§6.3. Discriminants.

k : a number field R : the ring of integers in k.

A : a quaternion algebra over k.

Def 6.3.1 Let $\mathcal{O}$ be an R-order in A. The discriminant of $\mathcal{O}$, $d(\mathcal{O})$, is the ideal in R generated by the set $\{\det(\mathrm{tr}(x_i x_j)), 1 \le i,j \le 4\}$, where $x_i \in \mathcal{O}$.

Note $\forall x_i x_j \in \mathcal{O} \Rightarrow \mathrm{tr}(x_i x_j) \in R$.

$\mathcal{O}$: a complete R-lattice $\Rightarrow \exists$ some set of four elements which are linearly independent over k.

$\Rightarrow$ the determinant in Def 6.3.1 for these elements is non-zero since the trace form is nondegenerate.

$\Rightarrow$ the discriminant is a non-zero ideal in R.

Theorem 6.3.2 If $\mathcal{O}$ has a free R-basis $\{u_1, u_2, u_3, u_4\}$, then $d(\mathcal{O})$ is the principal ideal $\det(\mathrm{tr}(u_i u_j))R$.

Proof) Clearly $\det(\mathrm{tr}(u_i u_j))R \subset d(\mathcal{O})$. Now let $x_1, \cdots, x_4 \in \mathcal{O}$ so that $x_i = \sum_{k=1}^{4} a_{ik} u_k$, $a_{ik} \in R$. Thus

$$\det(\mathrm{tr}(x_i x_j)) = (\det(a_{ik}))^2 \cdot \det(\mathrm{tr}(u_i u_k)).$$

$\Rightarrow$ the result follows. ▨

Example 6.3.3

1. If $\mathcal{O} = M_2(R)$, then $d(\mathcal{O}) = R$.

(∵) Let $x_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, x_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, x_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, x_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

$\Rightarrow \det(\mathrm{tr}(x_i x_j))R = (-1) \cdot R = R \subseteq d(\mathcal{O})$,

$\therefore d(\mathcal{O}) = R$.

2. $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$, with the standard basis $\{1, i, j, ij\}$.

$\mathcal{O} = \mathbb{Z}[1, i, j, ij]$, $\mathcal{O}' = \mathcal{O} + \alpha\mathbb{Z}$, $\alpha = (1+i+j+ij)/2$.

$\Rightarrow d(\mathcal{O}) = 16\mathbb{Z}$, $d(\mathcal{O}') = 4\mathbb{Z}$.

(∵ i) $\mathcal{O}$ has a free $\mathbb{Z}$-basis $\{u_1 = 1, u_2 = i, u_3 = j, u_4 = ij\}$.

$$\Rightarrow \det\left(tr(u_i u_j)\right) = \det\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix} = -16.$$

$\Rightarrow d(\mathcal{O}) = (-16)\mathbb{Z} = 16\mathbb{Z}$.

ii) $\mathcal{O}'$ has a free $\mathbb{Z}$-basis $\left\{u_1 = \frac{1+i+j+ij}{2}, u_2 = i, u_3 = j, u_4 = ij\right\}$

$$\Rightarrow \det\left(tr(u_i u_j)\right) = \det\begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & -2 & 0 & 0 \\ -1 & 0 & -2 & 0 \\ -1 & 0 & 0 & -2 \end{pmatrix} = -4.$$

$\Rightarrow d(\mathcal{O}') = (-4)\mathbb{Z} = 4\mathbb{Z}$. //

Note $\mathcal{O}$: an order in A over k, P: a prime ideal in R

$\Rightarrow d(R(v_p)\mathcal{O}) = d(\mathcal{O})R(v_p)$.

$\Rightarrow$ Each evaluation ring $R(v_p)$ is a principal ideal domain

$\Rightarrow$ We can use Theorem 6.3.2 to compute $d(R(v_p)\mathcal{O})$.

& By Lemma 6.2.2,

$$d(\mathcal{O}) = \bigcap_{\{P \text{ prime}\}} d(R(v_p)\mathcal{O}).$$

Now if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two orders in A with $\mathcal{O}_1 \subset \mathcal{O}_2$, clearly $d(\mathcal{O}_2) \mid d(\mathcal{O}_1)$. Supp. that $d(\mathcal{O}_1) = d(\mathcal{O}_2)$.

$\Rightarrow d(R(v_p)\mathcal{O}_1) = d(R(v_p)\mathcal{O}_2)$ for each P. ... (*)

Let $\{u_1, u_2, u_3, u_4\}$ be a free $R(v_p)$-basis of $R(v_p)\mathcal{O}_1$ and let $\{v_1, v_2, v_3, v_4\}$ be a free $R(v_p)$-basis of $R(v_p)\mathcal{O}_2$. Since $R(v_p)\mathcal{O}_1 \subset R(v_p)\mathcal{O}_2$, the transformation matrix T expressing

u_1, u_2, u_3, u_4 in terms of v_1, v_2, v_3, v_4 will have its entries in $R(v_p)$.

$\Rightarrow (\det T)^2 \det(\mathrm{tr}(v_i v_j)) = \det(\mathrm{tr}(u_i u_j)) \Rightarrow \det T$ is unit by (*).

$\Rightarrow T \in GL(4, R(v_p))$ and $R(v_p)\mathcal{O}_1 = R(v_p)\mathcal{O}_2$.

$\Rightarrow$ By Lemma 6.2.2, $\mathcal{O}_1 = \mathcal{O}_2$. $\Rightarrow$ we have proved following:

Theorem 6.3.4 Let A be a quaternion algebra over k. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be orders in A with $\mathcal{O}_1 \subset \mathcal{O}_2$. Then $d(\mathcal{O}_2) \mid d(\mathcal{O}_1)$ and $d(\mathcal{O}_1) = d(\mathcal{O}_2)$ if and only if $\mathcal{O}_1 = \mathcal{O}_2$.

Note $d(\mathcal{O})$ is a finitely generated R-module and each generator is a finite linear combination of elements of the form $\det(\mathrm{tr}(x_i x_j))$, where $x_1, x_2, x_3, x_4 \in \mathcal{O}$.

$\Rightarrow \exists$ a finite set $\mathcal{F}$ of 4-tuples s.t. $d(\mathcal{O})$ is the ideal gen. by $\det(\mathrm{tr}(x_i x_j))$, $\{x_1, x_2, x_3, x_4\} \in \mathcal{F}$.

$\Rightarrow$ For all but a finite number of prime ideals, $d(R(v_p)\mathcal{O}) = R(v_p)$. Let the finite number of exceptions be $P_1, \cdots, P_r$. In these cases, $d(R(v_{p_i})\mathcal{O}) = P(v_{p_i})^{n_i}$.

$$\Rightarrow d(\mathcal{O}) = \bigcap_{i=1}^{r} P(v_{p_i})^{n_i} \bigcap_{\{p\}} R(v_p) = R \cap \bigcap_{i=1}^{r} P(v_{p_i})^{n_i} = \bigcap_{i=1}^{r} P_i^{n_i} = \prod_{i=1}^{r} P_i^{n_i} \quad \cdots (**)$$

$\Rightarrow$ This can now be extended to the P-adic coefficients:

$$d(R_p \otimes_{R(v_p)} R(v_p)\mathcal{O}) = R_p \otimes_{R(v_p)} d(R(v_p)\mathcal{O}), \text{ i.e. } d(\mathcal{O}_p) = d(\mathcal{O})_p.$$

Recall that the unique prime ideal in R_p is PR_p.

$\Rightarrow$ (**) can be expressed as

$$d(\mathcal{O}) = \prod_{\{P \text{ prime}\}} d(\mathcal{O}_p).$$

As shown in (**), RHS is a finite product. //

§6.4. The Local Case - I.

Let K : a $\mathfrak{P}$-adic field, R : the ring of integers in K.

Recall (Corollary 2.6.4)

If A is a quaternion algebra over K, then A is isomorphic to exactly one of $M_2(K)$ or the unique division algebra $\left(\frac{\pi, u}{K}\right)$ where π is a uniformizer and u is a unit in R s.t. $K(\sqrt{u})$ is the unique unramified quad. extension of K. // $\quad \parallel F$.

$\Rightarrow$ We deal with the case $A = \left(\frac{\pi, u}{K}\right)$

$\Rightarrow$ A has a standard basis $\{1, i, j, ij\}$, where $i^2 = u$, $j^2 = \pi$.

Recall $\mathfrak{P} = \pi R$ is the unique maximal ideal and $\bar{K} = R/\mathfrak{P}$ is the finite residue field. If the non-Archimedean valuation $v : K \longrightarrow \mathbb{R}^+$ takes its value in $\{c^n \mid n \in \mathbb{Z}\}$, $0 < c < 1$, we let $v : K^* \longrightarrow \mathbb{Z}$ denote the logarithmic valuation $v = \log_c \circ v$.

$\Rightarrow$ We can define a valuation

$w : A^* \longrightarrow \mathbb{Z}$ by $w(x) = v(n(x))$, where n is the norm on A.

$\Rightarrow$ $\mathcal{O} = \{x \in A \mid w(x) \geq 0\}$ is the associated valuation ring and $\mathcal{Q} = \{x \in A \mid w(x) > 0\}$ is a two-sided ideal of $\mathcal{O}$.

Now we will show that $\mathcal{O}$ is the unique maximal order in A.

If $x \in A$ is an integer, then $n(x) \in R$ so that $w(x) \geq 0$.

$\Rightarrow$ $\mathcal{O}$ contains all the integers in A. Conversely, if $x \in \mathcal{O}$, then $\bar{x} \in \mathcal{O}$ ($\because n(x) = n(\bar{x})$) and so $x + \bar{x} \in \mathcal{O}$.

$\Rightarrow$ tr $x \in R$ so that x is an integer.

($\because x \in \mathcal{O} \Rightarrow v(n(x)) \leq 1 \Rightarrow n(x) \in R$, $K \cap \mathcal{O} = R$)

Furthermore, for any $x \in A$, $\exists\, r \in R$ such that $rx \in \mathcal{O}$.
($\because w(rx) = w(r) + w(x)$ for any $x \in A$). $\Rightarrow K\mathcal{O} = A$.
Thus $\mathcal{O}$ is the ring of all integers in A
$\Rightarrow \mathcal{O}$ contains every order in A by Lemma 2.2.1.
$\therefore \mathcal{O}$ is the unique maximal order in A.
In the same way, Q is a two-sided integral ideal so that Q is an ideal of the ring $\mathcal{O}$ in the usual sense.
Let $\{1, i, j, ij\}$ be the standard basis of $A \Rightarrow i^2 = u,\ j^2 = \pi$.
If $x \in \mathcal{O}$, then $w(xj) = w(x) + w(j) = w(x) + 1 > 0$.
($n(j) = -j^2 = -\pi \Rightarrow w(j) = 1$) $\Rightarrow xj \in Q \Rightarrow \mathcal{O}j \subseteq Q$.
Conversely, if $y \in Q$, then $w(yj^{-1}) \geq 0$ so that $Q = \mathcal{O}j$.
$\Rightarrow$ Note that $Q^2 = \mathcal{O}\pi$ by $j^2 = \pi$. By a similar argument, Q is a prime ideal. ($w(xy) > 0 \Rightarrow w(x) + w(y) > 0$, $w(x) \geq 0, w(y) \geq 0$
$\Rightarrow w(x) > 0$ or $w(y) > 0$)
Note that $A = F + Fj$. and $n|_F = N_{F|K}$. Since $F|K$ is unramified, π is also a uniformizer for F
($\because$ Let v' be the extension of v on F.
$\Rightarrow \forall y \in F$, $v'(y) = v\left(N_{F|K}(y)\right)^{1/[F:K]}$
$\Rightarrow$ for π, $v'(\pi) = v\left(N_{F|K}(\pi)\right)^{\frac{1}{2}} = \left((v(\pi))^2\right)^{\frac{1}{2}} = c^1$)
so that $R_F = \{x \in F \mid n(x) \in R\}$.
Now let $\alpha = x + yj \in A$. Then $\alpha \in \mathcal{O}$ iff $n(\alpha) \in R$. Further,
$n(\alpha) = (x+yj)(x-yj) = x^2 - y^2\pi = n(x) - n(y)\pi$. Since $n(x)$ and $n(y)$ are of the form $\pi^{2m}z$, where $z \in R^*$, we have that $n(\alpha) \in R$ iff $n(x), n(y) \in R$.
($\because n(\alpha) = n(x) - n(y)\pi = \pi^{2s} \cdot$ (an element of R) for some $s \in \mathbb{Z}$)

Thus, $\mathcal{O} = R_F + R_F j$. From this it follows that

$d(\mathcal{O}) = \delta_{F|K}^2 j^4 R = \pi^2 R$ since the discriminant ideal $\delta_{F|K}$ $= R$ as $F|K$ is unramified → direct calculation.

($\delta_{F|K}$ can be divided by ramified primes only).

Theorem 6.4.1 $\mathcal{O}$ is the unique maximal order in A and has discriminant $d(\mathcal{O}) = \pi^2 R = (PR)^2$.

Note Q is a two-sided integral ideal in $\mathcal{O}$. Indeed if I is any two-sided integral ideal in $\mathcal{O}$, then $I = \mathcal{O} j^m$ for some integer $m \geq 0$.

Note $\mathcal{O}^1 = A^1$, the normalizer $N(\mathcal{O}) = A^*$.

$w(\mathcal{O}^*) = 0$, $w(K^*) = 2\mathbb{Z}$

($\because x \in \mathcal{O}^* \Rightarrow n(x)$ is unit in R, $\alpha \in K^* \Rightarrow n(\alpha) = \alpha^2$)

$\Rightarrow$ We deduce that $[N(\mathcal{O}) : K^* \mathcal{O}^*] = 2$.

Lemma 6.4.2 $\exists$ a filtration of $\mathcal{O}^*$:

$$\mathcal{O}^* \supset 1+Q \supset 1+Q^2 \supset 1+Q^3 \supset \cdots$$

where $\mathcal{O}^*/(1+Q) \cong \bar{F}^* = (R_F/\pi R_F)^*$ and

$$(1+Q^i)/(1+Q^{i+1}) \cong \bar{F}^+$$

//