Arithmetic of Quaternion Algebra 2012

1 Quaternion Algebras

In this section, F is a field of characteristic $\neq 2$. Unless stated otherwise, all algebras considered here are finite dimensional algebras over F. If 1_A (or simply 1) is the identity of an F-algebra A, then the map $\alpha \mapsto \alpha 1_A$ is a monomorphism of F-algebras. This map identifies F as a subalgebra of A.

If R is a ring, then $R^\times$ denotes the group of units in R.

1.1 Basic Definitions

Definition 1.1 A *quaternion algebra* H over F is a 4-dimensional algebra over F with a basis $\{1, i, j, k\}$ such that

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

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

In this definition, notice that $k^2 = -ab$. The basis $\{1, i, j, k\}$ is called a *standard basis* for H and we write $H = \left(\frac{a,b}{F}\right)$. Note that there are infinitely many standard bases for H, and hence there could be another pair of nonzero elements $c, b \in F$, different from the pair a, b, such that $\left(\frac{c,d}{F}\right) = \left(\frac{a,b}{F}\right)$. For instance, $\left(\frac{a,b}{F}\right) = \left(\frac{ax^2,by^2}{F}\right)$ for any $x, y \in F^\times$, and $\left(\frac{a,b}{F}\right) = \left(\frac{a,-ab}{F}\right)$.

The notation $H = \left(\frac{a,b}{F}\right)$ is functorial in F, that is, if K is a field extension of F, then

$$\left(\frac{a,b}{F}\right) \otimes K \cong \left(\frac{a,b}{K}\right) \quad \text{as } K\text{-algebras.}$$

Example 1.2 In $M_2(F)$, let

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

Then $i^2 = j^2 = 1$ and $\{1, i, j, k\}$ is a basis for $M_2(F)$. Therefore, $M_2(F) = \left(\frac{1,1}{F}\right) = \left(\frac{1,-1}{F}\right)$.

Example 1.3 Another familiar example of quaternion algebras is Hamilton's quaternions $\mathbb{H}$. It is a quaternion algebra over $\mathbb{R}$ with a basis $\{1, i, j, k\}$ such that

$$i^2 = -1, \quad j^2 = -1, \quad ij = k = -ji.$$

This shows that $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. A simple calculation shows that any two elements from $\{i, j, k\}$ are anti-commutative. Moreover, $ij = k, jk = i$ and $ki = j$.

Theorem 1.4 *Let $a, b \in F^\times$. Then $\left(\frac{a,b}{F}\right)$ exists.*

Proof. Fix α, β in an algebraic closure E of F such that $\alpha^2 = a$ and $\beta^2 = -b$. Consider the two matrices

$$i = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}, \qquad j = \begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix}.$$

Direct computations show that

$$i^2 = a, \quad j^2 = b, \quad ij = \begin{pmatrix} 0 & \alpha\beta \\ \alpha\beta & 0 \end{pmatrix} = -ji.$$

Since $\{I_2, i, j, ij\}$ is clearly independent over E, it is also linearly independent over F. Therefore the F-span of $\{I_2, i, j, ij\}$ is a 4-dimensional algebra H over F, and $H = \left(\frac{a,b}{F}\right)$.□

Theorem 1.5 *A quaternion algebra over F is central simple, that is, its center is F and it does not have any nonzero proper two-sided ideal.*

Proof. Let H be a quaternion algebra over F, and $\{1, i, j, k\}$ be a standard basis of H over F. Consider an element $x = \alpha + \beta i + \gamma j + \delta k$ in the center of H, where $\alpha, \beta, \gamma, \delta \in F$. Then

$$0 = jx - xj = 2k(\beta + \delta j).$$

Since k is invertible in H, we must have $\beta = \delta = 0$. Similarly, $\gamma = 0$. Hence x is in F.

Next, we need to show that a nonzero two-sided ideal $\mathfrak{a}$ is H itself. It is sufficient to show that $\mathfrak{a}$ contains a nonzero element of F. Take a nonzero element $y = a + bi + cj + dk$ in $\mathfrak{a}$, where $a, b, c, d \in F$. We may assume that one of b, c and d is nonzero. By replacing y by one of iy, jy and ky, we may further assume that $a \neq 0$. Since $yj - jy \in \mathfrak{a}$ and $2k$ is invertible in H, we see that $b + dj$, and hence $bi + dk$ as well, are in $\mathfrak{a}$. This shows that $a + cj$ is in $\mathfrak{a}$. By the same token, $a + bi$ and $a + dk$ are also in $\mathfrak{a}$. As a result, $-2a = y - (a + bi) - (a + cj) - (a + dk)$ is a nonzero element of F lying in $\mathfrak{a}$.□

So, we may study quaternion algebras using the theory of central simple algebras. Below is a couple of well-known theorems concerning the structure of central simple algebras.

Theorem 1.6 (Wedderburn's Structure Theorem) *Let A be a finite dimensional simple algebra over F. Then A is isomorphic to $M_n(D)$, where $D \cong End_A(N)$ is a division algebra over F with N a nonzero minimal right ideal of A. The integer n and the isomorphism class of the division algebra D is uniquely determined by A.*

Theorem 1.7 (Skolem-Noether Theorem) *Let A be a finite dimensional central simple algebra over F and let B be a finite dimensional simple algebra over F. If ϕ, ψ are algebra homomorphisms from B to A, then there exists an invertible element $c \in A$ such that $\phi(b) = c^{-1}\psi(b)c$ for all $b \in B$. In particular, all nonzero endomorphisms of A are inner automorphisms.*

Theorem 1.8 *Let H be a quaternion algebra over F.*

(a) Either H is a division algebra or $H \cong M_2(F)$.

(b) Let E be a subfield of H which is a quadratic extension of F, and τ be the nontrivial automorphism of E/F. Then there exists $j \in H^\times$ such that $j^2 \in F^\times$, $H = E + Ej$, and $jx = \tau(x)j$ for all $x \in E$.

Proof. Part (a) is a direct consequence of Wedderburn's structure theorem. For part (b), since the characteristic of F is not 2, we can write $E = F(i)$ so that $i^2 \in F^\times$. Let τ be the nontrivial automorphism of E/F. By the Skolem-Noether Theorem, $-i = \tau(i) = jij^{-1}$ for some invertible element $j \in H$. Clearly $j \notin E$ and $1, i, j$ are linearly independent over F. If $ij = \alpha + \beta i + \gamma j$ with $\alpha, \beta, \gamma \in F$, then $(i - \gamma)j = \alpha + \beta i$. But $i - \gamma \neq 0$; thus $j \in F(i) = E$ which is impossible. Therefore, $\{1, i, j, ij\}$ is a basis for H. Note that $ij = -ji$ and so $j^2 ij^{-2} = i$. Therefore, j^2 is in the center of H which is F, and this means that $j^2 = b \in F$. Clearly, $H = E + Ej$.□

Definition 1.9 Let $\{1, i, j, k\}$ be a standard basis for a quaternion algebra H. The elements in the subspace H_0 spanned by i, j and k are called the *pure quaternions* of H.

The next proposition shows that H_0 does not depend on the choice of the standard basis for H.

Proposition 1.10 *A nonzero element $x \in H$ is a pure quaternion if and only if $x \notin F$ and $x^2 \in F$.*

Proof. Let $\{1, i, j, k\}$ be a standard basis for $H = \left(\frac{a,b}{F}\right)$. Let x be a nonzero element in H. We can write $x = a_0 + a_1 i + a_2 j + a_3 k$ with $a_\ell \in F$ for all ℓ. Then

$$x^2 = (a_0^2 + aa_1^2 + ba_2^2 - aba_3^2) + 2a_0(a_1 i + a_2 j + a_3 k).$$

If x is in the F-space spanned by i, j and k, then $a_0 = 0$ and hence $x \notin F$ but $x^2 \in F$. Conversely, suppose that $x \notin F$ and $x^2 \in F$. Then one of a_1, a_2 and a_3 is nonzero, and hence $a_0 = 0$. Thus x is a pure quaternion.□

Thus each $x \in H$ has a unique decomposition $x = a + \alpha$, where $a \in F$ and $\alpha \in H_0$. The *conjugate* of x, denoted $\overline{x}$, is defined by $\overline{x} = a - \alpha$. For any $x, y \in H$,

(i) $\overline{x + y} = \overline{x} + \overline{y}$;

(ii) $\overline{xy} = \overline{y}\,\overline{x}$;

(ii) $\overline{\overline{x}} = x$;

(iv) $\overline{rx} = r\overline{x}$ for all $r \in F$.

(v) $\overline{x} = x$ if and only if $x \in F$.

In particular, the conjugation is an involution on H (or, equivalently, an algebra isomorphism from H to its opposite algebra H°). In $M_2(F)$,

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Equivalently, if $M \in M_2(F)$, $\overline{M} = \mathrm{adj}(M)$, the adjoint of M.

Definition 1.11 For $x \in H$, the (reduced) *norm* and (reduced) *trace* of x are the elements $\mathrm{nr}(x) = x\overline{x}$ and $\mathrm{tr}(x) = x + \overline{x}$, respectively.

A direct computation shows that both $\mathrm{nr}(x)$ and $\mathrm{tr}(x)$ are elements of F. The norm is multiplicative, that is, $\mathrm{nr}(xy) = \mathrm{nr}(x)\mathrm{nr}(y)$ for all $x, y \in H$. The invertible elements of H are precisely those with nonzero norm. The trace, however, is linear as $\mathrm{tr}(ax + by) = a\mathrm{tr}(x) + b\mathrm{tr}(y)$ for all $a, b \in F$. For $M_2(F)$, the norm of an element is just its determinant.

1.2 The Matrix Algebras

In this subsection, we discuss when a quaternion algebra H over F is isomorphic to $M_2(F)$.

Definition 1.12 A nonzero element x in H is said to be *isotropic* if $\mathrm{nr}(x) = 0$.

Theorem 1.13 *For $H = \left(\frac{a,b}{F}\right)$, the following are equivalent:*

(a) $H \cong \left(\frac{1,1}{F}\right) \cong M_2(F)$.

(b) H *is not a division algebra.*

(c) H *has an isotropic element.*

(d) H_0 *has an isotropic element.*

(e) The equation $ax^2 + by^2 = 1$ *has a solution* $(x, y) \in F \times F$.

(f) If $E = F(\sqrt{b})$, *then* $a \in \mathbb{N}_{E/F}(E)$.

Proof. We have seen in Theorem 1.8 that (a) is equivalent to (b).

Suppose that H is not a division algebra. Then it has a nonzero element x which is not invertible. So, $\mathrm{nr}(x) = 0$. This proves (b) $\Rightarrow$ (c).

For (c) $\Rightarrow$ (d), let x be an isotropic element in H. Let $\{1, i, j, k\}$ be a standard basis for H and write

$$x = a_0 + a_1 i + a_2 j + a_3 k.$$

We may assume that $a_0 \neq 0$. So, at least one of a_1, a_2 and a_3 is also nonzero. Without loss of generality, we assume that $a_1 \neq 0$. From $\mathrm{nr}(x) = 0$, we obtain $a_0^2 - ba_2^2 = a(a_1^2 - ba_3^2)$. Let

$$y = b(a_0a_3 + a_1a_2)i + a(a_1^2 - ba_3^2)j + (a_0a_1 + ba_2a_3)k.$$

Check that $\mathrm{nr}(y) = 0$. If $y \neq 0$, then we are done. If $y = 0$, then $-aa_1^2 + aba_3^2 = 0$ and thus

$$\mathrm{nr}(a_1 i + a_3 k) = 0.$$

Since $a_1 \neq 0$, $a_1 i + a_3 k$ is an isotropic element in H_0.

Suppose that H_0 has an isotropic element $a_1 i + a_2 j + a_3 k$. Then $-aa_1^2 - ba_2^2 + aba_3^2 = 0$, and so at least two of a_1, a_2 and a_3 are nonzero. If $a_3 \neq 0$, then

$$a\left(\frac{a_2}{aa_3}\right)^2 + b\left(\frac{a_1}{ba_3}\right)^2 = 1.$$

If $a_3 = 0$, then

$$a\left(\frac{1+a}{2a}\right)^2 + b\left(\frac{a_2(1-a)}{2aa_1}\right)^2 = 1.$$

This proves (d) $\Rightarrow$ (e).

For (e) $\Rightarrow$ (f), we assume that $ax_0^2 + by_0^2 = 1$. If $x_0 = 0$, then $\sqrt{b} \in F$ and $E = F$, in which case (f) is certainly true. If $x_0 \neq 0$, then one can check that $\mathbb{N}_{E/F}(x_0^{-1} + x_0^{-1} y_0 \sqrt{b}) = a$.

Lastly, we suppose that a is a norm from $F(\sqrt{b})$. If $b = c^2$ for some $c \in F$, then $(c + j)(c - j) = 0$ and H is not a division algebra. So, we may assume that $\sqrt{b} \notin F$. Then $a = x_1^2 - by_1^2$ for some $x_1, y_1 \in F$. Since $\mathrm{nr}(x_1 + i + y_1 j) = 0$, H again is not a division algebra. This proves (f) $\Rightarrow$ (b). $\square$

Definition 1.14 Let K/F be a field extension. A quaternion algebra H over F *splits* over K if $H \otimes_F K \cong M_2(K)$. We say that a quaternion algebra over F splits if it splits over F.

Corollary 1.15 *If F is algebraically closed, then every quaternion algebra over F splits.*

Proof. This is clear since every element of F is a square in F.$\square$

Corollary 1.16 *The quaternion algebras $\left(\frac{1,a}{F}\right)$ and $\left(\frac{a,-a}{F}\right)$ splits.*

Proof. Apply (d) and (e) of Theorem 1.13.$\square$

Example 1.17 Theorem 1.13 is very useful in constructing quaternion algebras that do not split. For example, let p be a prime $\equiv -1 \bmod 4$. Then the congruence $-x^2 + py^2 \equiv z^2 \bmod 4$ does not have any solution with $\gcd(x, y, z) = 1$. Therefore, the equation $-x^2 + py^2 = 1$ does not have any rational solution. Thus, by Theorem 1.13(e), the quaternion algebra $\left(\frac{-1,p}{\mathbb{Q}}\right)$ does not split. However, if $p \equiv 1 \bmod 4$, then p is a sum of two integer squares, which means that p is a norm from $\mathbb{Q}(\sqrt{-1})$. So, when $p \equiv 1 \bmod 4$, the algebra $\left(\frac{-1,p}{\mathbb{Q}}\right)$ splits. Thus we have shown; *Let p be a prime. Then $\left(\frac{-1,p}{\mathbb{Q}}\right)$ splits if and only if $p \equiv 1$ mod* 4.

Proposition 1.18 *Let H be a quaternion division algebra over F. If E is a subfield of H which is a quadratic extension of F, then H splits over E.*

Proof. As is in the proof of Theorem 1.1, there exists a standard basis $\{1, i, j, k\}$ for H with $E = F(i)$ and $i^2 = a \in F$. Thus $H = \left(\frac{a,b}{F}\right)$ and hence $H \otimes_F E = \left(\frac{a,b}{E}\right) = \left(\frac{1,b}{E}\right) = M_2(E)$.$\square$

1.3 Quaternion Algebras over Finite Fields

Theorem 1.19 (Wedderburn's Little Theorem) *Let A be a finite division ring. Then A is a field.*

Proof. Let F be the center of A. Then F is a finite field of order q, a prime power ≥ 2. Let $n = \dim_F A$. We shall show that $n = 1$. Assume the contrary that $n > 1$. The finite group $A^\times$ acts on itself by conjugation. It follows from the class equation that

$$|A^\times| = q^n - 1 = q - 1 + \sum_a [A^\times : C_A(a)^\times],$$

where $C_A(a)$ is the centralizer of a, and the a in the summation runs over a (nonempty) set of representatives of non-singleton conjugacy classes of $A^\times$. Let $r(a) = \dim_F C_A(a)$. Then $1 \leq r(a) < n$, and the transitivity of dimensions shows that $r(a) \mid n$. Rewriting the class equation, we have

$$(*) \qquad q^n - 1 = q - 1 + \sum_a \frac{q^n - 1}{q^{r(a)} - 1}.$$

Let r be one of the $r(a)$ in the summation. Since $r \mid n$, we have the following factorization in $\mathbb{Z}[x]$:

$$x^n - 1 = \Phi_n(x)(x^r - 1)h(x), \qquad h(x) \in \mathbb{Z}[x],$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial. This equation implies that $(q^n-1)/(q^r-1)$ is always an integer divisible by $\Phi_n(q)$. It follows from $(*)$ that $\Phi_n(q)$ divides $q-1$ as well. In particular,

$$q - 1 \geq |\Phi_n(q)| = \prod |q - \zeta|,$$

where ζ ranges over all the primitive n-th roots of unity. This is impossible since $n > 1$ and $q \geq 2$ clearly implies that $|q - \zeta| > q - 1 \geq 1$ for each ζ.□

Corollary 1.20 *If A is a central simple algebra over a finite field F, then $A \cong M_n(F)$ for some $n \geq 1$. In particular, every quaternion algebra over a finite field splits.*

2 Quaternion Algebras as Quadratic Spaces

Let H be a quaternion algebra over F. The norm map is a quadratic form on H, that is, it satisfies:

(i) $\mathrm{nr}(\alpha x) = \alpha^2 \mathrm{nr}(x)$ for all $\alpha \in F$,

(ii) the function $B : H \times H \to F$ defined by

$$B(x, y) := \frac{1}{2}\left(\mathrm{nr}(x + y) - \mathrm{nr}(x) - \mathrm{nr}(y)\right) = \frac{1}{2}\mathrm{tr}(x\overline{y})$$

is a symmetric bilinear form on H.

In this section, we will review some results from the algebraic theory of quadratic forms that are useful for later discussion.

2.1 Quadratic Spaces

A quadratic space over a field F is a pair (V, Q), where V is a finite dimensional vector space over F and $Q : V \to F$ satisfies:

(a) $Q(ax) = a^2 Q(x)$ for all $a \in F$ and all $x \in V$;

(b) the function $B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$ is a symmetric bilinear form on V.

The function Q is called a quadratic form on V. Note that B determines Q by $B(x, x) = Q(x)$ for all $x \in V$. So we also use (V, B) to denote the quadratic space (V, Q). A nonzero vector v in a quadratic space (V, Q) over a field F is *isotropic* if $Q(v) = 0$; otherwise v is called anisotropic. The space V is said to be isotropic if it has an isotropic vector.

Two subsets X and Y of V are said to be orthogonal if $B(x, y) = 0$ for all $x \in X$ and $y \in Y$. The set of vector in V which are orthogonal to every vector in X is denoted by $X^\perp$. The space V is called *nondegenerate* if $V^\perp = \{0\}$, that is, there is no nonzero vector in V which is orthogonal to all vectors in V. A basis of V is called an orthogonal basis if its vectors are orthogonal to each other.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis for V. The symmetric matrix $M_\mathcal{B} = (B(v_i, v_j))$ is called the matrix of V with respect to $\mathcal{B}$. The following is a easy consequence from linear algebra.

Lemma 2.1 *If $\mathcal{B}$ and $\mathcal{B}'$ are two bases for V, then there exists a matrix T in $GL_n(F)$ such that $M_{\mathcal{B}'} = T M_\mathcal{B} T^t$.*

Let V^* be the dual space of V, the vector space of all linear maps $V \to F$. If $\mathcal{B} = \{v_1, \ldots, v_n\}$ is a basis for V, then $\mathcal{B}^* = \{v_1^*, \ldots, v_n^*\}$ denotes its dual basis for V^*, where

$$v_i^*(v_j) = \delta_{ij} \qquad \text{(Kronecker's delta)}.$$

The function $\hat{B} : V \to V^*$ defined by $\hat{B}(v)(u) = B(v, u)$ is obviously a linear transformation.

Lemma 2.2 *If $\mathcal{B}$ is a basis for V and $\mathcal{B}^*$ is its dual basis for V^*, then the matrix of the linear transformation $\hat{B}$ with respect to $\mathcal{B}$ and $\mathcal{B}^*$ is $M_\mathcal{B}$.*

Proof. From $\hat{B}(v_i)(v_j) = B(v_i, v_j)$ follows

$$\hat{B}(v_i) = \sum_{j=1}^{n} B(v_i, v_j) v_j^*$$

which is what is needed to be shown.□

Lemma 2.3 *If W is a subspace of V, then $W^\perp = \ker(\pi \circ \hat{B})$ where $\pi : V^* \to W^*$ is the linear map induced by restricting functions in V^* on W.*

Proof. A vector v of V is in $W^\perp$ if and only if $B(v, w) = 0$ for all $w \in W$. This means $\hat{B}(v)|_W = 0$ and hence $v \in \ker(\pi \circ \hat{B})$.□

Corollary 2.4 *A quadratic space (V, B) is nondegenerate if and only if $\hat{B}$ is an isomorphism or, equivalently, when the matrix $M_{\mathcal{B}}$ is invertible for one particular basis $\mathcal{B}$ for V.*

Proof. This follows from the previous two lemmas.□

Corollary 2.5 *If W is a nondegenerate subspace of V, then $V = W \perp W^{\perp}$ (orthogonal sum).*

Proof. Clearly, W and $W^{\perp}$ are orthogonal to each other. So it remains to show that $V = W \oplus W^{\perp}$. As W is nondegenerate, $W \cap W^{\perp} = \{0\}$. Let $v \in V$ and $f = \hat{B}(v)|_W$. Then because W is nondegenerate, there exists $w \in W$ with $\hat{B}(w) = f$. Hence for all $z \in W$,

$$B(v, z) = \hat{B}(v)(z) = f(z) = \hat{B}(w)(z) = B(w, z).$$

So, $v - w \in W^{\perp}$ and we can write $v = w + (v - w)$. Thereby $W \perp W^{\perp} = V$.□

Theorem 2.6 *Every quadratic space has an orthogonal basis.*

Proof. Let (V, B) be a quadratic space. If $B = 0$, then the assertion is clear. So, we assume that $B \neq 0$. Then there exist vectors $u, v \in V$ such that $B(u, v) \neq 0$. Since $2B(u, v) = Q(u + v) - Q(u) - Q(v)$, it follows that there must be a $w \in V$ with $Q(w) \neq 0$. Then the one-dimensional subspace $W = Fw$ is nondegenerate, and by the last corollary $V = W \perp W^{\perp}$. An application of the induction hypothesis to $W^{\perp}$ completes the proof.□

Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis for V, and let $Q(e_i) = a_i$ for all i. For any $v = \sum x_i e_i \in V$, we have

$$Q(v) = a_1 x_1^2 + \cdots + a_n x_n^2.$$

In this case, we shall write $V \cong \langle a_1, \ldots, a_n \rangle$.

Let (V, Q) and (V, Q') be quadratic spaces over F. A linear map $\sigma : V \to V'$ is an *isometry* if

(a) σ is a vector space isomorphism;

(b) $Q'(\sigma(x)) = Q(x)$ for all $x \in V$.

Two quadratic spaces are isometric if there is an isometry from one to the other. The set of all isometries from V to V itself form a group which is called the *orthogonal group* of V, denoted $O(V)$. Suppose that x is an anisotropic vector in V. Then the function $\tau_x : V \to V$ defined by

$$\tau_x(y) = y - \frac{2B(y, x)}{Q(x)} x$$

is called the *symmetry with respect to* x, which is an element in $O(V)$.

Theorem 2.7 (Witt's Cancellation Theorem) *If V, V_1 and V_2 are nondegenerate quadratic spaces over F such that $V \perp V_1 \cong V \perp V_2$, then $V_1 \cong V_2$.*

Proof. Since V is the orthogonal sum of 1-dimensional subspaces, it suffices to consider the case where $\dim_F(V) = 1$; thus $V = Fx$. Under an isometry $Fx \perp V_1 \to Fx \perp V_2$, x is sent to a vector $y \in Fx \perp V_2$. Let $u = (x+y)/2$ and $v = (x-y)/2$. Then $B(u,v) = 0$ and $Q(x) = Q(u) + Q(v)$. This implies that either $Q(u)$ or $Q(v)$ is nonzero. If $Q(u) \neq 0$, then $-\tau_u(x) = y$; otherwise $\tau_v(x) = y$. Therefore, there is an isometry $\Sigma : Fx \perp V_1 \to Fx \perp V_2$ such that $\Sigma(x) = x$. It is easy to see that Σ must send V_1 to V_2.□

2.2 The Norm Form

Let H be a quaternion algebra over F. Recall that the reduced norm nr is a quadratic map on H. So, H equipped with nr is a 4-dimensional quadratic space over F. If $\{1, i, j, k\}$ is a standard basis for $H = \left(\frac{a,b}{F}\right)$, then

$$\mathrm{nr}(x + yi + zj + wk) = x^2 - ay^2 - bz^2 + abw^2,$$

and so $\{1, i, j, k\}$ is an orthogonal basis of H. Moreover, since $ab \neq 0$, H is nondegenerate as a quadratic space. The subspace of pure quaternions H_0 equipped with nr is a nondegenerate 3-dimensional quadratic space over F. Note that for any $x \in H_0$, $\overline{x} = -x$, and thus for all $x, y \in H_0$ we have

$$\mathrm{nr}(x) = -x^2 \text{ and } B(x,y) = -\frac{1}{2}(xy + yx).$$

From now on, when we say that H or H_0 is a quadratic space, it will be understood that the associated quadratic form is the reduced norm. The main theorem of this subsection is the following classification theorem of quaternion algebras in terms of quadratic spaces.

Theorem 2.8 *Let H and H' be quaternion algebras over F. Then H and H' are isomorphic if and only if the quadratic spaces H_0 and H_0' are isometric.*

Proof. Let nr and nr$'$ be the reduced norms of H and H', respectively. Suppose first that there exists an algebra isomorphism $\phi : H \to H'$. Let x be a nonzero vector in H_0. Then $x \notin F$ but $x^2 \in F$. So, $\phi(x) \notin F$ and $\phi(x)^2 = \phi(x^2) \in F$. Therefore, $\phi(x) \in H_0'$, which shows that ϕ is a vector space isomorphism from H_0 into H_0'. For any $x \in H_0$, $\mathrm{nr}'(\phi(x)) = -\phi(x)^2 = \phi(-x^2) = \phi(\mathrm{nr}(x)) = \mathrm{nr}(x)$. Thus H_0 and H_0' are isometric.

Now suppose that $\sigma : H_0 \to H_0'$ is an isometry. Let $\{1, i, j, ij\}$ be a standard basis for $H = \left(\frac{a,b}{F}\right)$. Since $\mathrm{nr}(i) = -i^2 = -a$, therefore $\sigma(i)^2 = -\mathrm{nr}'(\sigma(i)) = a$. Similarly, we have $\sigma(j)^2 = b$. The elements i and j are orthogonal in H_0. Therefore, $\sigma(i)$ and $\sigma(j)$ are also orthogonal. So, $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i)$. Then one can easily check that $\sigma(i)$ does not commute with $\sigma(i)\sigma(j)$, which means that $\sigma(i)\sigma(j) \notin F$. Also, $(\sigma(i)\sigma(j))^2 = -ab \in F$. Thus $\sigma(i)\sigma(j) \in H_0'$. If $r\sigma(i) + s\sigma(j) + t\sigma(i)\sigma(j) = 0$ for some $r, s, t \in F$, then left multiplication by $\sigma(i)$ to this equation forces $r = 0$. By a similar token, $s = t = 0$. Thus $\{1, \sigma(i), \sigma(j), \sigma(i)\sigma(j)\}$ is a standard basis for H' so that $H' = \left(\frac{a,b}{F}\right)$.□

3 Quaternion Algebras over Local Fields

In this section, we give a more thorough discussion of quaternion algebras over a local field. A local field, by our definition, is the completion of a number field with respect to a nontrivial valuation. The complex numbers $\mathbb{C}$ and the real numbers $\mathbb{R}$ are examples of local fields. By Corollary 1.15, every quaternion algebra over $\mathbb{C}$ must split. Over $\mathbb{R}$, the only quaternion algebras are $\left(\frac{1,1}{\mathbb{R}}\right)$, $\left(\frac{1,-1}{\mathbb{R}}\right)$ and $\left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{H}$, since $\mathbb{R}^\times$ has only two square classes represented by 1 and -1 respectively. The first two are isomorphic to $M_2(\mathbb{R})$.

3.1 Local Fields

Let F be a number field, which is just a finite extension of $\mathbb{Q}$. By definition, every element of F is algebraic over F. In other words, every element α of F is a root of a monic polynomial over $\mathbb{Q}$. If this monic polynomial is over $\mathbb{Z}$, then we say that α is an algebraic integer in F. Let $\mathfrak{o}$ be the set of all algebraic integers in F. Then $\mathfrak{o}$ is a ring and we call it the ring of integers of F. It is well-known that the field of fractions of $\mathfrak{o}$ is F, and $\mathfrak{o}$ is a Dedekind domain, that is, it satisfies the following three properties:

(a) it is Noetherian, which means that every ascending chain of ideals must become stationary after finite number of steps ;

(b) it is integrally closed, which means that an element of F that is a root of a monic polynomial over $\mathfrak{o}$ is already in $\mathfrak{o}$;

(c) all its nonzero prime ideal are maximal.

A nontrivial consequence of these properties is that every nonzero ideal $\mathfrak{a}$ of $\mathfrak{o}$ is a product of prime ideals, and these prime ideals, counted with multiplicities, are uniquely determined by $\mathfrak{a}$.

A (multiplicative) valuation v on F is a function $v : F \to \mathbb{R}$ such that

(1) $v(x) \geq 0$ for all $x \in F$, and $v(x) = 0$ if and only if $x = 0$.

(2) $v(xy) = v(x)v(y)$ for all $x, y \in F$.

(3) $v(x + y) \leq v(x) + v(y)$ for all $x, y \in F$.

There is always the trivial valuation where $v(x) = 1$ for all $x \neq 0$. We assume throughout that *all valuations in the subsequent discussion are nontrivial.* Two valuations v and v' are equivalent if there exists $c \in \mathbb{R}^+$ such that $v'(x) = v(x)^c$ for all $x \in F$. A place of F is an equivalence class of valuations on F. The set of all places of F is denoted by Ω_F or simply Ω if F is understood from the discussion. If v is a valuation on F, we also use v to denote the place containing v.

A valuation v is called *nonarchimedean* if it satisfies in addition the ultra triangle inequality

$$(3)' \quad v(x + y) \leq \max\{v(x), v(y)\}$$

for all $x, y \in F$ with equality when $v(x) \neq v(y)$. A place v is called a *finite* place if it contains a nonarchimedean valuation. Otherwise it is called an *infinite* place. The set of all finite places of F and the set of infinite places of F are denoted by Ω_f and Ω_∞, respectively.

Let v be a place of F. The function $d(x, y) = v(x - y)$ defines a metric on F. The completion of F with respect to this metric is denoted by F_v, which is a locally compact complete metric space. The valuation v extends uniquely to a valuation on F_v which we also denote by v. It turns out that F_v is a field, and its addition, subtraction, multiplication and taking inverse are all continuous operations with respect to the metric topology. Associated to v is an embedding $\sigma_v : F \to F_v$, and we can identify F as a subfield of F_v through σ_v. We usually make no distinction between F and $\sigma_v(F)$. So, when we write $F \subseteq F_v$, it is understood that F is embedded in F_v through σ_v. In this way, we identify each element $a \in F$ with its image $\sigma_v(a)$ in F_v.

If v is a finite place, then F_v is called a $\mathfrak{p}$-adic field. The set $\{x \in F_v : v(x) \leq 1\}$ is a subring of F_v, which is called the ring of integers in F_v. It is a local ring with maximal ideal

$$\mathfrak{p}_v (\text{or simply } \mathfrak{p}) = \{x \in F_v : v(x) < 1\}.$$

Every nonarchimedean valuation of F is coming from a nonzero prime ideal of $\mathfrak{o}$ in the following way. Suppose that $\mathfrak{p}$ is a nonzero prime ideal of $\mathfrak{o}$. For any nonzero element x in $\mathfrak{o}$, the ideal $x\mathfrak{o}$ has an ideal factorization

$$x\mathfrak{o} = \mathfrak{p}^n \mathfrak{a},$$

where $\mathfrak{p} \nmid \mathfrak{a}$. Let $\mathbb{N}(\mathfrak{p}) := |\mathfrak{o}/\mathfrak{p}|$ be the norm of $\mathfrak{p}$ and set $v(x) = \mathbb{N}(\mathfrak{p})^{-n}$. Then v extends to an nonarchimedean valuation on F. It turns out that this way of constructing nonarchimedean valuations yields a bijection between Ω_f and the nonzero prime ideals of $\mathfrak{o}$. The residue field of F_v is the field $\mathfrak{o}_v/\mathfrak{p}_v$, which is isomorphic to $\mathfrak{o}/\mathfrak{p}$, a finite extension of the field $\mathbb{Z}/p\mathbb{Z}$ of p elements. A consequence of this is that $\mathfrak{o}_v$ is a compact subset in F_v, which makes F_v locally compact. The ring $\mathfrak{o}_v$ is a PID, and its maximal ideal $\mathfrak{p}_v$ is generated by any element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. In general, a generator of $\mathfrak{p}_v$ is called a *uniformizer* of F_v, which is an element in $\mathfrak{p}_v$ of the largest valuation. The nonzero ideals of $\mathfrak{o}_v$ are of the form $\mathfrak{p}_v^n$, $n \in \mathbb{N}$. Let π be a uniformizer of F_v. Then every nonzero element in $F_v^\times$ can be written as $\pi^m \epsilon$ with $m \in \mathbb{Z}$ and ϵ a unit in $\mathfrak{o}_v$.

Suppose that $[F : \mathbb{Q}] = n$. Then there are n different embeddings of F into $\mathbb{C}$. An embedding $\sigma : F \to \mathbb{C}$ is called a real embedding if $\sigma(F) \subseteq \mathbb{R}$; otherwise it is called a complex embedding. Since complex embeddings occur in pairs, $n = r + 2s$ where r (resp. s) is the number of real (resp. complex) embeddings of F. If σ is an embedding of F into $\mathbb{C}$, then $v(a) = |\sigma(a)|$ is a valuation on F. Here $|\ |$ is the complex modulus. Note that a complex embedding and its complex conjugation yield the same valuation. So the total number of inequivalent valuations obtained in this way is $r + s$, and they correspond to all the infinite places of F. An infinite place v of F is real if it corresponds to a real embedding; otherwise it is called a complex place. When v is a real (resp. complex) place, F_v is isomorphic to $\mathbb{R}$ (resp. $\mathbb{C}$).

Example 3.1 There is only one infinite place on $\mathbb{Q}$ which contains the usual absolute value on $\mathbb{R}$. This is clearly a real place. Let p be a prime number. For any nonzero rational number x, we can write $x = p^n z$, where z is a rational number for which p divides neither the numerator nor the denominator. Then $v(x) = p^{-n}$ is called the p-adic valuation on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to this valuation is called the field of p-adic numbers, denoted $\mathbb{Q}_p$. The ring of integers in $\mathbb{Q}_p$ is $\mathbb{Z}_p$, the ring of p-adic integers.

In this lecture notes, a local field always means the completion of a number field with respect to a valuation. Let K be a local field and E/K be a finite extension. It turns out that E is also a local field. If v is a valuation on K, then v extends uniquely to a valuation w on E by

$$w(x) = v(N_{E/K}(x))^{\frac{1}{[E:K]}},$$

where $N_{E/K}$ is the norm from E to K.

Definition 3.2 A finite extension of $\mathfrak{p}$-adic fields E/K is called unramified if a uniformizer in K is also a uniformizer in E. Otherwise E/K is ramified.

Let $\mathfrak{o}_K$ and $\mathfrak{o}_E$ be the ring of integers of K and E, respectively, and let π be a uniformizer of K. Then E/K is unramified if and only if π generates the maximal ideal of $\mathfrak{o}_E$. In general, if $\mathfrak{p}_E$ is the maximal ideal of $\mathfrak{o}_E$, then $\pi\mathfrak{o}_E = \mathfrak{p}_E^e$ for some positive integer e. This e is called the *ramification index* of E/K. Note that E/K is unramified exactly when $e = 1$. The residue field $\mathfrak{o}_E/\mathfrak{p}_E$ is a finite extension of the residue field $\mathfrak{o}_K/\mathfrak{p}_K$. Its degree of extension $[\mathfrak{o}_E/\mathfrak{p}_E : \mathfrak{o}_K/\mathfrak{p}_K]$ is called the residue degree of E/K, usually denoted by f.

Theorem 3.3 (Local Fundamental Identity) *If E/K is a finite extension of $\mathfrak{p}$-adic fields, then $ef = [E : K]$.*

The next theorem is an important result form local class field theory.

Theorem 3.4 (Local Norm Index) *Let E/K be a finite abelian extension of local fields. Then*

$$[K^\times : N_{E/K}(E^\times)] = [E : K].$$

Corollary 3.5 *Let E/K be a quadratic extension of $\mathfrak{p}$-adic fields. Then E/K is unramified if and only if $N_{E/K}(E^\times)$ contains all the units of the ring of integers in K.*

Proof. Suppose that E/K is unramified. If $\pi := N_{E/K}(x)$ is a uniformizer of K, then $w(x) = v(N_{E/K}(x))^{\frac{1}{2}} = v(\pi)^{\frac{1}{2}}$. But since π is also a uniformizer of E, we must have

$$1 > v(\pi) = w(\pi) \geq w(x) = v(\pi)^{\frac{1}{2}},$$

which is impossible. So, $N_{E/K}(E^\times)$ does not contain any uniformizer of K. Notice that $N_{E/K}(E^\times)$ contains $K^{\times 2}$, and that every coset in $K^\times/K^{\times 2}$ is represented by an element of

K of the form $\pi^\delta \epsilon$, where $\delta \in \{0,1\}$ and $\epsilon \in \mathfrak{o}_K^\times$. So, $[K^\times : \mathfrak{o}_K^\times K^{\times 2}] = 2$. It follows form the Local Norm Index Theorem that $N_{E/K}(E^\times)$ is equal to $\mathfrak{o}_K^\times K^{\times 2}$ in this case.

The converse now is obvious.□

We can say more about unramified quadratic extensions of $\mathfrak{p}$-adic fields. Inside one algebraic closure of a $\mathfrak{p}$-adic field K, there is only one unramified quadratic extension of K. This extension is given by $K(\sqrt{u})$, where u is some specific chosen unit of $\mathfrak{o}_K$. If K is nondyadic, that is when the residue field of K has odd characteristic, then u can be chosen to be any nonsquare unit in $\mathfrak{o}_K$. When K is dyadic, then u is chosen from one specific square class of units. In the special case $K = \mathbb{Q}_2$, we can choose δ to be 5.

3.2 Quaternion Algebras over $\mathfrak{p}$-adic fields

Let F be a $\mathfrak{p}$-adic field, with ring of integers $\mathfrak{o}$, uniformizer π, $\mathfrak{p} = \pi\mathfrak{o}$ the unique maximal ideal and $\overline{F} = \mathfrak{o}/\mathfrak{p}$ the residue class field. We fix a valuation v on F.

Let H be a quaternion division algebra over F. Define

$$w : H \to \mathbb{R}$$

by $w(x) = v(\mathrm{nr}(x))$. Note that $w(\pi) = v(\pi)^2$.

Lemma 3.6 *The function w is a nonarchimedean valuation on H*

Proof. We need to show that w satisfies the following two properties:

(a) $w(x) \geq 0$ for all $x \in H$, and $w(x) = 0$ if and only if $x = 0$;

(b) $w(xy) = w(x)w(y)$ for all $x, y \in H$;

(c) $w(x+y) \leq \max\{w(x), w(y)\}$ with equality when $w(x) \neq w(y)$.

Property (a) and (b) follow immediately from the definition of v and the multiplicative property of nr. For (c), let E be a quadratic field extension of F inside H. The restriction of nr on E is the norm $N_{E/F}$ of the extension E/F. Now $v \circ N_{E/F}$ is a nonarchimedean valuation on the $\mathfrak{p}$-adic field E. Thus w restricted to such a quadratic extension satisfies (c). So for $x, y \in H^\times$,

$$w(x+y)w(y)^{-1} = w(xy^{-1} - 1) \leq \max\{w(xy^{-1}), w(1)\}$$

with equality if $w(xy^{-1}) \neq w(1)$. Note that $w(1) = 1$ and that $w(xy^{-1}) = w(x)w(y)^{-1}$ from (b). Hence w satisfies (c).□

Corollary 3.7 *Let $\mathcal{O} = \{x \in H : w(x) \leq 1\}$ and $\mathcal{P} = \{x \in H : w(x) < 1\}$.*

(a) $\mathcal{O}$ is a ring and $\mathcal{P}$ is a two-sided ideal of $\mathcal{O}$. The unit group of $\mathcal{O}$ is precisely the set $\mathcal{O} \setminus \mathcal{P}$.

(b) $nr(\mathcal{O}) \subseteq \mathfrak{o}$ and $nr(\mathcal{P}) \subseteq \mathfrak{p}$.

(c) Let $z \in \mathcal{P}$ be such that $w(z)$ is maximal. Then $\mathcal{P} = z\mathcal{O} = \mathcal{O}z$.

(d) $\mathcal{P}^2 \subseteq \pi\mathcal{O} \subseteq \mathcal{P}$.

(e) The map $x + \mathcal{P} \longmapsto zx + \mathcal{P}^2$ is a $\overline{F}$-vector space isomorphism from $\mathcal{O}/\mathcal{P}$ to $\mathcal{P}/\mathcal{P}^2$.

Proof. Parts (a) and (b) are straightforward. For (c), if $y \in \mathcal{P}$, then $w(y) \leq w(z)$. Hence $w(z^{-1}y) = w(yz^{-1}) \leq 1$, which means that y is in $z\mathcal{O}$ and $\mathcal{O}z$.

For (d), it is clear that $\pi\mathcal{O} \subseteq \mathcal{P}$. Note that $w(\pi^{-1}z^2) = [v(\pi)^{-1}v(\mathrm{nr}(z))]^2 \leq 1$. So, $z^2 \in \pi\mathcal{O}$ and hence $\mathcal{P}^2 \subseteq \pi\mathcal{O}$.

For (e), the map $x + \mathcal{P} \longmapsto zx + \mathcal{P}^2$ is a $\overline{F}$-linear map. By (c), it is surjective. Suppose that $zx \in \mathcal{P}^2$. Then $x \in \mathcal{P}$ which shows that the map is injective. □

Proposition 3.8 *The quotient $\mathcal{O}/\mathcal{P}$ is a finite field.*

Proof. By part(a) of Corollary 3.7, $\mathcal{O}/\mathcal{P}$ is a division ring. We proceed to show that $\mathcal{O}/\mathcal{P}$ is a finite division ring. Then Wedderburn's Little Theorem says that every finite division ring is a field, whence the theorem.

For any $x \in H$, there exists $m \in \mathbb{Z}$ such that $\pi^m x \in \mathcal{O}$. It follows that $H = F\mathcal{O}$. We choose a basis $\{x_1, x_2, x_3, x_4\}$ of H such that $x_i \in \mathcal{O}$ for all i. Since H, equipped with the quadratic map 2nr, is a nondegenerate quadratic space over F, there exist $x_1^*, x_2^*, x_3^*, x_4^* \in H$ such that

$$B(x_i, x_j^*) = \delta_{ij} \quad \text{(Kronecker's delta)}$$

where B is the symmetric bilinear form associated to 2nr. The x_i^* are clearly linearly independent over F. If $x \in \mathcal{O}$ and $x = \sum_i a_i x_i^*$, then since $2\mathrm{nr}(y) \in 2\mathfrak{o}$ for all $y \in \mathcal{O}$, we have $a_i = B(x, x_i) \in \mathfrak{o}$ for all i. Thus

$$\sum_{i=1}^{4} \mathfrak{o}x_i \subseteq \mathcal{O} \subseteq \sum_{i=1}^{4} \mathfrak{o}x_i^*,$$

and $\mathcal{O}$ is a (necessarily) free $\mathfrak{o}$-module of rank 4. It follows that $\mathcal{O}/\pi\mathcal{O}$ is a 4-dimensional vector space over the finite field $\overline{F}$. So, $\mathcal{O}/\pi\mathcal{O}$ is a finite set. Since $\pi\mathcal{O} \subseteq \mathcal{P}$, $\mathcal{O}/\mathcal{P}$ is also a finite set.□

The $\mathfrak{p}$-adic field F has a unique unramified quadratic extension $K = F(\sqrt{u})$, where u is from a specific square class of units in $\mathfrak{o}$. Let $\overline{K}$ be the residue field of K. Then $\overline{K}$ can be regarded as a quadratic extension of $\overline{F}$. By Corollary 3.5, the norm group $N_{K/F}(K^\times)$ is a subgroup of index 2 in $F^\times$ which contains all the units in $\mathfrak{o}$, and the nontrivial element in the quotient group $F^\times/N_{K/F}(K^\times)$ is represented by a uniformizer π. Thus the quaternion algebra $\left(\frac{u,\pi}{F}\right)$ is a division algebra.

Theorem 3.9 *Up to isomorphism, $\left(\frac{u,\pi}{F}\right)$ is the only quaternion division algebra over F.*

Proof. Let H be a quaternion division algebra over F. The first step is to show that an unramified quadratic extension of F embeds in H. We have shown that $\mathcal{O}/\mathcal{P}$ is a finite

extension of $\overline{F}$. By Corollary 3.7(e), $\mathcal{O}/\mathcal{P}$ and $\mathcal{P}/\mathcal{P}^2$ have the same dimension as $\overline{F}$-vector spaces. Therefore $\dim_{\overline{F}}(\mathcal{O}/\mathcal{P}) > 1$, in particular, $\mathcal{O}/\mathcal{P} \neq \overline{F}$.

Now choose $\alpha \in \mathcal{O}$ such that $\mathcal{O}/\mathcal{P} = \overline{F}(\alpha + \mathcal{P})$. Then $\alpha \notin F$ and hence $K = F(\alpha)$ is a quadratic extension over F. Since $\overline{K}/\overline{F}$ is a nontrivial extension, therefore the residue degree f of K/F is at least 2. It then follows from the Local Fundamental Identity that f must be exactly 2 and the ramification index of K/F is 1. So, K/F is unramified, and hence there exists $i \in K$ such that $i^2 = u$.

The two square roots $\pm i$ of u give two embeddings of K into H. By the Skolem-Noether Theorem, there is a $j \in H^\times$ such that $-i = jij^{-1}$. Thus $\{1, i, j, ij\}$ is a basis of H (verify!). Since j^2 commutes with i, j^2 is in center of H and hence $j^2 \in F$. This implies that $\{1, i, j, ij\}$ is a standard basis of H.

Let $j^2 = \pi^m \epsilon$, where $\epsilon \in \mathfrak{o}^\times$. We may assume that $m = 0$ or 1. Since every ϵ in $\mathfrak{o}^\times$ is a norm of an element in K, $\left(\frac{u,\epsilon}{F}\right)$ splits. Thus $m = 1$, and there exists $a, b \in F$ such that $a^2 - ub^2 = \epsilon$. It remains to show that $H = \left(\frac{u,\pi}{F}\right)$. It suffices to show that H_0 has an orthogonal basis $\{e_1, e_2, e_3\}$ such that $\mathrm{nr}(e_1) = -u, \mathrm{nr}(e_2) = -\pi$ and $\mathrm{nr}(e_3) = \pi u$.

Since $H = \left(\frac{u,\pi\epsilon}{F}\right)$, H_0 has an orthogonal basis $\{f_1, f_2, f_3\}$ such that $\mathrm{nr}(f_1) = -u$, $\mathrm{nr}(f_2) = -\pi\epsilon$ and $\mathrm{nr}(f_3) = \pi\epsilon u$. Now, let $e_1 = f_1$, $e_2 = \epsilon^{-1}(af_2 + bf_3)$ and $e_3 = \epsilon^{-1}(ubf_2 + af_3)$. It is direct to check that $\{e_1, e_2, e_3\}$ is the desired orthogonal basis of H.□

Theorem 3.10 *Let L/F be a quadratic field extension. Then $\left(\frac{u,\pi}{F}\right)$ splits over L.*

Proof. If L is an unramified quadratic extension of F, then $L \cong F(\sqrt{u})$ and hence $\left(\frac{u,\pi}{L}\right)$ splits.

Now suppose that L/F is ramified. Let $K = F(\sqrt{u})$ and set $M = L(\sqrt{u})$. Then

$$[\overline{M} : \overline{F}] = [\overline{M} : \overline{L}][\overline{L} : \overline{F}] = [\overline{M} : \overline{L}]$$

since L/F is ramified. On the other hand,

$$[\overline{M} : \overline{F}] = [\overline{M} : \overline{K}][\overline{K} : \overline{F}] = 2[\overline{M} : \overline{K}].$$

So, $[\overline{M} : \overline{L}] = 2$ and M/L is unramified. Let ρ be a uniformizer for L such that $\pi = \rho^2 t$, where t is a unit of the ring of integers in L. Then

$$\left(\frac{u,\pi}{L}\right) = \left(\frac{u,\rho^2 t}{L}\right) = \left(\frac{u,t}{L}\right).$$

But t is a norm of an element in M since M/L is unramified. Thus $\left(\frac{u,t}{L}\right)$ splits.□

We can say a bit more when F is a nondyadic $\mathfrak{p}$-adic field. The following is a well known result in the theory of local fields.

Theorem 3.11 (Hensel's Lemma) *Let $f(x)$ be a monic polynomial in $\mathfrak{o}[x]$. Suppose that $f(x) \mod \mathfrak{p}$ admits a factorization $\overline{g}(x)\overline{h}(x)$, where $\overline{g}(x)$ and $\overline{h}(x)$ are relatively prime polynomials in $\overline{F}[x]$. Then $f(x)$ admits a factorization $g(x)h(x)$ in $\mathfrak{o}[x]$, where $g(x) \mod \mathfrak{p} = \overline{g}(x)$ and $h(x) \mod \mathfrak{p} = \overline{h}(x)$.*

Corollary 3.12 *Let F be a nondyadic $\mathfrak{p}$-adic field. Then $F^\times/F^{\times 2}$ is a group of order 4 whose elements are represented by $1, u, \pi$ and πu where u is a nonsquare unit in $\mathfrak{o}$.*

Proof. By Hensel's Lemma, an element $c \in \mathfrak{o}^\times$ is a square if and only if c is a square modulo $\mathfrak{p}$. Since the residue field $\mathfrak{o}/\mathfrak{p}$ is a finite field of odd characteristic, it has exactly two square classes. So, $\mathfrak{o}^\times$ also has exactly two square classes. The Corollary now follows immediately.□

Theorem 3.13 *Let F be a nondyadic $\mathfrak{p}$-adic field. Let $H = \left(\frac{a,b}{F}\right)$, where $a, b \in \mathfrak{o}$.*

(a) If $a, b \in \mathfrak{o}^\times$, then H splits.

(b) If $a \in \mathfrak{o}^\times$ and $b \in \mathfrak{p} \setminus \mathfrak{p}^2$, then H splits if and only if a is a square.

(c) If $a, b \in \mathfrak{p} \setminus \mathfrak{p}^2$, then H splits if and only if $-a^{-1}b$ is a square.

Proof. (a) We may assume that $a = u$. Then b is a norm of an element in $F(\sqrt{a})$. Hence H splits.

(b) Once again, we may assume that $a = u$, which is not a square mod $\mathfrak{p}$. Since $F(\sqrt{u})/F$ is unramified, b is not a norm from $F(\sqrt{u})$. Therefore, H does not split in this case.

(c) Note that $\left(\frac{a,b}{F}\right) = \left(\frac{a,-a^{-1}b}{F}\right)$ and $-a^{-1}b$ is a unit in $\mathfrak{o}$. Therefore, $\left(\frac{a,b}{F}\right)$ splits if and only if $-a^{-1}b$ is a square, by part (b).□

4 Quaternion Algebras over Number Fields

In this section, F is a number field and $\mathfrak{o}$ is the ring of integers of F.

4.1 Local to Global

Let K be a finite extension of F. The restriction of a valuation on K to F is a valuation on F. For every place v of F, there are only finitely many places w of K such that the restriction of any valuation in w on F is a valuation in v. Those w are said to be lying above v and we write $w \mid v$. Moreover,

$$(\sharp) \qquad K \otimes_F F_v \cong \prod_{w|v} K_w.$$

This decomposition gives

$$N_{K/F}(a) = \prod_{w|v} N_{w/v}(a)$$

and

$$T_{K/F}(a) = \sum_{w|v} T_{w/v}(a).$$

Here $N_{w/v}$ and $T_{w/v}$ are the norm and the trace of the extension K_w/F_v. Recall that the valuation on K_w that extends v on F_v is defined by $w(x) = v(N_{w/v}(x))^{1/[K_w:F_v]}$. It also follows from ($\sharp$) that

$$\sum_{w|v}[K_w : F_v] = [K : F].$$

If e_w and f_w are the ramification index and residue degree of K_w/F_v, then the Local Fundamental Identity implies:

$$\sum_{w|v} e_w f_w = [K : F] \quad \text{(Fundamental Identity)}.$$

We now mention some results from class field theory. An element $a \in F$ is called a global norm (of the extension K/F) if $a \in N_{K/F}(K)$. For any $v \in \Omega_F$, a is called a local norm at v if $a \in N_{w/v}(K_w)$ for all $w \mid v$.

Theorem 4.1 (Hasse's Norm Theorem) *Let K/F be a cyclic extension of number fields, and let $a \in F$. Then a is a global norm if and only if it is a local norm at every $v \in \Omega_F$.*

We shall be interested in the special case when K/F is a quadratic extension. In this case, $K = F(\sqrt{\delta})$ for some $\delta \notin F^2$. An element $a \in F$ is a global norm if the diophantine equation $x^2 - \delta y^2 = a$ has a solution over F. For every $v \in \Omega_F$, by ($\sharp$) there are either one or two places of w lying above v. The latter occurs exactly when δ is a square in F_v and we say that v splits in K. If there is only one w lying above v, then K_w/F_v is a quadratic extension and a is a local norm at v if and only if $x^2 - \delta y^2 = a$ has a solution over F_v. If there are two places of K lying above v, then every $a \in F$ is a local norm at v. At the same time, the equation $x^2 - \delta y^2 = a$ always has a solution over F_v. Hence Hasse's Norm Theorem in the special case can be rephrased as: $x^2 - \delta y^2 = a$ has a solution over F if and only if $x^2 - \delta y^2 = a$ has a solution over F_v for every $v \in \Omega_F$.

Theorem 4.2 (Global Square Theorem) *Let δ be an element in a number field F. Then δ is a square in F if and only if δ is a square in F_v for almost all $v \in \Omega_F$.*

Recall that a quadratic space (V, Q) is called isotropic if there exists a nonzero vector v in V such that $Q(x) = 0$; such a v is called an isotropic vector. The space V is called isotropic if it has an isotropic vector, and is called nondegenerate if it does not have any nonzero vector that is orthogonal to all vectors in V. If v is a place of F, then V_v denotes the quadratic space $F_v \otimes_F V$ with quadratic form $Q_v(a \otimes x) = a^2 Q(x)$ for all $a \in F_v$ and $x \in V$. We often abuse the notation and use the same Q, instead of Q_v, to denote the quadratic form on V_v.

The next theorem is one of the most important theorem in the algebraic theory of quadratic forms.

Theorem 4.3 (Hasse-Minkowski Theorem)

(a) Let V be a nondegenerate quadratic space over a number field F. Then V is isotropic if and only if V_v is isotropic for all places v of F.

(b) Let V and W be nondegenerate quadratic spaces over a number field F. Then V and W are isometric if and only if V_v and W_v are isometric for all places v of F.

Let us look at part (a) of the Hasse-Minkowski Theorem. We may assume, by scaling the quadratic form on V suitably, that there exists $v_1 \in V$ with $Q(v_1) = 1$. We can extend v_1 to an orthogonal basis $\{v_1, \ldots, v_n\}$ of V. If $n = 2$, then there exists a $\delta \in F^\times$ such that every $Q(v)$ is of the form $x^2 + \delta y^2$ with $x, y \in F$. So, V is isotropic if and only if $-\delta$ is a square in F. Thus part (a) in this case is just the Global Square Theorem. If $n = 3$, then the corresponding quadratic form on V is of the form $x^2 + \delta y^2 + \gamma z^2$. We may assume that $-\delta$ is not a square in F. Then V is isotropic if and only if γ is a norm from the quadratic extension $F(\sqrt{-\delta})$, and part (a) in this case is just Hasse's Norm Theorem. The rest of the proof for part (a) is an (nontrivial) induction on the dimension of V; see page 187 in O'Meara's book.

For part (b), we first observe that the case $n = 1$ the theorem is equivalent to the Global Square Theorem. Suppose that $n > 1$. It suffices to look at the "if" part of the statement. We may assume that V has a vector x such that $Q(x) = 1$. Then $V \cong \langle 1 \rangle \perp V'$ for some subspace V' of dimension $n-1$. At each v, there is a vector $w_v \in W_v$ such that $Q(w_v) = 1$, since $W_v \cong V_v$. This means that the space $\langle -1 \rangle \perp W_v$ is isotropic for every v and, by part (a), the space $\langle -1 \rangle \perp W$ is isotropic. Thus there exists a vector $w \in W$ with $Q(w) = 1$. So, $W \cong \langle 1 \rangle \perp W'$ for some subspace W' of dimension $n - 1$. Now, by Witt's Cancellation Theorem, $V'_v \cong W'_v$ for all places v. It follows from an induction on the dimension that $V' \cong W'$, whence $V \cong W$.

4.2 Classification

Let v be a place of F. For any $a, b \in F_v^\times$, define the *Hilbert Symbol*

$$(a, b)_v = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } F_v; \\ -1 & \text{otherwise.} \end{cases}$$

By Theorem 1.13, $(a, b)_v = 1$ if and only if the quaternion algebra $\left(\frac{a,b}{F_v}\right)$ splits. Now, suppose that a and b are in $F^\times$. For almost all finite places v, a and b are units of $\mathfrak{o}_v$. Therefore, by Theorem 3.13, $(a, b)_v = 1$ for almost all v.

Theorem 4.4 (Hilbert's Reciprocity Law) *Let $a, b \in F^\times$. Then*

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

where the product is taken over all places of F.

Let H be a quaternion algebra over F. For any place v of F, let H_v denote the quaternion algebra $F_v \otimes_F H$ over F_v. If v is a complex place, then H_v necessarily splits. However, if v is a real place or a finite place, then H_v either splits or is isomorphic to the unique quaternion division algebra over F_v. Note that H_v splits for almost all places v.

Theorem 4.5 *Let H be a quaternion algebra over a number field F. Then H splits over F if and only if H_v splits over F_v for all places v of F.*

Proof. By Theorem 1.13, H splits over F if and only if H_0 is isotropic. The theorem now follows immediately from the Hasse-Minkowski Theorem.□

Definition 4.6 Let H be a quaternion algebra over a number field F. Then H is said to be *ramified* at a place v if H_v is a division algebra. Otherwise, H splits at v. The set of places at which H is ramified is denoted by $\mathrm{Ram}(H)$.

Proposition 4.7 *The set $Ram(H)$ is a finite set containing even number of places.*

Proof. This is a consequence of Hilbert's Reciprocity Law.□

Theorem 4.8 *Let H and H' be quaternion algebras over a number field F. Then $H \cong H'$ if and only if $Ram(H) = Ram(H')$.*

Proof. By Theorem 2.8, H and H' are isomorphic if and only if H_0 and H'_0 are isometric as quadratic spaces. By the Hasse-Minkowski Theorem, H_0 and H'_0 are isometric if and only if $(H_0)_v$ and $(H'_0)_v$ are isometric for all places v, which is the same as saying that H_v and H'_v are isomorphic for all places v. But H_v and H'_v are isomorphic if and only if either they both split or they are both ramified. Thus H and H' are isomorphic if and only if they are ramified at the same set of places.□

5 Orders in Quaternion Algebras

5.1 Orders

Throughout this subsection, F is either a number field of a $\mathfrak{p}$-adic field. Its ring of integers $\mathfrak{o}$ is a Dedekind domain. In particular, F is the field of fractions of $\mathfrak{o}$, and $\mathfrak{o}$ is an integrally closed Noetherian ring in which every nonzero prime ideal is maximal.

Let I_F be the set of nonzero finitely generated $\mathfrak{o}$-submodule of F. The elements in I_F are called the fractional ideals of F. The nonzero ideals of $\mathfrak{o}$ are elements of I_F, and they are called the integral ideals of F. Let $\mathfrak{a}, \mathfrak{b}$ be two fractional ideals. Their product $\mathfrak{ab}$ is the $\mathfrak{o}$-module generated by the products ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. The inverse of $\mathfrak{a}$ is defined to be $\mathfrak{a}^{-1} = \{x \in F : x\mathfrak{a} \subseteq \mathfrak{o}\}$. It turns out that $\mathfrak{ab}$ and $\mathfrak{a}^{-1}$ are also fractional ideals. In fact, I_F is an abelian group under the multiplication of fraction ideals just defined. The identity element is $\mathfrak{o}$, and $\mathfrak{a}^{-1}$ is indeed the inverse of $\mathfrak{a}$, that is $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$. An important result about

Dedekind domain is that I_F is the free abelian group on the set of nonzero prime ideals of $\mathfrak{o}$. In other words, every fractional ideal $\mathfrak{a}$ has a unique prime ideal factorization

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t},$$

where each $\mathfrak{p}_i$ is a nonzero prime ideal of $\mathfrak{o}$ and each a_i is a nonzero integer.

Let P_F be the set of principal fractional ideals $\alpha\mathfrak{o}$, $\alpha \in F^\times$. Then P_F is a subgroup of I_F, and the quotient I_F/P_F is called the *ideal class group* of F. This group is a finite group for those fields F we are considering here. The order of this group is called the class number of F. When F is a $\mathfrak{p}$-adic field, its class number is always 1.

Definition 5.1 Let V be a finite dimensional vector space over F. An $\mathfrak{o}$-lattice in V is a finitely generated $\mathfrak{o}$-module contained in V. An $\mathfrak{o}$-lattice L in V is said to be *complete* if $FL = V$.

From now on, unless stated otherwise, every vector space is finite dimensional over F and every lattice in V is an $\mathfrak{o}$-lattice. Since $\mathfrak{o}$ is a Dedekind domain, every lattice L in a vector space V can be written as $L = \mathfrak{o}x_1 \oplus \cdots \oplus \mathfrak{o}x_{k-1} \oplus \mathfrak{a}x_k$ for some $x_1, \ldots, x_k \in V$ and a fractional ideal $\mathfrak{a}$. If L is complete, then $\{x_1, \ldots, x_k\}$ is necessarily a basis of V.

Theorem 5.2 (Invariant Factor Theorem) *Let L and M be two complete lattices in a vector space V over F. Then there is a basis $\{x_1, \ldots, x_n\}$ of V such that*

$$\begin{cases} L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_n x_n \\ M = \mathfrak{a}_1\mathfrak{r}_1 x_1 + \cdots + \mathfrak{a}_n\mathfrak{r}_n x_n \end{cases}$$

where $\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{r}_1, \ldots, \mathfrak{r}_n$ are fractional ideals of F with $\mathfrak{r}_1 \supseteq \mathfrak{r}_2 \supseteq \cdots \supseteq \mathfrak{r}_n$. The $\mathfrak{r}_i$ determined in this way are unique.

The fractional ideals $\mathfrak{r}_1, \ldots, \mathfrak{r}_n$ of the last theorem are called the *invariant factors of M in L*. It is clear that $M \subseteq L$ if and only if all the $\mathfrak{r}_i$ are integral ideals.

Corollary 5.3 *Let L be a complete lattice in a vector space V and M be an $\mathfrak{o}$-module contained in V. Then M is a complete lattice if and only if there exists nonzero $a \in \mathfrak{o}$ such that $aL \subseteq M \subseteq a^{-1}L$.*

Proof. Suppose that there is an $a \in \mathfrak{o}$ such that $aL \subseteq M \subseteq a^{-1}L$. Since $a^{-1}L$ is a finitely generated $\mathfrak{o}$-module and $\mathfrak{o}$ is Noetherian, M is also finitely generated. Moreover, since $aL \subseteq M$, M contains a basis of V. Thus M is a complete lattice.

Conversely, suppose that M is a complete lattice. By the Invariant Factor Theorem, there exists nonzero $a \in \mathfrak{o}$ such that $aL \subseteq M$ and $aM \subseteq L$.□

Definition 5.4 Let H be a quaternion algebra over F. An $\mathfrak{o}$-*ideal* in H is a complete $\mathfrak{o}$-lattice in H. An *order* in H is an $\mathfrak{o}$-ideal which is also a ring. A *maximal order* is an order which is maximal with respect to inclusion.

Henceforth, H is always a quaternion algebra over F. We first demonstrate the existence of an order in H. Unless stated otherwise, an ideal in H is always an $\mathfrak{o}$-ideal. If I is an ideal in H, then the *left order* of I and the *right order* of I are defined respectively by

$$\mathcal{O}_\ell(I) = \{\alpha \in H : \alpha I \subseteq I\}, \qquad \mathcal{O}_r(I) = \{\alpha \in H : I\alpha \subseteq I\}.$$

Lemma 5.5 *If I is an ideal in H, then $\mathcal{O}_\ell(I)$ and $\mathcal{O}_r(I)$ are orders in H.*

Proof. We shall show only that $\mathcal{O}_\ell(I)$ is an order; the argument for $\mathcal{O}_r(I)$ will be the same. Clearly, $\mathcal{O}_\ell(I)$ is a subring and an $\mathfrak{o}$-submodule of H.

Since I is an ideal in H, there exists a nonzero $s \in \mathfrak{o}$ such that $s \cdot 1 \in I$. Therefore, $\mathcal{O}_\ell(I)(s \cdot 1) \subseteq I$; whence $\mathcal{O}_\ell(I) \subseteq s^{-1}I$. This shows that $\mathcal{O}_\ell(I)$ is finitely generated as an $\mathfrak{o}$-module. So, $\mathcal{O}_\ell(I)$ is a lattice.

Now, for any $y \in H$, yI is a lattice in H. Therefore, there exists a nonzero $a \in \mathfrak{o}$ such that $ayI \subseteq I$. Then $ay \in \mathcal{O}_\ell(I)$ and hence $F\mathcal{O}_\ell(I) = H$. This complete the proof that $\mathcal{O}_\ell(I)$ is an order in H.□

Let $\mathcal{O}$ be an order in H. Since $\mathcal{O}$ is a finitely generated $\mathfrak{o}$-module and $\mathfrak{o}$ is Noetherian, every element of $\mathcal{O}$ is integral over $\mathfrak{o}$. More generally, suppose $\alpha \in H$ is integral over $\mathfrak{o}$. Since $\alpha^2 - \mathrm{tr}(\alpha)\alpha + \mathrm{nr}(\alpha) = 0$, it follows that $\mathrm{tr}(\alpha)$ and $\mathrm{nr}(\alpha)$ are in $\mathfrak{o}$.

Lemma 5.6 *Let $\mathcal{O}$ be a subring of H. Then $\mathcal{O}$ is an order in H if and only if $\mathcal{O}$ contains $\mathfrak{o}$, $F\mathcal{O} = H$ and $\mathcal{O}$ is integral over $\mathfrak{o}$.*

Proof. It is clear that if $\mathcal{O}$ is an order in H, then $\mathcal{O}$ has all the properties stated in the lemma.

For the converse, let $\{x_1, x_2, x_3, x_4\}$ be a basis of H such that $x_i \in \mathcal{O}$ for all i. It can be checked readily that H, equipped with the (reduced) trace tr as the symmetric bilinear form, is a nondegenerate quadratic space. Therefore, $d = \det(\mathrm{tr}(x_i x_j)) \neq 0$. Let L be the ideal spanned by the x_i. Then $L \subseteq \mathcal{O}$. Suppose that $\alpha \in \mathcal{O}$ so that

$$\alpha = \sum_{i=1}^{4} b_i x_i, \quad b_i \in F \text{ for all } i.$$

For each j, $\alpha x_j \in \mathcal{O}$ and so

$$\mathrm{tr}(\alpha x_j) = \sum_{i=1}^{4} b_i \mathrm{tr}(x_i x_j) \in \mathfrak{o}.$$

Thus $b_i \in d^{-1}\mathfrak{o}$ and $\mathcal{O} \subseteq d^{-1}L$. So, $\mathcal{O}$ is a finitely generated $\mathfrak{o}$-module which implies that $\mathcal{O}$ is an order.□

Corollary 5.7 *Every order in H is contained in a maximal order.*

Proof. Apply Zorn's Lemma and the characterization of orders given in the last lemma.□

The set of all elements in H that are integral over $\mathfrak{o}$ is not necessarily an order. For example, let $H = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ with standard basis $\{1, i, j, ij\}$. Then $\alpha = i$ and $\beta = (3i + 4j)/5$ are integral over $\mathbb{Z}$, but neither $\alpha\beta$ nor $\alpha + \beta$ is integral over $\mathbb{Z}$.

If $\mathcal{O}$ is an order in H and $\alpha \in H^\times$, then $\alpha\mathcal{O}\alpha^{-1}$ is also an order in H. So, the conjugate of a maximal order in H is also a maximal order. However, there could be more than one conjugacy classes of maximal orders in a quaternion algebra.

5.2 Localizations I

In this subsection, F is a number field and $\mathfrak{o}$ is the ring of integers in F. The symbol $\mathfrak{p}$ always denote a finite place of F or its associated prime ideal of $\mathfrak{o}$. For any $\mathfrak{p} \in \Omega_f$, let $\mathfrak{o}(\mathfrak{p})$ be the localization of $\mathfrak{o}$ with respect to the multiplicative set $\mathfrak{o} \setminus \mathfrak{p}$. In other words,

$$\mathfrak{o}(\mathfrak{p}) = \{a/b \in F : a \in \mathfrak{o}, b \in \mathfrak{o} \setminus \mathfrak{p}\}.$$

It is a local ring with maximal ideal

$$\tilde{\mathfrak{p}} = \{a/b \in F : a \in \mathfrak{p}, b \in \mathfrak{o} \setminus \mathfrak{p}\}.$$

Let x be an nonzero element in F. The exponent of $\mathfrak{p}$ appearing in the prime ideal factorization of the fractional ideal $x\mathfrak{o}$ is denote by $\mathrm{ord}_{\mathfrak{p}}(x)$. It is our convention that $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$. We claim that

$$\mathfrak{o}(\mathfrak{p}) = \{\alpha \in F : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0\}$$

and so

$$\tilde{\mathfrak{p}} = \{\alpha \in F : \mathrm{ord}_{\mathfrak{p}}(\alpha) > 0\}.$$

It is clear that $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$ for all $\alpha \in \mathfrak{o}(\mathfrak{p})$. Conversely, suppose that $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0$ and we can write $\alpha = a/b$, where $a, b \in \mathfrak{o}$. Then $\mathrm{ord}_{\mathfrak{p}}(a) \geq \mathrm{ord}_{\mathfrak{p}}(b)$. Suppose that $\mathrm{ord}_{\mathfrak{p}}(b) = n$, or equivalently, $b\mathfrak{o} = \mathfrak{p}^n\mathfrak{b}$ for some integral ideal $\mathfrak{b}$. Let $\mathfrak{a}$ be an integral ideal belongs to the ideal class containing $\mathfrak{p}^{-1}$. So, $\mathfrak{a}\mathfrak{p}$ is a principal ideal $t\mathfrak{o}$ for some $t \in \mathfrak{o}$.

If $\mathfrak{p} \nmid \mathfrak{a}$, then $\mathfrak{a} \not\subseteq \mathfrak{p}$. Then there exists $x \in \mathfrak{a}$ but $x \notin \mathfrak{p}$. Therefore, $x\mathfrak{o} = \mathfrak{a}\mathfrak{c}$, where $\mathfrak{p} \nmid \mathfrak{c}$. This implies

$$x^n b\mathfrak{o} = (\mathfrak{a}\mathfrak{p})^n\mathfrak{c}\mathfrak{b} = t^n\mathfrak{c}\mathfrak{b}.$$

Set $b' := x^n b/t^n$, which is an element in $\mathfrak{o} \setminus \mathfrak{p}$. Using the same argument we can show that the element $a' := x^n a/t^n$ is in $\mathfrak{o}$. Then $\alpha = a/b = a'/b' \in \mathfrak{o}(\mathfrak{p})$.

If $\mathfrak{p} \mid \mathfrak{a}$, then $\mathfrak{a} \subseteq \mathfrak{p}$. Choose an integral ideal $\mathfrak{i}$ such that $\mathfrak{i}\mathfrak{a}$ is principal generated by $\delta \in \mathfrak{o}$. Then $\mathfrak{i}\mathfrak{a} \not\subseteq \delta\mathfrak{p}$. Fix an $\epsilon \in \mathfrak{i}$ such that $\epsilon\mathfrak{a} \not\subseteq \delta\mathfrak{p}$ and set $\gamma = \epsilon/\delta$. Then $\gamma\mathfrak{a} \subseteq \mathfrak{o}$ and $\gamma\mathfrak{a} \not\subseteq \mathfrak{p}$. So, $\gamma\mathfrak{a}$ is an integral ideal in the ideal class containing $\mathfrak{p}^{-1}$ and $\mathfrak{p} \nmid \gamma\mathfrak{a}$. We can then replace $\mathfrak{a}$ by $\gamma\mathfrak{a}$ in the last paragraph.

Let I be a nonzero ideal of $\mathfrak{o}(\mathfrak{p})$. Among all the elements in I, choose one, say x, such that $\mathrm{ord}_{\mathfrak{p}}(x)$ is the smallest. For any $a \in I$, $\mathrm{ord}_{\mathfrak{p}}(a) \geq \mathrm{ord}_{\mathfrak{p}}(x)$, which implies that $\mathrm{ord}_{\mathfrak{p}}(ax^{-1}) \geq 0$, that is $ax^{-1} \in \mathfrak{o}(\mathfrak{p})$. Thus, $a \in x\mathfrak{o}(\mathfrak{p})$ and hence $I = x\mathfrak{o}(\mathfrak{p})$. This shows

that $\mathfrak{o}(\mathfrak{p})$ is a PID and its ideals are $\pi^n\mathfrak{o}(\mathfrak{p}) = \tilde{\mathfrak{p}}^n$, $n \geq 0$. The rings $\mathfrak{o}(\mathfrak{p})$ are subrings of F and $\mathfrak{o}$ can be recovered from them as

$$\mathfrak{o} = \bigcap_{\mathfrak{p} \in \Omega_f} \mathfrak{o}(\mathfrak{p}).$$

Lemma 5.8 *Let V be a finite-dimensional vector space over F and let L be an $\mathfrak{o}$-lattice in V. Then*

$$L = \bigcap_{\mathfrak{p} \in \Omega_f} \mathfrak{o}(p)L.$$

Proof. It is clear that L is contained in the intersection. For the converse, let $\{x_1, \ldots, x_k\}$ be a generating set for L as an $\mathfrak{o}$-module; thus it is also a generating set for $\mathfrak{o}(\mathfrak{p})L$ as an $\mathfrak{o}(\mathfrak{p})$-module for each $\mathfrak{p}$. Suppose that x is in the intersection. Let

$$J = \{y \in \mathfrak{o} : yx \in L\}.$$

Then J is an integral ideal of $\mathfrak{o}$. Fix a $\mathfrak{p}$ in Ω_f. We can write $x = \sum_{i=1}^k a_i x_i$ with $a_i = b_i/c_i$, where $b_i, c_i \in \mathfrak{o}$ and $c_i \notin \mathfrak{p}$ for all i. Let $c = c_1 \cdots c_k$ so that $c \notin \mathfrak{p}$. However, $c \in J$. Thus J is an integral ideal of $\mathfrak{o}$ which does not lie in any nonzero prime ideal of $\mathfrak{o}$. This shows that $J = \mathfrak{o}$. Thus $1 \in J$ and $x \in L$.□

This result will be applied to the case when V is a quaternion algebra H over F and L is an $\mathfrak{o}$-ideal in H.

Lemma 5.9 *Let I be an $\mathfrak{o}$-ideal in an quaternion algebra H over F. For each prime ideal $\mathfrak{p} \in \Omega_f$, let $I(\mathfrak{p})$ be an $\mathfrak{o}(\mathfrak{p})$-ideal in H such that $I(\mathfrak{p}) = \mathfrak{o}(\mathfrak{p})I$ for almost all $\mathfrak{p}$. Then*

$$J = \bigcap_{\mathfrak{p} \in \Omega_f} I(\mathfrak{p})$$

is an $\mathfrak{o}$-ideal in H such that $\mathfrak{o}(\mathfrak{p})J = I(\mathfrak{p})$ for all $\mathfrak{p}$.

Proof. Let $\{x_1, x_2, x_3, x_4\}$ be a basis of H in I, and let L be the $\mathfrak{o}$-ideal $\mathfrak{o}x_1 + \cdots + \mathfrak{o}x_4$. Then $L \subseteq I$, and there exists an nonzero $r \in \mathfrak{o}$ such that $rI \subseteq L$. For almost all $\mathfrak{p}$, r is a unit in $\mathfrak{o}(\mathfrak{p})$. Therefore, for almost all $\mathfrak{p}$,

$$\mathfrak{o}(\mathfrak{p})L = \mathfrak{o}(\mathfrak{p})I = I(\mathfrak{p}).$$

As a result, we can find an nonzero $a \in \mathfrak{o}$ such that

$$aI(\mathfrak{p}) \subseteq \mathfrak{o}(\mathfrak{p})L \subseteq a^{-1}I(\mathfrak{p}) \quad \text{for all } \mathfrak{p}.$$

Then

$$J = \bigcap_{\mathfrak{p} \in \Omega_f} I(\mathfrak{p}) \subseteq a^{-1} \bigcap_{\mathfrak{p} \in \Omega_f} \mathfrak{o}(\mathfrak{p})L = a^{-1}L$$

by Lemma 5.8. Thus J is an $\mathfrak{o}$-lattice in H. By the same token, $aL \subseteq J$; thus J is an $\mathfrak{o}$-ideal in H.

Now, for each $\mathfrak{p} \in \Omega_f$, $\mathfrak{o}(\mathfrak{p})J \subseteq \mathfrak{o}(\mathfrak{p})I(\mathfrak{p}) = I(\mathfrak{p})$. For the reverse inclusion, let $j_1, \ldots, j_k$ be a generating set for J as $\mathfrak{o}$-module. Let $x \in I(\mathfrak{p})$ so that $x = \sum_i a_i j_i$ with $a_i \in F$. Choose a nonzero $s_1 \in \mathfrak{o}$ so that $s_1 a_1 \in \mathfrak{o}$. Suppose that $s_1\mathfrak{o}$ has the following prime ideal factorization

$$s_1\mathfrak{o} = \mathfrak{p}^{n_0}\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_t^{n_t}$$

where $n_i \geq 1$ for $0 \leq i \leq t$. By the Chinese Remainder Theorem, there exists $d_1 \in \mathfrak{o}$ such that

$$d_1 \equiv \begin{cases} s_1 a_1 + s_1 & \mod \mathfrak{p}^{n_0+1}, \\ s_1 & \mod \mathfrak{q}_i^{n_i+1} \quad \text{for } 1 \leq i \leq t. \end{cases}$$

Then $b_1 = d_1/s_1$ is such that $b_1 - a_1 \in \mathfrak{o}(\mathfrak{p})$ and $b_1 \in \mathfrak{o}(\mathfrak{q})$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$. Repeat the same for each a_i to obtain a b_i, and let $y = \sum b_i j_i$. Then $y \in \mathfrak{o}(\mathfrak{q})J \subseteq I(\mathfrak{q})$ for all $\mathfrak{q} \neq \mathfrak{p}$. Also, $y - x = \sum(b_i - a_i)j_i \in \mathfrak{o}(\mathfrak{p})J \subseteq I(\mathfrak{p})$. Thus $y \in I(\mathfrak{p})$ and so $y \in J$. Hence $x = y - (y - x) \in \mathfrak{o}(\mathfrak{p})J$.□

Note that if $\mathcal{O}$ is an $\mathfrak{o}$-order in H, then $\mathfrak{o}(\mathfrak{p})\mathcal{O}$ is an $\mathfrak{o}(\mathfrak{p})$-order in H and the above lemma holds with "ideals" replaced by "orders".

Lemma 5.10 *Let $\mathcal{O}$ be an $\mathfrak{o}$-order in a quaternion algebra H over F. Then $\mathcal{O}$ is a maximal $\mathfrak{o}$-order if and only if $\mathfrak{o}(\mathfrak{p})\mathcal{O}$ is a maximal $\mathfrak{o}(\mathfrak{p})$-order for all $\mathfrak{p} \in \Omega_f$.*

Proof. Suppose that $\mathcal{O}$ is maximal but $\mathfrak{o}(\mathfrak{p})\mathcal{O} \subseteq \Lambda(\mathfrak{p})$ for some $\mathfrak{o}(\mathfrak{p})$-order $\Lambda(\mathfrak{p})$. Define an order $\mathcal{O}'$ by

$$\mathfrak{o}(\mathfrak{q})\mathcal{O}' = \begin{cases} \mathfrak{o}(\mathfrak{q})\mathcal{O} & \text{if } \mathfrak{q} \neq \mathfrak{p}; \\ \Lambda(\mathfrak{p}) & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

Then $\mathcal{O} \subseteq \mathcal{O}'$; so $\mathcal{O} = \mathcal{O}'$ and hence $\mathfrak{o}(\mathfrak{p})\mathcal{O} = \Lambda(\mathfrak{p})$.

Conversely, suppose that each $\mathfrak{o}(\mathfrak{p})\mathcal{O}$ is maximal and $\mathcal{O}$ is contained in a maximal $\mathfrak{o}$-order $\mathcal{O}'$. Then clearly $\mathfrak{o}(\mathfrak{p})\mathcal{O} \subseteq \mathfrak{o}(\mathfrak{p})\mathcal{O}'$ for all $\mathfrak{p}$. By maximality, we have

$$\mathfrak{o}(\mathfrak{p})\mathcal{O} = \mathfrak{o}(\mathfrak{p})\mathcal{O}' \quad \text{for all } \mathfrak{p}.$$

The result then follows from Lemma 5.8.□

In later discussion, we will identify $\mathfrak{o}(\mathfrak{p})\mathcal{O}$ with $\mathfrak{o}(\mathfrak{p}) \otimes_{\mathfrak{o}} \mathcal{O}$.

5.3 Localizations II

In this subsection, we shall interpret the local-global results obtained in the last subsection in the context of ideals and orders over the $\mathfrak{p}$-adics. If H is a quaternion algebra over F, then $H_{\mathfrak{p}}$ denotes the quaternion algebra $F_{\mathfrak{p}} \otimes_F H$. For any lattice L in H, $L_{\mathfrak{p}}$ denotes the $\mathfrak{o}_{\mathfrak{p}}$-lattice $\mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} L$ in $H_{\mathfrak{p}}$. If $\mathcal{O}$ is an order in H, then $\mathcal{O}_{\mathfrak{p}}$ is an $\mathfrak{o}_{\mathfrak{p}}$-order in $H_{\mathfrak{p}}$. Note that $\mathcal{O}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} \mathcal{O} = \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}(\mathfrak{p})} (\mathfrak{o}(\mathfrak{p})\mathcal{O})$.

Lemma 5.11 *There is a bijection between $\mathfrak{o}(\mathfrak{p})$-ideals (resp. orders) in a quaternion algebra H over F and the $\mathfrak{o}_\mathfrak{p}$-ideals (resp. orders) in the quaternion algebra $H_\mathfrak{p}$ over $F_\mathfrak{p}$ given by the map*

$$I \longmapsto \mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}(\mathfrak{p})} I$$

which has the inverse $J \mapsto J \cap H$.

Proof. Since $\mathfrak{o}(\mathfrak{p})$ is a PID, I is free as an $\mathfrak{o}(\mathfrak{p})$-module. Let $\{x_1, x_2, x_3, x_4\}$ be a basis of I over $\mathfrak{o}(\mathfrak{p})$. Then in $F_\mathfrak{p} \otimes_F H$, $(\mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}(\mathfrak{p})} I) \cap H$ consists of the $\mathfrak{o}_\mathfrak{p} \cap F = \mathfrak{o}(\mathfrak{p})$ linearly combinations of the x_i. Thus $(\mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}(\mathfrak{p})} I) \cap H = I$.

Now, suppose that J is an $\mathfrak{o}_\mathfrak{p}$-ideal in $H_\mathfrak{p}$ and that $\{y_1, y_2, y_3, y_4\}$ is a basis of J over $\mathfrak{o}_\mathfrak{p}$. Let $\{z_1, z_2, z_3, z_4\}$ be a basis of H over F so that $z_i = \sum_j b_{ij} y_j$ for all i. Then $B = (b_{ij})$ is an invertible matrix in $M_4(F_\mathfrak{p})$. Since F is dense in $F_\mathfrak{p}$, we can choose $c_{ij} \in F$ such that the entries of $C = (c_{ij})$ is close enough to those of B^{-1} to make CB to be a unit in $M_4(\mathfrak{o}_\mathfrak{p})$.

Now let $z_i' = \sum_j c_{ij} z_j = \sum_{j,k} c_{ij} b_{jk} y_k$. Then $\{z_1', z_2', z_3', z_4'\}$ is a basis of J over $\mathfrak{o}_\mathfrak{p}$, which is also a basis of H over F. Thus $J \cap H$ consists of the $\mathfrak{o}_\mathfrak{p} \cap F = \mathfrak{o}(\mathfrak{p})$ linear combinations of the z_i', and so is an $\mathfrak{o}(\mathfrak{p})$-ideal in H such that $\mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}(\mathfrak{p})} (J \cap H) = J$.□

Fix an $\mathfrak{o}$-ideal I in H. Let $\mathfrak{I}$ be the set of $\mathfrak{o}$-ideals in H, and let $\mathfrak{T}$ be the set of all sequences $(L_\mathfrak{p})$ such that $L_\mathfrak{p}$ is an $\mathfrak{o}_\mathfrak{p}$-ideal in $H_\mathfrak{p}$ for all $\mathfrak{p} \in \Omega_f$ and $L_\mathfrak{p} = I_\mathfrak{p}$ for almost all $\mathfrak{p}$.

Lemma 5.12 *The map $J \mapsto (J_\mathfrak{p})$ is a bijection from $\mathfrak{I}$ to $\mathfrak{T}$.*

Proof. If J is an $\mathfrak{o}$-ideal in H, then there exist nonzero $a, b \in F$ such that $aJ \subseteq I \subseteq bJ$. For almost all $\mathfrak{p}$, a and b are units in $\mathfrak{o}_\mathfrak{p}$ so that $J_\mathfrak{p} = I_\mathfrak{p}$ for almost all $\mathfrak{p}$.

Now, suppose that a sequence $(L_\mathfrak{p})$ in $\mathfrak{T}$ is given. Let $J(\mathfrak{p}) = H \cap L_\mathfrak{p}$, which is an $\mathfrak{o}(\mathfrak{p})$-ideal in H by Lemma 5.11. Furthermore, $J(\mathfrak{p}) = \mathfrak{o}(\mathfrak{p})I$ for almost all $\mathfrak{p}$. Then $J = \cap_\mathfrak{p} J(\mathfrak{p})$ is an $\mathfrak{o}$-ideal in H, and $J_\mathfrak{p} = L_\mathfrak{p}$ for all $\mathfrak{p}$. Thus the map $J \mapsto (J_\mathfrak{p})$ is surjective. Now if ideals J and J' have the same image under this map, then $\mathfrak{o}(\mathfrak{p})J = \mathfrak{o}(\mathfrak{p})J'$ for all $\mathfrak{p}$. Then, by Lemma 5.8, $J = J'$ and the map is injective.□

Corollary 5.13 *Let $\mathcal{O}$ be an $\mathfrak{o}$-order in the quaternion algebra H over F. Then $\mathcal{O}$ is maximal if and only if $\mathcal{O}_\mathfrak{p}$ are maximal $\mathfrak{o}_\mathfrak{p}$-orders in $H_\mathfrak{p}$ for all $\mathfrak{p} \in \Omega_f$.*

Proof. Exercise.□

5.4 Discriminants

In this subsection, F is the field of fractions of a Dedekind domain $\mathfrak{o}$, and H is a quaternion algebra over F.

Definition 5.14 Let $\mathcal{O}$ be an $\mathfrak{o}$-order in H. The *discriminant* of $\mathcal{O}$, denoted $d(\mathcal{O})$, is the fractional ideal of $\mathfrak{o}$ generated by the elements $\det(\mathrm{tr}(x_i x_j))$, where $x_1, x_2, x_3, x_4 \in \mathcal{O}$.

Since $\mathcal{O}$ is an $\mathfrak{o}$-order, it must contain a basis of H over F. Thus $d(\mathcal{O})$ is nonzero (recall that H together with $\mathrm{tr}(x^2)$ as the quadratic form is a nondegenerate quadratic space over F). Also, since every element in $\mathcal{O}$ is integral over $\mathfrak{o}$, $d(\mathcal{O})$ is an integral ideal.

Proposition 5.15 *If an $\mathfrak{o}$-order $\mathcal{O}$ in H is free with a basis $\{u_1, u_2, u_3, u_4\}$ over $\mathfrak{o}$, then $d(\mathcal{O})$ is the principal ideal generated by* $\det(tr(u_i u_j))$.

Proof. Let $x_1, x_2, x_3, x_4 \in \mathcal{O}$ so that $x_i = \sum_k a_{ik} u_k$ with $a_{ik} \in \mathfrak{o}$ for all i, k. Then

$$\det(\mathrm{tr}(x_i x_j)) = \det(a_{ik}) \det(\mathrm{tr}(u_i u_j)) \det(a_{ik})^t$$

and the result follows.□

Example 5.16 Let $\mathcal{O} = M_2(\mathfrak{o})$. It has a basis $\{E_{ij} : 1 \leq i, j \leq 2\}$, where E_{ij} is the matrix with 1 in the (i, j)-entry and 0 elsewhere. Using this basis one can easily compute $d(\mathcal{O}) = \mathfrak{o}$.

Example 5.17 Let H be the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\mathcal{O}$ be the $\mathbb{Z}$-order $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$. Then $d(\mathcal{O}) = 16\mathbb{Z}$. Let $\mathcal{O}'$ be the $\mathbb{Z}$- order $\mathcal{O} + \mathbb{Z}\alpha$, where $\alpha = (1 + i + j + ij)/2$. Then $\mathcal{O} \subseteq \mathcal{O}'$, and $d(\mathcal{O}') = 4\mathbb{Z}$.

Lemma 5.18 *Suppose that $\mathfrak{o}$ is a PID. If $\mathcal{O}_1$ and $\mathcal{O}_2$ are two $\mathfrak{o}$-orders in H with $\mathcal{O}_1 \subseteq \mathcal{O}_2$, then $d(\mathcal{O}_2) \mid d(\mathcal{O}_1)$, and $\mathcal{O}_1 = \mathcal{O}_2$ if and only if $d(\mathcal{O}_1) = d(\mathcal{O}_2)$.*

Proof. The first assertion is clear. For the second assertion, suppose that $d(\mathcal{O}_1) = d(\mathcal{O}_2)$. Let $\{u_1, u_2, u_3, u_4\}$ be an $\mathfrak{o}$-basis of $\mathcal{O}_1$, and let $\{v_1, v_2, v_3, v_4\}$ be $\mathfrak{o}$-basis of $\mathcal{O}_2$. Since $\mathcal{O}_1 \subseteq \mathcal{O}_2$, the matrix T that expresses the u_i in terms of the v_j has entries in $\mathfrak{o}$. But

$$\det(T)^2 \det(\mathrm{tr}(v_i v_j)) = \det(\mathrm{tr}(u_i u_j));$$

thus $T \in \mathrm{GL}_4(\mathfrak{o})$ and hence $\mathcal{O}_1 = \mathcal{O}_2$.□

Now, assume that F is a number field and $\mathfrak{o}$ is its ring of integers. Let $\mathcal{O}$ be an $\mathfrak{o}$-order in H. Then it can readily be shown that $d(\mathfrak{o}(\mathfrak{p})\mathcal{O}) = \mathfrak{o}(\mathfrak{p}) d(\mathcal{O})$ for all $\mathfrak{p} \in \Omega_f$. Each $\mathfrak{o}(\mathfrak{p})$ is a PID and we can compute $d(\mathfrak{o}(\mathfrak{p})\mathcal{O})$ using a basis of $\mathfrak{o}(\mathfrak{p})\mathcal{O}$. Then, by Lemma 5.8,

$$d(\mathcal{O}) = \bigcap_{\mathfrak{p} \in \Omega_f} d(\mathfrak{o}(\mathfrak{p})\mathcal{O}).$$

Theorem 5.19 *Suppose that F is a number field and $\mathfrak{o}$ is its ring of integers. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be $\mathfrak{o}$-orders in H with $\mathcal{O}_1 \subseteq \mathcal{O}_2$. Then $d(\mathcal{O}_2) \mid d(\mathcal{O}_1)$, and $d(\mathcal{O}_1) = d(\mathcal{O}_2)$ if and only if $\mathcal{O}_1 = \mathcal{O}_2$. In particular, $\mathcal{O}$ is maximal if $d(\mathcal{O}) = \mathfrak{o}$.*

Proof. The first assertion is clear. Suppose that $d(\mathcal{O}_1) = d(\mathcal{O}_2)$. Then $d(\mathfrak{o}(\mathfrak{p})\mathcal{O}_1) = d(\mathfrak{o}(\mathfrak{p})\mathcal{O}_2)$ for all $\mathfrak{p} \in \Omega_f$. It follows from Lemma 5.18 that $\mathfrak{o}(\mathfrak{p})\mathcal{O}_1 = \mathfrak{o}(\mathfrak{p})\mathcal{O}_2$ for all $\mathfrak{p}$, and so $\mathcal{O}_1 = \mathcal{O}_2$ by Lemma 5.8.□

Let us continue to assume that F is a number field and $\mathfrak{o}$ is its ring of integers. Suppose that

$$d(\mathcal{O}) = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

is the prime ideal factorization of $d(\mathcal{O})$. If $\mathfrak{p}$ is not one of those $\mathfrak{p}_i$, then $d(\mathfrak{o}(\mathfrak{p})\mathcal{O}) = \mathfrak{o}(\mathfrak{p})d(\mathcal{O}) = \mathfrak{o}(\mathfrak{p})$. For $i = 1, \ldots, t$, $d(\mathfrak{o}(\mathfrak{p}_i)\mathcal{O}) = \mathfrak{p}_i^{n_i}\mathfrak{o}(\mathfrak{p}_i)$. Thus

$$d(\mathcal{O}) = \prod_{\mathfrak{p}\in\Omega_f} (d(\mathfrak{o}(\mathfrak{p})\mathcal{O}) \cap \mathfrak{o}).$$

Over the $\mathfrak{p}$-adics, one can show that $d(\mathcal{O}_\mathfrak{p}) = d(\mathcal{O})_\mathfrak{p}$ for all $\mathfrak{p}$. Since the unique prime ideal in $\mathfrak{o}_\mathfrak{p}$ is $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$, one can, with an abuse of notation, re-write the above product as

$$d(\mathcal{O}) = \prod_{\mathfrak{p}\in\Omega_f} d(\mathcal{O}_\mathfrak{p}).$$

5.5 Orders in $M_2(F)$

In this subsection, we discuss the special case when $H = M_2(F)$. Here F is the field of fractions of a Dedekind domain $\mathfrak{o}$. Let V be a 2-dimensional vector space over F. We fix a basis $\{e_1, e_2\}$ of V so that $M_2(F)$ is identified with $\mathrm{End}(V)$. The $\mathfrak{o}$-lattice $\mathfrak{o}e_1 + \mathfrak{o}e_2$ is denoted by L_0.

If L is a complete $\mathfrak{o}$-lattice in V, define

$$\mathrm{End}(L) = \{\sigma \in \mathrm{End}(V) : \sigma(L) \subseteq L\}.$$

In particular, $\mathrm{End}(L_0)$ is identified with the $\mathfrak{o}$-order $M_2(\mathfrak{o})$. It is clear that $\mathrm{End}(L)$ is a subring of $\mathrm{End}(V)$ for any L. Moreover, $\mathrm{End}(L) = \mathrm{End}(aL)$ for all $a \in F^\times$.

For any complete $\mathfrak{o}$-lattice L in V, there exists nonzero $a \in \mathfrak{o}$ such that $aL_0 \subseteq L \subseteq a^{-1}L_0$. It follows that

$$a^2\mathrm{End}(L_0) \subseteq \mathrm{End}(L) \subseteq a^{-2}\mathrm{End}(L_0).$$

Thus $\mathrm{End}(L)$ is an $\mathfrak{o}$-order in H.

Lemma 5.20 *$M_2(\mathfrak{o})$ is a maximal $\mathfrak{o}$-order in $M_2(F)$.*

Proof. This is clear because the discriminant of $M_2(\mathfrak{o})$ is $\mathfrak{o}$.□

Lemma 5.21 *Let $\mathcal{O}$ be an $\mathfrak{o}$-order in End(V). Then there exists a complete $\mathfrak{o}$-lattice L in V such that $\mathcal{O} \subseteq$ End(L).*

Proof. Let $L = \{\ell \in L_0 : \mathcal{O}\ell \subseteq L_0\}$. Then L is an $\mathfrak{o}$-submodule of L_0. In particular, L is finitely generated. Also, if $0 \neq a$ in $\mathfrak{o}$ such that $a\mathrm{End}(L_0) \subseteq \mathcal{O} \subseteq a^{-1}\mathrm{End}(L_0)$, then for all $\ell \in L_0$, we have

$$\mathcal{O}a\ell \subseteq \mathrm{End}(L_0)\ell \subseteq L_0.$$

Thus $aL_0 \subseteq L$ and L is a complete $\mathfrak{o}$-lattice in V.

Let $\alpha \in \mathcal{O}$. For any $\ell \in L$, $\mathcal{O}\alpha\ell \subseteq \mathcal{O}\ell \subseteq L_0$. Therefore, $\alpha\ell \subseteq L$ and $\mathcal{O} \subseteq \mathrm{End}(L)$.□

Corollary 5.22 *Suppose that $\mathfrak{o}$ is a PID. Then the maximal $\mathfrak{o}$-orders in $M_2(F)$ are precisely the orders End(L). Every maximal $\mathfrak{o}$-order in $M_2(F)$ is conjugate to $M_2(\mathfrak{o})$.*

Proof. Let $\mathcal{O}$ be a maximal $\mathfrak{o}$-order in $M_2(F)$. By Lemma 5.21, there exists a complete $\mathfrak{o}$-lattice L in V such that $\mathcal{O} = \mathrm{End}(L)$. Conversely, if L is a complete $\mathfrak{o}$-lattice in V, then $L = \mathfrak{o}f_1 + \mathfrak{o}f_2$ for some basis $\{f_1, f_2\}$ of V. Let $\sigma \in \mathrm{End}(V)$ defined by $\sigma(e_i) = f_i$ with $i = 1, 2$. Then $L = \sigma(L_0)$ and hence $\mathrm{End}(L) = \sigma\mathrm{End}(L_0)\sigma^{-1} = \sigma M_2(\mathfrak{o})\sigma^{-1}$. This shows that End$(L)$ is a maximal $\mathfrak{o}$-order, and that every maximal $\mathfrak{o}$-order in $M_2(F)$ is conjugate to $M_2(\mathfrak{o})$.□

When $\mathfrak{o}$ is not a PID, not every L is free as an $\mathfrak{o}$-module. However, since $\mathfrak{o}$ is a Dedekind domain, there exists a basis $\{x, y\}$ of V and a fractional ideal $\mathfrak{a}$ such that $L = \mathfrak{o}x + \mathfrak{a}y$. Thus End$(L)$ is a conjugate of

$$M_2(\mathfrak{o}, \mathfrak{a}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, d \in \mathfrak{o}, b \in \mathfrak{a}^{-1}, c \in \mathfrak{a} \right\}.$$

Now suppose that F is a $\mathfrak{p}$-adic field with ring of integers $\mathfrak{o}$. Let π be a uniformizer for F and let q be the size of the residue field $\mathfrak{o}/\mathfrak{p}$. Then for any integer $n \geq 0$, $[\mathfrak{o} : \mathfrak{p}^n] = q^n$.

Lemma 5.23 *Let $\mathcal{O}$ and $\mathcal{O}'$ be maximal $\mathfrak{o}$-orders in $M_2(F)$. Then*

$$\frac{\mathcal{O}}{\mathcal{O} \cap \mathcal{O}'} \cong \frac{\mathcal{O}'}{\mathcal{O} \cap \mathcal{O}'}$$

as $\mathfrak{o}$-modules.

Proof. Suppose that $\mathcal{O} = \mathrm{End}(L)$ and $\mathcal{O}' = \mathrm{End}(L')$, where L and L' are complete $\mathfrak{o}$-lattices in V. By the Invariant Factor Theorem and scaling L' by an element in $F^\times$ if necessary, we can find a basis $\{e, f\}$ of L and $n \geq 0$ such that $\{e, \pi^n f\}$ is a basis of L'. Using $\{e, f\}$, we can identify $\mathcal{O}$ with $M_2(\mathfrak{o})$ and $\mathcal{O}'$ with $x\mathcal{O}x^{-1}$ where x is the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi^n \end{smallmatrix}\right)$. Then $\mathcal{O}' = \begin{pmatrix} \mathfrak{o} & \mathfrak{p}^n \\ \mathfrak{p}^{-n} & \mathfrak{o} \end{pmatrix}$. Thus

$$\frac{\mathcal{O}}{\mathcal{O} \cap \mathcal{O}'} \cong \frac{\mathfrak{o}}{\mathfrak{p}^n} \cong \frac{\mathcal{O}'}{\mathcal{O} \cap \mathcal{O}'}.$$

□

Definition 5.24 Let $\mathcal{O}$ and $\mathcal{O}'$ be maximal $\mathfrak{o}$-orders in $M_2(F)$. The *distance* between $\mathcal{O}$ and $\mathcal{O}'$ is defined to be $\log_q[\mathcal{O} : \mathcal{O} \cap \mathcal{O}']$. The orders $\mathcal{O}$ and $\mathcal{O}'$ are *neighbors* if the distance between them is 1.

Lemma 5.25 *Suppose that the distance between two maximal $\mathfrak{o}$-orders $\mathcal{O}$ and $\mathcal{O}'$ in $M_2(F)$ is n. Then $\mathcal{O}' = x\mathcal{O}x^{-1}$ for some $x \in GL_2(F)$ with $ord_{\mathfrak{p}}(\det(x)) = n$.*

Proof. This is clear from the proof of Lemma 5.23.

5.6 Orders in the Local Case

In this subsection, we deal with the case when F is a $\mathfrak{p}$-adic field and $\mathfrak{o}$ is its ring of integers. So, $\mathfrak{o}$ is a PID with prime ideal $\mathfrak{p} = \pi\mathfrak{o}$. Let H is the unique quaternion algebra $\left(\frac{u,\pi}{F}\right)$, where u is a nonsquare unit so that $F(\sqrt{u})/F$ is an unramified quadratic extension. If v is a valuation on F and $w = v \circ \mathrm{nr}$, then w is a valuation on H. Let $\mathcal{O}$ be the associated valuation ring $\{x \in H : w(x) \leq 1\}$. Note that $\mathcal{O}$ is also equal to $\{x \in H : \mathrm{nr}(x) \in \mathfrak{o}\}$.

Theorem 5.26 *The valuation ring $\mathcal{O}$ is the unique $\mathfrak{o}$-maximal order in H and has discriminant $d(\mathcal{O}) = \pi^2\mathfrak{o} = \mathfrak{p}^2$.*

Proof. For any $x \in H$, there exists a nonzero $r \in \mathfrak{o}$ such that $rx \in \mathcal{O}$. So, $F\mathcal{O} = H$. If $x \in \mathcal{O}$, then $\overline{x} \in \mathcal{O}$ and so $\mathrm{tr}(x) = x + \overline{x} \in \mathcal{O} \cap F = \mathfrak{o}$. But $\mathrm{nr}(x) \in \mathfrak{o}$ since $x \in \mathcal{O}$. Thus x is integral over $\mathfrak{o}$. This shows that $\mathcal{O}$ is an $\mathfrak{o}$-order in H.

If $x \in H$ is integral over $\mathfrak{o}$, then $\mathrm{nr}(x) \in \mathfrak{o}$ and hence $w(x) \leq 1$. Thus $x \in \mathcal{O}$, which means that $\mathcal{O}$ is precisely the set of elements in H that are integral over $\mathfrak{o}$. Hence $\mathcal{O}$ is the maximal $\mathfrak{o}$-order in H.

Let $\{1, i, j, ij\}$ be a standard basis of H such that $i^2 = u$ and $j^2 = \pi$. Let K be $F(\sqrt{u})$. Then $H = K + Kj$ and $\mathrm{nr}|_K$ is the norm $N_{K/F}$. Since K/F is unramified, π is also a uniformizer for K. Let $\mathfrak{o}_K$ be the ring of integers of K. Then

$$\mathfrak{o}_K = \{x \in K : \mathrm{nr}(x) \in \mathfrak{o}\}.$$

Now let $\alpha = x + yj \in H$ with $x, y \in K$. Then $\mathrm{nr}(\alpha) = \mathrm{nr}(x) - \mathrm{nr}(y)\pi$. Since $\mathrm{nr}(x)$ and $\mathrm{nr}(y)$ are of the form $\pi^{2m}z$, where $z \in \mathfrak{o}^\times$, we see that $\mathrm{nr}(\alpha) \in \mathfrak{o}$ if and only if $\mathrm{nr}(x)$ and $\mathrm{nr}(y)$ are in $\mathfrak{o}$. Thus $\alpha \in \mathcal{O}$ if and only if $\alpha \in \mathfrak{o}_K + \mathfrak{o}_K j$. Hence $\mathcal{O} = \mathfrak{o}_K + \mathfrak{o}_K j$.

Now, let $y \in \mathfrak{o}_K$ such that $\{1, y\}$ is a basis of $\mathfrak{o}_K$ over $\mathfrak{o}$. Then $\{1, y, j, yj\}$ is a basis of $\mathcal{O}$ over $\mathfrak{o}$. Note that $jy = \overline{y}j$ and $\mathrm{tr}(\alpha j) = 0$ for all $\alpha \in K$. From this it follows that

$$d(\mathcal{O}) = (y - \overline{y})^4\pi^2\mathfrak{o}.$$

Since K/F is unramified, the reside field of K is a quadratic extension of the reside field of F. Thus, if $y - \overline{y}$ is not a unit, then the images of y and $\overline{y}$ in the residue field of K would be the same, which means that the image of y is in the residue field of F. However, $\mathfrak{o}_K$ is equal to $\mathfrak{o}[y]$, and so the residue fields of K and F must be the same which is impossible. Therefore, $d(\mathcal{O}) = \pi^2\mathfrak{o}$.□

5.7 Orders in the Global Case

In this subsection, F is a number field and $\mathfrak{o}$ is the ring of integers in F. Let H be a quaternion algebra over F. Recall that $\mathrm{Ram}(H)$ is the set of places at which H is ramified. It is a finite set with even number of elements.

Definition 5.27 The *discriminant* of H, denoted $\Delta(H)$, is the product of all the finite places at which H is ramified.

Theorem 5.28 *Let $\mathcal{O}$ be an $\mathfrak{o}$-order in a quaternion algebra H over a number field F. Then $\mathcal{O}$ is a maximal $\mathfrak{o}$-order if and only if $d(\mathcal{O}) = \Delta(H)^2$. In particular, all maximal $\mathfrak{o}$-orders in H have the same discriminant.*

Proof. By Lemma 5.13, $\mathcal{O}$ is maximal if and only if $\mathcal{O}_\mathfrak{p}$ is maximal for every finite place $\mathfrak{p}$. By Example 5.16 and Theorem 5.26, the discriminant of a maximal $\mathfrak{o}_\mathfrak{p}$-order in $H_\mathfrak{p}$ is either $\mathfrak{o}_\mathfrak{p}$ or $\mathfrak{p}^2$ according to whether $H_\mathfrak{p}$ splits or is ramified. Furthermore, orders with these discriminants are necessarily maximal by Theorem 5.19. The result now follows from the fact that $d(\mathcal{O})$ is the product of all $d(\mathcal{O}_\mathfrak{p})$.□

Example 5.29 Let H be the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. Then H_p splits for all odd primes p; see Theorem 3.13. Since $|\mathrm{Ram}(H)|$ is even and $H \otimes_\mathbb{Q} \mathbb{R} = \mathbb{H}$, H is ramified at 2. Thus $\Delta(H) = 2\mathbb{Z}$. The discriminant of the $\mathbb{Z}$-order $\mathcal{O}'$ in Example 5.17 is $4\mathbb{Z}$. Thus $\mathcal{O}'$ is a maximal $\mathbb{Z}$-order in H.

6 Conjugacy Classes of Maximal Orders

In this section F is a number field. We keep all the relevant notations used in the previous section. When the ring of integers $\mathfrak{o}$ of F is a PID, then all the maximal orders in $M_2(F)$ are conjugate to $M_2(\mathfrak{o})$. This does not hold in general and in this section we give a formula for the number of conjugacy classes of maximal orders in a quaternion algebra over F.

6.1 Idele Group of a Quaternion Algebra

Let H be a quaternion algebra over F, and let $\mathcal{O}$ be a maximal $\mathfrak{o}$-order in H. The *idele group* of H is the set

$$H_\mathbb{A}^\times = \left\{ (x_v) \in \prod_{v\in\Omega} H_v^\times : x_v \in \mathcal{O}_v^\times \text{ for almost all finite places } v \right\}.$$

The elements of $H_\mathbb{A}^\times$ are called ideles of H. Clearly $H_\mathbb{A}^\times$ is a subgroup of the direct product $\prod_{v\in\Omega} H_v^\times$. For each $v \in \Omega$, there is an embedding $\sigma_v : H \hookrightarrow H_v = F_v \otimes_F H$, where $\sigma_v(x) = 1 \otimes x$ for all $x \in H$. Using this embedding, we can identify $H^\times$ as a subgroup of $H_v^\times$ and we will not make any distinction between x and $\sigma_v(x)$. If $x \in H^\times$, there exists $r \neq 0$ in F such that $rx^{-1} \in \mathcal{O}$. Since $r \in \mathfrak{o}_v^\times$ for almost all v, therefore $x \in \mathcal{O}_v^\times$ for almost all v; hence $H^\times$ can be identified as a subgroup of $H_\mathbb{A}^\times$.

Let $x = (x_v)$ be an idele of H. Define an order $x\mathcal{O}x^{-1}$ in H by specifying its local completion at a finite place v as

$$(x\mathcal{O}x^{-1})_v = x_v \mathcal{O}_v x_v^{-1}.$$

This definition is meaningful by Lemma 5.12 since $x_v \in \mathcal{O}_v^\times$ for almost all finite places v so that $(x\mathcal{O}x^{-1})_v = \mathcal{O}_v$ for almost all v. Since the conjugate of a maximal order in H_v is again maximal, the order $x\mathcal{O}x^{-1}$ is a maximal order in H by Corollary 5.13.

Lemma 6.1 *Let $\mathcal{O}'$ be another maximal order in H. Then $\mathcal{O}' = x\mathcal{O}x^{-1}$ for some $x \in H_{\mathbb{A}}^{\times}$.*

Proof. Let S be the set of finite places v for which $\mathcal{O}_v \neq \mathcal{O}'_v$. Then S is a finite set and $S \cap \mathrm{Ram}(H) = \emptyset$. If $v \in S$, then $H_v \cong M_2(F_v)$. Since $\mathfrak{o}_v$ is a PID, $\mathcal{O}'_v$ is conjugate to $\mathcal{O}_v$ and hence there exists $h_v \in H_v^{\times}$ such that $h_v \mathcal{O}_v h_v^{-1} = \mathcal{O}'_v$. Now define an idele $x \in H_{\mathbb{A}}^{\times}$ by

$$x_v = \begin{cases} 1 & \text{if } v \notin S; \\ h_v & \text{if } v \in S. \end{cases}$$

It is clear that $x\mathcal{O}x^{-1} = \mathcal{O}'$.□

Up to this point, we see that $H_{\mathbb{A}}^{\times}$ acts on the set of all maximal orders in H by conjugation and the action is transitive. For every $v \in \Omega_f$, let $\mathfrak{N}(\mathcal{O}_v)$ be the normalizer of $\mathcal{O}_v$, that is

$$\mathfrak{N}(\mathcal{O}_v) = \{x_v \in H_v^{\times} : x_v \mathcal{O}_v x_v^{-1} = \mathcal{O}_v\}.$$

It is easy to see that $\mathfrak{N}(\mathcal{O}_v)$ is a subgroup of $H_v^{\times}$. Moreover, $\mathcal{O}_v^{\times} \subseteq \mathfrak{N}(\mathcal{O}_v)$. Let

$$\mathfrak{N}(\mathcal{O})_{\mathbb{A}} = \{x = (x_v) \in H_{\mathbb{A}}^{\times} : x_v \in \mathfrak{N}(\mathcal{O}_v) \text{ for all } v \in \Omega_f\}.$$

Clearly $\mathfrak{N}(\mathcal{O}_v)$ is a subgroup of $H_{\mathbb{A}}^{\times}$. In fact, $\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ is the stabilizer of $\mathcal{O}$ in $H_{\mathbb{A}}^{\times}$.

Proposition 6.2 *The set of conjugacy classes of maximal orders in H is in bijection with the double coset space $H^{\times} \backslash H_{\mathbb{A}}^{\times} / \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$.*

Proof. Let $\mathcal{C}$ be the set of conjugacy classes of maximal orders in H. We shall set up a bijection Φ from the double coset space $H^{\times} \backslash H_{\mathbb{A}}^{\times} / \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ to $\mathcal{C}$.

Suppose that $H^{\times} x \mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^{\times} y \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. Then $x = hyn$, where $h \in H^{\times}$ and $n \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. So $x\mathcal{O}x^{-1} = h(y\mathcal{O}y^{-1})h^{-1}$ and thus $x\mathcal{O}x^{-1}$ and $y\mathcal{O}y^{-1}$ are in the same conjugacy class. This means that we can define a function $\Phi : H^{\times} \backslash H_{\mathbb{A}}^{\times} / \mathfrak{N}(\mathcal{O})_{\mathbb{A}} \to \mathcal{C}$ such that

$$\Phi(H^{\times} x \mathfrak{N}(\mathcal{O})_{\mathbb{A}}) = \text{ conjugacy class that contains } x\mathcal{O}x^{-1}.$$

Lemma 6.1 implies that Φ is surjective.

Now, let $x, y \in H_{\mathbb{A}}^{\times}$ such that $x\mathcal{O}x^{-1}$ and $y\mathcal{O}y^{-1}$ are in the same conjugacy class. Then $x\mathcal{O}x^{-1} = hy\mathcal{O}(hy)^{-1}$ for some $h \in H^{\times}$. So, $x^{-1}hy \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ and hence $y \in H^{\times} x \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. This shows that Φ is injective.□

6.2 Theorem on Norms

We continue to assume that H is a quaternion algebra over the number field F. Let v be an infinite place of F. If H_v splits, then clearly $\mathrm{nr}(H_v^{\times}) = F_v^{\times}$. If H_v is ramified, then v must be a real place and H_v is Hamilton's quaternions $\mathbb{H}$. If $\{1, i, j, ij\}$ is a standard basis of $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, then

$$\mathrm{nr}(x_1 + x_2 i + x_3 j + x_4 ij) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

and thus $\mathrm{nr}(H_v^{\times}) = \mathbb{R}^{\times 2}$.

Lemma 6.3 *If v is a finite place of F, then $nr(H_v^\times) = F_v^\times$.*

Proof. This is clear if $H_v = M_2(F_v)$. Thus we assume that H_v is the unique quaternion algebra $\left(\frac{\pi,u}{F_v}\right)$ over F_v, where π is a uniformizer for F_v and u is a nonsquare unit of $\mathfrak{o}_v$ so that $F_v(\sqrt{u})/F_v$ is unramified. The restriction of the reduced norm on $F_v(\sqrt{u})$ is the usual norm N of the field extension $F_v(\sqrt{u})/F_v$. Since $[F_v^\times : N(F_v(\sqrt{u})^\times)] = 2$ and $N(F_v(\sqrt{u})^\times)$ contains all the units of $\mathfrak{o}_v$, it remains to show that $\mathrm{nr}(H_v^\times)$ contains a uniformizer of F_v. But this is clear; $\mathrm{nr}(j) = -\pi$ if $\{1, i, j, ij\}$ is a standard basis for $\left(\frac{\pi,u}{F_v}\right)$.□

Let $\mathrm{Ram}_\infty(H)$ be the set of infinite places at which H is ramified. It is necessary that $F_v \cong \mathbb{R}$ for all $v \in \mathrm{Ram}_\infty(H)$. Let

$$F_H^\times = \{a \in F^\times : \ a \text{ is positive in } F_v \text{ for all } v \in \mathrm{Ram}_\infty(H)\}.$$

Proposition 6.4 (Theorem on Norms) *Let H be a quaternion algebra over a number field F. Then $nr(H^\times) = F_H^\times$.*

Proof. It is clear that $\mathrm{nr}(H^\times) \subseteq F_H^\times$. Let $a \in F_H^\times$. Then $a \in \mathrm{nr}(H_v^\times)$ for all $v \in \Omega$ by Lemma 6.3. Since H, when equipped with the reduced norm, is a nondegenerate quadratic space over F, we can apply Hasse-Minkowski Theorem to the present situation and deduce that $a \in \mathrm{nr}(H^\times)$.□

The *idele group* of F is the set

$$\mathbb{J}_F = \{x = (x_v) \in \prod_{v\in\Omega} F_v^\times : x_v \in \mathfrak{o}_v^\times \text{ for almost all finite places } v\}.$$

The elements of $\mathbb{J}_F$ are called the *ideles* of F. It is clear that $\mathbb{J}_F$ is indeed an abelian group under the operation $(x_v)(y_v) = (x_v y_v)$. For any $a \in F^\times$, $a \in \mathfrak{o}_v^\times$ for almost all finite places v. Therefore, a can be regarded as the idele whose v-component is a itself (of course, here we identify a with $\sigma_v(a)$ where $\sigma_v : F \to F_v$ is the embedding associated with the place v). Thus we can identify $F^\times$ as a subgroup of $\mathbb{J}_F$. Since $\mathrm{nr}(\mathcal{O}_v^\times) \subseteq \mathfrak{o}_v^\times$ for all finite places v, we can define the reduced norm $\mathrm{nr} : H_\mathbb{A}^\times \to \mathbb{J}_F$ by $\mathrm{nr}((x_v)) = (\mathrm{nr}(x_v))$.

For each $v \in \Omega$, let

$$\mathfrak{N}_v = \begin{cases} \mathrm{nr}(\mathfrak{N}(\mathcal{O}_v)) & \text{if } v \in \Omega_f; \\ \mathrm{nr}(H_v^\times) & \text{if } v \in \Omega_\infty. \end{cases}$$

Since $Z(H_v) = F_v$, $\mathfrak{N}_v$ contains $F_v^{\times 2}$. Let

$$\mathbb{J}_F(\mathcal{O}) = \{x = (x_v) \in \mathbb{J}_F : x_v \in \mathfrak{N}_v \text{ for all } v \in \Omega\}.$$

It is clear that $\mathbb{J}_F(\mathcal{O})$ is the image of $\mathfrak{N}(\mathcal{O})_\mathbb{A}$ under the reduced norm, and $\mathbb{J}_F(\mathcal{O}) \supseteq \mathbb{J}_F^2$.

Proposition 6.5 *Let v be a finite place of F. Then*

$$\mathfrak{N}_v = \begin{cases} \mathfrak{o}_v^\times F_v^{\times 2} & \textit{if } H_v \textit{ splits}; \\ F_v^\times & \textit{otherwise}. \end{cases}$$

Proof. Suppose that H_v is a division algebra. Then $\mathcal{O}_v$ is the unique maximal order in H_v. Thus $x\mathcal{O}_v x^{-1} = \mathcal{O}_v$ for all $x \in H_v^\times$. So $\mathfrak{N}(\mathcal{O}_v) = H_v^\times$, and hence $\mathfrak{N}_v = F_v^\times$ by Lemma 6.3.

Now suppose that $H_v = M_2(F_v) = \mathrm{End}(V)$ where V is a 2-dimensional vector space over F_v. We may assume that $\mathcal{O}_v = M_2(\mathfrak{o}_v) = \mathrm{End}(L)$, where L is a complete $\mathfrak{o}_v$-lattice in V. In this case, $\mathcal{O}_v^\times$ contains all invertible matrices in $M_2(\mathfrak{o}_v)$. Therefore, $\mathfrak{o}_v^\times F_v^{\times 2} \subseteq \mathfrak{N}_v$. For the other inclusion, let σ be an element in $\mathfrak{N}(\mathcal{O}_v)$. Then

$$\mathrm{End}(L) = \sigma \mathrm{End}(L)\sigma^{-1} = \mathrm{End}(\sigma(L)).$$

Since $\mathrm{End}(\sigma L) = \mathrm{End}(a\,\sigma(L))$ for all $a \in F_v^\times$, we may also assume that $\sigma(L) \subseteq L$ and, by choosing a suitably, that there exist a basis $\{e, f\}$ of L and $\alpha \in \mathfrak{o}_v$ such that $\{e, \alpha f\}$ is a basis of $\sigma(L)$. Let $\tau \in \mathrm{End}(V)$ be the map that sends e to e and f to αf. Then $\tau\sigma^{-1}$ is an element in $\mathrm{End}(\sigma(L))$. Thus $\mathrm{nr}(\sigma) = \alpha u$ for some $u \in \mathfrak{o}_v^\times$. We claim that α is also in $\mathfrak{o}_v^\times$ and this will conclude the proof of this case. For, let $\beta \in \mathrm{End}(V)$ be the element which switches e and f. Then $\beta \in \mathrm{End}(L)^\times$ and hence β is also in $\mathrm{End}(\sigma(L))^\times$. But then $\{f, \alpha e\}$ is also a basis of $\sigma(L)$, whence $\alpha \in \mathfrak{o}_v^\times$.□

6.3 Strong Approximation

Let v be a place of F, and let $\mathcal{B}$ be a basis of H_v over F_v. Using $\mathcal{B}$, H_v can be identified with F_v^4, and we can make H_v into a topological space by transporting the product topology from F_v^4. It is not hard to see that different bases for H_v produce the same topology on H_v. Moreover, with respect to this topology, H_v becomes a locally compact topological ring, that is, the addition and multiplication in H_v are continuous operations. We impose the subspace topology on $H_v^\times$. Let $x \in H_v^\times$. Then $x^{-1} = \overline{x}/\mathrm{nr}(x)$, where $\overline{x}$ is the conjugation on H_v. Let $\{1, i, j, ij\}$ be a standard basis for $H_v = \left(\frac{\alpha,\beta}{F_v}\right)$. If $x = a_0 + a_1 i + a_2 j + a_3 ij$, then $\mathrm{nr}(x) = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2$ and $\overline{x} = a_0 - a_1 i - a_2 j - a_3 ij$. Hence $x \mapsto x^{-1}$ is a continuous map, whence $H_v^\times$ is in fact a locally compact topological group.

Now suppose that v is a finite place of F and $\mathfrak{p}_v$ is the associated prime ideal. Let L be the $\mathfrak{o}_v$-lattice spanned by $\mathcal{B}$. Since $L \cong \mathfrak{o}_v^4$ and $\mathfrak{o}_v$ is both compact and open, L itself is also both compact and open. The collection of compact-open sets $\{\mathfrak{p}_v^n L\}$ is a fundamental system of compact neighborhoods of 0. For every $x \in H_v^\times$, the set $x + \mathfrak{p}_v^n L$ is contained in $H_v^\times$ for all sufficiently large integers n.

Let $\mathcal{O}$ be a maximal order in H. For each finite place v of F, the group $\mathcal{O}_v^\times$ is a compact-open subgroup of $H_v^\times$. It is because $\mathrm{nr} : \mathcal{O}_v \to \mathfrak{o}_v$ is a continuous map and $\mathcal{O}_v^\times = \mathrm{nr}^{-1}(\mathfrak{o}_v^\times)$ is both closed and open in the compact space $\mathcal{O}_v$. We now make $H_{\mathbb{A}}^\times$ into a topological group by specifying a fundamental system of neighborhoods of the identity in $H_{\mathbb{A}}^\times$ consisting of the sets of the form

$$\prod_{v \in \Omega} U_v,$$

where each U_v is an open neighborhood of 1 in $H_v^\times$ with $U_v = \mathcal{O}_v^\times$ for almost all finite places v. We call this topology the *restricted product* topology of $H_{\mathbb{A}}^\times$. If S is a finite subset of Ω

containing Ω_∞, let

$$H_{\mathbb{A}}^\times(S) = \prod_{v\in S} H_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times,$$

which is a subset of $H_{\mathbb{A}}^\times$. Then the restricted product topology on $H_{\mathbb{A}}^\times(S)$ coincides with the product topology. Since $\mathcal{O}_v^\times$ is compact for all $v \in \Omega_f$, $H_{\mathbb{A}}^\times(S)$ is locally compact. Since $H_{\mathbb{A}}^\times$ is the union of all these $H_{\mathbb{A}}^\times(S)$, $H_{\mathbb{A}}^\times$ is a locally compact topological group.

Example 6.6 The restricted product topology on $H_{\mathbb{A}}^\times$ is not the subspace topology induced by the product topology on $\prod_{v\in\Omega} H_v^\times$. The set

$$\mathcal{U} = \prod_{v\in\Omega_\infty} H_v^\times \times \prod_{v\in\Omega_f} \mathcal{O}_v^\times$$

is open in $H_{\mathbb{A}}^\times$. If the restricted product topology were the subspace topology induced from $\prod_{v\in\Omega} H_v^\times$, then $\mathcal{U}$ must contain a set of the form

$$\mathcal{W}_S = H_{\mathbb{A}}^\times \bigcap \left(\prod_{v\in S} W_v \times \prod_{v\notin S} H_v^\times \right)$$

where S is a finite subset of Ω and W_v is an open subset of $H_v^\times$ for each $v \in S$. But it is clear that for $\mathcal{U}$ does not contain any such $\mathcal{W}_S$.

For each $v \in \Omega$, let $H_v^1 = \{x_v \in H_v^\times : \mathrm{nr}(x_v) = 1\}$. Define

$$H_{\mathbb{A}}^1 = \{x = (x_v) \in H_{\mathbb{A}}^\times : x_v \in H_v^1 \text{ for all } v \in \Omega\}.$$

It is clear that $H_{\mathbb{A}}^1$ is the kernel of the reduced norm $\mathrm{nr} : H_{\mathbb{A}}^\times \to \mathbb{J}_F$. Thus $H_{\mathbb{A}}^1$ is a normal subgroup of $H_{\mathbb{A}}^\times$. Moreover, it contains the commutator subgroup of $H_{\mathbb{A}}^\times$. We give $H_{\mathbb{A}}^1$ the subspace topology induced by the restricted product topology on $H_{\mathbb{A}}^\times$. For any finite subset S of Ω, let

$$H_S^1 = \{x = (x_v) \in H_{\mathbb{A}}^1 : x_v = 1 \text{ for all } v \notin S\}.$$

Theorem 6.7 (Strong Approximation Theorem for H^1) *Let H be a quaternion algebra over a number field F, and let S be a finite subset of places of F containing Ω_∞ such that H_v splits for at least one place in S. Then $H^1 H_S^1$ is dense in $H_{\mathbb{A}}^1$.*

Here is a consequence (in fact, equivalent version) of the Strong Approximation Theorem which will be used. Fix a positive integer N and a complete $\mathfrak{o}$-lattice L in H. Let T be a finite subset of Ω_f which is disjoint from S. Suppose that $x_v \in H_v^1$ is given for each $v \in T$. Let

$$U_v = \{z \in H_v : z \equiv x_v \bmod \mathfrak{p}_v^N L_v\},$$

and set

$$\mathcal{U} = H_{\mathbb{A}}^1 \cap \left(\prod_{v\in S} H_v^\times \times \prod_{v\in T} U_v \times \prod_{v\notin T\cup S} \mathcal{O}_v^\times \right),$$

which is an open neighborhood of x in $H^1_{\mathbb{A}}$, where x is idele such that its v-th component is x_v for all $v \in T$ and 1 eleswhere. So, there exists $h \in H^1$ and $y \in H^1_S$ such that $hy \in \mathcal{U}$. This implies

(1) $h \equiv x_v \bmod \mathfrak{p}_v^N L_v$ for all $v \in T$;

(2) $h \in \mathcal{O}_v^\times$ for all $v \notin T \cup S$.

We shall apply the Strong Approximation Theorem to the case where $S = \Omega_\infty$. Thus it is useful to introduce the following standard notion to cover the circumstances under which the Strong Approximation Theorem will be applied.

Definition 6.8 A quaternion algebra H over a number field F is said to satisfy the *Eichler condition* if there is at least one infinite place of F at which H splits.

There is the restricted product topology on $\mathbb{J}_F$ which is defined similarly to the one on $H^\times_{\mathbb{A}}$. For each $v \in \Omega$, $F_v^\times$ is a locally compact; and for each $v \in \Omega_f$, $\mathfrak{o}_v^\times$ is compact. The restricted topology on $\mathbb{J}_F$ is defined by specifying a fundamental system of neighborhoods of the identity in $\mathbb{J}_F$ consisting of the sets of the form $\prod_{v\in\Omega} U_v$, where each U_v is an open neighborhood of 1 in $F_v^\times$ with $U_v = \mathfrak{o}_v^\times$ for almost all finite places v. With this topology, $\mathbb{J}_F$ is a locally compact topological group.

6.4 Type Number

If x, y are elements of $H^\times_{\mathbb{A}}$, then $xH^1_{\mathbb{A}} = H^1_{\mathbb{A}}x$, and the fact that $H^1_{\mathbb{A}}$ contains the commutator subgroup of $H^\times_{\mathbb{A}}$ implies that $xyH^1_{\mathbb{A}} = yxH^1_{\mathbb{A}}$; hence the set $xyH^1_{\mathbb{A}}$ is independent of the order of $H^1_{\mathbb{A}}, x$ and y. From this it follows that the set $H^1_{\mathbb{A}}H^\times\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ is independent of the order of $H^1_{\mathbb{A}}, H^\times$ and $\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$, and that this set is actually the group generated by $H^1_{\mathbb{A}}, H^\times$ and $\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. This group is a normal subgroup of $H^\times_{\mathbb{A}}$ and we can form the quotient group $H^\times_{\mathbb{A}}/H^1_{\mathbb{A}}H^\times\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$.

Lemma 6.9 *Let v be a finite place of F, and $\mathcal{O}'_v$ be a maximal order in H_v. If $x \in H_v^\times$, there exists an open neighborhood $\mathcal{U}$ of x such that $y\mathcal{O}'_v y^{-1} = x\mathcal{O}'_v x^{-1}$ for all $y \in U$.*

Proof. It suffices to prove the lemma for $x = 1$. For every $y \in U = 1 + \mathfrak{p}_v\mathcal{O}'_v \subseteq \mathcal{O}'_v$, $\mathrm{nr}(y)$ is a unit. So, $y^{-1} \in \mathcal{O}'_v$ and $y\mathcal{O}'_v y^{-1} = \mathcal{O}'_v$.□

Lemma 6.10 *If H satisfies the Eichler condition, then*

$$(*) \qquad H^\times x\mathfrak{N}(\mathcal{O})_{\mathbb{A}} \to H^\times xH^1_{\mathbb{A}}\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$$

is a well-defined bijection from $H^\times \backslash H^\times_{\mathbb{A}} / \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ to $H^\times_{\mathbb{A}}/H^1_{\mathbb{A}}H^\times\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$.

Proof. Suppose that $H^\times x\mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times y\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. Then there exist $h \in H^\times$ and $n \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ such that $y = hxn$. Thus

$$H^\times yH^1_{\mathbb{A}}\mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times xnH^1_{\mathbb{A}}\mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times xH^1_{\mathbb{A}}n\mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times xH^1_{\mathbb{A}}\mathfrak{N}(\mathcal{O})_{\mathbb{A}}.$$

This shows that $(*)$ is a well-defined function. Clearly it is surjective.

Now suppose that $H^\times x H^1_{\mathbb{A}} \mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times y H^1_{\mathbb{A}} \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. Then there exist $h \in H^\times$, $\alpha \in H^1_{\mathbb{A}}$ and $n \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ such that

$$hx = \alpha y n.$$

For the sake of convenience, we let $[z]\mathcal{O}$ be the order $z\mathcal{O}z^{-1}$ for $z \in H^\times_{\mathbb{A}}$, and $[z_v]\mathcal{O}_v$ be the order $z_v\mathcal{O}_v z_v^{-1}$ for all $z_v \in H_v^\times$ with $v \in \Omega_f$. Let

$$T = \{v \in \Omega_f : [hx_v]\mathcal{O}_v \neq [y_v]\mathcal{O}_v\}$$

and

$$J = \{v \in \Omega_f \setminus T : [y_v]\mathcal{O}_v \neq \mathcal{O}_v\}.$$

Both T and J are finite subsets of Ω_f.

Let $\mathcal{W}$ be an open set of $H^1_{\mathbb{A}}$ of the form

$$\prod_{v \in \Omega_\infty} H_v^1 \times \prod_{v \in T \cup J} U_v \times \prod_{v \in \Omega_f \setminus (T \cup J)} \mathcal{O}_v^1$$

where U_v is an open neighborhood of α_v (resp. 1) in H_v^1 if $v \in T$ (resp. $v \in J$). By the Strong Approximation Theorem, with suitably chosen U_v, there exists $\sigma \in H^1$ such that

(1) $[\sigma]\mathcal{O}_v = \mathcal{O}_v$ for all finite places v outside $T \cup J$;

(2) $[\sigma y_v]\mathcal{O}_v = [\alpha_v y_v]\mathcal{O}_v$ for all $v \in T$;

(3) $[\sigma y_v]\mathcal{O}_v = [y_v]\mathcal{O}_v$ for all $v \in J$.

If v is a finite place outside $T \cup J$, then

$$[\sigma y_v]\mathcal{O}_v = [\sigma]\mathcal{O}_v = \mathcal{O}_v = [hx_v]\mathcal{O}_v.$$

If $v \in T$, then

$$[\sigma y_v]\mathcal{O}_v = [\alpha_v y_v]\mathcal{O}_v = [hx_v]\mathcal{O}_v,$$

while if $v \in J$ we have

$$[\sigma y_v]\mathcal{O}_v = [y_v]\mathcal{O}_v = [hx_v]\mathcal{O}_v.$$

Therefore, $y^{-1}\sigma^{-1}hx \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ and thus $H^\times x \mathfrak{N}(\mathcal{O})_{\mathbb{A}} = H^\times y \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$. This proves that $(*)$ is injective.$\square$

Recall that $\mathbb{J}_F(\mathcal{O})$ is the image of $\mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ under the reduced norm. Let

$$\theta : H^\times_{\mathbb{A}} \to \mathbb{J}_F / F^\times \mathbb{J}_F(\mathcal{O})$$

be the homomorphism induced by the reduced norm.

Theorem 6.11 *Let H be a quaternion algebra over a number field F. Suppose that H satisfies the Eichler condition. Then the number of conjugacy classes of maximal orders in H is equal to the group index $[\mathbb{J}_F : F^\times \mathbb{J}_F(\mathcal{O})]$.*

Proof. It suffices to show that the homomorphism θ is surjective with $H^\times H^1_{\mathbb{A}} \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ as the kernel.

Let a be an element in $\mathbb{J}_F$. By the Weak Approximation Theorem for F, there exists $\alpha \in F^\times$ such that $a_v \alpha$ is positive in F_v for every $v \in \mathrm{Ram}_\infty(H)$. So we can assume that $a_v > 0$ for every $v \in \mathrm{Ram}(H)$. Thus for every $v \in \Omega_\infty$, $a_v = \mathrm{nr}(x_v)$ for some $x_v \in H_v^\times$. For almost all finite places v, H_v splits and a_v is a unit in $\mathfrak{o}_v$. At any one of these v, the maximal order $\mathcal{O}_v$ is isomorphic to $M_2(\mathfrak{o}_v)$; hence $\mathrm{nr}(\mathcal{O}_v^\times) = \mathfrak{o}_v^\times$. Therefore, $a_v = \mathrm{nr}(x_v)$ for some $x_v \in \mathcal{O}_v^\times$. For the remaining finitely many places v, it follows from Lemma 6.3 that $a_v = \mathrm{nr}(x_v)$ for some $x_v \in H_v^\times$. Then $x = (x_v)$ is an element in $H_{\mathbb{A}}^\times$ and $\mathrm{nr}(x) = a$. This proves that θ is surjective.

It is clear that $H^\times H^1_{\mathbb{A}} \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ is a part of the kernel of θ. Now, suppose that $\mathrm{nr}(x) \in F^\times \mathbb{J}_F(\mathcal{O})$. Then there exists $n \in \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$ such that $\mathrm{nr}(xn) \in F^\times$. Since $\mathrm{nr}(H_v^\times) = F_v^{\times 2}$ whenever $v \in \mathrm{Ram}_\infty(H)$, it follows that $\mathrm{nr}(xn) \in F_H^\times$. By Theorem 6.4, there exists $h \in H^\times$ with $\mathrm{nr}(hxn) = 1$. As a result, $hxn \in H^1_{\mathbb{A}}$ and hence the kernel of θ is precisely $H^\times H^1_{\mathbb{A}} \mathfrak{N}(\mathcal{O})_{\mathbb{A}}$.□

Definition 6.12 The *type number* of a quaternion algebra H over a number field is the number of conjugacy classes of maximal orders in H.

For our convenience, we let $\mathfrak{h}$ be the set $\mathrm{Ram}_\infty(H)$. Let

$$\mathbb{J}_F^{\mathfrak{h}} = \{x \in \mathbb{J}_F : x_v > 0 \text{ for all } v \in \mathfrak{h} \text{ and } x_v \in \mathfrak{o}_v^\times \text{ for all } v \in \Omega_f\}.$$

Let I_F be the group of fractional ideals of F, and let $P_F^{\mathfrak{h}}$ be the subgroup of principal fractional ideals that are generated by $a \in F^\times$ with a positive in F_v for all $v \in \mathfrak{h}$.

Let P_F^+ be the set of principal fractional ideals that are generated by totally positive elements in F. Then $P_F^2 \subseteq P_F^+$, and so P_F/P_F^+ is an elementary 2-group whose order is less than 2^r, where r is the number of real places of F. Thus the quotient I_F/P_F^+ is a finite abelian group, called the *narrow class group* of F, and its order is the *narrow class number* of F. Since $P_F^+ \subseteq P_F^{\mathfrak{h}} \subseteq P_F$, the quotient $I_F/P_F^{\mathfrak{h}}$ is also a finite abelian group and its order divides the narrow class number of F.

For any $x \in \mathbb{J}_F$, let (x) be the fractional ideal

$$(x) = \prod_{\mathfrak{p} \in \Omega_f} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$

The class of (x) in the quotient $I_F/P_F^{\mathfrak{h}}$ is denoted by $[x]$. Given an $x \in \mathbb{J}_F$, there exists $a \in F^\times$ such that $ax_v > 0$ for all $v \in \mathfrak{h}$. If b is another element in $F^\times$ such that $bx_v > 0$ for all $v \in \mathfrak{h}$, then $[ax] = [bx]$ in $I_F/P_F^{\mathfrak{h}}$. Hence we have a well-defined homomorphism

$$x \in \mathbb{J}_F/F^\times \longmapsto [ax] \in I_F/P_F^{\mathfrak{h}}.$$

It is clear that this homomorphism is surjective.

Lemma 6.13 $[\mathbb{J}_F : F^\times \mathbb{J}_F^{\mathfrak{h}}] = |I_F/P_F^{\mathfrak{h}}|$.

Proof. It suffices to show that the kernel of the above homomorphism is $F^\times \mathbb{J}_F^{\mathfrak{h}}/F^\times$. Take an idele $x \in \mathbb{J}_F^{\mathfrak{h}}$. Then $x_v \in \mathfrak{o}_v^\times$ for all finite places v, whence (x) is trivial. Therefore, $F^\times \mathbb{J}_F^{\mathfrak{h}}/F^\times$ is in the kernel. Conversely, suppose that x is in the kernel. Let $a \in F^\times$ be chosen so that $ax_v > 0$ for all $v \in \mathfrak{h}$. Then there exists $b \in F^\times$ such that $b > 0$ in F_v for all $v \in \mathfrak{h}$ and $(ax) = (b)$. Let $\beta = axb^{-1}$. Then $\beta_v \in \mathfrak{o}_v^\times$ for all finite places v, and $\beta_v > 0$ for all $v \in \mathfrak{h}$. Hence $\beta \in \mathbb{J}_F^{\mathfrak{h}}$ and $x \in F^\times \mathbb{J}_F^{\mathfrak{h}}$. Therefore the kernel of the above homomorphism is $F^\times \mathbb{J}_F^{\mathfrak{h}}$ and the lemma is proved.□

Corollary 6.14 *Let H be a quaternion algebra over a number field F. If H satisfies the Eichler condition, then its type number is finite; it divides the narrow class number of F.*

Proof. Let $\mathcal{O}$ be a maximal order in a quaternion algebra H over F. Then $\mathbb{J}_F(\mathcal{O})$ contains $\mathbb{J}_F^{\mathfrak{h}}$, hence $[\mathbb{J}_F : F^\times \mathbb{J}_F(\mathcal{O})]$ divides $[\mathbb{J}_F : F^\times \mathbb{J}_F^{\mathfrak{h}}]$ and the latter divides the narrow class number of F.□

Corollary 6.15 *Let H be a quaternion algebra over a number field F. If H satisfies the Eichler condition, then its type number is a power of* 2.

Proof. It is clear because $\mathbb{J}_F(\mathcal{O})$ contains $\mathbb{J}_F^2$.□

Corollary 6.16 *Let H be a quaternion algebra over $\mathbb{Q}$ which splits at the infinite place. Then the type number of H is* 1.

Remark 6.17 The type number of a quaternion algebra which does not satisfy the Eichler condition is also finite.

7 Sum of Three Squares

This section contains Venkov's proof of the following Theorem of Gauss. However, the proof we shall present is the modernized version by Rehm.

Theorem 7.1 *Let $m > 1$ be a squarefree integer such that $m \equiv 1, 2$ mod 4, $h(m)$ be the class number of the quadratic field $\mathbb{Q}(\sqrt{-m})$, and $\psi(m)$ be the number of integer solutions to the equation $x^2 + y^2 + z^2 = m$. Then $\psi(m) = 12\, h(m)$.*

7.1 The Hurwitz Quaternions

Throughout this section, we let H be the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. The reduce norm on H is the sum of four squares, and its restriction on H_0 is the sum of three squares. Let $\{1, i, j, k\}$ be a standard basis of H such that $i^2 = j^2 = -1$. Since it is an orthonormal basis of H, we can identify H, as a quadratic space over $\mathbb{Q}$, with the space $\mathbb{Q}^4$ in such a way that $\{1, i, j, k\}$ becomes the canonical basis of $\mathbb{Q}^4$.

Lemma 7.2 *Let u be a nonzero element in H. Then u, iu, ju, and ku are mutually orthogonal.*

Proof. Let p and q be two different elements from $\{1, i, j, k\}$. Then

$$\mathrm{tr}(pu\overline{qu}) = \mathrm{tr}(p\mathrm{nr}(u)\overline{q}) = \mathrm{nr}(u)\mathrm{tr}(p\overline{q}) = 0.$$

□

So, when $u \neq 0$, the set $\mathbb{Z}[i, j, k]u$, which is a complete $\mathbb{Z}$-lattice on H, produces a grid of 4-dimensional cubes in $\mathbb{Q}^4$. The side of any one of these cubes is $\sqrt{\mathrm{nr}(u)}$. Let $x \in H$. Then x must be in one of these cubes. Let su, $s \in \mathbb{Z}[i, j, k]$, be a corner of this cube that is closest to x. Then

$$x - su = (a_0 + a_2 i + a_3 j + a_4 k)u, \quad |a_i| \leq \frac{1}{2} \text{ for all } i.$$

So, $\mathrm{nr}(x - su) < \mathrm{nr}(u)$ unless x happens to be the midpoint of the cube, in which case all the a_i are equal to $\frac{1}{2}$ and so $\mathrm{nr}(x - su) = \mathrm{nr}(u)$. This shows that the order $\mathbb{Z}[i, j, k]$ does not have any division algorithm (with respect to nr).

Now, let $\mathcal{O}$ be the order $\mathbb{Z}[i, j, k, \delta]$, where $\delta = \frac{(1+i+j+k)}{2}$. We have seen in Example 5.29 that $\mathcal{O}$ is a maximal order in H. This order $\mathcal{O}$ is called the Hurwitz order of quaternions. Note that as a set, $\mathcal{O}$ is obtained by adding all the midpoints of the cubes formed by $\mathbb{Z}[i, j, k]$. Moreover, $\mathrm{nr}(\delta) = \mathrm{nr}(i) = \mathrm{nr}(j) = \mathrm{nr}(k) = 1$. Therefore, the elements in $\mathcal{O}$ are vertices of a grid of 4-dimensional rhombohedrons in H. If u is a nonzero Hurwitz quaternion, then the principal left ideal $\mathcal{O}u$ of $\mathcal{O}$ produces a grid of 4-dimensional rhombohedrons in H with side length $\sqrt{\mathrm{nr}(u)}$. Let x be an arbitrary element in H. Then x falls into one of these rhombohedrons. Let su be one of the closest corner. It is easy to see that $\mathrm{nr}(x - su) < \mathrm{nr}(u)$ and so $\mathcal{O}$ has a division algorithm.

Proposition 7.3 *Let $x \in H$ and u be a nonzero element of the Hurwitz order $\mathcal{O}$. Then there exist $s, r \in \mathcal{O}$ such that $x = su + r$ with $nr(r) < nr(u)$.*

It is clear that in the above discussion one can consider left multiplication of u and obtains an analogous division algorithm.

A nonzero ideal I in H is said to be a fractional $\mathcal{O}$-ideal if its left order is $\mathcal{O}$. In other words, I is a fractional $\mathcal{O}$-ideal if

$$\mathcal{O} = \{x \in H : xI \subseteq I\}.$$

Corollary 7.4 *Every left fractional $\mathcal{O}$-ideal in H is principal, that is, it is of the form $\mathcal{O}u$ for some $u \in H$.*

Proof. Let $\mathcal{A}$ be a nonzero left fractional $\mathcal{O}$-ideal in H. Since $\mathcal{A}$ is a finitely generated $\mathbb{Z}$-module, there exists a nonzero integer m such that all the elements in $m\mathcal{A}$ are integral over $\mathbb{Z}$. So, we may assume at the outset that all the elements in $\mathcal{A}$ are integral over $\mathbb{Z}$. In particular, the set of reduced norms of nonzero elements in $\mathcal{A}$ contains only positive

integers and hence it must have a minimum. Let $0 \neq u \in \mathcal{A}$ be chosen such that $\mathrm{nr}(u)$ is this minimum.

For any $x \in \mathcal{A}$, by Proposition 7.3 there exists $s \in \mathcal{O}$ such that $\mathrm{nr}(x - su) < \mathrm{nr}(u)$. Since $x - su$ is in $\mathcal{A}$, therefore $x - su$ must be zero. This shows that $\mathcal{A} = \mathcal{O}u$.□

Lemma 7.5 *The unit group of $\mathcal{O}$ is generated by i, j, δ, and it contains exactly 24 elements.*

Proof. This can be verified directly, using the fact that $x \in \mathcal{O}^\times$ if and only if $\mathrm{nr}(x) = 1$.□

Let $m > 1$ be a positive integer, and K be the quadratic field $\mathbb{Q}(\sqrt{-m})$. If $\mu \in \mathbb{H}_0$ such that $\mathrm{nr}(\mu) = m$, which is equivalent to $\mu^2 = -m$, then we have an embedding ϕ_μ from K to $K_\mu := \mathbb{Q}(\mu) \subseteq H$ which maps $\sqrt{-m}$ to μ.

Now, suppose that m is a positive integer such that $m \equiv 1, 2 \bmod 4$. The set of integer solutions of the diophantine equation $x^2 + y^2 + z^2 = m$ is in bijective correspondence with the set

$$R_m(\text{or simply } R) = \{\mu \in \mathcal{O} : \mu^2 = -m\}$$

which we call the *set of roots of m*. So, $|R| = \psi(m)$, which is always positive by a theorem of Legendre.

Let $\mu \in R$ and let $\mathfrak{o}_\mu = \mathcal{O} \cap K_\mu$. Then $\mathfrak{o}_\mu$ is an order in K_μ, and all its elements are integral over $\mathbb{Z}$. Thus $\mathfrak{o}_\mu$ is contained in the ring of integers of K_μ. However, since $m \equiv 1, 2 \bmod 4$, it is not hard to show that the ring of integers of K_μ is $\mathbb{Z}[\mu]$, and μ is clearly in $\mathfrak{o}_\mu$. Thus $\mathfrak{o}_\mu$ is precisely the ring of integers of K_μ.

Proposition 7.6 *If $\mathfrak{a}$ is a fractional ideal of $\mathfrak{o}_\mu$, then $\mathcal{O}\mathfrak{a} \cap K_\mu = \mathfrak{a}$.*

Proof. We may assume that $\mathfrak{a} \subseteq \mathfrak{o}_\mu$. It is clear that $\mathcal{O}\mathfrak{a}$ is a left $\mathcal{O}$-ideal in H. AS $1 \in \mathcal{O}$ and $\mathfrak{a} \subseteq K_\mu$, we have $\mathcal{O}\mathfrak{a} \supseteq \mathfrak{a}$.

For the other inclusion, note that $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}_\mu$. Clearly, $(\mathcal{O}\mathfrak{a} \cap K_\mu)\mathfrak{o}_\mu = \mathcal{O}\mathfrak{a} \cap K_\mu$, hence

$$\begin{aligned}
\mathcal{O}\mathfrak{a} \cap K_\mu &= (\mathcal{O}\mathfrak{a} \cap K_\mu)\mathfrak{a}^{-1}\mathfrak{a} \\
&\subseteq (\mathcal{O}\mathfrak{a}\mathfrak{a}^{-1} \cap K_\mu\mathfrak{a}^{-1})\mathfrak{a} \\
&= (\mathcal{O}\mathfrak{o}_\mu \cap K_\mu)\mathfrak{a} \\
&= (\mathcal{O} \cap K_\mu)\mathfrak{a} \\
&= \mathfrak{o}_\mu\mathfrak{a} = \mathfrak{a}.
\end{aligned}$$

□

Proposition 7.7 *Let $\mu \in \mathbb{H}$, $\mu \notin \mathbb{Q}$, then the centralizer of K_μ in H is K_μ itself.*

Proof. By the Noether-Skolem Theorem, there exists $t \in \mathbb{H}$ such that $1, \mu, t, \mu t$ form a standard basis of H. Then a direct computation shows that the centralizer of K_μ must be K_μ itself.□

Corollary 7.8 *If $\mu, \eta \in \mathbb{H}$ and $\mu^2 = \eta^2 = -m$, then $\{\alpha \in \mathbb{H} : \alpha\mu = \eta\alpha\}$ is a one dimensional right K_μ-vector space.*

Proof. Again, by the Noether-Skolem Theorem, the two embeddings ϕ_μ and ϕ_η are conjugate inside H, that is there exists $x \in H^\times$ such that $\phi_\mu(a) = x^{-1}\phi_\eta(a)x$ for all $a \in K$. In particular, $x\mu = \eta x$, and $\alpha\mu = \eta\alpha$ if and only if $x^{-1}\alpha$ centralizes K_μ. By Proposition 7.7, $x^{-1}\alpha \in K_\mu$, or equivalently, $\alpha \in xK_\mu$.□

7.2 Class Groups and Root Bundles

We continue to assume that $m > 1$ is a positive integer congruent to 1 or 2 mod 4. Let I_K be the group of fractional ideals of $K = \mathbb{Q}(\sqrt{m})$. For any $\mathfrak{a} \in I_K$, let $\mathfrak{a}_\mu = \phi_\mu(\mathfrak{a}) \subseteq K_\mu$. By Corollary 7.4, there exists $\kappa = \kappa(\mathfrak{a}, \mu) \in H$ such that

$$\mathcal{O}\mathfrak{a}_\mu = \mathcal{O}\kappa.$$

Note that κ is determined by $\mathfrak{a}$ and μ up to left multiplication of units of $\mathcal{O}$. So, $\kappa\mu\kappa^{-1}$ is determined up to inner automorphisms induced by units of $\mathcal{O}$.

Moreover,

$$\mathcal{O}\kappa\mu\kappa^{-1} = \mathcal{O}\mathfrak{a}_\mu\mu\kappa^{-1} = \mathcal{O}\mu\mathfrak{a}_\mu\kappa^{-1} \subseteq \mathcal{O}\mathfrak{a}_\mu\kappa^{-1} = \mathcal{O}\kappa\kappa^{-1} = \mathcal{O}.$$

Therefore, $\kappa\mu\kappa^{-1} \in \mathcal{O}$ and hence $\kappa\mu\kappa^{-1}$ is also a root.

We call the set $B(\mu) := \{\epsilon\mu\epsilon^{-1} : \epsilon \in \mathcal{O}^\times\}$ *bundle* of the root μ. For any $\mathfrak{a} \in I_K$, the root bundle $B(\kappa\mu\kappa^{-1})$ does not depend on the κ we choose for $\mathfrak{a}$. Therefore, if we let

$$\mathcal{W} = \{B(\mu) : \mu \in R\}$$

be the set of all root bundles, then we have a map

$$\Delta : I_K \times \mathcal{W} \to \mathcal{W}$$

defined by

$$\Delta(\mathfrak{a}, B(\mu)) = B(\kappa\mu\kappa^{-1}),$$

where $\kappa = \kappa(\mathfrak{a}, \mu)$ is chosen such that $\mathcal{O}\mathfrak{a}_\mu = \mathcal{O}\kappa$.

Lemma 7.9 *The map Δ defines an action of the group I_K on the set $\mathcal{W}$.*

Proof. Let $\mathfrak{a}, \mathfrak{b}$ be two fractional ideals of K. Let $\lambda = \kappa(\mathfrak{b}, \mu)\,\mu\,\kappa(\mathfrak{b}, \mu)^{-1}$; that is,

$$B(\lambda) = \Delta(\mathfrak{b}, B(\mu)).$$

Then ϕ_λ is ϕ_μ followed by the inner automorphism given by $\kappa(\mathfrak{b}, \mu)$. Therefore, it must be that $\mathfrak{a}_\lambda = \kappa(\mathfrak{b}, \mu)\mathfrak{a}_\mu\kappa(\mathfrak{b}, \mu)^{-1}$ and

$$\begin{aligned} \mathcal{O}\kappa(\mathfrak{a}, \lambda) &= \mathcal{O}\mathfrak{a}_\lambda \\ &= \mathcal{O}\kappa(\mathfrak{b}, \mu)\mathfrak{a}_\mu\kappa(\mathfrak{b}, \mu)^{-1} \\ &= \mathcal{O}\mathfrak{b}_\mu\mathfrak{a}_\mu\kappa(\mathfrak{b}, \mu)^{-1}; \end{aligned}$$

that is, $\mathcal{O}\kappa(\mathfrak{a},\lambda)\kappa(\mathfrak{b},\mu) = \mathcal{O}(\mathfrak{b}\mathfrak{a})_\mu = \mathcal{O}(\mathfrak{a}\mathfrak{b})_\mu$. So, we may choose $\kappa(\mathfrak{a}\mathfrak{b},\mu)$ to be the product $\kappa(\mathfrak{a},\mu)\kappa(\mathfrak{b},\mu)$, and find that

$$\kappa(\mathfrak{a},\lambda)\,\lambda\,\kappa(\mathfrak{a},\lambda)^{-1} = \kappa(\mathfrak{a}\mathfrak{b},\mu)\,\mu\,\kappa(\mathfrak{a}\mathfrak{b},\mu)^{-1}.$$

This shows that $\Delta(\mathfrak{a},\Delta(\mathfrak{b},B(\mu))) = \Delta(\mathfrak{a}\mathfrak{b},B(\mu))$, which proves the proposition.□

Let $\mu,\nu \in R$, and let

$$T_{\mu,\nu} = \{\lambda \in \mathcal{O} : \lambda\mu = \nu\lambda\}.$$

By Corollary 7.8, $T_{\mu,\nu}$ is the intersection of $\mathcal{O}$ with a two dimensional $\mathbb{Q}$-vector space; so it is a rank 2 $\mathbb{Z}$-submodule of $\mathcal{O}$. In particular, it is nonzero and hence $\mathcal{O}T_{\mu,\nu}$ is a complete $\mathbb{Z}$-lattice in H. So, $\mathcal{O}T_{\mu,\nu}$ is an ideal in H. It is easy to see that $\mathcal{O}T_{\mu,\nu}$ is in fact a left fractional ideal of $\mathcal{O}$.

Lemma 7.10 *For any roots μ,ν, we have $\mathcal{O}T_{\mu,\nu} = \mathcal{O}$.*

Proof. By Corollary 7.4, there exists $\rho \in \mathcal{O}$ such that $\mathcal{O}T_{\mu,\nu} = \mathcal{O}\rho$. We claim that ρ is a unit of $\mathcal{O}$. It suffices to show that $\mathrm{nr}(\rho)$ is not divisible by any prime in $\mathbb{Z}$. Let us suppose that $m \equiv 1 \bmod 4$ for the moment.

We first show that $2 \nmid \mathrm{nr}(\rho)$. It is enough to exhibit an element $\omega \in T_{\mu,\nu}$ such that $2 \nmid \mathrm{nr}(\omega)$. Since $\mu^2 = \nu^2 = -m$, $\alpha\mu + \nu\alpha \in T_{\mu,\nu}$ for all $\alpha \in \mathcal{O}$. Let $\mu = x_1 i + x_2 j + x_3 k$ and $\nu = y_1 i + y_2 j + y_3 k$ with $x_i, y_i \in \mathbb{Z}$ for all i. Since $m = x_1^2 + x_2^2 + x_3^2 \equiv 1 \bmod 4$, we may assume that $x_1 \equiv x_2 \equiv 0 \bmod 2$ and $x_3 \equiv 1 \bmod 2$. As to ν, it is enough to consider two cases

(1) $y_1 \equiv y_2 \equiv 0 \bmod 2$, and $y_3 \equiv 1 \bmod 2$;

(2) $y_1 \equiv y_3 \equiv 0 \bmod 2$, and $y_2 \equiv 1 \bmod 2$.

In (1), it is direct to check that $\mathrm{nr}(\mu+\nu) \equiv \mathrm{nr}(i\mu+\nu i) \equiv 0 \bmod 4$, but $\mathrm{nr}(\mu+\nu) - \mathrm{nr}(i\mu+\nu i) \equiv 4 \bmod 8$. Hence either $\mathrm{nr}(\mu+\nu)$ or $\mathrm{nr}(i\mu+\nu i)$ is not divisible by 8. Then we can take ω to be either $(\mu+\nu)/2$ or $(i\mu+\nu i)/2$. Note that ω will be in $\mathcal{O}$.

For (2), we use $\gamma = (1+j)\mu + \nu(1+j)$, which is

$$-(x_2+y_2) + (x_1+x_3+y_1-y_3)i + (x_2+y_2)j + (x_3-x_1+y_3+y_1)k.$$

Notice that all the coefficients in this linear combination are odd. Therefore, $\omega := \gamma/2$ is in $\mathcal{O}$, and hence $\omega \in T_{\mu,\nu}$. It is also easy to see that $2 \nmid \mathrm{nr}(\omega)$.

Now, suppose that $\mathrm{nr}(\rho)$ is divisible by an odd prime p. Since ρ is a right divisor of $\omega_0 := \mu+\nu$ and $\omega_1 := i\mu+\nu i$, therefore it is also a right divisor of $i(\omega_0 + i(\omega_1)) = i\nu - \nu i$ whose reduced norm is $4(y_2^2+y_3^2)$. We may conclude that $y_2^2+y_3^2 \equiv 0 \bmod p$. Using j, k instead of i, we obtain $y_1^2+y_3^2 \equiv 0 \equiv y_1^2+y_2^2 \bmod p$. These three congruences have only one common solution mod p, namely $y_1 \equiv y_2 \equiv y_3 \equiv 0 \bmod p$. This shows that $m = y_1^2+y_2^2+y_3^3 \equiv 0 \bmod p^2$, which is impossible.

The case $m \equiv 2 \bmod 4$ can be done by a similar argument.□

Proposition 7.11 *The action of I_K on $\mathcal{W}$ is transitive. Moreover, the stabilizer of any $B(\mu) \in \mathcal{W}$ is the subgroup of principal fractional ideals of K.*

Proof. Let $\mu, \nu \in R$. We have indicated earlier that $T_{\nu,\mu}$ is a $\mathbb{Z}$-module of rank 2. Let $\{\xi, \eta\}$ be a $\mathbb{Z}$-basis of $T_{\nu,\mu}$., and set

$$\mathfrak{b} := \mathfrak{o}_\mu \xi \overline{\eta} + \mathfrak{o}_\mu \mathrm{nr}(\eta).$$

Note that $\alpha \in T_{\nu,\mu}$ if and only if $\overline{\alpha} \in T_{\mu,\nu}$. Hence $\xi\overline{\eta}$ centralizes K_μ, and so $\xi\overline{\eta} \in K_\mu$ by Proposition 7.7. Thus $\xi\overline{\eta} \in K_\mu \cap \mathcal{O} = \mathfrak{o}_\mu$. This shows that $\mathfrak{b}$ is an ideal of $\mathfrak{o}_\mu$. By Lemma 7.10,

$$\mathcal{O}\mathfrak{b} = \mathcal{O}(\mathfrak{o}_\mu \xi\overline{\eta} + \mathfrak{o}_\mu \eta\overline{\eta}) = \mathcal{O}\xi\overline{\eta} + \mathcal{O}\eta\overline{\eta} = (\mathcal{O}\xi + \mathcal{O}\eta)\overline{\eta} = \mathcal{O}T_{\nu,\mu}\overline{\eta} = \mathcal{O}\overline{\eta}.$$

So, if we use $\mathfrak{a} = \phi_\mu^{-1}(\mathfrak{b})$ and $\overline{\eta} = \kappa(\mathfrak{a}, \mu)$, then $\mathfrak{a}_\mu = \mathfrak{b}$, $\mathcal{O}\mathfrak{a}_\mu = \mathcal{O}\overline{\eta}$, and $\overline{\eta} \in T_{\mu,\nu}$, that is $\overline{\eta}\mu\overline{\eta}^{-1}$. Hence

$$\Delta(\mathfrak{a}, B(\mu)) = B(\nu),$$

which means that the action of I_K on $\mathcal{W}$ is transitive.

For the second assertion, let $\alpha \in K^\times$ and $\mathfrak{a}$ be the principal fractional ideal of K generated by α. Then $\phi_\mu(\mathfrak{a}) = \mathfrak{o}_\mu\beta$, where $\beta = \phi_\mu(\alpha)$. We may then choose $\beta \in K_\mu$ to be $\kappa(\mathfrak{a}, \mu)$ and obtain

$$\Delta(\mathfrak{a}, B(\mu)) = B(\beta\mu\beta^{-1}) = B(\mu).$$

Conversely, suppose $\Delta(\mathfrak{a}, B(\mu)) = B(\mu)$. Then we may select $\kappa(\mathfrak{a}, \mu)$ such that $\kappa\mu\kappa^{-1} = \mu$. It follows from Proposition 7.7 that $\kappa \in K_\mu$. Hence

$$\mathcal{O}\mathfrak{a}_\mu = \mathcal{O}\kappa = \mathcal{O}\mathfrak{o}_\mu\kappa.$$

By Proposition 7.6, we have

$$\mathfrak{a}_\mu = \mathcal{O}\mathfrak{a}_\mu \cap K_\mu = \mathcal{O}\mathfrak{o}_\mu\kappa \cap K_\mu = \mathfrak{o}_\mu\kappa,$$

and so $\mathfrak{a}$ is principal.□

We have shown that the root bundle $\Delta(\mathfrak{a}, B(\mu))$ depends only the ideal class of $\mathfrak{a}$. So, given an ideal class $\mathcal{C} \in I_K$, we can define a function $\Pi_\mathcal{C} : \mathcal{W} \to \mathcal{W}$ by $\Pi_\mathcal{C}(B(\mu)) = B(\mathfrak{a}, B(\mu))$, where $\mathfrak{a}$ is *any* fractional ideal in $\mathcal{C}$. By Proposition 7.11, this function $\Pi_\mathcal{C}$ is a permutation on $\mathcal{W}$, and the map $\mathcal{C} \mapsto \Pi_\mathcal{C}$ is an isomorphism sending the ideal class group of K onto a sharply transitive permutation group of $\mathcal{W}$. As a result, $|\mathcal{W}| = h(m)$.

Finally, let us give a proof of Theorem 7.1. We need to count the number of roots belonging to a bundle $B(\mu)$. Let the group $\mathcal{O}^\times$ act on the set of roots R by conjugation. The stabilizer of a root μ is

$$\{\epsilon \in \mathcal{O}^\times : \epsilon\mu\epsilon^{-1}\} = \mathcal{O}^\times \cap K_\mu = \mathfrak{o}_\mu^\times = \{\pm 1\}.$$

The last equality is from the hypothesis that $m > 1$ and $m \equiv 1, 2 \bmod 4$. Hence $|B(\mu)| = |\mathcal{O}^\times|/2 = 12$, and thus

$$\psi(m) = |R| = 12|\mathcal{W}| = 12h(m).$$