mathbb{Z}$-sub module of $\mathbb{C}$ generated by the elements*

$$\phi_f(A_j(\infty)) - \phi_f(A_j(0)) \text{ for } j \in I \tag{1.2}$$

Proof: Let $L_f^{\circ} \subseteq L_f$ denote the $\mathbb{Z}$-submodule generated by the quantities (1.2). Let $a, m \in \mathbb{Z}$ with $m \geq 0$ and $(a, m) = 1$. We shall show that $\phi(f, \frac{a}{m}) \in L_f^{\circ}$ by induction on m.

For $m = 0$, $\phi(f, \frac{a}{m}) = 0 \in L_f^\circ$. Suppose $m > 0$, $(a, m) = 1$. Then we can find an $m' \in \mathbb{Z}$ such that $am' = 1(\text{mod } m)$, and $0 \leq m' < m$. Putting $a' = \frac{am'-1}{m}$ and $A = \begin{bmatrix} a & a' \\ m & m' \end{bmatrix}$, we get $A(\infty) = \frac{a}{m}$, and $A(0) = \frac{a'}{m'}$. Since $A = B.A_j$ for some $B \in \Gamma_0(N)$, we have :

$$\begin{aligned} \phi(f, \frac{a}{m}) - \phi(f, \frac{a'}{m'}) &= \phi(f, A(\infty)) - \phi(f, A(0)) \\ &= \phi(f, BA_j(\infty)) - \phi(f, BA_j(0)) \\ &= -\phi(f \mid BA_j, 0) \\ &= -\epsilon(B)\phi(f \mid A_j, 0) \\ &= \epsilon(B)[\phi(f, A_j(\infty)) - \phi(f, A_j(0))] \in L_f^\circ. \end{aligned}$$

By the induction hypothesis $\phi_f(\frac{a'}{m'}) \in L_f^\circ$. This implies that $\phi_f(\frac{a}{m}) \in L_f^\circ$.□

1.5 Modular Symbol

Now we will define the modular symbol λ using the modular integral ϕ. For $a, m \in \mathbb{Z}$, $m > 0$, and $f \in \mathcal{S}_2'$, we put

$$\lambda(f, a, m) : = \phi\left(f, -\frac{a}{m}\right) \tag{1.3}$$

$$= \phi\left(f\Big|\begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}, 0\right). \tag{1.4}$$

The second equality follows from (b) in the definition of ϕ.

Proposition 1.5.1 *: The modular symbol $\lambda(f, a, m)$ is $\mathbb{C}$ -linear in f. For fixed $f \in \mathcal{S}_2'$ and a,m $\in \mathbb{Z}$, the modular symbol $\lambda(f, a, m)$ takes values in L_f. For fixed f, $\lambda(f, a, m)$ depends only on a mod m.*

Proof: Except for the last part, the other parts are trivial. We have :

$$\begin{aligned}
\lambda(f, a+rm, m) &= \phi(f, -\frac{a+rm}{m}) \\
&= \phi(f, -\frac{a}{m} - r) \\
&= \phi(f, \begin{pmatrix} 1 & -(a+rm) \\ 0 & m \end{pmatrix}(0)) \\
&= \phi(f_{|\begin{pmatrix} 1 & -(a+rm) \\ 0 & m \end{pmatrix}}, 0) \\
&= \phi(f_{|\begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}}, 0) \\
&= \phi(f, -\frac{a}{m}) \qquad (\text{ because } f \text{ is } \Gamma_0(N) - \text{invariant}) \\
&= \lambda(f, a, m).
\end{aligned}$$

This implies that $\lambda(f, a, m)$ depends only on a mod m. $\square$

1.6 Action of the Hecke operators

Let $f \in \mathcal{S}_2(\Gamma_0(N),\ \epsilon)$. For every prime number p consider the operators

$$f \longrightarrow f_{|T_p} = \left(\sum_{u=0}^{p-1} f_{|\begin{bmatrix} 1 & u \\ 0 & p \end{bmatrix}} \right) + \epsilon(p).f_{|\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}}. \tag{1.5}$$

Proposition 1.6.1 *: For $f \in \mathcal{S}_2(\Gamma_0(N), \epsilon)$ and each prime number p, we have the formula :*

$$\lambda(f_{|T_p}, a, m) = \left[\sum_{u=0}^{p-1} \lambda(f, a - um, pm) \right] + \epsilon(p)\lambda(f, a, \frac{m}{p}). \tag{1.6}$$

Proof : We start from the right-hand side of (1.6) :

$$\begin{aligned}
&= \sum_{u=0}^{p-1} \lambda(f, a-um, pm) + \epsilon(p)\lambda(f, a, \frac{m}{p}) \\
&= \sum_{u=0}^{p-1} \phi(f, -\frac{(a-um)}{pm}) + \epsilon(p)\phi(f, -\frac{ap}{m}) \\
&= \sum_{u=0}^{p-1} \phi(f, \begin{bmatrix} 1 & -u \\ 0 & p \end{bmatrix}(-\frac{a}{m})) + \epsilon(p)\phi(f, -\frac{ap}{m}) \\
&= \sum_{u=0}^{p-1} \phi(f_{|\begin{bmatrix} 1 & -u \\ 0 & p \end{bmatrix}}, (-\frac{a}{m})) + \epsilon(p)\phi(f, -\frac{ap}{m}) \\
&= \sum_{u=0}^{p-1} \phi(f_{|\begin{bmatrix} 1 & -u \\ 0 & p \end{bmatrix}}, (-\frac{a}{m})) + \epsilon(p)\phi(f_{|\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}}, -\frac{a}{m}) \\
&= \phi(\sum_{u=0}^{p-1}(f_{|\begin{bmatrix} 1 & -u \\ 0 & p \end{bmatrix}} + \epsilon(p) f_{|\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}}, -\frac{a}{m}) \\
&= \phi(f_{|T_p}, -\frac{a}{m}) \\
&= \lambda(f_{|T_p}, a, m).
\end{aligned}$$

1.7 Relation of the modular symbols to the values of the complex L-function $L(f,s)$

If $f \in \mathcal{S}_2$ has Fourier series $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$ then the corresponding L-function $L(f,s)$ is defined by

$$L(f,s) = \sum_{n\geq 1} a_n . n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} . \int_0^\infty f(it) . t^s . \frac{dt}{t}. \tag{1.7}$$

For the convergence of integral and more details see ([DS] chapter V, section 5.9, page no. 200). Therefore we have:

$$\lambda(f,0,1) = \phi(f,0) = -2\pi i \int_0^{i\infty} f(z)dz = 2\pi \int_0^\infty f(it)dt = L(f,1). \tag{1.8}$$

1.8 Twists

Let χ be a Dirichlet character mod m. The Gauss sums are defined by the formulae:

$$\tau(n,\chi) := \sum_{a \bmod m} \chi(a) . e^{2\pi i n a/m} \tag{1.9}$$

and

$$\tau(\chi) := \tau(1, \chi) \tag{1.10}$$

As we know from character theory that

$$\begin{aligned} \tau(n,\chi) = \bar{\chi}(n).\tau(\chi) \quad &\text{for all} \quad n \in \mathbb{Z} \quad \text{if} \quad \chi \quad \text{is primitive mod } m, \text{and} \\ &\text{for} \quad (n,m) = 1, \quad \text{if } \chi \quad \text{is any character mod } m. \end{aligned}$$

Conversely if the first or second sentence holds for all $n \in \mathbb{Z}$, then χ is a primitive character mod m, and in this case

$$|\tau(\chi)|^2 = \chi(-1)\tau(\chi)\tau(\bar{\chi}) = m. \tag{1.11}$$

In particular, $\tau(\chi) \neq 0$.

For

$$f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$$

we put

$$f_\chi(z) = \sum_n \chi(n) a_n e^{2\pi i n z}$$

So if χ is primitive mod m, then we have

$$\begin{aligned} f_{\bar{\chi}}(z) &= \sum_n a_n \bar{\chi}(n) e^{2\pi i n z} \\ &= \sum_n a_n \frac{\tau(n,\chi)}{\tau(\chi)}\ e^{2\pi i n z} \\ &= \frac{1}{\tau(\chi)} \sum_n \sum_{a \ mod \ m} a_n e^{2\pi i n a/m}.e^{2\pi i n z} \\ &= \frac{1}{\tau(\chi)} \sum_{a \ mod \ m} \sum_n a_n \chi(a) e^{2\pi i n (z + a/m)} \\ &= \frac{1}{\tau(\chi)} \sum_{a \ mod \ m} \chi(a) f(z + \frac{a}{m}). \end{aligned}$$

For the modular Integral, this gives the following twisting rule

$$\begin{aligned} \phi(f_{\bar{\chi}}, r) &= \frac{1}{\tau(\chi)} \sum_{a \ mod \ m} \chi(a).\phi(f(z + \frac{a}{m}), r) \\ &= \frac{1}{\tau(\chi)} \sum_{a \ mod \ m} \chi(a).\phi(f \mid \begin{bmatrix} 1 & \frac{a}{m} \\ 0 & 1 \end{bmatrix}, r) \\ &= \frac{1}{\tau(\chi)} \sum_{a \ mod \ m} \chi(a).\phi\left(f, r + \frac{a}{m}\right) \end{aligned} \tag{1.12}$$

From the above, we get:

$$\begin{aligned}\lambda(f_{\bar{\chi}}, b, n) &= \phi(\ f_{\bar{\chi}}, -\frac{b}{n}) \\ &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a).\phi\left(f, -\frac{b}{n} + \frac{a}{m}\right) \\ &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a).\lambda(f, bm - an, mn). \end{aligned} \tag{1.13}$$

putting $b = 0$ and $n = 1$, we get, by equation (1.8),

$$\begin{aligned}L(f_{\bar{\chi}}, 1) &= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a).\lambda(f, -a, m) \\ &= \frac{\chi(-1)}{\tau(\chi)} \sum_{a \bmod m} \chi(a).\lambda(f, a, m) \\ &= \frac{\overline{\tau(\chi)}}{m} \sum_{a \bmod m} \chi(a).\lambda(f, a, m). \end{aligned} \tag{1.14}$$

This expresses the special value $L(f_{\bar{\chi}}, 1)$ of the L-function of all twists of f in terms of modular symbols for f.

1.9 p-adic distributions

Let p be fixed prime number. Suppose $f \in \mathcal{S}_2(\Gamma_0(N), \epsilon)$ is an eigenform for T_p with eigenvalue a_p. Suppose also that the polynomial $X^2 - a_p X + \epsilon(p)p$ has two distinct roots α and β with $\alpha \neq 0$. For $m \in \mathbb{Z},\ m > 0$ $\nu(m) = ord_p(m)$ is an integer such that $m.p^{-\nu(m)}$ is a p-adic unit. Define:

$$\mu_{f,\alpha}(a, m) = \frac{1}{\alpha^{\nu(m)}} \cdot \lambda_f(a, m) - \frac{\epsilon(p)}{\alpha^{\nu(m)+1}} \cdot \lambda_f(a, \frac{m}{p}). \tag{1.15}$$

It takes values in $\mathbb{Z}_p$.

Proposition 1.9.1 *: For a,m* $\in \mathbb{Z},\ m > 0$ *we have a distribution property : that is, we have:*

$$\sum_{\substack{b = a \bmod m \\ b \bmod pm}} \mu_{f,\alpha}(b, pm) = \mu_{f,\alpha}(a, m)$$

Proof: We have, using prop 1.5.1,

$$\begin{aligned}
\sum_{\substack{b \equiv a \ mod \ m \\ b \ mod \ pm}} \mu_{f,\alpha}(b, pm) &= \sum_{\substack{b \equiv a \ mod \ m \\ b \ mod \ pm}} \left(\frac{1}{\alpha^{\nu(m)+1}} . \lambda_f(b, pm) - \frac{\epsilon(p)}{\alpha^{\nu(m)+2}} . \lambda_f(b, m) \right) \\
&= \left[\sum_{\substack{b \equiv a \ mod \ m \\ b \ mod \ pm}} \frac{1}{\alpha^{\nu(m)+1}} . \lambda_f(b, pm) \right] - \frac{\epsilon(p)}{\alpha^{\nu(m)+2}} . p . \lambda_f(a, m) \\
&= \left[\sum_{r=0}^{p-1} \frac{1}{\alpha^{\nu(m)+1}} . \lambda_f(a + rm, pm) \right] - \frac{p \ \epsilon(p)}{\alpha^{\nu(m)+2}} . \lambda_f(a, m) \\
&= \left[\sum_{r=0}^{p-1} \frac{1}{\alpha^{\nu(m)+1}} . \phi \left(f, -\frac{a + rm}{pm} \right) \right] - \frac{\beta}{\alpha^{\nu(m)+1}} . \lambda_f(a, m) \\
&= \left[\sum_{r=0}^{p-1} \frac{1}{\alpha^{\nu(m)+1}} . \phi \left(f \mid \begin{bmatrix} 1 & -r \\ 0 & p \end{bmatrix}, -\frac{a}{m} \right) \right] - \frac{\beta}{\alpha^{\nu(m)+1}} . \lambda_f(a, m) \\
&= \frac{1}{\alpha^{\nu(m)+1}} . \phi \left(f \mid T_p - \epsilon(p) f \mid \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, -\frac{a}{m} \right) - \frac{\beta}{\alpha^{\nu(m)+1}} . \lambda_f(a, m) \\
&= \frac{a_p - \beta}{\alpha^{\nu(m)+1}} . \phi \left(f, -\frac{a}{m} \right) - \frac{\epsilon(p)}{\alpha^{\nu(m)+1}} . \phi \left(f \mid \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, -\frac{a}{m} \right) \\
&= \frac{1}{\alpha^{\nu(m)}} . \lambda_f(a, m) - \frac{\epsilon(p)}{\alpha^{\nu(m)+1}} . \lambda_f(a, \frac{m}{p}) \\
&= \mu_{f,\alpha}(a, m) . \square
\end{aligned}$$

Suppose ψ is Dirichlet character with conductor M such that $(p, M) = 1$. We find for n prime to M the following equality.

Proposition 1.9.2

$$\mu_{f\bar{\psi},\alpha\bar{\psi}(p)}(b, n) = \frac{\psi(p)^{\nu(n)}}{\tau(\psi)} . \sum_{a \ mod \ m} \psi(a) . \mu_{f,\alpha} \left(Mb - na, Mn \right) . \tag{1.16}$$

Proof: We start from the right hand side of (1.1.6) :

$$
\begin{aligned}
&= \frac{\psi(p)^{\nu(n)}}{\tau(\psi)}.\sum_{a \bmod M}\psi(a).\mu_{f,\alpha}\left(Mb-na,Mn\right)\\
&= \frac{\psi(p)^{\nu(n)}}{\tau(\psi)}.\sum_{a \bmod M}\psi(a)\left(\frac{1}{\alpha^{\nu(n)}}.\lambda_f(Mb-na,Mn)-\frac{\epsilon(p)}{\alpha^{\nu(n)+1}}.\lambda_f(Mb-na,\frac{Mn}{p})\right)\\
&= \frac{1}{(\alpha\bar{\psi}(p))^{\nu(n)}}.\frac{1}{\tau(\psi)}.\sum_{a \bmod M}\psi(a).\lambda_f(Mb-na,Mn)-\\
&\quad \frac{\epsilon(p)}{(\alpha\bar{\psi}(p))^{\nu(n)+1}}.\frac{1}{\tau(\psi)}.\sum_{a \bmod M}\Psi(ap).\lambda_f(Mb-na,\frac{Mn}{p})\\
&= \frac{1}{(\alpha\bar{\psi}(p))^{\nu(n)}}.\lambda(f_{\bar{\psi}},b,n)-\frac{\epsilon(p)}{(\alpha\bar{\psi}(p))^{\nu(n)+1}}.\frac{1}{\tau(\psi)}.\sum_{a \bmod M}\psi(a).\lambda_f\left(Mb-\frac{an}{p},\frac{Mn}{p}\right)\\
&= \frac{1}{(\alpha\bar{\psi}(p))^{\nu(n)}}.\lambda(f_{\bar{\psi}},b,n)-\frac{\epsilon(p)}{(\alpha\bar{\psi}(p))^{\nu(n)+1}}.\lambda\left(f_{\bar{\psi}},b,\frac{n}{p}\right)\\
&= \mu_{f\bar{\psi},\alpha\bar{\psi}(p)}(b,n).
\end{aligned}
$$

1.10 p-adic Integrals

Let M be a fixed integer greater than 0 and prime to p. Set:

$$
\begin{aligned}
\mathbb{Z}_{p,M} &= \varprojlim_{\nu}\left(\frac{\mathbb{Z}}{p^{\nu}M\mathbb{Z}}\right)\\
&= \varprojlim_{\nu}\left(\frac{\mathbb{Z}}{p^{\nu}\mathbb{Z}}\times\frac{\mathbb{Z}}{M\mathbb{Z}}\right)\\
&= \mathbb{Z}_p\times\frac{\mathbb{Z}}{M\mathbb{Z}}
\end{aligned}
$$

$$
\mathbb{Z}_{p,M}^{*} = \mathbb{Z}_p^{*}\times\left(\frac{\mathbb{Z}}{M\mathbb{Z}}\right)^{*}.
$$

We view $\mathbb{Z}_{p,M}^{*}$ as a p-adic analytic Lie group with a fundamental system of open disks $D(a,\nu)$ indexed by an integer a prime to pM and natural number $\nu\geq 1$, where

$$
D(a,\nu)=a+p^{\nu}M\mathbb{Z}_{p,M}\subseteq\mathbb{Z}_{p,M}^{*}. \tag{1.17}
$$

Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Fix an embedding

$$
i:\bar{\mathbb{Q}}\hookrightarrow\mathbb{C}_p
$$

where $\mathbb{C}_p$ = the completion of an algebraic closure of $\mathbb{Q}_p$
Let $\mathcal{O}_p\subseteq\mathbb{C}_p$ denote the ring of integers in $\mathbb{C}_p$ and let $\mathcal{O}_p^{*}$ be its topological group of

units. For a fixed modular form $f \in \mathcal{S}_2(\Gamma_0(N), \epsilon)$, consider the finite dimensional $\mathbb{C}_p$ - vector space

$$V_f \;=\; \mathbb{C}_p \otimes_{\bar{\mathbb{Q}}} L_f\bar{\mathbb{Q}}$$

and the $\mathcal{O}_p$ - lattice $\Omega_f \subseteq V_f$ generated by L_f .

Definition 1.10.1 *: If $U \subseteq \mathbb{Z}_{p,M}$ is an open subset, a function*

$$F : U \longrightarrow \mathbb{C}_p$$

is called locally analytic if there is a covering of U by open disks $D(a,\nu)$ such that on each $D(a,\nu)$, F is given by convergent power series

$$F(x) \;=\; \sum_{n\geq 0} c_n(x-a)^n. \tag{1.18}$$

Now our aim is to define a V_f-valued integral

$$(U, F) \longrightarrow \int_U F d\mu_{f,\alpha}, \tag{1.19}$$

where U ranges over compact open subsets of $\mathbb{Z}_{p,M}^*$ and F ranges over locally analytic functions on U.
So we are giving measures $\mu_{f,\alpha}$ as before on $\mathbb{Z}_{p,M}^*$ such that

$$\int_{D(a,\nu)} d\mu_{f,\alpha} \;=\; \mu_{f,\alpha}(a, p^\nu M) \tag{1.20}$$

where α is an admissible root of f. The equation (1.19) is $\mathbb{C}_p$- linear in F and finitely additive in U .

1.11 Choices of α

Let α and β be the two roots in $\bar{\mathbb{Q}}$ of the equation $X^2 - a_pX + \epsilon(p)p$. Let $\sigma = ord_p\alpha$, $\bar{\sigma} = ord_p\beta$ such that $\sigma < \bar{\sigma}$.

Definition 1.11.1 *: The form f is ordinary at p iff $\sigma = 0$, i.e. if and only if $a_p \in \mathcal{O}_p^*$.*

This depends on our embedding

$$i : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}_p.$$

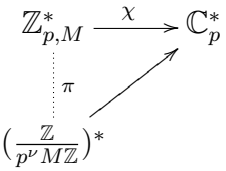
If f has good ordinary reduction at p i.e. $p \nmid a_p$, then α is always an admissible root.

1.12 p-adic L-functions

By a p-adic character we mean a continuous homomorphism

$$\chi : \mathbb{Z}_{p,M}^* \longrightarrow \mathbb{C}_p^* \tag{1.21}$$

for some p and M. We say that a character χ is primitive if it does not factor through $\mathbb{Z}_{p,M_1}^*$ for any proper divisor M_1 of M. For a p-adic character χ, there is a unique M such that χ is primitive on $\mathbb{Z}_{p,M}^*$. We call this M the p'-conductor of χ. It is an integer ≥ 1, prime to p.



Viewing $\left(\frac{\mathbb{Z}}{p^\nu M\mathbb{Z}}\right)^*$ as quotient of $\mathbb{Z}_{p,M}^*$, we can identify a primitive Dirichlet character of conductor $p^\nu M\mathbb{Z}$ with a p-adic character of p'-conductor M, and every character of finite order arises in this way.
If $x \in \mathbb{Z}_p^*$, we can write:

$$x = \omega(x) \cdot < x > \tag{1.22}$$

where $\omega(x)$ is a root of unity and

$$< x > \in 1 + p\mathbb{Z}_p \tag{1.23}$$

then $x \mapsto \omega(x)$, $x \mapsto < x >$ are p-adic characters of p'-conductor 1. If $\chi(x) = \psi(x)$, where ψ is a character of finite order, then we call χ special .

Let f be an eigenform for T_p and suppose that α is an admissible p-root for f. For each p-adic character χ, we put

$$L_p(f, \chi, s) \;=\; \int_{\mathbb{Z}_{p,M}^*} < x >^{s-1} \chi . d\mu_{f,\alpha} \tag{1.24}$$

If $\chi(x) = \psi(x)$ is a special character and ψ is a conductor of finite order $m = p^\nu M$, define the p-adic multiplier as

$$\begin{aligned} e_p(\alpha, \chi) &= e_p(\alpha, \psi) \\ &= \frac{1}{\alpha^\nu}\left(1 - \frac{\bar{\psi}(p)\epsilon(p)}{\alpha}\right)\left(1 - \frac{\psi(p)}{p}\right) \end{aligned} \tag{1.25}$$

Proposition 1.12.1 *: If χ is a special character as above, then*

$$L_p(f, \chi, 1) = e_p(\alpha, \psi) \cdot \frac{m}{\tau(\bar{\psi})} \cdot \lambda(f_{\bar{\psi}}, 0, 1) \tag{1.26}$$

$$= e_p(\alpha, \psi) \cdot \frac{m}{\tau(\bar{\psi})} \cdot L(f_{\bar{\psi}}, 1). \tag{1.27}$$

Proof: If $\nu > 0$, we need to show that:-

$$L_p(f, \chi, 1) = \frac{m}{\tau(\bar{\psi})}.\frac{1}{\alpha^\nu}\lambda(f_{\bar{\psi}}, 0, 1).$$

But this is true because:-

$$\begin{aligned}
L_p(f, \chi, 1) &= \int_{\mathbb{Z}^*_{p,M}} \chi.d\mu_{f,\alpha} \\
&= \int_{\mathbb{Z}^*_{p,M}} \psi.d\mu_{f,\alpha} \\
&= \sum_{a \ mod \ p^\nu M} \psi(a).\mu_{f,\alpha}(a, p^\nu M) \\
&= \sum_{a \ mod \ p^\nu M} \psi(a).\frac{1}{\alpha^\nu}.\lambda(f, a, p^\nu M) \\
&= \frac{1}{\alpha^\nu}.\frac{m}{\tau(\bar{\psi})}.L(f_{\bar{\psi}}, 1) \\
&= \frac{m}{\tau(\bar{\psi})}.\frac{1}{\alpha^\nu}.L(f_{\bar{\psi}}, 1) \\
&= \frac{m}{\tau(\bar{\psi})}.\frac{1}{\alpha^\nu}.\lambda(f_{\bar{\psi}}, 0, 1).
\end{aligned}$$

If $\nu = 0$, then we have to show that

$$L_p(f, \chi, 1) = e_p(\alpha, \psi).\frac{m}{\tau(\bar{\psi})}.\lambda(f_{\bar{\psi}}, 0, 1)$$

In this case $\nu = 0$ implies $m = M$. And if a is an integer prime to M, let

$$D(a, 0) = \mathbb{Z}^*_{p,M} \cap (a + M\mathbb{Z}_{P,M}).$$

Then,

$$D(a, 0) = \coprod_{\substack{b = a \ mod \ m, b \neq 0 \ mod \ p \\ b \ mod \ pm}} D(b, 1)$$

and $b \equiv a \ mod \ m$, $b \ \equiv 0 \ mod \ p$ is equivalent to $b \equiv \ pap' \ mod \ pm$ where $pp' \equiv 1 \ mod \ M$. Consequently,

$$\begin{aligned}
\int_{D(a,o)} \psi.d\mu_{f,\alpha} &= \sum_{\substack{b = a \ mod \ m, b \neq 0 \ mod \ p \\ b \ mod \ pm}} \psi(b)\mu_{f,\alpha}(b, pM) \\
&= \left(\sum_{\substack{b = a \ mod \ m, \\ b \ mod \ pm}} \psi(b)\mu_{f,\alpha}(b, pm) \right) - \psi(pap').\mu_{f,\alpha}(pap', pm) \\
&= \left(\sum_{\substack{b = a \ mod \ m, \\ b \ mod \ pm}} \psi(a)\mu_{f,\alpha}(b, pm) \right) - \psi(a).\mu_{f,\alpha}(pap', pm) \\
&= \psi(a)\mu_{f,\alpha}(a, m) - \psi(a)\mu_{f,\alpha}(pap', pm),
\end{aligned}$$

which implies that

$$\begin{aligned}
L_p(f, \chi, 1) &= \int_{\mathbb{Z}_{p,M}^*} \psi.d\mu_{f,\alpha} \\
&= \sum_{a \ mod \ m} \int_{D(a,o)} \psi.d\mu_{f,\alpha} \\
&= \sum_{a \ mod \ m} (\psi(a)\mu_{f,\alpha}(a, m) - \psi(a)\mu_{f,\alpha}(pap', pm)) \\
&= \sum_{a \ mod \ m} \psi(a) \left(\lambda_f(a, m) - \frac{\epsilon(p)}{\alpha}.\lambda_f(a, \frac{m}{p}) - \frac{1}{\alpha}\lambda_f(pap', pm) + \frac{\epsilon(p)}{\alpha^2}.\lambda_f(a, m) \right) \\
&= \sum_{a \ mod \ m} \psi(a) \left(\lambda_f(a, m) - \frac{\epsilon(p)}{\alpha}.\lambda_f(ap, m) - \frac{1}{\alpha}\lambda_f(ap', m) + \frac{\epsilon(p)}{\alpha^2}.\lambda_f(a, m) \right) \\
&= \sum_{a \ mod \ m} \psi(a)\lambda_f(a, m) - \frac{\epsilon(p)}{\alpha} \sum_{a \ mod \ m} \psi(a).\lambda_f(ap, m) - \\
&\quad \frac{1}{\alpha} \sum_{a \ mod \ m} \psi(a)\lambda_f(ap', m) + \frac{\epsilon(p)}{\alpha^2} \sum_{a \ mod \ m} \psi(a).\lambda_f(a, m) \\
&= \frac{m}{\tau(\bar{\psi})}.L(f_{\bar{\psi}}, 1) \left(1 - \frac{\epsilon(p)\bar{\psi}(p)}{\alpha} - \frac{\psi(p)}{\alpha} + \frac{\epsilon(p)}{\alpha^2} \right) \\
&= e_p(\alpha, \psi).\frac{m}{\tau(\bar{\psi})}.\lambda(f_{\bar{\psi}}, 0, 1).
\end{aligned}$$

2 Quaternion Algebras

In this chapter K is any field and K_s is a separable algebraic closure of K.

2.1 Quaternion algebras

Definition 2.1.1 *: A quaternion algebra H of K is a central algebra of dimension 4 over K such that there is a quadratic separable extension L of K with $H = L + Lu$, where $u \in H$ satisfies*

$$u^2 = \theta \in K^*, \qquad um = \bar{m}u \tag{2.1}$$

for all $m \in L$, where $m \to \bar{m}$ is a non trivial automorphism of L/K.

We will sometimes write $H = (L, \theta)$. But H does not determine L and θ uniquely. For example it is clear that one can replace θ by $\theta m\bar{m}$ if m is an element of L such that $m\bar{m} \neq 0$. The element u is not determined by (2.1) either if $m \in L$ is an element satisfing $m\bar{m} = 1$, we can replace u by mu.
We will give the law of multiplication in H using (2.1). That is if $m_i \in L$ for $1 \leq i \leq 4$ then :

$$(m_1 + m_2u)(m_3 + m_4u) = (m_1m_3 + m_2\bar{m}_4\theta) + (m_1m_4 + m_2\bar{m}_3)u.$$

Definition 2.1.2 *The conjugation on H is the K-endomorphism : $h \to \bar{h}$ on H which extended map of non trivial K - automorphism of L defined by $\bar{u} = -u$ & $\overline{mu} = -mu$ where $m \in L$.*

It is easy to check that this is an anti automorphism involution of H from the following relation.

$$\overline{ah + bk} = a\bar{h} + b\bar{k}, \bar{\bar{h}} = h, \overline{hk} = \bar{k}\bar{h} \quad a, b \in K, \quad h, k \in H.$$

Definition 2.1.3 *: Let $h \in H$. The reduced trace of h is t(h)=h+$\bar{h}$ and reduced norm is n(h)= h$\bar{h}$.*

So if $h \notin K$, then its minimal polynomial over K is :

$$(X - h)(X - \bar{h}) = X^2 - t(h)X + n(h).$$

The algebra $K(h)$ generated by h over K is quadratic over K. The reduced trace and the reduced norm of h are simply the image of h under the trace and norm of $K(h)/K$. The conjugation and the identity are the K-automorphisms of $K(h)$.

Lemma 2.1.4 : *The invertible elements of H are the elements of non-zero reduced norm. The reduced norm defines a multiplicative homomorphism from H^* to K^*. The reduced trace is K-linear and the application $(h,k) \mapsto t(hk)$ is a non-degenerate bilinear form.*

Proof: Since $n(hk) = hk\overline{hk} = hk\bar{k}\bar{h} = hn(k)\bar{h} = n(h)n(k)$, we have that h is invertible if and only if $n(h) \neq 0$: if $n(h) \neq 0$, then we can define $h^{-1} = \bar{h}n(h)^{-1}$. Then it defines a multiplicative homomorphism from H^* to K^*.

It is easy to check for $a, b \in K$, $h, k \in H$, $t(ah + bk) = at(h) + bt(k)$. Now we have to prove that application $(h,k) \mapsto t(hk)$ non-degenerate bilinear form, i.e., for given $h \in H$, $t(hk) = 0$ for all $k \in H$ implies $h = 0$.
Take $h = m_1 + m_2u$ and take $k = m \in L$.

$$\begin{aligned} t(hk) = t\left((m_1 + m_2u)m\right) = 0 \text{ for all } m \in L \\ \Rightarrow t(m_1m) + t(m_2um) = 0 \text{ for all } \ m \in L \\ \Rightarrow t(m_1m) = 0 \ \text{ for all } m \in L \end{aligned}$$

Since L/K is separable, this implies $m_1 = 0$. So $t(m_2uk) = 0$ for all $k \in H$. Take $k = \bar{u}$, then we will get $m_2 = 0$, this implies $h = 0$. Thus we are done.

For char$K \neq 2$, we get the classical definition of quaternion algebras. The pair (L, θ) is equivalent to a pair $\{a, b\}$, where $a, b \in K^*$ and the relations defining H as the basic K-algebra of basis $1, i, j, ij$ satisfying the following relation.

$$i^2 = a, \ j^2 = b, \ ij = -ji \tag{2.2}$$

The equation (2.1) is equivalent to equation (2.2) by taking $H = L + Lj, \ \ L = K(i)$ and $\theta = b$. We will put $ij = k$.
The conjugation, the reduced trace and the reduced norm have the following expressions : if $h = x + yi + zj + tk$

$$\bar{h} = x - yi - zj - tk, \ t(h) = 2x, \ n(h) = x^2 - ay^2 - bz^2 + abt^2. \tag{2.3}$$

The fundamental example of a quaternion algebra over K, is given by the algebra $M_2(K)$. The reduced trace and the reduced norm in $M_2(K)$ are the trace and determinant as usual. We identify K with its image in $M_2(K)$ under the K-homomorphism which sends the unit of K on the identity matrix.
Explicitely, if

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ \bar{h} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ t(h) = a + d, \ n(h) = ad - bc. \tag{2.4}$$

We will show that $M_2(K)$ satisfies the definition of a quaternion algebra in a following way : we will choose a matrix m of distinct eigenvalues and put $L = K(m)$. Since m has

distinct eigenvalues, there exists a matrix $u \in GL_2(K)$ such that $umu^{-1} = \bar{m}$. From here we will get $t(um) = t(u)m$ for all $m \in L$, and $t(um) \in K$. This implies $t(u) = 0$ and $u^2 = \theta \in K^*$. This proves that $M_2(K)$ satisfies the definition of quaternion algebra. Also we can take as the basis of $M_2(K)$ are $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ whose elements satisfy equations (2.2).

From now on we assume that $\text{char}(K) \neq 2$. Now our chief aim is to prove that the quaternion algebra is a simple central algebra and all simple central algebras of dimension 4 are quaternion algebras. From now on we will denote H by $\{a, b\}$ where $a, b \in K^*$and $H = K + Ki + Kj + Kk$ where i, j, k satisfy :

$$i^2 = a,\ j^2 = b,\ ij = -ji,\ ij = k.$$

Lemma 2.1.5 *:The quaternion algebra H is a simple central algebra whose center is K.*

Proof : To prove this lemma we introduce the Lie bracket operation $[x, y] = xy - yx$. If $x = c_0 + c_1 i + c_2 j + c_3 k \in H$. Then we get by simple calculation

$$[i, x] = 2ac_3 j + 2c_2 k, \quad [j, x] = -2bc_3 i - 2c_1 k, \quad [k, x] = 2bc_2 i - 2ac_1 j$$

and we know that $x \in Z(H)$ if and only if $[i, x] = [j, x] = [k, x] = 0$. This implies $c_0 = c_1 = c_2 = c_3 = 0$. i.e. $x \in K$. So $Z(H) = K$.
Suppose that $0 \neq x \in I$ is a two sided ideal of H. It must contain the Lie triple products

$$[j, [i, x]] = -4bc_2 i, \quad [k, [j, x]] = 4abc_3, \quad [i, [k, x]] = -4ac_1 k.$$

If one of c_1, c_2, c_3 is not zero then I contains the unit of H. If $c_1 = c_2 = c_3 = 0$ then $x = c_0$ is a unit belonging to I. So in all cases $I = H$. Hence quaternion algebras are simple central algebras .

Proposition 2.1.6 *: The following conditions are equivalent for $H = \{a, b\}$.*
(i) *H is a division algebra;*
(ii) $x \in H - \{0\}$ implies *n(x)*$\neq 0$*;*
(iii) *if* $(c_0, c_1, c_2) \in K^3$ *satisfy* $c_0^2 = ac_1^2 + bc_2^2$ *, then* $c_0 = c_1 = c_2 = 0$.

Proof : (i) $\Leftrightarrow$ (ii) follows from lemma 1.
Let us prove (ii) $\Rightarrow$ (iii). If $c_0^2 = ac_1^2 + bc_2^2$ with $(c_0, c_1, c_2) \neq (0, 0, 0)$, then $x = c_0 + c_1 i + c_2 j \neq 0$ and $n(x) = 0$. Therefore (ii) $\Rightarrow$ (iii). Finally (iii) implies (ii). Let $x = d_0 + d_1 i + d_2 j + d_3 k$ with $n(x) = 0$, that is

$$\begin{aligned} d_0^2 - ad_1^2 - bd_2^2 + abd_3^2 &= 0 \\ d_0^2 - bd_2^2 &= a(d_1^2 - bd_3^2) \\ a(d_1^2 - bd_3^2)^2 &= (d_0^2 - bd_2^2)(d_1^2 - bd_3^2) \\ a(d_1^2 - bd_3^2)^2 &= (d_0 d_1 + bd_2 d_3)^2 - b(d_0 d_3 + d_1 d_2)^2 \end{aligned}$$

From assumption (iii) $d_1^2 - bd_3^2 = 0$, and therefore $d_1 = d_3 = 0$, similarly $d_0 = d_2 = 0$, that is $x = 0$.

2.1.1 Isomorphism of Quaternion Algebras

For any quaternion algebra H/K, we will denote by H_0 the subset of H of quaternions with zero reduced trace, V and V_0 are the K-vector space sub-adjacent to H and H_0. For x, y in $H = \{a, b\}$, using the reduced norm we define:

$$\beta(x, y) = \frac{1}{2}(n(x + y) - n(x) - n(y)).$$

If $x = c_0 + z, y = d_0 + w$ with $c_0, \quad d_0 \in K$ and $z = c_1 i + c_2 j + c_3 k \in H_0, \quad w = d_1 i + d_2 j + d_3 k \in H_0$, we have :

$$\begin{aligned}
\beta(x, y) &= \frac{1}{2}((x + y)\overline{(x + y)} - x\bar{x} - y\bar{y}) \\
&= \frac{1}{2}((x + y)(\bar{x} + \bar{y}) - x\bar{x} - y\bar{y}) \\
&= \frac{1}{2}(x\bar{y} + y\bar{x}) \\
&= \frac{1}{2}\left((c_0 + z)(d_0 - w) + (d_0 + w)(c_0 - z)\right) \\
&= c_0 d_0 - \frac{1}{2}(zw + wz) \\
&= c_0 d_0 - ac_1 d_1 - bc_2 d_2 + abc_3 d_3.
\end{aligned}$$

These equations show that β is a bilinear mapping of $V \times V$ to K, which is symmetric and non-singular. Moreover $\beta(x, x) = n(x)$ and if $z, w \in V_0$ then

$$\beta(z, w) = -\frac{1}{2}(zw + wz) \text{ and } n(z) = -z^2. \tag{2.5}$$

This implies that β is a non degenerate bilinear form associated to the vector spaces V and V_0.
Also these equations are equivalent to $\beta(x, y) = \frac{1}{2}tr(x\bar{y})$.

Lemma 2.1.7 *: Let $H = \{a, b\}$ and $H' = \{a', b'\}$ be two quaternion algebras over K with the respective reduced norm n and n'. As K-algebras H is isomorphic to H' if and only if there is a vector space isomorphism $\phi : H_0 \to H'_0$ such that $n'(\phi(z)) = n(z)$ for all $z \in H_0$.*

Proof: We will start the proof with a characterization of H_0. If $x = c + z$ with $c \in K$ and $z \in H_0$, then

$$\begin{aligned}
x^2 &= c^2 + z^2 + 2zc \\
&= c^2 - n(z) + 2zc.
\end{aligned}$$

This implies that $x^2 \in Z(H) = K$ if and only if $z = 0$ or $c = 0$.
This calculation shows that

$$x \in H_0 \text{ if and only if } \quad x \notin Z(H) \quad \text{and} \quad x^2 \in Z(H). \tag{2.6}$$

We can similarly characterize H_0'. Therefore, for any algebra isomorphism

$$\begin{aligned} \phi : H &\longrightarrow H', \\ \text{we have :} \phi(Z(H)) = Z(H') &\text{ and } \phi(x^2) = (\phi(x))^2. \end{aligned}$$

It follows from this and equation(1.6) that $\phi(H_0) = H_0'$. If $z \in H_0$, then

$$n'(\phi(z)) = -(\phi(z))^2 = \phi(-z^2) = \phi(n(z)) = n(z).$$

Conversely, suppose that $\phi : H_0 \to H_0'$ is a vector space isomorphism such that $n'(\phi(z)) = n(z)$. We have to show that $H \cong H'$.
We will construct a basis for H' for which the structure constants are the same as the structure constants with the standard basis of H. By equation(2.5)

$$\phi(i)^2 = -n'(\phi(i)) = -n(i) = i^2 = b.$$

Similarly $\phi(j)^2 = b$. Moreover

$$\begin{aligned} \phi(i)\phi(j) + \phi(j)\phi(i) &= -2\beta'(\phi(i), \phi(j)) \\ &= -2\beta(i, j) \\ &= ij + ji \\ &= 0 \\ \Rightarrow \phi(i)\phi(j) &= -\phi(j)\phi(i) \\ \Rightarrow (\phi(i)\phi(j))^2 &= -ab \end{aligned}$$

From equation(2.6) it follows that $\phi(i)\phi(j) \in H_0$. In fact $\phi(i), \phi(j), \phi(i)\phi(j)$ is a basis of H_0' : if

$$\begin{aligned} c_1\phi(i) + c_2\phi(j) + c_3\phi(i)\phi(j) &= 0 \text{ with } (c_1, c_2, c_3) \in K^3 \\ \Rightarrow \phi(i)\left(c_1\phi(i) + c_2\phi(j) + c_3\phi(i)\phi(j)\right) &= 0 \\ \Rightarrow ac_1 + c_2\phi(i)\phi(j) + c_3a\phi(j) &= 0 \\ \Rightarrow c_1 &= 0 \end{aligned}$$

Similarly c_2 and $c_3 = 0$. Define a mapping

$$\begin{aligned} \psi : H &\longrightarrow H' \\ 1 &\longmapsto 1 \\ i &\longmapsto \phi(i) \\ j &\longmapsto \phi(j) \\ k &\longmapsto \phi(i)\phi(j). \end{aligned}$$

The preceding discussion shows that ψ is a K-algebra Isomorphism. □

Now we will translate the previous lemma in terms of quadratic forms. If $z = c_1 i + c_2 j + c_3 k \in H_0$, then $n(z) = \Phi(c_1, c_2, c_3)$, where Φ is the ternary quadratic form $-ax_1^2 - bx_2^2 + abx_3^2$.
That is

$$\Phi(x_1, x_2, x_3) = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \alpha \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \tag{2.7}$$

where α is $\begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix}$.
We say two quadratic forms are equivalent if it is possible to pass from one to other by a non-singular linear change of variables.

Proposition 2.1.8 *: The quaternion algebra $H = \{a, b\}$ and $H' = \{a', b'\}$ over K are isomorphic if and only if the quadratic forms $-ax_1^2 - bx_2^2 + abx_3^2$ and $-a'x_1^2 - b'x_2^2 + a'b'x_3^2$ are equivalent.*

Proof : Let $\Phi(x_1, x_2, x_3) = -ax_1^2 - bx_2^2 + abx_3^2$ and $\Phi'(x_1, x_2, x_3) = -a'x_1^2 - b'x_2^2 + a'b'x_3^2$ and let $z = c_1 i + c_2 j + c_3 k$, $z' = c_1' i' + c_2' j' + c_3' k'$, $n(z) = -ax_1^2 - bx_2^2 + abx_3^2$, and $n'(z') = -a'x_1^2 - b'x_2^2 + a'b'x_3^2$. Write

$$\alpha = \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix}, \alpha' = \begin{bmatrix} -a' & 0 & 0 \\ 0 & -b' & 0 \\ 0 & 0 & a'b' \end{bmatrix}, \xi = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}, \xi' = \begin{bmatrix} c_1' \\ c_2' \\ c_3' \end{bmatrix}$$

Then $n(z) = \xi^t \alpha \xi$ and $n'(z') = (\xi')^t \alpha' \xi'$, where the superscript t denotes matrix transposition. If $w = d_1 i + d_2 j + d_3 k$ and $w' = d_1' i' + d_2' j' + d_3' k'$, then $\beta(z, w) = \xi^t \alpha \eta$ and $\beta'(z', w') = (\xi')^t \alpha \eta'$, where

$$\eta = \begin{bmatrix} d_1 \\ d_2 \\ d_3 \end{bmatrix}, \eta' = \begin{bmatrix} d_1' \\ d_2' \\ d_3' \end{bmatrix}.$$

Suppose that $\phi : H_0 \longrightarrow H_0'$ is linear, that is $[\phi(i), \phi(j), \phi(k)] = [i', j', k']\, \delta$, where $\delta = [d_{ij}] \in M_3(K)$. The mapping is bijective if and only if δ is non singular. If $z = c_1 i + c_2 j + c_3 k = [i, j, k]\, \xi$, then

$$\phi(z) = [\phi(i), \phi(j), \phi(k)]\, \xi = [i', j', k']\, \delta \xi.$$

Similarly $\phi(w) = [i', j', k']\, \delta \eta$. Consequently,

$$\begin{aligned} \beta'(\phi(z), \phi(w)) &= (\delta \xi)^t \alpha' (\delta \eta) \\ &= \xi^t (\delta^t \alpha' \delta) \eta. \end{aligned}$$

Therefore ϕ satisfies $n'(\phi(z)) = n(z)$ for all $z \in H_0$, or equivalently
$\beta'(\phi(z), \phi(w)) = \beta(z, w)$ for all $z, w \in H_0$ if and only if $\xi^t \alpha \eta = \xi^t (\delta^t \alpha' \delta) \eta$ for all ξ, η in K^3. Clearly, this last condition is equivalent to $\alpha = \delta^t \alpha' \delta$. So the quaternion algebras $H = \{a, b\}$ and $H' = \{a', b'\}$ over K are isomorphic if and only if the quadratic forms $-ax_1^2 - bx_2^2 + abx_3^2$ and $-a'x_1^2 - b'x_2^2 + a'b'x_3^2$ are equivalent. □

Corollary 2.1.9 *:If a ,b and c are non zero elements K, then*

$$\left(H = \left\{ac^2, b\right\}\right) \cong \left(H' = \left\{a, bc^2\right\}\right) \cong \left(H'' = \{a, b\}\right). \tag{2.8}$$

Proof : This follows from the proposition. □

As a consequence of the corollary there are only three quaternion algebras over $\mathbb{R}$ up to isomorphism. They are
$\{1,1\}$, $\{1,-1\}$ and $\{-1,-1\}$. We will represent $\{-1,-1\}$ by $\mathbb{H}$ which is known as the Hamiltonian quaternion algebra.

To prove that every simple central algebra of dimension 4 is a quaternion algebra, we will use some theorems and definitions that we are going to state in the next subsection..

2.1.2 Maximal Subfields

In this section A is a K-algebra. A subfield of a K-algebra A is a sub-algebra E of A such that E is a field, and E contains the identity element of A. So we can view E as an extension of K. If there is no subfield F of A such that $E \subset F$, then E is called a maximal subfield of A.

Lemma 2.1.10 *:If B is a K-algebra with $\dim_K B = k < \infty$, and if $n \in \mathbb{N}$ is divisible by k, then B is isomorphic to a sub algebra of $M_n(K)$.*

Proof : If $k = n$, then we have nothing to prove. The general case follows from the map x $\rightarrow$ (x,x,x,x,...x) is an injective algebra homomorphism from B to a product A of n/k copies of B with $\dim_K A = n$. □

Lemma 2.1.11 *: Let D be a division algebra over K. If $x \in D$, then there is a subfield E of D such that $x \in E$. If $\dim_K D < \infty$, then the sub algebra $K[x] = \{\Phi(x) : \Phi \in K[X]\}$ is a subfield of D .*

Proof : Since $K \subseteq Z(D)$, $K[x]$ is a commutative sub-algebra of D and we have a map

$$\begin{aligned} \theta : K[X] &\longrightarrow K[x] \\ \Phi &\mapsto \Phi(x) \end{aligned}$$

which is an algebra homomorphism. Since D has no proper zero divisors, $K[x]$ is an integral domain, which implies that Ker(θ) is a prime ideal of $K[X]$. If $\dim_K D < \infty$ then Ker(θ) $\neq 0$, and Ker(θ) is a maximal ideal. This implies that $E = F[x]$ is a field containing x and contained in D. If Ker(θ) $= 0$, then

$$E = \left\{\Phi(x)\Psi(x)^{-1} : \Phi, \Psi \in F[X], \Psi \neq 0\right\}$$

is a subfield of D containing x. □

Now the $\mathfrak{S}(K)$ will denote the family of all finite dimensional simple central algebras over K. It follows from last lemma that if $D \in \mathfrak{S}(K)$ and D is a division algebra, then every sub-algebra of D is also a division algebra.
For $n \in \mathbb{N}$, we will say that the field K is n-closed if there is no proper extension E of K such that $[E : K]$ divides n. So every field is 1-closed and a field K is n-closed for all $n \in \mathbb{N}$ if and only if K is algebraically closed.

Lemma 2.1.12 *: If A is a simple finite dimensional K-algebra such that K is maximal subfield of A, then $A \cong M_n(K)$ and K is n-closed, where $n \in \mathbb{N}$ is $(\dim_K A)^{1/2}$.*

Proof: Since A is a simple finite dimensional algebra, Wedderburn's structure theorem implies that $A \cong M_n(D)$, where D is division algebra over K. In fact $D = K$, otherwise by the last lemma there would be a subfield E of D which properly contains K. The assumption that K is a maximal subfield of A excludes this possibility. If K is not n-closed, then there is a proper extension E/K such that $[E : K]$ divides n. In this case $M_n(K) \cong A$ contains a subfield that is isomorphic to E by the previous lemma, which again contradicts the maximality of K. □

If X is a subset of the algebra A , then the centralizer of X in A is defined to be

$$C_A(X) = \{y \in A : xy = yx \text{ for all } x \in X\}. \tag{2.9}$$

Lemma 2.1.13 *: Let X and Y be subsets of the algebra A, and suppose that B is a sub algebra of A.*
(i) *$C_A(X)$ is a sub algebra of A with $Z(A) \subseteq C_A(X)$.*
(ii) *If $X \subseteq Y$, then $C_A(Y) \subseteq C_A(X)$.*
(iii) *$X \subseteq C_A(Y)$ if and only if $Y \subseteq C_A(X)$; in particular, $X \subseteq C_A(C_A(X))$.*
(iv) *$B \cap C_A(B) = Z(B)$.*
(v) *$C_A(X) = A$ if and only if $X \subseteq Z(A)$.*

Proof : These are an easy consequence of definition. □

Theorem 2.1.14 *:Let $A \in \mathfrak{S}(K)$, and suppose that B is a simple sub-algebra of A.*
(i) *$C_A(B)$ is simple.*
(ii) *$(\dim_K B)(\dim_K C_A(B)) = \dim_K A$.*
(iii)*$C_A(C_A(B)) = B$.*

We are not going to give the proof of this theorem. For the proof see ([Pi], chapter 12). We will just use the statement of the theorem. This theorem is known as the double centralizer theorem (DCT).

Proposition 2.1.15 *: Let $A \in \mathfrak{S}(K)$, and suppose that E is a subfield of A with $[E : K] = k$. The following conditions are equivalent.*
(i)*E is a maximal subfield of A.*
(ii) *$C_A(E) \cong M_n(E)$ and E is n-closed.*
If (i) *and* (ii) *are satisfied, then $\dim_K A = (kn)^2$.*

Proof : Assume that E is a maximal subfield of A. Since E is simple so is $C_A(E)$ by the last theorem. Moreover $E \subseteq Z(C_A(E))$ because E is commutative. Thus $C_A(E)$ is a simple E -algebra, and since E is maximal in A, it is also maximal in $C_A(E)$. From Lemma(2.1.12), there exists $n \in \mathbb{N}$ such that $C_A(E) \cong M_n(E)$ and E is n-closed. The last theorem also gives

$$\dim_K(A) = (\dim_K E)(\dim_K(C_A(E)) = [E : K]\,(\dim_K M_n(E)) = n^2k^2.$$

Conversely suppose that (ii) is satisfied. Let $E \subseteq F$, F a maximal subfield of A. Then $F \subseteq C_A(E) \cong M_n(E)$. Hence F is a maximal subfield of $B = C_A(E) \in \mathfrak{S}(E)$. From the first part of the proof, we get

$$C_B(F) \cong M_m(F) \quad \text{and} \quad n^2 = \dim_E B = (m[F : E])^2.$$

So $[F : E]$ divides n but E is n -closed by assumption. This implies that $E = F$ is a maximal subfield of A. □

Corollary 2.1.16 *If $A \in \mathfrak{S}(K)$, then $\dim_K(A) = m^2$ for some $m \in \mathbb{N}$. For a subfield E of A, $[E : F]$ divides m.*

Proof : This follows from the proposition. □

The natural number m is called the degree of A. It will be denoted by Deg$A$. We have Deg$A = (\dim_K(A))^{1/2}$. We will say that a subfield E of $A \in \mathfrak{S}(K)$ is *strictly maximal* if $[E : K] =$ Deg$A$.

Corollary 2.1.17 *: A subfield E of $A \in \mathfrak{S}(K)$ is strictly maximal if and only if $C_A(E) = E$. If A is a division algebra, then every maximal subfield of A is strictly maximal.*

Proof : The first assertion follows from the double centralizer theorem because $E \subseteq C_A(E)$ and $(\text{Deg}A)^2 = \dim_K(A) = [E : K]\,(\dim_K C_A(E))$. If E is a maximal subfield of the division algebra A, so that $M_n(E) \cong C_A(E) \subseteq A$ by the proposition, then $n = 1$ since A has no non-zero nilpotent elements. Thus $C_A(E) = E$ and E is strictly maximal.

We are going to give the statement of the **Noether-Skolem Theorem**.
Statement : Let $A \in \mathfrak{S}(K)$ and suppose that B is a simple sub-algebra of A. If χ is an algebra homomorphism from B to A, then there exists $u \in A^*$ such that $\chi(y) = u^{-1}yu$ for all $y \in B$.
For the proof see ([Pi], chapter 12). Following corollaries are consequences of the theorem.

Corollary 2.1.18 *For all separable quadratic algebras L/K, contained in H, there exists $\theta \in K^*$ such that $H = \{L, \theta\}$.*

Proof: Let $L = K(m)$. By the above theorem, every K-automorphism of L is induced by an interior automorphism of H, that is, there exists $u \in K^*$ such that $umu^{-1} = \overline{m}$. It is easy to check that $t(u) = 0$ and $u^2 \in K^*$, say $u^2 = \theta$, which implies $H = \{L, \theta\}$.

Corollary 2.1.19 *The quaternion algebra $H = \{L, \theta\}$ is isomorphic to $M_2(K)$ if and only if either L is not a field or $\theta \in n(L)$.*

Proof: If L is not a field, then K is a maximal subfield and $H \cong M_2(K)$. We may thus assume that L is a field. We will show that if H is not a division algebra then $\theta \in n(L)$. We can choose a non-zero element of H, say $h = m_1 + m_2 u$, such that $n(h) = 0$. Then $n(h) = n(m_1) - n(m_2)\theta = 0$. We conclude that $n(m_2)\theta = n(m_1)$. Now, if $n(m_2) = 0$, then $n(m_1) = 0$ as well and we conclude that $h = 0$. Consequently, $n(m_2) \neq 0$ and we have $\theta = n(m_1 m_2^{-1}) \in n(L)$. Now we will show $H = \{L, \theta\}$ is isomorphic to $M_2(K)$ if and only if $\theta \in n(L)$. If $\theta \in n(L)$, then there exists an element in H other than ± 1 whose square is 1. If $h^2 = 1$ and $h \neq \pm$ then $h \pm 1$ is a zero divisor. We can choose an element in H, a divisor of zero, denoted by x and separable over K and and put $L' = K(x)$. From the Skolem -Noether theorem we can show that $H = \{L', \theta'\}$. As L' is not a field $H \cong M_2(K)$. If $\theta \notin n(L)$ then every non-zero element in H has a non-zero reduced norm, which implies that H is division algebra. □

Theorem 2.1.20 *: If $A \in \mathfrak{S}(K)$ has degree 2, i.e. A is a simple central Algebra of dimension 4 over K, then A is isomorphic to a quaternion algebra.*

Proof : Let E be a maximal subfield of A. If $E = K$, then $A \cong M_2(K) \cong (H = \{1, 1\})$ by Lemma 2.1.12. If $E \neq K$, then E is a quadratic extension of K and since char(K) $\neq 2$, we can write $E = K(x)$, where $x^2 = a \in K^*,\ x \notin K$.

The mapping $x \mapsto -x$ defines an automorphism of E, so by the Noether-Skolem theorem, there exists $y \in A^*$ such that $y^{-1}xy = -x$. Clearly $y \in A - E$. Therefore $\dim_K(K + Kx + Ky + Kxy) = 4 = dim_K(A)$. Note that $xy = -yx$ implies $xy^2 = -yxy = y^2x$. Hence $y^2 \in Z(A) = K$, say $y^2 = b \in K^*$. The above discussion shows that the correspondences

$$\begin{aligned} 1 &\to 1 \\ x &\to i \\ y &\to j \\ xy &\to k \end{aligned}$$

extends to K-algebra homomorphism from A to $H = \{a, b\}$. □

To prove the next corollary we will introduce the *Brauer Group*.

2.1.3 Brauer Group

Let A, B be a simple central algebras over K i.e. $A, B \in \mathfrak{S}(K)$. We will write $A \sim B$ if there exists a division algebra $D \in \mathfrak{S}(K)$ and positive integers m and n such that $A \cong M_n(D)$ and $B \cong M_m(D)$. It is easy to check that $\sim$ is an equivalence relation. From this equivalence relation we can say that every central simple algebra is equivalent to some division algebra over K.

We define the Brauer group of K as the set of equivalence classes of finite dimensional simple central algebras over K under this equivalence relation. We will denote the Brauer group of K by $\mathbb{B}(K)$. That is

$$\mathbb{B}(K) = \{[A] : A \in \mathfrak{S}(K)\} \tag{2.10}$$

We will not prove that this is a group. For the proof see ([Pi], chapter 12). We will just give the rule of multiplication in this group .

$$\begin{aligned} [A]\,[B] &= [A \otimes_K B] \\ [K] &= \text{ Identity element} \\ [A]^{-1} &= [A^*]\,. \end{aligned}$$

Where A^* is the opposite K-algebra of A .
As we know there is no finite dimensional division algebra over $\mathbb{C}$ except $\mathbb{C}$. This implies $\mathbb{B}(\mathbb{C}) = \{0\}$.
Now we are returning to the corollary which is known as **Frobenius theorem.**

Corollary 2.1.21 *(Frobenius Theorem) : Up to isomorphism , the only finite dimensional non-commutative division algebra over* $\mathbb{R}$ *is* $\mathbb{H} = \{-1, -1\}$. *Hence* $\mathbb{B}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Proof : Let D be a finite dimensional, non-commutative division algebra over $\mathbb{R}$. Since $\mathbb{C}$ is the only non-trivial algebraic extension of $\mathbb{R}$, either $Z(D) = \mathbb{R}$ or $\mathbb{C}$. The second possibility is excluded because $\mathbb{B}(\mathbb{C}) = \{0\}$. Thus $D \in \mathfrak{S}(\mathbb{R})$. Let E be a maximal subfield of D. By Corollary 2.1.17 , Deg $D = [\mathrm{E} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}]$. Thus D is a quaternion algebra , so that $D \cong \mathbb{H} = \{-1, -1)\}$.

From our earlier discussion we found that if H is a quaternion algebra over K, then it is either isomorphic to $M_2(K)$ or is a division algebra.
If K is a seprably closed field and H is quaternion algebra over K, then K will be the maximal subfield, and from Lemma 2.1.12 , $H \cong M_2(K)$.
Let F be a field containing K. The tensor product of a quaternion algebra H/K with F over K is a quaternion algebra over F, and which is equal to

$$F \otimes H = F \otimes \{L, \theta\} = \{F \otimes L, \theta\}\,.$$

We will denote it by H_F.

Definition 2.1.22 *: A field F/K such that* H_F *is isomorphic to* $M_2(F)$ *is called a neutralizing field of H.*

Definition 2.1.23 *: A quadratic form over a field K is said to be isotropic if there is a non zero vector on which it vanishes.*

Corollary 2.1.24 *: The following properties are equivalent* :
(1) *H is isomorphic to* $M_2(K)$.
(2) *V is an isotropic quadratic space .*
(3) V_0 *is an isotropic quadratic space .*
(4) *The quadratic form* $ax^2 + by^2$ *represents 1.*

Proof : (1) is equivalent to (2) and also (1) is equivalent to (3). For to prove (4) implies (1) we can choose a element $ix + jy$ whose square is $ax^2 + by^2$ and it is different from ± 1. So H is not a division algebra thus $H \cong M_2(K)$. Now we will prove (3) implies (4). If $ax^2 + by^2 - abz^2 = 0$ with $z \neq 0$, then it is clear that $ax^2 + by^2$ represents 1. If $z = 0$, then $b \in -ak^2$, then the quadratic form $ax^2 + by^2$ is equivalent to $a(x^2 - y^2)$ which represents 1.

2.2 Orders and Ideals

In this section we will give the definition of orders and ideals which we will be use in next chapters, when K is local field or global field.
Let R is a dedekind domain i.e. a noetherian ring, integrally closed and every prime ideal is maximal. Let K is fraction field of R and H is quaternion algebra over K.

Definition 2.2.1 *: Let V be a K-vector space. A lattice L in V is free R-module and has finite number of generators contained in V. We say a lattice L is complete if $K \otimes_R L = V$.*

Definition 2.2.2 *: An element $x \in H$ is integral over R if $R[x]$ is a R-lattice of H.*

This definition is equivalent to x is root of some monic polynomial in $R[X]$.

Lemma 2.2.3 *: An element $x \in H$ is integral if and only if the reduced trace and the reduced norm are elements of R.*

Proof : As we know x satisfy the equation $X^2 - t(x)X + n(x) = 0$. Which is equivalent to $R[x]$ is R-lattice if and only if $t(x), n(x)$ belongs to R.

Using this lemma we recognize that if an element is an integer, contrary to commutative case, the sum and the product of integers are not always integers. This implies that the set of integers does not form a ring here. So this is the main problem here if someone wants to make explicit calculation. Now we are going to define order and ideal here.

Definition 2.2.4 *: An ideal of H is a finitely generated R -submodule I of H, which is complete lattice. That is $K \otimes_R I \cong H$.*

Definition 2.2.5 *: A subset $\mathcal{O}$ of H is called an order if it satisfies the following equivalent conditions:*
(i) *$\mathcal{O}$ is an ideal of H which is also a subring of H.*
(ii) *$\mathcal{O}$ is a subring of H containing R, $K\mathcal{O} = H$, and every element of $\mathcal{O}$ is an integer of H.*

We are going to prove (i) and (ii) are equivalent. It is clear that (i) implies (ii). Conversely, let (a_i) is a basis of H/K contained in $\mathcal{O}$, and put $L = \sum Ra_i$. An element of $\mathcal{O}$ can be written as $h = \sum x_i a_i \quad , \quad x_i \in K$. As $\mathcal{O}$ is a ring , $ha_i \in \mathcal{O}$ and $t(ha_i) = \sum_j x_j t(a_j a_i) \in R$. This implies $L \subset \mathcal{O} \subset dL$, where $d = (\det(t(a_j a_i)))^{-1} \neq 0$. We deduce that $\mathcal{O}$ is an ideal. Hence we proved.

A *maximal* R-order in H is an R-order which is not properly contained in any other R-order. An *Eichler-order* is the intersection of two maximal orders.

Now our chief aim is to prove that H contains R-orders. Certainly there exist ideals. For example if $H = \sum Kx_i$, where (x_i) is a basis of H over K, then $I = \sum Rx_i$ is a full R-lattice in H, i.e. I is an ideal. We define the *left order* of I as

$$\mathcal{O}_l(I) = \{\ h \in H\ :\ hI \subset I\ \}$$

Clearly $\mathcal{O}_l(I)$ is a sub ring of H, and it is an R-module. So we only need to verify that it is a full R-lattice in H. For each $y \in H$, yI is an R-lattice in H and so there exists a non zero $r \in R$ such that $ryI \subset I$. Thus $ry \in \mathcal{O}_l(I)$, which proves that $K.\mathcal{O}_l(I) = H$. Next, there exists a non-zero $s \in R$ such that $s \in I$. Therefore $\mathcal{O}_l(I).s \subset I$, whence $\mathcal{O}_l(I) \subset s^{-1}I$. Since R is a noetherian ring and $s^{-1}I$ is an R-lattice, this implies that $\mathcal{O}_l(I)$ is also an R-lattice. This prove that $\mathcal{O}_l(I)$ is an R-order in H. Similarly, we define *right order* of I

$$\mathcal{O}_r(I) = \{\ h \in H\ :\ Ih \subset I\ \}.$$

It is an R-order in H.

Definition 2.2.6 *: We say that an ideal I whose left order is $\mathcal{O}_l$, and right order is $\mathcal{O}_r$, is bilateral if $\mathcal{O}_l = \mathcal{O}_r$, normal if $\mathcal{O}_l$ and $\mathcal{O}_r$ are maximal, integral if it is contained in $\mathcal{O}_l$ and $\mathcal{O}_r$, and principal if $I = \mathcal{O}_l h = h\mathcal{O}_r$ for some $h \in H^*$.*

We now define

$$I^{-1} = \{\ h \in H\ :\ I.h.I \subset I\ \}$$

Clearly

$$I^{-1} = \{\ h \in H\ :\ I.h \subset \mathcal{O}_l(I)\ \} = \{\ h \in H\ :\ h.I \subset \mathcal{O}_r(I)\ \}$$

If $\Lambda = \mathcal{O}_l(I)$, then $\alpha\Lambda \subset I \subset \beta\Lambda$ for some non zero $\alpha, \beta \in R$. Therefore $\alpha^{-1}\Lambda \supset I^{-1} \supset \beta^{-1}\Lambda$, since

$$\alpha^{-1}\Lambda = \{h \in H : \alpha\Lambda.h \subset \Lambda\} \supset \{h \in H : I.h \subset \Lambda\} = I^{-1}.$$

Similarly for the other inclusion. Thus I^{-1} is also a full R-lattice in H.

The product IJ of two ideals I, J is the set of finite sums of elements hk, where $h \in I$, $k \in J$. It is obvious that IJ is an ideal. From the definition, we see that the product of two ideals is associative .

Lemma 2.2.7 . (1) *The ideal I is an integral ideal if and only if it contained in one of the orders.*
(2) *The ideal I and I^{-1} satisfy*
$\mathcal{O}_l(I^{-1}) \supset \mathcal{O}_r(I)$, $\mathcal{O}_r(I^{-1}) \supset \mathcal{O}_l(I)$, $I\ I^{-1} \subset \mathcal{O}_l(I)$, $I^{-1}I \subset \mathcal{O}_r(I)$.

proof : This is an easy verification. □

2.2.1 Properties of principal ideals

Let $\mathcal{O}$ be an order, and $I = \mathcal{O}h$ be a principal ideal. The left order of I is equal to $\mathcal{O}$ and the right order is $\mathcal{O}' = h^{-1}\mathcal{O}h$. Then $I = h\mathcal{O}'$.

We have the following multiplication rules for principal ideals :
$\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1}) = I\ I^{-1}$, $\mathcal{O}_r(I) = \mathcal{O}_l(I^{-1}) = I^{-1}I$, $\mathcal{O}_l(IJ) = \mathcal{O}_l(I)$,
$\mathcal{O}_r(IJ) = \mathcal{O}_r(J)$, $(IJ)^{-1} = J^{-1}I^{-1}$
From now on we will assume that the above rules of multiplication hold true for the ideals and orders considered.

Definition 2.2.8 *We say that the product IJ of two ideals I and J is proper if $\mathcal{O}_r(I) = \mathcal{O}_l(J)$.*

Let I, J, C, D are four ideals such that the product CJ and JD are *proper*. We will show that the equality $I = CJ = JD$ is equivalent to $C = IJ^{-1}$ and $D = J^{-1}I$.
Since the product CJ is proper, this implies $\mathcal{O}_l(J) = \mathcal{O}_r(C)$. Now $I = CJ$, implies $IJ^{-1} = CJJ^{-1} = C\ \mathcal{O}_l(J) = C\ \mathcal{O}_r(C) = C$. Similarly we get the result: if $C = IJ^{-1}$ then $I = CJ$. Similarly for the other equality.

Lemma 2.2.9 *: The relation $I \subset J$ is equivalent to $I = CJ$ and to $I = JD$, where C and D are integral ideal and the products are proper.*

Proof : If $I \subset J$, take $C = IJ^{-1}$. Then $C = IJ^{-1} \subset JJ^{-1} = \mathcal{O}_l(J) = \mathcal{O}_r(C)$. So C is an integral ideal and equivalent to $I = CJ$. Conversely if
$I = CJ \subset \mathcal{O}_r(C)J \subset \mathcal{O}_l(J)J \subset J$. Similarly for the other possibilities.

This also gives the multiplication rules. From now on we will suppose that the product of ideals is proper.

2.2.2 Bilateral ideal or two sided ideal

Definition 2.2.10 *: Let $\mathcal{O}$ be an order. A prime ideal of $\mathcal{O}$ is a proper non zero two sided integral ideal P in $\mathcal{O}$ such that for every pair of two sided ideals I and J in $\mathcal{O}$, $IJ \subset P$ implies $I \subset P$ or $J \subset P$.*

We will show that I is a prime ideal if and only if it is strictly contained in no other ideal distinct from $\mathcal{O}$. Let I be an ideal which is strictly contained in no other ideal, and let J and J' two two-sided integral ideal of $\mathcal{O}$ such that $JJ' \subset I$. If $J \not\subset I$, then the ideal $I + J$ contains I strictly, hence is equal to $\mathcal{O}$. So $(I + J)\ J' = J'$, whence $IJ' + JJ' = J'$, and $J' \subset I$. Consequently I is a prime ideal. Conversely, if I is a prime ideal and J is a two-sided integral ideal such that $I \subset J$, then $I = JD$, where $D = J^{-1}I$ are two-sided integral ideal. From this we deduce that $D \subset I$, which is not possible.

Now we will show next that the product of two prime ideals in $\mathcal{O}$ commutes. Let P

and Q be two prime ideals and write $QP = PQ'$(applying the process of factorisation), where Q' is another two sided integral ideal. This implies $PQ' \subset Q \Rightarrow Q' \subset Q$, which implies $QP \subset PQ$. By symmetry of P and Q, we can similarly show that $PQ \subset QP$, whence $QP = PQ$.

Since $\mathcal{O}$ is a finitely generated R-module, any strictly increasing chain of ideals is finite. Using the above results and rules of multiplication, we will show that the family of two-sided ideal of $\mathcal{O}$ form a free group generated by the prime ideals.

Let I be an ideal, whose the left order is $\mathcal{O}$ and right order is $\mathcal{O}'$, and let P be prime ideal of $\mathcal{O}$. The product $I^{-1}PI$ is a two-sided ideal of $\mathcal{O}'$. If I is two-sided ideal of, then $I^{-1}PI = P$. If not, that is, $\mathcal{O}' \neq \mathcal{O}$, then $P' = I^{-1}PI$ is prime ideal of $\mathcal{O}'$, independent of the choice of Ideal I, whose left order is $\mathcal{O}$ and right order is $\mathcal{O}'$. We now verify this. Suppose P' is not a prime ideal, this implies $P' \subset M$, where M is a two-sided of $\mathcal{O}'$, which implies $P \subset IMI^{-1}$, that is, P contained in IMI^{-1}, which is two sided ideal of $\mathcal{O}$, contradiction. To show independence, of the choice of an ideal I whose left order is $\mathcal{O}$ and the right order is $\mathcal{O}'$, we can write every ideal whose left order is $\mathcal{O}$ and right order is $\mathcal{O}'$ in the form IJ' or JI , where J is a two-sided ideal of $\mathcal{O}$ and J' is a two sided ideal of $\mathcal{O}'$. From this independence of I is obvious..

2.2.3 Properties of non bilateral ideal

Let $\mathcal{O}$ be an order. We say that an non zero proper integral ideal P is irreducible if it is maximal with respect to inclusion in the set of all ideals whose left order is $\mathcal{O}$.

Its easy to see that the P is a maximal ideal in the set of integral ideals of $\mathcal{O}_r(P)$.

Theorem 2.2.11 *For each maximal left ideal P of a maximal R-order $\mathcal{O}$, there is a unique prime ideal $\mathfrak{P}$ of $\mathcal{O}$ such that*

$$\mathfrak{P} \subset P \subset \mathcal{O}, \qquad \mathfrak{P} = \operatorname{ann}(\mathcal{O}/P) = \{x \in \mathcal{O} : x\mathcal{O} \subset P\}.$$

We will not give the proof of this theorem. For the proof see ([Re], page no 195). Also, from this we will get that every integral ideal is product of irreducible ideals.

Definition 2.2.12 *: The reduced norm n(I) of an ideal I is the fractional-ideal of R generated by the reduced norms of their elements.*

If $I = \mathcal{O}h$ is a principal ideal , then $n(I) = Rn(h)$. If $J = \mathcal{O}'h'$ is another principal ideal, whose left order is $\mathcal{O}' = h^{-1}\mathcal{O}h$, then $IJ = \mathcal{O}hh'$, whence $n(IJ) = n(I)n(J)$. Also this results holds also for non-principal ideals.
Also, we can define the norm of an Ideal I, whose left order is $\mathcal{O}$ and right order is $\mathcal{O}'$ by $n(I) = \operatorname{ord}_R(\mathcal{O}/I)$, where $\operatorname{ord}_R(M/N)$, for two ideals M and N, is defined by $\operatorname{ord}_R(M/N) = \mathrm{E}_1\mathrm{E}_2....\mathrm{E}_r$, where

$$M = \mathrm{J}_1 m_1 \oplus \mathrm{J}_2 m_2 \oplus .... \oplus \mathrm{J}_r m_r, \quad N = \mathrm{E}_1\mathrm{J}_1 m_1 \oplus \mathrm{E}_2\mathrm{J}_2 m_2 \oplus .... \oplus \mathrm{E}_r\mathrm{J}_r m_r.$$

Here $\{m_i\} \in M$ and $\{\mathrm{J}_i\}$, $\{\mathrm{E}_i\}$ are fractional R-ideals.

2.2.4 Different and Discriminant

For an ideal I , we define a complementary ideal

$$\widetilde{I} = \{x \in H : t(xI) \subset R\}$$

Here,

$$t : H \times H \to K$$

is the non-degenerate bilinear trace form defined in section (2.1), that is,

$$t(h, k) = t(hk)$$

First we will prove that $\widetilde{I}$ is an ideal, i.e., it is full R-lattice in H. Since I is contained in some full R-lattice $N = \bigoplus_{i=1}^{4} Rx_i$, there exists $\{y_j\} \in H$ such that $t(x_i, y_j) = \delta_{ij}, 1 \leq i, j \leq 4$. Then

$$\widetilde{I} \supset \widetilde{N} = \bigoplus_{i=1}^{4} Ry_i.$$

Similarly, $\widetilde{I}$ is contained in some full R-lattice in H. Therefore $\widetilde{I}$ itself is a full R-lattice in H. The left order of $\widetilde{I}$ is $\left\{x \in H : t(x\widetilde{I}I) \subset R\right\} = \left\{x \in H : t(\widetilde{I}xI) \subset R\right\}$, because $t(xy) = t(yx)$. This implies that $\widetilde{I}$ is bilateral ideal. For the case when I is $\mathcal{O}$ itself, we note that $\widetilde{\mathcal{O}} \supset \mathcal{O}$ and $\widetilde{\mathcal{O}}\widetilde{\mathcal{O}}^{-1} \supset \widetilde{\mathcal{O}}^{-1}$, so $\widetilde{\mathcal{O}}^{-1}$ is an integral ideal.

The *different* of $\mathcal{O}$ of with respect to R is defined as

$$\mathfrak{D}(\mathcal{O}/R) = \tilde{\mathcal{O}}^{-1},$$

and the *discriminant* of $\mathcal{O}$ with respect to R is defined as

$$d(\mathcal{O}/R) = n(\widetilde{\mathcal{O}}^{-1}) = n(\mathfrak{D}(\mathcal{O}/R)).$$

Lemma 2.2.13 *If*

$$\mathcal{O} = \bigoplus_{\mathrm{i}=1}^{4} R\mathrm{x_i},\ 1 \leq \mathrm{i} \leq 4,$$

and $\mathcal{O}$ is principal, then

$$n(\tilde{\mathcal{O}}^{-1})^2 = R \cdot \det\left(\mathrm{t(x_i x_j)}\right),\quad 1 \leq \mathrm{i,j} \leq 4.$$

Proof : Since $\mathcal{O} = \bigoplus_{i=1}^{4} R\mathrm{x_i}$, there exists elements $\{\mathrm{y_j}\} \in H$ with $t(\mathrm{x_i y_j}) = \delta_{\mathrm{ij}}$, $1 \leq$ i,j ≤ 4. If $\mathrm{y_j} = \sum \mathrm{a_{jk} x_k}$, then $\mathrm{t(x_i y_j)} = \sum \mathrm{a_{jk} t(x_i x_k)}$. Then we get $\det(t(\mathrm{x_i y_j})) = \det(\mathrm{a_{ij}}) \det(t(\mathrm{x_i x_j}))$. Since $\widetilde{\mathcal{O}} = \mathcal{O}h$ for some $h \in H^*$, (because $\mathcal{O}$ is principal), then $(\mathrm{x_i}h)$ is another basis of $\widetilde{\mathcal{O}}$. For $\alpha \in \widetilde{\mathcal{O}}$, $n(\alpha)^2$ is the determinant of the endomorphism $h \to \alpha \mathrm{h}$, so we have $\det(\mathrm{a_{ij}}) = n(\alpha)^2 \mathrm{u}$, $\mathrm{u} \in R^*$. We conclude that R $(\det(t(\mathrm{x_i x_j}))) = n(\widetilde{\mathcal{O}})^{-2} = n(\widetilde{\mathcal{O}}^{-1})^2$. □

This lemma remains valid if $\mathcal{O}$ is not principal.

Corollary 2.2.14 *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders. If $\mathcal{O}' \subset \mathcal{O}$. Further $d(\mathcal{O}') \subset d(\mathcal{O})$ and $d(\mathcal{O}') = d(\mathcal{O})$ implies $\mathcal{O}' = \mathcal{O}$.*

Proof : Let $\mathrm{v_i}$ and $\mathrm{u_i}$ be R-bases of $\mathcal{O}'$ and $\mathcal{O}$ respectively. Since $\mathcal{O}' \subset \mathcal{O}$, we can write $\mathrm{v_i} = \sum_{\mathrm{j}} \mathrm{a_{ij} u_j}$ with $\mathrm{a_{ij}} \in R$. Then $\det(t(\mathrm{v_i v_j})) = (\det(\mathrm{a_{ij}}))^2 \det(t(\mathrm{u_i u_j}))$. This implies that $d(\mathcal{O}') \subset d(\mathcal{O})$. If $d(\mathcal{O}') = d(\mathcal{O})$, that is $(\mathrm{a_{ij}})$ is invertible, then $\mathcal{O}' = \mathcal{O}$.

2.2.5 Ideal classes

The two ideals I and J are called *equivalent on the left* if and only if $I = hJ$, for some $h \in H^*$. If $\mathcal{O}$ is an order, we define the set $\mathrm{Pic}_l(\mathcal{O})$ of left-ideal classes of $\mathcal{O}$ as the set of ideals with right order $\mathcal{O}$ modulo *equivalent on the left.* This is the correct way to define it, since modifying an ideal on the left does not change its right order. Of course there is a similar definition $\mathrm{Pic}_r(\mathcal{O})$ of right-classes of left $\mathcal{O}$-ideals.

Lemma 2.2.15 (1) *The application $I \mapsto I^{-1}$ induces a bijection between left classes and right classes of $\mathcal{O}$.*
(2) *Let J be given ideal. The application $I \mapsto JI$ induces a bijection between left classes of $\mathcal{O}_l(I) = \mathcal{O}_r(J)$ and the left classes of $\mathcal{O}_l(J)$.*

Proof : Easy. □

Two orders are said to be of the same *type* if they are conjugate by an element $h \in H^*$.

Linked orders: We say that two orders $\mathcal{O}$ and $\mathcal{O}'$ are *linked* if there exists an ideal I whose left order is $\mathcal{O}$ and whose right order is $\mathcal{O}'$. This is an equivalence relation, and we will speak of linkage classes of orders. As an example, the maximal orders lie in a single linkage class(since if $\mathcal{O}$ and $\mathcal{O}'$ are any two orders, put $I := \mathcal{O}.\mathcal{O}'$. Then $\mathcal{O} \subset \mathcal{O}_l(I)$ and $\mathcal{O}' \subset \mathcal{O}_r(I)$; if $\mathcal{O}$ and $\mathcal{O}'$ are maximal, we must have equality).

Lemma 2.2.16 . *Linked orders have the same number of (left or right) ideal classes.*

Proof: Suppose $\mathcal{O}$ and $\mathcal{O}'$ are linked by I. We define a map from the set of left $\mathcal{O}$-ideals to the set of right $\mathcal{O}'$-ideals by $J \mapsto J^{-1}I$. The map $P \mapsto IP^{-1}$ gives an inverse. Moreover, the map descends to ideal classes, since $Jh \mapsto (Jh)^{-1}I = h^{-1}J^{-1}I$.

Definition 2.2.17 *: The class number of H(with respect to R) is* $\#\mathrm{Pic}_l(\mathcal{O})$*, where* $\mathcal{O}$ *is any maximal order. Note that the preceding lemma shows that this is well defined. The type number of H is the number of conjugacy classes of maximal orders of H.*

Lemma 2.2.18 *Let* $\mathcal{O}$ *and* $\mathcal{O}'$ *be two orders. The following properties are equivalents.*
(1) $\mathcal{O}$ *and* $\mathcal{O}'$ *are of the same type.*
(2) $\mathcal{O}$ *and* $\mathcal{O}'$ *are linked by a principal ideal.*

Proof : (1) $\Leftrightarrow$(2)
If $\mathcal{O}' = h^{-1}\mathcal{O}h$, then the principal ideal $\mathcal{O}h$ links $\mathcal{O}$ to $\mathcal{O}'$, and conversely.

Corollary 2.2.19 *. If the class number of H is one, its type number is one.*

Proof: Since any two maximal orders are linked by some ideal, this follows immediately from the lemma.

The number of types of orders of H is the number of types of its maximal orders. So we get from the above lemma that the number of types t of the orders connected to a given order is less than or equal to the number of classes h of these orders.

Definition 2.2.20 *: Let L/K be a separable algebra of dimension 2 over K. Let B be an R-order of L and* $\mathcal{O}$ *an R-order of H. An embedding* $f : L \to H$ *is maximal with respect to* $\mathcal{O}/B$ *if* $f(L) \cap \mathcal{O} = f(B)$*. As the restriction of f to B determines f, we also say that f is a maximal embedding of B in* $\mathcal{O}$*.*

Let us suppose that $L = K(h)$ is contained in H. From the Skolen-Noether theorem, the conjugacy classes of h in H^*,

$$C(h) = \left\{xhx^{-1}, x \in H^*\right\}.$$

are in bijection with the set of embeddings of L in H. This is equal to

$$C(h) = \{x \in H, t(x) = t(h), \text{and } \ n(x) = n(h)\}$$

The set of maximal embedding of B in $\mathcal{O}$ are in bijection with the following subset of the conjugacy classes of h in H^* :

$$C(h, B) = \left\{xhx^{-1}, x \in H^* \ K(xhx^{-1}) \cap \mathcal{O} = xBx^{-1}\right\}.$$

We have a disjoint union

$$C(h) = \bigcup_B C(h, B)$$

where B varies over the orders of L. Consider a subgroup G of the normalizer of $\mathcal{O}$ in H^* :

$$N(\mathcal{O}) = \left\{ x \in H^* \ , \quad x\mathcal{O}x^{-1} = \mathcal{O} \right\}.$$

For $x \in H^*$, note that $\widetilde{x} : y \to xyx^{-1}$ is the interior automorphism of H associating to x, and $\widetilde{G} = \{\widetilde{x} \ , x \in G\}$. The set $C(h, B)$ is stable under the left action of $\widetilde{G}$.

Definition 2.2.21 *: A class of maximal embeddings of B in $\mathcal{O}$ is a class of maximal embeddings of B in $\mathcal{O}$ for the equivalence relation $f = \widetilde{x}f'$, $\widetilde{x} \in \widetilde{G}$. The conjugacy class modulo G of $h \in H^*$ is $C_G(h) = \{xhx^{-1} \ \ , x \in G\}$.*

Thus we see that the set of conjugacy classes modulo G of elements $x \in H^*$ such that $t(x) = t(h), n(x) = n(h)$ is equal to

$$\widetilde{G} \setminus C(h) = \bigcup_B \widetilde{G} \setminus C(h, B).$$

In particular if $\#(\widetilde{G} \setminus C(h, B))$ is finite and zero for almost all orders $B \subset L$, we have

$$\#(\widetilde{G} \setminus C(h)) = \sum_B \#(\tilde{G} \setminus C(h, B)).$$

2.2.6 Group of units in an order

The units of an order $\mathcal{O}$ are the invertible elements which are contained in this order. They naturally form a group which is denoted $\mathcal{O}^*$. The units of norm 1 also form a group denoted by $\mathcal{O}^1$.

Lemma 2.2.22 *: An element of $\mathcal{O}$ is a unit if and only if its reduced norm is a unit of R.*

Proof: If x, x^{-1} belongs to $\mathcal{O}$, then $n(x), n(x)^{-1}$ are in R. Conversely if $x \in \mathcal{O}$, and $n(x)^{-1} \in R$, then $x^{-1} = n(x)^{-1}\bar{x} \in \mathcal{O}$, because $\bar{x} \in \mathcal{O}$.

3 Quaternion Algebras over Local Fields

In this chapter K is a local field, i.e. it is a finite extension of K/K' of a field K' which can be one of the following :
- $\mathbb{R}$ the field of real numbers ,
- $\mathbb{Q}_p$ the field of p-adic numbers ,
- $\mathbb{F}_q[[\mathrm{T}]]$ the field of formal series in one variable over a finite field $\mathbb{F}_q$.

If $K' \neq \mathbb{R}$ let R be the ring of integrals of K and $\pi, k = R/\pi R$ a uniformizer and the residue field of K respectively and L_{ur} is a quadratic unramified extension of K in a separable closure K_s.

We will prove that L_{ur} is the unique quadratic unramified extension up to isomorphism. Since L_{ur} is unramified, it has residue degree $\mathrm{f} = 2$ and ramification index $\mathrm{e} = 1$, implies that π is also a uniformizer of L_{ur}. Let L_1 and L_2 be two unramified extension of degree 2 over K and, let R_{L_1} and R_{L_2} be their rings of integers. Since $R_{L_1}/\pi R_{L_1}$ and $R_{L_2}/\pi R_{L_2}$ are degree 2 extensions over k. They are isomorphic. From this we can deduce that $L_1 \cong L_2$.

We will denote by R_L the ring of integers of L_{ur} and by k_L the residue field of L_{ur}. Also, we note that $n(R_L^*) = R^*$.

Let H/K be a quaternion algebra. All the notations of orders and ideals in H are relative to R.

3.1 Classification

In this section we will give the classification of quaternion algebras over local fields. The following theorem classifies the quaternion algebras over local fields.

Theorem 3.1.1 . *Over local fields $K \neq \mathbb{C}$, there exists a unique quaternion division algebra up to isomorphism.*

After developing the necessary theory we will give a proof of this theorem at the end of the section. For $K = \mathbb{R}$, the Frobenius theorem shows that there exists a unique quaternion division algebra namely, Hamilton's quaternions, and for $K = \mathbb{C}$, $M_2(\mathbb{C})$ is the unique quaternion algebra.

Let $\mathrm{Quat}(K)$ be the set of isomorphism classes of quaternion algebras over K. We define an isomorphism of $\mathrm{Quat}(K)$ taking values in $\{\pm 1\}$ by asigning to a quaternion algebra H/K the values : $\varepsilon(H) = -1$ if H is a division algebra, $\varepsilon(H) = 1$ otherwise. We call $\varepsilon(H)$ the Hasse invariant of H.

From theorem 3

$$\mathrm{Quat}(K) \cong \{\pm 1\} \text{ if } K \neq \mathbb{C} \quad , \quad \mathrm{Quat}(\mathbb{C}) \cong \{1\}\,.$$

If $\mathrm{char}(K) \neq 2$, and if a and b $\in K^*$, the Hasse invariant of a , b is defined by

$$\varepsilon(\text{ a , b }) = \varepsilon(\{\mathrm{a}, \mathrm{b}\})$$

where $H = \{\mathrm{a}, \mathrm{b}\}$ is the quaternion algebra described in Chapter II. The Hilbert symbol of a , b is defined by

$$(\mathrm{a}\ ,\ \mathrm{b}) = \begin{cases} 1 \text{ if } \mathrm{ax}^2 + \mathrm{by}^2 - \mathrm{z}^2 = 0 \text{ has a non trivial solution in } K^3 \\ -1 \text{ otherwise} \end{cases} .$$

So from Corollary 2.1.24, Proposition 2.1.6 and Theorem 3.1.1 we conclude that the Hilbert symbol and Hasse invariant agree and satisfy the following properties :
(1) $(\mathrm{ax}^2, \mathrm{by}^2) = (\mathrm{a}, \mathrm{b})$
(2) $(\mathrm{a}, \mathrm{b})\,(\mathrm{a}, \mathrm{c}) = (\mathrm{a}, \mathrm{bc})$
(3) $(\mathrm{a}, \mathrm{b}) = (\mathrm{b}, \mathrm{a})$
(4) $(\mathrm{a}, 1\text{-a}) = 1$
(5) $(\mathrm{a}, \mathrm{b}) = 1$, for all $\mathrm{b} \in \mathrm{K}^*$ implies $\mathrm{a} \in \mathrm{K}^2$
(6) $(\mathrm{a}, \mathrm{b}) = 1$ is equivalent to $\mathrm{a} \in n(\mathrm{K}(\sqrt{b}))$ or $\mathrm{b} \in n(\mathrm{K}(\sqrt{a}))$.
We will not prove these properties. For more details see ([BS], chapter I, section 6).

We suppose from now on that $K \neq \mathbb{R}, \mathbb{C}$. The classification theorem follows from the following more precise theorem.

Theorem 3.1.2 *Let K be a non archimedian local field. Then $H = \{L_u r, \pi\}$ is the unique quaternion division algebra over K up to isomorphism. A finite extension F/K neutralises H if and only if its degree $[F : K]$ is even.*

The proof of the theorem consists of several steps. From now we consider H/K a quaternion divison algebra. To prove the above theorem we will define discrete valuations.

Definition 3.1.3 *A discrete valuation v on a division algebra X is a function $v : X^* \to \mathbb{Z}$ satisfying*
(1) $v(xy) = v(x) + v(y)$
(2) $v(x+y) \geq inf(v(x)\ ,\ v(y))$ for all $x\ ,\ y \in X^*$ with equality if $v(x) = v(y)$.

A non zero element u of minimal valuation is called a *uniformizer* of X. We can extend this application v to a map $v : X \to \mathbb{Z} \cup \{\infty\}$ by setting $v(0)= \infty$. The set $A = \{x \in X, v(x) \geq 0\}$ is the discrete valuation ring associated to v. It has a unique non zero prime ideal, namely $\mathfrak{M} = Au = \{x \in X, v(x) > 0\}$. The field $A/\mathfrak{M}$ is called the $residue field$ of A and the group $A^* = \{x \in X, v(x) = 0\}$ is called the group of units of A. We may suppose that v is surjective, i.e., $v(X^*) = \mathbb{Z}$.

Let H/K be a quaternion algebra which is a division algebra and let v be a valuation on K. We define

$$w : H^* \to \mathbb{Z}$$

by

$$w(h) = v \circ n(h) \qquad\qquad (h \in H^*),$$

where $n : H^* \to K^*$ is the reduced norm map defined in Chapter II. Since the norm is multiplicative, therefore w satisfies the property (1). Since K is a local field, it is commutative and L is an extension of K contained in H, and we conclude that the restriction of w to L is a valuation.

For $h, k \in K^*$ take $L = K(hK^{-1})$. To prove that w is a valuation on H, we have to prove that w satisfies the property(2), that is $w(h + k) \geq inf\,(w(h), w(k))$. We may assume $w(h) \geq w(k)$, so we have to prove that $w(h + k) \geq w(k)$. Now

$$\begin{aligned} w(h+k) - w(k) &= w(hk^{-1} + 1) \\ &\geq inf\left(w(hk^{-1}), w(1)\right), \text{because the restriction of } w \text{ to } L \text{ is a valuation} \\ &\geq 0 \end{aligned}$$

So w satisfies the property (2), that is w, is a discrete valuation of H.

Let us denote by $\mathcal{O}$ the valuation ring associated to the valuation w. For all finite extensions L/K contained in H, $\mathcal{O} \cap L$ is the valuation ring of the restriction of w to L. Then $\mathcal{O} \cap L$ is the ring R_L of integers of L. So we deduce that $\mathcal{O}$ is an order of H, in fact it is unique maximal order in H. From here we get that every normal ideal is a two-sided ideal. If $u \in \mathcal{O}$ is a uniformizer, $P = \mathcal{O}u$ is a unique prime ideal of $\mathcal{O}$. All the normal ideals are of the form $P^n, \quad n \in \mathbb{Z}$.

Lemma 3.1.4 *The unramified quadratic extension L_{ur}/K is isomorphic to a subfield of H.*

Proof : Suppose otherwise. If L_{ur} is not embedded in H, then for all $x \in \mathcal{O} - R$ the extension $K(x)/K$ is ramified. Let us denote by P the only prime ideal of $\mathcal{O}$, $P_1 = P \cap K(x), P_0 = P \cap R$ and $\mathcal{O}_x = \mathcal{O} \cap K(x)$. Since L/K is ramified, we have $P_0\mathcal{O}_x = P_1^2$

and $\mathcal{O}_x/P_1 \cong R/P_0$. This implies that there exists $a \in R$ such that $x = a+ux_1$, with$x_1 \in \mathcal{O} - R$. Proceeding in a similar way we get

$$x = a + ua_1 + u^2a_2 + u^3a_3 + ...$$

with $a, a_1, a_2, a_3, a_4, .. \in R$. Hence $\mathcal{O} = R[[u]] = R[u]$ and therefore $H = K[u]$, which is quadratic over K. This is a contradiction. □

Corollary 3.1.5 *.The unique quaternion division algebra H is isomorphic to $\{L_{ur}, \pi\}$. Its prime ideal is $P = \mathcal{O}u$ and satisfies $P^2 = \mathcal{O}\pi$. Its ring of integers $\mathcal{O}$ is isomorphic to $R_L + R_L u$. The discriminant $d(\mathcal{O})$ of $\mathcal{O}$ is equal to $n(P) = R\pi$.*

Proof : From the corollary 2.1.18 and corollary 2.1.19, we have $H \cong \{L_{ur}, x\}$ where $x \in K^*$ and $x \notin n(L_{ur}^*)$. Since $n(R_L^*) = R^*$, this implies that we can choose $x = \pi y^2$, where $y \in K^*$. We can put $x = \pi$, which proves the first part of the corollary. The element u satisfies $u^2 = x = \pi$, which implies that it has minimal valuation. Then $P = \mathcal{O}u$ satisfying $P^2 = \mathcal{O}\pi$. So the prime ideal $R\pi$ is ramified in $\mathcal{O}$ and $\mathcal{O}$ is the valuation ring of the valuation w, which implies that $\mathcal{O} = \{h \in H : n(h) \in R\}$. Also, $R_L = \{m \in L_{ur} : n(m) \in R\}$. If $h = m_1 + m_2u$ with $m_1, m_2 \in L_{ur}$, then $n(h) \in R$ is equivalent to $n(m_i) \in R,\ i = 1, 2$. This shows that $\mathcal{O} = R_L + R_L u$. We use the formula of Lemma 2.2.13 to calculate $d(\mathcal{O})$, and because of the fact that $d(R_L) = R$, we get $d(\mathcal{O}) = R\pi$. Since $P = \mathcal{O}u$, this implies that $n(P) = R \cdot n(u) = R\pi$. So we get that $\mathrm{d}(\mathcal{O}) = n(P) = R\pi$ and $\widetilde{\mathcal{O}}^{-1} = P$. □

Definition 3.1.6 *Let Y/X be a finite extension of division algebras with discrete valuation whose valuation rings are $A_{y.}, A_x = X \cap A_y$. Let $P_y, P_x = P_y \cap A_x$ be the prime ideals and $k_{\mathrm{y}}, \mathrm{k}_x$ the residue division algebra respectively. The residue degree* f *of Y/X is the degree $[k_y : k_x]$. The ramification index of Y/X is the integer* e *such that $A_y P_x = P_y^{\mathrm{e}}$.*

We have deduced that an unramified quadratic extension L_{ur}/K has ramification index 1 and residue degree 2. The quaternion division algebra H/K has ramification index 2 and residue degree 2.

Let F/K be a finite extension of fields of ramification index e and residue degree f. We have ef $= [F : K]$, because the order of k is finite, and $R_F/\pi R_F \cong R_F/\pi_F^e R_F$ if π_F is a uniformizer of F.

Lemma 3.1.7 *The following properties are equivalent :*

(1) f *is even*
(2) $F \supset L_{ur}$
(3) $F \otimes L_{ur}$ *is not a division algebra*
Proof : Suppose f is even. We know from Serre [1], Corollary 2, Chap 3, Section 6 that the sub extensions of F/K which are unramified over K are in one-to-one correspondence with the separable sub extensions k_F/k, where k_F is residue field of F. This implies that $F \supset L_{ur}$. This proves that (1)⇒ (2). Suppose now that $F \supset L_{ur}$.

Since $F \supset L_{ur}$ has even residue degree, f is even. This gives (2)$\Rightarrow$ (1). Now, since L_{ur} is a separable extension of degree 2 over K, we have $L_{ur} = K[X]/P(X)$, where $P(X)$ is the irreducible polynomial of degree 2 in $K[X]$ and $P(X) = (X-\alpha)(X-\alpha')$ with $\alpha, \alpha' \in L_{ur}$. Then $F \otimes L_{ur} = F \otimes K[X]/P(X) = K[X]/P(X)$, which implies that $F \otimes L_{ur}$ is not division algebra if and only if $P(X)$ has a root in F which is equivalent to $F \supset L_{ur}$. This proves (2) $\Leftrightarrow$ (3).

Let us consider now $H_F \cong \{F \otimes L_{ur}, \pi\}$. If π_F is a uniformizer of F, we can suppose that $\pi = \pi_F^{\mathrm{e}}$. From corollary 2.1.19 and the previous lemma, we get that if e or f is even then $H_F \cong \mathrm{M}(2, F)$, i.e., F neutralizes H. If not, i.e., if $[F : K]$ is not even, then $H_F \cong \{F \otimes L_{ur}, \pi_F\}$, where $F \otimes L_{ur}$ is a quadratique unramified extension of F in K_s. Then F is quaternion division algebra over F. The proof of theorem 3.1.2 is complete.

We remark the following:
All quadratic extensions of K are isomorphic to a sub-division algebra of H. So that if B is an order of a maximal subfield of H, then for it to be embedded maximally in H, it is necessary and sufficient that it be maximal.

3.2 Calculation of Hilbert symbol

Lemma 3.2.1 *If the characteristic of K is not 2, and if e is a unit of R^* which is not a square, then the set $\{1, e, \pi, e\pi\}$ forms a system of representatives in K^* of K^*/K^{*2}. Moreover L_{ur} is isomorphic to $K(\sqrt{e})$.*

Proof : Let us consider the digram
$$\begin{array}{ccccccccc} 1 & \longrightarrow & R_1^* & \longrightarrow & R^* & \longrightarrow & k^* & \longrightarrow & 1 \\ & & \downarrow 2 & & \downarrow 2 & & \downarrow 2 & & \\ & & R_1^* & \longrightarrow & R^* & \longrightarrow & k^* & & \end{array}$$
where the vertical arrows are the homomorphism $h \mapsto h^2$, and $R_1^* = \{1 + \pi \mathrm{a}, \mathrm{a} \in R\}$. We have $\left[k^* : k^{*2}\right] = 2$ and $R_1^* = R_1^{*2}$, because

$$(1 + \pi \mathrm{a})^{1/2} = 1 + \pi \mathrm{a}/2 + \ldots\ldots\ldots$$

converges in K.
From the diagram we have

$$\frac{R^*}{R_1^*} \cong k^*$$

Also from the above diagram we have an exact sequence

$$1 \longrightarrow R_1^* \longrightarrow R^{*2} \longrightarrow k^{*2} \longrightarrow 1$$

which gives

$$\frac{R^{*2}}{R_1^*} \cong k^{*2}$$

Then

$$\frac{R^*}{R^{*2}} \cong \frac{R^*/R_1^*}{R^{*2}/R_1^*} \cong \mathrm{k}^*/\mathrm{k}^{*2}$$

This implies $\left[R^* : R^{*2}\right] = \left[k^* : k^{*2}\right] = 2$. Since $K^* \cong \mathbb{Z} \times R^*$ and $K^{*2} \cong 2\mathbb{Z} \times R^{*2}$, we have $\left[K^* : K^{*2}\right] = 4$. If $e \in R^* - R^{*2}$, then $\{1, e, \pi, e\pi\}$ is a system of representatives of K^*/K^{*2}. π is also a uniformizer for $K(\sqrt{e})$, which characterizes $L_{nr} = K(\sqrt{e})$. □

Using this lemma and the properties that we have discussed in section (2.1), we will give the table for the Hilbert symbol of quaternion algebras over local fields. We put ϵ = 1 if -1 is square in K, and ϵ = -1 otherwise.

a\b	1	e	π	πe
1	1	1	1	1
e	1	1	-1	-1
π	1	-1	ϵ	-ϵ
πe	1	-1	-ϵ	ϵ

Definition 3.2.2 . *Let p be a prime number and a an integer prime to p. The Legendre symbol* $\left(\frac{a}{b}\right)$ *is defined by* :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if a is square modulo } p \\ -1 \text{ otherwise.} \end{cases}$$

From the above definition we see immediately that the Hilbert symbol $(a,p)_p$ of a, p in $\mathbb{Q}_p$ is equal to the Legendre symbol $\left(\frac{a}{p}\right)$. We can also calculate the Hilbert symbol $(a,b)_p$ in $\mathbb{Q}_p$ of two integers a, b, if $p \neq 2$, using the properties of the Hilbert symbol that we have discussed in section (2.1) :

$$(a,b)_p = \begin{cases} 1 \text{ if } p \nmid a, p \nmid b \\ \left(\frac{a}{p}\right) \text{ if } p \nmid a,\ p \parallel b \end{cases}$$

3.3 Study of M(2,K)

Let V be a vector space of dimension 2 over K. Let us fix a basis $\{e_1, e_2\}$ of V/K such that $V = Ke_1 + Ke_2$. This basis allows to identify $M_2(K)$ with the ring of endomorphisms $End(V)$ of V. If $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$, the associated endomorphism is : $v \to v.h$, where $v.h$ is the product of the row matrix (x, y) by h if $v = xe_1 + ye_2$. If L, M are two complete lattices in V. We will denote by $End(L, M)$, or $End(L)$ if $L = M$, the ring of R-endomorphisms of L in M.

Lemma 3.3.1 (1) *The maximal orders of End(V) are the rings End(L), where L varies over the set of complete lattices in V.*
(2) *The normal ideals of End(V) are the ideals End(L,M), where L , M vary over the complete lattices in V.*

Proof:(1) Let $\mathcal{O}$ be an order of $End(V)$ and M a complete lattice in V. We put

$$L = \{m \in M : m.\mathcal{O} \subset M\}$$

which is equivalent to setting

$$L = \{m \in M : f(m) \in M \text{ for all } f \in \mathcal{O}\}.$$

This implies that $\mathcal{O} \subset End(L)$ and $L \subset M$. Its enough to prove that L is a complete lattice. Since M is complete lattice. We have $M \otimes_R K = V$, whence $End(M) \otimes_R K = End(V)$ and $End(M)$ is complete full R-lattice in $End(V)$ as R-module. This implies that there exists $a \in R$ such that

$$aEnd(M) \subset \mathcal{O} \subset a^{-1}End(M).$$

We deduce that for all $f \in \mathcal{O}$, $af \in End(M)$, i.e., $af(m) \in M$ for all $m \in M$. Thus $f(am) \in M$ for all $m \in M$ which implies $am \in L$. This implies that $aM \subset L \subset M$, hence we are done.
(2) Let I be given. Then $\mathcal{O}_l(I)$ is a maximal order in $End(V)$. Choose a lattice $L \subset V$ such that $\mathcal{O}_l(I) = End(L)$ and define

$$M = R(\{i(m) : i \in I, m \in M\}).$$

Clearly M is a complete lattice. By definition $I \subset End(L, M)$ and $\mathcal{O}_r(I) \subset End(L)$, hence $\mathcal{O}_r(I) = End(L)$. Since L and M are complete lattices, we can view $End(L, M)$ as being isomorphic to $M_2(R)$. We can suppose that $L = Re_1 + Re_2$, where $\{e_1, e_2\}$ is a basis of V/K. Hence $I \subset M_2(R)$ is a sub R-module such that M(2,R) = $\mathcal{O}_l(I)$, $M_2(R)$ = $\mathcal{O}_r(I)$ and the column of all elements of I generate R^2 i.e. I is a two-sided ideal in $M_2(R)$. Let $i = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$ be such that $a \in R^*$, or $b \in R^*$, or $c \in R^*$, or $d \in R^*$. By elementary row and column operations $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are in I. So $I = M_2(R)$, whence $I = End(L, M)$. □

So we have proved that the map

$$K^* \backslash \{ (L, M) |\ L,\ M \text{ are complete lattices in } V\} \longrightarrow \{ \text{Normal ideal } I \subset End(V)\}$$

is surjective.

We will now list some classical results of the theory.

Lemma 3.3.2 . *Let $L \subset M$ two complete lattices in V.*
(1) *There exists an R-basis $\{f_1, f_2\}$ of M and an R-basis $\{f_1\pi^a, f_2\pi^b\}$ of L where a, b are uniquely determined integers.*
(2) *If $\{f_1, f_2\}$ is a R-basis of L, there exists a unique basis of M/R of the form $\{f_1\pi^n, f_1r + f_2\pi^m\}$, where n,m are integers, and r belongs to a given system U_m of representatives of R modulo $\pi^m R$.*

Proof. (1) It follows at once from invariant factor theorem.
(2) The basis of M are $\{f_1a + f_2c, f_1b + f_2d\}$ is such that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $L.A = M$. We can replace A by XA if $X \in M_2(R)^*$ and we can check without difficulty that A can be reduced to the form $A = \begin{pmatrix} \pi^n & r \\ 0 & \pi^m \end{pmatrix}$ where n, m are integers and $r \in U_m$.

We will express the results in terms of matrices:

Theorem 3.3.3 . (1) *The maximal orders of $M_2(K)$ are conjugate to $M_2(R)$.*
(2) *The two sided ideals of $M_2(R)$ form a cyclic group generated by a prime ideal $P = M_2(R)\pi$,*
(3) *The integral ideals whose left order is $M_2(R)$ are the distinct ideals*

$$M_2(R)\begin{pmatrix} \pi^n & r \\ 0 & \pi^m \end{pmatrix}, \quad \text{where } n, m \in \mathbb{N} \text{ and } r \in U_m$$

where U_m is a set of representatives for R modulo $\pi^m R$.
(4) *The number of integral ideals whose left order is $M_2(R)$ and have reduced norm $R\pi^d$ is equal to $1 + q + q^2 + ... + q^d$, where q is number of elements of residue field $k = R/\pi R$.*

Proof. Everything follows from our earlier discussion. □

Let $\mathcal{O} = End(L)$ and $\mathcal{O}' = End(M)$ be two maximal orders in $End(V)$, where L, M are two complete lattices of V. If x, y belong to K^*, we also have $End(Lx) = \mathcal{O}$ and $End(Ly) = \mathcal{O}'$. Also, we can suppose that $L \subset M$. Then there exist bases $\{f_1, f_2\}$ and $\{f_1\pi^a, f_2\pi^b\}$ of L/R and M/R, where $a,\ b \in \mathbb{N}$. The integer $|b - a|$ does not change if we replace L, M by Lx, My. It is called the distance between the two maximal orders $\mathcal{O},\ \mathcal{O}'$ and we will denote it by $d(\mathcal{O}, \mathcal{O}')$.
For example, the distance between the two maximal orders $M_2(R)$ and $\begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix}$ is equal to n.

Eichler order

Definition 3.3.4 . *An* Eichler order *of level $R\pi^n$ is an intersection of two maximal orders of distance n. We denote by $\mathcal{O}_{\underline{n}}$ the* Eichler order *of level $R\pi^n$ and equal to*

$$\mathcal{O}_{\underline{n}} = M_2(R) \cap \begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix} = \begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}.$$

An Eichler order of V is of the form $\mathcal{O} = End(L) \cap End(M)$, where L, M are two complete lattices of V which we can suppose to be of the form $L = Rf_1 + Rf_2$ and $M = Rf_1 + R\pi^n f_2$. This is also the set of endomorphisms $h \in End(L)$ such that $h.f_1 \in Rf_1 + \pi^n L$. The properties which we will prove in the following lemma justify the definition of the level of an Eichler order.

Lemma 3.3.5 . *Let $\mathcal{O}$ be an order of $M_2(K)$. The following properties are equivalent:*
(1) *There exists a unique pair of maximal orders $(\mathcal{O}_1, \mathcal{O}_2)$ such that*
$\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$.
(2) *$\mathcal{O}$ is an* Eichler order.
(3) *There exists a unique integer $n \in \mathbb{N}$ such that $\mathcal{O}$ is conjugate to*
$\mathcal{O}_{\underline{n}} = \begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}$.
(4) *$\mathcal{O}$ contains a subring conjugate to* $\begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix}$.

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are obvious. We will show (4)$\Rightarrow$ (1). Let $\mathcal{O}$ be an order containing $\begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix}$. We can check very easily check that it is of the form $\begin{pmatrix} R & \pi^a R \\ \pi^b R & R \end{pmatrix}$ with $a + b = m \geq 0$. A maximal order containing $\mathcal{O}$ is of the form $\begin{pmatrix} R & \pi^c \\ \pi^{-c} & R \end{pmatrix}$, with $a - m \leq c \leq a$. We conclude that there exist more than two maximal orders containig $\mathcal{O}$, corresponding to $c = a$ and $c = a - m$. $\square$

Let us denote by $N(\mathcal{O})$ the normalizer in $GL_2(K)$ of an Eichler order $\mathcal{O}$ of $M_2(K)$. By definition $N(\mathcal{O}) = \{x \in GL_2(K),\ x\mathcal{O}x^{-1} = \mathcal{O}\}$. Let $\mathcal{O}_1, \mathcal{O}_2$ be maximal orders containing $\mathcal{O}$. The interior automorphism associated to an element of $N(\mathcal{O})$ fixes the pair $(\mathcal{O}_1, \mathcal{O}_2)$. The study of the two-sided ideals in maximal orders has showed that the two-sided ideals of a maximal order are generated by the non zero elements of K. Then we have $N(\mathcal{O}) = K^*\mathcal{O}^*$ if $\mathcal{O}$ is maximal. If $\mathcal{O}$ is not maximal, then we can suppose that $\mathcal{O} = \mathcal{O}_{\underline{n}}$, with $n \geq 1$. Then we see that $N(\mathcal{O}_{\underline{n}})$ is generated by $K^*\mathcal{O}^*$ and $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$. We can easily check that the reduced discriminant of an Eichler order is equal to its level.

The tree of maximal order

A graph Γ consists of a set $\mathcal{V}(\Gamma)$, a set $\mathcal{E}(\Gamma)$ and two maps the first of which is

$$\begin{aligned}\mathcal{E}(\Gamma) &\longrightarrow \mathcal{V}(\Gamma) \times \mathcal{V}(\Gamma) \ , \\ \mathrm{y} &\mapsto (\mathrm{o(y)}, \mathrm{t(y)})\end{aligned}$$

where the elements of $\mathcal{V}(\Gamma)$ are called vertices of Γ , the elements of $\mathcal{E}(\Gamma)$ are called edges of Γ, o(y) is called the origin of y and t(y) is called the terminal of y. The second map is an involution of $\mathcal{E}(\Gamma)$

$$\begin{aligned}\mathcal{E}(\Gamma) &\longrightarrow \mathcal{E}(\Gamma), \\ \mathrm{y} &\longmapsto \bar{\mathrm{y}}\end{aligned}$$

such that the origin of y is the terminal of $\bar{\mathrm{y}}$ and such that $\mathrm{y} \neq \bar{\mathrm{y}}$.

A path in a graph Γ is a succession of edges $(\mathrm{y}_1, \mathrm{y}_2, \mathrm{y}_3, ..., \mathrm{y}_{\mathrm{i}+1}.....)$ such that the terminal of y_i is the origin of $\mathrm{y}_{\mathrm{i}+1}$, for all i. The given path is equivalent to a succession of vertices such that two consecutive vertices are always the origin and the end of an edge. A finite path $(\mathrm{y}_1, \mathrm{y}_2, ..., \mathrm{y}_\mathrm{n})$ is said to be of length n. It joints the origin of y_1 to the terminal of y_n. A pair $(\mathrm{y}_\mathrm{i}, \bar{\mathrm{y}}_\mathrm{i})$ in a path is called a backtracking. A finite path without backtracking such that origin of y_1 is the terminal y_n) is called a circuit. A graph is connected if there is always a path joining two distinct vertices. A tree is a connected non empty graph without circuits.

Now consider the graph whose vertices are the maximal orders of $M_2(K)$ and such that two vertices are connected by a single edge if and only if the two maximal order have distance one. This is also equivalent to considering graphs with vertices which are lattices in V up to homothety.

We will show that this graph is the homogeneous tree of order $q+1$(where q is the cardinality of the residue field of K), called the Bruhat-Tits tree of $PGL_2(K)$ denoted by $\mathcal{T}$. At first we will prove that this graph is connected. Let $\mathcal{O}'$ be a maximal order such that $d(\mathcal{O}, \mathcal{O}') = n$. Then we can take $\mathcal{O} = End(L)$ and $\mathcal{O}' = End(M)$ such that $L = Re_1 + Re_2$ and $M = Re_1 + R\pi^n e_2$ where $\{e_1, e_2\}$ is a basis of V over K. The succession of vertices $(\mathcal{O}, \mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_i, ...\mathcal{O}')$, where $\mathcal{O}_\mathrm{i} = \mathrm{End}(\mathrm{Re}_1 + \mathrm{R}\pi^\mathrm{i}\mathrm{e}_2)$, $1 \leq \mathrm{i} \leq \mathrm{n}\text{-}1$ is a path joining $\mathcal{O}$ to $\mathcal{O}'$ of length n. This shows that this graph is connected.

In order to prove that the above graph is a tree, it is sufficient to show that if $(\mathcal{O}_0, \mathcal{O}_1, ..., \mathcal{O}_n)(n > 2)$ is a sequence of vertices in a path without backtracking in the above graph, there exist R-lattices $L_i \supset L_{i+1} \supset L_i\pi$ such that $\mathcal{O}_i = End(L_\mathrm{i})$ for $0 \leq i \leq n$. The path is without backtracking if $L_i\pi \neq L_{i+2}$ for all $0 \leq i \leq n-2$. We

have

$$L_{i+1} \supset L_i\pi \supset L_{i+1}\pi$$
$$L_{i+1} \supset L_{i+2} \supset L_{i+1}\pi$$

and $L_{i+1}/L_{i+1}\pi$ is a k-vector space of dimension 2. Then $L_i\pi + L_{i+2} = L_{i+1}$, whence $L_i\pi + L_{i+j+2} = L_{i+1}$, for all $i, j \geq 0, \quad i + j + 2 \leq n$. Then $L_0\pi$ does not contain L_i for all $i \geq 1$ hence $d(\mathcal{O}_0, \mathcal{O}_i) = i$ for $1 \leq i \leq n$.

Hence we get that maximal orders form a tree. Now consider $\mathcal{O}$ a maximal order in $M_2(K)$. We can suppose that $\mathcal{O} = End(L)$, where L is a lattice in V. Each vertex $\mathcal{O}'$ of the above tree $\mathcal{T}$ is represented by a unique lattice $M \subset L$ such that $L/M \cong R/\pi^n R$, where $n = dist(\mathcal{O}, \mathcal{O}')$ and $\mathcal{O}' = End(M)$. The $R/\pi^n R$-module $L/\pi^n L$ is free of rank 2, and $M/\pi^n L$ is a direct factor of rank 1. From here we see that the vertices of the tree $\mathcal{T}$ at distance n from $\mathcal{O}$ correspond bijectively to direct factors of $L/\pi^n L$ of rank 1, that is, to points of the projective line $\mathbb{P}(L/\pi^n L) \cong \mathbb{P}^1(R/\pi^n R)$. For $n = 1$, this implies that the edges with origin $\mathcal{O}$ correspond bijectively to the points of $\mathbb{P}(L/\pi L)$, which are equal in number to the order of $\mathbb{P}^1(R/\pi R)$ i.e. $q + 1$.

For example take $K = \mathbb{Q}_p, R = \mathbb{Z}_p, \pi = p$. In this case the vertices of the Bruhat-Tits tree are the maximal $\mathbb{Z}_p$-orders in $M_2(\mathbb{Q}_p)$ i.e. complete lattices in $\mathbb{Q}_p^2$ up to homothety, two vertices being adjacent if their intersection is an Eichler order of level p. As we defined the notion of Bruhat Tits tree, $GL_2(\mathbb{Q}_p)$ acts on the vertices and edges transitively. If $v = End(L)$ is a vertex of the tree, where $L = [\mathbb{Z}_p \oplus \mathbb{Z}_p]$, then the stabilizer of $v = \mathbb{Q}_p^* GL_2(\mathbb{Z}_p)$. So we have

$$PGL_2(\mathbb{Q}_p)/GL(\mathbb{Z}_p) \cong \mathcal{V}(\mathcal{T}).$$

If $e = ([\mathbb{Z}_p \oplus \mathbb{Z}_p], [\mathbb{Z}_p \oplus p\mathbb{Z}_p])$ is an edge of the tree, then the stabilizer of the edge is equal to $\mathbb{Q}_p^* \Gamma_0(p\mathbb{Z}_p)$, where $\Gamma_0(p\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}_p) \text{ such that } c = 0 \ mod\ p\mathbb{Z}_p \right\}$. So we have

$$PGL_2(\mathbb{Q}_p)/\Gamma_0(p\mathbb{Z}_p) \cong \mathcal{E}(\mathcal{T}).$$

3.4 Maximal embedding of orders

Let H/K be a quaternion algebra, and L/K a quadratic separable algebra over K contained in H. We are given an order B of L over the ring of integers R of K. Let $\mathcal{O}$ be an Eichler order of H. We recall that B is maximally embedded in $\mathcal{O}$ if $\mathcal{O} \cap L = B$. A maximal embedding of B in $\mathcal{O}$ is an embedding f of L in H such that $\mathcal{O} \cap f(L) = f(B)$. We will determine all maximal embeddings of B in $\mathcal{O}$. It is clear that we can replace $\mathcal{O}$ by an order which is conjugate to it: if H is a division algebra then there is only one Eichler

order, and if $H = M_2(K)$ we may suppose that $\mathcal{O} = \mathcal{O}_{\underline{n}}$ for $n \geq 0$. If $\widetilde{h}$ is an interior automorphism defined by an element h of normalizer equal to the normalizer $N(\mathcal{O})$ of $\mathcal{O}$ in H^*, it is clear that $\widetilde{h}f$ is also a maximal embedding of B in $\mathcal{O}$. We will show that the number of maximal embeddings of B in $\mathcal{O}$, modulo interior automorphisms defined by a group G, $\mathcal{O}^* \subset G \subset N(\mathcal{O})$, is finite. We can calculate this number explicitly. The result of the calculation is rather complicated if $\mathcal{O}$ is a level $R\pi^n$ with $n \geq 2$. Since we will not be using the result for $n \geq 2$. We will just prove the complete result in the case $n \leq 1$. However, the proofs are given in the general case.

Definition 3.4.1 *Let L/K be a quadratic separable extension of K. Let π be a uniformizer of K. We define the Artin symbol $\left(\frac{L}{\pi}\right)$*

$$\left(\frac{L}{\pi}\right) = \begin{cases} -1 & \text{if } L/K \text{ is non ramified,} \\ 0 & \text{if } L/K \text{ is ramified} \end{cases}$$

Let B be an order in a separable quadratic extension L/K. We define the Eichler symbol to be $\left(\frac{B}{\pi}\right)$ equal to the Artin symbol $\left(\frac{L}{\pi}\right)$ if B is a maximal order, and 1 otherwise.

Now we will suppose that H is division algebra.

Theorem 3.4.2 *Let L/K be a separable quadratic extension of K and let B be an order in L. Let $\mathcal{O}$ be a maximal order in H. If B is a maximal order, the number of maximal embeddings of B in $\mathcal{O}$ modulo the interior automorphisms defined by a group* G *is equal to :*

$$\begin{aligned} &1 && \text{if } \ G = N(\mathcal{O}) \\ &1 - \left(\frac{L}{\pi}\right) && \text{if } \ G = \mathcal{O}^*. \end{aligned}$$

If B is not maximal, then it is not maximally embedded in $\mathcal{O}$.

Proof: Let $f : L \to H$ be an embedding of L in H. As we seen in section (3.1), f is maximal embedding of ring of integers R_L of L in a maximal order $\mathcal{O}$ of H. Thus, if B is not maximal, then it is not maximally embedded in $\mathcal{O}$. After Chap II, page no. 49, the number of maximal embeddings of R_L in $\mathcal{O}$ modulo G is equal to number of conjugacy classes in H of an element $m \in L,\ m \notin K$, modulo $\widetilde{G}$. As $N(\mathcal{O}) = H^*$, we have $m(L, N(\mathcal{O})) = 1$. Also $\widetilde{\mathcal{O}^*} \cup \widetilde{\mathcal{O}^*}\widetilde{u} = \widetilde{H^*}$ if $u \in H$ is an element of reduced norm π, we have $m(L, \mathcal{O}^*) = 1$ if we can choose $u \in L$, i.e. if L/K is ramified, and $m(L,\ \mathcal{O}^*)$ =2 if not, i.e. if L/K is not ramified. $\square$

Now suppose that $H = M_2(K)$. The analogous result is then:

Theorem 3.4.3 . *Let L/K be a seprable quadratic extension and let B be an order of L. Let $\mathcal{O}$ be a maximal order of $M_2(K)$. Then we can embed B maximally in $\mathcal{O}$ and the number of maximal embeddings of B in $\mathcal{O}$ modulo interior automorphisms defined by $\mathcal{O}^*$ is equal to 1. Let $\mathcal{O}'$ be an Eichler order of level $R\pi$ of $M_2(K)$. The number of maximal embeddings of B in $\mathcal{O}'$ modulo interior automorphisms associated to G is equal to:*

$$\begin{cases} 0 \text{ or } 1 & \text{if } G = \mathrm{N}(\mathcal{O}') \\ 1 + \left(\frac{B}{\pi}\right) & \text{if } G = \mathcal{O}'^* \end{cases} .$$

This theorem shows that B is not embedded maximally in $\mathcal{O}'$ if and only if B is maximal and L/K is not ramified. The proof of this theorem will be given following ([H1], Hijikata). We will study in general maximal embeddings of B in an Eichler order $\mathcal{O}_{\underline{n}}$.

Definition 3.4.4 . *If B is an order in L, there exists $s \in \mathbb{N}$ such that $B = R + Rb\pi^s$, where $R + Rb$ is a maximal order of L. The integer s characterizes B, and we will write $B = B_s$. The ideal $R\pi^s$ is called the conductor of B. If $u \leq s$, we have $B_s \subseteq B_u$. The ideal $R\pi^{s-u}$ is called the relative conductor of B_s in B_u.*

Let f be an embedding of L in $M_2(K)$ and let $g \in B,\ g \notin R$. We let $p(X) = X^2 - tX + m$ be minimal polynomial of g over K, $R\pi^r$ the relative conductor of $R[g]$ in B and set $f(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Lemma 3.4.5 . *Let $\mathcal{O}_{\underline{n}}, n \geq 0$ be an Eichler order in $M_2(K)$. The following properties are equivalent.*
(1) *f is maximal embedding of B in $\mathcal{O}_{\underline{n}}$.*
(2) *r is the greatest integer i such that $(R + f(g)) \cap \pi^i \mathcal{O}_{\underline{n}}$ is non empty.*
(3) *The elements $\pi^{-r}b, \pi^{-r}(a-d), \pi^{-r-n}c$ are relatively prime integers.*
(4) *The congruence $p(x) \equiv 0$ mod $R\pi^{n+2r}$ admits a solution x in R satisfying: $t \equiv 2x$ mod $R\pi^r$, and there exists $u \in N(\mathcal{O}_{\underline{n}})$ such that $uf(g)u^{-1} = \begin{pmatrix} x & \pi^r \\ -p(x) & t - x \end{pmatrix}$.*

Proof: We will denote by $f_x(g)$ the matrix $uf(g)u^{-1}$ defined above. The equivalence of properties (1), (2), (3) is easy and (4) $\Rightarrow$ (3) is obvious. Now we will show that (3) $\Rightarrow$ (4). If $\pi^{-r}b$ is a unit, put $u = \begin{pmatrix} 1 & 0 \\ 0 & \pi^{-r}b \end{pmatrix}$. Then $uf(g)u^{-1} = f_x(g)$, where x is a solution in R of the congruence $p(x) \equiv 0$ mod $R\pi^{n+2r}$. It is thus a question of being reduced to the case where $\pi^{-r}b$ is a unit. If $\pi^{-r-n}c$ is a unit, we conjugate $f(g)$ by $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$. If not, we conjugate $f(g)$ by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which replaces b by $-(a+c)+b+d$ and this is the product of a unit by π^r. $\square$

Now we have a criterion of existence of a maximal embedding of B in $\mathcal{O}_{\underline{n}}$. We will now compute these embeddings. We write $E = \{x \in R,\ t \equiv 2x \bmod R\pi^r,\ p(x) \equiv 0 \bmod R\pi^{n+2r}\}$. This is the set is introduced in (4) of the previous lemma.

Lemma 3.4.6 . *Let f, f' be two maximal embeddings of B in $\mathcal{O}_{\underline{n}}$. Let $n_f = \widetilde{h}_n f$, whence $\widetilde{h}_n$ is the interior automorphism induced by $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$.*
(1) *f is equivalent to f' modulo N($\mathcal{O}_{\underline{n}}$) if and only if f is equivalent either to f' or to $n_{f'}$ modulo $\mathcal{O}^*_{\underline{n}}$. If $n = 0$, the equivalence modulo N($\mathcal{O}_{\underline{0}}$) coincides with the equivalence modulo $\mathcal{O}^*_{\underline{0}}$.*
(2) *Let $x, x' \in E$ and $f_x, f_{x'}$ defined as in the previous lemma. Then f_x is equivalent to $f_{x'}$ modulo $\mathcal{O}^*_{\underline{n}}$ if and only if $x \equiv x' \bmod \pi^{r+n}$.*
(3) *If $\pi^{-2r}(t^2-4n)$ is a unit in R (resp. it is not unit in R), then f_x is equivalent to $n_{f_{x'}}$ if and only if $x \equiv t-x' \bmod \pi^{r+n}$ (resp. $x \equiv t-x' \bmod \pi^{r+n}$ and $p(x') \not\equiv 0 \bmod \pi^{n+2r+1}$).*

Proof: (1) is obvious. (2): If $x \equiv x' \bmod \pi^{r+n}$, put $a = \pi^{-r}(x-x')$ and $u = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$. Then $u \in \mathcal{O}^*_{\underline{n}}$ and $uf_x(g)u^{-1} = \begin{pmatrix} x' & \pi^r \\ * & * \end{pmatrix} = f_{x'}(g)$. Conversely suppose that f_x is equivalent to $f_{x'}$ modulo $\mathcal{O}^*_{\underline{n}}$. As all elements of $\mathcal{O}^*_{\underline{n}}$ are upper triangular modulo π^n, if $u \in \mathcal{O}^*_{\underline{n}}$, $\pi^{-r}(uf_x(g)u^{-1} - x)$ has the same diagonal modulo π^n than $\pi^{-r}(f_x(g) - x)$, whence $x \equiv x' \bmod \pi^{r+n}$.
(3) If $\pi^{-n-2r}f(x')$ is a unit, $n_{f_{x'}}(g)$ satisfies the condition (3) of the previous lemma. Hence it is equivalent to $\begin{pmatrix} t-x' & \pi^r \\ -\pi^{-r}f(x') & x' \end{pmatrix}$. Also, after (2), f_x is equivalent to $n_{f_{x'}}$ modulo $\mathcal{O}^*_{\underline{n}}$ if and only if $x \equiv t-x' \bmod \pi^{r+n}$. If $\pi^{-n-2r}f(x')$ is not a unit , for $b \in R$, let $u = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ and $un_{f_x}(g)u^{-1} = (x_{ij})$. Modulo π^{r+n}, $x_{11} = t-x'$ and $x_{12} = b(2x'-t) - \pi^{-n+r}f(x')$. Thus, if $\pi^{-r}(2x'-t)$ is a unit, or equivalently if $\pi^{-2r}(t^2-4n)$ is a unit, we can choose b so that $\pi^{-r}x_{12}$ is a unit and the new (x_{ij}) is equivalent to $\begin{pmatrix} t-x' & \pi^r \\ -\pi^{-r}f(x') & x' \end{pmatrix}$ modulo $\mathcal{O}^*_{\underline{n}}$. Finally suppose that $\pi^{-n-2r}f(x')$ and $\pi^{-2r}(t^2-4n)$ are not units, then if we note that $\mathcal{O}^*_{\underline{n}}$ is generated modulo π^n by diagonal matrices and matrix of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, we see that, for all $u \in \mathcal{O}^*_{\underline{n}}$, if $un_{f_{x'}}(g)u^{-1} = (x_{ij})$, then $\pi^{-r}x_{12}$ is never a unit. Hence $n_{f_{x'}}$ can not be equivalent to f_x modulo $\mathcal{O}^*_{\underline{n}}$.

We deduce from the preceding two lemmas the following proposition which makes it possible to count the number of maximal embeddings of B_s in $\mathcal{O}_{\underline{n}}$ modulo the group of interior automorphisms induced by $G = \mathrm{N}(\mathcal{O}_{\underline{n}})$ or $\mathcal{O}^*_{\underline{n}}$. The theorem 3.4.3 is an immediate corollary.

Proposition 3.4.7 (1) *B is embedded maximally in $\mathcal{O}_{\underline{n}}$ if and only if E is not empty.*
(2) *The number of maximal embedding of B in $\mathcal{O}_{\underline{n}}$ modulo the interior automorphism*

induced by $\mathcal{O}^*_{\underline{n}}$ is equal to the cardinal of the image of E in $R/\pi^{2r+n}R$ if $\mathcal{O}_{\underline{n}} = \mathcal{O}_{\underline{0}}$ is maximal, or if $\pi^{-r}(t^2-4m)$ is unit. Otherwise, this number is the sum of the preceding cardinal and the cardinal of the image of $F = \{x \in E,\ \ p(x) \equiv 0 mod\ R\pi^{n+2r+1}\}$ in $R/\pi^{2r+n}R$.

Proof of theorem 3.4.3. We suppose that $\mathcal{O} = \mathcal{O}_{\underline{0}}$ is a maximal order. As $N(\mathcal{O}) = K^*\mathcal{O}^*$ the number of maximal embedding modulo interior automorphism induced by a group $G,\ \mathcal{O}^* \subset G \subset N(\mathcal{O})$, does not depend on G. This number is not zero because E is not empty. We deduce from (2) that this number is equal to 1. We suppsoe that $\mathcal{O} = \mathcal{O}_{\underline{1}}$. We now recall that $B = R + Rb\pi^s$, where $R + Rb$ is a maximal order in L. If B is not maximal, $s \geq 1$, then $x = 0$ is solution of the congruence $p(x) = x^2 - t(b)\pi^s x + \pi^{2s} n(b) = 0 \mod\ R\pi^2$. As the discriminant of the polynomial is not a unit, an application of the proposition (with $r = 0$) shows that there exist two maximal embeddings of B in $\mathcal{O}$ modulo interior automorphisms induced by $\mathcal{O}^*$. If B is a maximal order, and if L/K is not ramified, then $E = \emptyset$ because the residue field of L and and that of K are distinct. If L/K is ramified, then $n(b) \in R^*\pi$ and the discriminant of $p(x)$ belongs to $R\pi$. Modulo πR, the set E is reduced to only one element $\{0\}$ and $F = \emptyset$.
The theorem is proved if $G = \mathcal{O}^*$. To obtain it when $G = N(\mathcal{O})$, we use the fact that $N(\mathcal{O})$ is the group generated by $\mathcal{O}^*$ and $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$. The matrices $\begin{pmatrix} 0 & 1 \\ -n & t \end{pmatrix}$ and $\begin{pmatrix} t & -\pi^{-1}n \\ \pi & 0 \end{pmatrix}$ are conjugates modulo $N(\mathcal{O})$. This implies that the number of maximal embeddings of B in $\mathcal{O}$ modulo interior automorphisms of $N(\mathcal{O})$ is equal to 0 or 1.

3.5 Zeta Function

In this section we present some basic results which we use in chapter IV: it includs no theorem but definitions and preparatory calculations which will facilitate proofs in the next chapters, which use adelic techniques. We use the definition of local zeta function as defined in ([W1], Weil), the normalisation of measures and certain calculations of volume and integrals that we will need later.

Let X be a local field K or a quaternion algebra H/K which does not contain $\mathbb{R}$. Let $\mathcal{B}$ be an order in X which contains the valuation ring R of K. The norm of an integral ideal I of $\mathcal{B}$ is equal to $N_X(I) = \mathrm{Card}(\mathcal{B}/I)$.
By multiplicativity, we extend the definition of norm to fractional ideals. With this definition :

$$\begin{aligned} N_K(R\pi) &= \mathrm{Card}(R/R\pi) = \mathrm{Card}(k) = q \\ N_H(P) &= \begin{cases} \mathrm{Card}(\mathcal{O}/\mathcal{O}u) = q^2, & \text{if } H \text{ is division algebra,} \\ \mathrm{Card}(\mathcal{O}/\mathcal{O}\pi) = q^4, & \text{if } H \cong M_2(K), \end{cases} \end{aligned}$$

where P is a two-sided integral maximal ideal of a maximal order $\mathcal{O}$ of H. The norm of a principal ideal $\mathcal{O}h$ is natuarally equal to the norm of the ideal $h\mathcal{O}$. After the Corollary 3.1.5 and Theorem 3.3.3, we have :

Lemma 3.5.1 . *The number of left (or right) integral ideals of a maximal order in H of norm q^n , $n \geq 0$, is equal to*

$$\begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}, \text{if } H \text{ is division algebra}$$

$$1 + q + q^2 + ... + q^n, \quad \text{if } H \cong M_2(K).$$

Definition 3.5.2 *The zeta function of $X = H$ or K is the following function of the complex variable*

$$\zeta_X(s) = \sum_{I \subset \mathcal{B}} N(I)^{-s}$$

where the sum extends over the left (or right) integral ideals I of maximal orders $\mathcal{B}$ of X.

The previous lemma allows us to calculate explicitely $\zeta_H(s)$ in terms of $\zeta_K(s)$. We have

$$\begin{aligned} \zeta_K(s) &= \sum_{n \geq 0} q^{-ns} = (1 - q^{-s})^{-1} \\ \zeta_H(s) &= \sum_{n \geq 0} q^{-2ns} = \zeta_K(2s), \quad \text{if } H \text{ is a division algebra} \\ \zeta_H(2s) &= \sum_{n \geq 0} \sum_{0 \leq d \leq n} q^{d-2ns} = \sum_{d \geq 0} \sum_{d' \geq 0} q^{d-2(d+d')s} = \zeta_K(2s)\zeta_K(2s-1), \end{aligned}$$

if $H \cong M_2(K)$.

There exists a more general definition of the zeta function which is valid when $X \supset \mathbb{R}$. The idea for these zeta functions comes from Tate [1], in the case of local fields. Their generalisation to simple central algebras is due to Godement [1] and Jacquet-Godement [1]. The starting point is to notice that the classical zeta-function can also be defined as integral on the locally compact group X^* of the characteristic function of a maximal order multiplied by $\chi(x) = N(x)^{-s}$, for a certain Haar measure. This definition then generalises to define the zeta function of a Schwartz-Bruhat function, and a quasi - character, and extends naturally to the archimedean case. This is what we will do. We will follow the book of Weil[1].

Definition 3.5.3 . *Let G be a locally compact group and let dg be a Haar measure on G. For any isomorphism a of G let $d(ag)$ the Haar measure on G defined by $\int_G f(g)dg = \int_G f(ag)d(ag)$, for all measurable functions on G. The ratio of these two measures, $\|a\| = d(ag)/dg$, is called the modulus of the isomorphism a.*

We check without difficulties that :
(1) $\text{vol}(aZ) = \|a\|\text{vol}(Z)$, for all measurable sets, $Z \subset G$,
(2)$\|a\|\,\|b\| = \|ab\|$, where $a,\ b$ are two isomorphisms of G.
Note that (2) shows that the modulus does not depend on the measure used in its definition.

Definition 3.5.4 *The modulus of an element $x \in X^*$, denoted by $\|x\|_X$, is the modulus in the above definition of the isomorphism induced by left(or right) multiplication by x on $X = H$ or $X = K$. The norm $N_X(x)$ of x is the inverse of the modulus of x.*

In $\mathbb{R}$ or $\mathbb{C}$ we will denote by $|x|$ the usual modulus of an element x. We check immediately the following properties: if $x \in X^*$,
$\|x\|_{\mathbb{R}} = |x|$, $\|x\|_{\mathbb{C}} = |x|^2$, $\|x\|_X = N_X(x)^{-1} = N_X(\mathcal{B}x)^{-1}$ if $X \not\supset \mathbb{R}$.
Now we will normalise the measure on X, X^*.

Definition 3.5.5 . *If $X \not\supset \mathbb{R}$, we denote by dx or dx_X the additive Haar measure such that the volume of a maximal order $\mathcal{B}$ is equal to 1. We denote by dx^* or dx_X^* the multiplicative Haar measure $(1-q^{-1})^{-1}\|x\|_X^{-1} dx_X$.*

Lemma 3.5.6 . *For the multiplicative measure dx^*, the volume of the group of units $\mathcal{B}^*$ of a maximal order $\mathcal{B}$ of X is given by:*
$\mathrm{vol}(R^*) = 1$,
$\mathrm{vol}(\mathcal{O}^*) = (1-q^{-1})^{-1}(1-q^{-2})$, *where $\mathcal{O}$ is the ring of integers of a division quaternion algebra H/K,*
$\mathrm{vol}(GL_2(R)) = 1 - q^{-2}$.

Proof: Suppose that X is a division algebra. Let $\mathfrak{m}$ be a maximal ideal of $\mathcal{B}$. For the additive measure dx, we have the equality

$$\begin{aligned}\mathrm{vol}(\mathcal{B}^*) &= \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(\mathfrak{m}) = 1 - \|x\| = 1 - N(x)^{-1} = 1 - \mathrm{Card}(\mathcal{B}/\mathfrak{m}) \\ &= \begin{cases} 1-q^{-1} & \text{if } X = K \\ 1-q^{-2} & \text{if } X = H. \end{cases}\end{aligned}$$

The volume of $\mathcal{B}^*$ for the multiplicative measure dx^* is equal to volume of $\mathcal{B}^*$ for the additive measure $(1-q^{-1})^{-1}dx$. We easily deduced the lemma, if X is a division algebra.
Now we assume that $X = M_2(K)$.
The canonical map $:R \to k$ induces a surjection from $GL_2(R) \to GL_2(k)$ whose kernel Z is the of the group of matrices congruent to the identity modulo the ideal $R\pi$. The number of elements of $GL_2(k)$ is equal to the cardinality of a basis of a k-vector space of dimension 2, which is $(q^2-1)(q^2-q)$. The volume of Z for the measure dx is $\mathrm{vol}(R\pi)^4 = q^{-4}$. The volume of $GL_2(R)$ for dx^* is then equal to the product
$q^{-4}(q^2-1)(q^2-q)(1-q^{-1})^{-1} = 1-q^{-2}$. □

Lemma 3.5.7 . *We have:*

$$Z_X(s) = \int_{\mathcal{B}} N(x)^{-s} dx^* = \begin{cases} \zeta_K(s) & , \quad \text{if} \quad X = K, \\ \frac{\zeta_H(s)}{\zeta_K(2)} \cdot \begin{cases} (1-q^{-1})^{-1} & , \quad \text{if } X = H \text{ is a division algebra,} \\ 1 & , \quad \text{if } X = M_2(K). \end{cases} \end{cases}$$

Proof: The number of elements of $\mathcal{B}$ modulo $\mathcal{B}^*$, of norm q^n $(n \geq 0)$ is the number of integral ideal of $\mathcal{B}$ of norm q^n. The integral is then equal to $\zeta_X(s)\mathrm{vol}(\mathcal{B}^*)$. □

Definition 3.5.8 *Let dx be the Lebesgue measure on $\mathbb{R}$. Let $X \supset \mathbb{R}$ and (e_i) be an $\mathbb{R}$-basis of X. For $x = \sum x_i e_i \in X$, we denote by $T_X(x)$ the usual trace of the $\mathbb{R}$-endomorphism of X given by left (or right) multiplication by x. We denote by dx_X the additive Haar measure on X such that*

$$dx_X = |\det(T_X(e_i e_j))|^{1/2} \prod dx_i.$$

We denote by dx_X^* the multiplicative Haar measure $\|x\|_X^{-1} dx_X$.

We check that the above definition is explicitely given by :
(1) $dx_{\mathbb{C}} = 2dx_1 dx_2 \quad$, if $x = x_1 + ix_2 \quad$, $x_i \in \mathbb{R}$,
(2) $dx_H = 4dx_1 ... dx_4 \quad$, if $x = x_1 + ix_2 + jx_3 + ijx_4 \quad$, $x_i \in \mathbb{R}$,
(3) $dx_{M_2(K)} = \prod dx_i \quad$, if $x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \in M_2(K)$, $K = \mathbb{R}$ or $\mathbb{C}$.

We denote by x^t the transpose of the matrix x. In an explicit way, the real number $T_X(x^t \bar{x})$ is equal to

$$\begin{cases} x^2 & , \text{ if } X = \mathbb{R}, \\ 2x\bar{x} & , \text{ if } X = \mathbb{C}, \\ 2n(x) & , \text{ if } X = H, \\ \sum x_i^2 & , \text{ if } X = M_2(\mathbb{R}), \\ 2\sum x_i \bar{x_i} & , \text{ if } X = M_2(\mathbb{C}), \end{cases}$$

We put:

$$Z_X(s) = \int_{X^*} \exp(-\pi T_X(x^t \bar{x})) N(x)^{-s} dx$$

Lemma 3.5.9 . *We have*

$$\begin{aligned} Z_{\mathbb{R}}(s) &= (*)\pi^{-s/2}\Gamma(s/2) \\ Z_{\mathbb{C}}(s) &= (*)(2\pi)^{-s}\Gamma(s) \\ Z_H(s/2) &= (*)Z_K(s)Z_K(s-1) \cdot \begin{cases} s-1 & , \text{ if } H \text{ is division algebra,} \\ 1 & , \text{ if } H = M_2(K), \end{cases} \end{aligned}$$

where "(*)" is a constant which is independent of s.

Proof: For $X = \mathbb{R}$,

$$\begin{aligned} Z_{\mathbb{R}}(s) &= \int_{\mathbb{R}^*} e^{-\pi x^2} \|x\|_{\mathbb{R}}^s \|x\|_{\mathbb{R}}^{-1} dx \\ &= 2\int_0^\infty e^{-\pi x^2} x^{s-1} dx \\ &= 2\pi^{-1/2-s/2} \int_0^\infty e^{-t} t^{s/2-1} dt \qquad (\text{put } t = -\pi x^2) \\ &= (*)\pi^{-s/2}\Gamma(s/2). \end{aligned}$$

Similarly for $X = \mathbb{C}$ and $X = H$. $\square$

Definition 3.5.10 . *The Schwartz- Bruhat space of X is*
$S = \begin{cases} \text{The functions which are rapidly decreasing infinitely diffrentiable if } X \supset \mathbb{R} \\ \text{The functions which have compact support and are locally constant if } X \not\supset \mathbb{R} \end{cases}$.

A quasi-character of a locally compact group G is a continuous homomorphism of G in $\mathbb{C}$. If it takes values of modulus 1, we call it a character.

For example, the quasi-charcters of a compact group are always characters.
An example of a quasi-character on X is $x \mapsto N(x)^s$. It is a character if and only if s is a purely imaginary number. The quasi-characters of H^* are trivial on groups of commutators. As we know the commutator subgroup of H^* is equal to the group H^1 of quaternions of reduced norm 1. All quasi-characters of H^* are of the form

$$\chi_H = \chi_K \circ n$$

where χ_K is a quasi-character of K.

Definition 3.5.11 *: The zeta function associated to a function f in the Schwartz-Bruhat space and a quasi-charcter χ is the integral :*

$$Z_X(f, \chi) = \int_{X^*} f(x)\chi(x)dx^*.$$

The canonical function Φ of X is :
$\Phi = \begin{cases} \text{The characteristic function of a maximal order if } X \not\supset \mathbb{R} \\ \exp(-\pi T_X(x^t \bar{x})) \qquad \text{if } X \supset \mathbb{R} \end{cases}$.
Then the functions $Z_X(s)$ as defined earlier agree with $Z_X(\Phi, N(x)^{-s})$.

We will end this section by defining Tamagawa measures, a concept which is more or less equivalent to that of *discriminant*. We choose on X a quasi-character ψ_X, called a canonical character, defined by the conditions :
- $\psi_{\mathbb{R}}(x) = \exp(-2i\pi x)$
- $\psi_{K'}(x)$ is trivial on the ring of integers $R_{K'} = R'$ and $R_{K'}$ is self dual with respect to $\psi_{K'}$ if K' is a non archimedean prime subfield of K.
- $\psi_K(x) = \psi_{K'} \circ T_X(x)$ if K' is the prime subfield of K.

The topological isomorphism $x \mapsto (y \mapsto \psi_X(xy))$ between X and its dual allows us to write the Fourier tranformation :

$$f^*(x) = \int_X f(y)\psi_X(xy)dy$$

where $dy = d_X y$ is the additive measure on X normalized as above. The dual measure is the measure d^*y such that the inversion formula holds

$$f(x) = \int_X f^*(y)\psi_X(-yx)d^*y.$$

Definition 3.5.12 . *The Tamagawa measure on X is the Haar additive measure on X which is self dual for the Fourier transformation associated to the canonical character ψ_X.*

Lemma 3.5.13 . *The Tamagawa measure on X is the measure dx if $K' = \mathbb{R}$. If $K' \neq \mathbb{R}$, the Tamagawa measure is the measure $D_X^{-1/2}dx$, where D_X is the discriminant of X i.e.*

$$D_X = \|\det(T_X(e_i e_j))\|_K^{-1}$$

where (e_i) is an R'- basis of a maximal order in X.

Proof: If $K' = \mathbb{R}$, the global definition of dx shows us that it is self dual(i.e. equal to its dual measure) for ψ_X. Suppose then $K' \neq \mathbb{R}$ and let us choose a maximal R'-order which we denote by B. We denote by Ψ its characteristic function. The Fourier transform of Φ is the characteristic function of the dual B^* of B with respect to the trace. In the same way, we see that $B^{**} = \mathrm{vol}(B^*)\Phi$ (because $B^{**} = B$). The self dual measure of X is then $\mathrm{vol}(B^*)^{-1/2}dx$. If (e_i) is an R'- basis of B, denote by (e_i^*) its dual basis so that $T_X(e_i e_j^*) = 0$, if $i \neq j$ and $T_X(e_i e_j^*) = 1$, if $i = j$. The dual basis is an R'-basis of B^*. If $e_j^* = \sum_i a_{ji} e_i$, let A be the matrix (a_{ij}). We have $\mathrm{vol}(B^*) = \|\det(A)\|_{K'} \mathrm{vol}(B) = \det(A)$ for the measure dx. In addition, it is clear that $\mathrm{vol}(B) = \|\det T_X(e_i e_j)\|_{K'}^{-1}$. We have consequently showed that the dual measure of dx is $D_X^{-1/2}dx$. □

Lemma 3.5.14 *The discriminants of H and K are related by the relation*

$$D_H = D_K^4 N_K(d(\mathcal{O}))^2$$

where $d(\mathcal{O})$ is the reduced discriminant of maximal R'-order $\mathcal{O}$ in H.

Proof: With the notation of Chapter II, we have $\mathcal{O} = \{h \in H,\ \ t(h\mathcal{O}) \subset R^*\}$, from which we easily deduce that

$$\mathcal{O}^* = \begin{cases} R^* & \text{if } H = M_2(K) \\ R^* u^{-1} & \text{if } H \text{ is a division algebra.} \end{cases}$$

We have $D_H = \mathrm{vol}(\mathcal{O}^*) = N_H(\mathcal{O}^{*-1}) = N_K n^2(R^{*-1}) N_K(d(\mathcal{O}))^2 = D_K^4 N_K(d(\mathcal{O}))^2$. □

Remarks. If $K' \neq \mathbb{R}$, the modulus group $\|X^*\|$ is a discrete group. It provides a measure which assigns to each element its own value (modulus).
In all other cases, the discrete groups which we will consider provide us with a discrete measure which assigns to each element the value 1.

Compatible measures. Let Y, Z, T be topological groups provided with Haar measures dy, dz, dt and let the following be an exact sequence with continuous functions :

$$1 \longrightarrow Y \xrightarrow{i} Z \xrightarrow{j} T \longrightarrow 1\,.$$

We say that the measures dy, dz, dt are compatibles with this sequence, or still that $dz = dydt$, $dy = dz/dt$, or $dt = dz/dy$, if for all the functions f such that the integrals below make sense, we have the equality :

$$\int_Z f(z)dz = \int_T dt \int_Y f(i(y)z)dy, \quad \text{with } t = j(z).$$

This allows us to define, whenever we have two measures and an exact sequence, a third measure by compatibility. Such a construction will be frequently used. But it is necessaary to be careful : the third measure depends on the exact sequence. Let us give an example. Let X_1 be the kernel of the modulus and let X^1 be the kernel of the reduced norm. One naturally provides them with induced measures from the measures normalized above, and the exact sequence that their definition suggests. We denote the measures by dx_1 or dx^1. These measures are different, although the sets X_1 and X^1 can be equal. For an explicit example on the calculation of volumes, see the exercises of chapterII of [Vi 80]. If $K' \neq \mathbb{R}$, we remark that dx_1 is the restriction to X_1 of the measure dx^*.

4 Quaternion algebras over global fields

In this chapter we will give the fundamental results of the theory of quaternion algebras over global fields. In particular, we will state : the classification theorem, the strong approximation theorem for the quaternions of reduced norm 1, calculations of Tamagawa numbers, trace formulas. We will obtain them by analytical methods.
We will start with the basic concept of Adeles. We will follow the book ([W1], Weil)

4.1 Adeles

A global field K/K' is a finite extensions of a field K' called its ground field, which is equal to

- $\mathbb{Q}$ the field of rational numbers ,
- $\mathbb{F}_q(T)$ the field of rationals in one variable T with coefficients in finite fields $\mathbb{F}_q$, where q is a power of prime number. If $\mathbb{Q} \subset K$, we say that K is number field. if $\mathbb{F}_p(T) \subset K$, we say that K is function field.

Let us consider the set of embeddings $i : K \to L$ of the local field L such that the image $i(K)$ of K is dense in L. Two such embeddings $i,\ i'$ are said to be *equivalent* if there exists an isomorphism $f : L \to L'$ of local fields such that $i' = f \circ i$. An equivalence class is called a place of K. It is usually denoted by v, and we denote $i_v : K \to K_v$ a dense embedding of K in a local field K_v represented by a place v. We distinguish archimedean places or infinite places as being those such that K contains a field isomorphic to $\mathbb{R}$. The other places are called finite places.
Notations. We fix the representatives $i_v : K \to K_v$ of places v of K. Then we view K as being contained in each K_v. We denote by V the set of all places, ∞ is the set of infinite places, and P is a set of finite places. K_v is a local field as defined in chapter III with an index v. If S is a finite set of places of K, such that $\infty \in S$, we write

$$R_{(S)} = \bigcap_{v \notin S} (R_v \cap K)$$

the ring of elements of K which are integral at the places not belonging to S. It is a Dedekind ring. We write, if K is number field, $R_\infty = R$. It is the ring of integers of K. If $v \in P$, the number of elements of in the residue field k_v is denoted by N_v. We call it the norm of v.

Examples: Places of $\mathbb{Q}$: Infinite places, represented by natural embeddings of $\mathbb{Q}$ in the field of real numbers; the finite places represented by the natural embeddings of $\mathbb{Q}$ in the p-adic fields $\mathbb{Q}_p$ for all prime numbers p.

Places of $\mathbb{F}_p(T)$: They are all finite places, associated to irreducible polynomials and to T^{-1}. The set of elements of K whose image belongs to R_v, for all $v \in V$, is $\mathbb{F}_p$, non associated to T^{-1} is equal to $\mathbb{F}_p[T]$. The irreducible polynomials are bijection with the prime ideals of $\mathbb{F}_p[T]$

Definition 4.1.1 *Let H/K be a quaternion algebra. A place v of K ramifies in H if the tensor product $H_v = H \otimes K_v$ is a division algebra.*

For example if the characterstic of K is other than 2, and if $H = \{a, b\}$(as defined in Chapter II), a place v of K is ramified in $H = \{a, b\}$ if and only if the Hilbert symbol $(a, b)_v$ of $a,\ b$ in K_v is equal to -1. This allows us to obtain the places that ramify in $H = \{a,\ b\}$.
It will be pointed out that the definition of ramification is quite natural. The ramified places of K in H are places v of K such that H_v/K_v is ramified.

Lemma 4.1.2 . *The number of places of K that ramify in H is finite.*

Proof: Let $(e_i),\ 1 \leq i \leq 4$ be a basis of H/K. For almost all finite places v, the lattice generated by (e_i) over R_v is an order of reduced discriminant $d_v = R_v$ (From lemma 2.2.13). From the discussion in Chapter 3, section 1, we get that $H_v = \mathrm{M}_2(K_v)$. Hence the lemma is proved.
Also we can prove this lemma using the well known fact that there does not exist a quaternion division algebra over finite field.

Definition 4.1.3 *The product of the finite places of K which ramify in H is called the reduced discriminant of H/K. If K is a number field, it is identified with an integral ideal of the ring of integers of K. We denote it by d or by d_H. It is an element of the free group generated by p.*

The set of places of K which ramify in H plays a fundamental role in the classification problem. It is denoted by $\mathrm{Ram}(H)$. We will denote sometimes $\mathrm{Ram}_\infty H$, $(\mathrm{Ram}_f H)$ the set of infinite places (finite places) which ramify in H.

Let us consider the situation where for every place $v \in V$ we are given a locally compact group G_v, and for every place v not belonging to a finite set $S \subset V$, an open compact sub-group C_v of G_v.

Definition 4.1.4 . *The restricted product G_A of the the locally compact groups G_v with respect to the compact subgroups C_v is defined by*

$$G_A = \left\{ x = (x_v) \in \prod_{v \in V} G_v,\ x_v \in C_v \text{ for almost all places } v \notin S \right\}$$

To define a topology on G it is enough to give fundamental neighbourhoods of unity given by the sets $\prod_{v\in V} U_v$, $U_v = C_v$, for almost all $v \notin S$, and U_v is an open neighbourhood of unity in G_v. For more details to these these groups see Bourbaki[3]. There it is shown that G_A is a locally compact topological group which does not depend on S.

The above situation arises if G is an algebraic group over K. Then G_v is the set of points of G taking values in K_v, C_v is the set of points of G taking values in R_v for v not belonging to a finite set $S \ni \infty$. The group G_A is called the group of adeles of G.

We now give some examples.
(1) **The ring of adeles of K**,
we choose $G_v = K_v,\ S = \infty,\ C_v = R_v$
The corresponding adelic group is called the ring of adeles of K. It is also the group of adeles of the algebraic group induced by the additive group structure on K. We denote it by A_K. More precisely, the adele ring of K is

$$A_K = \prod\nolimits'_{v\in V} K_v = \left\{ (x_v) \in \prod_{v\in V} K_v, x_v \in C_v \text{ for all but finitely many } v \right\}$$

This product is given a topology as follows : $U \subset A_K$ is open if and only if for all $a \in A_K$, the set

$$(a+U) \cap \left(\prod_{v|\infty} K_v \times \prod_{v<\infty} R_v \right)$$

is open in the product topology.

For a specific example take $K = \mathbb{Q}$. The adele ring of $\mathbb{Q}$ is

$$A_{\mathbb{Q}} = \prod\nolimits'_{p} \mathbb{Q}_p = \left\{ (x_p) \in \prod_{p} \mathbb{Q}_p, \quad x_p \in \mathbb{Z}_p \text{ for almost but finitely many } p \right\} \cdot \mathbb{R}.$$

Here p is prime number.

(2) **The group of ideles of K**. We choose
$G_v = K_v^*,\ S = \infty,\ C_v = R_v^*$
The corresponding adelic group is called the group of ideles of K. It is the group of units of A_K. We denote by A_K^*. Observe that the idele group of K is

$$A_K^* = \left\{ (x_v) \in \prod_{v\in V} K_v^*, \quad x_v \in C_v^* \text{ for all but finitely many } v \right\}$$

Since inversion is not a continuous operation in the relative topology (the topology induced on A_K^* from A_K), we have to endow A_K^* with a new topology such that inversion

becomes a continuous operation. The new topology on A_K^* is given as follows: $U \subset A_K^*$ is open if and only, if for all $a \in A_K^*$, the set

$$aU \cap \left(\prod_{v|\infty} K_v^* \times \prod_{v<\infty} R_v^* \right)$$

is open in the product topology. In general, if R is a topological ring, R^* becomes a topological group when we give R^* the relative topology induced by

$$\begin{aligned} R^* &\subset (R \times R) \\ x &\mapsto \left(x, x^{-1}\right). \end{aligned}$$

(3) **Adelic group defined by H**
(a) $G_v = H_v, \quad S \supset \infty, \quad S \neq \emptyset, \quad C_v = \mathcal{O}_v$
where $\mathcal{O}$ is an order in H over the ring $R_{(S)}$, and $\mathcal{O}_v = \mathcal{O} \otimes R_v$, the tensor product being taken over $R_{(S)}$. Then we define the ring of adeles of H , which we denote by A_H. It is equal to $A \otimes H$, where the tensor product is taken over K.
(b) $G_v = H_v^*, \quad S \ni \infty, \quad S \neq \emptyset, \quad C_v = \mathcal{O}_v^*$
We define the group of units of A_H, denoted by A_H^*.
(2) $G_v = {H_v}^1, \quad S \ni \infty, \quad S \neq \emptyset, \quad C_v = \mathcal{O}_v^1$
Where X^1 denotes the set of elements in X of reduced norm 1. We define the adelic group and denoted it by A_H^1.
All these adelic groups are also examples of groups of adeles of algebraic groups.

Morphisms. Let us suppose that there is another restricted product ${G'}_A$ of locally compact groups G'_v with respect to locally compact subgroups C'_v. We can suppose that the set $S' \subset V$ is such that, for $v \notin S', \quad C'_v$ is defined, is equal to S (Mainly we can assume that S′ = S). Now assume that for every place $v \in V$, we have a homomorphism $f_v : G_v \to G'_v$ such that if $v \notin S, \quad f_v(C_v) \subset C'_v$. Then the restriction of $\prod f_v$ to G_A defines a morphism of G_A to ${G'}_A$ which is denoted by f_A. If the function f_v is continuous, then f_A is continuous as well.
For example we define the reduced trace map is $t_A : A_H \to A_K$ and the reduced norm map is $n_A : A_H^* \to A_K^*$ which are induced from the maps $tr : H_v \to K_v$ and $n : H_v^* \to K_v^*$.

We now suppose that G' is a group whose unit element is 1, and that for every place $v \in V$ we have a homomorphism $f_v : G_v \to G'$ such that $f_v(C_v) = 1$ for almost all $v \notin S$. Then we can define in G' the product

$$f_A(x) = \prod_{v \in V} f_v(x_v), if \quad x = (x_v) \in G_A$$

For example we may define the norm N_A and the modulus $\|.\|_A$ on A_H^* and A_K^* in this way.

NOTATIONS. For the sake of convenience we consider G_v as embedded in G_A by identifying canonically with $\prod_{w \neq v} 1_w \times G_v$, where 1_w is the unit of G_w, $w \in V$. When G_A is a group of adeles of an algebraic group defined over K, then the group G_K will be the group of K-rational points of G taking values in K. For every place $v \in V$, we choose an embedding of G_K in G_v, denoted i_v. For almost every place v, $i_v(G_K) \subset C_v$, whence the function $\prod_{v \in V} i_v$ defines an embedding of G_K into G_A.

We put $X = X_K = H$ or K, and $Y_v = \mathcal{O}_v$ or R_v, for almost all places $v \in S$.

Quasi-characters. Recall the definition of a quasi-character from the previous chapter. It is a continuous homomorphism from a locally compact group to $\mathbb{C}^*$. Let Ψ_A be a quasi-character of G_A. By restriction to G_v, it defines a quasi-character Ψ_v of G_v. Naturally we have the relation

$$\Psi_A(x) = \prod_{v \in V} \Psi_v(x_v) \text{ if } x = (x_v) \in G_A$$

For the product to converge in $\mathbb{C}^*$, it is necessary and sufficient that $\Psi_v(C_v) = 1$ for almost all $v \in S$. In effect, if this property were not satisfied, we could find $c_v \in C_v$ such that $|\Psi_v(c_v) - 1| > \frac{1}{2}$ for almost all $v \notin S$ and the product would not converge on the elements x such that $x_v = c_v$ for almost all $v \notin S$. We have showed :

Lemma 4.1.5 *The application $\Psi_A \to (\Psi_v)$ is a group isomorphism of quasi-characters of G_A onto the group* $\{ (\Psi_v),\ \Psi_v$ a quasi-character of $G_v,\ \ \Psi_v(C_v) = 1,$ for almost all $v \notin V\}$.

We can apply the local results of the previous chapter to the quasi-characters of A_X. Let $\Psi_A = \prod_{v \in V} \Psi_v$ (the product of characters).

Local canonical characters(taken from exercise 4.1 of [Vi 80]): The product is well-defined because $\Psi_v(Y_v) = 1$ for almost all $v \notin S$. The previous lemma shows that all characters of A_X are of the form $x \to \Psi_A(ax), a = (a_\mathrm{v}) \in X_v$, and $a_v \in \ker(\Psi_v)$ for almost all $v \notin S$. As $\ker(\Psi_v) = Y_v$ for almost all $v \notin S$, we deduce that $a \in A_K$. Then A_X is self-dual. By reducing to the case $X = \mathbb{Q}$ or $\mathbb{F}_p(T)$ is a prime field, we check that Ψ_A is trivial on X_K and that the dual of A_X/X_K is X_K (cf. Weil [1]). Hence we get the following proposition :

Proposition 4.1.6 . *A_X is self-dual and X_K is dual of A_X/X_K.*

Now we will give main theorem on the adeles A_X and A_X^*. These theorems are still true if X is a simple central algebra over K. The proof in our case will give a good idea of the proof in general.

Theorem 4.1.7 ***Adeles.***
(1) *X_K is discrete in A_X and A_X/X_K is compact.*
(2)(**Approximation theorem**). *For every place v, $X_K + X_v$ is dense in A_X.*

Ideles.
(1) *X_K^* is discrete in A_X^*.*
(2)*(**Product formula**) For all $x \in X_K^*$, the modulus of x is 1.*
(3)*(**Fujisaki theorem**). If X is a division algebra, the image in A_X^*/X_K^* of the set*

$$Y = \{x \in A_X^* \quad 0 < m \leq ||x|| \leq M\}\,;\ m, M \in \mathbb{R}$$

is compact.
(4) *For every place v, infinite if X_K is not division algebra, there exists a compact set C of A_X^* such that $A_X^* = \overline{X_K^* X_v^* C}$.*

Proof: **Adeles**.
(1) To show that X_K is discrete in A_X, it is sufficient to check that 0 is not a limit point of X_K. In a sufficiently small neighbourhood of 0 in A_X, the only possible elements of X_K are integers at all the finite places: then they are finite in number if K is a function field and belong to $\mathbb{Z}$ if $X = \mathbb{Q}$. In these two cases, it is clear that 0 can not be a limit point. The same holds for all X, because X is a finite dimensional vector space over $\mathbb{Q}$ or a function field. The dual group of a discrete group is compact: thus A_X/X_K is compact.
(2)**Approximation theorem**. We will show that the characters on A_X which are trivial on X_K are determined by their restrictions to X_v. In effect, a trivial character on X_K and on X_v is of the form $x \to \Psi_A(ax)$, where Ψ_A is a canonical character with a in X_K and $\Psi_v(ax_v) = 1$ for all $x_v \in X_V$. This implies that $a = 0$ and that the character $\Psi_A(ax)$ is trivial. If $X_K + X_v$ were not dense in A_X, there would be a non-trivial character of A_X which would be trivial both on X_K and on X_v; this is a contradiction.
Ideles.
(1) To show that tX_K^* is discrete in A_X^*, it is sufficient to check that 1 is not a limit point of X_K^*. A sequence of elements (x_n) of X_K^* converges towards 1 if and only if (x_n) and (x_n^{-1}) converge towards 1. Then 1 is limit point of a X_K in A_X. This is not possible after the first part of the proof.
Product formula. Let x be an element of X_K; In order to show that the modulus of x is equal to 1, is necessary and sufficient to check that the volume of a measurable set $Y \subset A_X$ is equal to the volume of xY for some Haar measure. We have :

$$\mathrm{vol}(xY) = \int_{A_X} \varphi(x^{-1}y)dy = \int_{X_K\backslash A_X} \left(\sum_{z \in X_K} \varphi(zx^{-1}y) \right) d\dot{y}$$
$$\int_{X_K\backslash A_X} \sum_{z \in X_K} \varphi(zy)d\dot{y} = \mathrm{vol}(Y)$$

where φ is the characteristic function of Y, and $d\dot{y}$ is a measure on $X_K\backslash A_X$ obtained by compatibility with dy and the discrete measure on X_K, takes value 1 on each element of X_K.
Fujisaki theorem. A compact set of A_X^* is of the form

$$\left\{x \in A_X^*,\ \ (x, x^{-1}) \in C \times C'\right\}$$

for two compact subsets C and C' of A_X. For x an element of Y, that is

$$0 < m \leq ||x|| \leq M$$

we find an element of X_K^* such that $xa \in C$ and $a^{-1}x^{-1} \in C'$. We choose in A_X a compact set of sufficiently large volume greater than $(\mathrm{vol}(A_X/X_K)\ \mathrm{Sup}(m^{-1}, M))$ then the volume of $x^{-1}C''$ and $C''x$ are strictly greater than the volume of A_X/X_K. We put then $C = C'' - C'' = \{x - y : x,\ y \in C''\}$. It is a compact subset of A_X since the map $(x, y) \to x - y$ is continuous. There exist $a, b \in X_K$ such that $xa \in C$, $bx^{-1} \in C$. At this point we suppose that X is a division algebra: then we can choose a, b in X_K^*. We have $ba \in C^2$, which is compact in A_X. Then the number of possible values for $ba = c$ is finite, and we choose $C' = \cup c^{-1}C$.
(4) By Fujisaki' theorem, this is obvious for a division algebra X. In effect, with the choice made for v, the group of modulus of X_v is let finite index in the corresponding group for A_X^*, and if we denote by $A_{X,1}^*$, the elements of A_X of modulus 1, we have just shown that $A_{X,1}^*/X_K^*$ is compact. There remains the case of $M_2(K)$. We will use the well known existence of the " Siegel Set " . But in the very simple case which interests us the proof is simple. Let P be the group of the upper triangular matrices, let D be that of diogonal matrices, and N be the group of unipotent matrices of P. By triangulation, we have

$$GL_2(A_X) = A_P.C = A_D A_N C,$$

where C is a maximal compact subgroup of $GL_2(A_X)$. After the approximation theorem in the adeles $A_X = A_N$ and the property (4), being show for K, we have:

$$A_P = D_K D_v C'.N_K N_v C''.$$

The elementary permutation relation

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & ax/b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

implies that $A_P = P_K P_v C''$ where $C'' \subset A_P$ is compact, which implies (4).

5 Anticyclotomic p-adic L-functions attached to (E, K)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, let E have good ordinary reduction at a prime p, $p \neq 2$ and let K be an imaginary quadratic field of dicriminant D_K. Write K_∞/K for the anticyclotomic $\mathbb{Z}_p$-extension of K and set $G_\infty = \mathrm{Gal}(K_\infty/K)$. It will be assumed throughout that the discriminant of K is prime to N, so that K determines a factorisation

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

where N^+ (resp.N^-) is divisible only by primes different from p which are split (resp. inert) in K. Also we will assume that N^- is the square-free product of an odd number of primes.

The following statement plays a vital role in our scheme of things.
Let B be a quaternion division algebra over some global field. From the classification of quaternion algebras over global fields, we know that the number $|\mathrm{Ram}(B)|$ of places where B ramifies is even. For all finite sets S of places of that global field of order $|S|$, assumed to be even there exists a unique quaternion algebra B over that global field, upto isomorphism, such that $S = \mathrm{Ram}(H)$.

Let B be a definite quaternion division algebra over $\mathbb{Q}$ of discriminant $N^-\infty$, that is ramified at all primes dividing N^-. The algebra B is unique up to isomorphism from the above statement. For a prime l, we fix an isomorphism (as $\mathbb{Q}_l$-algebra) such that

$$\begin{array}{ll} \text{if } l \not| N^-\infty & B \otimes \mathbb{Q}_l \cong M_2(\mathbb{Q}_l) \\ \text{if } l \mid N^-\infty & B \otimes \mathbb{Q}_l \text{ is a division algebras over } \mathbb{Q}_l \\ \text{if } l = \infty & B \otimes \mathbb{R} = \mathbb{H}, \text{the Hamiltonian algebra.} \end{array}$$

Now let R be an Eichler $\mathbb{Z}[\frac{1}{p}]$-order of level N^+ in B. The Eichler order R is unique up to conjugation by B^*. For more details see (cf. [Vi , chap3 , section 4 and section 5]). For a prime l we fix an isomorphism (as $\mathbb{Z}_l$) algebra such that

$$\begin{array}{ll} \text{if } \ l \not| N\infty & R \otimes \mathbb{Z}_l \cong M_2(\mathbb{Z}_l) \\ \text{if } \ l \mid \ N^- & R \otimes \mathbb{Z}_l \text{ is the maximal order in } B \otimes \mathbb{Z}_l, \\ \text{if } l \mid \ N^+ & R \otimes \mathbb{Z}_l \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_l) : N^+ \mid c \right\} \end{array}$$

Denote by $\mathcal{T}$ the Bruhat-Tits tree of ${B_p}^*/{\mathbb{Q}_p}^*$, where

$$B_p := B \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$$

The set $\mathcal{V}(\mathcal{T})$ of vertices of $\mathcal{T}$ is indexed by the maximal $\mathbb{Z}_p$-orders in B_p, two vertices being adjacent if their intersection is an Eichler order of level p. Let $\overrightarrow{\mathcal{E}}(\mathcal{T})$ denote the set of ordered edges of $\mathcal{T}$, that is, the set of ordered pairs (s,t) of adjacent vertices of $\mathcal{T}$. If e = (s,t), the vertex s called source or origin of e and the vertex t is called the target or terminal of e. They are denoted by s(e) and t(e) respectively.

The tree $\mathcal{T}$ is endowed with a natural left action of ${B_p}^*/{\mathbb{Q}_p}^*$ by isometries corresponding to conjugation of maximal orders by element of ${B_p}^*$. This action is transitive on both $\mathcal{V}(\mathcal{T})$ and $\overrightarrow{\mathcal{E}}(\mathcal{T})$. Let R^* denote the group of invertible elements of R. The group $\Gamma := R^*/\mathbb{Z}[\frac{1}{p}]^*$ - a discrete subgroup of ${B_p}^*/{\mathbb{Q}_p}^*$ in the p-adic topology-acts naturally on $\mathcal{T}$, and the quotient $\mathcal{T}/\Gamma$ is a finite graph.

Notations. Let $\hat{\mathbb{Z}} = \prod_l \mathbb{Z}_l$ denote the usual profinite completion of $\mathbb{Z}$, and write $\hat{\mathbb{Q}} := \hat{\mathbb{Z}} \otimes \mathbb{Q}$ for the ring of finite rational adeles. Let

$$\hat{R} := R \otimes \hat{\mathbb{Z}}, \qquad \hat{B} := B \otimes \hat{\mathbb{Q}} = \hat{R} \otimes \mathbb{Q}.$$

Definition 5.0.8 . *A modular form on the quaternion algebras B of weight 2 and level $\hat{R}^*$ is a $\mathbb{Z}_p$-valued function f on $\mathcal{V}(\mathcal{T})$ satisfying such that*

$$f(\gamma \mathrm{v}) = f(\mathrm{v}) \quad \text{for all} \quad \gamma \in \Gamma$$

Denote by $\mathcal{M}_2(B)$ the space of all such modular forms. It is a free $\mathbb{Z}_p$-module of finite rank.

Action of Hecke-operators: The Hecke operators T_p act on $f \in \mathcal{M}_2(B)$ by

$$\left(f_{|T_p}\right)(v) = \sum_{v' \to v} f(v')$$

where v' are the vertices adjacent to v.
For all prime $l \not| pN$, there is a Hecke operator T_l on $\mathcal{M}_2(B)$ given by elements $\gamma_1, \gamma_2, \gamma_3 .... \gamma_{l+1}$ of R, such that

$$\Gamma M_l \Gamma = \gamma_1 \Gamma \cup \gamma_2 \Gamma \cup \gamma_3 \Gamma ..... \cup \gamma_{l+1} \Gamma$$

with $M_l \in R$ of reduced norm l. See [BD01] for the precise definition.

The Jacquet-Langlands correspondence. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. The complex vector space $\mathcal{M}_2(\mathcal{H}/\Gamma_0(N))$ of classical modular forms of weight 2 on $\mathcal{H}/\Gamma_0(N)$ is similarly endowed with an action of Hecke operators which will also denoted by the symbols T_p. Let $f_E \in \mathcal{M}_2(\Gamma_0(N))$ be an eigenform for the "good " Hecke operators. That is $f_{E|T_p} = a_p.f_E$ for all $p \not| N$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$. We have the following theorem due to Jacquet-Langlands :

Theorem 5.0.9 . *Let f_E be as above. Then there exists an eigenform $f \in \mathcal{M}_2(B)$ for all T_l, $l \not| N$ such that $f_{|T_l} = a_l.f$ (a_l are the ones for f_E).*

We will not give the prove of this theorem. For the proof see ([BD01] , page no 8).

Assumption on K: Let $\mathcal{O} = \mathcal{O}_K[\frac{1}{p}] \subset K$, where $\mathcal{O}_K$ is the ring of integers of K. For simplicity, we assume that the class number of $\mathcal{O}$ is 1.

We can embed K in B because B is definite of discriminant N^- and the algebra K is an imaginary quadratic field in which all prime divisors of N^- are inert. Fix an embedding

$$\Psi : K \hookrightarrow B \text{ satisfying } \Psi(K) \cap R = \Psi(\mathcal{O}). \tag{5.1}$$

Such a Ψ exists if and only if all the primes dividing N^+ are split in K. So from our initial assumption it does exist, and it is unique up to conjugation by elements in B^*. Now

$$\Psi_p : K_p = K \otimes \mathbb{Q}_p \hookrightarrow B_p = B \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$$

This induces a map

$$\Psi_p : {K_p}^* \hookrightarrow GL_2(\mathbb{Q}_p).$$

Now, since ${\mathbb{Q}_p}^* \subset {K_p}^*$ and ${\mathbb{Q}_p}^*$ is embedded in $GL_2(\mathbb{Q}_p)$ by

$$\mathrm{a} \mapsto \begin{pmatrix} \mathrm{a} & 0 \\ 0 & \mathrm{a} \end{pmatrix}.,$$

the embedding Ψ induces an embedding of K_p^* into B_p^* and hence yields an action of ${K_p}^*/{\mathbb{Q}_p}^*$ on $\mathcal{T}$.

Since $p \not| D_K$, we have that either p is inert in K or p splits in K. Now we will study the structure of ${K_p}^*/{\mathbb{Q}_p}^*$ in these two cases.
Case1. Suppose p is inert in K. This implies that K_p is an unramified extension of residue degree 2. In this case

$$\begin{aligned} {\mathbb{Q}_p}^* &= p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p), \\ \text{and} \quad {K_p}^* &= p^{\mathbb{Z}} \times \mu_{p^2-1} \times (1 + p\mathcal{O}_{K_p}) \end{aligned}$$

which implies that ${K_p}^*/{\mathbb{Q}_p}^* \cong \frac{\mu_{p^2-1}\times(1+p\mathcal{O}_{K_p})}{\mu_{p-1}\times(1+p\mathbb{Z}_p)} \cong \frac{\mu_{p^2-1}}{\mu_{p-1}} \times \frac{1+p\mathcal{O}_{K_p}}{1+p\mathbb{Z}_p}$.
Also we see in this case that

$$K_p^* = \mathbb{Q}_p^* \cdot \mathcal{O}_{K_p}^*. \tag{5.2}$$

Let $\gamma \in K_p$ be such that $\gamma^2 = D_K$. Then an embedding (local) of

$$\Psi_p : K_p \hookrightarrow M_2(\mathbb{Q}_p)$$

is determined by
(1) $\Psi_p(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ if $a \in \mathbb{Q}_p$
and
(2) $\Psi_p(\gamma) = A$ such that $A^2 = \begin{pmatrix} D_K & 0 \\ 0 & D_K \end{pmatrix}$, i.e. $\text{trace}(A) = 0$ and $\det(A) = -D_K$.
We can change the isomorphism defined previously (page. 81), so that A has the form $\begin{pmatrix} 0 & 1 \\ -D_k & 0 \end{pmatrix}$. Note that the choice of the matrix of the isomorphism does not affect the further calculations we do. Now $\Psi_p(a + b\gamma) = a \cdot Id + b \cdot A$, $a,\ b \in \mathbb{Q}_p$.

K_p as a $\mathbb{Q}_p$-vector-space is equal to $\mathbb{Q}_p \oplus \mathbb{Q}_p\gamma \cong \mathbb{Q}_p \oplus \mathbb{Q}_p$ ($1 \mapsto (1, 0)$, $\gamma \mapsto (0, 1)$).

Consider the lattice $L_0 = (\mathbb{Z}_p \cdot Id) \oplus (\mathbb{Z}_p \cdot A)$ in $(\mathbb{Q}_p \cdot Id) \oplus (\mathbb{Q}_p \cdot A) \subset M_2(\mathbb{Q}_p)$.
At first we will show that $\Psi_p(K_p^*/\mathbb{Q}_p^*)$ fixes the vertex of the tree $v_0 = [L_0]$ i.e. $\Psi_p(K_p^*/\mathbb{Q}_p^*)$ stabilizes the class $[L_0]$.

Since $\Psi_p(\mathbb{Q}_p^*)$ acts trivially on the class of lattices, from equation 5.2 just we have to see how $\Psi_p(\mathcal{O}_{K_p}^*)$ acts on $[\mathbb{Z}_p \cdot Id \oplus \mathbb{Z}_p \cdot A]$, which is equivalent to seeing how $\mathcal{O}_{K_p}^*$ acts on $[\mathbb{Z}_p \oplus \mathbb{Z}_p\gamma]$. It is easy to see the action of $\mathcal{O}_{K_p}^*$ by left multiplication takes this lattice to itself and hence stabilizes its class.

We know that the vertices at distance n from v_0 corresponds to one dimensional factors of L_0/p^nL_0 (as a $\mathbb{Z}_p/p^n\mathbb{Z}_p$)-module). Let $v_n = [(\mathbb{Z}_p \cdot Id) \oplus p^n(\mathbb{Z}_p \cdot A)]$. Clearly v_n is at distance n from v_0. Now our aim is to find the stabilizer of the class $[(\mathbb{Z}_p \cdot Id) \oplus p^n(\mathbb{Z}_p \cdot A)]$ under the action of $\Psi_p(K_p^*/\mathbb{Q}_p^*)$. We have the surjection map $\mathcal{O}_{K_p}^* \longrightarrow \mathcal{O}_{K_p}/p^n\mathcal{O}_{K_p} \cong L_0/p^nL_0$ (as a $\mathbb{Z}_p/p^n\mathbb{Z}_p$)-module) and so $\mathcal{O}_{K_p}^*$ acts on L_0/p^nL_0 by left multiplication. This action is the same as the action of $\Psi_p(\mathcal{O}_{K_p}^*)$ on the vertices which are at distance n from v_0. v_n corresponds to the one dimensional factor in L_0/p^nL_0 generated by (1,0) i.e. identity in $\mathcal{O}_{K_p}/p^n\mathcal{O}_{K_p}$. i.e. $a \in \mathcal{O}_{K_p}^*$ fixes this if and only if $\bar{a} = 1$ in $\mathcal{O}_{K_p}/p^n\mathcal{O}_{K_p}$ i.e. $a \in 1 + p^n\mathcal{O}_{K_p}$. So in $K_p^*/\mathbb{Q}_p^*$,

$$\frac{1 + p^n\mathcal{O}_{K_p}}{\mathbb{Q}_p^* \cap (1 + p^n\mathcal{O}_{K_p})} = \frac{1 + p^n\mathcal{O}_{K_p}}{1 + p^n\mathbb{Z}_p}$$

fixes the vertex v_n.

Put $\mathrm{U}_n = \frac{1+p^n\mathcal{O}_{K_p}}{1+p^n\mathbb{Z}_p}$. After taking p-adic logarithms we can prove that $\mathrm{U}_n = \frac{1+p^n\mathcal{O}_{K_p}}{1+p^n\mathbb{Z}_p} \cong \frac{p^n\mathcal{O}_{K_p}}{p^n\mathbb{Z}_p}$. As $\mathrm{U}_1 \subseteq {K_p}^*/{\mathbb{Q}_p}^*$ with index $p+1$, (because $\frac{\mu_{p^2-1}}{\mu_{p-1}}$ is cyclic group of order $p+1$) and $\mathrm{U}_n \subseteq \mathrm{U}_{n-1}$ with index p because as additive groups, if $\mathcal{O}_{K_p} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ then $p^n\mathcal{O}_{K_p} \cong p^n\mathbb{Z}_p \oplus p^n\mathbb{Z}_p$, which implies that $\mathrm{U}_n \cong p^n\mathbb{Z}_p$ and therefore $[\mathrm{U}_n : \mathrm{U}_{n-1}] = p$ and $[\mathrm{U}_n : {K_p}^*/{\mathbb{Q}_p}^*] = p^{n-1}(p+1)$. So we have:

$$.....\mathrm{U}_n \subseteq \mathrm{U}_{n-1}..... \subseteq \mathrm{U}_2 \subseteq \mathrm{U}_1 \subseteq {K_p}^*/{\mathbb{Q}_p}^*.$$

From global class field theory we have $G_\infty = \mathrm{Gal}(K_\infty/K) = (K_p^*/{\mathbb{Q}_p}^*)/(\mu_{p^2-1}/\mu_{p-1})$. Let $\widetilde{G}_\infty$ denote the group

$$K^* \setminus \hat{K}^* / \ (\hat{\mathbb{Q}}^*.\prod_{l\neq p}(\mathcal{O}_K \otimes \mathbb{Z}_l)^*),$$

which is the union of the ring class fields of K of conductor p^n for every n. By passing to the adelisation in equation (5.1) the embedding Ψ induces a map

$$\hat{\Psi} : \widetilde{G}_\infty \longrightarrow B^* \setminus \hat{B}^*/\hat{\mathbb{Q}}^*.\prod_{l\neq p}(\mathcal{O}_K \otimes \mathbb{Z}_l)^* = B^* \setminus \hat{B}^*/\hat{\mathbb{Q}}^*.\prod_{l\neq p} {R_l}^* \tag{5.3}$$

By strong approximation ([Vi, chapter 3 , section 4]), the double coset space appearing on the right has a fundamental region containing ${B_p}^* \subset B^*$. In fact, strong approximation yields a canonial identification

$$\eta : B^* \setminus \hat{B}^*/\hat{\mathbb{Q}}^*.\prod_{l\neq p} {R_l}^* \longrightarrow \Gamma \setminus {B_p}^*/{\mathbb{Q}_p}^*$$

For more details see ([N], chapter IV).

Now our aim is to define a $\mathbb{Z}_p$ valued measure on $K_p^*/{\mathbb{Q}_p}^*$. For that we choose a sequence of vertices $v_0, v_1, ...v_n....$ of consecutive edges on $\mathcal{T}$ satisfying

$$\mathrm{Stab}_{K_p^*/{\mathbb{Q}_p}^*}(v_j) = \mathrm{U}_j, j = 1, 2, 3.....n, ..$$

and $({K_p}^*/{\mathbb{Q}_p}^*)/\mathrm{U}_n$ acts transitively on the vertices at distance n from v_0.

Let $f \in \mathcal{M}_2(B)$ with eigenvalue a_p. Let α be the unit root of $X^2 - a_pX + p = 0$ in ${\mathbb{Z}_p}^*$. For $a \in G_\infty, \quad n \geq 1$, we define:

$$\mu(a\mathrm{U}_n) = \alpha^{-n} f(av_n) - \alpha^{-n-1} f(av_{n-1}),$$

We would like to show that μ is a measure on G_∞. Let $b_1, b_2, ...b_{\mathrm{p}}$ be representatives of $\mathrm{U}_n/\mathrm{U}_{n+1}$, for $a \in G_\infty$, we need to show

$$\mu(a\mathrm{U}_n) = \sum_{i=1}^{p} \mu(a.b_i\mathrm{U}_{n+1})$$

Now,

$$\begin{aligned}\sum_{i=1}^{p}\mu(a.b_i\mathrm{U}_{n+1}) &= \sum_{i=1}^{p}\left(\alpha^{-n-1}f(ab_iv_{n+1})-\alpha^{-n-2}f(ab_iv_n)\right)\\ &= \alpha^{-n-1}\sum_{i=1}^{p}f(ab_iv_{n+1})-p\alpha^{-n-2}f(av_n)\end{aligned}$$

Since $(f_{|T_p})(av_n)=\sum_{i=1}^{p}f(ab_iv_{n+1})+f(ab_iv_{n-1})$ and $f_{|T_p}=a_pf$, we get

$$\begin{aligned}\sum_{i=1}^{p}\mu(a.b_i\mathrm{U}_{n+1}) &= \alpha^{-n-1}\left(a_pf(av_n)-f(ab_iv_{n-1})\right)-p\alpha^{-n-2}f(av_n)\\ &= \alpha^{-n-1}\left(\alpha f(av_n)-f(av_{n-1})\right)\\ &= \alpha^{-n}f(av_n)-\alpha^{-n-1}f(av_{n-1})\\ &= \mu(a\mathrm{U}_n).\end{aligned}$$

Now $\mathrm{Gal}(K_p/\mathbb{Q}_p)=\langle x\mapsto\bar{x}\rangle$, where $x\mapsto\bar{x}$ is the non-trivial automorphism of $K_p/\mathbb{Q}_p$. We define a function

$$K_p{}^{*}\longrightarrow\mathcal{O}_{K_p}{}^{*},\qquad x\longrightarrow\frac{x}{\bar{x}},$$

whose kernel is $\mathbb{Q}_p{}^{*}$. Then $K_p{}^{*}/\mathbb{Q}_p{}^{*}\hookrightarrow\mathcal{O}_{K_p}{}^{*}$,
and the image is $\left\{x\in\mathcal{O}_{K_p}{}^{*}\ \mid\ \mathrm{N}_{K_p/\mathbb{Q}_p}(x)=1\right\}$.

If $\chi:K_p^{*}/\mathbb{Q}_p{}^{*}\to\mathbb{C}_p{}^{*}$ is a finite order character of conductor p^n, define:

$$L_p(E/K,\chi,s)=\int_{K_p^{*}/\mathbb{Q}_p{}^{*}}\left(\frac{x}{\bar{x}}\right)^{s-1}\chi(x)\mu(x).$$

Case 2. p splits K.
Say $p\mathcal{O}_k=\mathfrak{P}\bar{\mathfrak{P}}$, where $\mathfrak{P}$ is a prime ideal in K, $\mathfrak{P}\neq\bar{\mathfrak{P}}$, and $\mathcal{O}_K/\mathfrak{P}\cong\mathcal{O}_K/\bar{\mathfrak{P}}\cong\mathbb{F}_p$.
In this case,

$$K_p=K\otimes_{\mathbb{Q}}\mathbb{Q}_p\cong K_{\mathfrak{P}}\times K_{\bar{\mathfrak{P}}}\cong\mathbb{Q}_p\times\mathbb{Q}_p$$

and $\mathbb{Q}_p$ is embedded in K_p by $x\to(x,x)$.

We can change the isomorphism defined previously (page. 81) such that in this case we have an embedding

$$\Psi_p:K_p\hookrightarrow M_2(\mathbb{Q}_p)$$

determined by
(1) $\Psi_p(a,b)=\begin{pmatrix}a&0\\0&b\end{pmatrix}$, $a,b\in\mathbb{Q}_p$.

Now ${K_p}^*/{\mathbb{Q}_p}^* = \frac{{\mathbb{Q}_p}^* \times {\mathbb{Q}_p}^*}{{\mathbb{Q}_p}^*}$. We define a map

$$\mathrm{V} : \frac{{\mathbb{Q}_p}^* \times {\mathbb{Q}_p}^*}{{\mathbb{Q}_p}^*} \longrightarrow \mathbb{Z}, \quad (a,b) \mapsto \mathrm{V}\left(\frac{a}{b}\right).$$

where V is the valuation on $\mathbb{Q}_p$. This map is well defined, surjective and $\mathrm{Ker(V)} = {\mathbb{Z}_p}^*$. Since the given map is surjective, ${K_p}^*/{\mathbb{Q}_p}^*$ is not compact, but the kernel of this map is compact. Since $\mathrm{Ker(V)} = {\mathbb{Z}_p}^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. Put $\mathrm{V}_0 = \mathrm{Ker(V)}$, and let V_i be the subgroup of V_0 corresponsing to the subgroup $(1 + p^i\mathbb{Z}_p), \quad i = 1, 2, ...$ of $\mathbb{Z}_p$. So we have

$$...\mathrm{V}_n \subset .....\mathrm{V}_2 \subset \mathrm{V}_1 \subset \mathrm{V}_0,$$

with $[\mathrm{V}_0 : \mathrm{V}_n] = (p-1)p^{n-1}$ and $[\mathrm{V}_0 : \mathrm{V}_1] = p - 1$

We had an embedding

$$\Psi : K \hookrightarrow B$$

$$\Psi_p : {K_p}^* \hookrightarrow GL_2(\mathbb{Q}_p)$$

As we proved earlier, that $\left({K_p}^*/{\mathbb{Q}_p}^*\right)/\mathrm{V}_0 \cong \mathbb{Z}$. In this case we will first prove that the action of ${K_p}^*/{\mathbb{Q}_p}^*$ does not fix any vertex.

Consider the lattice $L_0 = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, where $\{e_1, e_2\}$ is a basis for $\mathbb{Q}_p^2$ over $\mathbb{Q}_p$ as a vector space. Let $v_0 = [L_0]$, where $L_0 = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ be a vertex of the tree. Let $\delta = (a,b) \in (\mathbb{Q}_p^* \times {\mathbb{Q}_p}^*)$, then $\Psi_p(\delta) \cdot [L_0] = [\mathbb{Z}_p a e_1 \oplus \mathbb{Z}_p b e_2]$, so $[L_0] = [\mathbb{Z}_p a e_1 \oplus \mathbb{Z}_p b e_2]$ if and only if $\mathrm{V}(\frac{a}{b}) = 0$. We can choose $(a,b) \in (\mathbb{Q}_p^* \times {\mathbb{Q}_p}^*)$ such that $\mathrm{V}(\frac{a}{b}) \neq 0$, which implies that the action of ${K_p}^*/{\mathbb{Q}_p}^*$ does not fix a vertex.

Consider the line $.....[\mathbb{Z}_p e_1 \oplus p^{-1}\mathbb{Z}_p e_2], [\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2], [\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2], ...[\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p^n e_2].....$ denoted by $\mathfrak{g}$ in the tree $\mathcal{T}$. V_0 fixes this line $\mathfrak{g}$ in $\mathcal{T}$ i.e. it fixes a line of edges, i.e. for all $\sigma \in \mathrm{V}_0, \quad v \in \mathfrak{g}, \ \sigma v = v$ and $\left({K_p}^*/{\mathbb{Q}_p}^*\right)/\mathrm{V}_0$ acts by translation on $\mathfrak{g}$. Now we define for some $v \in \mathrm{V}(\mathcal{T}), \quad \mathrm{dist}(v, \mathfrak{g}) = \min\{\mathrm{dist}(v, v'), \quad v' \in \mathfrak{g}\}$.

Let $v_n = [\mathbb{Z}_p e_1 \oplus p^{-n}\mathbb{Z}_p(e_1 + e_2)]$. Clearly it is at distance n from the line $\mathfrak{g}$, mainly it is at distance n from $[\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2]$. We can easily calculate the stabilizer of v_n inside V_0 which is equal to V_n and $({K_p}^*/{\mathbb{Q}_p}^*)/\mathrm{V}_n$ acts transitively on the set of vertices at distances n from $\mathfrak{g}$.

The group S = the group of p-units of $\mathcal{O}_K\left[\frac{1}{p}\right]$ of norm 1 is generated by u_p.
As we defined earlier, $\Psi\left(\mathcal{O}_K\left[\frac{1}{p}\right]\right) = K \cap R \Rightarrow \Psi\left(\mathcal{O}_K\left[\frac{1}{p}\right]^*\right) \subseteq R^* = \Gamma$.

By complex multiplication and global class field theory, we have:

$$\left({K_p}^*/\mu_{p-1}{\mathbb{Q}_p}^*\right)/{u_p}^{\mathbb{Z}} \cong G_\infty = \mathrm{Gal}(K_\infty/K).$$

So we have :

$$\left({K_p}^*/{\mathbb{Q}_p}^*\right)/{u_p}^{\mathbb{Z}} \cong \mathbb{Z}_p \times (\mathbb{Z}/M\mathbb{Z})$$

with $M = p - 1$. Define:

$${K_p}^*/{\mathbb{Q}_p}^* \longrightarrow \mathbb{Z}_p \times (\mathbb{Z}/M\mathbb{Z}), \qquad \mathrm{V}_i \longrightarrow [\mathrm{V}_i]$$

Write for $a \in {K_p}^*/{\mathbb{Q}_p}^*$, $[a] \in G_\infty$. For $v \in \mathcal{T}$ and $f \in \mathcal{M}_2(B)$, we have :
Claim. $f([a].v) := f(a.v)$ is well defined.
Proof. Let $a' = a.{u_p}^n$ for some $n \in \mathbb{N}$. Then $f(a'v) = f(\Psi({u_p}^n).a.v) = f(a.v)$ because $\Psi(u_p) \in \Gamma$.

To define a $\mathbb{Z}_p$-valued measure on $({K_p}^*/{\mathbb{Q}_p}^*)/u_p^{\mathbb{Z}}$, choose a connected sequence of vertices $v_0, v_1, v_2, \ldots\ldots$ such that v_n is at distance n from $\mathfrak{g}$. For $f \in \mathcal{M}_2(B)$ with eigenvalue a_p, let α be the unit root of $X^2 - a_pX + p = 0$ in ${\mathbb{Z}_p}^*$. For $a \in G_\infty, \quad n \geq 0$ define:

$$\mu(a\mathrm{V}_n) = \alpha^{-n} f(av_{n+1}) - \alpha^{-n-1} f(av_n), \quad a \in G_\infty.$$

Similar to last time we can show that μ satisfies the distribution property. For $\chi : ({K_p}^*/{\mathbb{Q}_p}^*)/u_p^{\mathbb{Z}} \to {\mathbb{C}_p}^*$ a finite order character define

$$L_p(E/K, \chi, s) = \int_{({K_p}^*/{\mathbb{Q}_p}^*)/u_p^{\mathbb{Z}}} x^{s-1}\chi(x)\mu(x).$$

Conclusion

In this concluding section we briefly give an overview what we studied in this thesis and the consequences of the main results.

As we mentioned in the introduction, this thesis is an attempt to give a glance at what happens when analysis meet arithmetic. The romance of analysis and arithmetic is among the deepest and most enticing themes in all of mathematics. In recent decades p-adic analysis, a hybrid of arithmetic and analysis has emerged as a fascinating offspring of this union. We know that analytically defined quantities like the order of vanishing (or pole) and the leading coefficient of the Taylor series of L-functions attached to an arithmetic object X sometimes encode global arithmetic invariants of X. For X an elliptic curve over $\mathbb{Q}$ the conjecture of Birch and Swinnerton-Dyer predicts that the order of vanishing of $L(X, s)$ at $s = 1$ is equal to the rank of the group of rational points on X and that the leading coefficient of the Taylor series encodes the order of the Tate-Shafarevich group as well as the height regulator.

The structure of such special values is usually expressed through their arithmetic properties. We sometimes find that the special values of a given L-function (and its twists) satisfy enough congruences to guarantee the existence of an array of p-adic L-functions that interpolate essentially the same values at special points as the complex L-function. Even more remarkable is the apparent fact that the p-adic analytic properties of these L-functions mirror those of the complex L-function.

In this thesis we have studied how to attach certain p-adic L-functions to to the data consisting of an elliptic curve E over $\mathbb{Q}$ and a quadratic imaginary field K with some conditions on the elliptic curve and the field. We then expect following the general philosophy outlied in the previous paragraphs, that the values at integers (special points) of these L-functions are related to the corresponding values taken by the classical L-function. In a paper by M.Bertolini and H.Darmon they formulate and prove a more precise statement involving this relation.

Bibliography

[1] [**MTT**] B.Mazur, J.Tate, J.Teitelbaum *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inv.Math.84 (1986) 1-48.

[2] [**Vi**] M-F.Vigneras, *Arithmétique des algèbres des quaternions*, LNM 800 Springer.

[3] [**DS**]F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Maths. 228, Springer, New York, 2005

[4] [**G**] S.S. Gelbart, *Automorphic forms on adele groups* , Princeton Univ. Press (1975)

[5] [**BD01**] M.Bertolini and H.Darmon, *Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions* , Annals of Mathematics, 162 (2005), 1-64

[6] [**N**] J. Neukirch, *Class field theory*, Springer (1986)

[7] [**Si**] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag (1986).

[8] [**BS**] Z.I.Borevich, I.R.Shafarevich, *Number Theory*, Academic press, New York(1975)(Translation from russian)(German translation: Birkhäuser, 1966)

[9] [**Pi**] Richard S.Pierce, *Associative Algebras*, Graduate Texts in Mathematics, Vol.88, Berlin-Heidelberg-New York, Springer Verlag, 1982.

[10] [**Re**] I. Reiner, Maximal Orders. Academic Press (1975).

[11] [**W1**] A. Weil, *Basic Number Theory*. Springer-Verlag (1967).

[12] [**H1**] H. Hijikata, *Explicit Formula of the traces of Hecke operators for* $\Gamma_0(N)$. J.Math.Z.92 (1966), 269-280

[13] [**serre [1]**] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, 1979(GTM 67).

[14] [**serre [4]**] Jean-Pierre Serre, *Trees,* Springer-Verlag, 1980

[15] [**Tate [1]**] J.Tate, *Fourier analysis in number fields and Hecke's zeta function*. Thesis Princeton Univ.(1950). Algebraic Number Theoery, J.W.S Cassels and A. Frölich, Academic press, (1967).

[16] R.GODEMENT, H.JACQUET[1] *Zeta Functions of Simple Central Algebras*. Springer-Verlag Lecture Notes 260 (1972)

[17] R.GODEMENT [1] *Les fonctions ζ des algèbres simples I et II.* Sèminaire Borbaki 1958/1959, Exposès 171 et 176

[18] N. BOURBAKI [3] *Topologie Génŕale, ch. 5 à 8.* Herman, Paris (1971).