The Arithmetic of Quaternion Algebra

M-F Vigneras

August 2, 2006

Contents

Chapter 1

Quaternion Algebra over a field

In this chapter K always denotes a commutative field of arbitrary characteristics if no particular mention, and K_s is the separable closure of K.

1.1 Quaternion Algebra

Definition 1.1. *A quaternion algebra H with center K is a central algebra over K of dimension 4, such that there exists a separable algebra of dimension 2 over K, and an invertible element θ in K with $H = L + Lu$, where $u \in H$ satisfies*

$$u^2 = \theta, \qquad um = \overline{m}u \tag{1.1}$$

for all $m \in L$, and where $m \mapsto \overline{m}$ is the nontrivial K-automorphism of L.

We denote H sometimes by $\{L, \theta\}$, but H does not determine this pair $\{L, \theta\}$ uniquely. For example, it is clear that one could replace θ by $\theta m\overline{m}$, if m is an element of L such that $m\overline{m} \neq 0$. the element u is not determined by (1). If $m \in L$ is an element with $m\overline{m} = 1$, we could replace u by mu. the definition can be used in the case of arbitrary character. .we can verify easily that H/K is a central simple algebra, i.e. an algebra with center K and without any nontrivial two-sided ideal.conversely, we can prove that every cental simple algebra of dimension 4 over K is a quaternion algebra.The rule of multiplication is deduced from (1). If $m \in L$, we have

$$(m_1 + m_2u)(m_3 + m_4u) = (m_1m_3 + m_2\overline{m}_4\theta) + (m_1m_4 + m_2\overline{m}_3)u. \tag{1.2}$$

Definition 1.2. *The conjugation is the K-endomorphism of H: $h \to \overline{h}$, which is the extension of the nontrivial K-automorphism of L defined by $\overline{u} = -u$.*

It is easy to verify it is an involutive anti-automorphism of H. It can be expressed by the following relations: if $h, k \in H$ and $a, b \in K$, we have

$$\overline{ah + bk} = a\overline{h} + b\overline{k}, \overline{\overline{h}} = h, \overline{hk} = \overline{kh}.$$

Definition 1.3. *Assume $h \in H$. The reduced trace of h is $t(h) = h + \overline{h}$. The reduced norm of h is $n(h) = h\overline{h}$.*

If $h \notin K$, its' minimal polynomial on K is

$$(x-h)(x-\overline{h}) = x^2 - t(h)x + n(h)$$

The algebra $K(h)$, generated by h over K, is a quadratic extension over K. The reduced trace and the reduced norm of h are simply the images of h by the operations trace and norm on $K(h)/K$. The conjugation and the identity are the K-automorphism of $K(h)$. Under the usual definition of the trace and the norm of a K-algebra [cf.Bourbaki[1]], the trace of H/K is $T = 2t$, The norm of H/K is $N = 2n$. We denote the group of the units in a ring X by $X^\times$.

Lemma 1.1.1. *The invertible elements in H are that with their reduced norm nontrivial. The reduced norm defines a multiplicative homomorphism from $H^\times$ into $K^\times$. The reduced trace is K-linear, and the mapping $(h,k) \mapsto t(hk)$ is a bilinear form non-degenerated on H.*

Proof. We leave the verification of the following very simple properties to reader as an exercise:
$n(hk) = n(h)n(k)$
$n(h) \neq 0$ is equivalent to The invertibility of h , and in this case $h^{-1} = \overline{h}n(h)^{-1}$,
$t(ah+bk) = at(h) + bt(k), t(hk) = t(kh)$, if $a, b \in K, and h, k \in H$.
The fact that the mapping $(h,k) \to t(hk)$ being non-degenerate comes from the assumption that L/K has been separable. In fact, if $t(hk) = 0$ whatever $k \in H$, we have $t(m_1 m = 0$ for every $m \in L$, if $h = m_1 + m_2 u$,then $m_1 = 0$. Similarly $t(m_2 m = 0$ for every $m \in L$, whence $m_2 = 0$ and $h = 0$. □

we note that, one of the advantage of the reduced trace is that, in the case of characteristic 2 the trace $T = 2t$ is zero, but the reduced trace is non-degenerate. In case characteristic not 2, we recover the classical definition of the quaternion algebra. the couple $\{L, \theta\}$ is equivalent with a couple $\{a, b\}$ formed by two nontrivial elements a, b in K and the relations (1) are determine H as the the K-algebra with basis $1, i, j, ij$, where the elements $i, j \in H$ satisfy

$$i^2 = a, j^2 = b, ij = -ji. \tag{1.3}$$

The transition between(1)and(3) carries out for example by setting $L = K(i), \theta = b, u = j$. Setting $k = ij$ one can write the table of multiplication of i, j, k , which shows these three elements acting symmetrically . The entities in the table are the products hh':

h\ h'	t	j	k
i	a	k	-j
j	-k	b	i
k	j	-i	-ab

The conjugation,the reduced trace, and the reduced norm have their expression as follows: if $h = x + yi + zj + tk$, then

$$\overline{h} = x - yi - zj - tk, t(h) = 2x, \quad \text{and } n(h) = x^2 - ay^2 - bz^2 + abt^2,$$

the coefficient of k in h should not be confused with the reduced trace. We notice the another important property: the reduced norm defines a quadratic form on the K-vector space V of the subjacent H.

We shall see that, the quaternion algebra H is defined by the relations(1) or (3) to the forms $\{L, \theta\}$ or $\{a, b\}$ when the case is permitted. we also shall consider these notation $u, i, j, t(h), \overline{h}$ as the standard notation.
The fundamental example of a quaternion algebra over K is given by the algebra $M(2, k)$, the matrices of 2 with entities in K. The reduced trace and the reduced norm are the trace and the determinant as the usual sense in $M(2, K)$. It can be identify K with its image in $M(2, K)$ of the K-homomorphism which convert the unit of K to the identity matrix. Explicitly if $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, K)$, $\overline{h} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, $t(h) = a + d$, $n(h) = ad - bc$. We are going to show that $M(2, k)$ satisfies the definition of a quaternion algebra as follows. We choose a matrix with a distinguish value, and set $L = K(m)$. Since $\overline{m}$ has the same distinguish value as m , it is similar to m.: there exists then an $u \in GL(2, k)$ such that $umu^{-1} = \overline{m}$. We verify that $t(u) = 0$, since $t(um) = t(u)m \in K$ for each $m \in L$,from this we deduce $u^2 = \theta \in K'$. In the following remark we are likely going to explain why is $M(2, K)$ the fundamental example:
Over a separably closed field, $M(2, K)$ is the unique quaternion algebra up to an isomorphism. In fact, every separable algebra of dimension 2 over K can not be a field sent by the norm on $K^\times$ surjectively, and being included in $M(2, k)$(an inclusion is an injective K-homomorphism). From this we derive that, it is isomorphic to $\{K + K, 1\} \simeq M(2, K)$ thanks to the realization of $M(2, K)$ as a quaternion algebra done above. tensor product. Let F be a commutative field containing K. We verify directly by the definition the tensor product of a quaternion algebra with F over K is a quaternion algebra over F, and that

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

. We write the obtained quaternion algebra by H_F too. The algebra H is included in H_F in a natural way. Taking the separable closure K_s of K as F we see that H is included in $M(2, K_s)$.

Definition 1.4. *The fields F/K such that H_F to be isomorphic to $M(2, F)$ is called the neutralized fields of H in $M(2, k)$. The inclusions of H in $M(2, F)$ is called the F-representations.*

Examples.
(1) The quaternion algebra over K has no any K-representation if it is not isomorphic to $M(2, K)$.
(2)We define the following matrices:
$I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $IJ = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. These matrices satisfy the relations (3) with $a = b = 1$. We derived from them in the case of characteristic unequal to 2, a quaternion algebra $\{a, b\}$ is isomorphic to

$$\{\begin{pmatrix} x + \sqrt{a}y & \sqrt{b}(z + \sqrt{a}t \\ \sqrt{b}(z - \sqrt{a}t) & x - \sqrt{a}y \end{pmatrix} | x, y, z, t \in K\},$$

where $\sqrt{a}$ and $\sqrt{b}$ are two roots of a and b in K_s .
(3) The quaternion field of Hamilton. Historically, the first quaternion algebra (different from a matrices algebra) was introduced by Hamilton. We denote

it by $\mathbb{H}$. It is the quaternion field defined over $\mathbb{R}$ with $a = b = -1$, called the quaternion field of Hamilton. It has a complex representation:

$$H = \begin{pmatrix} z & z' \\ -\overline{z'} & \overline{z} \end{pmatrix}, z, z' \in \mathbb{C}.$$

The group consisting of the quaternion with reduced norm 1 is isomorphic to $SU(2, \mathbb{C})$ and will be introduced for the geometric reason (cf. the §3 geometry). Sometimes we call these quaternions the generalized quaternions (compare with that of Hamilton) ,or hypercomplex numbers (perhaps it comes from the possible interpretation of the quaternions of Hamilton as a mixture of fields each being isomorphic to $\mathbb{C}$), but the general tendency is simply to say as quaternions.

Exercises

1. zero divisor. Assume H/K a quaternion algebra over a commutative field K. An element $x \in H$ is a zero divisor if and only if $x \neq 0$ and there exists $y \in H, \quad y \neq 0$ such that $xy = 0$. Prove x is a zero divisor if and only if $n(x) = 0$. Prove if H contains at least one zero divisor, then H contains a zero divisor which is separable over K.

2. Multiplication of the quadratic forms. Prove that the product of two sums of 2 square integers is a sum of 2 squares integers. Prove the same result for the sums of 4 squares. Does the result still valid for the sums of 8 squares? Concerning with the last question, one can define the quasi-quaternions(Zelinsky [1]) or bi-quaternions(Benneton [3],[4]), or octonions of Cayley(Bourba Algebra, ch. 3,p.176) and study their arithmetic.

3. (Benneton [2]). Find the properties of the following matrix A, and from these to show a method to construct the matrices having the same properties:
$$\begin{pmatrix} 17 & 7 & 4 & 0 \\ 6 & -14 & -1 & 11 \\ 5 & -3 & -16 & 8 \\ 2 & -10 & 9 & 13 \end{pmatrix}.$$

4. prove an algebra of the matrices $M(n, K)$ over a commutative field K is a K-central simple algebra

5. The mapping $(h, k) \rightarrow (t(h\overline{k})$ is a bilinear non-degenerate form on H (lemma 1.1).

6. underlinecharacteristic 2.If K is of char 2, then a quaternion algebra H/K is a central algebra of dimension 4 over K, such that there exists a couple $(a, b) \in K^\times \times K^\times$ and the elements $i, j \in H$ satisfying
$$i^2 + i = a, j^2 = b, ij = j(1 + i)$$
such that $H = K + Ki + Kj + Kij$.

1.2 The theorem of automorphisms and the neutralizing fields

In this section it includes the applications of the fundamental theorems in the central simple algebra to the quaternion algebra. these theorems can be found in Bourbaki[2], Reiner [1], Blanchard [1], Deuring [1]. As in the next two chapters, in this section we prefer to follow the book of Weil[1]. Let H/K be a quaternion algebra.

Theorem 1.2.1. *(Automorphisms, theorem of Skolem-Noether). Assume L, L' be two K-commutative algebra over K, contained in a quaternion algebra H/K. Then every K-isomorphism of L to L' can be extended to an inner automorphism of H. In particular, the K-automorphisms of H are inner automorphism.*

Recall that, the inner automorphism of H is an automorphism $k \mapsto hkh^{-1}, k \in H$, associated with the invertible elements $h \in H$. Before proving this important theorem, we are going to give a number of its applications.

Corollary 1.2.2. *For every separable quadratic algebra L/K contained in H, there exists $\theta \in K^\times$ such that $H = \{L, \theta\}$.*

. There is an element $u \in H^\times$ which induces on L the nontrivial K-automorphism by the inner automorphism. We verify that $t(u) = 0$ (cf. §3), then $u^2 = \theta \in K$. We have also realized H in the form $\{L, \theta\}$.

Corollary 1.2.3. . *The group $Aut(H)$ of the K-automorphisms of H is isomorphic to the quotient group $H^\times/K^\times$. If L satisfy the corollary 2.2, the subgroup $Aut(H, L)$ consisting of the automorphisms fixing L globally is isomorphism to $(L^\times \cup uL^\times)/K^\times$, therefore the subgroup of the automorphisms fixing L is isomorphism to $L^\times/K^\times$ exactly.*

.

Corollary 1.2.4. *(Characterization of matrix algebra) A quaternion algebra is either a field or isomorphic to a matrix algebra $M(2, K)$. The quaternion algebra $\{L, \theta\}$ is isomorphic to $M(2, K)$ if and only if L is not a field or if $\theta \in n(L)$.*

Proof. .If L is not a field, it is clear that L, θ is isomorphic to $M(2, K)$ (cf. the passage in §1 concerning with the quaternion algebras over the separably closed fields). We then suppose L is a field.We shall prove that, if H is not a field, then $\theta \in n(L)$. We choose an element $h = m_1 + m_2 u$ with reduced norm zero. We then have that $0 = n(m_1) + \theta n(m_2)$ and $n(m_1) = 0$ is equivalent to $n(m_2)$. Since L is a field, the property $h \neq 0$ implies both m_1, m_2 are not zero, therefore $\theta \in n(L)$. We shall show $\theta \in n(L)$ if and only if $\{L, \theta\}$ is isomorphic to $M(2, K)$. If $\theta \in n(L)$, it exists in H an element with its square being 1, but different from ± 1,and then a zero divisor. We choose in H a zero divisor which is separable over K (see exercise 1.1), and denote it by x. Set $L' = K(x)$. The corollary show us that $H = \{L', \theta'\}$. Since L' is not a field, H is isomorphic to $M(2, K)$. If $\theta \notin n(L)$, the non-zero elements of H have a non-zero reduced norm and H is a field. □

Corollary 1.2.5. *(Theorem of Frobenius) A non-commutative field containing $\mathbb{R}$ in its center, of finite dimension over $\mathbb{R}$, is isomorphic to the field of Hamilton quaternion $\mathbb{H}$.*

. The proof of the theorem relays on the fact that the field of complex numbers $\mathbb{C}$ is the unique commutative extension of finite dimension over the real field $\mathbb{R}$. The argument of the proof is similar essentially with that in the following corollary (over a finite field there is no any quaternion field). Assume $d \in D - \mathbb{R}$, the field $\mathbb{R}(d)$ is commutative, hence it is true for $\mathbb{R}(i)$ with $i^2 = -1$. It is different from D since it is not commutative. Suppose $d' \in D$, such that $\mathbb{R}(d') = \mathbb{R}(u)$ is different from $\mathbb{R}(i)$ and $u^2 = -1$. The new element u does not commute with i, and we can replace it by an element of zero trace: $j = iui + u$, such that $ij = -ji$. The field $\mathbb{R}(i, j)$ is isomorphic to the quaternion field of Hamilton, $\mathbb{H}$, and it is contained in D. If it is different from D again, by the same reason we are allowed to construct $d \in D$ but not belonging to$\mathbb{R}(i, j)$, such that $di = -id$ and $d^2 \in \mathbb{R}$. But then, dj commute with i, so belongs to $\mathbb{R}$. It is absurd.

Corollary 1.2.6. *(Theorem of Wedderburn).There is no any finite quaternion field.*

There is a weak form of the theorem of Wedderburn : every finite field is commutative. The proof for the special case gives well the idea of that in the general case. It uses the fact that every finite field $\mathbb{F}_q$ (the index q indicates the number of the elements of the field) has an extension of a given degree uniquely determined up to an isomorphism. If H is a quaternion field, its center is then a finite field $\mathbb{F}_q$, and all of its commutative maximum subfield are isomorphic to $\mathbb{F}_{q'}$, where $q' = q^2$. It allows us to write H as a finite union of the conjugates of $h\mathbb{F}_{q'}h^{-1}$. Let us compute the number of H : $q^4 = n(q^2 - q) + q$, where n is the number of the maximum commutative subfield of H. From (2), $n = (q^4 - 1)/2(q^2 - 1)$. It leads to a contradiction.

Now we show the theorem of automorphism. We begin to prove a preliminary result. If V is the vector space over K of the subjacent space H. We are going to determine the structure of the K-algebra $End(V)$ formed by the K-endomorphisms of V. We remind here that the tensor product is always taken over K if without a contrary mention.

Lemma 1.2.7. *The mapping of $H \otimes H$ to $End(V)$ given by $h \otimes h' \mapsto f(h \otimes h')$, where $f(h \otimes h')(x) = h \times \overline{h'}$, for $h, h', x \in H$, is an algebraic K-isomorphism.*

Proof. It is obvious that f is a K-homomorphism of K-vector spaces . The fact that the conjugation is an anti-isomorphism (i.e. $\overline{hk} = \overline{hk}, h, k \in H$) implies that f is a K-homomorphism as a K-algebra. Since the dimensions of $H \otimes H$ and $Edn(V)$ over K is equal, for showing f is a K-isomorphism it is sufficient to verify that f is injective. We can take an extension H_F of H such that H_F is isomorphic to $M(2, F)$. The extended mapping f_F is injective since it is not zero: its kernel (a two-sided ideal of $H_F \otimes_F H_F$) is zero since $H_F \otimes_F H_F$ is isomorphic to $M(4, F)$ which is simple (exercise 1.4). □

The proof of the theorem of automorphism. Let L be a commutative K-algebra contained in H but different from K, and let g is a non-trivial K-isomorphism of L to H. We want to prove that g is the restriction of an inner

K-automorphism of H. We can consider H as a left L-module by two ways: putting $m.h = mh$ or $m.h = g(m)h$ for $m \in L$ and $h \in H$. From this it follows there exists a K-endomorphism of V,denoted by z, such that $z(mh) = g(m)z(h)$. apply the Lemma 2.7,and write$z = f(x)$, where $x \in H \otimes H$. Fixing a base (b) of H/K so that there exist elements (a) of K ,uniquely determined, such that $x = \sum a \otimes b$. We obtain a relation $\sum amb\bar{b} - g(m)\sum ah\bar{b}$ which is equivalent to the relation $\sum(am - g(m)a)h\bar{b} = 0$, which is valid for all $m \in L$ and all $h \in H$. There is at least an element a non-zero. For this element, we have $am = g(m)a$, then the theorem would been proved if a is invertible. Now we prove that a is invertible. since $a \in L$,we have $H = L + aL$. It follows that Ha is a Two-sided ideal, since $HaH = HaL + HaaL \subset [Hg(L) + Hag(L)]a \subset Ha$. But H is simple, or the same it is sufficient to use that $H_F \simeq M(2, F)$ is simple(exercise 1.4) if F is a neutralized field. Therefore the non-zero ideal $H_F a$ equals to H_F. Hence a is invertible. Now we give the following important result but without proof. We shall prove it in the next two chapters, where K is a local field or a global field.

Theorem 1.2.8. *(neutralized field) Suppose L is a quadratic extension of K. Then L is a neutralized field of a quaternion algebra if and only if L is isomorphic to a maximal commutative sub-field of H.*

We recall that a extension of K is a commutative field containing K. The different inclusion of L in H will study in details when K is a local field or a global field (see the definition in the §4 too). We are going now to consider the tensor product over K of a quaternion algebra H/K with another quaternion algebra H'.

Theorem 1.2.9. *(tensor product) Let H/K and H'/K be two quaternion algebra. If H and H' have an isomorphic maximal commutative sub-field, then $H \otimes H$ is isomorphic to H" $\otimes M(2, K)$, where H" is a quaternion algebra over K uniquely determined up to isomorphisms.*

The above theorem allows one to define a group structure on the classes of isomorphisms of the quaternion algebras over K, if K possess the property: Two quaternion algebra over K always have an isomorphic commutative maximal sub-field. We shall see this property is valid for the local and global field. the group (if been defined) will be denoted by $Quat(K)$. It is a subgroup of index 2 in the Brauer group of H formed by the classes of the central algebra over K and equipped with the product induced by the tensor product. We shall verify in exercise the relation: $\{L.\theta\} \otimes \{L, \theta'\} \simeq \{L, |theta\theta'\} \otimes M(2, K)$. For the case of characteristic different from 2, one can read the book of Lam [1]. As for general case, see Blanchard [1], and the exercise III. 5,6.

Exercise

1. (Co-restriction) Let L/K be a separable extension of K of degree 2, and H/L be a quaternion algebra. To every K-inclusion $\sigma_i, 1 \leq i \leq n$, of L in K_s is associated with the algebra $H_i = H \otimes_L (K_s, \sigma_i)$ obtained by the scalar extension to K_s. Verify the followings :
   a) $D = \otimes_{i=1}{}^n H_i$ is a central simple algebra of dimension 4^n over K.

b)Every element τ in the group $Gal(K_s/K)$ of the K-automorphism of K_s induces a permutation r of $1, ..., n$:

$$\tau.\sigma_i = \sigma_{r(i)},$$

it is a K-isomorphism of H_i on $H_{r(i)}$, by the restriction of the mapping :

$$\tau(h \otimes k) = h \otimes \tau(k), h \in H, k \in K_s,$$

and a K-isomorphism of D.
c) The elements of D being invariant by $Gal(K_s/K)$ constitute a central simple algebra of dimension 4^n over K. The construction below proceeds naturally when H is a central simple L-algebra. The algebra constructed over K is denoted by $Cor_{L/K}(H)$. It corresponds to the co-restriction mapping under the cohomology interpretation of the Brauer groups.

2. Let L/K be a separable extension of K of degree 2, and $m \to \overline{m}$ be the nontrivial K-automorphism of L. Prove
a) The set $\{g = \begin{pmatrix} m & n \\ \overline{n} & \overline{m} \end{pmatrix}\}$ forms a K-algebra which is isomorphic to $M(2, K)$.
b) If g is invertible, prove that g^{-1} is conjugate to g by an element of the form $\begin{pmatrix} r & 0 \\ 0 & \overline{r} \end{pmatrix}$ with $r \in L^\star$.

1.3 Geometry

In this section we assume the characteristic of the field is different from 2. For every quaternion algebra H/K we use H_0 to denote the set of the quaternions with zero reduced trace. The reduced norm provides the K-vector space V, V_0, the subjacent spaces of H, H_0 respectively, a non-degenerate quadratic form. We denote the associated bilinear form by $< h, k >$ for $h, k \in V$ or v_0. It is defined by $< h, k >= t(h\overline{k}$, from it we deduce $< h, h >= 2n(h)$. If the elements h, k belong to V_0 we have a simple formula $< h, k >= -(hk + kh)$. We see also that the product of two elements of H_0 is an element of H_0 if and only if these elements anti-commute ($hk = -kh$), It is also equivalent to that, these two elements are orthogonal in H_0. We now study the quaternion algebra with the point of view of their quadratic spaces.

Lemma 1.3.1. *Let H, H' be two quaternion algebras over K, and $V, V_0, V'V'_0$ be the correspondent quadratic spaces respectively. The following properties are equivalent:*
(1) H and H' are isomorphic,
(2) V and V' are isomorphic.
(3) V_0 and V'_0 are isomorphism.

Proof. (1) implies (2), because an automorphism preserving the norm induces an isomorphism. (2) implies (3) by the theorem of Witt, and the the orthogonal decomposition $V = K + V_0$, which is deduced from (3) in §1. (3) implies (1), because an isometry preserves the orthogonality, hence if $i, j \in H$ satisfy (3) in §3, then $f(i)$ and $f(j)$ satisfy the same relations and $H = H'$. □

Corollary 1.3.2. *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 space, (4) the quadratic form ax^2+by^2 represents* 1.

Proof. (1) is equivalent to (2) comes from the characterization of matrix algebra considered in §1. (1) is equivalent to (3), it is clear too. (4) implies (1), since the element $ix+jy$ is of square 1 if $ax^2+by^2=1$, and it is different from ∓ 1 , then $H$is not a field.(3) implies (4) since if $ax^2+by^2-abz^2=0$ with $z\neq 0$,it is clear that ax^2+by^2 represent 1, and otherwise $b\in -aK^2$, and the quadratic form ax^2+by^2 is equivalent to $a(x^2-by^2)$ which represents 1. □

According to the theorem of Cartan (Dieudonné[1]), every isometries of a K vector space of finite dimension m equipped with a quadratic form is the product of at most m symmetries. The theorem shows that the proper isometries(i.e. of determinant 1) of V_0 are the products of two symmetries of V_0. The symmetry of V of a non isotropic vector q can be written as

$$h \to s_q(h) = h - qt(h\overline{q})/n(q) = -q\overline{h}\overline{q}^{-1}, h \in H$$

. If q,h are in V_0, this symmetry is simply defined by $s_q(h) = -qhq^{-1}$. The product of two symmetries s_q, s_r of V_0 is defined by $s_q s_r(h) = qrh(qr)^{-1}$. Conversely, we shall prove every inner automorphism of H induces on V_0 a proper isometry. If the isometry induces on V_0 by an inner automorphism is not proper, then there would exist $r \in H^\times$ such that for $x \in V_0$ the image of x equals $-rxr^{-1}$. We then deduce from this that $h \to r\overline{h}r^{-1}$ is an inner automorphism, it is absurd. We have proved the following theorem too.

Theorem 1.3.3. *The proper isometries of V_0 are obtained by the restriction of the inner automorphism of H to the quaternions with zero trace. The group of proper isometries of V_0 is isomorphic to $H^\times/K^\times$.*

The last assertion comes from corollary 2.3. By the same token we demonstrated a quaternion can be written as the product of two quaternions exactly by an element of K. The theorem allows us to rediscover some classical isomorphisms between the orthogonal groups and some quaternion groups. We denote the group $GL(2,K)/K^\times$ by $PGL(2,K)$; the proper isometric group of the quadratic form $x^2-y^2-z^2$ over K by $SO(1,2,K)$; the rotation group $SO(3,\mathbb{R})$ of $\mathbb{R}^{\not\perp}$ has a non-trivial covering of degree 2, denoted by $Spin(3,\mathbb{R})$. If H/K is a quaternion algebra, $\mathbb{H}^1$ denotes the kernel of the reduced norm.

Theorem 1.3.4. *We have the isomorphisms:*
1) $PGL(2,K) \simeq SO(1,2,K)$;

2) $SU(2,\mathbb{C})/\mp 1 \simeq SO(3,\mathbb{R})$;

3) $\mathbb{H}^1 \simeq Spin(3,\mathbb{R})$.

The proof of the isomorphisms 1) and 2) come immediately from the precedent theorem, the $\mathbb{C}$-representation of the the Hamilton quaternion field given in §1, and the isomorphism 3),which we are going to describe in detail(Coxeter [2]). We consider the Hamilton quaternions with reduced norm 1. In which those having zero traces can be identified with the vectors of length 1 of $\mathbb{R}^3$.

We now show the rotation $(r, 2\alpha)$ of the space $\mathbb{R}$ (identifying with the Hamilton quaternion of zero reduced trace) of angle 2α, and of the axis being carried out by a vector of r units, is induced by the inner automorphism associated with $q = \cos\alpha + r\sin\alpha$. In fact, we have $r^2 = -1$, and by the theorem 2.1 of automorphisms we can choose a quaternion $s \in H$ such that $s^2 = -1$ and $rs = -sr$. The pure quaternions form the $\mathbb{R}$-vector space with basis r, s, rs. Under this basis we shall verify the restriction of the inner automorphism induced by q to the quaternions with zero trace is the rotation defined above. We have:

$$(\cos\alpha + r\sin\alpha)r(\cos\alpha - rsin\alpha) = r,$$

$$(\cos\alpha + r\sin\alpha)s(\cos\alpha - r\sin\alpha) = \cos 2\alpha.s + \sin 2\alpha.rs,$$

$$(\cos\alpha + r\sin\alpha)s(\cos\alpha - r\sin\alpha) = \cos 2\alpha.rs - \sin 2\alpha.s.$$

We derive from this that $\mathbb{H}^1/\mp 1$ is isomorphic to $SO(3, \mathbb{R})$. We now show $\mathbb{H}^1$ is a non-trivial covering of $SO(3, \mathbb{R})$. Otherwise, $\mathbb{H}^1$ would contain a subgroup of index 2, hence distinguished. There would exist a surjective homomorphism c of $\mathbb{H}^1$ to ∓ 1. We shall see it is impossible. Since -1 is a square in $\mathbb{H}^1$, we have $c(-1) = 1$. All of the elements of square -1 being conjugated by an inner automorphism of $\mathbb{H}^1$, we have $c(i) - c(j) = c(ij)$ or i, j are defined as that in §1. From it we obtain $c(i) = 1$, and $c(x) = 1$ for every quaternion of square -1.

Because every quaternion of $\mathbb{H}^1$ is the product of two quaternions of square -1 and of a sign, we then deduce c equals 1 on $\mathbb{H}^1$ identically. We note that $\mathbb{H}^1/\mp 1$ being isomorphic to $SO(3, \mathbb{R})$ is a simple group. It is well-known that $PSL(2, K) = SL(2K)/\mp 1$ is a simple group if the field K is not a finite field consisting of 2 or 3 elements (Dieudonné,[1]). the property can not be generalized. The group $\mathbb{H}^1/\mp 1$ is not always simple. It can be found in Dieudonné an infinite number of examples where the groups are not simple. Put the following question: if K is a global field, and H/K a quaternion algebra such that for the completion of K_v of K, the group $H_v/\mp 1$ is simple(where $H_v = H \otimes K_v$), is $H_v/\mp 1$ a simple group? The group of commutator of a group G is the group generated by the elements of G of the form $uvu^{-1}v^{-1}$, $u, v \in G$. The group of commutator of $H^\times$ is then contained in $\mathbb{H}^1$

Proposition 1.3.5. *The group of the commutators of $H^\times$ equals H^1.*

Proof. Let h be a quaternion of reduced norm 1. If the algebra $K(h)$ is a separable quadratic algebra over K, the theorem 90 of Hilbert indicates there exists an element $x \in K(h)^\times$ such that $h = x\overline{x}^{-1}$. We can moreover verify this property directly: if $K(h)$ is a field, we choose $x = h+1$ if $h \neq -1$, and $x \in H_0^\times$; if $K(h)$ is not a field, it is isomorphic to $K + K$, and if $h = (a, b) \in K + K$ is of norm $ab = 1$, we then choose $x = (c, d)$ with $cd^{-1} = a$. Since $x, \overline{x}$ are conjugate by an inner automorphism (they satisfy the same minimal polynomial), we deduce from this that h is a commutator.
If $K(h)/K$ is not separable quadratic extension, we then have $h = \overline{h}$,hence $(h - 1)^2 = 0$. If H is a field, then $h = 1$, otherwise H is isomorphic to $M(2, K)$, and we would have the assertion: $SL(2K)$ is the group of commutator of $GL(2, K)$, cf. Dieudonneé[1]. □

The explanation of the group $\mathbb{H}^1/\mp 1$ as the group of rotations of $\mathbb{R}^3$ permits us to determine the structure of the finite groups of real quaternions as that of finite rotation groups(Coxeter,[1]).We start from recalling this well-known result about the structure of finite rotation groups.

Theorem 1.3.6. *The finite rotation group in $\mathbb{R}^3$ are (Coxeter,[1],ch.4):*
the cyclic group of order n,denoted by C_n,
the dihedral group of order 2n, denoted by D_n,
three exceptional groups: the tetrahedral group of order 12 being isomorphic to the alternating group A_4; the octahedral group of order 24 being isomorphic to the symmetry group S_4; and the icosahedral group of order 60 being isomorphic to alternating group A_5.

A finite group of real quaternions contains only the elements of reduced norm 1. If it does not contain -1, it is isomorphic to a finite rotation group not containing any rotation of angle π, cf. the proof of theorem 3.4. It is then is a cyclic group of order odd. If it contains -1, it is then the preimage of the mapping $(\cos\alpha + r\sin\alpha) \to r, 2\alpha)$ of a finite group of real quaternions. It is useful to have an explicit description for these groups: we get it by putting these regular polygons in a convenient mark, and using the geometric description of the groups.The elements $i, j, k, \in \mathbb{H}^1$ satisfying the classical relations $i^2 = -1, j^2 = -1, k = ij = -ji$, identify with an orthogonal basis of $\mathbb{R}^3$ and we put these polygons as indicating in the pictures. The origin is always the barycenter.

Here are two pictures!!!
fig.1 . . . fig.2 the regular tetrahedrons.

The dihedral group of order 2n(Fig 1): the rotation group of a regular polygon with n vertices, generated by the rotations $(i, 2\pi/n)$ and (j, π). The group A_4: the rotation group of a regular tetrahedron, formed by the identity, the rotations of angle $\mp 2\pi/3)$, around the line joining the vertex to the center of its opposite face as axis, and of angle π, around the line joining the centers of a pair of opposite edges as axis. The group of symmetry of tetrahedron is the symmetric group S_4 acting on its four vertices. The rotation group is isomorphic to alternating group A_4
The group S_4(Fig.3,4): the rotation group of a cube or of a regular dodecahedron. The group of cube is generated by the the group of its circumscribed tetrahedron and by the rotation of angle $\pi/4$ around the the line joining the centers of the opposite faces.
The rotation group of cube permuting the four diagonals is isomorphic to the symmetric group S_4.
The group A_5 (Fig. 5,6): The rotation group of a regular icosahedron or of a regular dodecahedron. the group of dodecahedron is generated by the group of the circumscribed tetrahedron and by the rotations of angle$2\pi/5$ around the lines joining the centers of the opposite faces.
The five vertices of the dodecahedron are the vertices of its inscribed tetrahedron. Each rotation is a even permutation of the 5 tetrahedron and the group of icosahedron is isomorphic to the alternating group A_5.

(there are four figures: fig.3, the cube; fig.4, the octahedron; fig.5,the icosahedral, and fig.6, the dodecahedral.)!!!

Theorem 1.3.7. *(The finite Group of real quaternion) The finite subgroup of $H^\times$ are conjugate to the following groups:*

(1) the cyclic groups of order n generated by $s_n = \cos(2\pi/n) + i\sin(2\pi/n)$.

(2)the group of order 4n generated by s_{2n} and j called dicyclic.

(3)the group of order 24, called the bilinear tetrahedral group,

$$E_{24} = \{\pm 1, \pm i, \pm j, \pm ij, \frac{\pm 1 \pm i \pm j \pm ij}{2}\}$$

.

(4)the group of order 48, called the bilinear octahedral group,

$$E_{24} \cup 2^{-\frac{1}{2}} x,$$

where x = all the sums or differences of the possible two distinct elements among $1, i, j, ij$.

(5) the group of order 120, called the bilinear icosahedral group, $E_{120} = E_{24} \cup 2^{-1}x$,,$x$ = all the product of an element of E_{24} and $+i, +\tau j, +\tau^{-1}ij$, where $\tau = (\sqrt{5}+1)/2$.

We obtain by the same reason the description of all the possible finite groups of quaternion algebra embedded in $\mathbb{H}$, i.e. such that the center K is embedded in $\mathbb{R}$, and $H_{\mathbb{R}} = \mathbb{H}$.

Generators and relations(Coxeter [2],pp.67-68). Let (p, q, r) be the group defined By

$$x^p = y^q = z^r = xyz = 1.$$

the group is finite for $(2, 2, n), (2, 3, 3), (2, 3, 4), (2, 3, 5)$ and isomorphic to the rotation groups D_n, A_4, S_4, A_5. Using the correspondence $1 \leftrightarrow 2$ given by the mapping $(\cos\alpha + r\sin\alpha) \to (r, 2\alpha)$ which was defined in the proof of theorem 3.4, we see that the group $< p, q, r >$ defined by

$$x^p = y^q = z^r = xyz = u, u^2 = 1$$

has the following special cases: the dicyclic group $< 2, 2, n >$ of order $4n$, the bilinear tetrahedral group $< 2, 3, 3 >$ of order 24, the bilinear octahedral group $< 2, 3, 4 >$ of order 48, the bilinear icosahedral group $< 2, 3, 5 >$ of order 120.

Proposition 1.3.8. *(Classical isomorphisms). The bilinear tetrahedral group is isomorphic to the group $SL(2, \mathbb{F}_3)$. The bilinear icosahedral group is isomorphic to the group $SL(2, \mathbb{F}_5)$*

We shall prove this isomorphism in Ch.V,§3.

Exercises

1. The isotropic group of the finite quaternion group)(Vigneras[3]). Let K is a finite extension of $\mathbb{Q}$ and H/K is a quaternion algebra having an inclusion in $\mathbb{H}$. The group $H^\times$acts on H^1 by inner automorphism. Prove

the isotropic groups in $H^\times$ of the finite subgroup of H^1 are given in the following table:

group	isotropic group
cyclic $< s_n >, n > 2$	$< K(s_n)^\times, t_n >$ where $t_n s_n = s_n^{-1} t_n, t_n \in H^\times$
dicyclic $< s_{2n}, j?, n \leq 2$	$< s_{2n}, j, 1 + s_{2n}, K^\times >$
binary tetrahedral $E_{24}, or < i, j >$	$< K^\times E_{24}, 1 + i >$
binary octahedral E_{48}	$K^\times E_{48}$
binary icosahedral E_{120}	$K^\times E_{120}$

2. The order of the elements of the finite quaternion group. 1)Prove the elements in quaternion group of order 4n which are generated by s^{2n} and j has the form $s_{2n}^t j$, where $0 \leq t \leq 2n-1$ is always of order 4. 2)Find in the bilinear groups E_{24}, E_{48}, E_{120} the number of elements with a given order(it suffices to notice that the elements with reduced trace 0, respectively $,-1, 1, \pm\sqrt{2}.\tau or - \tau^{-1}, \tau^{-1} or - \tau$, are of order 4, respectively, 3, 6, 8, 5, 10). 3)Deduce from 2) that the bilinear octahedral group E_{48} is not an isomorphic to the group $GL(2, \mathbb{F}_3)$ of order 48. [1]

3. a characterization of the quaternion fields (Van Praag[1]). prove, if H is a quaternion field with its center a commutative field K, then the set consisting of 0 and the elements $x \in H, x^2 \in K, \text{but} x \notin K$ is an additive group. Conversely, if H is a field of characteristic different from 2, such that the set mentioned above is a nonzero additive group, then H is a quaternion field.

4. The rotations of H (Dieudonné [2] or Bourbaki [3]). A rotation of H is a proper isometry of the subjacent quaternion space of H. prove every rotation of H is the mapping of the form:

$$u_{a,b} : x \to axb$$

, where a, b ar two quaternions such that $n(a)n(b) \neq 0$. Show that two notations $u_{a,b}$ and $u_{c,d}$ are equal if and only if $a = kc, b = k^{-1}d$, where k is a nonzero element of the center of H (suppose the characteristic is not 2).

1.4 Orders and ideals

The aim of this section is to give some definitions based on the orders, the ideals, and the reduced discriminants, which will be used in the subsequent chapters, where K is a local or global field. Our purpose is not to reestablish a frame of a theory on a Dedekind ring, but only make some definitions more precise, and these definitions will be adopted in sequel. For a more complete exposition one can consult the book of Reiner [1] or Deuring [1]. The notations used here are standard in the following chapters.
Let R be a Dedkind ring, i.e. a noetherian, integrally closed (hence integral) ring such that all of its nonzero prime ideals are maximal.
Examples: $\mathbb{Z}, \mathbb{Z}[\frac{1}{p}]$ for prime p, $\mathbb{Z}[i]$ and generally the integer ring of a local or

[1] This remark is made by Daniel Perrin friendly.

global field (ch.II and ch.III).
Let K be the fractional field of R and H/K be a quaternion algebra over K. In sequel of this section , we fix R, K, H.

Definition 1.5. *A R-lattice of a K-vector space V is a finitely generated R-module contained in V. A complete R-lattice of V is a R-lattice L of V such that $K \otimes_R L \simeq V$.*

Definition 1.6. *An element $x \in H$ is an integer (over R) if $R[x]$ is a R-lattice of H.*

Lemma 1.4.1. *(Bourbaki [1]) An element $x \in H$ is an integer if and only if its reduced trace and reduced norm belong to R.*

If an element is integer this lemma is valid. contrary to the commutative case, the sum and the product of two integers are not always integer: it is the source of several rings if we want to do some very explicit computation. It is not a surprise ,for example, in the case of $M(2, \mathbb{Q})$ the following matrices are integers:

$$\begin{pmatrix} \frac{1}{2} & -3 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{5} \\ 5 & 0 \end{pmatrix}$$

, but either their sum, nor their product are integer. The set of integers does not constitute a ring, and it leads us to consider some subrings of integers, called orders.

Definition 1.7. *An ideal of H is a complete R-lattice. An order $\mathcal{O}$ of H is :*
(1) an ideal which is a ring, or equivalently,
(2) a ring $\mathcal{O}$ consisting of integers and containing R, such that $K\mathcal{O} = H$.
A maximal order is an order which is not contained in any other order. An Eichler order is the intersection of two maximal orders.

There certainly exist some ideals, for example, the free R-module $L = R(a_i)$ generated by a basis $\{a_i\}$ of H/K. Let I be an ideal, it is associated canonically with two orders:

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

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

are called its left order and right order respectively. It is clear that such an order is a ring, an R-module, and a complete lattice because of that, if $a \in R \cap I, \mathcal{O}_l \subset a^{-1}I$ and if h is an element of H, it exists $b \in R$,such that $bhI \subset I$,so $H = K\mathcal{O}_l$.

Proposition 1.4.2. *(the properties of orders). The definitions (1) and (2) for order are equivalent.It does exist orders. Every order is contained in a maximal order.*

Proof. The definition (2) shows that every order is contained in a maximal order. It is clear that (1) implies (2). inversely, Let a_i be a basis of H/K contained in $\mathcal{O}$. An element h of $\mathcal{O}$ can be written as $h = \sum x_i a_i, x_i \in K$. Since $\mathcal{O}$ is a ring, so $ha_i \in \mathcal{O}$ and $t(ha_i) = \sum x_j t(a_i a_j) \in R$. The Cramer rule implies that $L \subset \mathcal{O} \subset dL$ where $d^{-1} = det(t(a_i a_j)) \neq 0$. From this we obtain that $\mathcal{O}$ is an ideal, hence (1) implies (2). □

Definition 1.8. . *We say that the ideal I is to the left of $\mathcal{O}_l$, to the right of $\mathcal{O}_r$, two-sided 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 in $\mathcal{O}_r$, principal if $I = \mathcal{O}_l h = h\mathcal{O}_r$ Its inverse is $I^{-1} = h \in H | IhI \subset I$.*

The product IJ of two ideals I and J is the set of the finite sum of the elements hk, where $h \in I, k \in J$. It is evident that the product IJ of two ideals is an ideal too.

Lemma 1.4.3. *(1)The product of ideals is associative.*
(2) The ideal I is integral if and only if it is contained in one of its orders.
(3) The inverse of an ideal I is an ideal I^{-1} satisfying

$$\mathcal{O}_l(I^{-1}) \supset \mathcal{O}_r(I), \mathcal{O}_r(I^{-1}) \supset \mathcal{O}_l(I)$$

,

$$II^{-1} \subset \mathcal{O}_l(I), I^{-1}I \subset \mathcal{O}_r(I)$$

.

Proof. (1) is clear,since the product in H is associative.
(2)$I \subset \mathcal{O}_l$ implies $II \subset I$ hence $I \subset \mathcal{O}_r$.
(3) Let $m \in R^\times$ such that $mI \subset \mathcal{O}_l \subset m^{-1}I$. We have on one side $I.m\mathcal{O}_l.I \subset \mathcal{O}_l I = I$ hence $m\mathcal{O}_l \subset I^{-1}$ and on other side $m^{-1}II^{-1}m^{-1}I \subset m^{-2}I$ hence $I^{-1} \subset m^{-2}I$. From this we obtain I^{-1} is an ideal. Therefore $I\mathcal{O}_r I^{-1}\mathcal{O}_l I \subset I$ hence $\mathcal{O}_l(I^{-1}) \supset \mathcal{O}_r$ and $\mathcal{O}_r(I^{-1} \supset \mathcal{O}_l$. We have $II^{-1}I \subset I$ then $II^{-1} \subset \mathcal{O}_l$, and $I^{-1}I \subset \mathcal{O}_r$. □

properties of the principal ideals
Let $\mathcal{O}$ be an order, and $I = \mathcal{O}h$ is a principal ideal. The left order of I equals the order $\mathcal{O}$, and its right order $\mathcal{O}'$ is the order $h^{-1}\mathcal{O}h$. We have then $I = h\mathcal{O}$ too. We consider a principal ideal $I' = \mathcal{O}h'$ of the left order $\mathcal{O}'$. We have

$$I^{-1} = h^{-1}\mathcal{O} = \mathcal{O}'h^{-1}$$

,

$$II^{-1} = \mathcal{O}, I^{-1}I = \mathcal{O}',$$
$$I' = \mathcal{O}hh' = hh'\mathcal{O}''$$

where $\mathcal{O}'' = h'^{-1}\mathcal{O}'h'$ is the right order of I'.
We then have the multiplicative rule as follows.

$$\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1}), \mathcal{O}_r(I) = \mathcal{O}_l(I^{-1}) = I^{-1}I$$

,

$$\mathcal{O}_l(IJ) = \mathcal{O}_l(I), \mathcal{O}_r(IJ) = \mathcal{O}_r(J), (IJ)^{-1} = J^{-1}I^{-1}$$

. We assume afterwards that the multiplicative rule above are satisfied for the orders and the ideals in consideration. It is always the case which we are interested in.

Definition 1.9. *The product IJ of two ideals I and J is a coherent product, if $\mathcal{O}_l(J) = \mathcal{O}_r(I)$.*

Assume I, J, C, D to be four ideals such that the products CJ, JD to be coherent. Therefore the equality $I = CJ = JD$ is equivalent to $C = IJ^{-1}$ and $D = J^{-1}I$.

Lemma 1.4.4. *The relation $I \subset J$ is equivalent to $I = Cj$ and to $I = JD$, where C and D are the integral ideals and the products are coherent.*

We suppose afterwards that every product of ideals is coherent. two-sided ideals

Definition 1.10. *Let $\mathcal{O}$ be an order. We call a two-sided, integral, ideal P being different from $\mathcal{O}$ a prime if it is non-zero, and if the inclusion $IJ \subset P$ implies $I \subset P$ or $J \subset P$, for any two integral two-sided ideals I, J of $\mathcal{O}$.*

Theorem 1.4.5. *The two-sided ideals of $\mathcal{O}$ constitute a group which is freely generated by the prime ideals.*

Proof. The multiplicative rule shows that if I, J are two two-sided ideal of $\mathcal{O}$ such that $I \subset J$, then IJ^{-1} and $J^{-1}I$ are integral and two-sided. If I is a two-sided ideal, and if it is contained in an ideal $J \neq I$, we shall have consequently $I = JI'$ where I' is integral, two-sided, and contains I strictly. Since $\mathcal{O}$ is a R-module of finite type, each strictly decreasing chain of ideals is finite. We shall have proved the factorization of the two-sided integral ideal of $\mathcal{O}$, if we prove that an ideal which is not strictly contained in any ideal different from $\mathcal{O}$ is a prime. Let I is such an ideal and J, J' be two integral two-sided ideals of $\mathcal{O}$ such that $JJ' \subset I$. If $J \nsubseteq I$, the ideal $I + J$ contains strictly I, and hence equals $\mathcal{O}$. We have $IJ' + JJ' = J'$, then $J' \subset I$. We from this deduce that I is a prime ideal. Inversely, a prime ideal is not contained strictly in any integral two-sided ideal which is different from $\mathcal{O}$. Because, if P is a prime ideal, and I is an integral two-sided ideal of $\mathcal{O}$, such that $P \subset I$, we have then $P = I(I^{-1}P)$, where $J = I^{-1}P$ is an integral two-sided ideal. ¿From this it follows $J \subset P$, It is absurd. Therefore we obtain that, if Q is another prime ideal, $QP = PQ'$ (applying the process of factorization), where $Q \subset Q'$ and hence $Q' = Q$. The product of two two-sided ideals is then commutative. We see immediately, the factorization is unique (the fact that if a product of two-sided ideals is contained in a prime ideal$P$, then at least one of the factors of the product equals P). The theorem has been proved. □

Let I be the ideal to the left of $\mathcal{O}$, and P is a prime ideal of $\mathcal{O}$. the product $I^{-1}PI$ is a two-sided ideal of the order to the right of I. We denote the order by $\mathcal{O}'$. If I is a two-sided ideal, then $I^{-1}PI = P$. Otherwise, $\mathcal{O}' \neq \mathcal{O}$, and the ideal $P' = I^{-1}PI$ is a prime ideal of $\mathcal{O}'$. The verification is immediate. In order to prove P' is prime, it suffices to utilize the two-sided ideals with form $I^{-1}JI$, where J is a two-sided ideal of $\mathcal{O}$, and to apply the definition of the prime ideal. As for showing that P' is independent of I, it suffices to use the fact that the ideal to the left of $\mathcal{O}$ and to the right of $\mathcal{O}'$ can be write as IJ' or JI, where J' is a two-sided ideal of $\mathcal{O}'$ and J is a two-sided ideal of $\mathcal{O}$.

Definition 1.11. *An order $\mathcal{O}'$ is said to be tied to $\mathcal{O}$ if it is the right order of an ideal which is to the left of $\mathcal{O}$. The model of the two-sided ideal J of $\mathcal{O}$ is the set of ideals of form $I^{-1}JI$, where I runs through all the ideals to the left of $\mathcal{O}$.*

Under the notations of the precedent definitions, we have $PI = IP'$, the orders $\mathcal{O}'$, $\mathcal{O}$ are tied, and the prime two-sided ideals P, P' belong to the same model. We denote the model of P by (P), and define the product $(P)I$ by setting $(P) = PI = IP'$. We see at once the product is commutative: $(P)I = I(P)$.

Proposition 1.4.6. *The product of a two-sided ideal J by an ideal I equals the product $JI = IJ'$, where J' is a two-sided ideal belonging to the model of J.*

. For example, the maximal orders are tied each other, and the normal ideal commute with the models of the normal two-sided ideals.
Properties of the non two-sided ideal.
Let $\mathcal{O}$ be an order. An integral ideal P to the left order $\mathcal{O}$ is said to be irreducible if it is nonzero, different from $\mathcal{O}$, and maximal for the inclusion in the set of the integral ideals to the left of the order $\mathcal{O}$.
We leave the verification of the following properties (they had been proved in Deuring [1], or Reiner [1])as an exercise :
1) P is a maximal ideal in the set of the integral ideal to the right of $\mathcal{O}_r(P)$.
2) If $\mathcal{O}$ is a maximal order, P contains a unique two-sided ideal of $\mathcal{O}$.
3) If $M = \mathcal{O}/P$, the ideal $I = x \in \mathcal{O}, xM = 0$, the annihilator of M in $\mathcal{O}$, is a two-sided ideal contained in P (assuming $\mathcal{O}$ to be maximal).
4) an integral ideal is a product of irreducible ideals.

Definition 1.12. *The reduced norm $n(I)$ of an ideal I is the fractional ideal of R generated by the reduced norms of its elements.*

If $I = \mathcal{O}h$ is a principal ideal, $n(I) = Rn(h)$. If $J = \mathcal{O}'h'$ is a principal ideal, to the left of the order $\mathcal{O}' = h^{-1}\mathcal{O}h$, then we have $IJ = \mathcal{O}hh'$ and $n(IJ) = n(I)n(J)$. the last relation remains valid for the non-principal ideals. For proof it can be utilized that an ideal is finitely generated over R. One can find the proof in Reiner's or just to do as an exercise.For the ideals we shall consider in the following chapters (principal or locally principal), the the multiplicative of the norm of ideal can be derived from the multiplicative of the norm over the principal ideals.
Different and discriminant

Definition 1.13. *The different $\mathcal{O}^{\star -1}$ of an order $\mathcal{O}$ is the inverse of the dual of $\mathcal{O}$ by the bilinear form induced by the reduced trace: $\mathcal{O}^\star = \{x \in H, t(x\mathcal{O}) \subset R\}$. Its reduced norm $n(\mathcal{O}^{\star -1})$ is called the reduced discriminant of $\mathcal{O}$, denoted by $D(\mathcal{O})$.*

We have the following lemma.

Lemma 1.4.7. *(1) Let I be an ideal. The set $I^\star = \{x \in H, |t(xy) \in R, \forall y \in I\}$ is a two-sided ideal.*
(2) Let $\mathcal{O}$ be an order. The ideal $\mathcal{O}^{\star -1}$ is an integral two-sided ideal.
(3) If $\mathcal{O}$ is a free R-module with basis (u_i) and a principal ring, then $n(\mathcal{O}^{\star -1})^2 = R(det(t(u_i u_j))$.

Proof. (1) It is clear, $I^\star$ is a R-module . By the analogy with what we used in the proof of the equivalence of that two definition of orders (prop. 4.1), we can prove there exists $d \in R$ such that $d\mathcal{O} \subset I^\star \subset d^{-1}\mathcal{O}$, thus $I^\star$ is an ideal. Its left order $\{x \in H|t(xI^{star}I) \subset R\}$ equals its right order $\{x \in H|t(I^\star xI)\}$,

because of $t(xy) = t(yx)$.
(2) Since $1 \in \mathcal{O}^\star$, we have $\mathcal{O}^\star\mathcal{O}^{\star -1} \supset \mathcal{O}^{\star -1}$.
(3) $\mathcal{O}^\star$ is an ideal generated over R by the dual basis $u_i^\star$ defined by $t(u_iu_j) = 1$ if $i = j$, and 0 if $i \neq j$. If $u_i^\star = \sum a_{ij}u_j$, then $t(u_iu_j^\star = \sum a_{jk}t(u_iu_k)$. From this we have $det(t(u_iu_j^\star)) = det(a_{ij})det(t(u_iu_j))$. On the other side, $\mathcal{O}^\star = \mathcal{O}x, x \in H^\times$, because $\mathcal{O}$ is principal, and then (u_ix) is the another basis of the R-module $\mathcal{O}^\star$. Since $n(x)^2$ is the determinant of the endomorphism $x \to hx$, cf.,§1, we then have $det(a_{ij}) = n(x)^2u, u \in R^\times$. it follows $R(det(t(u_iu_j))) = n(\mathcal{O}^\star)^{-2} = n(\mathcal{O}^{\star -1})^2$. The property (3) is even true if $\mathcal{O}$ is not principal. We leave the proof of it as an exercise. □

Corollary 1.4.8. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders. If $\mathcal{O}' \subset \mathcal{O}$, then $d(\mathcal{O}') \subset d(\mathcal{O})$, and $d(\mathcal{O}') = d(\mathcal{O})$ implies $\mathcal{O}' = \mathcal{O}$.*

Proof. If $v_i = \sum a_{ij}u_j$, we have $det(t(v_iv_j)) = (det(a_{ij}))^2det(t(u_iu_j))$. □

The corollary is very useful for understanding the case when an order is maximal.
Examples:
(1) The order $M(2, R)$ in $M(2, K)$ is maximal because its reduced discriminant equals R.
(2) In the quaternion algebra $H = \{-1, -1\}$ defined over $\mathbb{Q}$ (cf. §1), the order $\mathbb{Z}(1, i, j, ij)$ with reduced discriminant $4\mathbb{Z}$ is not maximal. It is contained in the order $\mathbb{Z}(1, i, j, (1 + i + j + ij)/2)$ with discriminant $2\mathbb{Z}$, which is maximal as we shall see in chapter III, or as one can verifies it easily.
Ideal class

Definition 1.14. *Two ideals are equivalent by right if and only if $I = Jh, h \in H^\times$. The class of the ideals to the left of an order $\mathcal{O}$ is called the class to the left of $\mathcal{O}$. We define by the evident way the class to the right of $\mathcal{O}$.*

The following properties can be verified easily:

Lemma 1.4.9. *(1) The mapping $I \to I^{-1}$ induces a bijection between the class to the left and the class to the right of $\mathcal{O}$.*
(2)Let J be an ideal. The mapping $I \to JI$ induces a bijection between the class to the left of $\mathcal{O}_l(I) = \mathcal{O}_r(J)$ and the class to the left of $\mathcal{O}_l(J)$.

Definition 1.15. *The number of class, (the class number), of the ideals related to a given order $\mathcal{O}$ is the number of classes (finite or not) of the ideals to the left (or to the right) of an arbitrary one of these orders .The class number of H is the number of classes of maximal orders.*

Definition 1.16. *Two orders being conjugate by an inner automorphism of H are said to have a same type.*

Lemma 1.4.10. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders. The following properties are equivalent.*
(1 $\mathcal{O}$ and $\mathcal{O}'$ are of the sane type.
(2) $\mathcal{O}$ and $\mathcal{O}'$ are tied by a principal ideal.

(3)$\mathcal{O}$ and $\mathcal{O}'$ are tied, and if I, J are the ideals having the left order $\mathcal{O}$ and the right order $\mathcal{O}'$ respectively, we have $I = J(A)h$, where $h \in H$ and (A) is a model of two-sided ideal of $\mathcal{O}$.

Proof. If $\mathcal{O}' = h^{-1}\mathcal{O}h$, the principal ideal $\mathcal{O}h$ ties $\mathcal{O}$ to $\mathcal{O}'$ and reciprocally. If $\mathcal{O}' = h^{-1}\mathcal{O}h$, then $J^{-1}Ih$ is a two-sided ideal of $\mathcal{O}'$. Inversely, if $\mathcal{O}$ and $\mathcal{O}'$ are tied, and if I and J satisfy the conditions of (3), then $\mathcal{O}' = J^{-1}J = h\mathcal{O}h^{-1}$. □

Corollary 1.4.11. *The number of the orders of type t which are related to a given order is less than or equal to the class number h of this order, if h is finite.*

The number of order type of H is the number of the maximal order type.

Definition 1.17. *Let L/K be a separable algebra of dimension 2 over K. let B be a R-order of L and $\mathcal{O}$be a R-order of H. An inclusion $f : L \to H$ is a maximal inclusion respect to $\mathcal{O}/B$ if $f(L) \cap \mathcal{O} = B$.Since the restriction of f to B determines f, we also say that f is a maximal inclusion of B in $\mathcal{O}$.*

Suppose $L = K(h)$ to be contained in H. By theorem 2.1 the conjugate class of h in $H^\times$

$$C(h) = \{xhx^{-1} | x \in H^\times\}$$

corresponds bijectively to the set of the inclusions of L to H. We also have

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

. The set of maximal inclusions of B to $\mathcal{O}$ corresponds bijectively to a subset of the conjugate class of $h \in H^\times$ which equals

$$C(h, B) = \{xhx^{-1} | x \in H^\times, K(xhx^{-1}) \cap \mathcal{O} = xBx^{-1}\}$$

and we have the disjoint union

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

where B runs through the orders of L. Consider a subgroup G of the normalization of $\mathcal{O}$ in $H^\times$:

$$N(\mathcal{O}) = \{x \in H^\times | x\mathcal{O}x^{-1} = \mathcal{O}.$$

For $x \in H^\times$, we denote $\tilde{x} : y \to xyx^{-1}$ the inner automorphism of H associated with x, and $\tilde{G} = \{\tilde{x} | x \in G\}$. The set $C(h, B)$ is stable under the right operation of $\tilde{G}$.

Definition 1.18. *. A maximal inclusion class of B in $\mathcal{O}$ mod G is the class of maximal inclusion of B in $\mathcal{O}$ under the equivalent relation $f = \tilde{x}f''$ $\tilde{x} \in \tilde{G}$. The conjugate class mod G of $h \in H^\otimes$ is $C_G(h) = \{xhx^{-1} | x \in G\}$.*

We see also that the set of conjugate class mod$G$ of the elements $x \in H$ such that $t(h) = t(x), n(x) = n(h)$ is equal to

$$\tilde{G}\backslash C(h) = \bigcup_B \tilde{G}\backslash C(h, B)$$

. In particular if $Card(\tilde{G}\backslash C(h,B)$ is finite and is zero for almost every order $B \subset L$, then we have

$$Card(\tilde{G}\backslash C(h)) = \sum_B Card(\tilde{G}\backslash C(h,B)).$$

The relation is useful for every explicit computation of the conjugate classes: the trace of Heck operators(Shimizu [2]), class number of ideal or of the type number of order(ch.V), the number of conjugate class of a quaternion group of reduced norm 1 and of a given reduced trace (ch.IV).

The group of units of an order.

The unit of an order is the invertible element which and its inverse both are contained in the order. They constitutes naturally a group denoted by $\mathcal{O}^\times$. The units of reduced norm 1 form a group too denoted by $\mathcal{O}^1$.

Lemma 1.4.12. *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} belong to $\mathcal{O}$, then $n(x), n(x^{-1} = n(x)^{-1}$ are in R. Inversely, if $x \in \mathcal{O}$, and $n(x)^{-1} \in R$, we then have $x^{-1} = n(x)^{-1}\overline{x} \in \mathcal{O}$, because $\overline{x} \in \mathcal{O}$ □

Exercises

1. Prove, if the right order of an ideal is maximal, then its left order is maximal too. From this deduce that a maximal order is such an order which ties to one of the other orders.

2. Prove, if R is principal, the order $M(2,R)$ is principal. Deduce from it that the maximal orders of $M(2,K)$ are all conjugate each other, i.e. of the same type.

3. Let H be a quaternion algebra $\{-1,-1\}$ over $\mathbb{Q}$ (cf. §1). Prove there exists in an integral ideal an element of minimal reduced norm. Prove, if $h \in H$, there exists $x \in \mathbb{Z}(1,i,j,ij)$ such that $n(x-h) \leq 1$, and even in some case $x(n-h) < 1$. Deduce from it that $\mathbb{Z}(1,i,j,(1+i+j+(1+i+j+ij)/2)$ is principal.

4. Theorem of four squares(Lagrange). Every integer is a sum of 4 squares. Using 4.3 prove it. You can firstly verify the set of the sums of 4 squares in $\mathbb{Z}$ is stable under multiplication, then every prime number is the sum of 4 squares.

5. Abelian variety(Shimura [1]). Let H be a quaternion algebra over $\mathbb{Q}$ possessing a R-representation f. If $z \in \mathbb{C}$, and $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2,\mathbb{R})$, we use $e(z)$ to denote the column vector $\begin{pmatrix} z \\ 1 \end{pmatrix}$ and $x(z) = (az+b)(cz+d)^{-1}$. Let $\mathcal{O}$ be an order of H over $\mathbb{Z}$. For every $z \in \mathbb{C}$ with its imaginary part being positive strictly , set

$$D(z) = f(\mathcal{O})z = \{f(x)z | x \in \mathcal{O}\}.$$

Prove $D(z)$ is a lattice of $\mathbb{C}^2$, i.e. a discrete sub group of $\mathbb{C}^2$ of rank 4.
If $a \in H$ is an element with its square a^2 being a strictly negative rational number, we set $\hat{x} = a^{-1}\overline{x}a$ for $x \in H$. Prove that $x \mapsto \hat{x}$ is an involution of H, and that $t(x\hat{x})$is strictly positive if $x \neq 0$.
Show it is possible to define a bilinear $\mathbb{R}$-form $< x, y >$ over $\mathbb{C}$ such that$< f(x)z, f(y)z >= t(ax\bar{y})$ for all $x, y \in H$.
Verify there exists an integer $c \in \mathbb{N}$ such that $E(x, y) = c < x, y >$ is a riemannian form over the complex torus $\mathbb{C}^2/D(z)$, i.e.
– $E(x, y)$ is an integer for every $(x, y) \in D(z) \times D(z)$,
– $E(x, y) = -E(y, x)$,
– the $\mathbb{R}$-bilinear form $E(x, \sqrt{-1}y)$ is bilinear and positively definite in (x, y).
It is known that the existence of a riemannian form on a complex torus is equivalent to the existence of a structure of an abelian variety.

6. Normalization. Let H/K be a quaternion algebra, and $h \in H$. Demonstrate

   (1) $\mathcal{O}h$ is an ideal if and only if h is invertible.

   (2) $\mathcal{O}h$ is a two-sided ideal if and only if (1) is valid and $\mathcal{O}h = h\mathcal{O}$.

   (3) the normalization of $\mathcal{O}$ is the group consisting of the elements $h \in H$ such that $\mathcal{O}h$ is a two-sided ideal.

7. The equation of polynomials over quaternion(Beck [1]). Let H/K be a quaternion field, and $H[x]$ be the set of polynomials $P(x) = \sum a_i x^i$, where the coefficients $a_i$belong to H. $H[x]$ is equipped with a ring structure such that the indeterminate x commute with the coefficients.

   (a) Prove that every polynomial $P(x)$ can be factored in a unique way as the product of a monic polynomial with coefficients in K, a constant in $H^\times$, and a monic polynomial of $H[x]$ which can not be divided by a non-unit polynomial in $K[x]$.

   (b) Prove that the equation $P(x) = 0$ has a solution of element $x = a$ belonging to K if and only if $x - a$ divides $P(x)$.

   (c) Show the coefficients of the polynomial $n(P) = \sum a_i \bar{a}_j x^{i+j}$ is in K. We call it thereduced norm of P.
   We want to find the solutions of the equation $P(x) = 0$ in H, then we study the associate solution in H of the equation $n(P)(x) = 0$. We can suppose P to be monic, and has no any solution in K, according what said above. If h is a Quaternion, we denote its minimal polynomial by P_h.

   (d) Prove that if P_h divides P, then every conjugation of h in H is the root of P. Particularly, the equation $P(x) = 0$ has an infinitely many solutions in H.

   (e) Prove that if P_h does not divide P, then the equation $P(x) = 0$ has at most a conjugation of h as a solution. This happens if and only if P_h divides $n(P)$.

(f) From it deduce that if $P(x)$ has only a finite number of roots, the number is less than or equal to the degree of P.

(g) Suppose H to be the field $\mathbb{H}$ of Hamilton quaternion. Prove that if $P(x)$ is not the polynomial 1, then $P(x) = 0$ always has a root in $\mathbb{H}$, and has an infinite number of roots if and only if $P(x)$ is divided by an irreducible polynomial with real coefficients of degree 2.

(h) Let $h_1, h_2, ..., h_r$ be the elements in H, but not belonging to$K$ and not conjugate pairwise, and $m_1, m_2, ..., m_r$ be the integers being greater than or equal to 1. We say that h is a root of $P(x)$ of multiplicity m if P_h^m divides $n(P)$, and P_h^{m+1} does not divide $n(P)$. Show if every m_i equals 1, there exists a unique monic polynomial $P(x)$, its roots are only these quaternions h_i $(1 \leq i \leq r)$ with multiplicity m_i, and the degree of $P(x)$ equals $m = \sum m_i$. If not the case, Prove there exists an infinitely many monic polynomials of degree m with this property.

Chapter 2

Quaternion algebra over a local field

In the chapter, K is a local field, in other words, a finite extension K/K' of a field K' called its prime subfield[1] are equal to one of the following fields:
– $\mathbb{R}$,the field of real numbers,
– $\mathbb{Q}_p$, the field of p-adic numbers,
– $\mathbb{F}_p[[T]]$, the field of formal series of one indeterminate over the finite field $\mathbb{F}_p$. The fields $\mathbb{R}, \mathbb{C}$ are called archimedean, the field $K \neq \mathbb{R}, \mathbb{C}$ are called non-archimedean.
If $K' \neq \mathbb{R}$. Let R be the integral ring of K and $\pi, k = R/\pi R$ be the uniform parameter and residue field respectively. We use L_{nr} to denote the unique quadratic extension of K in the separable closure K_s of K which is non ramified, i.e. satisfies one of the following equivalent properties:
(1) π is a uniform parameter of L_{nr},
(2) $R^\times = n(R_L^\times)$ where R_L is the integral ring of L_{nr},
(3) $[k_L : k] = 2$, where k_L is the residue field of L_{nr}.
Let H/K be a quaternion algebra. All of the notions about the orders and the ideals in H are relative to R.

2.1 Classification

The following theorem provides a very simple classification of the quaternion algebra over a field.

Theorem 2.1.1. *(Classification). Over a local field $K \neq \mathbb{C}$ there exists a quaternion field uniquely determined up to an isomorphism.*

We have seen in ch.1,§1 that $M(2, K)$ is the unique quaternion algebra over $\mathbb{C}$ up to isomorphism. The theorem of Frobenius implies this theorem in the case of $K = \mathbb{R}$. Before giving the proof of the theorem we give some application of it.

Definition 2.1. *We shall define an isomorphism ε of $Quat(K)$ to $\{\mp 1\}$ by setting for a quaternion algebra H/K, $\varepsilon(H) = -1$ if H is a field, $\varepsilon(H) = 1$*

[1] This notation for the prime subfield is not the usual one, but it will be used in the sequel.

otherwise. We call $\varepsilon(H)$ the Hasse invariant of H.
A variant of the above theorem is :

$$Quat(K) \simeq \{\mp 1\}, \text{ if } K \neq \mathbb{C},\ Quat(\mathbb{C}) \simeq \{1\}.$$

Definition 2.2. *If the characteristic of K is different from 2, and if $a, b \in K^\times$, the Hasse invariant of a, b is defined by*

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

where $H = \{a, b\}$ is the quaternion algebra described in Ch.I.(3). The Hilbert symbol of a, b is defined by

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

where the "non-trivial solution" means a solution $(x, y, z) \neq (0, 0, 0)$.

A variant of the above theorem in characteristic different from 2 is expressed as an equality between the Hilbert symbol and the Hasse invariant, and a variety of properties of Hilbert symbol deduced from it.

Corollary 2.1.2. *(Properties of Hilbert symbol). Let K is a local field of char. different from 2.Let $a, b, c, x, y \in K^\times$. The Hilbert symbol $\{a, b\}$ equals the Hasse invariant $\varepsilon(a, b)$. It satisfies the following properties:*
(1) $(ax^2, by^2) = (a, b)$ (modulo the square),
(2) $(a, b)(a, c) = (a, bc)$ (bilinearity),
(3) $(a, b) = (b, a)(symmetry)$,
(4)(a,1-a) = 1 (symbol),
(5) $(a, b) = 1$ for all $b \in K^\times$ implies $a \in K^{\times 2}$ (non degenerate),
(6)$(a, b) = 1$ is equivalent to one of the following properties:
$-a \in n(K(\sqrt{b}))$
or $b \in n(K(\sqrt{a}))$,
or $-ax^2 + by^2$ represents 1

Proof. The equation $ax^2 + by^2 - z^2 = 0$ has a non trivial solution in H^3 if and only if the quadratic vector space V_0 associated with pure quaternion of $\{a, b\}$ is isotropic. From ch.I, corollary 3.2, the space V_0 is isotropic if and only if $\{a, b\}$is isomorphic to a matrix algebra. Therefore $(a, b) = 1$ if and only if $\varepsilon(a, b) = 1$. it follows $(a, b) = \varepsilon(a, b)$. The properties (1),(2),(3),(4),(5),(6) are the consequence of the earlier results.
(1),(3): Define the elements i, j by the formula I.1.(3) and replace i, j by xi, yj, then by j, i.
(2). Use the tensor product(I,Thm 2.9).
(4),(6). Use the characterization of the matrix algebra (I,Corollary 2.4) and the geometric consideration (I,Corollary 3.2)
(5).Obtain from that, all the quadratic extension of K can be included in the quaternion field over K, if $K \neq \mathbb{C}$. This property will be proved more precisely later(II,Corollary 1.9). □

We suppose afterwards that $K \neq \mathbb{R}, \mathbb{C}$. The theorem of classification has the following very precise statement.

Theorem 2.1.3. *Let K be a non archimedean local field. then $H = \{L_{nr}, \pi\}$ is the unique quaternion field over K up to isomorphism. A finite extension F/K neutralize H if and only if its degree $[F : K]$ is even.*

The second part of the theorem is an easy consequence of the first part. It has two variants:
(1) H possess a F-representation if and only if $[F : K]$ is even.
(2) $\varepsilon(H_F) = \varepsilon(H)^{[F:K]}$.
The proof of the theorem is divided into several steps. Consider a quaternion field H/K. We extend a valuation v of K to a valuation w of H. it shows L_{nr} can be embedded in H. Using I.Corollary 2.2 and 2.4 we obtain $H \simeq \{L_{nr}, \pi\}$. The existence of the valuation w in addition gives the uniqueness of the maximal order and the group structure of the normal ideals. We are going now to proceed along this line. Reference: Serre [1].

Definition 2.3. *A discrete valuation on a field X [2] is a mapping $v : X^\times \to \mathbb{Z}$ satisfying*
(1) $v(xy) = v(x) + v(y)$,
(2) $v(x + y) \geq inf(v(x), v(y))$, with the equality if $v(x) \neq v(y)$ for every $x, y \in X^\times$. An element u which has a positive minimal valuation is called a uniform parameter of X. v can be extended to a mapping of 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 with v. Its unique prime ideal is $\mathcal{M} = Au = \{x \in X | v(x) > 0\}$. The field $A/\mathcal{M}$ is the residue field and the group $A^\times = \{x \in X | v(x) = 0\}$ is the unit group of A.

We choose a discrete valuation v of K; it can be suppose that $v(K^\times) = \mathbb{Z}$. We define a mapping $w : H^\times \to \mathbb{Z}$ by setting

$$w(h) = v \circ n(h), \tag{2.1}$$

where $h \in H^\times$ and $n : H^\times \to K^\times$ is the reduced norm. The multiplicative of the reduced norm (I,Lemma 1.1) implies w satisfies (1). We utilize a well known fact that the local commutative field being the restriction of w to L is a valuation if L/K is an extension of K contained in H. It follows then $w(h + k) - w(k) = w(hk^{-1} + 1) \geq inf(w(hk^{-1}), w(1)$ with the equality if $w(hk^{-1}) \neq w(1)$. From this we deduce that w satisfies (2). We have proved :

Lemma 2.1.4. *The mapping w is a discrete valuation of H.*

We denote the ring of the valuation W by $\mathcal{O}$. For every finite extension L/K contained in H, the intersection $\mathcal{O} \cap L$ is the ring of the valuation of the restriction of w to L. Therefore , $\mathcal{O} \cap L$ is the integral ring R_L of L. It follows that $\mathcal{O}$ is an order consisting of all the integers of of H. We then have

Lemma 2.1.5. *The ring $\mathcal{O}$ of valuation w is the unique maximal order of H.*

Therefore, we deduce that every normal ideal of H is Two-sided.If $u \in \mathcal{O}$ is a uniform parameter, $P = \mathcal{O}u$ is the unique prime ideal of $\mathcal{O}$. Thus the normal ideals are of the form P^n, $n \in \mathbb{Z}$.

Lemma 2.1.6. *The quadratic unramified extension L_{nr}/K of K is isometric to a commutative subfield of H.*

[2] not necessary to be a commutative field

Proof. We shall lead an absurdity. If L_{nr} was not contained in H, then for every $x \in \mathcal{O}, x \notin R$, the extension $K(x)/K$ would be ramified. There exists then $a \in R$ such that $x - a \in P \cap K(x)$. We could then write $x = a + uy$ with $y \in \mathcal{O}$. Iterating this procedure, the element x could be written as $\sum_{n\geq 0} a_n u^n$, $a_n \in R$. The field $K(u)$ being complete would be closed. We thus had $\mathcal{O} \subset K(u)$. It is absurd. □

Corollary 2.1.7. *The quaternion field H is isomorphic to $\{L_{nr}, \pi\}$.Its prime ideal $P + \mathcal{O}u$ satisfies $P^2 = \mathcal{O}\pi$. Its integer ring $\mathcal{O}$ is isomorphic to $R_L + R_L u$. The reduced discriminant $d(\mathcal{O})$ of $\mathcal{O}$ equals $n(P) = R\pi$.*

Proof. According to I, Corollary 2.2 and 2.4, we have $H \simeq \{L_{nr}, x\}$ where $x \in K^\times$ but $x \notin n(L_{nr}^\times)$. From (1), (2) of the beginning of this chapter it follows $x = \pi y^2$ where $y \in K^\times$. We can suppose $x = \pi$, then the first part of the corollary follows. Now suppose $H = \{L_{nr}, \pi\}$. The element $u \in H$ satisfying I.(1) is the non zero minimal valuation, thus $P = \mathcal{O}u$satisfies $P^2 = \mathcal{O}\pi$. The prime ideal $R\pi$ is then ramified in $\mathcal{O}$. according to Lemma 1.4, we have $\mathcal{O} = \{h \in H, n(h) \in R\}$. similarly, $R_L = \{m \in L_{nr}, n(m) \in R\}$. We can verify easily that, if $h = m_1 + m_2 u$ with $m_i \in L_{nr}$, the property $n(h) \in R$ is equivalent to $n(m_i) \in R$, $i = 1, 2$. We can show too that $\mathcal{O} = R_L + R_L u$. Using the formula involving the determinant in I, Lemma 4.7, we compute the reduced discriminant $d(\mathcal{O})$. Since $d(R_L) = R$, we see easily that $d(\mathcal{O}) = R\pi$. Hence it follows $d(\mathcal{O}) = n(P)$ or the different of $\mathcal{O}$ is $\mathcal{O}^{\star -1} = P$. □

Definition 2.4. *Let Y/X be a finite extension of field equipped with a valuation, and ring of it is $A_Y, A_X = X \cap A_Y$. Let P_Y, $P_X = P_Y \cap A_X$ be the prime ideals and k_X, k_Y be the corresponding residue field. The residue degree f of Y/X is the degree $[k_Y : k_X]$ of the residue extension k_Y/k_X. The ramification index of Y/X is the integer e such that $A_Y P_X = P_Y^e$.*

We then deduce that the unramified quadratic extension L_{nr}/K has the ramification index 1, and the residue degree 2. The quaternion field H/K has the ramification index 2, and the residue degree 2.
Let F/K be a finite extension of commutative field with ramification index e and residue degree f. We have $ef = [F : K]$ because the cardinal of k is finite and $R_F/\pi R_F \simeq R_F/{\pi_F}^e R_F$, if π_F is a uniform parameter of F.

Lemma 2.1.8. *The following properties are equivalent:*
(1) f is even,
(2) $F \supset L_{nr}$,
(3) $F \otimes L_{nr}$ in not a field.

Proof. For the equivalence (1) $\longleftrightarrow$ (2) see Serre [1],Ch. 1. For the equivalence (2) $\longleftrightarrow$ (3), it is convenient to write L_{nr} as the $K[X]/(P(X))$ where $(P(X))$ is a polynomial of degree 2. Thus $F \otimes L_{nr}$ equals $F[X]/(P(X))_F$ where $(P(X))_F$ is the ideal generated by $(P(X))$ in the polynomial ring $F[X]$. Since $P(X)$ is a polynomial of degree 2, it is reducible if and only if it admits a root in F, i.e. if $F \supset L_{nr}$.
Consider now $H_F \simeq \{F \otimes L_{nr}, \pi\}$. If π_F is a uniform parameter of F, it may as well suppose that $\pi = {\pi_F}^e$. According to I. Corollary 2.4, and Lemma 1, we find that, if e or f are even then we have $H_F \simeq M(2, F)$, hence F neutralizes H. Otherwise, that is to say if $[F : K]$ is odd, $H_F \simeq \{F \otimes L_{nr}, \pi_F\}$,where

$F \otimes L_{nr}$ is the unramified quadratic extension of F in K_s. Therefore H_F is a quaternion field over F. The Theorem 1.2 is proved completely. □

For the use latter we make a remark here.

Corollary 2.1.9. *Every quadratic extension of K is isomorphic to a subfield of H. For an order of a maximal commutative subfield of H can be embedded maximally in H, if and only if it is maximal.*

The computation of Hilbert symbol

Lemma 2.1.10. *If the characteristic of k is different from 2, and if e is a unit of R which is not a square, then the set $\{1, e, \pi, \pi e\}$ form a group of representations in $K^\times$ of $K^\times/K^{\times 2}$. Moreover L_{nr} is isomorphic to $K(\sqrt{e})$.*

Proof. Consider the diagram

$$\begin{array}{ccccccc} 1 \to & R_1^\times & \to & R^\times & \to & K^\times & \to \quad 1 \\ & \downarrow 2 & & \downarrow 2 & & \downarrow 2 & \\ & R_1^\times & \to & R^\times & \to & K^\times & \end{array}$$

The vertical arrows represent the homomorphism $h \to h^2$, and $R_1^\times = \{h = 1 + \pi a, a \in R\}$. We have $[k^\times : k^{\times 2}] = 2$, and $R_1^\times = R_1^{\times 2}$ because of

$$(1 + \pi a)^{\frac{1}{2}} = 1 + \pi a/2 + ... + C_n^{\frac{1}{2}} + ...$$

converges in K. Thus $[R^\times : R^{\times 2} = 2$, and $[K^\times : K^{\times 2}] = 4$. If $e \in R^\times - R^{\times 2}$, $R^\times \subset n(K(\sqrt{e}))$, and this characterize $L_{nr} = K(\sqrt{e})$. □

Set $\varepsilon = 1$ if -1 is a square in K, and $\varepsilon = -1$ otherwise.
Table of Hilbert symbol:

$a\backslash b$	1	e	π	πe
1	1	1	1	1
e	1	1	-1	-1
π	1	-1	ε	$-\varepsilon$
πe	1	-1	$-\varepsilon$	ε

Definition 2.5. *Let p be an odd prime number, and a be an integer prime to p. The Legendre symbol $(\frac{a}{p})$ is defined by*

$$(\frac{a}{p}) = \begin{cases} 1, & \text{if } a \text{ is a square mod } p \\ -1, & \text{otherwise} \end{cases}.$$

We see immediately that the Hilbert symbol $(a, p)_p$ of a, p in $\mathbb{Q}_p$ equals Legendre symbol $(\frac{a}{p})$. It is easy to compute Hilbert symbol $(a, b)_p$ of two integers a, b in $\mathbb{Q}_p$ if $p \neq 2$. We use the the computation rule of Hilbert symbol (Corollary 2.2) and

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

2.2 Study of $M(2, K)$

Let V be a vector space of dimension 2 over K. Suppose a basis (e_1, e_2) of V/K to be fixed such that $V = e_1K + e_2K$. This basis allowed us to identify $M(2, K)$ with the ring of endomorphisms $End(V)$ of V. If $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, K)$, it associates an endomorphism $:v \mapsto v.h$, which is defined by the product of the row matrix (x, y) by h, if $v = e_1x + e_2y$. Recall that a complete lattice in V is a R-module containing a basis of V/K. If L, M are two complete lattices in V, we denote the ring of R-endomorphisms from L to M by $End(L, M)$, or $End(L)$ if $L = M$.

Lemma 2.2.1. *(1) The maximal orders of $End(V)$ are the rings $End(L)$, where L runs through the complete lattices of V.*
(2) The normal ideals of $End(v)$ are the ideals $End(L, M)$, where L, M runs through the complete lattices of V.

Proof. (1) Let $\mathcal{O}$ be an order of $End(V)$ and M a complete lattice of V. Set $L = \{m \in M | m \in \mathcal{O}\}$. It is a R-module contained in V. There exists $a \in R$ such that $aEnd(M) \subset M\}$. It follows $aM \subset L \subset M$, hence L is a complete lattice. It is clear that $\mathcal{O} \subset End(L)$. (2) Let I be an ideal to the left of $End(L)$. We identify I to a R-module $f(I)$ of V^2 by the mapping $h \mapsto f(h) = (e_1h, e_2h)$. Let $x_{i,j}$be the endomorphism permuting e_1 and e_2 if $i \neq j$, but fixing e_i if $i = j$, and taking the other element of the basis to zero. Choosing all the possibility for (i, j), and computing $f(x_{i,j}$, we see that $f(I)$ contains $(e_1.h, 0), \quad (0, e_2.h) \quad (e_2h, e_1.h)$. Therefore $f(I) = M + M$ by putting $M = L.I$. We then see easily that M is a complete lattice. It follows finally $I = End(L, M)$. □

We recall here some classical results about the elementary theory of divisors.

Lemma 2.2.2. *Let $L \subset M$ be two complete lattices of V.*
(1) There exists a R-basis (f_1, f_2) of M and a R-basis $(f_1\pi^a, f_2\pi^b)$ of L whee a, b are integers uniquely determined.
(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 set U_m of the representation of $R/(\pi^m R)$ in R.

Proof. (1) is classical. We prove (2). The basis$f_1a + f_2b, f_1c + f_2d)$ of M are such that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies $L.A = M$. We can replace A by XA if $X \in M(2, R)^\times$. We verify without difficulty that it can be modified again to $A = \begin{pmatrix} \pi^n & r \\ 0 & \pi^m \end{pmatrix}$ where n, m are integers and $r \in U_m$ □

We are going to express these results in terms of matrix.

Theorem 2.2.3. *(1) The maximal orders of $M(2, K)$ are conjugate to $M(2, R)$.*
(2) The two-sided ideal of $M(2, R)$ forms a cyclic group generated by the prime ideal $P = M(2, R)\pi$.
(3)The integral ideals to the left of $M(2, R)$ are the distinct ideals

$$M(2, R) \begin{pmatrix} \pi^n & r \\ 0 & \pi^m \end{pmatrix}$$

where $n, m \in \mathbb{N}$ and $r \in U_m$, here U_m is a set of representation of $R/(\pi^m R)$ in R.
(4) The number of the integral ideals to the left of $M(2,R)$ with reduced norm $R\pi^d$ equals $1+q+...+q^d$, if q is the number of the elements of the residue field $k = R/(\pi R)$.

Definition 2.6. *Let $\mathcal{O} = End(L)$ and $\mathcal{O}' = End(M)$ be two maximal orders of $End(V)$, where L, M are two complete lattices of V. If x, y belong to $K^\times$, we have also $End(Lx) = \mathcal{O}$ and $End(My) = \mathcal{O}'$. It can then assume that $L \subset M$. There exists the 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. We call it the distance of two maximal orders $\mathcal{O}$ and $\mathcal{O}'$, denoted by $d(\mathcal{O}, \mathcal{O}')$.*

Example.
The distance of the maximal order $M(2,R)$ and $\begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix}$ equals n.
Eichler order

Definition 2.7. *A Eichler order of level $R\pi^n$ is the intersection of two maximal orders between them the distance is n. We write $\mathcal{O}_{\underline{n}}$ for the following Eichler order of level $R\pi^n$:*

$$\mathcal{O}_{\underline{n}} = M(2,R) \cap \begin{pmatrix} R & \pi^{-n}R \\ \pi^n R & R \end{pmatrix} = \begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}$$

An Eichler order of V is the form $\mathcal{O} = End(L) \cap End(M)$, where L, M are two complete lattice of V which can be assumed the forms $L = f_1R + f_2R$ and $M = f_1R + f_2\pi^n R$. It is also the set of endomorphisms $h \in End(L)$ such that $f_1.h \in f_1R + L\pi^n$. The properties in the next lemma explain the justification of the definition of the level of an Eichler order.

Lemma 2.2.4. *(Hijikata,[1]).Let $\mathcal{O}$ be an order of $M(2,K)$. The following properties are equivalent:*
(1) There exists uniquely a couple 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 which is conjugate to $\begin{pmatrix} R & 0 \\ 0 & R \end{pmatrix}$.

Proof. The implications of (1)→ (2)→ (3)→ (4) are evident. We now prove (4)→ (1). Let $\mathcal{O}$ be an order containing $\begin{pmatrix} R & R \\ \pi^n R & R \end{pmatrix}$. We verify easily that it has the form $\begin{pmatrix} R & \pi^a R \\ \pi^b R & R \end{pmatrix}$, with $a + b = m \geq 0$. A maximal order containing $\mathcal{O}$ has the form $\begin{pmatrix} R & \pi^c R \\ \pi^{-c} R & R \end{pmatrix}$ with $a - m \leq c \leq a$. One can convince himself easily that it exists at most two maximal orders containing $\mathcal{O}$ and corresponding to $c = a$ and $c = a - m$. □

Use $N(\mathcal{O})$ to denote the normalizer of an Eichler order $\mathcal{O}$ of $M(2,K)$ in $GL(2,K)$. 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 the maximal orders containing $\mathcal{O}$. The inner automorphism associating to an element of $N(\mathcal{O})$ fixes the couple $(\mathcal{O}_1, \mathcal{O}_2)$. The study of two-sided ideal of maximal order has showed that the two-sided ideal of a maximal order is generated by the nonzero elements of K. Hence it follows $\mathcal{O} = \mathcal{O}_{\underline{n}}$ with $n \geq 1$. therefore we see that $N(\mathcal{O}_{\underline{n}})$ is generated by $K^{\times}\mathcal{O}_{\underline{n}}{}^{\times}$ and $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$. We can verify without difficulty that the reduced discriminant of an Eichler order equals its level.

The tree of maximal order

Definition 2.8. *(Serre [3], Kurihara [1]). A graph is given by*
– a set $S(X)$ whose element is called a vertex of X,
– a set $Ar(X)$ whose element is called an edge of X,
– a mapping: $Ar(X) \to S(X) \times S(X)$ defined by $y \mapsto (s, s')$ where s is called the origin of y and s' the extremity of y,
– an involution of $Ar(X)$ denoted by $y \mapsto \bar{y}$ such that the origin of y to be the extremity of $\bar{y}$ and such that

$$y \neq \bar{y} \tag{1}$$

.
A chain of a graph X is a sequence of edges $(y_1, ..., y_{i+1}...)$ such that the extremity of y_i to be the origin of y_{i+1} for all i. To give a chain is equivalent to give a sequence of vertices such that two consecutive vertices to be always the origin and the extremity of an edge. A finite chain $(y_1, ..., y_n)$ is called to have the length n, and we say it joins the origin of y_1 and the extremity of y_n. A pair $(y_i, \bar{y_i})$ in a chain is called a loop. A finite chain without any loop such that the origin of y_1 to be the extremity of y_n is called a circuit. A graph is connect if it always exists a chain joining two distinct vertices. A tree is a connect graph and without circuit.

We see the set X of maximal orders of $M(2,K)$ is provided with a structure of graph denoted still by X , such that these maximal orders are the vertices of X and the pair $(\mathcal{O}, \mathcal{O}')$ of maximal orders of distance 1 are the edges of X.

Lemma 2.2.5. *Let $\mathcal{O}$ be a maximal order. The maximal orders at distance n to $\mathcal{O}$ are the extremities of some chains which have no loops, their origins are $\mathcal{O}$ and the length are n.*

Proof. Let $\mathcal{O}'$ be a maximal order such that $d(\mathcal{O}, \mathcal{O}') = n$. Therefore, $\mathcal{O} = End(e_1R + e_2R)$ and $\mathcal{O}' = End(e_1R + e_2\pi^n R)$, for an appropriate basis (e_1, e_2) of V. The sequence of vertices $(\mathcal{O}, \mathcal{O}_1, ..., \mathcal{O}_i, ..., \mathcal{O}')$, where $\mathcal{O}_i = End(e_1R + e_2\pi^i R)$, $1 \leq i \leq n-1$, is a chain without loops, joining $\mathcal{O}$ and $\mathcal{O}'$, of length n. Inversely, provided there is a chain of length $n > 2$ given by a sequence of vertices $(\mathcal{O}_0, ..., \mathcal{O}_n)$. There exist the R-lattices $L_i \supset L_{i+1} \supset L_{i\pi}$ such that $\mathcal{O}_i = End(L_i)$ for $0 \leq i \leq n$. the chain has no loops if $L_i\pi \neq L_{i+2}$ for $0 \leq i \leq n-2$. 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. Thus $L_i\pi + L_{i+2} = L_{i+1}$ whence $L_i\pi + L_{i+j+2} = L_{i+1}$ for every $i, j \geq 0$, $i+j+2 \leq n$. Consequently $L_0\pi$ does not contain L_i for every $i \geq 1$ hence then $d(\mathcal{O}, \mathcal{O}_i) = i$ for $1 \leq i \leq n$. □

Drawing the tree when the number of elements of k is $q = 2$

Here is a picture of tree.
!!!

We notice that the tree not depends on the value of q. The number of vertices of the tree which has the distance n to one of these vertices is $q^{n-1}(1+q)$. It is also the number of the Eichler orders of level $R\pi^n$ contained in $M(2,R)$.

Exercise

1. Let $\mathbb{Z}[X]$ is a free group generated by the vertices of the tree. Define the homomorphism of $\mathbb{Z}[X]$ by putting (Serre [3] p.102)

$$f_n(\mathcal{O}) = \sum_{d(\mathcal{O},\mathcal{O}')=n} \mathcal{O}'$$

for every integer $n \geq 0$. Verify by means of the description of tree the following relations:

$$f_1 f_1 = f_2 + (q+1)f_0, f_1 f_n = f_{n+1} + q f_{n-1} \text{if } n \geq 2.$$

We set $T_0 = f_0, T_1 = f_1, T_n = f_n + T - 2$ if $n \geq 2$. Prove the new homomorphism T_n satisfies for all integer $n \geq 1$ a unique relation

$$T_1 T_n = T_{n+1} + q T_{n-1}.$$

Deduce the identity

$$\sum_{n \geq 0} T_n x^n = (1 - T1x + qx^2)^2,$$

where x is an indeterminant.

2. The group $PGL(2,K)$ acts naturally on the tree X of maximal orders. A $g \in GL(2,K), \mathcal{O} \in S(X)$, by associating the maximal order with $g\mathcal{O}g^{-1}$. Prove the action of $PGL(2,K)$ is transitive and $S(X)$ is identified with $PGL(2,K)/PGL(2,R)$. Show the orbit of a maximal order $\mathcal{O}$ by the action of $PSL(2,K)$ consists of the maximal orders at a even distance to $\mathcal{O}$.

3. We say that a group G acts on a graph with inversion if it exists $g \in G$, $y \in Ar(X)$ such that $gy = \bar{y}$. Prove that, $PGL(2,K)$ acts on the tree X of maximal orders with inversion, but $PSL(2,K)$ acts without inversion.

2.3 Orders embedded maximally

Let H/K be a quaternion algebra, and L/K be a quadratic algebra separably over K contained in H. It can be given an order B of L over the integer ring R of K. Let $\mathcal{O}$ be an Eichler order of H. Recall that we say B is embedded maximally in $\mathcal{O}$ if $\mathcal{O} \cap L = B$. A maximal inclusion of B in $\mathcal{O}$ is an isomorphism f of L in H such that $\mathcal{O} \cap f(L) = f(B)$. We are trying to determine all the maximal inclusion of B in $\mathcal{O}$. It is clear that, it can be replaced $\mathcal{O}$ by an order being conjugate to it: if H is a field, the maximal order is the only Eichler order, if $H = M(2, K)$ it can suppose that $\mathcal{O} = \mathcal{O}_n$ for $n \geq 0$. If $\tilde{h}$ is an inner automorphism defined by an element h of the normalizer $N(\mathcal{O})$ of $\mathcal{O}$ in $H^\times$, it is clear that $\tilde{h}f$ is a maximal inclusion of B in $\mathcal{O}$ too. We shall prove the number of maximal inclusion of B in $\mathcal{O}$ modulo the inner automorphism defined by a group with $\mathcal{O}^\times \subset G \subset N(\mathcal{O})$, is finite. It can be calculated explicitly. The results of that calculation are very complicate if $\mathcal{O}$ has a level $R\pi^n$ with $n \geq 2$. It will not be used here, but we only give the complete results if $n \leq 1$. Sometimes the proof are given in the general case. One can carry out it as an exercise to the end, or refer to Hijikata [1].

Definition 2.9. *Let L/K be a quadratic separable extension . Let π be a uniform parameter of K. We define the Artin symbol $(\frac{L}{\pi})$ by*

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

Definition 2.10. *Let B be order of a separable quadratic extension L/K. We define that the Eichler symbol $(\frac{B}{\pi})$ equals Artin symbol $(\frac{L}{\pi})$ if B is a maximal order, and equals 1 otherwise.*

Now we suppose that H is a quaternion field. We have

Theorem 2.3.1. *Let L/K be a separable quadratic extension of K and B be an order of L. Let $\mathcal{O}$ be a maximal order of H. If B is a maximal, the number of maximal inclusion of B in $\mathcal{O}$ modulo the inner automorphisms defined by a group G equals*

$$\begin{cases} 1, & \text{if } G = N(\mathcal{O}) \\ 1 - (\frac{L}{\pi}), & \text{if } G = \mathcal{O}' \end{cases}.$$

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

Proof. Let $fz; L \to H$ be an inclusion of L in H, The Lemma 1.4 implies that f is a maximal inclusion of the integer ring R_L of L in the maximal order $\mathcal{O}$. Therefore, if B is not maximal, it is then not embedded maximally in $\mathcal{O}$. According to I.§4, paragraph [class of ideals], the number of maximal inclusions denoted by $m(L, G)$ of R_L in $\mathcal{O}$ modulo G equals the number of the conjugation classes in H of the element $m \in L$, $m \notin K$, modulo $\tilde{G}$. Since $N(\mathcal{O}) = H^\times$, it follows $m(L, N(\mathcal{O})) = 1$. Since $\tilde{\mathcal{O}}^\times \cup \tilde{\mathcal{O}}\tilde{u} = \tilde{H}^\times$ if $u \in H$ is an element of reduced norm π, we then have $m(L, \mathcal{O}^\times) = 1$ if it can choose $u \in L$, i.e. if L/K is ramified, and $m(L, \mathcal{O}^\times) = 2$ otherwise, i.e. if L/K is unramified . □

We suppose now that $H = M(2, K)$. Then there is a similar result:

Theorem 2.3.2. *Let L/K be a separable quadratic extension and B be an order of L. Let $\mathcal{O}$ be a maximal order of $M(2,K)$. We can embed maximallyB in $\mathcal{O}$ and the numberof maximal inclusion of B in $\mathcal{O}$ modulo the inner automorphisms defined by $\mathcal{O}^\times$ equals 1. Let $\mathcal{O}'$ be an Eichler order of $M(2,K)$ with level $R\pi$. The number of maximal inclusions of B in $\mathcal{O}'$ modulo inner automorphism associating with G equals*

$$\begin{cases} 0 \quad or \quad 1, & if \quad G = N(\mathcal{O}) \\ 1 + (\frac{B}{\pi}), & if \quad G = \mathcal{O}^{\times\prime} \end{cases}.$$

The theorem shows that B can not be embedded in $\mathcal{O}$

if and only if B is maximal and L/K is unramified. The proof of the theorem will be proved following Hijikata [1]. We are going to study in general the maximal inclusion of B in an Eichler order $\mathcal{O}_{\underline{n}}$.

Definition 2.11. *If B is an order of L, it exists $s \in \mathbb{N}$ such that $B = R + Rb\pi^s$, where $R + Rb$is the maximal order of L. Integer s characterize B, and then we write $B = B_s$. The ideal $R\pi^s$ is called the <u>conductor</u> of B. If $u \leq s$, we have $B_s \subset B_u$, and the ideal $R\pi^{s-u}$ is called the <u>relative conductor</u> of B_s in B_u.*

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

Lemma 2.3.3. *(Hijikata [1]). Let $\mathcal{O}_{\underline{n}}$, $n \geq 0$ be an Eichler order of $M(2,K)$. The following properties are equivalent:*
(1) f is a maximal inclusion 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 $\pi^{-i}b$, $\pi^{-i}(a-d)$, $\pi^{-r-n}c$ are 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 denote the matrix $uf(g)u^{-1}$ defined above by $f_x(g)$. The equivalence of (1),(2),(3) is easy and leave as an exercise. Since (4) implies (3) by an evident way, we shall prove (3)→ (4) only. 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 $p(x) = 0 mod(R\pi^{n+2r})$. The problem then leads to the case where $\pi^{-r}b$ is a unit. If $\pi^{-r-n}c$ is a unit, we conjugate $f(g)$ by $\begin{pmatrix} 0 & 1 \\ \pi^n & 0 \end{pmatrix}$. Otherwise, conjugating $f(g)$ by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then b is replaced by $-(a+c)+b+d$ which is the product of a unit by π^r. □

We have therefore a criterion of the existence of the maximal inclusion of B in $\mathcal{O}_{\underline{n}}$. Now we intend to consider the inclusion. Set $E = \{x \in R | t \equiv 2x mod(R\pi), \quad p(x) \equiv 0 mod(R\pi^{n+2r})\}$. The set is introduced by (4) of the above lemma.

Lemma 2.3.4. *(Hijikata [1]). Let f, f' be two maximal inclusions of B in $\mathcal{O}_{\underline{n}}$. Let ${}^n f = \tilde{h}_n f$, where $\tilde{h}_n$ is the inner 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 to f' or ${}^n f'$ modulo $\mathcal{O}^\times_{\underline{n}}$. If $n = 0$, the equivalence modulo $N(\mathcal{O}_{\underline{n}})$ coincides with the equivalence modulo $\mathcal{O}^\times_{\underline{0}}$.
(2) Let $x, x' \in E$ and $f_x, f_{x'}$ defined as that in the above lemma. Then f^x is equivalent to $f_{x'}$ modulo $\mathcal{O}^\times_{\underline{n}}$ if and only if $x \equiv x' mod(\pi^{r+n})$.
(3) If $\pi^{-2n}(t^2 - 4n)$ is a unit in R (rep. not a unit in R), Then f_x is equivalent to ${}^n f_{x'}$ if and only if $x = t - x' mod(\pi^{r+n})$ (rep. $x \equiv t - x' mod(\pi^{r+n}$ and $p(x') \not\equiv 0 mod(\pi^{n+2r+1}))$

Proof. (1) is obvious. (2): if $x \equiv x' mod(\pi^{r+n}$, we put $a = \pi^{-r}(x - x')$ and $u = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$. Hence $u \in \mathcal{O}^\times_{\underline{n}}$ and $u f_x(g) u^{-1} = \begin{pmatrix} x' & \pi^r \\ \star & \star \end{pmatrix}$. Inversely, suppose that f_x is equivalent to $f_{x'}$ modulo $\mathcal{O}^\times_{\underline{n}}$. Since every element of $\mathcal{O}^\times_{\underline{n}}$ is upper triangular modulo π^n, if $u \in \mathcal{O}^\times_{\underline{n}}$, $\pi^{-r}(u f_x(g) u^{-1} - x)$ has the same diagonal modulo π^n with $\pi - r(f_x(g) - x)$, then $x \equiv x' mod(\pi^{n+r})$. (3): If $\pi^{-n-2r} f(x')$ is a unit, and ${}^n f_{x'}(g)$ satisfies the condition (3) of the above lemma, then it is equivalent to $\begin{pmatrix} t - x' & \pi^r \\ -\pi^{-r} f(x') & x' \end{pmatrix}$. Besides, from (2) f_x is equivalent to ${}^n f_{x'}$ modulo $\mathcal{O}^\times_{\underline{n}}$ if and only if $x = t - x' mod(\pi^{r+n})$. If $\pi^{-n-2r} f(x')$ is not a unit, we set $u = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ for $b \in R$, and $u^n f_x(g) u^{-1} = (x_{ij})$. Modulo π^{n+r}, then $x_{ij} = t - x'$, $x_{12} = b(2x' - t) - \pi^{-n+r} f(x')$. Therefore if $\pi^{-r}(2x' - t)$ is a unit, or in an equivalent way 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 $\mathcal{O}^\times_{\underline{n}}$. Finally, suppose that $\pi^{-n-2r} f(x')$ and $\pi^{-2r}(t - 4n)$ are not units, then if we note that $\mathcal{O}^\times_{\underline{n}}$ is generated modulo π^n by the diagonal matrices and the matrices of form $\begin{pmatrix} 1 & b \\ 0 & b \end{pmatrix}$, we see that for all the $u \in \mathcal{O}^\times_{\underline{n}}$, if $u^n f_{x'}(g) u^{-1} = (x_{ij})$, $x_{12} \pi^{-r}$ is never a unit hence ${}^n f_{x'}$ can not be equivalent to f_x modulo $\mathcal{O}^\times_{\underline{n}}$. □

From these two lemmas we deduce the following proposition which allow us to compute the number of maximal inclusion of B_s in $\mathcal{O}_{\underline{n}}$ modulo the group of inner automorphism induced by $G = N(\mathcal{O}_{\underline{n}})$ or $\mathcal{O}^\times_{\underline{n}}$. The theorem 3.2 is a consequence of it.

Proposition 2.3.5. *(1) B can be embedded maximally in $\mathcal{O}_{\underline{n}}$ if and only if E is non-empty.*
(2) The number of maximal inclusion of B in $\mathcal{O}_{\underline{n}}$ modulo the inner automorphisms induced by $\mathcal{O}^\times_{\underline{n}}$ equals the cardinal of the image of E in $R/(\pi^{n+2r} R)$ if $\mathcal{O}_{\underline{n}} = \mathcal{O}_{\underline{0}}$ is maximal, or if $\pi^{-r}(t^2 - 4m)$ is a unit. otherwise, the number is the sum of the last cardinal and the cardinal of the image of $F = \{x \in E | p(x) \equiv 0 mod(R\pi^{n+2r+1})\}$ in $R/(\pi^{n+2r} R)$.

Proof. The proof of theorem 3.2. Suppose $\mathcal{O} = \mathcal{O}_{\underline{0}}$ is a maximal order. Since $N(\mathcal{O}) = K^\times \mathcal{O}^\times$, the number of the maximal inclusion modulo the inner automorphism induced by a group G with $\mathcal{O}^\times \subset G \subset N(\mathcal{O})$ depends not on G.

This number is not zero since E is not empty. From (2) we obtain that the number equals 1. Suppose $\mathcal{O} = \mathcal{O}_{\underline{1}}$. We recall $B = R + Rb\pi^s$, where $R + Rb$ is a maximal order of L. If B is not maximal, $s \geq 1$, then $x = 0$ is a solution of the congruence $p(x) = x^2 - t(b)\pi^s x + \pi^{2s} n(b) = 0 \bmod R\pi^2$. Since the discriminant of the above polynomial is not a unit, the mapping in the above proposition (with $r = 0$) shows that there exists two maximal inclusions of B in $\mathcal{O}$ modulo the inner automorphisms induced by $\mathcal{O}^\times$. If B is a maximal order , and if L/K is unramified, then $E = \varnothing$ because the residue field of L and of K are distinct. If K/L is ramified, $n(b) \in R^\times \pi$ and the discriminant of $p(x)$ belongs to $R\pi$. Modulo πR, The set E is reduced to a single element 0, and $F = \varnothing$.
The theorem is proved if $G = \mathcal{O}^\times$. In order to obtain the proof is case of $G = N(\mathcal{O})$, we shall use the fact that $N(\mathcal{O})$ is the group generated by $\mathcal{O}^\times$ and $\begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$. Let matrices $\begin{pmatrix} 0 & 1 \\ -n & 0 \end{pmatrix}$ and $\begin{pmatrix} t & -\pi^{-1}n \\ \pi & 0 \end{pmatrix}$ conjugate modulo $N(\mathcal{O})$. this implies the number of maximal inclusions of Bin $\mathcal{O}$ modulo the inner automorphisms of $N(\mathcal{O})$ equals 0 or 1. □

We note that if the level of the Eichler order $\mathcal{O}_{\underline{n}}$ is enough small, that is to say if the integer n is enough large, $\mathcal{O}_{\underline{n}}$ does not contain the root of the polynomial $p(x)$.
One can find the computation of the explicit formulae of trace by the method similar to what we made here in the following references: Eichler [13] to [20], Hashimoto [1], Oesterie [1], Pizer [1] to [5], Prestel [1],Schneider [1], shimizu [1] to [3], Vigneras [1], and Yamada [1].

Exercise

Use the proof of the above proposition to prove if B is a maximal order of a separable quadratic extension L/K, then B can not be embedded maximally in an Eichler order of $M(2, K)$ of level $R\pi^m$ with $m \geq 2$.

2.4 Zeta function

This section is a preliminary for Chapter III: it contains no theorems but the definitions and the preparatory computations for facilitating the statement in sequels and the proof of the results in the forthcoming chapters when using the adele technique. We shall find here the definition of local zeta function in the sense of Weil [1], the normalization of measures, some computations of volumes or of integrals which will be needed very later.

Definition 2.12. *Let X be a local field K or a quaternion algebra H/K not containing $\mathbb{R}$. Let $\mathcal{B}$ be an order of X containing the valuation ring R of K. The norm of an integral ideal I of $\mathcal{B}$ equals $N_{X(I)} = Card(\mathcal{B}/I)$*

We can verify easily the relation $N_H = N_K n^2$. By means of multiplication we define the norm of fractional ideal. Then by the definition we have

$$N_K(R\pi) = Card(R/R\pi) = Card(k) = q,$$

$$N_H(P) = \begin{cases} Card(\mathcal{O}/\mathcal{O}u) = q^2 & \text{if } H \text{ is a field} \\ Card(\mathcal{O}/\mathcal{O}\pi) = q^4 & \text{if } H \simeq M(2, K) \end{cases}.$$

where P is the two-sided integral maximal ideal of a maximal order $\mathcal{O}$ of H. The norm of a principal ideal $\mathcal{O}h$ is naturally equal to the norm of the ideal $h\mathcal{O}$. By the Corollary 1.7 and the Theorem 2.3, we have

Lemma 2.4.1. *The number of the integral ideals to the left (to the right) of a maximal order of H with norm q^n, $n \geq 0$, is equal to*

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

if H is a field;

$$1 + q + ... + q^n,$$

if $H \simeq M(2, K)$.

Definition 2.13. *The zeta function of $X = H$ or K is a complex function of a complex variable*

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

where the sum is taken over the the integral ideal to the left (right) of a maximal order $\mathcal{B}$ of H.

The above lemma allow to compute explicitly $\zeta_H(s)$ as the function of $\zeta_K(s)$. We have

$$\zeta_K = \sum_{n \geq 0} q_{-ns} = (1 - q^{-s})^{-1},$$

$$\zeta_H = \sum_{n \geq 0} q^{-2ns} \zeta(2s), \text{ if } H \text{ is a field,}$$

$$\zeta_H = \sum_{n \geq} 0 \sum_{0 \leq d \leq n} q^{d-2ns} = \sum_{d \geq 0} \sum_{d' \geq 0} q^{d-2(d+d')s} = \zeta_K(2s)\zeta_K(2s-1),$$

if $H \simeq M(2, K)$. We then have

Proposition 2.4.2. *The zeta function of $X = K$ or H equals*

$$\zeta_K(s) = (1 - q^{-s})^{-1}$$

or

$$\zeta_H = \begin{cases} \zeta_K(2s), & \text{if } H \text{ is a field} \\ \zeta(2s)\zeta_K(2s-1), & \text{if } H = M(2, K) \end{cases}.$$

There is a more general definition of zeta function available for $X \supset \mathbb{R}$. The idea of such function comes from Tate [1] in the case of local field. Their generation to the cental simple algebra is due to Godement [1], and to Jacquet-Godemant [1]. The crucial point is to observe that the classical zeta function can also be defined as the integral over the locally compact group $X^\times$ of the character function of a maximal order multiplied by $\chi(x) = N(x)^{-s}$ for a certain Haar measure. This definition can be generalized then to the zeta function of a so called Schwartz-Bruhat function, of a quasi-character , and extends naturally to the archimedean case. This is what we shall do. We proceed along Weil's book [1], for more details one can refer to it.

Definition 2.14. *Let G be a locally compact group and dg be a Haar measure on G. For every automorphism a of G , let $d(ag)$ be the Haar measure on G defined by $\int_G f(g)dg = \int f(ag)d(ag)$ for every measurable function on G. the proportional factor of these two measures $||a|| = d(ag)/d(g)$ is called the modulus of the isomorphism a*

The followings can be verified easily :
(1) $vol(aZ) = ||a||vol(Z)$, for every measurable set $Z \subset G$
(2) $||a||.||b|| = ||ab||$, if a, b are two isomorphism of G,
and they show that the modulus is independent of the modulus used in the original definition.

Definition 2.15. *The modulus of an element $x \in X^\times$, denoted by $||x||_X$ is the common modulus of two left (or right) multiplicative isomorphisms in $X = H$ or K. The norm $N_X(x)$ of x is the inverse of the modulus.*

Note in $\mathbb{R}$ or $\mathbb{C}$, $||x||$ of an element x is the modulus in the usual sense. We can verify immediately the following properties: if $x \in X^\times$

$$||x||_{\mathbb{R}} = |x|, ||x||_{\mathbb{C}} = |x|^2, ||x||_X = N_X(x)^{-1} = N_X(\mathcal{B}x)^{-1}, \text{if } X \not\supseteq \mathbb{R}.$$

Now we are going to normalize the measures on $X, X^\times$

Definition 2.16. *If $X \not\subseteq \mathbb{R}$, 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 $dx^\cdot$ or $dx^\cdot_X$ the multiplicative Haar measure $(1 - q^{-1})^{-1}||x||_X^{-1}dx$.*

Lemma 2.4.3. *For the multiplicative measure $dx^\cdot$, the volume of the unit group $\mathcal{B}^\times$ of an maximal order $\mathcal{B}$ of X is given by*

$$vol(R^\times) = 1,$$

$$vol(\mathcal{O}^\times) = (1 - q^{-1})^{-1}(1 - q^{-2})$$

where $\mathcal{O}$ is the the integer ring of the quaternion field H/K,

$$vol(GL(2, K)) = 1 - q^{-2}$$

.

Proof. Suppose that X is a field. Let $\mathcal{M}$ be the maximal ideal of $\mathcal{B}$. For the additive measure dx we have the equalities

$$vol(\mathcal{B}^\times = vol(\mathcal{B}) - vol(\mathcal{M}) = 1 - N(x)^{-1} = 1 - Card(\mathcal{B}/\mathcal{M}) = \begin{cases} 1 - q^{-1} & \text{if } X = K \\ 1 - q^{-2} & \text{if } X = H \end{cases}.$$

for the multiplicative measure $dx^\cdot$, The volume of $\mathcal{B}^\times$ for the multiplicative measure $dx^\cdot$, equals the volume of of $\mathcal{B}^\times$ for the additive measure $(1-q^{-1})^{-1}dx$. We obtain the lemma if X is a field. Suppose now $X = M(2, K)$. The canonical mapping $R \to k$ induces a surjection from $GL(2, R)$ to $GL(2, k)$, its kernel Z consists of the matrices congruent to the identity modulo the ideal $R\pi$. The number of the elements of $GL(2, k)$ equals the number of the basis of a k-vector space of dimension 2, being $(q^2 - 1)(q^2 - q)$. The volume of Z for the measure dx is $vol(R\pi)^4 = q^{-4}$. The volume of $GL(2, R)$ for $dx^\cdot$ is then equal to the product $q^{-4}(q^2 - 1)(q^2 - q)(1 - q^{-1})^{-1} = 1 - q^{-2}$. □

Lemma 2.4.4. *We have*

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

Proof. The number of the elements of $\mathcal{B}$ modulo $\mathcal{B}^\times$ with norm q^n, $n \geq 0$ is the number of the integral ideals of $\mathcal{B}$ with norm q^n. The integral is then equal to

$$\zeta_X(s) vol(\mathcal{B}^\times).$$

The function $\zeta_X(s)$ is hence given by Proposition 4.2. □

Definition 2.17. *Let dx be the Lebesque measure on $\mathbb{R}$. Let $X \subset \mathbb{R}$, and (e_i) be a $\mathbb{R}$-basis of X. For $x = \sum x_i e_i \in X$, we denote by $T_X(x)$ the common trace of the $\mathbb{R}$-endomorphisms of X given by the multiplication by x to the left and to the right. We denote by dx_X the additive Haar measure on X such that*

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

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

We can verify that the above definition is given explicitly by
(1) $dx_{\mathbb{C}} = 2dx_1 dx_2$, if $x = x + ix$, $x_i \in \mathbb{R}$,
(2) $dx_{\mathbb{H}} = 4dx_1 ... dx_4$, if $x = x_1 + ix_2 + jx_3 + ijx_4$, $x_i \in \mathbb{R}$,
(3) $dx_{M(2,K)} = \Pi(dx_i)_K$, if $x = \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in M(2,K)$, $K = \mathbb{R}$ or $\mathbb{C}$.
We denote by ${}^t x$ the transpose of x in a matrix algebra. By an explicit manner the real number $T_X({}^t x \bar{x})$ equals to
(0)' x^2, if $X = \mathbb{R}$,
(1)' $2x\bar{x}$, if $X = \mathbb{C}$,
(2)' $2n(x)$, if $X = \mathbb{H}$,
(3)' $\sum x_i^2$, if $X = M(2,\mathbb{R})$,
(3)" $2\sum x_i \bar{x}$, if $X = M(2,\mathbb{C})$.
We put

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

Lemma 2.4.5. *We have*

$$Z_{\mathbb{R}} = *\pi^{-s/2}\Gamma(s/2),$$

$$Z_{\mathbb{C}}(s) = *(2\pi)^{-s}\Gamma(s),$$

$$Z_{\mathbb{H}} + *Z_K(s)Z_K(s-1) \cdot \begin{cases} (s-1) & \text{if } H \text{ is a field} \\ 1, & \text{if } H = M(2,K) \end{cases}$$

where $*$ represents a constant independent of s.

Leave the proof of the lemma as an exercise. If $X = M(2,K)$ we shall utilize the Iwasawa's decomposition of $GL(2,K)$. Every element $x \in GL(2,K)$ can be written by unique way as

$$x = \begin{pmatrix} y & t \\ 0 & z \end{pmatrix} u, \quad y, z \in \mathbb{R}^+, t \in K, u \in U$$

, where U is the group consisting of the matrices satisfying ${}^t\bar{y}y = 1$. If $n = [K : \mathbb{R}]$, then the integrand function is $(yz)^{2ns}exp(-n\pi(y^2 + z^2 + t\bar{t}))$

Definition 2.18. *The Schwartz-Bruhat space S of X is*

$$S = \begin{cases} \text{the infinitely differentiable functions with fast decreasing if } X \supset \mathbb{R} \\ \text{the locally constant functions with compact support, if } X \not\supseteq \mathbb{R}. \end{cases}$$

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

An example of quasi-character on X is $x \mapsto N(x)^s$. It is a character if and only if s is a pure imaginary. The quasi-characters of $H^\times$ are trivial on the commutator group of it. According to I,3.5, the commutator group of $H^\times$ equals the group of the quaternions of reduced norm 1. Every quasi-character of $H^\times$ has the form

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

where χ_K is a quasi-character of K.

Definition 2.19. *The zeta function of a function f of the Schwartz-Bruhat and a quasi-character χ is the integral*

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

The canonical function Φ of X is

$$\Phi = \begin{cases} \text{the characteristic function of a maximal order if } X \not\supseteq \mathbb{R}, \\ exp(-\pi T_X({}^t\bar{x}x)), \text{ if } X \supset \mathbb{R} \end{cases}$$

Therefore the function $Z_X(s)$ of Lemma 4.4 and 4.5 are equal to $Z_X(\Psi, Nx^{-s})$. We include this section with the definition of Tamagawa measure, a notion more or less equivalent to that of discriminant. We choose on X a character ψ_X ,called a canonical character, defined by the conditions:
– $\psi_{\mathbb{R}}(x) = exp(-2i\pi x)$,
– $\psi_{K'}$ is trivial on the integer ring $R_{K'} = R'$ and $R'$is self-dual with respect to $\psi_{K'}$, if K' is a non-archimedean prime field.
– $\psi_K(x) = \psi_{K'} \circ T_X(x)$, if K' is the sub prime field of K.
We shall see in exercise 4.1 the explicit construction of $\psi_{K'}$.
The isomorphism $x \mapsto (y \mapsto \psi_X(xy))$ between X and its topological dual can be written as the Fourier transformation on X too:

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

where $dy = dy_X$ is the the additive measure normalized as above. The dual measure is the measure d^*y such that the following inversion formula is valid:

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

Definition 2.20. *The Tamagawa measure on is the Haar measure on X, which is self-dual for the Fourier transformation associated with the canonical character ψ_X.*

Lemma 2.4.6. *The Tamagawa measure of 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, that is to say,*

$$D_X = ||det(T_X(e_i e_j)||_{K'}^{-1},$$

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

Proof. If $K' = \mathbb{R}$, the global definition of dx shows it is self-dual (i.e. equals its dual measure) for ψ_X. Suppose then $K' \neq \mathbb{R}$ and to choose a R'-maximal order which we denote by B. Let Φ denote its characteristic function. The Fourier transform of Φ is the the characteristic function of the dual B^* of B with respect to trace. By the same way, the bidual of B equals B itself, we see that $\Phi^{**} = vol(B^*\Phi$. The self-dual measure of X is thus $vol(B^{*-1/2}dx$. If (e_i) is a R'-basis of B, we denote by e_i^*) its dual basis defined by $T_X(e_i, e_j) = 0$ if $i \neq j$ and $T_X(e_i, e_i) = 1$. The dual basis is a R'-basis of B^*. If $e_j^* = \sum a_{ij}e_i$, let A be the matrix (a_{ij}). We have $vol(B^*) = ||det(A)||_{K'} \cdot vol(B) = det(A)^{-1}$ for the measure dx. On the other hand, it is clear, $det(T_X(e_i e_j)) = det(A)^{-1}$. We then have $vol(B) = ||det(T_X(e_i e_j))||_{K'}^{-1}$. By the same reason we prove the dual measure of measure dx is $D_X^{-1}dx$. □

Lemma 2.4.7. *The discriminant of H and of K are connected by the relation*

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

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

Proof. With the notations in §1, we have $\mathcal{O} = \{h \in H | t(h\mathcal{O}) \subset R^*\}$, it follows easily that

$$\mathcal{O}^* = \begin{cases} R^*, & \text{if } H = M(2, K) \\ R^*u - 1, & \text{if } H \text{ is a field} \end{cases}.$$

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

Remark 2.4.8. *If $K' \neq \mathbb{R}$, the modulus group $||X^\times||$ is a discrete group. We endow it a measure which assigns every element its proper value. In all of the other cases, the discrete group considered in the following chapters will be endowed with the discrete measure which assigns every element with the value 1.*

compatible measure. Let Y, Z, T be the topological groups equipped with Haar measure dy, dz, dt and there be an exact sequence of continuous mappings

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

We say the measure dy, dz, dt are compatible with this exact sequence, or either say that $dz = dydt$, or $dy = dz/dt$ or $dt = dz/dy$, if for each function f such that the integral below exists and the equality is valid:

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

From this , while knowing two of these measures and the exact sequence we can define a third measure by compatibility. Such a construction will be applied very frequently. but it must be careful: the third measure depends on the exact sequence. Take for example, let X_1 be the kernel of modulus, X^1 be the kernel of the reduced norm. We give them the natural measures which deduced the normalized measures above , and the exact sequence suggested by their definitions. We denote their measure by dx_1 and dx^1 respectively. These measures are different, though the sets X_1 and X^1 may equal. We shall compute explicitly the volume in the exercises of this chapter. If $K' \neq R$, we notice that dx_1 is the restriction of the measure $dx^{\cdot}$ to X_1 because of its naturalness.

Excercise

1. Prove the following characters ψ_K are the canonical characters.
   If $K = \mathbb{Q}_p$, $\psi_K(x) = exp(2i\pi < x >)$, where $< x >$ is the unique number ap^{-m}, $m \geq 0$, which is a rational locating between 0 and 1 such that $x - < x > \in \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the integer ring of $\mathbb{Q}_p$.
   If $K = \mathbb{F}_p[[T]]$, $\psi_{K(x)} = exp(2i\pi, < x >)$ where $< x >= a_{-1}p^{-1}$ if $x = \sum a_i T^i$, $0 \leq a_i \leq p$.
   If $x \in \mathbb{Q}$, we denote $\psi_p(x) = \psi_{\mathbb{Q}_p}(x)$, and $\psi_{infty} = \psi\mathbb{R}(x)$, where $psi_{\mathbb{R}}(x) = exp(-2i\pi x)$ is the canonical character of $\mathbb{R}$. Prove $\psi = \psi_{infty}\pi_p\psi_p$ defines on $\mathbb{Q}$ a character which equals trivial character.

2. Computing volumes. With the measure defined by compatibility coming from the canonical measures (Remark 4.8) prove the formula

$$vol(\mathbb{R}_1) = 2, \quad vol(\mathbb{C}_1) = 2\pi, \quad vol(\mathbb{H}_1) = 2\pi^{2'} \quad vol(\mathbb{H}^1) = 4\pi^2.$$

   we notice that $2vol(\mathbb{H}_1) = vol(\mathbb{H}^1)$ for the chosen measures (Remark 4.8) though the sets $\mathbb{H}_1, \mathbb{H}^1$ are the same. Calculate the integral $\int_{\mathbb{H}} e^{-n(h)} n(h)^2 4dh/n(h)^2$.

3. The volume of groups in Eichler orders. Let $\mathcal{O}_{\underline{m}} = \begin{pmatrix} R & R \\ p^m R & R \end{pmatrix}$ be the order of The canonical Eichler order of level Rp^m with $m \neq 0$ in $M(2, K)$, with K non archimedean and p be a uniform parameter of K. Set

$$\Gamma_0(p) = \mathcal{O}^1_{\underline{m}} = SL_2(R) \cap \mathcal{O}_{\underline{m}},$$

$$\Gamma_1(p^m) = \{x \in \Gamma_0(p^m) | x \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} mod(\mathcal{O}_{\underline{0}} p^m)\},$$

$$\Gamma(p^m) = \{x \in \Gamma_1(p^m) | x \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod(\mathcal{O}_{\underline{0}} p^m)\}.$$

   On $X = K, H, M(2, K)$ we choose the Tamagawa measure $D_X^{-1/2} dx$, and on $X^\times$ choose the measure $||x||^{-1} D_X^{-1/2} dx$, cf. Lemma 4.6 and Remark 4.8. Verify the following formulae:
   formulae.

$$vol(\Gamma_0(p^m)) = D_K^{-3/2}(1 - Np^{-2})(Np + 1)Np^{1-m},$$

$$vol(\Gamma_1(p^m)) = D_K^{-3/2} Np^{-2m},$$

$$vol(\Gamma(p^m) = D_K^{-3/2} Np^{-3m}.$$

where Np is the number of elements of residue field k of K. If $\mathcal{O} = \mathcal{O}_{\underline{0}}$ is a maximal order of a quaternion algebra H/K, we have

$$vol(\mathcal{O}_{\underline{0}}^1) = D_K^{-3/2}(1 - Np^{=2}) \cdot \begin{cases} (Np-1)^{-1}, & \text{if } H \text{ is a field} \\ 1, & \text{if } H = M(2,K) \end{cases}.$$

4. (Pitzer [3]).Let $\{L_{nr}, p\}$ be the quaternion field over K, uniquely up to isomorphism. It has the following representation

$$H = \{L_{nr}, p\} = \{\begin{pmatrix} a & b \\ pb & a \end{pmatrix} | a, b \in L_{nr}\}$$

where $4p$ is a uniform parameter of K and L_{nr}/K is a ramified quadratic extension. We denote simply the above matrix by $[a, b]$. The order $\mathcal{O}_{2r+1} = \{[a, p^r b] | a, b \in R_L\}$ is called the canonical order of level Rp^{2r+1}, where R_L is the integer ring of L_{nr}. Verify $\mathcal{O}_{2r+1}$ is actually an order, and either directly or on the discriminant that $\mathcal{O}_1$ is the maximal order. Verify that an order $\mathcal{O}$ is isomorphic to $\mathcal{O}_{2r+1}$ for a $r \geq 0$ if and only if it contains a sub-ring being isomorphic to R_L. Prove, if $[a, b] \in \mathcal{O}_1^\times$, it can be written as $[a, b] = [a', p^r b'][1, c]$, where $c = b/amod(p^r)$ and $a', b' \in R_L$. Deduce $[\mathcal{O}_1^\times : \mathcal{O}_{2r+1}^\times] = Np^{2r}$.
Deduce the volume of $\mathcal{O}_m^1$ for the Tamagawa measure is equal to

$$vol(\mathcal{O}_m^1) = D_K^{-3/2}(1 - Np^{-2})(Np-1)^{-1} Np^{1-m}, \quad m \geq 1.$$

The formula is a natural generation of that in the above formulae.

5. Maximal compact subgroup. Let K be a non-archimedean local field, and H/K be a quaternion algebra. Set $X = H$ or K. Prove the maximal compact subgroups of $X^\times$ are the unit group $B^\times$ of the maximal order B of X.

Chapter 3

Quaternion algebra over a global field

We wish in this chapter to give the fundamental results of the quaternion algebra over a global field. They are: the classification theorem, the strong approximation theorem for the quaternions with reduced norm 1, the computation of the Tamagawa numbers, and the trace formula. We shall obtain these results by the analytic method. The key point is the functional equation of adele zeta function.

3.1 Adeles

We suggest the reader who is familiar the notion of adele to read §2 directly; and only consult this section when further reading needs.

Definition 3.1. *A global field K is a commutative field which is a finite extension K/K' of a field called its prime subfield K', which equals one of the following field:*
– $\mathbb{Q}$, the field of rational numbers;
– $\mathbb{F}_p(T)$, the field of rational fractions in one variable T, with coefficients in the finite field $\mathbb{F}_p$, where p is a prime number. If $K \supset \mathbb{Q}$, we say that K is a number field. If $K \supset \mathbb{F}_p(T)$, we say that K is a function field.

Definition 3.2. *Consider the set of inclusions $i : K \to L$ i the local field L such that the image $i(K)$ of K is dense in L. Two inclusions i, i' are said to be equivalent if it exists an isomorphism $f : L \to L'$ of local fields which appear in their definition such that $i' = fi$. An equivalent class is called a place of K. We denote it usually by v, and by $i_v : K \to K_v$ denote a dense inclusion of K in a local field K_v representing the place v. We distinguish the archimedean places or infinite places so that K_v contains a field isomorphic to $\mathbb{R}$ from other places, which is called the finite places.*

Notations
We fix the representation $i_v : K \to K_v$ of the place v of K. Then K may be considered as being contained in each K_v. V denotes the set of all places, ∞ the set of infinite places, and P the set of finite places. We use again the local

field K_v in the sense of the definition in chapter II, but with an index v. If S is a finite set of places of K, such that $S \supset \infty$, we denote by

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

the ring of elements in K, which are integers for that places which do not belong to S. It is a Dedekind ring. If K is a number field we write $R_\infty = R$. It is the integer ring of K. If $v \in P$, the cardinal of the residue field k_v is denoted by $Nv.$, and call it the norm of v.
EXAMPLE. Places of $\mathbb{Q}$: One infinite place, represented by the natural inclusion of $\mathbb{Q}$ in the field of real numbers; the finite places, represented by the natural inclusion of $\mathbb{Q}$ in the p-adic field $\mathbb{Q}_p$ for every prime numbers p.
Places of $\mathbb{F}_p(T)$: Every finite places uniquely associate to a irreducible polynomial, and to T^{-1}, cf. Weil [1]. The set of the elements of K with its image belonging to R_v for every $v \in V$ is $\mathbb{F}_p$. The set of the elements of K with its images belonging to R_v for every $v \in V$ but T^{-1} is $\mathbb{F}_p[T]$. The monic irreducible polynomials correspond bijectively to the primer ideals of $\mathbb{F}_p[T]$.

Definition 3.3. *Let H/K be a quaternion algebra. A place v of K is ramified in H if the tensor product (over K) $H_v = H \otimes K_v$ is a field.*

EXAMPLE. If the characteristic of K is different from 2, and if $H = \{a, b\}$ defined in I,1 (3), a place v of K is ramified in $\{a, b\}$ if and only if the Hilbert symbol $(a, b)_v$ of a, b in K_v is equal to -1 by II.1.1, This afford a rapid way to obtain the ramified places in $\{a, b\}$.
We notice that the definition of ramification is quite natural. According to II,1, the ramified places of K in H are the places v of K such that H_v/K_v is ramified.

Lemma 3.1.1. *The number of ramified places of K in H is finite.*

Proof. Let (e) be a basis of H/K. For almost every finite place v, the lattice generated by (e) over R_v is an order (cf. I,§5) of the reduced discriminant $d_v = R_v$. We deduce from II, that $H_v = M(2, K_v)$ and $R_v[e]$ is a maximal order almost everywhere. □

Definition 3.4. *The product of the ramified finite places of K in H is called the reduced discriminant of H/K. If K is a number field, it identifies with an integral ideal of the integer ring of K. We denote it by d or d_H. It is an element of the free group generated by P.*

The set of ramified places of K in H plays a fundamental role in the classification, we denote the set by $Ram(H)$. Sometimes we use $Ram_\infty H$, $Ram_f H$ to denote the set of infinite places, and of finite places respectively.
Consider the case where for every place $v \in V$ a locally compact group G_v and for every place not belonging to a finite set $S \subset V$ a compact open subgroup C_v of G_v are defined.

Definition 3.5. *The restricted product G_A of locally compact groups G_v with respect to compact subgroup C_v is*

$$G_A = \{x = (x_v) \in \prod_{v \in V} G_v | x_v \in C_v p.p.\}$$

where p.p. means "for almost each place $v \notin S$". We provide G_A with a topology such that the fundamental neighborhood system of the unit is given by the set

$$\prod_{v\in V} U_v, \quad U_v = C_v, p.p. U_v \text{ is an open neighborhood of the unit of } G_v$$

One can find the discussion of these groups in Bourbaki [3]. It can be showed that G_A is a locally compact topological group, and not depends on S.
This case appears when G is an algebraic group defined over K. In such a case G_v is the set of points of G with values in K_v, and C_v is the set of points of G with values in R_v defined for v not belonging to a finite set of places $S \supset \infty$. The group G_A is called the adele group of G. Here are some examples.
1)The adele ring of K. We choose

$$G_v = K_v, \quad S = \infty, \quad C_v = R_v^{\times}.$$

The correspondent adele group is called the adele ring of K. It is also an algebraic group induced by the additive group of K. Denote it by A or K_A.
2) The adele group of K. We choose

$$G_v = K_v^{\times}, \quad S = \infty, \quad C_v = R_v^{\times}.$$

The correspondent adele group is called the adele group of K. It is the group of units in A with the topology induced by the inclusion $x \to (x, x^{-1})$ in $A \times A$. The adele group is also a algebraic group induced by the multiplicative group of K. Denote it by $A^{\times}$ or $K_A^{\times}$.
3)The adele group defined by H. We choose a)

$$G_v = H_v, \quad S \supset \infty, \quad S \neq varnothing, \quad C_v = \mathcal{O}_v,$$

where $\mathcal{O}$ is an order of H over the ring $R_{(S)}$, and $\mathcal{O}_v = \mathcal{O} \otimes R_v$, where the tensorial product is taken over $R_{(S)}$.
We can define the adele ring of H too, and denote it by H_A. It equals $A \otimes H$, where the tensorial product is taken over K.
b)

$$G_v = H_v^{\times}, \quad S \supset \infty \quad S \neq \varnothing \quad C_v = \mathcal{O}_v^{\times}.$$

It defines the unit group of H_A and denoted by $H_A^{\times}$
c)

$$G_v = H_v^1 (or H_{v,1}), \quad S \supset \infty, \quad S \neq \varnothing, \quad C_v = \mathcal{O}_v^1 = \mathcal{O}_{v,1},$$

where X^1 (or X_1) presents the kernel of the reduced norm (or of the modulus) in X. It defines the adele group H_A^1 (or $H_{A,1}$). All of these adele groups are also the examples of the adele groups of algebraic groups.
Morphisms. Suppose there is an other restricted product G'_A of locally compact groups G'_v with respect to the compact subgroups C'_v. We may suppose that the set $S' \subset V$ to be such that for $v \notin S'$ where C'_v being defined it coincides with S. Suppose that for every place $v \in V$ we have defined a homomorphism $f_v : G_v \to G'_v$ such that if $v \notin S$, $f_v(C_v) \supset C'_v$. Therefore the restriction of $\prod f_v$ to G_A defines a morphism from G_A to G'_A ,denoted by f_A. If the mapping f_v, $v \in V$, are continuous then f_A is continuous.
EXAMPLE. We can define the reduced trace by $t_A : H_A \to A$, and the reduced

norm $n_a : H_A^\times \to A^\times$ too.
Suppose that G' is a group with unit 1, and for every place $v \in V$ we have defined the homomorphism $f_{v\,G_v} \to G'$ such that $f_v(C_v) = 1$ p.p.. We can then define in G' the product

$$f_{A(x)} = \prod_{v \in V} f_v(x_v), \text{if } x = (x_v) \in G_A.$$

EXAMPLE. We can define the norm N_A, the modulus $||\cdot||_A$ in $H_A^\times$, and $A^\times$ too.
NOTATIONS. It is convenient to consider G_v as that which has been embedded in G_A and identifies 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 the adele group of an algebraic group defined over K, the group G_K then is the group of points in G with its value in K. For every place $v \in V$ we choose an inclusion of G_K in G_v denoted by i_v. For almost every place $i_v(G_K) \supset C_v$, then the mapping $\prod_{v \in V} i_v$ defines an inclusion of G_K in G_A. We put $X = X_K = H$ or K, and $Y_v = \mathcal{O}_v$ or R_v,p.p..
Quasi-characters. Recall that a quasi-character of a locally compact group is a continuous homomorphism of the group in $\mathbb{C}^\times$. Let ψ_A be a quasi-character of G_A. By restricting to G_v it defines a quasi-character ψ_v of G_v. We have naturally the relation

$$\psi_A = \prod_{v \in V} \psi_v(x_v) \text{if } x = (x_v) \in G_A.$$

For the convergence of the product in $\mathbb{C}^\times$ if and only if $\psi_v(C_v) = 1, p.p.$. In fact, if this property is not satisfied, we then could find $c_v \in C_v$ such that $|\psi_v(c_v) - 1| > 1/2, p.p.$ and the product would not be convergent for the elements x such that $x_v = c_v p.p.$. Thus we have proved the following theorem.

Lemma 3.1.2. *The mapping $\psi_A \mapsto (\psi_v)$ is an isomorphism of the group of quasi-characters of G_A and the group $\{(\psi_v)\}$ such that ψ_v is the quasi-character of G_v, and $\psi_v(C_v) = 1, p.p.$*

We can apply the local results of last chapter to the quasi-characters of X_A. Let $\psi_A = \prod_{v \in V} \psi_v$ be the product of the canonical local character (exercise II.4.1); the product is well-defined because of $\psi_v(Y_v) = 1, p.p.$. The above lemma shows that every character of X_A is of the form $x \mapsto \psi_a(ax)$, where $a = (a_v) \in X_v$, and $a_v \in Ker(\psi_v), p.p.$. Since $Ker(\psi_v) = Y_v, p.p.$, it follows that $a \in A$. Therefore, X_A is self-dual. Let us turn firstly to the case where $X = \mathbb{Q}$ or $\mathbb{F}_p(T)$ is a prime field, we shall verify that ψ_A is trivial on X_K, and the dual of X_A/X_K is X_K, cf. Weil [1].

Proposition 3.1.3. *X_A is self-dual, and X_K is the dual of X_A/X_K.*

We are going now to give the principal theorems of adeles X_A and $X_A^\times$. These theorems are still valid if X is a central simple algebra over K. The proof in the special case treated by us gives a good idea of the proof in the general case (Weil [1]).

Theorem 3.1.4. *(Fundamental Theorem) Adeles.*
1) X_K is discrete in X_A and X_A/X_K is compact.

2)(theorem of approximation). For every place v, $X_K + X_v$ is dense in X_A.
Ideals.
1)$X_K^\times$ is discrete in $X_A^\times$.
2)(product formula) The modulus equals 1 on $X_K^\times$
3) (Fujisaki's theorem [1]). If X is a field, the image in $X_A^\times/X_K^\times$ of the set

$$Y = \{x \in X_A^\times | 0 < m \leq ||x||_A \leq M, \quad n, m \text{ is real}\}$$

is compact.
4) For every place v or infinity if K is a number field, there exists a compact set C of X_A such that $X_A^\times = \overline{X_K^\times X_v^\times} C$.

Proof. Adeles.1) We prove that X_K is discrete in X_A. It suffices to verify that 0 is not an accumulative point of X_K. In a sufficiently small neighborhood of 0, the only possible elements of X_K are the integers for every finite places: hence a finite number of it if K is a function field, and belonging to $\mathbb{Z}$ if $X = \mathbb{Q}$. In these two cases, it is clear, 0 is impossible to be an accumulative point. We have the same result for every X, since X is a vector space of finite dimension over $\mathbb{Q}$ or a function field. The dual group of a discrete group is compact, and hence X_A/X_K, dual to X_K, is compact.
2)Theorem of approximation. We show that a character of X_A being trivial on X_K is determined by its restriction to X_v. In fact, a character being trivial on X_K and on X_v has the form $x \mapsto \psi_A(ax)$ where ψ_A is the canonical character with a in X_K and $\psi_v(ax_v) = 1$ for every $x_v \in X_v$. It implies $a = 0$, and the character $\psi_A(ax)$ is trivial.
Ideals. 1) Prove $X_K^\times$ is discrete in $X_A^\times$ it is sufficient to prove that 1 is not an accumulative point. A series of elements (x_n) of $X_K^\times$ converges to 1 if and only if (x_n) and x_n^{-1}) converge to 1. It suffices that (x_n) converges to 1, hence that 1 is an accumulative point of X_K in X_A. It is impossible according to the theorem of adeles.
Product formula. Let x be an element of X_K; For proving the modulus of x equals equals 1, it is necessary and sufficient to verify the volume of an measurable set $Y \subset X_A$ equals the volume xY for an arbitrary Haar measure. We have

$$vol(xY) = \int_{X_A} \varphi(x^{-1}y)dy = \int_{X_K \backslash X_A} \sum_{z \in X_K} \varphi(zx^{-1}y)dy^{\cdot}$$
$$= \int_{X_K \backslash X_A} \sum_{z \in X_K} \varphi(zy)dy^{\cdot} = vol(Y),$$

where φ is the characteristic function of Y, and $dy^{\cdot}$ is the measure on $X_K \backslash X_A$ induced by the compatibility with dy and the discrete measure on X_K.
Fusijaki's theorem. A compact set of $X_A^\times$ has the form

$$\{x \in X_A^\times | (x, x^{-1}) \in C \times C'\}$$

for two compact sets C and C' of X_A. For element x of Y, i.e.

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

we look for an element of $X_K^\times$ such that $xa \in C$ and $a^{-1}x^{-1} \in C'$. We choose in X_A a compact set C'' of volume sufficiently large, greater than

$$vol(X_A/X_K)Sup(m^{-1}, M)$$

so that the volumes of $x^{-1}C''$ and $C''x$ are strictly greater than the volume of X_A/X_K. We set then $C = C'' - C'' = \{x - y | x, y \in C''\}$. It is a compact set of X_A since the mapping $(x, y) \mapsto x - y$ is continuous. There exist $a, b \in X_K$ such that $xa \in C, \quad bx^{-1} \in C$. Now we suppose that X is a field, then we can choose a, b in $X_K^\times$. We have $ba \in C^2$ which is compact in X_A. The number of possible value for $ba = c$ is then finite, and hence we choose $C' = \bigcup c^{-1}C$.
4)In view of Fusijaki's theorem, it is evident for a field X. In fact, with the choice of v, the group of modulus of $X_v^\times$ is of finite index in that of $X_A^\times$, and if $X_{A,1}^\times$ denotes the elements of X_A with modulus 1, we then prove immediately that $X_{A,1}/X_K$ is compact. It remains to the case of $M(2, K)$ to prove. It is well known that we can use the existence of the "Siegel sets". But in the very simple case which we are interested in, the proof is quite easy. Let P be the group of upper triangular matrices, D the group of diagonal matrices, and N the unipotent group of P.By triangulation (II,lemma 2.2 for $v \in P$), we have

$$GL(2, A) = P_A \cdot C = D_A N_A C$$

where C equals a maximal compact subgroup of $GL(2, A)$. According to the theorem of approximation in the adeles $A \simeq N_A$, and the property 4) having been proved for K, we have

$$P_A = D_K D_v C' \cdot N_K N_v C''.$$

The elementary relation of permutation

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

implies $P_A = P_K P_v C''$ where $C'' \subset P_A$ is compact. 4) is proved. □

Exercise

1. Let X be a global field K, or a quaternion field H/K. Prove that $X_A^\times/X_K^\times$ is the direct product of the compact group $X_{A,1}/X_K^\times$ and a group being isomorphic to $\mathbb{R}_+ = \{x \in \mathbb{R} | x > 0\}$ or to $\mathbb{Z}$, depending on the characteristic of K is zero or not. It follows that the group of quasi-characters (continuous homomorphisms to $\mathbb{C}^\times$) of $X_A^\times$ being trivial on $X_K^\times$ is isomorphic to the direct product of the group of characters (homomorphism with value in $\{z \in \mathbb{C} | \quad |z| = 1\}$) of $X_{A,1}/X_K^\times$ by the group of quasi-characters of $\mathbb{R}_+$ or $\mathbb{Z}$. Prove then that every quasi-character of $X_A^\times$ being trivial on $X_K^\times$ has the form

$$\chi(x) = c(x)||x||^s$$

where $s \in \mathbb{C}$, and c is a character of $X_A^\times$ being trivial on $X_K^\times$.

3.2 Zeta function, Tamagawa number

Definition 3.6. *The Classic zeta function of X, where X is a global field K or a quaternion field H/K, is the product of the zeta functions of X_v, here $v \in P$.*

The product is absolutely convergent when the complex variable s has a real part $Res > 1$. We therefore have

$$\zeta_A(s) = \prod_{v \in P} \zeta_v(s), \quad Res > 1.$$

It follows from II,4.2 the following formula, called the multiplicative formula:

$$\zeta_H(s/2) = \zeta_K(s)\zeta_K(s-1) \prod_{v \in Ram_f H} (1 - Nv^{1-s})$$

where Nv is the number of the prime ideal associated with the finite place $v \in P$.

This formula plays a basic role in the classification of the quaternion algebra over a global field. The definition of general zeta function is intuitive: not only restrict to the finite places.

Definition 3.7. *The zeta function of X is the product $Z_X(s) = \prod_{v \in V} Z_{X_v}(s)$ of the local zeta functions of X_v for $v \in V$.*

By abuse of terms we call by zeta function of X the product of Z_X by a non-zero constant too, The functional equation is not modified.

Proposition 3.2.1. *(Multiplicative formula). The zeta function of global field K equals*

$$Z_K(s) = Z_{\mathbb{R}}(s)^{r_1} Z_{\mathbb{C}}^{r_2} \zeta_{K(s)},$$

where r_1, r_2 denote the numbers of real places, complex places of K respectively, and the the archimedean local factors are the gamma functions:

$$Z_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad Z_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s).$$

The zeta function of quaternion algebra H/K equals

$$Z_H(s) = Z_K(2s)Z_K(2s-1)J_H(2s),$$

where$J_H(2s)$ depends on the ramification of H/K, and $J_H(s) = \prod_{v \in RamH} J_v(s)$, with $J_v(s) = \begin{cases} 1 - Nv^{1-s}, & \text{if } v \in P \\ s-1, & \text{if } s \in \infty \end{cases}$.

Now we shall use the following adele measures:

$$textoverX_A, dx'_a = \prod_v dx'_v \text{with } dx'_v = \begin{cases} dx_v, & x \in \infty \\ D_v^{-1/2} dx^v, & v \in P. \end{cases}$$

$$\text{over } X_A^\times, dx_A^* = \prod_v dx_v^* \text{with} dx_v^* = \begin{cases} dx_v^\cdot, & v \in \infty \\ D_v^{-1/2} dx_v^\times, & v \in P \end{cases}$$

For the local definition see II,4.
From this we obtain by the compatibility the adele measures on the groups $X_{A,1}, H_A^1, H_A^1/K_A'$, denoted by $dx_{A,1}, dx_A^1, dx_{A,P}$ respectively. We denote by the same way the adele measure on G_A, and that on G_A/G_K obtained by compatibility with the discrete measure assigning every element of G_K with value 1 if G_K is a discrete subgroup of G_A.

Definition 3.8. *The discriminant of X is the product of the local discriminants D_v. We denote it by $D_X = \prod_{v\in P} D_v$.*

The number D_X is well-defined, because of $D_v = 1, p.p.$. We also have

$$D_H = D_K^4 N(d_H)^2 \text{or } N(d_H) = \prod_{v\in Ram_f H} Nv$$

is the norm of reduced discriminant of H/K.
Fourier transformation. It is defined with the canonical character $\psi_A = \prod_v \psi_v$ and the self-dual dx'_A on X_A:

$$f^*(x) = \int_{X_A} f(y)\psi_A(xy)dy'_A.$$

The group X_K is discrete, cocompact, of covolume

$$vol(X_A/X_K) = 1$$

in X_A for the measure dx'_A, then according to theorem 1.4, we have the
POISSON FORMULA

$$\sum_{a\in X_K} f(a) = \sum_{a\in X_K} f^*(a)$$

for every admissible function f, i.e. f, f^* are continuous and integrable, and for every $x \in X_A$, $\sum_{a\in X_K} f(x+a)$ and $\sum_{a\in X_K} f^*(x+a)$ converge absolutely and uniformly with respect to parameter x.

Definition 3.9. *The Schwartz-Bruhat functions on X_A are the linear combination of the functions of the form*

$$f = \prod_{v\in V} f'_v$$

where f_v is a Schwartz-Bruhat function on X_v. We denote by $\mathcal{S}(X_a)$ the space of these functions.

EXAMPLE. The canonical function of X_A equals the product of the local canonical functions : $\Phi = \prod_{v\in V} \Phi_v$.
The general definition of zeta functions brings in the quasi-characters χ of $X_{A^\times}$ being trivial on $X_K^\times$ If X is a field, Fusijiki's theorem (theorem 1.4 and exercise 1.1) proves that

$$\chi(x) = c(x)||x||^s, \quad x \in \mathbb{C},$$

where c is a character of $X_A^\times$ being trivial on $X_K^\times$.

Definition 3.10. *The zeta function of a Schwartz-Bruhat function $f \in \mathcal{S}(X_A$, and of a quasi-character $\chi(x) = c(x)||x||^s$ of $X_A^\times$ being trivial on $X_K^\times$ is defined by the integral*

$$Z_X(f,\chi) = \int_{X_A^\times} f(x)\chi(x)dx_A^*,$$

denoted also by

$$Z_X(f,c,s) = \int_{X_A^\times} f(x)c(x)||x||^s dx_A^*,$$

when the integral converges absolutely.

We notice that the zeta function of X , up to a multiplicative constant being independent of s, equals to

$$Z_X(\Phi, 1, s).$$

The functional equation of zeta functions is a key-point of the theory of quaternion algebra.

Theorem 3.2.2. *(Functional equation.)*
1) The zeta function $Z_X(f, c, s)$ is defined by a integral which converges absolutely for $Res > 1$.
2)If X is afield, it can be extended to a meromorphic function on $\mathbb{C}$ satisfying the functional equation:

$$Z_X(f, c, s) = Z_X(f^*, c^{-1}, 1 - s).$$

a) The only possible poles are
– $s = 0, 1$ with residue $-m_X(c)f(0)$, $m_X(c)f^*(0)$ respectively if K is a number field.
– $s \in \frac{2\pi i\mathbb{Z}}{Logq}$, $\frac{1+2\pi i\mathbb{Z}}{Logq}$, with residue $-m_X(c)f(0)/Logq$ and $m_X(c)f^*(0)/Logq$ respectively, if K is a function field, and $||X_A|| = q^{\mathbb{Z}}$. Here we have put

$$m_X(c) = \int_{X_{A,1}\backslash X_K^\times} c^{-1}(x)dx_{A,1}.$$

In particular, if c is a nontrivial character, the zeta function $Z_X(f, c, s)$ is entire.
b) The volume $vol(X_{A,1}/X_K^\times)$ is equal to $m_{X(1)} = \lim_{s\to 1}\zeta_K(s)$, denoted by m_K.

Corollary 3.2.3. *The zeta function of X defined in 2.1 satisfies the functional equation:*

$$Z_X(s) = D_X^{\frac{1}{2}-s} Z_X(1 - s),$$

if X is a field.

Definition 3.11. *The dual quasi-character χ^* of a quasi-character χ of $X_A^\times$ being trivial on $X_K^\times$ equals*

$$\chi^*(x) = \chi(x)^{-1}||x||.$$

If X is a field , by this definition the functional equation of $Z_X(f, \chi)$ can be written as

$$Z_X(f, \chi) = Z_X(f^*, \chi^*).$$

Proof of the functional equation.
1) For obtaining the functional equation of the Riemann zeta function

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1}, \quad s \in \mathbb{C}, \quad Res > 1$$

we consider

$$Z(s) = \int_0^\infty e^{-\pi x^2} x^{-s}\Gamma(s/2)\zeta(s),$$

We divide $\mathbb{R}_+$ into two parts : $\mathbb{R}_+ = [0, 1] \cup [1, \infty]$. The integral restricted on $[0, 1]$ defines a entire function. For the integral restricted on $[1, \infty]$ we apply

a change of variables $x \mapsto x^{-1}$. The Poisson formula allow us to find again an entire function , plus a rational fraction with simple poles 0 and 1. Sine it is already allowed a constant, $Z_X(f,c,s)$ is a generalization of Riemann zeta function. The method for proving the functional equation is the same.
2) Applying to $Z_X(f,c,s)$. We shall treat the problem of convergence far behind. Temporarily we admit that $Z_X(f,c,s)$ converges for Res sufficiently large, and that X is a field. We choose a function φ which separates $\mathbb{R}_+$ into two parts $[0,1]$ and $[1,\infty]$ by putting

$$\varphi = \begin{cases} 0, & \text{if} \quad 0 \leq x < 1 \\ 1/2, & \text{if} \quad x = 1 \\ 1, & \text{if} \quad x > 1 \end{cases} .$$

We consider firstly the integral taking for $||x||^{-1} \in [0,1]$,

$$Z_X^1(f,c,s) = \int_{X_A^\times} f(x)c(x)\varphi(||x||)||x||^s dx_A^*,$$

which defines an entire function on $\mathbb{C}$. In fact if $Z_X^1(f,c,s)$ converges absolutely for $Res \geq Res_0$, it converges also absolutely for $Res \leq Res_0$ because of $||x||^s \leq ||x||^{s_0}$ if $||x|| \geq 1$. The remaining integral is taken for $||x||^{-1} \in [1,\infty]$, after the change of variables $x \mapsto x^{-1}$, it can be written as

$$I = \int_{X_A^\times} f(x^{-1})c(x^{-1})\varphi(x||)||x||^{-s} dx_A^*.$$

After seeing that every term in the symbol of the integral except for $f(x^{-1}$ only depend on the class of x in $X_A^\times / X_K^\times$ we can apply Poisson formula to it. Utilizing that X is a field, writing it as $X_K = X_K^\times \cup \{0\}$.

$$I = \int_{X_A^\times \setminus X_K^\times} c(x^{-1})\varphi(||x||)||x||^{-s} \{ \sum_{a \in X_K} f(ax^{-1} - f(0))\} dx_A^*,$$

where the terms in the embrace, transformed by Poisson formula, is

$$||x||[f^*(0) + \sum_{a \in X_K^\times} f^*(xa)] - f(0).$$

Regrouping the terms, I can be written as the sum of one entire function and the other two terms:

$$I = Z^1(f^*, c^{-1}, 1-s) + J(f^*, c, 1-s) - J(f,c,-s)$$

with

$$J(f,c,-s) = f(0) \int_{X_A^\times / X_K^\times} c(x^{-1})||x||^{-s}\varphi(||x||) dx_A^*.$$

applying the exact sequence

$$1 \to X_{A,1}/X_K^\times \to X_A^\times / X_K^\times \to ||X_A^\times|| \to 1$$

we obtain

$$J(f,c,-s) = f(0) \int_{||X_A^\times||} t^{-s}\varphi(t) dt^{\cdot} \int_{X_{A,1}/X_K^\times} c^{-1}(y) dy.$$

The function J is the product of three terms. The first integral only depends on s, the second one on c. Because there exists s_0 such that the first integral converges, it follows the second one converges for every c. We regain this way without appealing to Fujisaki's formula the formula

$$m_X(c) = \int_{X_{A,1}/X_K^\times} c^{-1}(y)dy < \infty$$

Compute the integral of s: according to K is a number field, or a function field, we have

$$\int_1^\infty t^{-s}dt/t \quad \text{or} \quad \frac{1}{2} + \sum_{m\geq 1} q^{-ms}, \text{if} \quad ||X||_A = q^{\mathbb{Z}}$$

that is to say,

$$s^{-1}, \quad \text{or} \quad \frac{1}{2}(1-q^{-s})^{-1}(1+q^{-s}$$

. Combining these results together we obtain the following expression for zeta function:

$$Z_X(f,c,s) = Z_X^1 = Z_X^1(f,c,s) + Z_X^1(f^*, c^{-1}, 1-s)$$

$$-m_X(c)\cdot\begin{cases} f^*(0)(1-s)^{-1} + f(0)s^{-1}, & \text{if } K \text{ is a number field} \\ \frac{f^*(0)}{2}\frac{q^{s-1}}{-1+q^{s-1}} + \frac{f^*(0)}{2}\frac{1+q^{-s}}{1-q^{-s},}, & \text{if } K \text{ is a function field,and } ||X||_A = q^{\mathbb{Z}} \end{cases}$$

. From this the functional equation and the poles of $Z_X(f,c,s)$ are deduced if X is a field.

3) computing $m_X(1)$. The residue of the particular zeta function $Z_X(\Phi,1,s)$ at point $s=1$ by definition is

$$\lim_{s\to 1}(s-1)\int_{X_A^\times} \Phi(x)||x||^s dx_A^*$$

where $dx_A^* = ||x||^{-1}\prod_{v\in P}(1-Nv^{=1})dx_v'\prod_{v\in\infty} dx_v'$.
we show that the residue equals

$$\int_{X_A} \Phi(x)dx_A' \cdot \lim_{s\to 1}(s-1)\zeta_K(s) = \Psi^*(0)\cdot\lim_{s\to 1}(s-1)\zeta_K(s).$$

On the other hand, we have seen in 2) that the residue is equal to $m_X(1)\Phi^*(0)$. Comparing them we obtain the value of $m_X(1)$:

$$m_X(1) = vol(X_{A,1}/X_K) = \lim_{s\to 1}(s-1)\zeta_K(s) = m_K.$$

We then obtain the value of Tamagawa number of X_1:

$$\tau(X_1) = \int_{X_{a,1}/X_K} m_K^{-1}dx_{A,1} = 1.$$

This computation is an example of the very rich similitude between $Z_H(s)$ and $Z_K(s)$. We on one side have a functional equation for $Z_H(s)$ obtained from 2) if H is afield, and on other side we have a multiplicative formula relating $Z_H(s)$ to $Z_K(s)$ according to 2.1.We can then deduce from the functional equation of $Z_K(s)$the properties and the functional equation of $Z_H(s)$ for every H. Compare

the results obtained by the two methods: we shall have a chance to obtain some apparently different results but which essentially should be the same. It will deduce from it in §3 a large part of the theorem of classification.
4)Convergence. The Riemann zeta function converges absolutely for $Res = \sigma > 1$ since $\zeta(\sigma) = n^{-\sigma}$ satisfies

$$1 < \zeta(\sigma) < 1 + \int_1^\infty t^{-\sigma} dt.$$

If K is a finite extension of $\mathbb{Q}$ of degree d, there are in K at most d prime ideals over a ideal of $\mathbb{Z}$, and

$$1 < \zeta_K(\sigma) < \prod_P (1 - NP^{-\sigma})^{-1} \leq \zeta(\sigma)^d,$$

where P runs through the prime ideals of K. Therefore the zeta function converges for $Res > 1$.
If K is a function field $\mathbb{F}_q(T)$, the zeta function is a rational fraction in q^{-s} and the problem of convergence do not arise.

Convergence of the quadratic zeta functions.Let f be a function of Schwartz-Bruhat space, and c be a character of $X_{A,1}$. There are positive real numbers $M.N$ such that $N\Phi < r < M\Phi$, and $|c| = 1$, hence the integral $Z_X(f, c, s)$ converges absolutely because of that the the zeta function of X which we denote by $Z_X(s)$ converges absolutely. We have seen that it can be expressed as a product of zeta functions of the center: $Z_K(2s)Z_K(1-s)$, by use of this the convergence is no problem. We see that $Z_X(s)$ is defined by an absolutely convergent integral for $Res > 1$.

Definition 3.12. *The Tamagawa measure on X_A, where $X = H$ or K , is the Haar measure dx'_A . the Tamagawa measure on $X_A^\times$ is the Haar measure m_K^*. the measures dx'_A, dx_A^* have been defined already in §2, this chapter, and m_K is the residue at the point $s = 1$ of the classical zeta function ζ_K of K. We introduce the Tamagawa measures on $X_{A,1}$, H_A^1, $H_A^\times/K_A^\times$ respectively in a standard way as the kernels of the modulus $||\cdot||_X$ on X, of the reduced norm, projective group.*

Definition 3.13. *The Tamagawa number of $X = H, or \quad K, X_1, H^1, G = H^\times/K^{times}$ are the volumes computed for the canonical measures obtained from the Tamagawa measures*

$$\begin{array}{ll} \tau(X) = vol(X_A/X_K) & \tau(X_1) = vol(X_{A,1}^\times/X_K^\times) \\ \tau(H^1) = vol(H_A^1/H_K^1) & \tau(G) = vol(H_A^\times/K_A^\times H_K^\times). \end{array}$$

In these definition it is assumed these volumes are finite. It is true actually in our cases.

We have

Theorem 3.2.4. *The Tamagawa numbers of X, X_1, H^1, G have the following values:*

$$\tau(X) = \tau(X_1) = \tau(H^1) = 1, \quad \tau(G) = 2.$$

Proof. When X is a field, the computation of Tamagawa number is implicitly contained in the theorem 2.2 of the functional equation. If $X = M(2, K)$, it can compute directly. The theorem 2.3 can be extended to the central simple algebra X. In this case we have $\tau(X) = \tau(X_1) = \tau(H^1) = 1$ and $\tau(G) = n$, if $[X : K] = n^2$. Reference: Weil [2]. By the definition of Tamagawa measure, $\tau(X) = 1$. We shall prove $\tau(G) = 2\tau(H^1)$ and $\tau(H_1) = \tau(H^1)$, after that then $\tau(H^1) = 1$. The proof is analytic, and the Poisson formula is involved. The exact sequence which is compatible with thee Tamagawa measures

$$1 \longrightarrow H_A^1/H_K^\times \longrightarrow H_{A,1}/H_K^\times \xrightarrow{n} K_{A,1}/K^\times \longrightarrow 1$$

proves that $\tau(H^1) = \tau(H_1)\tau(K_1^{-1})$. The theorem 2.2 shows $\tau(H_1) = \tau(K_1) = 1$ if H is a field because of the definition of Tamagawa measure itself. Therefore $\tau(H^1 = \tau(H_1)$ for every quaternion algebra H/K. It follows from the proof of Theorem 2.2 that

$$2\int_{K_A^\times/K^\times} f(||k||_K)dk_A^* = \int_{K_A^\times/K^\times} f(||k||_{K^2})dk_A^*$$

for every function f such that the integrals converge absolutely. Applying $||h||_H = ||n(h)||_{K^2}$ if $h \in H_A^{times}$, we see that

$$\int_{H_A^\times/H_K^\times} f(||h||_H)dh_A \cdot \tau(H^1) \int_{K_A^\times/K^\times} f(||k||_K)dk_A^* = \tau(G) \int_{K_A^\times/K^\times} f(||k||_K)dk_{A^*},$$

it follows $\tau(G) = 2\tau(H^1)$. The Theorem has been proved when $X = H$ or K is a field.
It remains to prove $\tau(SL(2, K)) = 1$. The starting point is the formula

$$(2) \qquad \int_{A^2} f(x)dx = \int_{SL(2,A)/SL(2,K)} [\sum_{a \in K^2 - \begin{pmatrix}0\\0\end{pmatrix}} f(ua)]\tau(u),$$

where f is an admissible function on A^2, cf. II,§2, and $\tau(u)$ is a Tamagawa measure on $SL(2, A)/SL(2, K)$, and where A^2 is identified with the column vectors of two elements in A on which $SL(2, A)$ operates by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

The orbit of $\begin{pmatrix}0\\1\end{pmatrix}$ is $A^2 - \begin{pmatrix}0\\0\end{pmatrix}$ and its isotropic group is $N_A = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} | x \in A\}$. We apply Poisson formula,

$$\sum_{a \in K^2} f(ua) = \sum_{a \in K^2} f^*({}^t u^{-1} a)$$

because of $det(u) = 1$. Here we give an other expression for the integral (2) in function of f^*. In fact, it prefers to write the integral in f^* into the function on $f^{**} = f(-x)$. Since $\tau({}^t u^{-1}) = \tau(u)$, we obtain

$$(3) \qquad \int_{A^2} f^*(x)dx = \int_{SL(2,A)/SL(2,K)} [\sum_{a \in K^2} f(ux) - f^*(0)]\tau(u).$$

The difference (2) - (3) is

$$\int_{A^2}[f(x)-f^*(x)]=\int_{SL(2,A)/SL(2,K)}[f^*(0)-f(0)\tau(u).$$

It follows that the volume of $SL(2,A)/SL(2,K)$ for the measure τ equals 1. □

Historic note

The zeta function of a central simple algebra over a number field was introduced by K. Hey in 1929, who showed his functional equation in the case where the algebra is a field. M. Zorn noticed in 1933 the application of the functional equation to the classification of quaternion algebra(§3). The results of K.Hey were generalized by H.Laptin [1], M.Eichler [4], and H.Maass [2] to the notion of L-functions with characters. Applying the adele technique to their study is made by Fusijaki 1, and the formulation of the most generality of zeta functions is due to R. Godement [1], [2]. One can find the development of their theories in T.Tamagawa [3], H. shimizu [3]. The application of the functional equation to the computationof Tamagawa numbers can be found in A.Weil [2].

Exercise

Riemann zeta function. Deduce from the functional equation (Theorem 2.2) that of the Riemann zeta function $\zeta(s)=\sum_{n\geq n}n^{-s}$, $Res>1$, with the known formula

$$\zeta(s)=\pi^{-s/2}\Gamma(s/2)\zeta(s)$$

is invariant by $s\mapsto 1-s$, or again :

$$\zeta(1-s)=\frac{2}{(2\pi)^s}\cos(\pi s/2)\Gamma(s)\zeta(s).$$

Prove then for every integer $k\geq 1$, the numbers $\zeta(-2k)$ are zero, the numbers $\zeta(1-2k)$ are nonzero and given by

$$\zeta(1-2k)=\frac{2(-1)^k(2k-1))!}{(2\pi)^{2k}}\zeta(2k)$$

and

$$\zeta(0)=-\frac{1}{2}.$$

We know Bernoulli numbers B_{2k} are defined by the expansion

$$\frac{x}{e^x-1}=1-x/2+\sum_{k\geq 1}(-1)^{k+1}B_{2k}\frac{x^{2k}}{(2k)!}.$$

Demonstrate

$$\zeta(2k)=\frac{2^{2k-1}}{(2k)!}B_{2k}\pi^{2k}.$$

Deduce the number $\zeta(1-2k)$ are rational and are given by the formula

$$\zeta(1-2k)=(-1)^k\frac{B_{2k}}{2k}.$$

Verify the following numerative table:

$$\begin{array}{lll} \zeta(-1) = -\frac{1}{2^2\cdot 3}, & \zeta(-3) = \frac{1}{2^3\cdot 3\cdot 5}, & \zeta(-5) = -\frac{1}{2^2\cdot 3^2\cdot 7} \\ \zeta(-7) = \frac{1}{2^4\cdot 3\cdot 5}, & \zeta(-9) = \frac{1}{3\cdot 2^2\cdot 11}, & \zeta(-11) = \frac{691}{2^3\cdot 3^2\cdot 5\cdot 7\cdot 13} \end{array} .$$

3.3 Cassification

We intend to explain how the classification theorem can be proved by zeta functions, and how one can deduce from it the reciprocal formula for Hilbert symbol and the Hasse-Minkowski principle for quadratic forms.

Theorem 3.3.1. *(Classification). The number $|Ram(H)|$ of ramified places in a quaternion algebra H over K is even. For every finite set S of the places of K with even number S, it exists one and only one quaternion algebra H over K, up to isomorphism, such that $S = Ram(H)$.*

Another equivalent statement of the theorem is formulated by an exact sequence :

$$1 \longrightarrow Quat(K) \xrightarrow{i} \oplus Quat(K_v) \xrightarrow{\varepsilon} \{\mp 1\} \longrightarrow 1,$$

where i is the mapping which assigns an algebra H the set of its localization modulo isomorphism, and ε is the Hasse invariant: it associates (H_v) with the product of the Hasse invariants H_v, i.e. -1 if the number of H_v which are fields is odd, 1 otherwise.
Proof of part of the classification thanks to the zeta functions.
If H is a field, we saw in Theorem 2.2 that $Z_H(s)$ has the simple poles at 0 and 1, and is holomorphic elsewhere. The expression Z_H in function of Z_K which we recall in (2.1) that

$$Z_H(s/2) = Z_K(s)Z_K(s-1)J_H(s)$$

where $J_H(s)$ has a zero of order $-2 + Ram(H)$ at point $s = 1$, shows the order of Z_H at point $s = 1/2$ equals the order $-2 + Ram(H)$. Then the fundamental result follows:
Property I.
Characterization of matrix algebra : for $H = M(2, K)$ if and only if $H_v = M(2, K_v$ for every place v.
It follows then (Lam [1], O'Meara [1]):

Corollary 3.3.2. *(Hasse-Minkowski principle for quadratic forms). Let q be a quadratic form over a global field of characteristic unequal 2. Then q is isotropic over K if and only if q is isotropic over K_v for every place v.*

We notice that in the two theorems, one can replaces "for every place" by " for every place possibly excluding someone"
We now explain how the Hasse-Minkowski principle can be derived from the theorem of the characterization of matrix algebra. Let n be the number of variables of the quadratic form q.
$n = 1$, there is nothing to prove.
$n = 2$, $q(x, y) = ax^2 + by^2$, up equivalence on K, and the principle is equivalent to the square theorem: $a \in {K_\times}^2 \leftrightarrow a \in K_v^{\times 2}$, $\forall v$. We shall give it a proof by in advantage of the zeta functions. If $L = K(\sqrt{a})$ is isomorphic locally to $K \oplus K$

everywhere, hence $Z_L(s) = Z_K(s)^2$ has a double pole at $s = 1$, this implies that L is not a field and then $a \in K^{\times 2}$.
$n = 3$, $q(x, y, z) = ax^2 + by^2 + z^2$, up to equivalence on K. Choosing H to be the quaternion algebra associating to $\{a, b\}$, the principle is equivalent to the characterization of matrix algebra.
$n \geq 4$, It turns back by induction to the precedent cases, cf. Lam [1],p.170. Since J_H and Z_K satisfy the functional equations:

$$J_H(s) = (-1)^{|Ram(H)|} \prod_{p \in Ram_f(H)} Np^{1-s} \cdot Z_H(2-s),$$

$$Z_K(s) = D_K^{s-1/2} Z_K(s).$$

We obtain a functional equation for Z_H:

$$Z_H(s) = (D_H^4 N(d_H)^2)^{\frac{1}{2}-s} (-1)^{|Ram(H)|} Z_H(1-s)$$

which, if comparing it with the functional equation (thm.2.2)$Z_H = D_H^{\frac{1}{2}-s} Z_H(1-s)$ obtained directly when H is a field, shows that $D_H = D_K^4 N(d_H)^2$, but immediately:
Property II.
The number of places ramified in a quaternion algebra is even.
In the case of characteristic different from 2, this statement is equivalent to the reciprocal formula of Hilbert symbol.

Corollary 3.3.3. *(Reciprocal formula of Hilbert symbol). Let K be a global field of characteristic different from 2. For two elements a, b of $K^\times$, let $(a, b)_v$ be their Hilbert symbol on K_v. We have the product formula*

$$\prod_v (a, b)_v = 1$$

where the product takes on every place v of K.

Application:
1) Choosing $K = \mathbb{Q}$ and for a, b two odd prime numbers, one can verifies the process for obtaining the quadratic reciprocal formula
2)Computation of symbol $(a, b)_2$. The Hilbert symbol of two rational numbers a, b on $\mathbb{Q}_p$ can be computed easily with the rule described in II,§1. We shall calculate $(a, b)_2$ by using the product formula:$(a, b)_2 = \prod_{v \neq 2} (a, b)_v$.
Before proving the property of existence of a quaternion algebra of the given local Hasse invariants, we extract some consequences of property I and property II above. The extension L/K are always assumed to be separable.

Corollary 3.3.4. *(Norm theorem in quadratic extension). Let L/K be a separable quadratic extension, and $\theta \in K^\times$. For θ to be a norm of an element in L if and only if θ is a norm of an element in $L_v = K_v \otimes L$ for every place v excluding possibly one.*

Proof. The quaternion algebra $H = \{L, \theta\}$ is isomorphic to $M(2, K)$ if and only if $\theta \in n(L)$ by I,2.4., and for that if and only if $H_v \simeq M(2, K)$ for every place v excluding possibly one byu property I and II. Since $H_v \simeq \{L_v, \theta\}$, the corollary is proved. □

Corollary 3.3.5. *(characterization of neutralized field). an extension of finite degree L/K neutralize a quaternion algebra H over K if and only if L_w neutralize H_v for every place $W|v$ of L.*

Proof. For L neutralizing H if and only if $L \otimes H \simeq M(2,K)$, According to Property I, if and only if that for every place w of L we have $(L \otimes H)_{w \simeq M(2,L_w}$. Using then the equality $(L \otimes H)_{w=L_w} \otimes H_v$ if $v = w|_K$; the second tensor product is taken on K_v. □

Lemma 3.3.6. *Let K be a local field, and $L = K(x)$ be a separable quadratic extension of K. Let $f(x)$ be the minimal polynomial of x over K:*

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

If $a, b \in K$ are enough near to $t(x)$, $n(x)$ respectively , then the polynomial

$$g(X) = X^2 - aX + b$$

is irreducible over K and has a root in L.

Proof. If $K = \mathbb{R}$, the discriminant $t(x)^2 - 4n(x)$ is strictly negative, hence $a^2 - 4b$ is so if a and b are enough near to $t(x)$ and $n(x)$. If $K \neq \mathbb{R}$, let $y \in K_s$ such that $y^2 = ay + b$. If $||a|| < A$ and $||b|| < A$, where A is a strictly positive constant, the inequalities finally prove that $||y|| < A$. We have $(y - x)(y - \bar{x}) = (t(x) - a)y = (n(x) - b)$, and hence can take $||(y - x)(y - \bar{x})||$ also small as we like if choosing a and b sufficiently near to $t(x)$ and $n(x)$. But $x \neq \bar{x}$ since the extension is separable, and it is possible to choose a and b such that

$$||y - x|| < \varepsilon, \quad ||y - \bar{x}|| > varepsilon.$$

There does not exist a K-automorphism f such that $f(x) = \bar{x}, \quad f(y) = y$! Thus $K(y) \supset K(x)$, and because of $[K(y) : K] \leq 2$, so $K(x) = K(y)$. □

This lemma and the theorem of approximation (thm. 2.2) allow us to obtain

Lemma 3.3.7. *It exists a separable quadratic extension L/K such that L_v/K_v is equal to a given separable extension for v belonging to a finite set of places.*

Theorem 3.3.8. *Let L/K be a quadratic extension and n the norm of L/K which is extended to ideals. We have $[K_A^\times : K^\times n(L_A^\times)] = 2$.*

Proof. Let χ be a character of $K_A^\times$ being trivial on $K^\times n(L_A^\times)$. Locally $\chi_v^2 = 1$, and $Z_v = K_A^\times \cap \{K^\times n(L_v^\times) \prod_{w \neq v} K_v^\times\}$ is closed in $K_A^\times$, because of

$$\chi = \prod_{v \in V} x_v, \quad \text{and} \quad K^\times n(L_A^\times = \bigcap_{v \in V} Z_v.$$

We shall also prove the inequality $[K_A^\times : K^\times n(L_A^\times] \leq 2$. We construct an element i_v of $K_A^\times$ not belongs to $K^\times n(L_A^\times)$:

$$i_v = (x_w), \quad \text{with} x_w = \begin{cases} 1, & \text{if } w \neq v \\ u_v, & \text{where } u_v \notin n(L_v^\times) \text{ if } w = v \end{cases},$$

for every place v of K such that L_v is a field. This element does not belong to $K^\times n(L_A^\times)$. If it belongs to $K^\times n(L_a^\times)$, it would exist an element $x \in K^\times$ such that $x \notin n(L_v^\times)$ but $x \in n(L_w^\times), \quad \forall w \neq v$. it contradicts with 3.4. □

Theorem 3.3.9. *(Maximal commutative subfield). For a quadratic extension L/K can be embedded in a quaternion field H if and only if that L_v is a field for $v \in Ram(H)$. Two quaternion algebras have always some common maximal commutative subfields (up to isomorphism) and the group $Quat(K)$ is defined.*

Proof. For a quadratic extension L/K to be contained in a quaternion field H/K it is obviously necessary that for every v of K the algebra L_v to be contained in H_v. therefore, L_v should be a field if H_v is a field. If $v \in Ram(H)$, v then can not be decomposed in L. Conversely, if this condition is satisfied, we then choose an element θ of the set

$$K^\times \cap \prod_{v \in Ram(H)} i_v n(L_a^\times)$$

which is non-empty since $|Ram(H)|$ is even by 3.7. Because that $\theta \in n(L_u^\times$ if $u \notin Ram(H)$, and $\theta \notin n(L_v^\times)$ if $v \in Ram(H)$, the quaternion algebra $\{L, \theta\}$ is isomorphic to H. If H and H' are two quaternion algebras over K, Lemma 3.6 allows to construct an extension L, such that L_v is a field if $v \in Ram(H) \cup Ram(H')$. The precedent results give then the inclusion in H and H'. The group $Quat(K)$ is hence defined, see I, the end of §2. □

The structure of group $Quat(K)$ is given by the following rules: if $H < H'$ are two quaternion algebras over K, we define HH' up to isomorphism by

$$H \otimes H' \simeq M(2, K) \oplus HH'.$$

It satisfies

$$(HH')_v \simeq H_v H'_v, \varepsilon(HH')_v = \varepsilon(H_v)\varepsilon(H'_v).$$

It follows that the ramification of HH' can be deduce from that of H and that of H' by

$$Ram(HH') = \{Ram(H) \cup Ram(H')\} - \{Ram(H) \cap Ram(H')\}.$$

The classification theorem results then from the property of existence:
Property III.
For two places $v \neq w$ of K there exists a quaternion algebra H/K such that $Ram(H) = \{v, w\}$.

Proof. If L/K is a separable quadratic extension such that L_v, L_w are the fields (3.6), and $\theta \in i_v i_w n(L_A^\times \cap k^\times$ (see their definition in the proof of 3.7), thus $Ram(\{L, \theta\}) = \{v, w\}$. □

Example: The quaternion algebra over $\mathbb{Q}$.
The quaternion algebras over $\mathbb{Q}$ denoted by $\{a, b\}$ generated by i, j satisfying

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

is ramified at the infinity if and only if a and b are both negative. Its reduced discriminant d is the product of a odd number of prime factors if $a, b < 0$ and of an even number otherwise. For example,

$$\{-1, -1\}, d = 2; \{-1, -3\}, d = 3; \{-2, -5\}, d = 5; \{-1, -7\}, d = 7;$$

$$\{-1, -11\}, d = 11; \{-2, -13\}, d = 13; \{-3, -119\}, d = 17; \{-3, -10\}, d = 30.$$

A rapid method for obtaining the examples is to use the likeness in order to avoid the study of $\{a,b\}_2$, with remarking that if p is a prime number with $p \equiv -1(mod4)$, then $\{-1,-p\}$ has the discriminant p, finally for $p \equiv 5mod(8)$, then $\{-2,-p\}$ has discriminant p. A little attempt allows to find easily a quaternion algebra with a given discriminant, that is to say, two integer numbers , of which the local Hilbert symbols are given in advance. For example,

$$\{-1,3\}, d = 6; \{3,5\}, d = 15; \{-1,7\}, d = 14.$$

If p is a prime, $p \equiv -1(mod4)$, then $\{2,p\}$ has the discriminant $2p$; if $p \equiv 5(mod8)$, then $\{-2,p\}$ has the discriminant $2p$.

3.4 Norm theorem and strong approximation theorem

. The norm theorem was proved in 1936-1937. Hasse and Schilling [1], Schilling [1],Maass [1], Eichler [3], [4] made contribution to its proof.
Its application to the euclidean order, and to the functional equation of L function was made by Eichler [5]. The strong approximation theorem for for the unit group with reduced norm 1 of the central simple algebra over number fields is due to Kneser [1], [2], [3]. A recent article have proved this theorem in the case of function field(Prasad [1]).

Theorem 3.4.1. *(Norm theorem) Let K_H be the set of the elements of K which are positive for the infinite real place of K and ramified in H. Then $K_H = n(H)$.*

Proof. The condition is natural since $n(\mathbb{H}) = \mathbb{R}_+$. Conversely let $x \in K_H^\times$; we construct a separable quadratic extension L/K such that :
– $x \in n(L)$,
– for every place $v \in Ram(H)$, L_v/K_v is a quadratic extension. Therefore, L is isomorphic to a commutative subgroup of H by 3.8, and $x \in n(H)$. This is an exercise of using the approximation theorem and the lemma on polynomials. Let S be a finite set of places of K. For the finite v we see that $H_v$contains an element of reduced norm π_v. Since H is dense in H_v, we see that H contains an element of reduced norm a uniform parameter of K_v, and by multiplying x with $n(h)$ for a suitable element $h \in H$, we can assume that for a finite set S of places of K:
x is a unit for $p \in S \cap P$.
We choose for every $v \in S$ an extension L_v such that : – $L_v - \mathbb{C}$ if v is real,
– L_v is the unramified quadratic extension of K_v if $v \in P \cap S$.
for every $v \in S$,it exists $y_v \in L_v$ of norm x. The minimal polynomial of y_v over K_v can be written as

$$p_v(X) = X^2 - a_v X + x.$$

We choose $a \in K$ very near to a_v if $v \in S$ (and the same if one needs an integer for every place of K excluding possibly one place $v \notin S$), so that the polynomial

$$p(X) = X^2 + aX + x$$

is irreducible and defines an extension $K \subsetneq K(y) \simeq K[X]/(p(X)) \subset X_s$, such that $K(y)_v = L_v$, if $v \in S$.

We apply this construction to $S = Ram(H)$ and hence obtain this norm theorem. □

We can even obtain a little bit stronger form of it.

Corollary 3.4.2. *Every element of K_H which is integral for every place excludin possibly one $w \notin Ram(H)$ is the reduced norm of ann element of H which is integral excluding possibly for w.*

The strong approximation theorem.
Let S be a nonempty set of places of K containing at least an infinite place if K is a number field. Let H^1 be the algebraic group induced by the quaternions which belongs to a quaternion field H over K and is of reduced norm 1. For a finite set $S' \subset V$ put

$$H^1_{S'} = \prod_{v \in S'} H^1_v.$$

Recall that H^1_v is compact if and only if $v \in Ram(H)$. Otherwise, $H^1_v = SL(2, K_v)$.

Theorem 3.4.3. *(Strong approximation). If H_{S^1} is not compact, then $H^1_K H^1_S$ is dense in H^1_A.*

The theorem was proved by Kneser [1], [2], [3] as an application of Eichler's norm theorem if K is a number field and $S \supset \infty$. The condition is natural. If H^1_S is compact, since H^1_K is discrete in H^1_A $H^1_S H^1_K$ is closed, and hence different from H^1_A definitely.
The condition introduced in the statement of this theorem play a basic role in the quaternion arithmetics.

Definition 3.14. *A nonempty finite set of the places of K satisfies the Eichler condition for H denoted by C.E., if it contains at least a place of K which is unramified in H.*

Proof. of the theorem 4.3. Let $\overline{H^1_K H^1_S}$ be the closure of $H^1_K H^1_S$ in H^1_A. It is stable under multiplication. It then suffices prove the theorem for every place $v \notin S$, for every element

$$(1) \qquad a = (a_w), \quad \text{with} \quad a_w = \begin{cases} a_v, & \text{integral over } R_v, \text{if } w = v \\ 1, & \text{if } w \neq v \end{cases}$$

for every neighborhood U of a, we have $H^1_K H^1_S \cap U \neq \varnothing$. For that, it is necessary $t(H^1_K H^1_S) \cap t(U) \neq \varnothing$, where t is the reduced trace which has been extended to adeles (see III, §3, the Example above Lemma 3.2). We have

$$(2) \qquad t(a) = t_w \quad \text{with} \quad t_w = \begin{cases} t(a_v), & \text{if } w = v \\ 2, & \text{if } w \neq v \end{cases}.$$

Since t is an open mapping, it suffices to prove that for every neighborhood $W \subset K_A$ of $t(a)$, we have $t(H^1_K H^1_S) \cap W \neq \varnothing$. It suffices to prove there exists $t \in K$ satisfying the following conditions: $*$ the polynomial $p(X, t) = X^2 - tX + 1$ is irreducible over K_v if $v \in Ram(H)$,
(3) $*$ t is near to $t(a)$ in K_A, that is to say, t is near to $t(a_v)$ in K_v for a finite number of places $w \neq v, w \notin S$.

We can prove these conditions in virtue of 3.6 and 1.4. Two elements of the same reduced trace and the same reduced norm are conjugate (I,2.1), and $H_A^\times = H_K^\times H_S^\times D^{-1}$ where D is compact in H_A by (3.4) hence $H_K^1 H_S^1 \cap \tilde{D}(U) \neq \varnothing$. Recall that if $x \in H^\times$, we denoted earlier $\tilde{x}(y) = xyx^{-1}$, $y \in H^\times$, and if $Z \subset H^\times$, we denote $\tilde{Z} = \{\tilde{z} | z \in \mathbb{Z}\}$, see I,§4, Exercise. There exists then $d \in D$ such that $\tilde{d}(a) \in \overline{H_K^1 H_S^1}$. Let (b) be an sequence of elements of $H_K^\times$ which converges in H_v to the v-adic part of d^{-1}. Therefore, $\overline{bd}(a) \in \overline{H_K^1 H_S^1}$ converges to a: it is true for v-adic by constructions, and if $w \neq v$, $a_{w=1}$. Finally it concludes that $a \in \overline{H_K^1 H_S^1}$. □

It will be found in 5.8 and 5.9 the applications of the theorem.

3.5 Orders and ideals

Fix a nonempty set S of the places of K, which contains the infinite places if K is a number field. Thus the ring

$$R = R_S = \{x \in K | x \in R_v, \forall v \notin S\}$$

is a Dedekind ring (Weil [1]).
Example. Let $S = \infty$, and $K \supset \mathbb{Q}$, then R is the integer ring of K. If S is reduce to one place, and K is a function field, then $R \simeq \mathbb{F}_p[T]$.
Let H/K be a quaternion algebra over K; the lattices, orders, and ideals in H are relative to R (see definition I,4).We study the orders and the ideals in virtue of their local properties. The present section is consists of three parts:
A: General properties of orders and ideals.
B: class Numbers and order types.
C: Trace formulae for the maximal inclusion.
We suppose frequently that S satisfying the Eichler condition defined above and denoted by C.E., in order to obtain the results more simply. The case where C.E. not satisfied will be treated in chapter V.
A:General properties.
Let Y be a lattice of H. We write $Y_v = R_v \otimes_R Y$ if $v \in V$. When $v \in S$ we have $R_v = K_v$, and $Y_v = H_v$.

Definition 3.15. *For every complete R-lattice Y of H, and for every place $v \notin S$ of K, the R_v-lattice $Y_v = R_v \otimes_R Y$ is called the localization of lattice Y at v.*

Since $S \supset \infty$, the places which not belong to S are finite. If (e) is a basis of H/K, the lattice X generated over R by (e) is a global lattice in H which can be obtained from the local lattices in H_v, $v \notin S$ in the way described in the following proposition.

Proposition 3.5.1. *Let X be a lattice of H. There exists a bijection between the lattices Y of H and the set of lattices $\{(Y_p) | Y_p$ is the lattice of H_p, $Y_p = X_p$, p.p.$\}$ given by the inverse mapping of one to another:*

$$Y \mapsto (Y_p)_{p \notin S} \quad \text{and} \quad (Y_p)_{p \notin S} \mapsto Y = \{x \in H | x \in Y_p, \forall p \notin S\}.$$

Proof. According to the definition of lattice (I.4), for a given lattice Y, there exists $a, b \in K^\times$ such that $aY \subset X \subset bY$. For almost every $v \notin \infty$, a_v, b_v are units. Thus $X_p = Y_p$, p.p. We shall prove $V \mapsto (V_p)_{p\notin S}$ is surjective. If $(Z_p)_{p\notin S}$ is a set of local lattices which are almost everywhere equal to X_p, we then set $Y = \bigcap_{p\notin S}(H \cap Z_p)$. We want to prove Y is a lattice, and $Y_p = Z_p$. There exists $a \in R$ such that $aX_p \supset Z_p \supset a_p^{-1}$ for every $p \notin S$. It follows $aX \supset Y \supset a^{-1}X$, hence Y is a lattice. Since $S \neq \varnothing$, according to 1.4, H is dense in $\prod_{p\notin S} H_p$. From this we have $H \cap (\pi Z_p) = Y$ is dense in πZ_p. in particular, Y is dense in Z_p, thus $Y_p = Z_p$ if $p \notin S$. We now prove $Y \mapsto (Y_p)_{p\notin S}$ is injective. let $Z \prod_{p\notin S}(Y_p \cap H)$. We claim that $Y = Z$. It is true that $Y \subset Z$, and there exists $a \in R$ such that $aZ \supset Y \supset Z$. Let $z \in Z$. There exists $y \in Y$ very near to z by p-adic for every place $p \notin S$, such that a is not a unit in R_p. In fact, we have $Y_p = Z_p$ if $p \notin S$, and we utilize the approximation theorem 1.4. There exists then $y \in Y$ such that $y - z \in aZ$. We conclude that $z \in Y$. The proposition is proved. □

Definition 3.16. *A property $\star$ of lattice is called a local property when a lattice Y has the property $\star$ if and only if Y_p has the property $\star$ for every $p \notin S$.*

Examples of local property: The properties for a lattice to be

1. an order,
2. a maximal order,
3. an Eichler order, i.e. the intersection of two maximal orders,
4. an ideal,
5. an integral ideal,
6. a two-sided ideal,

are the local properties. This can be deduced easily by the proposition 5.1. We utilize that if I is an ideal, then its left order $\mathcal{O}_l(I)$ (cf. I.4, above Prop.4.2) satisfies $\mathcal{O}_l(I)_p = \mathcal{O}_l(I_p)$ for all $p \notin S$.

Definition 3.17. *The level of Eichler order $\mathcal{O}$ is an integral ideal of R, denoted by N such that N_p is the level of $\mathcal{O}_p$ $\forall p \notin S$.*

Corollary 3.5.2. *Let I be an ideal of H, and $\mathcal{O}$ be an order of H. $n(I)$ denotes the reduced norm of I, and $d(\mathcal{O})$ the reduced discriminant of $\mathcal{O}$. Then we have*

$$n(I_p) = n(I)_p \quad \textit{and} \quad d(\mathcal{O}_p) = d(\mathcal{O})_p.$$

Proof. If (f) is a finite system of generators of I/R, by the definition (I. above the lemma 4.7) $n(I)$ is the R-ideal generated by $n(f)$. Moreover (f) is also a finite system of generators of I_p/R_p. It follows that $n(I_p) = n(I)_p$. By the definition in I,§4, above the lemma 4.9,

$$I^* = \{x \in H | t(xf) \in R, \forall f\}.$$

By the proposition 5.1 we obtain $(I_p)^* = (I^*)_p$. Replacing I by $\mathcal{O}$, and taking the reduced norm, we see that

$$d(\mathcal{O})_p = n(\mathcal{O}^{*-1})_p = [n(\mathcal{O}^*)^{-1}]_p = n(\mathcal{O}^*)_p^{-1} = n(\mathcal{O}_p^{*-1} = d(\mathcal{O}_p).$$

□

From II.1.7 and II.2.3 we obtain a characterization of maximal orders by their reduced discriminant. This permit us to use it for the construction of a maximal order, or to distinguish whether a given order is maximal.

Corollary 3.5.3. *For an order $\mathcal{O}$ to be a maximal order if and only if its reduced discriminant to be equal to*

$$d(\mathcal{O}) = \prod_{p \in Ram(H), p \notin S} p.$$

Set $d(\mathcal{O}) = D$; the reduced discriminant of an Eichler order of level N is equal to DN. However, the Eichler orders are not characterized by their reduced discriminant unless it is square-free. Since $(D, N) = 1$, it is equivalent to say that N is square-free. See exercise 5.3.
Example: let H be the quaternion field over $\mathbb{Q}$ of reduced discriminant 26, i.e. the field generated over $\mathbb{Q}$ by i, j satisfying

$$i^2 = 2, j^2 = 13, ij = -ji.$$

In fact, The Hilbert symbol $(2, 13)_v$ for the valuations v of $\mathbb{Q}$ are

$$(2, 13)_\infty = 1, \quad (2, 13)_{13} = (\frac{2}{13}) = -1, \quad (2, 13)_p = 1, \quad \text{if } p \neq 2, 13$$

and the product formula $\prod (2, 13)_v = 1$ gives $(2, 13)_2 = 1$. We can show that $\mathcal{O} = \mathbb{Z}[1, i, (1+j)/2, (i+ij)/2]$ is a maximal order if and only if it makes sure that

1. $\mathcal{O}$ is a ring,
2. the elements of $\mathcal{O}$ are integers; the reduced trace and the reduced norm are integers,
3. $\mathcal{O}$ is a $\mathbb{Z}$-lattice, $\mathbb{Q}(\mathcal{O}) = H$ (the last property is obvious for it),
4. The reduced discriminant of $\mathcal{O}$ equals 26.

Addition table: The trace of the sum of two integers is an integer , we verify that the norm remains integer in the following table.

	i	$(1+j)/2$	$(i+ij)/2$
i	$2i$	$i + (1+j)/2$	$i + (i+ij)/2$
	$(n = -8)$	$(n = -5)$	$(n = 4)$
$(1+j)/2$	$*$	$1 + j$	$(1 + i + j + ij)/2$
		$(n = -12)$	$(n = 3)$
$(1+ij)/2$	$*$	$*$	$1 + ij$
			$(n = 24)$

Multiplication table : The norm of the product of two integers is integer, we verify in the following table that the reduced trace remains integer too, and the product is stable in $\mathcal{O}$.

left\right	i	$(1+j)/2$	$(i+ij)/2$
i	2	$(i+ij)/$	$1 + j$
$(1+j)/2$	$(i - ij)/2 = i - (i+ij)/2$	$(7+j)/2 = 3 + (1+j)/2$	$-3i$
$(i+ij)/2$	$1 - j = 2 - 2(1+j)/2$	$(7i+ij)/2 = 3i + (i+ij)/2$	7

Therefore, $\mathcal{O}$ is an order.It is maximal because the reduced discriminant $|det(e_i e_j)|^{\frac{1}{2}}$ of the order $\mathbb{Z}[e_1, ..., e_4] = \mathbb{Z}[1, i, j, i]$ is $13 \cdot 8$hence the reduced discriminant of $\mathcal{O}$ which is deduced from the above order by a base change of determinant $1/4$ equals $13 \cdot 8/4 = 26$. We shall see other examples in exercise 5.1,5.2,5.6.
The properties of normal ideals.
These are such ideals whose left and right orders are maximal. The local-global correspondence in Lattices, and the the properties mentioned in chapter II show that these ideals are locally principal. We leave as an exercise the following properties (utilize the definitions of chapter I,8.5 and the properties of normal ideals of a quaternion algebra over a local field as we saw in chapter II,§1,2):
(a) A ideal to the left of a maximal order has a maximal right order.
(b) If the right order of ideal I is equal to the left order of ideal J, then the product IJ is an ideal and $n(IJ) = n(I)n(J)$. Its left order equals that of I, and its right order equals that of J.
(c) The two-sided ideals "commute" with the ideals in a sense of $CI = IC'$, where C is a two-sided ideal of the left order of I and C' is the unique two-sided ideal of the right order of I such that $n(C) = n(C')$.
(d)If I is an integral ideal of reduced norm AB, where A and B are integral ideals of R, then I can be factorized
into a product of two integral ideals of reduced norm A and B.
(e) The two-sided ideals of a maximal order $\mathcal{O}$ constitute a commutative group generated by the ideals of R and the ideals of reduced norm P, where P runs through the prime ideals of R which are ramified in H. We shall utilize the fact that the single two-sided ideal of a maximal order $\mathcal{O}_p$ of H_p of norm R_p is $\mathcal{O}_p$. These properties are true too for the the locally principal ideals of Eichler orders of a square-free level N.

B:The class number of ideals and the type number of orders .
Unfortunately, the property for an ideal being principal is not a local property. It is just one of the reasons that we work very often on adeles instead of working globally. It means that we often like to replace a lattice Y by the set (Y_p) of its localizations (5.1). We denote

$$Y_A = \prod_{v \in V} Y_v, \quad \text{with } Y_v = H_v \text{ if } v \in S.$$

From now on the orders in consideration will always be Eichler orders, and the ideals will be principal locally. Fix an Eichler order $\mathcal{O}$ of level N. The adele object associated with it is denoted by $\mathcal{O}_A$, the units of $\mathcal{O}_A$ by $\mathcal{O}_A^\times$, the normalizer of $\mathcal{O}_A$ in H_A by $N(\mathcal{O}_A)$.
The global-adele dictionary.
Ideals: The left ideals of $\mathcal{O}$ correspond bijectively with the set $\mathcal{O}_A^\times / H_A^\times$; the ideal I is associated with $(x_v) \in H_A^\times$ such that $I_p = \mathcal{O}_p x_p$ if $p \notin S$.
Two-sided ideals: correspond bijectively with $\mathcal{O}_A^\times \backslash N(\mathcal{O}_A)$.
Eichler orders of level N: correspond bijectively with $N(\mathcal{O}_A)\backslash H_A^\times$; the order $\mathcal{O}'$ is associated with $(x_v) \in H_A^\times$ such that $\mathcal{O}'_p = x_p^{-1}\mathcal{O}_p x_p$.
Classes of ideals: The classes of left ideals of $\mathcal{O}$ correspond bijectively with $\mathcal{O}_A^\times \backslash H_A^\times / H_K^\times$. The classes of two-sided ideals correspond bijectively with $\mathcal{O}_A^\times \backslash N(\mathcal{O}_A)/(H_K^\times \cap N(\mathcal{O}_A))$, the types of Eichler order of level N correspond bijectively with $H_K^\times \backslash H_A^\times / N(\mathcal{O}_A)$.

Theorem 3.5.4. *The class number of the ideals to the left of $\mathcal{O}$ is finite.*

Proof. According to the fundamental theorem 1.4, we have $H_A^\times = H_A^\times H_v^\times C$ for every place v,and infinity if K is a number field, and where C is a compact set (dependent of v). Since $\mathcal{O}_A^\times$ is open in $H_A^\times$ by the definition of the topology on it, and $\mathcal{O}_A^\times \supset H_v^\times$, where v satisfies the above conditions, then it follows that the class number of ideals is finite by using the global-local dictionary. □

Corollary 3.5.5. *The class number of two-sided ideals is finite. the type number of Eichler orders of level N is finite.*

In fact, these numbers are less than or equal to the number of the classes of left ideals of $\mathcal{O}$. Two Eichler orders of the same level being always tied by an ideal (of which the left order is one of these order, and the right order is the other one) since two Eichler orders of the same level are locally conjugate (ch.II), the number of classes of two-sided ideals of $\mathcal{O}$ not depends on the choice of $\mathcal{O}$, but more precisely on its level N. By contrast, the number of classes of two-sided ideals of $\mathcal{O}$ possibly depends on the choice of $\mathcal{O}$, or more precisely on the type of $\mathcal{O}$.
NOTATION. we denote by $h(D,N) = h(Ram(H),N)$
the class number of the ideals to the left of $\mathcal{O}$, by $t(D,n) = t(Ram(H),N)$
the type number of Eichler order of level N, and for $1 \leq i \leq t$, by $h_i'(D,N)$
the class number of two-sided ideals of an order of the type of $\mathcal{O}_i$, where $\mathcal{O}_i$ runs through a system of representative of Eichler orders of level N.

Lemma 3.5.6. *We have $h(D,N) = \sum_{i=1}^t h_i'(D,N)$.*

Proof. The types of orders correspond to the decomposition $H_A^\times = \bigcup_{i=1}^t N(\mathcal{O}_A)x_i H_K^\times$. Let $\mathcal{O}_i$ be the right order of ideal $\mathcal{O}x_i$. We have $N(\mathcal{O}_{i,A}) = x_i^{-1}N(\mathcal{O}_A)x_i$ and $\mathcal{O}_{i,A}^\times = x_i^{-1}\mathcal{O}_{i,A}^\times x_i$. It follows $N(\mathcal{O}_A)x_iH_K^\times = x_iN(\mathcal{O}_{i,A})H_K^i$ and $\mathcal{O}_A^\times \backslash N(\mathcal{O}_A)x_iH_K^\times/H_K^\times = \mathcal{O}_{i,A}^\times \backslash N(\mathcal{O}_{i,A})/(H_K \cap N(\mathcal{O}_{i,A})) = h_i'(D,N)$. □

In particular, if the class number of two-sided ideals does not depend on the chosen type, and is denoted by $h'(D,N)$, we then have the relation

$$h(D,N) - t(D,N)h'(D,N).$$

This is the case when S satisfies the Eichler's condition (see the beginning of this section): it is an application of the strong approximation theorem(Thm 4.1 and Thm. 4.3)

Definition 3.18. *Let $K_H = n(H)$ and let P_H be the group of the ideals of R generated by the elements of K_H. Two ideals I and J in R are equivalent in the restrict sense induced by H if $IJ^{-1} \in P_H$. Since H/K is fixed, we simply say "in the restrict sense".*

We denote by h the class number of ideals of K in the restrict sense. Recall $K_H = \{x \in K | x$ is positive for the real places being ramified in H. Therefore h only depends on K and the real places of $Ram(H)_\infty$.

Theorem 3.5.7. *(Eichler,[3],[4]). If S satisfies C.E., an ideal to the left of an Eichler order is principal if and only if its reduced norm belongs to P_H*

Corollary 5.7 (bis.) If S satisfies C.E., then

1. The class number $h(D,N)$ of the ideals to the left of an Eichler order of level N in a quaternion algebra H/K of reduced discriminant D is equal to h.

2. The type number of the Eichler order of level N in H is equal to $t(D,N) = h/h'(D,N)$, where $h'(D,N)$ is the class number of the two-sided ideals of an Eichler order of level N.

3. $h'(D,N)$ is equal to the class number in the restrict sense of the ideals belonging to the group generated by the square of the ideals of R, The prime ideal dividing D and the prime ideals I such that $I^m||N$ with a odd power.

Proof. The reduced norm induces a mapping:

$$\mathcal{O}_A^\times \backslash H_A^\times / H_K \simeq\rightarrow^n R_{A^\times} \backslash K_A^\times / K_H,$$

which is surjective , since $n(H_v^\times) = K_v^\times$ if $\notin Ram_\infty(H)$, and injective if $v \in R_\infty(H)$, $R_A^\times \supset K_v^\times$, since $H_A^\times \subset \mathcal{O}_A^\times H_K^\times$ by the approximation theorem 4.3 for H^1 and $n(\mathcal{O}_p\times) = R_p^\times$ if $p \notin S$. It follows the theorem and the part (1) of the corollary.
We have

$$n(N(\mathcal{O}_p)) = \begin{cases} K_p^\times, & \text{if } p|D \text{ or if } p^m||N \text{ with } m \text{ odd} \\ K_p^{\times 2} R_p^\times, & \text{otherwise} \end{cases}.$$

It follows that the group of reduced norms of two-sided ideals of an Eichler order of level N is generated by the squares of ideals of R and the prime ideals I which divide D, or such that $I^m||N$ with an odd power m. The class number of two-sided ideals of $\mathcal{O}$ is equal to the class number in the restrict sense of the norms of two-sided orders.It is then independent of the choice of $\mathcal{O}$ (among the orders of the same level). The type number of orders of a given level is then equal to the quotient of the class number of ideals (this number is independent of the level) by the class number of two-sided ideals of an order of the level. □

Exercise

5.5-5.8.

We consider an Eichler order $\mathcal{O}$, an element $x \in \mathcal{O}$, a two-sided ideal I of $\mathcal{O}$, such that x is prime to I, that is to say, $n(x)$ is prime to $n(I)$. We shall give a generalization of the theorem of Eichler on the arithmetic progressions:

Proposition 3.5.8. *The reduced norm of the set $x + I$ equals to the set $K_H \cap \{n(x) = J\}$ where $J = I \cap R$ if S satisfies C.E.*

Proof. We verify easily that it is true locally. If $x = 1$, we utilize:
a) the trivial relation $n(\begin{pmatrix} 1+\pi^n x & 0 \\ 0 & 1 \end{pmatrix}) = 1 + \pi^n x$,
b) if H_p/K_p is a field, then $H_p \simeq \{L_{nr}, u\}$ by II,1.7, and we have a well-known result (Serre [1]) that the units of L_{nr} being congruent to 1 modulo p^n is sent surjectively to the units of K_p being congruent to 1 modulo p^n.

If $x \neq 1$ and x is is a unit in $\mathcal{O}_p$ for every place p such that $I_p \neq \mathcal{O}_p$, and then we turn back to the precedent case. If $I_p = \mathcal{O}_p$ we use $n(\mathcal{O}_p) = I_p$. It follows the global result from the local result by means of 4.1 and 4.3. Choose $y \in K_H \cap \{n(x) + J\}$ such that
– $z \in H$,$n(z) = y$, is integer except for possibly $z \in S$,
– $h_v \in \mathcal{O}_v$, $n(h_v) = y, \forall v \in V$ and $h_p \in x + I_p$ if $p \notin S$.
There exists $u \in H^1_K$ very near to $z^{-1}h_v \in H^1_v$ excluding possibly a place $z \in S$. The element zu of reduced norm y can be chosen such that $zu \in \mathcal{O}$ and $zu \in x + I$. □

Corollary 3.5.9. *For every Eichler order $\mathcal{O}$ we have $n(\mathcal{O}) = K_H \cap R$.*

The proposition allows to decide whether a maximal order is euclidean. The non-commutativity is obliged to distinguish the notion of euclidean order by right and left.

Definition 3.19. *An order $\mathcal{O}$ is right euclidean if for every $a, b \in \mathcal{O}$ there exist $c, d \in \mathcal{O}$ with*

$$a = bc = d, d = 0 \quad or \quad Nn(d) < Nn(b)$$

where N is the norm defined by $N(x) = Card(R/Rx)$ if $x \in R$. We define the left euclidean in a natural way.

Definition 3.20. *We say that R is euclidean modulo W , where W is a set of real places of K, if for every $a, b \in R$ there exist $c, d \in R$ with $a = bc + d, d = 0$ or $Nd < Nb$ and d is positive for the places $w \in W$.*

Theorem 3.5.10. *If R is euclidean modulo $Ram_\infty(H)$, every maximal R-orderof H is left and right euclidean when S satisfies C.E.*

Proof. Let a, b belong to an order $\mathcal{O}$ of H. There exist $x, y \in R$ such that

$$n(a) = n(b)x + y \quad \text{with} \quad y = 0 \quad \text{or} \quad N(y) < Nn(b) \quad \text{and} \quad y \in K_H.$$

If $n(a), n(b)$ are prime to each other, $y \neq 0$, and according to 5.9, it exists $d \in \mathcal{O}$ such that

$$a \in I + d\text{with } n(d) = y, I \cap R = Rn(b)$$

where I is a two-sided ideal of $\mathcal{O}$. We can verify easily that $I \supset b\mathcal{O}$ from this it follows that there exist $c, d \in \mathcal{O}$ with

$$a = bc + d, Nn(d) < Nn(b).$$

Coming along $n(a), n(b)$ being prime to each other, we suppose that $\mathcal{O}$ is a maximal order. We begin by observing that we can assume a, b have no common left divisors, if one is interested in the right euclidean. The maximal R-orders are principal if R is euclidean modulo $Ram_\infty(H)$. We can suppose also that the irreducible divisor $P = \mathcal{O}x$ of the left ideal $\mathcal{O}a$ are distinct from that of the ideal $\mathcal{O}b$. We shall show that it exists an element $x \in \mathcal{O}$ such that $n(b)$ and $n((a - bx)$ are prime to each other, then the theorem will be proved. Let P be an irreducible divisor of $\mathcal{O}_{n(b)}$ in $\mathcal{O}$. If $b \in P$ then $a \notin P$ and for every $x \in \mathcal{O}$, $a - bx \notin P$. If $b \notin P$, then $a - bx \in P$ and $a - bx' \in O$ implies $b(x - x') \in P$, Hence $(x - x') \in P$. Therefore there exists an infinity of $x \in \mathcal{O}$ such that $a - bx \notin P$. The number of irreducible divisors of $\mathcal{O}_{n(b)}$ is finite, thus we can find x with the property $a - bx \notin P, \quad \forall P | \mathcal{O}_{n(b)}$. Then $n(b)$ and $n(a - bx)$ are prime to each other. □

Remark. (Beck)The non-maximal R-orders are never euclidean for the norm, if K is a number field

Proof. If $\mathcal{O}' \subsetneq \mathcal{O}$ is non-maximal R-order, it exists $x \in \mathcal{O}$ but $x \notin \mathcal{O}'$, and for every $c \in \mathcal{O}'$, $Nn(x-c) \geq 1$. If $x = b^{-1}a$, where $a, b \in \mathcal{O}'$, the division of a by b in $\mathcal{O}'$ is impossible. In the contra-example, $n(b)$ and $n(a)$ can not be rendered as being prime to each other. □

C:Trace formula for the maximal inclusions.
Let X be a nonempty finite set of places of K containing the infinite place if K is a number field. Let L/K be a quadratic algebra and separable over K, and B be a R-order of L. Let $\mathcal{O}$ be an Eichler order over R of level N in H, and DN be the discriminant of $\mathcal{O}$ (D is the product of places, identifying to the ideals of R and being ramified in H and not belonging to S).
For each $p \notin S$, it can be given a group G_p such that $\mathcal{O}_p^\times \subset G_p \subset N(\mathcal{O}_p$. For $v \in S$, set $G_v = H_v^\times$. The group $G_a = \prod_{v \in V} G_v$ is a subgroup of $H_A^\times$. Denote $G = G_A \cap H^\times$
We intend to consider the inclusions of L in H which is maximal with respect to $\mathcal{O}/B$ modulo the inner automorphisms induced by G. cf. I.5 and II.3. We obtain by an adele argument a "trace formula" which can be simplified if S satisfying Eichler's condition.

Theorem 3.5.11. *(Trace formula). Let $m_p = m_p(D, N, B, \mathcal{O}^\times)$ be the number of the maximal inclusions of B_p in $\mathcal{O}_p$ modulo $\mathcal{O}_p^\times$ for $p \notin S$. Let $(I_i), 1 \leq ileqh$ be a system of representatives of classes of ideals to the left of $\mathcal{O}$, $\mathcal{O}^{(i)}$ be the right order of I_i, and $m_{\mathcal{O}^\times}^{(i)}$ be the number of maximal inclusions of B in $\mathcal{O}^{(i)}$ modulo $\mathcal{O}^{(i)\times}$. we have*

$$\sum_{i=1}^{h} m_{\mathcal{O}^\times}^{(i)} = h(B) \prod_{p \in S} m_p$$

where $h(B)$ equals the class number of ideals in B.

Proof. If $\prod m_p = 0$, the formula is trivial, so suppose it is nonzero. We then can embed L in H so that for every finite place $p \notin S$ of K we have $L_p \cap \mathcal{O}_p = B_p$; we identify L with its image by a given inclusion. Consider then the set of the adeles $T_A = \{x = (x_v) \in H_A^\times\}$, such that for every finite place $p \notin S$ of K, we have $x_p L_p x_p^{-1} \cap \mathcal{O}_p = x_p B_p x_p^{-1}$ which describes the set of the maximal local inclusions of L_p in H_p with respect to $\mathcal{O}_p/B_p$. The trace formula is resulted from the evaluation by two different methods of number $Card(G_A \backslash T_A / L^\times)$.

$$(1) \qquad Card(G_A \backslash T_A / L^\times) = Card(B_A^\times \backslash L_A / L^\times) Card(G_A \backslash T_A / L_A^\times)$$

, where $B_A^\times = B_A \cap G_A$. we notice firstly that $Card(G_A \backslash T_A / L_A^\times)$ is equal to the product of the numbers m_p of maximal inclusions of B_p in $\mathcal{O}_p$ modulo G_p, and since the numbers are finite and almost always equal to 1 (cf ch.II,§3), then it is a finite number. Let X be a system of representatives of these double classes. The equivalent relation:

$$g_A t_A l_A l = t'_A l'_{A,t_{A'}} t'_A \in X, l_{A'} l'_A \in L_A, l \in L^\times, g_A \in G_A$$

is equivalent to

$$t_A = t'_A, l'_A = g'_A l_A l, g'_A \in t_A^{-1} G_A t_A \cap L_A = B'_A,$$

from (1). The second evaluation uses the disjoint union:

$$H_A^\times = \bigcup_{i=1}^{t} N(\mathcal{O}_A) x_i H_K^\times$$

and the adele objects $\mathcal{O}_A^{(i)} = x_i^{-1}\mathcal{O}_A x_i$, $G_A^{(i)} = x_i^{-1} G_A x_i$ correspond globally to a system of representatives of the type of Eichler orders of level N ,$\mathcal{O}^{(\rangle)} = H \cap \mathcal{O}_A^{(i)}$ and to the groups $G^{(i)} = H \cap G_A^{(i)}$. We shall prove :

$$(2) \qquad Card(G_A \backslash T_A / L^\times) = \sum_{i=1}^{t} Card(G_A^{(i)} \backslash N(\mathcal{O}_A^{(i)}/H^{(i)}) Card(G^{(i)} \backslash T^{(i)} / L^\times)$$

where $H^{(i)} = N(\mathcal{O}_A^{(i)} \cap H^\times$, $T^{(i)} = T_A \cap \mathcal{O}^{(i)}$. Remark that $Card(G^{(i)} \backslash T^{(i)} / L^\times)$ is the number of the maximal inclusions of B in $\mathcal{O}^{(i)}$ modulo $G^{(i)}$. we have the disjoint union

$$T_A = \bigcup_{i=1}^{t} N(\mathcal{O}) x_i T_i / L^\times \quad \text{disjoint union.}$$

On other hand, $Card(G_A \backslash N(\mathcal{O}_A) x_i T_i / L^\times) = Card(G_A^{(i)} \backslash N(\mathcal{O}_A^{(i)} / L^\times)$
$= Card(G_A^{(i)} \backslash N(\mathcal{O}_A^{(i)} / H^{(i)} Card(G^{(i)} \backslash T_i / L^\times)$. We denote $H'^{(i)}_G = Card(G_A^{(i)} \backslash N(\mathcal{O}_A^{(i)} / H_i)$ and $h_G(B) = Card(B'_A \backslash L_A / L^\times)$. When $G = \mathcal{O}^\times$ the numbers are respectively the class number of two-sided ideals of $\mathcal{O}^{(i)}$ and the class number of the ideals of B. The expressions (1) and (2) gives the Theorem(bis). Let $m_p = m_p(D, N, B, G)$ the number of the maximal inclusion of B_p in $\mathcal{O}_p$ modulo G_p, if $p \notin S$. Let $\mathcal{O}^{(i)}, 1 \leq i \leq t$ be a system of the representatives of the type of Eichler order of level N, and $m_G^{(i)}$ be the number of the maximal inclusion of B in $\mathcal{O}^{(i)}$ modulo G_i. We have by the precedent definition:

$$\sum_{i=1}^{t} H'^{(i)} m_G^{(i)} = h_G(B) \prod_{p \notin S} m_p.$$

The theorem is proved. □

Definition 3.21. *Let L/K be a separable quadratic extension. If p is a prime ideal of K, we define Artin symbol $(\frac{L}{p})$ by*

$$(\frac{L}{p}) = \begin{cases} 1, & \text{if } p \text{ can be decomposed in } L \ (L_p \text{ is not a field}) \\ -1, & \text{if } p \text{ is inertia in } L \ (L_p/K_p \text{ is an unramified extension}) \\ 0, & \text{if } p \text{ is ramified in } L \ (L_p/K_p \text{ is a ramified extension}) \end{cases}.$$

Definition 3.22. *Let B be a R-order of a separable quadratic extension L/K. We define Eichler symbol $(\frac{B}{p})$ to be equal to Artin symbol if $p \in S$ or B_p is a maximal order, and equal to 1 otherwise. The conductor $f(B)$ of B is the integral ideal $f(B)$ of R satisfying $f(B)_p = f(B_p), \forall p \notin S$.*

With these definitions the theorem II.3.1 and II,3.2 show that if the level N of the Eichler order $\mathcal{O}$ is square-free,

$$\prod_{p\notin S} m_p(D,N,B,\mathcal{O}^\times)\prod_{p|D}(1-(\frac{B}{p}))\prod_{p|N}(1+(\frac{B}{p}))$$

and according to the number is zero or not, we have

$$\prod_{p\notin S} m_p(D,N,B,N(\mathcal{O}^\times))=0 \quad \text{or} \quad 1.$$

It follows

Corollary 3.5.12. *If $\mathcal{O}$ is an Eichler order of a square-free level N,*

$$\sum_{i=1}^{h} m^{(i)}_{\mathcal{O}^\times} = h(B)\prod_{p|D}(1-(\frac{B}{p}))\prod_{p|N}(1+(\frac{B}{p}))$$

and

$$\sum_{i=1}^{h} m^{(i)}_{N(\mathcal{O})} = 0 \quad or \quad h'(B)$$

according to the precedent number is zero or not, where $h'(B)$ is the quotient of $h(B)$ by the class number of group of ideals of B generated by:
– the ideals of R,
– the prime ideal of B which is over an ideal of R and ramified in H and in B.

We compute $h(B)$ in practice by the Dedkind's formula [1], if K is a number field and $S=\{\infty\}$:

$$h(B)=h(L)N[f(B)]\prod_{p|f(B)}(1-(\frac{L}{p})Np^{-1})\cdot[B_L^\times : B^\times]^{-1}$$

where $h(L)$ is the class number of a maximal R-order B_L of L, and N is the norm of K over $\mathbb{Q}$. By definition, if I is an integral ideal of R,

$$N(I)=Card(R/I).$$

It is useful to extend the trace formulae (theorem 5.11 and 5.11 bis.) to all of the groups G which are contained in the normalizer of $\mathcal{O}$, and containing the kernel $\mathcal{O}^1$ of the reduced norm in $\mathcal{O}$.

Corollary 3.5.13. *With the notations of theorem 5.11 and 5.11 bis, if G is a group such that $\mathcal{O}^1\subset G\subset N(\mathcal{O}$, the number of the maximal inclusion of B in $\mathcal{O}$ modulo G satisfies*

$$m_G = m_{\mathcal{O}}[n(\mathcal{O}^\times) : n(G)n(B^\times)].$$

The above index is finite by the Dirichlet's theorem on the units, cf. chapter V below. In fact, it suffices to write $m_G = Card(G\backslash T/L^\times)$ and to notice that the inclusion f of L in H is maximal with respect to $\mathcal{O}/B$, Then we have

$Card(G\backslash\mathcal{O}^\times f(L^\times)/f(L^\times)) = Card(G\backslash\mathcal{O}^\times/f(B^\times)) = [n(\mathcal{O}^\times) : n(G)n(B^\times)]$.
It follows that $Card(G\backslash\mathcal{O}^\times tL^\times/L^{times}) = Card(G\backslash\mathcal{O}^\times/\tilde{t}(L^\times))$, where $\tilde{t}$ is the inner automorphism associated with t, is independent of $t \in T$.
The trace formula can be used for the computation of the the number of conjugate classes modulo G (for the definition see I.4): It allows to give an explicit form to Selberg's trace formula,and in its special case (trace of the Hecke operators, Selberg's zeta function) when the groups are provided by quaternion algebras.

Definition 3.23. *a conjugate class of $H^\times$ is separable if its elements are the roots in $H^\times$ of a polynomial $X^2 - tX + n$ which is irreducible and separable over K. We call t, n the reduced trace and reduced norm of the class respectively, and $X^2 - tX + n$ its characteristic polynomial.*

Recall (I.4) that the conjugate class modulo G of $h \in H^\times$ is

$$C_{G(h)} = \{ghg^{-1} | g \in G\}.$$

Corollary 3.5.14. *Let $X^2 - tX + n$ be a separable irreducible polynomial over K which has a root $h \in H^\times$. Let G be a Group such that $\mathcal{O}^1 \subset G \subset N(\mathcal{O})$. The number of conjugate classes in $\mathcal{O}$ modulo G with characteristic polynomial $X^2 - tX = n$ is equal to*

$$\sum_B m_G(B),$$

where B runs through the orders of $K(h)$ containing h,and $m_G(B)$ is defined in 5.13 and 5.11.

EXAMPLE.
Computation of the number of conjugate classes of $SL_2(\mathbb{Z})$ of reduced trace $t \neq \mp 2$. We obtain

$$(2) = \sum_B h(B).$$

If $x \in \mathbb{Q}_S$ is a root of $X^2 - tX + 1$, then B runs through the orders of $\mathbb{Q}(x)$ containing x, and we set

$$(2) = \begin{cases} 1, & \text{if } \mathbb{Q}(x) \text{ contains a unit with norm } -1 \\ 2, & \text{otherwise} \end{cases}.$$

If $t = 0, \mp 1$, we find two conjugate classes with reduced trace t.
When S satisfies the Eichler condition (definition §4.) C.E., the term of the left side of the trace formula can be simplified. Thus we obtain

Theorem 3.5.15. *If S satisfies C.E., with the notations of Theorem 5.11 and 5.11 bis, the number of maximal inclusion of B in $\mathcal{O}$ Modulo G is equal to dm for $1/d$ the type of Eichler of level N and is equal to 0 for the others, with*

$$m = h_G(B)/h \prod_{p \notin S} m_p,$$

$$d = [K_A^\times : R_A^\times n(T_A)]$$

where h is the class number of ideals of R in the restrict sense induced by H.

Proof. The approximation theorem 4.3 of H^1 and the fact that S satisfies E.C. (thus $G_A \supset H_v^\times, v \notin Ram(H)$) lead to
1) $H^{'(i)}$ is independent of $\mathcal{O}^{()}$, it equal the class number of two-sided ideals of an Eichler order of level N.
2) If $T_A \neq \varnothing$, the type number of Eichler orders of level N which B can be embedded maximally in is equal to $1/[K_A^\times : R_A^\times n(T_A)]$ times the total type number. In fact, if B is embedded maximally in one of these orders $\mathcal{O}$, the other orders in which B is embedded maximally are the right order of ideals I with $I_p = \mathcal{O}_p x_p$ if $p \notin S$, where $(x_p) \in T_{A \cap \prod_{p \notin S}} H_p^\times$. We utilize then the theorem 5.7,5.8 of ideal class when E.D. is satisfied.
3) The number of maxima inclusions of B in $\mathcal{O}$ modulo G, if it is not zero, is independent of the choice of the Eichler order $\mathcal{O}$ of level N. Actually, the natural mapping $G\backslash T/L^\times \to G_A\backslash T'_A/L^\times$ is bijective if $T'_A = \{x \in T_a | n(x) \in K'\}$. It is obviously injective, and it is surjective because of $T'_A \subset G_A(H \cap T_a) \subset G_A T$. The properties 1), 2), 3) complete the proof of the theorem. □

In order that the theorem 5.15 to be applicable it is useful to know when the number d in consideration is equal to 1. In this case all of the Eichler orders of a given level play the same role.

Proposition 3.5.16. *Suppose S satisfies C.E.. With the notations of the precedent theorem, the number of the maximal inclusions of B in an Eichler order of level N modulo G is independent of the choice of the order, and is equal to m if $H \neq M(2, K)$ or if it exists a place such that:*
1) v is ramified in L,
or
2) $v \in S$, v is not decomposed in L.

Proof. Since $T_A \supset L_A^\times N(\mathcal{O}_A)$, we raise d to $d' = [K_A^\times : K^\times n(L_A^\times) R_A^\times n(N(\mathcal{O}_A))]$ and use the theorem 3.7. If there exists a place v such that $K_v^\times \neq n(L_v^\times)$, or turning back to the same thing that v is not decomposed in L, and such that $K_v^\times$ is contained in the group $K^\times n(L_A^\times) R_A^\times n(N(\mathcal{O}_A))$, then the degree d' is 1.Since $K_A^\times \subset R_A^\times$ if $v \in S$, the condition 2) is valid immediately for whole H. It is automatically satisfied if there exists an infinite place ramified in H. If p is a finite place ramified in L, then $K_v^\times = R_v^\times = R_v^\times n(L_v^\times)$ and $d' = 1$. If p is a finite place ramified in H, then $K_v^\times = n(N(\mathcal{O}_v))$ and hence $d' = 1$. □

When the number of quadratic extension L/K unramified is finite, we can say that in general the number of maximal inclusion of B in $\mathcal{O}$ only dependent on $\mathcal{O}$ by intervening of its level. Therefore, in general, the number of conjugate classes in $\mathcal{O}$ modulo G , with the given characteristic polynomial, only depends on $\mathcal{O}$ by its its level, if S satisfies C.E.

Corollary 3.5.17. *Suppose that S satisfies C.E. With the notations of 5.12 if $K(h)/K$ satisfies the condition of 5.16 and if N is square-free, then*

$$\sum_{h \in B} \frac{h(B)}{h} \prod_{b|D} (1 - (\frac{B}{p})) \prod_{p|N} (1 + (\frac{B}{p}))$$

is equal to the number of conjugate classes in $\mathcal{O}$ modulo $\mathcal{O}^\times$, of the characteristic polynomial being equal to that of h.

We shall obtain easily with 5.12 and 5.13 the correspondent formula for the conjugate classes modulo $\mathcal{O}^1$ or $N(\mathcal{O})$.

Exercise

1. Prove the quaternion field over $\mathbb{Q}$ of reduced discriminant 46 is generated by i, j satisfying $i^2 = -1, j^2 = 23, ij = -ji$ and $\mathcal{O} = \mathbb{Z}[1, i, j, (1 + i + j + ij)/2]$ is a maximal order.

2. Prove the quaternion field over $\mathbb{Q}$ is a maximal order if:

$$p = 2, \{a, b\} = \{-1, -1\}, \mathcal{O} = \mathbb{Z}[1, i, j, (1 + i + j + ij)/2];$$
$$p \equiv -1 mod 4, \{a, b\} = \{-1, -p\}, \mathcal{O} = \mathbb{Z}[1, i, (i + j)/2, (1 + ij)/2];$$
$$p \equiv 5 mod 8, \{a, b\} = \{-2, -p\}, \mathcal{O} = \mathbb{Z}[i, (1 + i + j)/2, j, (2 + i + ij)/4];$$
$$p \equiv 1 mod 8, \{a, b\} = \{-p, -q\}, \mathcal{O} = \mathbb{Z}[(1 + j)/2, (1 + aij)/2, ij]$$

   where q is a positive integer which is congruent to -1 modulo $4p$, and a is an integer which is congruent to ∓ 1 modulo q. We can find in Pizer [6] a method which allows to obtain the Eichler order of level N explicitly (one is permitted $p|N$ to the condition that the local order at p is isomorphic to the canonical order of Exercise II,4.4.

3. Let p be a prime ideal of R, which is prime to the reduced discriminant D of H/K, where R, K, H are defined as that in §5. Using II. 2.4, II. 2.6, III. 5.1, prove
   a) $\forall n \geq 2$, there exist the orders in H of the reduced discriminant Dp^n which are not the Eichler orders.
   b) every order in H of reduced discriminant Dp is an Eichler order.

4. Prove the normalizer $N(\mathcal{O})$ of an order of H/K (with the notation in §5) satisfies
$$N(\mathcal{O}) = \{x \in H | x \in N(\mathcal{O}_p), \forall p \notin S\}.$$
   Suppose that $\mathcal{O}$ is an Eichler order. Prove the group $N(\mathcal{O})/K^\times \mathcal{O}^\times$ is a finite group which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ where m is less or equal to the number of prime divisors of the reduced discriminant of $\mathcal{O}$.

5. Let $S = \infty$, K a number field and h^+ the class number of ideals of K in the restrict sense induced by all of the classes real infinite places of K. Prove
   a) if h^+ is odd, every quaternion algebra over K which is unramified at least at one infinite place, and contains a single type of Eichler order (over the integer ring of K) of a given level.
   b) if $h^+ = 1$, with the same hypothesis as in a) all of the Eichler orders are principal.
   In particular if $K = \mathbb{Q}$, every quaternion algebra $H/\mathbb{Q}$ such that $H \otimes \mathbb{R} \simeq M(2, \mathbb{R})$ contains a unique Eichler order $\mathcal{O}$ of a given level up to conjugations. This Eichler order is principal. If DN is its level, then the group $N(\mathcal{O})/\mathbb{Q}^\times \mathcal{O}^\times$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$, where m is the number of prime divisors of DN (Exercise 5.4).

6. Tensor product. With the notations of this section, let H_i/K be the quaternion algebras such that
$$D = H_1 \otimes H_2 = H_0 \otimes H_3$$

with the R-orders $\mathcal{O}_i$ of H_i, and t_i, n_i, d_i be the reduced trace, the reduced norm, the reduced discriminant of $\mathcal{O}_i$ in H_i respectively. Set

$$T(h_i \otimes h_j) = t_i(h_i)t_j(h_j), N(h_i \otimes h_j) = n_i(h_i)n_j(h_j)$$

if $i + j = 3, h_i \in H_i$. Verify the reasonableness of the definitions of T, N.Give their properties, in particular prove that T is K-bilinear, non-degenerate. Let $\underline{\mathcal{O}}$ be an R-order of D, and

$$\underline{\mathcal{O}}^* = \{x \in D | T(x\underline{\mathcal{O}}) \subset R\}.$$

Verify that $N(\underline{\mathcal{O}}^*)^{-2}$ is the ideal generated by

$$\{det(T(x_i x_j)) | 1leqi \leq 16, x_i \in \underline{O}\}.$$

We set $d(\underline{O}) = N(\underline{O}^*)^{-1}$. Verify $\mathcal{O}_i \otimes \mathcal{O}_j, i + j = 3$, is an order of D satisfying

$$d(\mathcal{O}_i \otimes \mathcal{O}_j) = d_i d_j.$$

Choosing $H_0 = M(2, K)$, and $\mathcal{O}_0, \mathcal{O}_3$ the maximal orders, we obtain a maximal order $\mathcal{O}_0 \otimes \mathcal{O}_\ni$ of D of which the discriminant $d = d_3$ is the common discriminant of the maximal orders of D.

7. Prove that in $M(2, K)$ a system of the representatives of types of Eichler orders of level N over R (with notations in this section) consists of the orders:

$$\begin{pmatrix} R & I^{-1} \\ NI & R \end{pmatrix},$$

where I runs through a system of of ideals of R modulo the group generated by the principal ideals , the square of ideals, and the prime ideals J such that $J^m || N$ with an odd power.

8. Eichler-Brandt matrices (Brandt [1],[2], Eichler [8] p.138). The notations are that in §5. let I_i be a system of representatives of the ideals to the left of a given order $\mathcal{O}$. We construct the matrices called Eichler-Brandt as follows,

$$P(A) = (x_{i,j}(A))$$

where A is an ideal of R and $x_{i,j}(A)$ is the number of integral ideals of reduced norm A which is equivalent from right to $I_i^{-1} I_j$. The ideal A defines a permutation of the indices $f : I_i A$ is equivalent to $I_{f(i)}$. It defines the matrix of this permutation :

$$L(A) = (d_{i,f(i)}), d_{i,j} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}.$$

Prove the following properties: let $\mathcal{O}$ be an Eichler order,
a) The sum of the column of $P(A)$ is the same for every column . Denote it by $c(A)$.
b) The formula for $c(A)$:

$$\begin{array}{ll} c(A)c(B) = c(AB) & \text{if } (A, B) = 1 \\ c(p^a) = 1 & \text{if } p|D \\ c(p^a) = (Np^{a+1} - 1)/(Np - 1) & \text{if } p \nmid DN \\ c(p^a) = 2(Np^{a+1} - 1)/(Np - 1) & \text{if } p||N \end{array} .$$

c) The multiplication rule for $P(A)$:

$$\begin{array}{ll} P(A)P(B) = P(AB) & \text{if } (A,B)=1 \\ P(p^a)P(p^b) = P(p^{a+b}) & \text{if } p|D \\ P(p^a)P(p^b) = \sum_{n=0}^{b} N(p)^n P(p^{a+b-2n})L(p^{-1})^n, a \geq b, & \text{if } (p,DN)=1 \end{array}.$$

d) The Brandt's matrices and the matrices of permutation generate a commutative R-algebra.

9. We still keep the notations of §5. Let I be the model of two-sided ideal of H, see the definition in I. the place above Theorem 4.5. We say an element $x \in H^\times$ is congruent multiplicatively to 1 modulo I,written as

$$x \equiv 1 \quad mod^\circ I,$$

if there exists a maximal order $\mathcal{O}$, and $a, b \in \mathcal{O}$ such that

$$x = ab^{-1}, a, b\text{are prime to } I,\ a - b \in I.$$

a)Prove that $x \equiv 1 \quad mod^\circ I$ if and only if there exist two elements $a, b \in H^\times$ such that

$$s = ab^{-1}, a, b, a+b, ab \quad \text{are integer,} \quad n(a), n(b) \quad \text{are prime to} \quad I, \text{and} \quad a-b \in I.$$

b) we extend naturally the definition of the multiplicatively congruence over K to the quaternion algebra over the local field and to the ideals. An element $x \in H_A$ is congruent multiplicatively to 1 modulo I, if its local components x_p for $p \notin S$ satisfy

$$x_p \equiv 1 \quad mod^\circ I_p.$$

When these notions are defined, we by $X(I)$ denote the set of elements of X which are congruent multiplicatively to 1 modulo I. Prove that if S satisfies C.E., then $H_S^1 H_K^1$ is dense in $H_A^1(A)$
c) Prove $n(H(I)) = K_H \cap K(J)$ if $J = R \cap I$.
d) Prove that if S satisfies C.E., an ideal to the left of a maximal order $\mathcal{O}$ is generated by an element of $H(I)$ if and only if its reduced norm is generated by an element of $K_H \cap K(J)$.

10. Corestriction. Let H/L be a quaternion algebra over a quadratic field L. We intend to determine the corestriction $D = cor_{L/\mathbb{Q}}(H)$ of H to $\mathbb{Q}$, see I,exercise 2.1. Prove, if v is a place of $\mathbb{Q}$, and H_v is the quaternion field over $\mathbb{Q}_v$, we have:

$$D_v \simeq M(2, H_v)$$

if v is lifted in L to two distinct places, and if one and only one of the two places is ramified in H.
we have:

$$D_v \simeq M(4, \mathbb{Q}_v)$$

in the other cases.

11. Symbols. Let $K/\mathbb{Q}$ be a quadratic extension of discriminant $d \equiv 0 \quad \text{or} 1 \quad mod(4)$. Prove the Artin symbol $(\frac{L}{p})$ is equal to the Legendre symbol $(\frac{d}{p})$.

Chapter 4

Applications to Arithmetic Groups

Let $(K_i^\times)$ be a nonempty finite set of local fields. Consider the group

$$G^1 = \prod_i SL(2, K_i').$$

we are interested in some discrete subgroups of finite covolume of G^1. More precisely, they are obtained in such a way: consider a quaternion algebra H/K over a global field K such that there exist a set S of places of K satisfying
— $(K_v^\times)_{v\in S} = (K_i)$ up to permutation.
— no any place $v \in S$ is ramified in H. Every archimedean place not belonging to S is ramified in H.
These groups play an important role in various domains. Their usefulness will be well studied soon in utilizing the arithmetic of quaternions (chapter III).

4.1 Quaternion groups

Fix a global field K, a quaternion algebra H/K, a set S of places of K containing ∞ and satisfying Eichler's condition denoted by C.E.. WE consider the group

$$G^1 = \prod_{v\in S, v\notin Ram(H)} SL(2, K_v).$$

This group is non-trivial because S contains at least an unramified place in H. We denote by $R = R_{(S)}$ the elements of K integral relative to the places which do not belong to S, and by Ω the se of R-orders of H. We are interested in the quaternion groups of reduced norm 1, in the orders $\mathcal{O} \in \Omega$:

$$\mathcal{O}^1 = \{x \in \mathcal{O} | n(x) = 1.$$

For each place v we fix an inclusion of K in K_v, and choose an inclusion $\varphi_v : H \to H_v'$, where

$$H_v' = \begin{cases} M(2, K_v), & \text{if } v \notin Ram(H) \\ \mathbb{H}_v, & \text{if } v \in Ram(H) \end{cases}$$

where $\mathbb{H}_v$ denotes the quaternion field over K_v. From this we obtain an inclusion

$$\varphi : H \to \prod_{v \in S, v \notin Ram(H)} M(2, K_v) = G$$

which send $\mathcal{O}^\infty$ on a subgroup of G^1. By abuse of notations, we identify H'_v with H_v in sequel. Note that two inclusion φ, φ' is different by an inner automorphism of $G^\times$

Theorem 4.1.1. *(1) The group $\varphi(\mathcal{O}^1)$ is isomorphic to $\mathcal{O}^1$. It is a discrete subgroup, of finite covolume of G^1. It is cocompact if H is a field.*
(2) The projection of $\varphi(\mathcal{O}^1)$ onto a factor $G' = \prod_v SL(2, K_v)$ of G^1 , with $1 \neq G' \neq G^1$, is equal to $\mathcal{O}^1$. It is dense in G'.

Proof. The nontrivial part of the theorem is an application of the fundamental theorem III.1.4 and III.2.3. The isomorphism with $\mathcal{O}^1$ is trivial since the image of $\mathcal{O}^1$ in G' with $1 \neq G'$ is $\prod \varphi_v(\mathcal{O}^1)$ which is isomorphic to $\mathcal{O}^1$. The idea is to describe the group H^1_A/H^1_K. Set

$$U = G^1 \cdot C \quad \text{with } C = \prod_{v \in S \quad \text{and } v \in Ram(H)} \mathbb{H}^1_v \prod_{v \notin S} \mathcal{O}^1_v.$$

The group U is an open subgroup in H^1_A satisfying:

$$H^1_A = H^1_K \quad \text{and } H^1_K \, U = \mathcal{O}^1.$$

From this we deduce a bijection between

$$H^1_A/H^1_K U \quad \text{and } U/\mathcal{O}^1.$$

According to III.1.4, and III.2.3, we have
(1) H^1_K is discrete in H^1_A of the finite covolume being equal to $\tau(H^1 = 1$, cocompact if H is a field.
According to III.4.3, we have
(2) $H^1_K G''$ is dense in H^1_A if $G'' = \prod SL(2, K_v)$ with $i \neq G''$.
It follows
(1) $\mathcal{O}^1$ is discrete in U of finite covolume being equal to 1 for the Tamagawa measures, cocompact if H is a field.
(2) The image of $\mathcal{O}^1$ in $G \cdot C$ is dense.
We thus utilize the following lemma for finishing the proof of theorem 1.1.

Lemma 4.1.2. *Let X be a locally compact group, Y a compact group, Z the direct product $X \cdot Y$, and T a subgroup of Z with its projection V in X. We have the following properties:*
a) If T is discrete in Z, then V is discrete in X. Moreover, T is of a finite covolume (resp. cocompact) in Z if and only if V has the same property in X.
b) If T is dense in Z, then V is dense in X.

Proof. a) Suppose K to be discrete in Z. For every compact neighborhood D of the unit in X, we show that $V \cap D$ has only a finite number of elements. In fact, $X \cap (D \cdot C)$ has a finite number of elements, being great or equal to that of $V \cap D$. Hence V is discrete in X. Let $F_T \subset Z, F_V \subset X$ be the fundamental sets of T in Z, and of V in X. It is clear that $F_V \cdot C$ contains a fundamental

set of T in Z, and the projection of F_T in X contains a fundamental set of V in X. (a) has been deduced.
b) Suppose that T is dense in Z. every point $(x, y) \in X \cdot Y$ is the limit of a sequence of points $(v, w) \in T$. Hence every point $x \in X$ is the limit of a sequence of points $v \in V$, and V is dense in X. □

Therefore, the theorem is proved. □

Definition 4.1. *Two subgroups X, Y of a group Z are commensurable if their intersection $X \cap Y$ is of a finite index in X and Y. The commensurable degree of X with respect to Y is*

$$[X : Y] = [X : (X \cap Y)][Y : (X \cap Y)]^{-1}.$$

The commensurator of X in Z is

$$C_Z(X) = \{x \in Z | X \quad \text{and } xXx^{-1} \text{ is commensurable}\}.$$

Definition 4.2. *We call the group $\varphi(\mathcal{O}^1)$ a quaternion group of G^1. A subgroup of G^1 which is conjugate in G^1 to a commensurable group with a quaternion group (hence of the form $\varphi(\mathcal{O}^1)$ for an appropriate choice of a given K, H, S, φ, Ω) is called an arithmetic group.*

We leave the verification of the following elementary lemma as an exercise to readers.

Lemma 4.1.3. *Let Z be a locally compact group, X and Y be two subgroups of Z Which are commensurable. Therefore X is discrete in Z if and only if Y is discrete in Z. Moreover, X is of a finite covolume (resp. cocompact) if and only if Y is of a finite covolume (resp. cocompact). In this case, we have :*

$$vol(Z/X)[X : Y] = vol(Z/Y).$$

EXAMPLE.
A subgroup Y of a finite index of a group X is commensurable to X. The commensurable degree $[X : Y]$ is the index of Y in X. The commensurator of Y in X is equal to X. For every $x \in X$, we have $[X : xYx^{-1}] = [x : Y]$.

Remark 4.1.4. *Takeuchi ([1]-[4]) determined all the arithmetic subgroup of $SL(2, \mathbb{R})$ which is triangular, that is to say, it admit a presentation:*

$$\Gamma =< \gamma_1, \gamma_2, \gamma_3 | \gamma_1^{e_1} = \gamma_2^{e_2} = \gamma_3^{e_3} = \gamma_1\gamma_2\gamma_3 = \mp 1 >,$$

where e_i are integers, $2 \leq e_i \leq \infty$. He determined the commensurable class of a quaternion group in $SL(2, \mathbb{R})$ too.

Proposition 4.1.5. *The groups $\mathcal{O}^1$ for $\mathcal{O} \in \Omega$ are pairwise commensurable. The commensurator of a pair in*

$$G^{\times} = \prod_{v \in S, v \notin Ram(H)} GL(2, K_v)$$

is equal to $Z\varphi(H^{\times})$, where Z is the center of $G^{\times}$.

Proof. The first part comes from Proposition 1.4. If $x \in G^\times$ belongs to the commensurator of $\varphi(\mathcal{O}^1)$, it induces an inner automorphism $\tilde{x}$ fixing $\varphi(H)$. Every automorphism of $\varphi(H)$ fixing $\varphi(K)$ pointwise is inner. Therefore $x \in Z\varphi(H^\times)$. Inversely it is clear that $Z\varphi(H^\times)$ is contained in the commensurator of $\varphi(\mathcal{O}^1)$ in $G^\times$. □

Definition 4.3. *Let I be a two-sided integer of an order $\mathcal{O} \in \Omega$. The kernel $\mathcal{O}^1(I)$ in $\mathcal{O}^1$ of the canonical homomorphism : $\mathcal{O} \to \mathcal{O}/I$ is called the principal congruent group of $\mathcal{O}^1$ modulo I. A congruent group of $\mathcal{O}^1$ modulo I is a subgroup of $\mathcal{O}^1$ containing $\mathcal{O}^1(I)$.*

The congruent group are of the commensurable groups among them. We have

$$[\mathcal{O}^1 : \mathcal{O}^1(I)] \leq [\mathcal{O} : I].$$

If $\mathcal{O}'$ is an Eichler order of level N contained in a maximal order $\mathcal{O}$, then the group $\mathcal{O}'^1$ is a congruent group of $\mathcal{O}^1$ modulo the two-sided ideal $N\mathcal{O}$. The groups so constructed with the Eichler orders and the principal groups are the groups for which we have certain arithmetic information:
– the value of covolume, indices (Theorem 1.7),
– the value of the number of conjugate classes of a given characteristic polynomial(III. 5.14,and 5.17).
Partially for this reason we often encounter them. Another collection of groups we encounter sometimes(for the same reason). They are the normalizers $N(\varphi(\mathcal{O}^1))$ in G^1 of groups $\varphi(\mathcal{O}^1)$, where $\mathcal{O}$ is an Eichler order. The quotient groups $N(\varphi(\mathcal{O}^1))/\varphi(\mathcal{O}^1$ are of type $(2, 2, ...)$.
We deduce from IV.5.14,5.16,5.17, and exercise 5.12 the next proposition:

Proposition 4.1.6. *Every group $\mathcal{O}^1$ for $\mathcal{O} \in \Omega$ contains a subgroup of finite index which contains only the the elements different from unit and of finite orders.*

The relation $\tau(H^1) = 1$, in the form $vol(G^1 \cdot C/\mathcal{O}^1) = 1$, allow us to compute the covolume of $\varphi(\mathcal{O}^1)$ in G^1:

$$vol(G^1/\varphi(\mathcal{O}^1)) = vol(C)^{-1}$$

for Tamagawa measures. By using the definition of

$$C = \prod_{v \in S, \text{ and } v \in Ram(H)} \mathbb{H}^1_v \prod_{p \notin S} \mathcal{O}^1_p$$

we can then compute the the global commensurable degree from the local commensurable degrees.

Theorem 4.1.7. *The commensurable degree of two groups $\mathcal{O}^1, \mathcal{O}'^1$ for $\mathcal{O}, \mathcal{O}' \in \Omega$ is equal to the product of the local commensurable degrees:*

$$[\mathcal{O}^1 : \mathcal{O}'^1] = \prod_{p \notin S} [\mathcal{O}^1_p : \mathcal{O}'^1_p] = \prod_{p \notin S} vol(\mathcal{O}^1_p) vol(\mathcal{O}'^1_p)^{-1}.$$

For Tamagawa measure,

$$vol(G^1/\varphi(\mathcal{O}^1))^{-1} = \prod_{v \in Ram(H) and\ v \in S} vol(H^1_v) \prod_{p \notin S} vol(\mathcal{O}^1_p).$$

The explicit formulae (II,exercise 4.2,4.3) of the local volumes for the Tamagawa measures have obtained already for the principal congruent groups obtained with the Eichler orders. By using these we obtain for example

Corollary 4.1.8. *If $\mathcal{O}$ is a maximal order, then*

$$vol(G^1/\varphi(\mathcal{O}^1))^{-1} = \zeta_K(2)(4\pi^2)^{-|Ram_\infty(H)|}D_K^{3/2}\prod_{p\in Ram_f(H)}(Np-1)\prod_{p\in S\cap P, p\notin Ram_f(H)}D_p^{-3/2}(1-Np^{-2}).$$

We shall give another examples.
EXAMPLES.

1. H is an indefinite quaternion algebra over $\mathbb{Q}$, i.e. $H_{\mathbb{R}} = M(2,\mathbb{R})$, hence the covolume of $\mathcal{O}^1$ if $\mathcal{O}$ is a maximal $\mathbb{Z}$-order is
$$\frac{\pi^2}{6}\prod_{p|D}(p-1),$$
where D is the reduced discriminant of H.

2. $H = M(2,\mathbb{Q}(\sqrt{-1}))$ and $\mathcal{O}^1 = SL(2,\mathbb{Z}(\sqrt{-1}))$, then the covolume is $8\zeta_{\mathbb{Q}(\sqrt{-1})}(2)$ times by a number for which we are ignorant of its arithmetic nature: we don't know if it is transcendental. The group $\mathcal{O}^1$ is called now and then the Picad group.

3. H is a quaternion algebra over $\mathbb{Q}$ ramified at the infinity and unramified at p and $S = \{\infty, p\}$. For a maximal order $\mathcal{O}$, the group $\mathcal{O}^1$ is a cocompact discrete subgroup of $SL(2,\mathbb{Q}_p)$ and of the covolume
$$\frac{1}{24}(1-p^{-2})\prod_{q|D}(q-1),$$
where D is the reduced discriminant of H.

4. Congruent groups. Let K be a non-archimedean local field of an integer ring R, and let p be a uniform parameter of R. For every integer $m \geq 1$, we defined (II.exercise 4.3) in the canonical Eichler order of levle $p^m R$ of $M(2,K)$ the groups $\Gamma_0(p^m) \supset \Gamma_1(p^m) \supset \Gamma(p^m)$, by which we computed the volumes for Tamagawa measure. Consider now a global field K, a set of places S satisfying C¿E¿ for a quaternion algebra H/K, and R the ring of elements of K which are integral for $v \notin S$. For every ideal N of R being prime to the reduced discriminant D of H/K, let $\mathcal{O}$ be an Eichler R-order in H of level N. For every prime ideal $p|N$, and such that $p^m||N$, we choose an inclusion $i_p : K \to K_p$, where K_p is a non-archimedean local field. We can extend i_p to an inclusion of H in $M(2,K_p)$,denoted by the same way, such that $i_p(\mathcal{O})$ is the canonical Eichler order of level $p^m R_p$. The preimage by i_p of the groups $\Gamma_0(p^m)$ and $\Gamma(p^m)$ is $\mathcal{O}^1$ and $\mathcal{O}^1(p^m)$ respectively. We define the congruent groups of mixed type by considering the subgroup Γ of $\mathcal{O}^1$ defined by
$$\Gamma = \{x \in \mathcal{O}^1 | i_p(x) \in \begin{cases}\Gamma_0(p^m) & p|N_0 \\ \Gamma_1(p^m) & \text{if } p|N_1 \text{ , or } p^m||N \\ \Gamma(p^m) & \text{if } p|N_2\end{cases}$$

[1] for all the decompositions $N = N_0N_1N_2$ of N into factors N_0, N_1, N_2 which are prime to each other. We can consider therefore an inclusion ψ of $H^\times$ in $G^\times = \prod GL(2, K_v)$ where $v \in S$ but $v \notin Ram(H)$, and the image $\varphi(\Gamma)$ in G^1. The volume of $\phi(\Gamma)\backslash G^1$ for Tamagawa measure can be calculate explicitly. We have:

$$vol(\phi(\Gamma)/backslash G^1) = (4\pi^2)^{-|Ram_\infty H|} \cdot D_K^{3/2} \zeta_K(2) \cdot \prod_{p|D} (Np-1) \cdot N_0 N_1^2 N_2^3 \cdot$$

$$\prod_{p|N_0} (1 + Np^{-1}) \cdot \prod_{p|N_1N_2} (1 - Np^{-2}) \cdot \prod_{p \in S, p \notin Ram(H)} D_p^{-3/2}(1 - Np^{-2}).$$

We notice that the volume depends uniquely on the given objects: $D_K, \zeta_K(2), |Ram_\infty(H)|, D, N_0, $

5. Arithmetic group.
a)The arithmetic groups of $SL(2, \mathbb{R})$ are the commensurable groups to the quaternion group defined by the quaternion algebra H/K over field K , totally real K, such that $H \otimes R = M(2, \mathbb{R}) \oplus \mathbb{H}^{n-1}$, where $n = [K; \mathbb{Q}]$, and by $S = \infty$. If $\mathcal{O}$ is a maximal order of H over the the integer ring of K, and if Γ^1 is the image of $\mathcal{O}^1$ in $SL(2, \mathbb{R})$ by an inclusion of H in $M(2, \mathbb{R})$, we then have for Tamagawa measure:

$$vol(\Gamma^1\backslash SL(2, \mathbb{R})) = \zeta_K(2) D_K^{3/2} (4\pi^2)^{1-[K:\mathbb{Q}]} \prod_{p|D} (Np - 1)$$

where D_K is the reduced discriminant of H/K.
b) The arithmetic subgroups of $SL(2, \mathbb{C})$ are the commensurable groups to the quaternion groups defined as follows. H/K is a quaternion algebra over a number field K such that $H \otimes R = M(2, \mathbb{C}) \oplus \mathbb{H}[\mathbf{K}; \mathbb{Q}] - \mathbf{2}$, and $S = \infty$. If $\mathcal{O}$ is a maximal order of H over the integer ring of K, and Γ^1 is an image being isomorphic to $\mathcal{O}^1$ in $SL(2, \mathbb{C})$, we have for Tamagawa measure :

$$vol(\Gamma^1\backslash SL(2, \mathbb{C})) = \zeta_K(2) D_K^{3/2} (4\pi^2)^{2-[K:\mathbb{Q}]} \prod_{p|D} (Np - 1).$$

c) If p is a finite place of a global field K, the arithnetic subgroup of $SL(2, K_p)$ are the commensurable groups to the quatrnion groups defined as follows.
— if K is a function field, $S = \{p\}$, H/K is unramified at p,
— if K is a number field, H/K is toally ramified at the infinity, that is to say, $Ram_\infty(H) = \infty$, unramified at p, and $S = \{p\}$.
If $\mathcal{O}$ is a maximal order of H over the ring of elements of K which are integral at the places not belonging to S, and Γ^1 is the image of $\mathcal{O}^1$ in $SL(2, K_p)$, we have for Tamagawa measure

$$vol(\Gamma^1\backslash SL(2, K_p)) = \zeta_K(2) D_K^{3/2} D_p^{-3/2} (1 - Np^{-2}) \prod_{p|D} (Np - 1) \cdot (4\pi^2)^{-n}$$

where $n = 0$ if K is a function field, and $n = [K : \mathbb{Q}]$ otherwise.

[1] The number m depends on p obviously.

6. Hilbert's modular group. If K is a totally real number field, and if $H = M(2,K)$, then the group $SL(2,R)$ where R is the integer ring of K is called the Hilbert modular group. It is a discrete subgroup of $SL(2,\mathbb{R})^{[K:\mathbb{Q}]}$, and for Tamagawa measure we have

$$vol(SL(2,R)\backslash SL(2,\mathbb{R})^{[K:\mathbb{Q}]}) = \zeta_K(-1)(-2\pi^2)^{-[K:\mathbb{Q}]}.$$

It can be seen by using the relation between $\zeta_K(2)$ and $\zeta_K(-1)$ obtained by the functional equation:

$$\zeta_K(2)D_K^{3/2}(-2\pi^2)^{-[K:\mathbb{Q}]} = \zeta_K(-1).$$

7. Let H/K be a quaternion algebra. If S is a set of places satisfying C.E., therefore $S' = \{v \in S | v \notin Ram_f(H)\}$ satisfies C.E. If $\mathcal{O}$ is an order over the ring of the elements of K which are integral at the places $v \in S$, then $\mathcal{O}' = \{x \in \mathcal{O} | x \text{ is integral for } v \in Ram_f(H)\}$ is an order over the ring of the elements of K which are integral at the places $v \notin S'$. It is easy to check that $\mathcal{O}^1 = \mathcal{O}'^1$. It follows that in the study of quaternion groups we can suppose $Ram_f(H) \cap S = \varnothing$.

4.2 Riemann surfaces

Let $\mathcal{H}$ be the upper half-plane equipped with a hyperbolic metric ds^2:

$$\mathcal{H} = \{z = (x,y) \in \mathbb{R}^2 | y > 0\}, ds^2 = y^{-2}(dx^2 + dy^2).$$

The group $PSL(2,\mathbb{R})$ acts on $\mathcal{H}$ by homographies. A discrete subgroup of finite covolume
$bar\Gamma \subset PSL(2,\mathbb{R})$ defines a Riemann surface $\bar{\Gamma}\backslash\mathcal{H}$. Consider those which are associated with the quaternion groups $\Gamma \subset SL(2,\mathbb{R})$ with image $\bar{\Gamma} \subset PSL(2,\mathbb{R})$.
The results of III.5, IV.1 allow us conveniently obtain – the genus,
– the number of the elliptic points of a given order,
– the number of the minimal geodesic curves of a given length.
We shall deduce them with simple examples and the explicit expression of the isospetral (for laplacian) but not isometric riemannian surfaces(§3)

Definition 4.4. *A complex homography is a mapping of $\mathbb{C}\cup\infty$ in $\mathbb{C}\cup\infty$ of the form*

$$z \mapsto (az+b)(cz+d)^{-1} = t, \text{ where } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C}).$$

We set $t = \bar{g}(z)$ and $\bar{X} = \{\bar{x} | x \in X\}$ for every set $X \subset GL(2,\mathbb{C})$.

We are interested henceforth only in real homographies induced by $SL(2,\mathbb{R})$. We have

$$Y = y|cz+d|^{-2}.$$

These homographies preserve the upper (lower) half-plane $\mathcal{H}$ and the real axis. Differentiating the relation of t, we have

$$dt = (cz+d)^{-2}dz.$$

It follows two consequences:
1) If $c \neq 0$, the location of points such that $|dt| = |dz|$ is the circle $|cz + d| = 1$. the circle is called the isometric circle of the homography, which play an important role in the construction of fundamental domain explicitly of discrete subgroup $\Gamma \subset PSL(2, \mathbb{R})$ in $\mathcal{H}$.
2) $PSL(2, \mathbb{R})$ acts on $\mathcal{H}$ by the isometry of the upper half-plane $\mathcal{H}$ equipped with its hyperbolic metrics. The isotropic group of point $i = (01)$ in $SL(2, \mathbb{R})$ is $SO(2, \mathbb{R})$. The action of $PSL(2, \mathbb{R})$ on $\mathcal{H}$ is transitive. We have then a realization:

$$\mathcal{H} = SL(2, \mathbb{R})/SO(2, \mathbb{R}).$$

W e thus can talk about length, area, geodesic for the hyperbolic metrics on $\mathcal{H}$. WE obtain

Definition 4.5. *The hyperbolic lengthof a curve in $\mathcal{H}$ is the integral*

$$\int |dz| y^{-1},$$

taking along this curve.
The hyperbolic surface of an area of in $\mathcal{H}$ is the double integral

$$\int\int y^{-2} dx dy,$$

taking in the interior of this area.
The hyperbolic geodesic are the circles with its center at the real axis (including the line perpendicular to the real axis).

(Here is a picture)!!!

The real axis is the line to the infinity of $\mathcal{H}$.
The isometric group of $\mathcal{H}$ is isomorphic to $PGL(2, \mathbb{R})$. We associate to $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$ the homography

$$t = \begin{cases} (az + b)(cz + d)^{-1}, & \text{if } ad - bc > 0 \\ (a\bar{z} + b)(c\bar{z} = d)^{-1}, & \text{if } ad - bc < 0. \end{cases}$$

Proposition 4.2.1. *2.1. The hyperbolic distance of two points $z_1, z_2 \in \mathcal{H}$ is equal to*

$$d(z_1, z_2) = |arccosh(1 + |z_1 = z_2|^2/2 z_1 z_2|.$$

Proof. (Here is a picture!!!)

If the geodesic between the two points is a vertical line,$ds = |\int_{y_1}^{y_2} dy/y| = |\log(y_2/y_1)|$. If the geodesic is an arc of the circle with center on the real axis, $\int ds = \int_{\theta_1}^{\theta_2} d\theta/\sin\theta = |\log|tg(\theta_1/2)/tg(\theta_2/2)||$. In all of these two cases we find that given formula. □

Corollary 4.2.2. *Let N be a positive real number. For every point $z^0 \in \mathcal{H}$ of its real part zero, we have*

$$\log N = d(z_0, Nz_0) = \inf_{z \in \mathcal{H}} d(z, Nz).$$

Proof. $d(z, Nz) = arccosh(1 + \frac{(N-1)^2}{2N}(1 + \frac{x^2}{y^2}))$ is minimal for $x = 0$ and equal to $\log N$. □

Proposition 4.2.3. *The area of a triangle whose vertices are at the infinity is equal to π.*

Proof. (A picture here!!!)

$$\int\int y^{-2} dxdy = \int_0^{\pi} -\sin\theta d\theta \int_{\sin\theta}^{\infty} y^{-2} dy = \pi.$$

The common area of these triangles can be taken as the definition of the value π. □

Proposition 4.2.4. *The area of a hyperbolic triangle of the angles at the vertices being $\theta_1, \theta_2, \theta_3$ is equal to $\pi - \theta_1 - \theta_2 - \theta_3$,*

Proof. The formula is true if every vertex is at infinity. We use the Green formula if no any vertex is at the infinity: if $C_i, i = 1, 2, 3$ are the edges of the triangle , then $\int\int y^{-2} dxdy = \sum_i \int_{C_i} dx/y$

Here are two pictures!!!

$\int_C dx/y = \int_{\theta_1}^{\theta^2} r\sin u/(-r\sin u)du = \alpha$.
The area is thus $I = \alpha_1 + \alpha_2 + \alpha_3$. The total rotation of the turning normal along is the triangle 2π, and that around a vertex of angle θ is $\pi - \theta$. It follows $2\pi = \sum_i (\pi - \theta_i) + \sum_i \alpha_i$, from this we have $I = \pi - \theta_1 - \theta_2 - \theta_3$. It turns back to one of these two cases when one of the angles is zero (its vertex corresponds to the infinity). By the triangulation we can compute the area of a polygon. □

Corollary 4.2.5. *The area of a hyperbolic polygon with the angles at vertices $\theta_1, ..., \theta_n$ equals $(n-2)\pi - (\theta_1 + ... + \theta_2)$.*

EXAMPLE. A <u>fundamental domain</u> of $PSl(2, \mathbb{Z})$. The group $PSL(2, \mathbb{Z})$ is generated by the homographies $t = z + 1$ and $t = -1/z$. We show that the hatching domain in the picture is a fundamental set

$$F = \{z \in \mathbb{C} | Imz > o, |z| \geq 1, -1/2 \leq Rez \leq 1/2\}.$$

It ia a triangle with one of its vertices being at the infinity. Its area is $\pi - 2\pi/3 = \pi/3$. It equals the area of the triangle without hatching, which is also a fundamental set of $SL(2, \mathbb{Z})$ in $\mathcal{H}$.

Here is a picture!!!

We give am exact sequence of continuous mapping:

$$1 \longrightarrow SO(2,\mathbb{R}) \xrightarrow{i} SL(2,\mathbb{R}) \xrightarrow{\varphi} \mathcal{H} \longrightarrow 1$$

where i is the natural inclusion, and $\varphi(g) = \bar{g}(i)$, a Haar measure on $SL(2,\mathbb{R})$ with the compatibility of the hyperbolic measure of $\mathcal{H}$ and a Haar measure $d\theta$ of $SL(2,\mathbb{R})$. Denote it by

$$y^{-2}dxdyd\theta.$$

It is false in general that for a discrete subgroup of finite covolume $\Gamma \subset SL(2,\mathbb{R})$ we could have for this measure:

$$(1) \qquad vol(\bar{\Gamma}\backslash\mathcal{H})vol(SO(2,\mathbb{R}) = vol(\Gamma\backslash SL(3,\mathbb{R})),$$

but it is true if Γ acts without fixed point in $\mathcal{H}$.

Corollary 4.2.6. *The Tamagawa measure on $SL(2,\mathbb{R})$ equals $y^{-2}dxdyd\theta$, where $d\theta$ is normalized by $vol(SO(2,\mathbb{R}) = \pi$.*

Proof. In view of 1.6, the group $SL(2,\mathbb{Z})$ possesses a subgroup Γ of finite index which does not contain the root of unit different from 1. A group with this property acts without fixed points and faithfully o $\mathcal{H}$. according to 1.3, we have

$$vol(\Gamma\backslash SL(2,\mathbb{R})) = vol(SL(2,\mathbb{Z})\backslash SL(2,\mathbb{R}))[SL(2,\mathbb{Z}) : \Gamma].$$

On the other hand, if F is a fundamental domain of $PSL(2,\mathbb{Z})$ in $\mathcal{H}$, then $\cup\gamma F$, with $\gamma \in \bar{\Gamma}\backslash PSL(2,\mathbb{Z})$ is a fundamental domain of $\bar{\Gamma}$ in $\mathcal{H}$, thus

$$vol(\bar{\Gamma}\backslash\mathcal{H}) = vol(PSL(2,\mathbb{Z})\backslash\mathcal{H})[PSL(2,\mathbb{Z}) : \bar{\Gamma}].$$

Since $[SL(2,\mathbb{Z}) : \Gamma] = 2[PSL(2,\mathbb{Z}) : \bar{\Gamma}]$, it follows from (1) the relation

$$(2) \qquad vol(PSL(2,\mathbb{Z})\backslash\mathcal{H})vol(SO(2,\mathbb{R})) = 2vol(SL(2,\mathbb{Z})\backslash SL(2,\mathbb{R}).$$

We saw in the precedent example and 1) in §1 that

$$vol(PSL(2,\mathbb{Z})\backslash\mathcal{H}) = \pi/3 \text{ for the hyperbolic measure,}$$

$$vol(SL(2,\mathbb{Z})\backslash SL(2,\mathbb{R})) = \pi^2/6 \text{ for Tamagawa measure.}$$

Corollary 2.6 then follows. □

In the proof we obtain also the following property.

Corollary 4.2.7. *Let Γ be an arithmetic group. The volume of $\bar{\Gamma}\backslash\mathcal{H}$ for the hyperbolic measure is equal to*

$$\frac{1}{\pi}vol(\Gamma\backslash SL(2,\mathbb{R}))\begin{cases}1, & \text{if } -1 \notin \Gamma\\ 2, & \text{if } -1 \in \Gamma\end{cases} \text{ calculated for Tamagawa measure.}$$

It allows to calculate by 1.7 the hyperbolic volume of $\bar{\Gamma}\backslash\mathcal{H}$. We consider a nontrivial real homography associated with $g = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL(2,\mathbb{R})$. It has two

double points in $\mathbb{C} \cap \infty$:

(1) distinct, real if $(a+d)^2 > 4$,
(2) distinct, complex conjugation, if $(a+d)^2 < 4$,
(3) mingling if $(a+d)^2 = 4$.
We obtain the above statement easily in virtue of the equalities:

$$z = (az+b)(cz+d)^{-1} \text{ is equivalent to } cz^2 + (d-a)z - b = 0.$$

The discriminant of the quadratic equation is $(d+a)^2 - 4$.

Definition 4.6. *In the case (1), the homography is said to be hyperbolic. Its norm or its multiplicator is equal to $N = \lambda^2$, where λ is the proper value of g which is great than 1 strictly.*
In case (2), it said to be elliptic. Ita angle or its multiplicatoris equal to $N = \lambda^2$, where $\lambda = e^{i\theta}$ is the proper value of g such that $0 \leq \theta \leq \pi$.
In case (3), it is said to be parabolic.

These definitions depend only on the conjugate class of g in $GL(2, \mathbb{R})$, and hence can be extended to the conjugate classes.

Proposition 4.2.8. *Let $\bar{g}$ be a homography of norm N. We have*

$$\log N = d(z_0, \bar{g}(z_0) = \inf_{z \in \mathcal{H}} d(z, \bar{g}(z))$$

for every element z_0 belonging to the geodesic joining the double points of $\bar{g}$.

Proof. Since $GL(2, \mathbb{R})$ acts by isometry, it follows that $\bar{g}(z) = Nz$, and then use 2.2. □

compactificaton of $\mathcal{H}$. We shall compactify $\mathcal{H}$ by embeding it in the space $\mathcal{H} \cup \mathbb{R} \cup \infty$ which is equipped a topology as follows: the system of basic neighborhoods at the infinity is the open neighborhoods $V_y, y > 0$ defined as below :

two pictures here!!!

for $\infty : V_y = \{z \in \mathcal{H} | Imz > 0\}$, for $A \in \mathbb{R} : V_y = \{z \in \mathcal{H} | d(B - z) < y\}$.
Fundamental domains. We recall a certain number of classic results about the construction of fundamental domains.
References: Poincare [1], Siegal [3].
Let Γ be a discrete subgroup of $SL(2, \mathbb{R})$ of finite covolume, and $\bar{\Gamma}$ be the group of the homographies associate with Γ.

1. For every element $z_{0 \in \mathcal{H}}$ which is not the double point of any elliptic matrix of Γ (the existence of such point is easy to prove), the set

   $$F = \{z \in \mathcal{H} | d(z, z_0 \leq d(\bar{g}(z), z_0) \quad \forall \bar{g} \in \bar{\Gamma}\}$$

   is a hyperbolic polygon and a fundamental set of Γ in $\mathcal{H}_2$.

2. The edges of F are even in number and congruent pairwise modulo $\bar{\Gamma}$. We can also rearrange them in pairs $(C_i, \bar{g}_i(C_i)), 1 \leq i \leq n$.

3. The group $\bar{\Gamma}$ is of finite type, and generated by the homographies $\{\bar{g}_i, 1 \leq i \leq n\}$. It comes from that $\{\bar{g}F | \bar{g} \in \bar{\Gamma}\}$ forms a pavement of $\mathcal{H}$. If $\bar{g} \in \bar{\Gamma}$, it exists $\bar{g}'$ belonging to the group generated by these $\bar{g}_i$ such that $\bar{g}F = \bar{g}'F$, hence $\bar{g} = \bar{g}'$. by Using again an argument of pavement we see:

4. A cycle of F being a equivalent class of vertices of F in $\mathcal{H} \cup R \cup \infty$ modulo $\bar{\Gamma}$,The sum of the angles around the vertices of a cycle is of the form $2\pi/q$ where q is an integer great than 1, or $q = \infty$.

Definition 4.7. *A cycle is said to be*
hyperbolic if $q = 1$,
elliptic of order q *if* $q > 1, q \neq \infty$,
parabolic if $q = \infty$.
The angle $2\pi/q$ *is the angle of cycle.* e_q *denotes the number of cycles of angle* $2\pi/q$.

Definition 4.8. *A point of* $\mathcal{H} \cup R \cup \infty$ *is said to be elliptic of order* q *(rep. parabolic or a point) for* $\bar{\Gamma}$ *if it is a double point of an elliptic homography of order* q *(resp. parabolic) of* $\bar{\Gamma}$.

It is easy to show that the elliptic cycles of order q constitute a system of representatives modulo $\bar{\Gamma}$ of the elliptic points of order q. It is the same for the parabolic points . The interior of F contains no any elliptic point, no any parabolic. The union of $\mathcal{H}$ and the points of $\bar{\Gamma}$ is denoted by $\mathcal{H}^*$.
Searching cycles. We look for the cycles in such a way: Let $A, B, C, ...$ be the vertices of F in $\mathcal{H}^*$ when we run along the boundary of F in a sense given in advance. In order to find the cycle of A, we run along the edge $AB = C_1$ and then the edge which is congruent to $A'B' = g_1(C_1)$ in the chosen sense. It remains that $B' = A_2$, and runs along the next edge C_2, then the edge which is congruent to $g_2(C_2)$ with its end point A_3,... till to that when we find again $A = A_m$. Integer m is the length of the cycle.
EXAMPLE:
1)The fundamental domain of modular group $PSL(2, \mathbb{Z})$:

A picture here !!!

a point $\{\infty\}$, a cycle $\{A, C\}$ of order 3, a cycle B of order 2. The group is generated by the homographies $z \mapsto z + 1$ and $z \mapsto -1/z$.
2)
A picture here!!!

In the example given by this figure, we have two points $\{A, B, E\}$ and ∞, and two cycles of order 2: $\{B\}, \{D\}$.

Lemma 4.2.9. *The number of elliptic cycles of order* q *is equal to the half of the number of conjugate classes of* Γ *of the characteristic polynomial* $X^2 - 2\cos(2\pi/aq)X + 1$, *where* a *is the index of the center in* Γ.

Proof. The two numbers defined in (1), (2) are equal to e_q:
(1) The number of the equivalent classes modulo $\bar{\Gamma}$ of the set $E_q = \{z \in H |$ elliptic of order $q\} = \{z \in H |\ \bar{\Gamma}_z$ is cyclic of order $q\}$, where $\bar{\Gamma}_z$ is the isotropic group of z in $\bar{\Gamma}$.

(2) The number of the conjugate classes in Γ of the cyclic subgroups of order $2q$ if $-1 \in \Gamma$, and of order q if $-1 \notin \Gamma$, i.e. of order aq.
Two elements q, q' of order aq in an cyclic group of order $aq > a$ contained in Γ are not conjugate. Otherwise, it would be $g' = g''gg''^{-1}$. Since $aq \neq 2$ the common trace of g and g' is not zero, therefore $g' = g$. the lemma is proved. □

This lemma together with III.5,14-17, allow us to calculate explicitly the number e_q for the quaternion groups.
The surface $\bar{\Gamma}\backslash\mathcal{H}^*$ is compact. It is a Riemann surface (Shimura [6]) which is locally equivalent to $\mathcal{H}$ if it is not in. the neighborhood of an elliptic point. Its genus is given by the classic formula:

$$2 - 2g = P + S - A$$

for every subdivision in polygons which is consists of P polygons, S vertices, A faces. Let s be the number of cycles in the fundamental domain F, and suppose the pairs $(C_i, \bar{g}_i(C_i))$ not to be congruent modulo $\bar{\Gamma}$. We then have by 2.5:

$$-\frac{1}{2\pi} vol(\bar{\Gamma}\backslash\mathcal{H}^*) = 1 - n + \sum_{q>1} e_q/q = 1 - n + s - \sum_{q\geq 1} e_q \frac{q-1}{q} - e_\infty.$$

Therefore we have

Proposition 4.2.10. *The genus of the Riemann surface $\bar{\Gamma}\backslash\mathcal{H}^*$ is given by*

$$2 - 2g == -\frac{1}{2\pi} vol(\backslash\mathcal{H}^*) + \sum_{q\geq 1} \frac{q-1}{q} + e_\infty.$$

Corollary 4.2.11. *If Γ does not contain hyperbolic elements, the genus of the compact Riemann surface $\bar{\Gamma}\backslash\mathcal{H}$ is strictly great than 2. It is given by*

$$2 - 2g = -\frac{1}{2\pi} vol(\bar{\Gamma}\backslash\mathcal{H}^*).$$

In view of 2.7, 2.8 we can calculate explicitly the genus of the quaternion group. Notice that a being an integer, the number

$$-\frac{1}{2\pi} vol(\bar{\Gamma}\backslash\mathcal{H})$$

is rational. It remind of replacing the hyperbolic measure by the arithmetic measure with the name of Euler-Poincare:

$$-\frac{dxdy}{2\pi y^2}.$$

Denote by $vol_a(X)$ an area of the surface for the measure. We relate the Tamagawa measures and the arithmetic measures with 2.7

$$vol_a(\backslash\mathcal{H}) = -\pi^{-2} vol(\Gamma\backslash SL(2,\mathbb{R})) \cdot \begin{cases} 1 & \text{if } -1 \in \Gamma \\ 1/2 & \text{if } -1 \notin \Gamma \end{cases}.$$

We obtain by example 5),6) in §1 the corollary below.

Corollary 4.2.12. *If K is a totally real field, then $\zeta_K(-1)$ is rational.*

It is a special case of a theorem of Siegel which asserts that the numbers $\zeta_K(1-n)$ for $n \geq 1$ are the rational number.
The number e_∞ of points for an arithmetic group is not zero if and only if the group is commensurable to $PSL(2,\mathbb{Z})$. For the congruent group $\Gamma(N)$ and $\Gamma_0(N)$, the formula for the number of points can be found in the book of Shimura [6],p.25.

Exercise

. Let Γ be the group of the proper automorphisms of the quadratic form

$$x^2 + y^2 - D(z^2 + t^2)$$

where D is an integer great or equal to 1. Prove
1) Γ is the the unit group of reduced norm 1 and of order $\mathcal{O} = \mathbb{Z}[1, i, j, ij]$ of the quaternion algebra $H/\mathbb{Q}$ generated by the elements i, j satisfying

$$i^2 = -1, j^2 = D, ij = -ji.$$

2) The volume V of a fundamental domain of Γ in $\mathcal{H}_2$ for the hyperbolic metric given by Humbert formula:

$$V = D \prod_{p|D, p\neq 2} (1 + (\frac{-1}{p})p^{-1}).$$

Hint: Write $V = \frac{pi}{=} 3 \prod_{p|D} V_p$, where

$$V_2 = 2^{m-1}(1 + \frac{1}{2}) \text{ if } 2^m || D,$$

$$V_p = p^m(1 + (\frac{-1}{p})p^{-1}) \text{ if } p^m || D.$$

Then compare V_p with the volume of $\mathcal{O}_p^1$ for Tamagawa measure.

4.3 Examples and Applications

A. congruent groups. Let $H/\mathbb{Q}$ be a quaternion algebra contained in $M(2,\mathbb{R})$, of reduced discriminant D, and Γ be a congruence group of level $N = N_0, N_1, N_2$, for the definition see example 4) in §1. The genus of $\bar{\Gamma}\backslash\mathcal{H}^*$ is given by

$$2 - 2g = vol_a(\bar{\Gamma}\backslash\mathcal{H}_2) + e_2/2 + 2e_3/3 + e_\infty.$$

The volume of $\bar{\Gamma}\backslash\mathcal{H}_2$ which is calculated for Euler-Poicare measure is equl to

$$vol_a(\bar{\Gamma}\backslash\mathcal{H}_2) = -\frac{1}{6}\prod_{p|D}(p-1) \cdot N_0 N_1^2 N_2^3 \cdot \prod_{p|N_0}(1+p^{-1}) \cdot \prod_{p|N_1 N_2}(1-p^{-2}) \cdot (1/2)$$

by putting $(1/2) = 1$ if $N_1 N_2 \leq 2$ and $(1/2) = 1/2$ otherwise.
Let the quadratic cyclotomic extension of $\mathbb{Q}$ be $Q(x)$ and $Q(y)$ with x, y being

the solutions of $x^2+1=0$ and $y^2+y+1=0$, and the roots of unit be of order 2 and 3, we see that $e_q=0$ if $q\neq 2,3$. We shall show solution then the above equations have no solutions in Γ if $N_2>1$ or if $N_1>2$. Since $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ are of the maximal order in $\mathbb{Q}(x)$ and $\mathbb{Q}(y)$, according to Chapter II, exercise 3.1. we has then $e_2=0$ if $4|N$ and $e_3=0$ if $9|N$. In other cases, e_2 and e_3 can be calculated by III,5.17. Suppose the Eichler condition to be satisfied, there is an order $\mathcal{O}$ which contains an element of reduced norm -1, and if $B=\mathbb{Z}[x]$ or $\mathbb{Z}[y]$, we then have $[n(\mathcal{O}^\times):n(B^\times)]=2$. Therefore if $N=N_0$, we have

$$e_2=\prod_{p|D}(1-(\frac{-4}{p}))\prod_{p|N}(1+(\frac{-4}{p}))\quad \text{if } 4\nmid N,$$

$$e_3=\prod_{p|D}(1-(\frac{-3}{p}))\prod_{p|N}(1+(\frac{-3}{p}))\quad \text{if } 3\nmid N.$$

It can proceed the calculations for every N without any difficulty, by using II.3, if necessary.

REFERENCES. The formulae for the volume and the number of elliptic points of given order are well known. Here is a list of articles where they are used, and often re-prove them in a particular cases for want of the general references: Eichler [7]-[14], Fueter [1], Hashimoto [1], hijikata [1], Pizer [1]-[5], Ponomarev [1]-[5], Prestrl [1], Schneider [1], Shimizu [1]-[3], Vigneras [1]-[3], Vigneras-Gueho [1]-[3], Yamada [1].

It will be evident particularly in all the explicit formulae of the trace of Hecke operators. This explains their concern with theory of automorphic forms.

B. Normalizers (Michon [1]). It is given here a quaternion field over $\mathbb{Q}$, included in $M(2,\mathbb{R})$ of reduced discriminant $D=p_1\cdots p_{2m}$. Let $\mathcal{O}$ be a maximal order. Using III. exercise 5.4, we see that its normalizer $N(\mathcal{O})$ satisfies

$$N(\mathcal{O})/\mathcal{O}^\times\mathbb{Q}^\times\simeq(\mathbb{Z}/2\mathbb{Z})^{2m}.$$

The elements of $N(\mathcal{O})$ of positive reduced norm forms a group. Its image by the mapping $x\mapsto xn(x)^{-\frac{1}{2}}$ is a subgroup of $SL(2,\mathbb{R})$, denoted by G. The group $\mathcal{O}^1=\Gamma$ is distinguished in G and

$$G/\Gamma\simeq(\mathbb{Z}/2\mathbb{Z})^m.$$

It defines also a covering $\bar{\Gamma}\backslash\mathcal{H}\to\bar{G}\backslash\mathcal{H}$ of degree 2^{2m} explicitly, The elements of G can be described by $xn(x)^{-1/2}$ with $x\in\mathcal{O}$ and $n(x)|D$. Note that $e_q(\Gamma),e_q(G)$ are the number of elliptic cycles of Γ,G of order q.

Lemma 4.3.1. *The volume of $\bar{\Gamma}\backslash\mathcal{H}$ and $\bar{G}\backslash\mathcal{H}$ for Euler-Poincare measure, denoted by V_Γ and V_G, are*

$$V_\Gamma=-\frac{1}{6}\prod_{p|D}(p-1),\quad V_G=2^{-2m}V_\Gamma.$$

The genus of $\Gamma\backslash\mathcal{H},\bar{G}\backslash\mathcal{H}$, denoted by g_Γ,g_G, satisfying

$$2-g_\gamma=V_\Gamma+\frac{1}{2}e_2(\Gamma)+\frac{2}{3}e_3(\Gamma),$$

$$2-2g_G=V_G+\frac{1}{2}e_2(G)+\frac{3}{4}e_4(G)=\frac{5}{6e_6}(G).$$

Proof. The assertion for Γ comes from Example 2.1. As for G, it suffices to verify that the possible values of the order of the cyclic groups which are contained in G are $1, 2, 4, 6, 8, 12$. It can be obtained at once from the structure of $G\backslash\Gamma$ and the order of the cyclic groups in Γ. □

The formulae for $e_q(G)$ are not so simple as for $e_q(\Gamma)$ but can be obtained by elementary method.
The following table gives the list of all surfaces $bar\Gamma\backslash\mathcal{H}$ of genus 0,1,2.

here is Table 1 !!!

Using the results of Ogg about the hyperelliptic Riemann surfaces of genus $g \geq 2$, we can determine the surfaces $\bar{\Gamma}\backslash\mathcal{H}$ of genus $g \geq 2$ which are hyperelliptic. In all these cases, the hyperelliptic involution is induced by an element of G.
We denote by π_i the element of $\mathcal{O}$ of reduced norm p_i $(1 \leq i \leq 2m)$ and g_d the element of G defined by

$$g_d = d^{-1/2}\pi_1^{\varepsilon_1}...\pi_{2m}^{\varepsilon_{2m}} \quad \text{for } d = \pi_1^{\varepsilon_1}...\pi_{2m}^{\varepsilon_{2m}}, \quad \varepsilon_i = 0 \text{ or } 1$$

The table below gives the list of the hyperelliptic surfaces with their genus and the element of G which induces the hyperelleptic involution:
Here is a talbe!!!

C The construction of a fundamental domain for Γ and G in The case of $D = 15$.(Michon [1]). The quaternion algebra is generated by i, j satisfying

$$i^2 = 3, j^2 = 5, ij = -ji.$$

The order $\mathcal{O}$ generated over $\mathbb{Z}$ by

$$1, i, (i + j)/2, (i + k)/2$$

is maximal. It has the matrix representation

$$\mathcal{O} = \{\frac{1}{2}\begin{pmatrix} x & \sqrt{5}y \\ \sqrt{5}\bar{y} & \bar{x} \end{pmatrix}, |x, y \in \mathbb{Q}(\sqrt{3}) \quad \text{are integer, and } x \equiv y \bmod (2)\}.$$

The group $\Gamma = \mathcal{O}^1$ is consists of the above matrices such that

$$(1) \qquad n(x) - 5n(y) = 4.$$

The group G normalizing Γ is consists of the matrices satisfying

$$(2) \qquad n(x) - 5n(y) = 4, 12, 20, \quad \text{or } 60$$

divided by the square root of their determinants. The fixed points in $\mathbb{C}$ of an element of G are distinct and given by

$$z = \frac{b\sqrt{3} \mp \sqrt{a^2 - 4}}{\sqrt{5}(y)} \quad \text{if } x = a + b\sqrt{3}, a, b \in \mathbb{Z}.$$

The elliptic fixed points corresponds to $a = -1$, or 1. It can be restricted to $a = 0$ or 1, since the change of sign of the matrix does not change the

homography. The elliptic points are distributed on the ray staring from origin and with slope b^{-1}. All the elliptic points which locate on an admissible ray obtained by solving the following equation

$$(3) \qquad -5n(y) = 4 - N(x), y \text{ is integer in } \mathbb{Q}(\sqrt{3}).$$

If z_0 is an elliptic point, we see that $\varepsilon^n z_0, n \in \mathbb{Z}$ is also an elliptic point if ε is fundamental unit of $\mathbb{Q}(\sqrt{3})$. Let η be the fundamental unit of $\mathbb{Q}\sqrt{5}$, namely $\frac{1}{2}(1+\sqrt{5})$. It has norm -1. Consider its square η^2 included in Γ, with image

$$k = \frac{1}{2}\begin{pmatrix} 3 & \sqrt{5} \\ \sqrt{5} & 3 \end{pmatrix}.$$

In view of the symmetry, $k^n(z_0), n \in \mathbb{Z}$ is also an elliptic point. The first values of b such that the equation (3) having a solution are $b = \mp 2, \mp 8$. for $b = 2$, it becomes

$$-n(y) = 3, \quad y \quad \text{is integer in } \mathbb{Q}(\sqrt{3}).$$

For $b = 8$, it becomes

$$-n(y) = 37, \quad y \quad \text{is integer in } \mathbb{Q}(\sqrt{3}).$$

Denote

$$A = \frac{1}{\sqrt{5}}\frac{2+i}{2-\sqrt{3}}, C = \frac{1}{-}\sqrt{5}\frac{8+i}{4+\sqrt{3}}, C' = \frac{1}{5}\frac{8+i}{4-\sqrt{3}}.$$

The set of elliptic points on the line of slope $1/2$ is $\{\varepsilon^n, n \in \mathbb{Z}\}$; on the line on slope $1/8$, it is $\{\varepsilon^n C, \varepsilon^n C', n \in \mathbb{Z}\}$. Denote by B, B' the symmetry of A, A' with respect to the imaginary axis with $A' = \varepsilon^2 A$.

Lemma 4.3.2. *The hyperbolic hexagon $BACC'A'B'$ is a fundamental domain of Γ.*

Proof. Let

$$h = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, l = \frac{1}{2}\begin{pmatrix} -4+\sqrt{3} & -\sqrt{15} \\ \sqrt{15} & -4-\sqrt{3} \end{pmatrix}.$$

We have

$$\begin{array}{ll} A' = h(A), & B' = h(B) \\ C = k(B), & C' = k(B') \\ A = l(A'), & C = l(C') \end{array}.$$

The hexagon has for the angles at vertices $B, B'C, C'$ are $\pi/6$, and $\pi/3$ at A, A'. It is a fundamental domain for the group

$$< l, h, k >$$

generated by $l.h.k$. It has two cycles $\{A, A'\}$, $\{B, B'C, C'\}$ each of order 3. Its hyperbolic volume is

$$(6-2)\pi - 2\frac{2\pi}{3} = \frac{8\pi}{3}.$$

On the other hand, for the hyperbolic measure the volume of $\bar{\Gamma}\backslash\mathcal{H}$ from the first table of the precedent exercise is equal to $8\pi/3$. Therefore, $\Gamma =< l, h, k >$ and the polygon is fundamental. The same procedure allows to treat by the same way the case of G. □

We denote

$$E = \frac{i}{2+\sqrt{3}}, E' = \frac{i}{2-\sqrt{3}}, F+i, H = -\frac{1+2i}{\sqrt{5}},$$

$$u = \begin{pmatrix} 0 & -\sqrt{15} \\ \sqrt{15} & 0 \end{pmatrix}, v = \frac{1}{2}\begin{pmatrix} -\sqrt{3} & -\sqrt{15} \\ \sqrt{15} & \sqrt{3} \end{pmatrix}.$$

The transformation u fixes F and exchange E and E'. The transformation v fixed H and exchange B and B'.

Lemma 4.3.3. *The hyperbolic quadrilateral $BEE'B'$ is a fundamental domain of G. The transformations $h, u/\sqrt{15}, v/\sqrt{3}$ generates G. Its area is $8\pi/6$.*

Here are tree figures:
1)fundamental domain of Γ . 2) fundamental domain of G 3)Unit disc. these pictures are designed by C.Leger.

D Minimal geodesic curves.

Definition 4.9. *Let g be a hyperbolic matrix of Γ of norm N. Let P is a point of the geodesic of $\mathcal{H}$ joining the double points of $\bar{g}$. The image of $\bar{\Gamma}\backslash\mathcal{H}$ of the orient segment of the geodesic joining P to $g(P)$ is an orient closed curve, being independent of P, of length $\log N$, called the minimal geodesic curve of $\bar{g}$.*

Definition 4.10. *an element $\bar{g} \in \bar{\Gamma}$is primitive if it not the power of the other element of $\bar{\Gamma}$ with exponent strictly great than 1. Its conjugate class in $\bar{\Gamma}$ is said to be primitive too.*

If $\bar{g}$ is primitive, hyperbolic, then it generates the cyclic group of elements of $\bar{\Gamma}$ which has the same fixed points. Its minimal geodesic curve is passes through a single time. If $g' = g^m$, $m \in \mathbb{Z}, m \neq 0$, the norm of g' is N^m, and the minimal geodesic curve of g' is the curve obtain by passing through that of g m times, in the same direction if $m > 0$, and in the contrary direction otherwise. The minimal geodesic curve of the hyperbolic $\bar{g}, \bar{g'} \in \bar{\Gamma}$ are the same if and only if $\bar{g}$ and $\bar{g'}$ are conjugate in $\bar{\Gamma}$. We have thus the following result.

Lemma 4.3.4. *The number of the minimal geodesic curves of length logN is equal to the number of conjugate classes of the elements of Γ with the characteristic polynomial $X^2 - (N^{1/2} + N^{-1/2})X + 1$. Denoted it by $e(N)$.*

Notice that if g, g^{-1} are conjugate in Γ, ther exists then $x \in \Gamma$ satisfying

$$xgx^{-1} = g^{-1} \Rightarrow x^2 \in \mathbb{R}(x) \cap \mathbb{R}(g) = \mathbb{R},$$

hence $x^2 = -1$. If Γ does not contain such an element, $e(N)$ is even. For the quaternion group, $e(N)$ can be computed explicitly(III.5). EXAMPLE: Γ is the unit group of reduced norm 1 of a maximal order of a quaternion field over $\mathbb{Q}$ of its discriminant 26. We have the following results:

1.) Γ is embedded in $SL(2, \mathbb{R})$, since $26 = 2 \cdot 13$ is the product of two prime factors.

2.) Γ does not contain any parabolic element according to 1.1.

3.) Γ does not contain any elliptic element, since $(\frac{-1}{13}) = (\frac{-3}{13}) = 1$ according to III,3.5.

4.) The genus g of $\bar{\Gamma}\backslash\mathcal{H}$ is equal to 2, since by A,

$$g = 1 + \frac{1}{12}(2-1)(13-1) = 2.$$

5.) The conjugate classes of hyperbolic $\bar{\Gamma}$, have its norm ε^{2m}, $m \geq 1$, where ε runs through the fundamental units of norm 1 of real quaternion field, In them not 2 nor 3 can be decomposed.

6.) The number of the primitive conjugate classes of $\bar{\Gamma}$ with reduced norm ε^{2m} is equal to

$$(2)h(B) \prod_{p=2,13} (1 - (\frac{B}{p}))$$

where $(2) = 1$ or 2 according to $\mathbb{Q}(\varepsilon)$ containing a unit of -1 or not, where B runs the orders of $\mathbb{Q}(\varepsilon)$ of which the unit group of norm 1 is generated by ε^{2m}, and the number of classes of B is related to that of $L = \mathbb{Q}(\varepsilon)$ by the formula

$$h(B) = h_L f(B)[R_L^\times : B^\times]^{-1} prod_{p|f(B)}(1 - (\frac{L}{p})p^{-1})$$

with R_L = the integer ring of L, of class number h_L, $f(B)$ = conductor of B.

EXAMPLE. $\bar{\Gamma}$ is the modular group $PSL(2,\mathbb{Z})$. We have $e_2 = 1, e_3 = 1, e_\infty = 1$ and the genus of the surface $\bar{\Gamma}\backslash\mathcal{H}_2^*$ is 0, since

$$g = 1 + 1/12 - e_2/4 - e_3/3 - e_\infty/2 = 0.$$

The number of the hyperbolic primitive conjugate classes of a given norm is

$$(2)\sum h(B)$$

with the same notations as that in the precedent example.
E The examples of Riemann surfaces which are isospectral but not isometric. There are some numerical invariants as follows. — $vol(\bar{\Gamma}\backslash\mathcal{H})$
— e_q = the number of elliptic points of order q in $\bar{\Gamma}\backslash\mathcal{H}$
— e_∞ =the number of points of $\bar{\Gamma}\backslash\mathcal{H}$
— $e(N)$ = the the number of the minimal geodesic of length $\log N$ of $\bar{\Gamma}\backslash\mathcal{H}$ which are not depend on the isometric class of the surface $\bar{\Gamma}\backslash\mathcal{H}$.
Using the properties of Selberg (Cartier-Hejhal-Selberg) zeta function we can prove: — To give the spectral for the hyperbolic laplacian in $L^2(\bar{\Gamma}\backslash\mathcal{H})$ is equivalent to give the invariants.
– Two groups of the same invariants but for a finite number between them, have the same invariants.

We may ask if two surfaces $\bar{\Gamma}\backslash\mathcal{H}$ and $\bar{\Gamma}'\backslash\mathcal{H}$ of the same numerical invariants are isometric. The answer is NO. We can restrict ourselves to the cocompact groups Γ without elliptic points. Our examples shall utilize the quaternion

groups. In those examples, like in the tori of dimension 16 of Milnor (1), two isospectral riemannian manifolds have the isometric covering of finite degree. This comes from the arithmetic nature of those examples.

We make a note to the terminology: a riemannian surface is a surface equipped with a riemannian metric. Two riemannian surfaces are equal if they are isometric.
They will proceed from the simple observation that the Eichler orders of level N in a quaternion field H/K over a number field K which is totally real such that there exists one and only one infinite place of K nonramified in H, define the surfaces they have the same invariants. But it is well known that it can be chosen K such that the class number of K is divided by a power of 2 as large as we like. For example we can take K as a real quadratic field of its discriminant divisible by by a great number of prime numbers. The formula for the type number of orders leads us to choose K, H, N such that the the type number of Eichler order of level N in H is as large as we desire(III,5.7).
Examine then the condition of the isometry for two compact riemannian surfaces. Fix the Notations: H/K, and H'/K' are two quaternion field satisfying the above conditions, and not containing any roots of unit different from ∓ 1. Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders of H and H' over the integer rings R and R' of the center K and K' respectively. We say an automorphism σ of $\mathbb{C}$ that means a complex automorphism and suppose that K, and K' are embedded in $\mathbb{C}$. We denote by $\sigma(H)$ the quaternion field over $\sigma(K)$ such that $Ram(\sigma(H)) = \{\sigma(v)|v \in Ram(H)\}$. We still denote by σ the isomorphism of H in $\sigma(H)$ which extending $\sigma : K \to \sigma(K)$.
EXAMPLE: If $H = \{a, b\}$ is the K-algebra of base i, j related by

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

where a, b are the nonzero elements of K, thus $\sigma(H) = \{\sigma(a), \sigma(b)\}$ is the K-algebra of base $\sigma(i), \sigma(j)$ related by

$$\sigma(i)^2 = \sigma(a), \sigma(j)^2 = \sigma b, \sigma(i)\sigma(j) = -\sigma(j)\sigma(i).$$

We denote by $\sigma(K)$ and $\sigma(K')$ the inclusion of K and K' in $\mathbb{R}$ such that $H \otimes \mathbb{R}$ and $H' \otimes \mathbb{R}$ is isomorphic to $M(2, \mathbb{R})$. We can suppose then $\sigma(H)$ and $\sigma'(H')$ are contained in $M(2, \mathbb{R})$. The images $\sigma(\mathcal{O}^1)$ and $\sigma(\mathcal{O}'^1)$are the groups which we denoted above by Γ and Γ'. Their canonical images in $PSL(2, \mathbb{R})$ are denoted by $\bar{\Gamma}$ and $\bar{\Gamma}'$.

Theorem 4.3.5. *The riemannian surface $\bar{\Gamma}\backslash\mathcal{H}_2$ and $\bar{\Gamma}'\backslash\mathcal{H}_2$ are isomorphic if and only if there exists a complex automorphism σ such that*

$$H' = \sigma(H), \mathcal{O}' = \sigma(a\mathcal{O}a^{-1}), a \in H^{\times}.$$

Proof. We prove first that $H = \mathbb{Q}(\mathcal{O}^1)$. Actually this assertion is true under a general hypothese. Let (e) be a base of H/K contained in $\mathcal{O}^1$. Every element of $\mathbb{Q}(\mathcal{O}^1)$ is of the form $x = \sum a_e e$, where the coefficients a_e belongs to K. The reduced trace being non-degenerated, then the Cramer system $t(xe') = \sum a_e t(ee')$ can be solved. The coefficients hence like $t(xe')$ belong to $\mathbb{Q}(\mathcal{O})$. Set $k = K \cap \mathbb{Q}(\mathcal{O}^1)$. we have just proved that $\mathbb{Q}(\mathcal{O}^1) = k(e)$. It

follows that $\mathbb{Q}(\mathcal{O}^1)$ is a central simple algebra over k of dimension 4. It is simple because that by performing tensor product of it with K over k, it becomes simple. Therefore $\mathbb{Q}(\mathcal{O})$ is a quaternion algebra over k. an infinite place w of k which is extended to a place v of K ramified in H is definitely ramified in $\mathbb{Q}(\mathcal{O})$. An infinite place w of k which is unramified in $\mathbb{Q}(\mathcal{O}^1)$ has their every extension v in K to be unramified in H. A place w associating with a real inclusion $i_w : k \to \mathbb{R}$ can be extended in $[K : k]$ real places. It deduces from 1.1 that $k = K$.
Every isometry of $\bar{\Gamma}\backslash\mathcal{H}_2$ to $\bar{\Gamma}'\backslash\mathcal{H}_2$ is lifted to an isometry of the universal covering $\mathcal{H}_2$. The isometries of $\mathcal{H}_2$ forms a group which is isomorphic to $PGL(2,\mathbb{R})$. It follows that $\bar{\Gamma}\backslash\mathcal{H}_2$ and $\bar{\Gamma}'\backslash\mathcal{H}_2$ are isomorphic if and only if Γ and Γ' are conjugate in $GL(2,\mathbb{R})$. From it $\mathbb{Q}(\sigma(\mathcal{O}^1))$ and $\mathbb{Q}(\sigma'(\mathcal{O}'^1))$ are conjugate in $GL(2,\mathbb{R})$. The center remains fixed, thus $\sigma(K) = \sigma'(K')$. The quaternion algebra $\mathbb{Q}(\sigma(\mathcal{O}^1))$ and $\mathbb{Q}(\sigma'(\mathcal{O}'^1))$ are hence isomorphic. It may then suppose they are equal. Every automorphism of a quaternion algebra is inner one, therefore there exists $a \in H^\times$ such that $\sigma'(\mathcal{O}') = \sigma(a\mathcal{O}a^{-1})$. We finally have $H' = \sigma'^{-1}\sigma(H)$ and $\mathcal{O}' = \sigma'^{-1}\sigma(a\mathcal{O}a^{-1})$. □

It is clear that this proof can be generalized to riemanian manifold ΓX where X is a product of $\mathcal{H}_2$ and $\mathcal{H}_3$, and $\bar{\Gamma}$ here is the image of a quaternion group. The isometric group of X is determined in virtue of a theorem of de Rham [1].

Corollary 4.3.6. *If the type number of the order of H is great than the degree $[K : \mathbb{Q}]$, then it exists in H two maximal orders $\mathcal{O}$ and $\mathcal{O}'$ such that the surfaces $\bar{\Gamma}\backslash\mathcal{H}$ and $\bar{\Gamma}'\backslash\mathcal{H}$ are isospectral but not isometric.*

In fact, the number of the conjugate $\sigma(H)$ of H is dominated by the degree $[K : \mathbb{Q}]$. The corollary can be refined considerably, if necessary, by observing:
– the non-maximal orders
– a better upper bound of $Card\{\sigma(H)\}$, depending on the given (K, H).
EXAMPLE. Suppose that K is a real quadratic field, of which the class number is great than or equal to 4, for example $\mathbb{Q}(\sqrt{82})$. Suppose that $Ram(H)$ is consists of just one infinite place and of the finite places such that all of their correspondent prime ideals are principal. Therefore, it exists at least 4 types of maximal orders, and we can construct some isospectral riemannian surfaces but they are not isometric. We can thus compute the genera of the obtained surfaces, by the genus formula and the tables of $\zeta_K(-1)$ calculated by Cohen [1].
EXAMPLE. H is the quaternion field over $K = \mathbb{Q}(\sqrt{10})$ which is ramified at an infinite place, and above the principal prime ideals $(7), (11), (11 + 3\sqrt{10})$ H does not contain the roots of unit other than ∓ 1 since (7) is decomposed into two cyclotomic quadratic extensions of K, i.e. $K(\sqrt{-1})$ and $K(\sqrt{-3})$. H is never fixed by any $\mathbb{Q}$-automorphism and contains two types of maximal orders, because the class number of $\mathbb{Q}(\sqrt{10})$ is 2. The unit groups of reduced norm 1 of two non-equivalent maximal orders allow us to construct two isospectral but non-isometric surfaces.

Remark 4.3.7. *The construction can be generalized and is allowed to construct some isospectral but non isometric riemannian surfaces in all the dimension $n \geq 2$.*

F Hyperbolic space of dimension 3 . We want to extend a complex homography to a transformation of $\mathbb{R}^3$. Every complex homography is an even product of inversions with respect to the cicles in plane which is identified with $\mathbb{C}$. Consider now the spheres which have the same circle and same rays as that circles, and the operation of $\mathbb{R}^3$ consistent with the performance of the product of the inversion with respect to these spheres. extend then a complex homography to $\mathbb{R}^3$. We now verify the consistence of this definition (Poincarè[1]). It remains to find the equations of the transformation. We identify the points of $\mathbb{R}^3$ with the points

$$u = (z, v) \in \mathbb{C} \times \mathbb{R}$$

or with the matrices

$$u = \begin{pmatrix} z & -v \\ v & \bar{z} \end{pmatrix}.$$

The operation of $\mathbb{R}3$ extending the homography associated with $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{C})$ is $u \mapsto U = (au + b)(cu + d)^{-1}$. Set $U = \bar{g}(u) = (Z, V)$. We verify the following formulae:

$$Z = ((az + b)\overline{(cz + d)} + a\bar{c}v^2)(|cz + d|^2 + |c|^2v^2)^{-1},$$

$$V = v(|cz + d|^2 + |c|^2v^2)^{-1}.$$

Differentiating the formula $U = g(u)$ we see that

$$V^{-1}dU = v^{-1}du.$$

We equip $\mathcal{H}_3 = \{u \in \mathbb{R}^3 | v > 0\}$ the upper half-space the hyperbolic metric

$$v^{-2}(dx^2 + dy^2 + dv^2), u = (x + iy, v).$$

The group $SL(2, \mathbb{C})$ acts on the hyperbolic half-space by isometries. Its action is transitive. the isotropic group of $(1, 0)$ is equal to $SU(2, \mathbb{C})$ and $SL(2, \mathbb{C})/SU(2, \mathbb{C})$ is homeomorphic to $\mathcal{H}_3$. The group of all the isomorphisms of $\mathcal{H}_3$ is generated by the mapping $(z, v) \mapsto (\bar{z}, v)$ and the group is isomorphic to $PSL(2, \mathbb{C})$ of isometries associated with $SL(2, \mathbb{C})$.The geodesics are the circles(or the straight lines) orthogonal to plane $\mathbb{C}$.

Definition 4.11. *The volume element deduced from the hyperbolic metric is*

$$v^{-3}dxdydv.$$

Definition 4.12. *Milnor (Thurston, [1]) introduced a function, i.e. the Lobachevski function,*

$$\mathcal{L}(\theta) = -\int_0^\theta \log|2\sin u|du.$$

The function allows to express the volume of a tetrahedron. The function is related to the values of the zeta functions of the (complex) number field at point 2, hence we have the relation

$$(1) \qquad \mathcal{L}(\theta) = 1/2 \sum_{n \geq 1} \sin(2n\theta)/n^2, \quad 0 \leq \theta \leq \pi$$

deduced from the relation between $\mathcal{L}(\theta)$ and the dilogarithm

$$\psi(z) = -\int_{0^z} \log(1-w)dw/w = \sum_{n\geq 1} z^n/n^2,$$

for $|z|leq1, |w|leq1$, obtained by setting $z = e^{2i\theta}$:

$$\psi(e^{2i\theta} - \psi(1) = -\theta(\pi-\theta) + 2i\mathcal{L}(\theta).$$

From this and using the Fourier transformation we have

$$(2) \qquad \sum_{kmod(D)} (\frac{-D}{k})\mathcal{L}(\pi k/D) = \sqrt{D}\sum_{n\geq 1}(\frac{-D}{n})n^{-2} = \sqrt{D}\zeta_{\mathbb{Q}(\sqrt{-D})}(2)/\zeta_{\mathbb{Q}}(2) = 6\pi^{-2}\sqrt{D}\zeta_{\mathbb{Q}(\sqrt{-D})}(2).$$

We also have the relations

$$(3) \qquad \mathcal{L}(\theta) \quad \text{is periodic of period } \pi \text{ and odd.}$$

$$(4) \qquad \mathcal{L}(n\theta) = \sum_{jmod(n)} n\mathcal{L}(\theta + j/n), \quad \text{for every integer } n \neq 0.$$

The relation (3) is immediate, the relation (4) is deduced from the trigonometric identity $2\sin u = \sum_{jmod(n)} 2\sin(u+j\pi/n)$ which can be proved by factoring the polynomial $X^n - 1$.
Milnor conjecture that every rational linear relation among the real numbers $\mathcal{L}(\theta)$, for the angles which are the rational multiples of π, is a consequence of (3) and (4). See also Lang [1].
Volume of a tetrahedron of which one vertices is at the infinity.
A picture here!!!

The base of such a tetrahedron is a sphere with center on $\mathbb{C}$. The projection on $\mathbb{C}$ from the tetrahedron is a triangle, of which the angles are the dihedral angles of their edges meeting at the infinity:$= \alpha, \beta, \gamma$. Therefore,

$$\alpha + \beta + \gamma = \pi.$$

Suppose $\gamma = \pi/2$ and A is projected to $(0,0)$, and let V be the volume of the tetrahedron

$$V = \int\int\int v^{-3}dxdydv = \int\int_t dxdy/2(1-x^2-y^2)$$

where $t = \{(x,y)|0 < x \leq x\tan\alpha\}$, we obtain by setting $x = \cos\theta$,

$$V = -1/4\int_{\pi/2}^{\delta} \log(\sin(\theta+\alpha)/\sin(\theta-\alpha))d\theta,$$

then

$$V = 1/4(\mathcal{L}(\alpha+\delta) + \mathcal{L}(\alpha-\delta) + 2\mathcal{L}(\pi/2-\alpha)).$$

If the vertex B is in C (two vertices are at the infinity), we have $\delta = \alpha$ and

$$V = 1/2\mathcal{L}(\alpha).$$

Volume of a tetrahedron of which its three vertices are at the infinity.

A picture here!!!
Since in the neighborhood of each vertex the sum of dihedral angles is π, the opposite dihedral angles are equal: we have then at most 3 distinct dihedral angles. Let they be α, β, γ and by intersecting the dihedral with the tetrahedron of the precedent type, we see that

Proposition 4.3.8. *The volume of a tetrahedron of which the vertices are at the infinity, and of the dihedral angles α, β, γ, is equal to*

$$V = \mathcal{L}(\alpha) + \mathcal{L}(\beta) + \mathcal{L}(\gamma).$$

EXAMPLE. A fundamental domain for Picard group $PSL(2, \mathbb{Z}[i])$. The domain defined by the relation (Picard [1]):

A picture here!!!

$$x^2 + y^2 + z^2 geq 1, \quad x \leq 1/2, \quad y \leq 1/2, \quad 0 \leq x + y$$

is a fundamental domain for $PSL(2, \mathbb{Z}[i])$ in $\mathcal{H}_3$. It is the union of four equal tetrahedrons all of which have a vertex at the infinity. With the above definitions we have $\delta = \pi/3$ and $\alpha = \pi/4$. The volume of the domain then is

$$\begin{aligned} V &= \mathcal{L}(\pi/4 + \pi/3) + \mathcal{L}(\pi/4 - \pi/3) + 2\mathcal{L}(\pi/2 - \pi/4) \\ &= 1/3 \cdot \mathcal{L}(3\pi/4 - \pi) + \mathcal{L}\pi/4) \\ &= 1/3 \cdot \mathcal{L}(-\pi/4) + \mathcal{L}(\pi/4) \\ &= 2/3 \cdot \mathcal{L}(\pi/4) \\ &= (4\pi^2)^{-1} \cdot D_K^{3/2} \cdot \zeta_K(2), \quad \text{if } K = \mathbb{Q}(i) \end{aligned} .$$

On the other side, for Tamagawa measure we have $vol(SL(2, \mathbb{Z}(i) \backslash SL(2, \mathbb{C})) = 4\pi^2 V$. Using the same argument to $SL(2, \mathbb{R})$, we can prove the following corollary by compare.

Corollary 4.3.9. *The Tamagawa measure on $SL(2, \mathbb{C})$ is the product of the hyperbolic measure on $\mathcal{H}_3$ by the Haar measure on $SL(2, \mathbb{C})$ such that*

$$vol(SU(2, \mathbb{C})) = 8\pi^2.$$

Therefore, if Γ is a discrete subgroup of $SL(2, \mathbb{C})$ of finite covolume

$$vol(SL(2, \mathbb{C})/\Gamma) = \begin{cases} 4\pi^2 vol(\bar{\Gamma} \backslash \mathcal{H}_3) \text{if } -1 \in \Gamma \\ 8\pi^2 vol(\bar{\Gamma} \backslash \mathcal{H}_3) \qquad \text{if } -1 \notin \Gamma \end{cases} .$$

We find again Humbert formula for $PSL(2, R)$ if R is the integer ring of an imaginary quadratic field K:

$$vol(PSL(2, R) \backslash \mathcal{H}_3) = 4\pi^2 \zeta_K(2) D_K^{3/2}.$$

Remark 4.3.10. *Let H/K be a quaternion algebra satisfying the properties in the beginning of chapter IV, and C be a maximal compact subgroup of G^1. The*

groups Γ *of units of reduced norm 1 in the* $R_{(S)}$*-order of* H *are allowed to define the arithmetic variety :*

$$X_\Gamma = \Gamma\backslash G^1/C.$$

The results of Chapter III have then the interesting applications to the study of varieties X_Γ*. We refer reader to the works of Ihara, Shimura, SErre, Mumford, Cerednik, Kurahara cited in the bibliography.*

Chapter 5

Quaternion arithmetic in the case where the Eichler condition is not satisfied any more

Let H/K be a quaternion algebra over a global field, ramified over every archimedean place of K, if it exists. Let S be a nonempty finite set of places of K containing the archimedean places, and not satisfying Eichler condition:

$$S \neq \varnothing, \infty \subset\subset Ram(H).$$

Let $R = R_{(S)}$ be the ring of the elements of K which are integral to the places that are not contained in S, and $\mathcal{O}$ be a R-order of H. Set

$$X = H \quad \text{or} \quad K, \quad Y = R \quad \text{or} \quad \mathcal{O}.$$

The algebra X satisfies the fundamental property:

$$X_v = Y_v \text{ is a field if } v \in S.$$

It is allowed to give
1. The structure of unit group of Y (the generalization of Dirichlet theorem).
2. an analytic formula for the class number of ideals of Y (the generalization of Dirichlet formula).
So obtained formula is traditionally called a formula "of mass" or "with weight", it combines the trace formulae (III.5.11) together and can be used to calculate the class number and the type number of Eichler orders of the give levels if $X = H$.
The methods used here are the same as in VI,1.
The results 1.2 are from the direct application of III.1.4 and III.2.2, more precisely, of the following results:
the group $X_K^\times$ is discrete, cocompact in $X_{A,1}$, and of the covolume 1 for Tamagawa measure.

5.1 Units

If $v \in S$, then $X_v = Y_v$ is a field. Therefore for every place v,

$$Z_v = \{y \in Y_v | ||y||_v \leq 1\}$$

is compact in X_v. It follows that $Z_A = X_A \cap (\prod Z_v)$ is compact in X_A, and that the group

$$Z_A \cap X_K = \{y \in Y | ||y||_v \leq 1 \quad \forall v \in V\}$$

which is discrete in Z_A by III.1.4 is a finite group. It is hence equal to the torsion group Y^1 of Y. We have proved the

Lemma 5.1.1. *The Group Y^1 of the roots of unit in Y is a finite group.*

If $X = K$ is commutative, it is a cyclic group according to the classical result about the finiteness of the subgroup of commutative field. If $X = H$, it is not commutative in general. When K is a number field it can be embedded in a finite subgroup of the real quaternions. Its structure is well known(I.3.1).
According to III.1.4, the group $X_K^\times$ is discrete, cocompact in $X_{A,1}$. Let us proceed as in IV.1.1, and describe $X_{A,1}/X_K^\times$. By III.5.4 we have a finite decomposition (at present it is not reduced to one term):

$$(1) \qquad X_{A,1} = \cup Y_{A,1} x_i X_K^{\times, \quad x_{i \in X_{A,1}}}, \quad 1 \leq i \leq h$$

where we set

$$Y_{A,1} = G \cdot C' \quad \text{with } G = \{x \in X_{A,1'|x_v} = 1 \text{ if } v \notin S\}$$

and C' is a compact group which is equal to $\prod_{v \notin S} Y_v^\times$. It follows from Lemma 1.1 that

$$Y^{\times = Y_{A,1}} \cap X_K^\times \quad \text{is discrete, cocompact in } G.$$

LEt f be the mapping which for $x \in G$ associates with $(||x_v||_v)_{v \in S}$. According to 1.1, we have the exact sequence

$$1 \longrightarrow Y^1 \longrightarrow Y^\times \xrightarrow{f} f(G) \cdot$$

It follows that $f(Y^\times)$ is a discrete, cocompact subgroup of a group which is isomorphic to $\mathbb{R}^a \cdot \mathbb{Z}^b$, $a + b = CardS - 1$, supposing

$$f(G) = \{(x_v) \in \prod_{v \in S} ||X_v|| \quad | \prod x_v = 1\}.$$

Therefore, $f(Y^\times)$ is a free group with $CarsS - 1$ generators.

Theorem 5.1.2. *Let $Y^\times$ be the unit group of Y. Then it exists an exact sequence:*

$$1 \to Y^1 \to Y^\times \to \mathbb{Z}^{CardS-1} \to 1$$

and Y^1 which is the group of the roots of unit contained in Y is finite.

When $X = K$ is commutative, we deduce from it that $Y^\times$ is the direct product of Y^1 by a free group with $CardS - 1$ generators. It is not true if $X = H$ as what Exercise 1.1 points out. The theorem 1.2 is an analogue of IV.1.1

Definition 5.1. *The regulator of Y is the volume of $f(G)/f(Y^\times)$ calculated for the measure induced by Tamagawa measure. we denote it by $\mathcal{R}_Y$.*

Exercise

1. Structure of unit group if K is a number field. Keep the hypotheses and what are given in §1 unchanging. Suppose in addition that K is a number field.
   a) Prove K is totally real (i.e. all of its archimedean places are real).
   b) Deduce from 1.2 that $[\mathcal{O}^\times : \mathcal{O}^1 R^\times]$ is finite.
   c) If L/K is a quadratic extension, and R_L is the integer ring of L. Prove $[R_{L^\times} : R_L^1 R^\times] = 1$ or 2. (Solution: see Hasse [1]).
   d) Utilizing I.3.7 and exercise 3.1 prove that

$$e = [\mathcal{O}^\times : \mathcal{O}^1 R^\times] = 1, 2, \quad \text{or } 4.$$

   (Solution: Vignéras-Guého [3]). Prove more precisely, with the notations of I.3.7 and exerise 3.1 that we have
   $e = 4$, if $\mathcal{O}^1$ is cyclic, generated by s_{2n} of order $2n$, and it exists e_1, e_2 two units of $\mathcal{O}$, of which the reduced norms are not the squares (evidently a necessary condition) and satisfy

$$e_1 e_2 = -e_2 e_1, \quad \text{if } n = 1,$$

$$e_1 \in K(s_{2n}), e_2 s_{2n} = s_{2n}^{-1} e_2.$$

   $e = 2$, if $e \neq 4$, if it exists $e_1 \in \mathcal{O}$ of which the reduced norm is not a square, and
   if $\mathcal{O}^1$ is cyclic, dicyclic, or binary octahedral, with: if $\mathcal{O}^1$ is cyclic generated by $s_{2n}, e_1 \in K(s_{2n})$ or $e_1 s_{2n} = s_{2n}^{-1} e_1$,
   if $\mathcal{O}^1 =< s_{2n}, j >$ is dicyclic of order $4n$, $e_1 \in (1 + s_{2n})K^\times$,
   if $\mathcal{O}^1 = E_{48}$ is the binary octahedal, $e_1 \in (1 + i)K^\times$, where $i \in \mathcal{O}^1$ is of order 4.
   $e = 1$ in all other cases.

2. Let $K = \mathbb{Q}(\sqrt{m})$ and H be the quaternion field $\{-1, -1\}$ over K (notation as in I.1). Prove:
   a)All the infinite places of K is ramified in H.
   b) There is no any finite place to be ramified in H if 2 can not be decomposed in K. Otherwise, if v, w are two places of K above 2, , then $Ram_f(H) = \{v, w\}$.
   c) $m = 2$. Thus

$$\mathcal{O} = \mathbb{Z}[\sqrt{2}][1, (1 + i)/\sqrt{2}, (1 + j)/\sqrt{2}, (1 + i + j + ij)/2]$$

   is a maximal order and its unit group is (with notation in I.3.7)

$$\mathcal{O}^\times = E_{48} \cdot \mathbb{Z}[\sqrt{2}].$$

   d) $m = 5$, if $\tau = (1 + \sqrt{5})/2$ is the golden number we then set

$$e_{1=\frac{1}{2}}(1 + \tau^{-1} i + \tau j),$$
$$e_{2=\frac{1}{2}}(\tau^{=1} i + j + ij),$$
$$e_3 = \tfrac{1}{2}(\tau i + \tau^{-1} j + \tau ij),$$
$$e_4 = \tfrac{1}{2}(i + \tau j + \tau^{-1} ij).$$

Therefore,

$$\mathcal{O} = \mathbb{Z}[\tau][e_1, e_2, e_3, e_4]$$

is a maximal order, of which the unit group id

$$\mathcal{O}^\times = E_{120} \cdot \mathbb{Z}[\tau]^\times.$$

3. Regulator Suppose $X = H$. Keeping the notations of §1, Prove:
a) $[\mathcal{O}^\times : R^\times] = [\mathcal{O}^1 : R^1][f(\mathcal{O}^\times) : f(R^\times)]$.
b) $[f(\mathcal{O}^\times) : f(R^\times)] = 2^{2CardS-1}\mathcal{R}_R/\mathcal{R}_\mathcal{O}$.
Prove also that the regulator of $\mathcal{O}$ and of R are related by the relation:

$$\mathcal{R}_\mathcal{O} = \mathcal{R}_R 2^{2CardS-1}[\mathcal{O}^1 : R^1][\mathcal{O}^1 : R^\times]^{-1}$$

or the same:

$$\frac{\mathcal{R}_\mathcal{O}}{Card\mathcal{O}^1} = [\mathcal{O}^\times : R^\times]^{-1}\frac{\mathcal{R}_R}{CardR^1}2^{2CardS-1}.$$

5.2 Class number

The equality $\tau(X_1) = 1$ given in II.2.2 and 2.3 takes by means of the relation (1) of §1 the form

$$1 = vol(X_{A,1}/X_K^\times) = \sum_{i=1}^{h} vol(Y_{A,1}x_i X_K^\times/X_K^\times).$$

Put

$$Y^{(i)} - X_K \cap x_i^{-1}Y_A x_i.$$

The global-adele dictionary in III.§5,B allows us to recognize the following properties:
1) h is the class number of ideals to the left of Y.
2)A system of representative of these ideals is described by the set $\{Y_A x_i \cap X_K | 1 \leq i \leq h\}$. The set of right order of the ideals is $\{Y^{(i)} | 1 \leq i \leq h\}$ According to the definition of regulator of Y we have

$$1 = \sum vol(Y_{A,i}^{(i)}/{Y^{(i)}}^\times) = vol(C)\sum e_i^{-1}\mathcal{R}_{Y^{(i)}}$$

where C is a compact group being equal to

$$C = \prod_{v\in S} X_v^1 \prod_{p\notin S} Y_p^\times.$$

We have proved then the following theorem which is analogue with IV.1.7.

Theorem 5.2.1. *With the notations of chapter V, we have*

$$\sum_{i=1}^{h} e_i^{-1}\mathcal{R}_{Y^{(i)}} = vol(C)^{-1}.$$

Corollary 5.2.2. *(Dirichlet's analytic formula). Let K be a number field, of integer ring R, having $r_1(r_2)$ real (complex) places . Let $h, \mathcal{R}, D_R, w$ be the class number, the regulator, the discriminant, the number of the roots of unit in R respectively. Therefore,*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{h\mathcal{R}}{w\sqrt{D_R}}2^{r_1}(2\pi)^{r_2}.$$

Proof. We apply the theorem to compute $vol(C)$ in use of the explicit formula II.4.3 and exercises 4.2,4.3:

$$vol(C) = m_K^{-1}2^{r_1}(2\pi)^{r_2}D_R^{-1/2,} \quad {}^{m_K} = \lim_{s\to 1}(s-1)\zeta_K(s).$$

□

Corollary 5.2.3. *Let H/K be a quaternion field ramified at every archimedean place of a number field K, and $\mathcal{O}$ be an Eichler order of K. Keeping the notations of corollary 2.2 we denote by D the reduced discriminant of H and by N the level of $\mathcal{O}$. We choose a system (I_i) of the representatives of the ideal classes to the left of $\mathcal{O}$. If $\mathcal{O}_i$ is the right order of I_i, then $w_i = [\mathcal{O}_i^\times : R^\times]$. We have (by setting $n = r_1$):*

$$\sum w_i^{-1} = 2^{1-n}|\zeta_K(-1)|hN\prod_{p|D}(Np-1)\prod_{p|N}(Np^{-1}+1).$$

Proof. We proceed as in 2.2 by using the relation between R and the regulator of $\mathcal{O}$ which we saw in exercise 1.3. We obtain

$$\sum w_i^{-1} = vol(C)^{-1}(\frac{\mathcal{R}}{w}2^{2n-1})^{-1} = (m_K volC)^{-1}hD_R^{-1/2}2^{1-n}$$

$$m_K volC = (2\pi^2)^n D_R^{-2}\zeta_K(2)f(D,N),$$

$$f(D,N) = N\prod_{p|D}(Np-1)\prod_{p|N}(Np^{-1}+1)$$

where we notice that K is totally real, hence $n = r_1$, and the functional equation of the zeta function permit to connect $\zeta_K(2)$ with $\zeta_K(-1)$:

$$\zeta_K(2)D_R^{-3/2}(-2\pi^2)^{-n} = \zeta_K(-1).$$

2.3 follows. □

In order to go further, it is necessary to use the trace formula III.5.11:

$$\sum_{\mathcal{O}}^{(i)} = h(B)\prod_{p\notin S} m_p.$$

When C.E. is not satisfied, the structure of $\mathcal{O}^\times$ implies the number of maximal inclusions of B in $\mathcal{O}^{(i)}$ is finite and equal to

$$Card\{xgx^{-1}|x \in T^{(i)}$$

if $B = R[g] \subset H$ in the notations of III.5. It follows that if $w_i = [\mathcal{O}^{(i)} : R^\times]$ and $w(B) = [B^\times : R^\times]$, we then have

$$m_i = m_{\mathcal{O}}^{(i)} \quad w_i/w(B) = m_i(B).$$

It follows

$$\sum m_i/w_i = \frac{h(B)}{w(B)} \prod_{p \notin S} m_p.$$

Definition 5.2. *We call*

$$M = \sum_{i=1}^{h} 1/w_i, M(B) = \sum_{i=1}^{h} m_i/w_i$$

the mass of $\mathcal{O}$ and the mass of B in $\mathcal{O}$.

We consider then the Eichler-Brandt matrices $P(A)$ defined in III. exercise 5.8 for the integral ideal of R. these are the matrices in $M(h, \mathbb{N})$. The entries at i- place of the diagonal $\alpha_{i,i}$ is equal to the number of the principal ideals in $\mathcal{O}^{(i)}$ with reduced norm A. When C.E. is not satisfied the traces of the matrices can be calculate in use of III.5.11 and V.2.3. The result is given below. Suppose K to be a number field.

Proposition 5.2.4. *(The trace of Eichler-Brandt matrix). The trace of matrix $P(A)$ is null if A in not a principal ideal. If A is not the square of a principal ideal, it is equal to*

$$\frac{1}{2} \sum_{(x,B)} M(B).$$

Otherwise, it is equal to

$$M + \frac{1}{2} \sum_{(x,B)} M(B)$$

where (x, B) runs through all the pairs formed by an element $x \in K_s$, and a commutative order B satisfying:
– x is the root of an irreducible polynomial $X^2 - tX + a$, where (a) is a system of representatives of the generators of A modulo ${R^\times}^2$, and $t \in R$; – $R[x] \subset B \subset K(x)$.

Proof. If A is not principal, this is clear. Otherwise, we utilize

$$2w_i\alpha_{i,i} = \sum_a Card\{x \in \mathcal{O}^{(i)} | n(x) = 1\}.$$

Introduce now the pairs (x, B). By the definitions of III.5.11, we see that

$$2w_i\alpha_{i,i} = \sum_{(x,B)} + \begin{cases} 0 & \text{if } A \text{ is not a square} \\ 2 & \text{if } A \text{ is a square} \end{cases}.$$

We then use the precedent definition for mass. □

Corollary 5.2.5. *(class number). The class number of the ideals to the left of $\mathcal{O}$ equals*

$$M + \frac{1}{2}\sum_B M(B)(w(B)-1)$$

where B runs through the orders of the quadratic extensions L/K Contained in K_s.

Proof. 2.4 will be used with $A = R$. We utilize that B being fixed, the sum over x is equal to $w(B)$, since the units ∓ 1 are gained by M. The order B only appear when $w(B) \neq 1$. This happens only a finite number of times. □

This explicit formula can be recover by the computation of II.4. We can obtain by the same procedure a formula for the type number of the orders of $\mathcal{O}$. Let $2^r = [N(\mathcal{O}_A) : \mathcal{O}_A^\times K_A^\times]$, and h_i' be the class number of the two-sided ideals of $\mathcal{O}^{(i)}$. Choose a system (A) of principal integral ideals of R, representing that ideals which are principal, of reduced norm the two-sided ideals of $\mathcal{O}$, and modulo the squares of the principal ideals. Therefore,

$$h_i' = h2^r / \sum \alpha_{i,i}(A).$$

It follows

$$\sum_A traceP(A) = th2^r$$

from it we have a expression for t.

Corollary 5.2.6. *The type number of orders of an Eichler order is equal to*

$$\frac{1}{h2^{r+1}}\sum_B M(B)w(B)x(B) + \frac{M}{h2^r}$$

where $x(B)$ is the number of pricipal integral ideals of B of reduced norm in (A). The orders B runs all the orders of the quadratic extensions $L \subset K_s$ over K.

In this general formula we find again that results which were proved in the particular cases by different authors (Deuring [3], Eichler [2], [8], Latimer [2], Pizer [1], Vigneras-Gueho [2]). We can find some applications of these results to the forms defined by quaternions in the articls of Ponomarv [1]-[5] and Peters [1].

5.3 Examples

A Quaternion algebra over $\mathbb{Q}$.
Let $H/\mathbb{Q}$ be a quaternion algebra such that $H_{\mathbb{R}} = \mathbb{H}$, and of reduced discriminant D. It is interesting to consider the maximal orders of $\mathbb{H}$. Let $\mathcal{O}$ be such an order. The group of its units is equal to the group of its units with reduced norm 1. Let h be the class number of $\mathcal{O}$. We have

Proposition 5.3.1. *The unit group of of a maximal order is cyclic of order $2, 4$ or 6, except for*

$$H = \{-1,-1\},\ \textit{where } D = 2, h = 1, \mathcal{O}^\times \simeq E_{24};$$
$$H\{-1,-3\},\ \textit{where } D = 3, h = 1, \mathcal{O}^\times \simeq < s_6, j >.$$

The notations used here are that in I.3.7. Suppose $D \neq 2, 3$ and denote by h_i the class number of ideals I to the left of $\mathcal{O}$ such that the unit group of $I^{-1}I$ is of order $2i$. Applying 2.4 and the formula for mass $M(B)$, with $B = \mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-3}]$, we have

Proposition 5.3.2. *The class number h, h_2, h_3 are equal to*

$$\begin{array}{ll} h & = \frac{1}{12}\prod_{p|D}(p-1) + \frac{1}{4}\prod_{p|D}(1-(\frac{-4}{p})) + \frac{1}{3}\prod_{p|D}(1-\frac{-3}{p})) \\ h_2 & = \frac{1}{2}\prod_{p|D}(1-(\frac{-4}{p})) \\ h_3 & = \frac{1}{2}\prod_{p|D}(1-(\frac{-3}{p})) \end{array} .$$

We can give another proof of the formula for h in a pure algebraic way . It will use the relation between the quaternion algebras and the elliptic curves (Igusa [1]). We shall give a table for h and for the type number of maximal orders t in the end of §3.

B.Arithmetic graphes.

We shall give a geometric interpretation of the class numbers h, h_2, h_3, and the Brandt matrices i terms of graphs. Let p be a prime number which does not divide D. The tree $X = PGL(2, \mathbb{Z}_p \backslash PGL(2, \mathbb{Q}_p)$ admits a description by the orders and the ideals of H: we fix first a maximal order $\mathcal{O}$,

– The vertices of X correspond bijectively to the maximal orders $\mathcal{O}'$ such that $\mathcal{O}_q = \mathcal{O}'_q, \quad \forall q \neq p$;

– The edges of X of the starting $\mathcal{O}'$ are correspond bijectively to the integral ideals which are to the left of $\mathcal{O}'$ and with reduced norm $p\mathbb{Z}$.

Precisely, to $x \in X$, with the representative $a \in GL(2, \mathbb{Q}_p) = H_p^\times$, we associate the order $\mathcal{O}'$ such that $\mathcal{O}'_p = a^{-1}\mathcal{O}_p a$, and $\mathcal{O}'_q = \mathcal{O}_q$ if $q \neq p$. SEE II.2.5 and 2.6.

Let $\mathbb{Z}^{(p)}$ be the set of the rational number of the form $a/p^n, a \in \mathbb{Z}, n \in \mathbb{N}$. The maximal orders $\mathcal{O}'$, i.e. the vertices of X, generate the same $\mathbb{Z}^{(p)}$-order $\mathcal{O}^{(p)} = \prod_{q \neq p}(\mathcal{O}_q \cap H)$. The unit group $\mathcal{O}^{p\times}$ defines an isometric group $\Gamma = \mathcal{O}^{(p)^\times}/\mathbb{Z}^{(p)^\times}$ of the tree X of which the quotient graph is finite. The group $\Gamma_{\mathcal{O}'}$of the isometries of Γ fixing a vertex $\mathcal{O}'$ is equal to $\mathcal{O}'^\times/\mathbb{Z}^\times$. It is from the above results :

—A cyclic group of order $1, 2, 3$;

—A_4, if $H = \{-1, -1\}$;

—D_3, if $H = \{-1, -3\}$.

By definition $Card(\Gamma_{\mathcal{O}'})$ is the order of vertex of X/Γ defined by $\mathcal{O}'$.

Proposition 5.3.3. *The number of the vertices of the quotient graph X/Γ is equal to the number of class h of H.*
If $H = \{-1, -1\}$ resp. $H = \{-1, -3\}$, the quotient graph has a single vertex of order 12, resp, of order 6. In the other cases, the number of the vertices of order i of the quotient graph is equal to h_i.

In fact, this is the consequence of a formal computation in the ideles : Since $\{\infty, p\}$ satisfies the Eichler condition, and $\mathbb{Z}^{(p)}$ is principal, the order $\mathcal{O}^{(p)}$ is principal(Ch.III), thus it has the decomposition $H_A^\times = \prod \mathcal{O}_q^\times H_\infty^\times H_p^\times H^\times$, the product is taken on all the prime numbers $q \neq p$. By using the decomposition $\mathbb{Q}_A^\times = \mathbb{Q}^\times \mathbb{Z}_p^\times \prod \mathbb{Z}_q^\times$ expressing that $\mathbb{Z}$ is principal, we see that the class number of maximal orders (over $\mathbb{Z}$) of H is the cardinal of one of the sets which is

isomorphic to

$$\mathbb{Q}_A^\times H_\infty^\times \mathcal{O}_p^\times \prod \mathcal{O}_q^\times \backslash H_A^\times / H^\times = \mathcal{O}_p^\times \mathbb{Q}_p \backslash H_p^\times / {\mathcal{O}^{(p)}}^\times = X/\Gamma.$$

Precisely, if (I_i) is a system of the representatives of classes of the ideals to the left of $\mathcal{O}$, the right orders the ideals I_i , denoted by $\mathcal{O}(i)$, constitute a system of representatives of the quotient graph X/Γ. An order $\mathcal{O}'$, vertices of the tree X, is Γ-equivalent to $\mathcal{O}^{(i)}$ if it is joined to $\mathcal{O}$ by an ideal I which is equivalent to I_i.
The Brandt matrix can be explained geometrically as the homomorphism of the free group $\mathbb{Z}[X/\Gamma]$ generated by the vertices of the quotient graph X/Γ. Let $f : \mathbb{Z}[X] \to \mathbb{Z}[X/\Gamma]$ be the homomorphism induced by the surjection $X \to X/\Gamma$. For every integer $n \geq 1$, let P_n be the homomorphism od $\mathbb{Z}[X/\Gamma]$ such that $P_n f = f T_n$ where T_n is the homomorphism of $\mathbb{Z}[X]$ defined by the relations, Ch.II,§1,

$$T_0(\mathcal{O}') = \mathcal{O}', \quad T_1(\mathcal{O}') = \sum_{d(\mathcal{O}',\mathcal{O}'')=1} \mathcal{O}'', \quad T_1 T_n = T_{n+1} + q T_{n-1}.$$

The Brandt matrices $P(p^n)$ are the matrices of homomorphism P_n on the basis of $\mathbb{Z}[X/\Gamma]$ consisting of the vertices x_i , the images of the maximal order $\mathcal{O}_i$.
In fact, it suffices to prove for $n = 0, 1$, since the last relation of T_n is true for P_n and $P(p^n)$. For $n = 0$, It is evident because $P(1)$ is the identity matrix. For $n = 1$, the coefficient a_{ij} of the matrix P_1 on the basis x_i defined by $P_1(x_i) = \sum a_{ij} x_j$, is:

$$a_{ij} = Card\{\mathcal{O}'' | f(\mathcal{O}'') = \mathcal{O}_j, d(\mathcal{O}_i, \mathcal{O}'') = 1\}.$$

this is the number of the integral ideals I to the left of $\mathcal{O}_i$ with reduced norm $p\mathbb{Z}$ such that $I_i I$ is equivalent to I_j. We do discover here the definition of Brandt matrix $P(p)$.
The group $\Gamma_{(\mathcal{O}',\mathcal{O}'')}$ of the isometries of Γ which fix an edge $(\mathcal{O}', \mathcal{O}'')$ with starting point $\mathcal{O}'$ and end point $\mathcal{O}''$ is $({\mathcal{O}'}^\times \cap {\mathcal{O}''}^\times)/\mathbb{Z}^\times$. The number $Card\Gamma_{(\mathcal{O}',\mathcal{O}'')}$ is called the order of the edge of quotient graph X/Γ,which is the image of $(\mathcal{O}', \mathcal{O}'')$. For every vertex x of the quotient graph X/Γ we denote by $A(x)$, resp. $S(x)$ the set of the edges y of X/Γ with the starting point x, resp. of the end points of that edges with starting point x, and $e(x)$, resp. $e(y)$, the order of vertex x, resp. the order of the edge y. We have

$$q + 1 = e(x) \sum_{y \in A(x)} e(y)^{-1}$$

and the homomorphism P_1 is given by

$$P_1(x) = e(x) \sum_{x' \in S(x)} e(y)^{-1} x', \qquad \text{where } x' \text{ is the end point of } y.$$

We see thus immediately that the matrix of P_1 is symmetric with respect to the basis $(e(x)^{-1/2}x)$, where x runs through the vertices of X/Γ. This is simply the matrix $(a(x, x'))$, where $a(x, x') = e(x, x')^{-1}$ if the vertices x, x' are joined by an edge $y = (x, x')$ and $a(x, x') = 0$ if there is no any edge joining x to x'.

C Classical isomorphism.
We are going to explain How certain isomorphisms of finite groups can be proved by taking advantage of quaternion. Let $q = p^n, n \geq 0$ be a power of a prime number p, we have then $Card(GL(2, \mathbb{F}_q)) = (q^2 - 1)(q^2 - q)$ and $Card(SL(2, \mathbb{F}_q)) = (q - 1)q(q + 1)$. In particular, $Car(SL(2, \mathbb{F}_3)) = 24$, $Card(GL(2, \mathbb{F}_3)) = 48$, $Card(SL(2, \mathbb{F}_4)) + 60$, $Card(SL(2, \mathbb{F}_5)) = 120$.

Proposition 5.3.4. *The tetrahedral binary group E_{24} of order 24 is isomorphic to $SL(2, \mathbb{F}_3)$. The Alternate group A_5 of order 60 is isomorphic to $SL(2, \mathbb{F}_4)$ and the icosahedral binary group E_{120} of order 120 is isomorphic to $SL(2, \mathbb{F}_5)$.*

Proof. E_{24} is isomorphic to the unit group of a maximal order(uniquely determined up to isomorphism) $\mathcal{O}$ of a quaternion field $\{-1, -1\}$ over $\mathbb{Q}$ of reduced discriminant 2, and the natural homomorphism $\mathcal{O} \to \mathcal{O}/3\mathcal{O} = M(2, \mathbb{F}_3)$ induces an isomorphism of E_{24} onto $SL(2, \mathbb{F}_3$. E_{120} is isomorphic to the unit group of reduced norm 1 of a maximal order (unique up to isomorphism) $\mathcal{O}$ of the quaternion field $\{-1, -1\}$ over $\mathbb{Q}(\sqrt{5})$ which is unramified at the finite places. The natural homomorphism $\mathcal{O} \to \mathcal{O}/2\mathcal{O} = M(2, \mathbb{F}_4$ induces a homomorphism of E_{120} onto $SL(2, \mathbb{F}_4)$ with kernel $\{\mp 1\}$, hence $A_5 = E_{120}/\{\mp 1\}$ is isomorphic to $SL(2, \mathbb{F}_4)$. The natural homomorphism $\mathcal{O} \to /\sqrt{5}\mathcal{O}$ induces an isomorphism of E_{120} onto $SL(2, \mathbb{F}_5)$. □

D The construction of Leech lattice.
Recently Jacques Tits gave a nice construction of Leech lattice in virtue of quaternions which we shall give as an example of the application of the arithmetic theory of quaternion. We shall point out that J.Tits in this manner obtained an elegant geometric description of the twelve among the twenty-four sporadic groups defined in practice (these 12 groups appear as the subgroups os automorphisms of Leech lattice).

Definition 5.3. *A $\mathbb{Z}$-lattice of dimension n is a subgroup of $\mathbb{R}^n$ which is isomorphic to $\mathbb{Z}^n$. We denote by $x \cdot y$ the usual scalar product in $\mathbb{R}^n$. We say that the lattice L is even if all the scalar product $x \cdot y$ are integers for $x, y \in L$, and if all the scalar products $x \cdot x$ are even for $x \in L$. We say that L is Unimodular if it is equal to its dual lattice $L' = \{x \in \mathbb{R}^n | x \cdot L \subset \mathbb{Z}\}$ with respect to the scalar product. We say that two lattices are equivalent if it exists an isomorphism from one group to another such that it conserves the scalar product invariant.*

We can show easily that a unimodular even lattice is of dimension divided by 8, and even classify these lattices in the dimension $8, 16, 24$ where they have $1, 224$ classes respectively. In the higher dimension, the Minkowski-Siegel formula, the mass formula analogue to what we have proved for the quaternion algebra, and that it amounts to as a formula for a Tamagawa number, show that the class number is gigantic: it increases with the number of variables, and it in dimension 32 is already great than 80 millions! Leech discovered that one of these lattices in dimension 24 has a remarkable property which characterizes the following

Proposition 5.3.5. *The Leech lattice is the only lattice which is even,unimadular, of dimension 24, and not containing any vector x with $x \cdot x = 2$.*

The method for constructing the even unimodular lattice.
Choose a commutative field K which is totally real and of even degree $2n$ such

that the difference of K is totally principal in the restrict sense and denote by H the unique quaternion field(up to isomorphism)which is totally defined over K and unramified at the finite places. Let R, Rd be the integer ring of K and its difference respectively.

Proposition 5.3.6. *The maximal R-orders of H equipped with the scalar product:*

$$x \cdot y = T_{K/\mathbb{Q}}(d^{-1}t(x\bar{y})$$

are the unimodular, even lattice of dimension $8n$.

Proof. Recall that the inverse of the difference is the dual of the integer ring R of K with respect to the bilinear form $T_{K/\mathbb{Q}}(x\bar{y})$ defined by the trace $T_{K/\mathbb{Q}}$ of K over $\mathbb{Q}$. Let $\mathcal{O}$ be a maximal R-order of H. It is clear that $\mathcal{O}$ is isomorphic to a $\mathbb{Z}$-lattice of dimension $8n$. It should prove that the bilinear form defined in the proposition is equivalent to the usual scalar product, or in another words, the quadratic form defined by $q(x) = 2T_{K/\mathbb{Q}}(d^{-1}n(x))$ is positively definite. In fact, $x \in H^{\times}$ implies That $d^{-1}n(x)$ is totally positive and the trace is strictly positive.
We verify that
a) $x \cdot y \in \mathbb{Z}$ and $x \cdot x \in 2\mathbb{Z}$, because the inverse of the difference Rd^{-1} were sent to each other by the trace in $\mathbb{Z}$.
b) $\mathcal{O}$ is equal to its dual $\mathcal{O}' = \{x \in H | T_{K/\mathbb{Q}}(d^{-1}t(x\mathcal{O})) \subset \mathbb{Z} = \{x \in H | t(x\mathcal{O}) \in R\}$ because H is not ramified at the finite places. □

The construction of Leech lattice.
For the reasons prior to the curiosity of a non-specialist in the theory od finite groups which is justified by the presence of the binary icasahedral group in the automorphisms of Leech's lattice, The construction of Tits for the lattice utilizes the quternion field H which is totally defined and unramified over $K = \mathbb{Q}(\sqrt{5})$. We have seen that a maximal R-order $\mathcal{O}$ equipped with the scalar product in the precedent proposition is a unimodular even latticeof order 8, and recall that, if $\tau = (1 + \sqrt{5})/2$, Then

$$R = \mathbb{Z}[1, \tau] \quad \text{and } x \cdot y = T_{K/\mathbb{Q}}(2x\bar{y}/(5 + \sqrt{5})).$$

We shall observe later that the only integers x which are totally positive in R of trace $T_{K/\mathbb{Q}}(x) \leq 4$ are

$$(1) \qquad 0, 1, 2, \tau^2 = (3 + \sqrt{5})/2, \tau^{-2} = (3 - \sqrt{5})/2.$$

Although it is not used here, it bears in mind that we have given an explicit R-basis of an order $\mathcal{O}$ in exercise. The unit group of reduced norm 1 of $\mathcal{O}$ denoted by $\mathcal{O}^1$ is isomorphic to the icosahedral binary group of order 120, and contains the cubic roots of unit. Let x be one of them, put $e = x + \tau$. We can prove immediately that $n(e) = 2$, and $e^2 = emod(2)$.
We denote by h the standard hermitian form of the H-vector space H^3:

$$h(x, y) = \sum x_i \bar{y}_i, \quad \text{if } x = (x_i) \text{ and } y = (y_i) \text{ belong to } H^3,$$

from it we deduce on that on $\mathbb{R}^{24}$ there is a scalar product induced by the $\mathbb{Q}$-bilinear form of $\mathbb{Q}$-vector space H^3 of dimension 24:

$$x \cdot y = T_{K/\mathbb{Q}}(2h(x, y)/(5 + \sqrt{5}))$$

. The Leech lattice is the lattice in $\mathbb{R}^{24}$ equipped with the above scalar product and defined by one of the following equivalent ways:

$$(a) \qquad L = \{x \in \mathcal{O}^3 | ex_1 \equiv ex_2 \equiv ex_3 \equiv \sum x_i mod(2)\},$$

$$(b) \qquad L \quad \text{is the free } \mathcal{O}\text{-module of basis } f = (1, 1, e), g = (0, \bar{e}, \bar{e}), h = (0, 0, 2).$$

we shall prove that we obtain rightly the Leech lattice. Actually the lattice L is
– even, since $x, y \in \mathbb{Z}$, and $x \cdot x \in 2\mathbb{Z}$, it is evident.
– unimodular, since if $x \in H^3$ the equality $x \cdot L \subset \mathbb{Z}$ is equivalent to $h(x, L) \subset 2R$ and the definition (b) shows the last inclusion is equivalent to $x \in L$.
– not contains any element x such that $x \cdot x = 2$. Otherwise $x \in L$, $x \cdot x = 2$, then put $r_i = n(x_i)$. It follows that $\sum r_i = 2$, and since the elements r_i are totally positive, (1) implies that one of them at least should be annihilated. The definition (a) of lattice implies then that $ex_i \in 2\mathcal{O}$ for every $1 \leq i \leq 3$, From it we have $2n(x_i) \in 4R$ and $x_i \in 2\mathcal{O}$. Taking again the same reason, we see that at most one of x_i is nonzero and $r_i \in 4R$, It leads to a contradiction.
E Tables.
If H is a quaternion algebra totally defined over $\mathbb{Q}$, i.e. $H_R = \mathbb{H}$ the Hamilton quaternion field, of reduced discriminant $D = \prod_{p \in Ram(H)} p$, the class number and the type number of t are given by the formulae:

$$h = h(D, N) = \frac{1}{12} \prod_{p|D} (p-1) \prod_{p|N} (p+1) + \frac{1}{4} f(D, N)^{(1)} + \frac{1}{3} f(D, N)^{(3)}, \quad t = 2^{-r} \sum_{m|DN} tr(m)$$

where r is the number of prime divisors of DN,

$$f(D, N)^{(m)} = \prod_{p|D} (1 - (\frac{d(-m)}{p})) \prod_{p|N} (1 + (\frac{d(-m)}{p})$$

$d(-m), h(-m)$ are the discriminant and the class number of $\mathbb{Q}(\sqrt{m})$ respectively.

$$d(-m) = \begin{cases} -m, & \text{if } m \equiv -1 mod(4) \\ -4m, & \text{if } m \not\equiv -1 mod(4) \end{cases}, d(-1) = -4, d(-3) = -3,$$

$$g(D, N)^{(m)} = 2 \prod_{p|D} (1 - (\frac{d(-m)}{p})) \prod_{p|(N/2} (1 + (\frac{d(-m)}{p})), \quad \text{defined if } N \text{ is even.}$$

Set:

$$a(m) = \begin{cases} 1, & \text{if } m \not\equiv -1 mod 4 \\ 2, & \text{if } m \equiv 7 mod 8 \text{ or } m = 3 \\ 4, & \text{if } m \equiv 3 mod 8 \text{ and } m \neq 3 \end{cases},$$

$$b(m) = \begin{cases} a(m), & \text{if } m \not\equiv 3 mod 8 \text{ or } m = 3 \\ 3, & \text{if } m \equiv 3 mod 8 \text{ and } m \neq 3 \end{cases},$$

the number $tr(m)$ are the traces of the Brandt matrices $P(\mathbb{Z}_m)$ for $m|DN$:

$$2tr(m) = \begin{cases} f(D, N)^{(m)} h(-m), & \text{if } D \text{ is even} \\ f(D, N)^{(m)} h(-m) a(m), & \text{if } DN \text{ is odd} \\ g(D, N)^{(m)} h(-m) b(m), & \text{if } N \text{ is even} \end{cases}.$$

The class number of ideals for the relation $J = aIb$, I, J are the ideals of the order of level N, $a, b \in H^{\times}$ is given by the formula

$$h^{+} = 2^{-r} \sum_{m|DN} tr(m)^2.$$

these tables were computed by Henri Cohen of The Center of Computation at Bordeaux.
Here are tables occupying two pages!!! See this original book, pp.153,154.

With the help of these tables, we can prove that there are 10 Eichler orders of the level N without square factors , of a quaternion field totally defined over $\mathbb{Q}$, and of the reduced discriminant D, and of the class number 1 (up to isomorphisms). We obtain them with:

D	N
2	1,3,5,11
3	1,2
5	1,2
7	1
13	1

The explicit computation for the quaternion algebra totally defined over a real quadratic field $\mathbb{Q}(\sqrt{m})$ Allows to prove that the Eichler orders of level N without square factor of the quaternion algebras , which are totally defined over $\mathbb{Q}(\sqrt{m})$ of the reduced discriminant D, have the class number equal to h_m^+, and have the class number in the restrict sense of $\mathbb{Q}(\sqrt{m})$, are obtained with the following data:

m	D	N
2	$1, p_2p_3, p_2p_5, p_2p_7^{(i)}$	1
	1	$p_2, p_7^{(i)}, p_{23}^{(i)}$
3	$p_2p_3, p_2p_5, p_2p_{13}^{(i)}, p_3p_{13}^{(i)}$	1
	1	$p_2, p_3, p_{11}^{(i)}$
5	$1, p_2p_5, p_2p_{11}^{(i)}$	1
	1	$p_2, p_3, p_5, p_{11}^{(i)}, p_{19}^{(i)}, p_{29}^{(i)}, p_{59}^{(i)}$
6	$p_2p_3, p_3p_5^{(i)}$	1
13	$1, p_2p_3^{(i)}$	1
	1	$p_5^{(i)}$
15	p_2p_3	1
17	1	$1, p_2^{(i)}$
21	$1, p_2p_3$	1
	1	$p_5^{(i)}$
33	$p_2^{(i)}p_3$	1

There are 54 couples (D, N). The ideals $p_a^{(i)}, i = 1, 2$ represent the prime ideals

of $\mathbb{Q}(\sqrt{m})$ above a. For the different values of m we have

m	2	3	5	6	7	13	15	17	21	33
$\zeta_{\mathbb{Q}(\sqrt{m})}(-1)$	1/12	1/6	1/30	1/2	2/3	1/6	2	1/3	1/3	1
h_m^+	1	2	1	2	2	1	4	1	2	2

Abelian cubic field: The Eichler order of level N without square factor,of discriminant D, in a quaternion algebra totally defined over an abelian cubic field of discriminant m^2, and which has a class number equal to the class number h_m^+ of center, are the 19 maximal orders given by the following list:

m	*equation*	$\zeta(-1)$	D
7	$x^3 - 7x - 7$	$-1/21$	$p_2, p_3, p_{13}^{(i)}, p_{29}^{(i)}, p_{43}^{(i)}$
9	$x^3 - 3x + 1$	$-1/9$	$p_3, p_{19}^{(i)}, p_{37}^{(i)}$
13	$x^3 - x^2 - 4x - 1$	$-1/3$	p_{13}

Reference: Vigneras-Gueho [3].

Exercise

Euclidean orders. Prove it exists exactly 3 quaternion algebras totally defined over $\mathbb{Q}$, of which the maximal orders (over $\mathbb{Z}$) are euclidean for the norm. Their reduced discriminants are 2,3,5 respectively.

(I translate this book just for those who want read it but up to now still has a little difficulty for reading French. I am not an expert both in quaternion algebra and French language, so definitely there are many mistakes both in mathematics and in language. When you read it you must be more careful than usual. Correct them please.—translator,27 Sept. 2006. Beijing)