6. Orders in Quaternion Algebras

§6.1. Integers, Ideals and Orders.

R : a Dedekind domain

k : the field of quotients of R, a number field or a P-adic field.

k : a number field $\Rightarrow R = R_k$: the ring of integers in k.

Recall a Dedekind domain is an integrally closed Noetherian ring in which every nontrivial prime ideal is maximal.

Recall k : a number field. S : a finite set of non-Archimedean places.

$\Rightarrow R_S = \{\alpha \in k \mid v_p(\alpha) \leq 1$ for all prime ideals $P \notin S\}$.

Recall A : a quaternion algebra over k.

$\Rightarrow \alpha \in A$ is an integer over R if $R[\alpha]$ is an R-lattice in A.

$\Leftrightarrow tr(\alpha), n(\alpha) \in R$.

A complete R-lattice in A is called an ideal I.

An order $\mathcal{O}$ in A is an ideal which is also a ring with 1.

$\Rightarrow$ Orders in A can be characterized as rings $\mathcal{O}$ of integers in A which contain R and are such that $k\mathcal{O} = A$.

$\Rightarrow$ Maximal orders exist and every order is contained in a maximal order.

Def. 6.1.1 An order $\mathcal{O}$ in A is an Eichler order if there exist distinct maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in A s.t. $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$.

ex) $A = M_2(k)$, $M_2(R)$ is a maximal order.

If R is a principal ideal domain, all maximal orders are

conjugate to $M_2(R)$.

Generally, $M_2(k) = End(V)$ where V is a two-dimensional space over k.

⇒ for every complete R-lattice L in V, $End(L)$ is an order in $End(V)$.

⇒ It will be shown that each $End(L)$ is maximal, i.e. every order in $End(V)$ is contained in some $End(L)$.

Recall I: an ideal in A ⇒ we define

$$O_\ell(I) = \{\alpha \in A \mid \alpha I \subset I\}, \quad O_r(I) = \{\alpha \in A \mid I\alpha \subset I\}.$$

Def. 6.1.2 Let I be an ideal in a quaternion algebra A.

- I is said to be <u>two-sided</u> if $O_\ell(I) = O_r(I)$.
- I is said to be <u>normal</u> if $O_\ell(I), O_r(I)$ are maximal orders.
- I is said to be <u>integral</u> if I lies in both $O_\ell(I)$ and $O_r(I)$.

<u>Note</u> If I is an integral two-sided ideal, it is an ideal in the related ring O in the usual sense of an ideal in a non-commutative ring.

Def. 6.1.3 I: an ideal in the quaternion algebra A over k.

⇒ The <u>norm of I</u>, $n(I)$, is the fractional ideal of R gen. by the elements $\{n(x) \mid x \in I\}$.

<u>Notation</u> O^1 = Group of units of reduced norm $1 = \{x \in O \mid n(x) = 1\}$

$O^* =$ Group of units of $O = \{x \in O \mid \exists\, y \in O \text{ s.t. } xy = 1\}$

$N(O) =$ The normalizer of $O = \{x \in A^* \mid xOx^{-1} = O\}$.

<u>Note</u> $O^1 \subset O^* \subset N(O)$.

§6.2. Localization.

Let R be a Dedekind domain with field of quotients k.
Let P be a prime ideal in R and let v_P be the associated valuation on k.

⇒ The local ring $R(v_P) = \{\alpha \in k \mid v_P(\alpha) \le 1\}$ has a unique prime ideal $P(v_P) = \{\alpha \in k \mid v_P(\alpha) < 1\}$.

⇒ The ring $R(v_P)$ can be identified with the localization of R at the multiplicative set $R \setminus P$, which is the ring of fractions $\{a/b \mid a \in R, b \in R \setminus P\}$

⇒ These local rings are principal ideal domains and a generator π of the ideal $P(v_P) = \pi R(v_P)$ is a <u>uniformizer</u>.

<u>Note</u> The rings $R(v_P)$ are all subrings of k and R can be recovered from them as

$$R = \bigcap_{\{P \text{ prime}\}} R(v_P)$$

where the intersection is over all non-zero prime ideals of R.

<u>Example 6.2.1</u> $R = \mathbb{Z}$, p : a prime.

$\Rightarrow R(v_p) = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$.

If $a/b \in \mathbb{Q}$, $p \nmid b$ for any prime p, then $a/b \in \mathbb{Z}$.

$$\Rightarrow R = \mathbb{Z} = \bigcap_{\{\text{prime } p\}} R(v_p).$$

<u>Lemma 6.2.2</u> V : a fin. dim. space over k. L : an R-lattice in V.

$\Rightarrow L = \bigcap R(v_P) L$, where the intersection is over all prime ideals of R.

Proof) For each P, $1 \in R(v_P) \Rightarrow L \subset R(v_P) L$.

$\Rightarrow L \subset \bigcap R(v_p)L$.

Conversely, let $\{x_1, \cdots, x_r\}$ be a generating set for L over R.

$\Rightarrow \{x_1, \cdots, x_r\}$ is a generating set for $R(v_p)L$ over $R(v_p)$.

Suppose that $x \in \bigcap R(v_p)L$. Define the set J by

$J = \{y \in R \mid yx \in L\}$. $\Rightarrow J$ is an ideal in R.

Now, for any prime P, $x \in R(v_p)L \Rightarrow x = \sum_{k=1}^{r} a_k x_k$ with $a_k = \frac{b_k}{c_k}$, where $b_k, c_k \in R$ and $c_k \notin P$. Let $c = c_1 \cdots c_r$ so that $c \notin P$.

However, $c \in J$. Thus J does not lie in any prime P and so $J = R$. Thus $1 \in J$ and $x \in L$. ▨

Note This result will be applied in the situation where V is a quaternion algebra over k and L is an ideal or an order. //

Lemma 6.2.3 R: a Dedekind domain, I: an ideal in the quaternion algebra A over k. For each prime P in R, let $I(v_p)$ be an $R(v_p)$-ideal in A s.t. $I(v_p) = R(v_p)I$ for almost all P.

Then $J = \bigcap I(v_p)$

is an R-ideal in A s.t. $R(v_p)J = I(v_p)$ for all P.

Proof) Let $x_1, x_2, x_3, x_4 \in I$ be linearly independent over k and let $L = R[x_1, x_2, x_3, x_4]$. Then L is an R-ideal and $L \subset I$, so $\exists\, r \in R$ s.t. $rI \subset L$. (See Lemma 2.2.2).

$\Rightarrow r$ is unit in $R(v_p)$ for almost all P.

$\Rightarrow R(v_p)L = R(v_p)I$ //

$\Rightarrow R(v_p)L = I(v_p)$ //

Thus choose $a, b \in R$ s.t.

$aI(v_p) \subset R(v_p)L \subset bI(v_p)$.

for all P. Then

$$J = \bigcap I(v_p) \subset a^{-1} \bigcap R(v_p)L = a^{-1}L.$$

by Lemma 6.2.2. Thus J is an R-lattice in A. Furthermore, in the same way, $L \subset bJ$ so J is an ideal in A.

Now, $R(v_p)J \subset R(v_p)I(v_p) = I(v_p)$. To obtain the reverse inclusion, we need the Chinese Ramainder Theorem (CRT):

Lemma 0.3.6 (CRT). Let $Q_1, Q_2, \cdots, Q_r$ be ideals in R_k such that $Q_i + Q_j = R_k$ for $i \neq j$. Then

$$Q_1 \cdots Q_r = \bigcap_{i=1}^{r} Q_i \quad \text{and} \quad R_k/Q_1 \cdots Q_r \cong \oplus \sum_i R_k/Q_i . \; //$$

Let $j_1, \cdots, j_r$ be a generating set for J. Let $x \in I(v_p)$ so that $x = \sum a_i j_i$ with $a_i \in k$. Choose $s_1 \in R$ so that $s_1 a_1 \in R$.

Suppose $s_1 R = P^{n_0} Q_1^{n_1} \cdots Q_t^{n_t}$, where $n_0 \geq 0$ and $n_i \geq 1$ for $1 \leq i \leq t$.

By the CRT, choose x_1 s.t. $x_1 \equiv s_1 \pmod{Q_i^{n_i+1}}$ for $1 \leq i \leq t$ and $x_1 \equiv s_1 a_1 + s_1 \pmod{P^{n_0+1}}$. Then we set $b_1 = x_1/s_1$.

$\Rightarrow$ For a prime P, $v_p(b_1 - a_1) = v_p\left(\frac{x_1 - a_1 s_1}{s_1}\right)$

$$= v_p(x_1 - a_1 s_1)/v_p(s_1) \leq 1,$$

since $x_1 - s_1 a_1 \equiv s_1 \pmod{p^{n_0+1}}$, $s_1 \in p^{n_0} \Rightarrow x_1 - s_1 a_1 \in p^{n_0}$.

& for each Q_i, $v_{Q_i}(b_1) = v_{Q_i}\left(\frac{x_1}{s_1}\right) = v_{Q_i}(x_1)/v_{Q_i}(s_1) \leq 1$

since $x_1 - s_1 \equiv 0 \pmod{Q_i^{n_i+1}}$, $s_1 \in Q_i^{n_i} \Rightarrow x_1 \in Q_i^{n_i}$.

& for a prime $p' \neq P, Q_i$'s, $v_{p'}(b_1) \leq 1$ since $\begin{cases} v_{p'}(s_1) = 1 \\ v_{p'}(x_1) \leq 1 \end{cases}$.

$\Rightarrow$ We can see that $b_1 - a_1 \in R(v_p)$ and $b_1 \in R(v_{p'})$ for all prime ideals $p' \neq P$. Repeat for each a_i's and let $y = \sum b_i j_i$

Then $y \in R(v_{p'})J \subset I(v_{p'})$ for all $p' \neq p$.
Also, $y - x = \sum (b_i - a_i) j_i \in R(v_p)J \subset I(v_p)$. Thus $y \in I(v_p)$ and so $y \in J = \cap I(v_p)$. Thus $x = y - (y-x) \in R(v_p)J$. ▨

Note if $\mathcal{O}$ is an order in A, then $R(v_p)\mathcal{O}$ is an $R(v_p)$-order in A and the above result holds with "ideal" replaced by "order".

Now ideals I and orders $\mathcal{O}$ are complete lattices so that
$k \otimes_R I \cong k \otimes_R \mathcal{O} \cong A$. by def.
$\Rightarrow$ Identifying I with its image $1 \otimes I$, this can be expressed as $kI = A$. Similarly for $\mathcal{O}$. Also the ideal I embeds in $R(v_p) \otimes_R I$ which is written $R(v_p)I$. //

Lemma 6.2.4 Let $\mathcal{O}$ be an R-order in a quaternion algebra A over k. Then $\mathcal{O}$ is maximal iff $R(v_p) \otimes_R \mathcal{O}$ is maximal for each prime P.

Proof) Supp. that $\mathcal{O}$ is maximal and i is the mapping identifying $\mathcal{O}$ with its image in $R(v_p) \otimes_R \mathcal{O}$, via $i(x) = 1 \otimes x$. Suppose $R(v_p) \otimes_R \mathcal{O}$ is contained in an $R(v_p)$-order Ω. Choose $\alpha \in R$ s.t. $\alpha\Omega \subset R(v_p) \otimes_R \mathcal{O}$. Now $i^{-1}(\alpha\Omega) = \Delta$ will be an ideal of A. Furthermore, $\mathcal{O} \subset \mathcal{O}_r(\Delta)$ since $R(v_p) \otimes_R \mathcal{O} \subset \Omega$.
$\Rightarrow$ Since $\mathcal{O}$ is maximal, $\mathcal{O} = \mathcal{O}_r(\Delta)$.
$\Rightarrow R(v_p) \otimes_R \mathcal{O} = R(v_p) \otimes_R \mathcal{O}_r(\Delta) = \mathcal{O}_r(R(v_p) \otimes_R \Delta)$
$= \mathcal{O}_r(\alpha\Omega) = \Omega$.
If, conversely, each $R(v_p) \otimes_R \mathcal{O}$ is maximal and $\mathcal{O} \subset \Omega$, then clearly $R(v_p) \otimes_R \mathcal{O} \subset R(v_p) \otimes_R \Omega$. for all p.

$\Rightarrow$ By maximality, $R(v_p)\otimes_R \mathcal{O} = R(v_p)\otimes_R \Omega$ and by Lemma 6.2.2,

$$\mathcal{O} = \bigcap R(v_p)\otimes_R \mathcal{O} = \bigcap R(v_p)\otimes_R \Omega = \Omega. \quad \blacksquare$$

Recall k_p is the completion of k w.r.t. the valuation v_p with ring of integers R_p.

Lemma 6.2.5 There is a bijection between $R(v_p)$-ideals (resp. orders) in a quaternion algebra A over k and the R_p-ideals (resp. orders) in the quaternion algebra $k_p\otimes_k A$ over k_p given by the mapping $I \longmapsto R_p\otimes_{R(v_p)} I$, which has the inverse $J \longmapsto J\cap A$.

Proof) Since $R(v_p)$ is a principal ideal domain, I will have a free basis $\{x_1, x_2, x_3, x_4\}$. Then $(R_p\otimes_{R(v_p)} I)\cap A$ consists of the $R_p\cap k = R(v_p)$-combinations of $\{x_1, x_2, x_3, x_4\}$.

$\Rightarrow (R_p\otimes_{R(v_p)} I)\cap A = I$.

Now suppose J is an R_p-ideal in $k_p\otimes_k A$ which will have a free basis $\{y_1, y_2, y_3, y_4\}$. Let A have basis $\{z_1, z_2, z_3, z_4\}$ so that $z_i = \sum b_{ij} y_j$ and $B = [b_{ij}]$ is an invertible matrix in $M_4(k_p)$. Since k is dense in k_p, (a topology is given by the metric $d(x,y) = v_p(x-y)$), choose $c_{ij}\in k$ s.t. the entries of $C=[c_{ij}]$ are close to those of B^{-1}.

$\Rightarrow CB$ is a unit in the ring $M_4(R_p)$.

Now let $z_i' = \sum c_{ij} z_j = \sum c_{ij}\left(\sum b_{jk} y_k\right) = \sum c_{ij} b_{jk} y_k$.

$\Rightarrow \{z_1', z_2', z_3', z_4'\}$ is a free basis of J and also a basis of A.

$\Rightarrow J\cap A$ is the set of $R(v_p)$-combinations of $\{z_1', z_2', z_3', z_4'\}$ and so is an $R(v_p)$-ideal in A s.t. $R_p\otimes_{R(v_p)}(J\cap A) = J$. $\blacksquare$

Def. 6.2.6 A: a quaternion algebra over the number field k.
R: the ring of integers of k.
$\Rightarrow A_p = k_p \otimes_k A$. If $\mathcal{O}$ is an R-order in A, let
$\mathcal{O}_p = R_p \otimes_R \mathcal{O} = R_p \otimes_{R(v_p)} (R(v_p) \otimes_R \mathcal{O})$.
so that $\mathcal{O}_p$ is an order in A_p. Likewise, define I_p for an ideal I in A.

Lemma 6.2.7 A, k, R. Let I be an R-ideal in A.
$\Rightarrow \exists$ a bijection between R-ideals J of A and sequences of ideals $\{(L_p) : P$ a prime, L_p an R_p-ideal in A_p s.t. $L_p = I_p$ for almost all $P\}$
given by $J \longmapsto (J_p)$.

Proof) If J is an ideal in A, $\exists\ a, b \in k^*$ s.t. $aJ \subset I \subset bJ$.
$\Rightarrow$ For almost all P, a and b are units in R_p so that $J_p = I_p$ for almost all P.
Now suppose we have a collection of ideals (L_p).
Let $J(v_p) = A \cap L_p$ which is an $R(v_p)$-ideal in A by Lemma 6.2.5. Furthermore, $J(v_p) = R(v_p)I$ for almost all P.
$\Rightarrow J = \bigcap J(v_p)$ is an R-ideal in A by Lemma 6.2.3 and the mapping $J \longmapsto (J_p)$ is surjective.
Now if ideals J and L have the same image, then $R(v_p)J = R(v_p)L$ for all P, so that, by Lemma 6.2.2, $J = L$ and the map is injective. ▨

Cor. 6.2.8 An order $\mathcal{O}$ is maximal iff $\mathcal{O}_p$ is maximal for all primes P in R.