§2.4. Orthogonal Groups.

A: a quaternion algebra over the field F.

A^*: the group of invertible elements in A.

A_0: the pure quaternions of A.

$\Rightarrow A_0$ is a regular three dim. quadratic space with a bilinear form $B(x,y) = -\frac{1}{2}(xy+yx)$ & a quad. form $n(x) = -x^2$.

$(x \in A_0 \Rightarrow \bar{x} = -x)$.

Def The orthogonal group $O(A_0, n)$ is defined by

$$O(A_0,n) = \{T : A_0 \longrightarrow A_0 \mid T \text{ is linear}, n(Tx) = n(x)\ \forall x \in A_0\}.$$

The mapping $c : A^* \longrightarrow O(A_0,n)$, $\alpha \longmapsto c(\alpha)$, defined by

$$c(\alpha)(x) = \alpha x \alpha^{-1}, \quad \alpha \in A^*, x \in A_0$$

is a group homo. into $O(A_0,n)$, and its kernel is the center of A^*.

Recall (V,B): a regular quad. space.

$\Rightarrow O(V) :=$ the group of isometries of V. $\Rightarrow$ orthogonal group.

$$= \{\tau : V \longrightarrow V \mid B(\tau(v),\tau(w)) = B(v,w)\ \forall v,w\}.$$

$\Rightarrow$ A vector $v \neq 0 \in V$ is called isotropic if $q(v) = B(v,v) = 0$.

& " " anisotropic if " $\neq 0$.

For any anisotropic vector $v \in V$, we can define a reflection τ_v in the hyperplane orthogonal to v. This is given by

$$\tau_v(x) = x - \frac{2B(x,v)}{q(v)}v.$$

$\Rightarrow \tau_v \in O(V)$ (we can easily see this from a direct calculation).

fixes all vectors orthogonal to v and $\tau_v(v) = -v$.

$\Rightarrow \tau_v$ has determinat -1. $\left(\because \tau_v \Rightarrow *^{-1}\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & -1 \end{pmatrix} *\right)$

⇒ These reflections generate $O(V)$.

Theorem 0.9.11 If (V, B) is a regular quad. space of dim. n, then every isometry of $O(V, B)$ is a product of at most n reflections. //

⇒ In this situation, $O(A_0, n)$ is generated by reflections, where, for an anisotropic vector $y \in A_0$, the reflection τ_y is defined by

$$\tau_y(x) = x - \frac{2B(x,y)}{n(y)} y = x - \frac{xy+yx}{y^2} y = -yxy^{-1}.$$

Thus $\tau_y = -c(y)$. Now $\det(\tau_y) = -1$ and so $SO(A_0, n)$ (:= the subgroup of $O(A_0, n)$ consisting of the elements of $O(A_0, n)$ having determinant 1.) is generated by products $\tau_{y_1}\tau_{y_2}$, where y_1, y_2 are anisotropic vectors in A_0. However, $\tau_{y_1}\tau_{y_2} = c(y_1 y_2)$, with $y_1 y_2 \in A^*$. ⇒ $SO(A_0, n)$ lies in the image of c.

We now show that $SO(A_0, n; F)$ is precisely the image of c. If not, then every reflection in $O(A_0, n)$ lies in the image of c. Supp. that $\tau_i = c(\alpha)$ for some $\alpha \in A^*$ and i is one of the standard basis vectors. However, then $-Id$ lies in the image of c; say $c(\beta) = -Id$. ⇒ $c(\beta^2) = Id$ and $\beta^2 \in Z(A)$. Clearly $\beta \notin Z(A)$. so that $\beta \in A_0$. ⇒ $c(\beta)(x) = \beta x \beta^{-1} = -x$ for $\forall\, x \in A_0$. ⇒ $\beta x = -x\beta$ for $\forall\, x \in A_0$. Choosing $x = \beta$ gives a contradiction //

Theorem 2.4.1 $A^*/Z(A^*) \cong SO(A_0, n; F)$. //

§2.5. Quaternion Algebras over the Reals.

Note Lemma 2.1.2 : $\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2, by^2}{F}\right)$ for any $a, b \in F^*$.

Since every positive real number is a square in the reals, the Hilbert symbol of a quaternion algebra over $\mathbb{R}$ can have one of the forms $\left(\frac{1,1}{\mathbb{R}}\right)$, $\left(\frac{1,-1}{\mathbb{R}}\right)$ or $\left(\frac{-1,-1}{\mathbb{R}}\right)$.

⇒ The first two are isomorphic to $M_2(\mathbb{R})$. and the third, which is Hamilton's quaternions $\mathcal{H}$, is not iso. to $M_2(\mathbb{R})$.

Theorem 2.5.1 A quaternion algebra $\left(\frac{a,b}{\mathbb{R}}\right)$ is iso. to exactly one of $\mathcal{H}$ and $M_2(\mathbb{R})$, according to whether both a and b are negative or not. //

Now let k be a number field with $[k:\mathbb{Q}] = n$. Recall that there are n (Galois) field embeddings of k into $\mathbb{C}$ where $n = r_1 + 2r_2$.

Here r_1 = # of embeddings σ s.t. $\sigma(k) \subset \mathbb{R}$ (# of real places).

& r_2 = # of pairs $(\sigma, \bar{\sigma})$, where $\sigma(k) \not\subset \mathbb{R}$ (# of complex places)

Recall that if $k \subset L$, so that L is a field ext. of k, then

$$\left(\frac{a,b}{k}\right) \otimes_k L \cong \left(\frac{a,b}{L}\right).$$

More generally, let $\sigma : k \longrightarrow L$ be a field embedding. Then, w.r.t. that embedding, we obtain an isomorphism

$$\left(\frac{a,b}{k}\right) \otimes_\sigma L \cong \left(\frac{\sigma(a),\sigma(b)}{L}\right)$$

induced by

$$(a_0 + a_1 i_1 + a_2 j_1 + a_3 i_1 j_1) \otimes_\sigma \alpha \longmapsto \alpha \cdot \left(\sigma(a_0) + \sigma(a_1) i_2 + \sigma(a_2) j_2 + \sigma(a_3) i_2 j_2\right)$$

where $\{1, i_1, j_1, i_1 j_1\}$ is the standard basis of $\left(\frac{a,b}{k}\right)$

and $\{1, i_2, j_2, i_2 j_2\}$ " " of $\left(\frac{\sigma(a),\sigma(b)}{L}\right)$.

For any complex embedding σ,

$$\left(\frac{a,b}{k}\right)\otimes_\sigma \mathbb{C} \cong \left(\frac{\sigma(a),\sigma(b)}{\mathbb{C}}\right) \cong M_2(\mathbb{C}).$$

& for a real embedding $\sigma: k \to \mathbb{R}$,

$$\left(\frac{a,b}{k}\right)\otimes_\sigma \mathbb{R} \cong \left(\frac{\sigma(a),\sigma(b)}{\mathbb{R}}\right) \cong \mathcal{H} \text{ or } M_2(\mathbb{R}).$$

Def. 2.5.2 If $\sigma: k \to \mathbb{R}$ is a real embedding of k, then $\left(\frac{a,b}{k}\right)$ is said to be <u>ramified at σ</u> if $\left(\frac{\sigma(a),\sigma(b)}{\mathbb{R}}\right) \cong \mathcal{H}$. //

<u>Note</u> Recall that $v: k \to \mathbb{R}^+$ defined by $v(x) = |\sigma(x)|$ defines an (Archimedean) valuation on k.

$\Rightarrow$ k embeds naturally in the completion k_v. &, if σ is a real embedding, then $k_v \cong \mathbb{R}$.

$\Rightarrow \left(\frac{a,b}{k}\right)\otimes_k k_v \cong \left(\frac{\sigma(a),\sigma(b)}{\mathbb{R}}\right)$.

We thus speak of $\left(\frac{a,b}{k}\right)$ being ramified at k_v or ramified at the real place corresp. to σ.

Conversely, the quaternion algebra $\left(\frac{a,b}{k}\right)$ is <u>unramified</u> or <u>split</u> at k_v if $\left(\frac{a,b}{k}\right)\otimes_k k_v \cong M_2(\mathbb{R})$.

<u>Example 2.5.3</u> $k = \mathbb{Q}(\sqrt{2-\sqrt{5}}) \Rightarrow k$ has one complex place and two real places corresp. to the embeddings given by $\sigma(\sqrt{2-\sqrt{5}}) = \pm\sqrt{2+\sqrt{5}}$.

Let $A = \left(\frac{-1,-5+\sqrt{2-\sqrt{5}}}{k}\right)$. Then A is ramified at both the real embeddings since -1, $-5\pm\sqrt{2+\sqrt{5}}$ are all negative. //

Since $\begin{cases} -1 \longmapsto -1 < 0 \\ -5+\sqrt{2-\sqrt{5}} \longmapsto -5-\sqrt{21+\sqrt{5}} < 0 \end{cases}$

$\left(\frac{-1,-1}{\mathbb{R}}\right) \cong \mathcal{H}$

§2.6. Quaternion Algebras over P-adic Fields.

K : a P-adic field. R : the ring of integers of K.
$\Rightarrow$ With a uniformizer π, $P = \pi R$ is the unique maximal ideal & $\bar{K} = R/P$ is the finite residue field.
If the non-Archimedean valuation $v : K \longrightarrow \mathbb{R}^+$ takes its values in $\{ c^n \mid n \in \mathbb{Z} \}$, we let $\nu : K^* \longrightarrow \mathbb{Z}$ denote the logarithmic valuation $\nu = \log_c \circ v$.
Let A be a quaternion division algebra over K. Let us define

$$w : A^* \longrightarrow \mathbb{Z}$$

by $w(x) = \nu(n(x))$, where n is the norm on A.

Lemma 2.6.1 (a) $w(xy) = w(x) + w(y)$ for all $x, y \in A^*$.
(b) $w(x+y) \geq \min\{w(x), w(y)\}$ with equality when $w(x) \neq w(y)$.
Thus w defines a valuation on A.

Pf) (a)
$$\begin{aligned} w(xy) &= \nu(n(xy)) = \log_c \circ v(n(xy)) \\ &= \log_c (v(n(x)n(y))) \\ &= \log_c (v(n(x)) \cdot v(n(y))) \\ &= \log_c (v(n(x))) + \log_c (v(n(y))) \\ &= w(x) + w(y). \end{aligned}$$

(b) Let $\alpha \in A \setminus K$ so that $K(\alpha)$ is a quad. ext. of K and $n|_{K(\alpha)} = N_{K(\alpha)/K}$ $\Rightarrow$ $K(\alpha)$ is complete w.r.t the valuation $(v \circ N)^{1/2}$ (by Theorem 0.7.9). $\Rightarrow$ $\log_c \circ (v \circ N)^{1/2}$ is a discrete valuation on $K(\alpha)$. $\Rightarrow$ $\log_c \circ (v \circ N) = \nu \circ N$ is a discrete valuation on $K(\alpha)$.
$\Rightarrow$ $\nu \circ N = w|_{K(\alpha)}$ satisfies (b).
Thus for $x, y \in A^*$, we have

$w(x+y)-w(y) = w(xy^{-1}+1) \geq \text{Min}\{w(xy^{-1}), w(1)\}$
with equality if $w(xy^{-1}) \neq w(1)$ using the quad. ext. $K(xy^{-1})$.
$\Rightarrow$ Using (a) again,
$w(x+y) \geq \text{Min}\{w(xy^{-1}), w(1)\} + w(y)$
$= w(y) \cdot \text{Min}\{w(xy^{-1}), w(1)\}$
$= \text{Min}\{w(x), w(y)\}$ //

Extending the definition of w so that $w(0)=\infty$, yields this result:

Cor. 2.6.2 The set $\mathcal{O} = \{x \in A \mid w(x) \geq 0\}$ is a ring (the valuation ring of A) and $\mathcal{Q} = \{x \in A \mid w(x) > 0\}$ is a two-sided ideal of $\mathcal{O}$.

Recall (Theorem 0.1.13) the P-adic field K has a unique unramified quad. ext. $F = K(\sqrt{u})$, where $u \in R^*$, the gp of units of R. And the group $K^*/N(F^*)$ has order 2 with the non-identity element represented by π.
$\Rightarrow$ If we define $A = \left(\frac{u,\pi}{K}\right)$, then by Thm 2.3.1 (f), A is a division algebra.
(Thm 2.3.1 (b) $A = \left(\frac{a,b}{F}\right)$ is not a division algebra
$\Leftrightarrow$ (f) If $E = F(\sqrt{b})$, then $a \in N_{E|F}(E)$.
$\Rightarrow \pi \notin N_{F|K}(F) \Rightarrow A = \left(\frac{u,\pi}{K}\right)$ is a division algebra.)

Theorem 2.6.3 There is a unique quaternion division algebra over K and it is isomorphic to $\left(\frac{u,\pi}{K}\right)$, where $F = K(\sqrt{u})$ is the unique unramified quad. ext. of K. //

Proof) It remains to show that if A is any quaternion division algebra over K, then A is isomorphic to $\left(\frac{u,\pi}{K}\right)$.

The first step is to show that an unramified quad. ext. of K embeds in A. Recall that for any $\alpha \in A \setminus Z(A)$, $K(\alpha)/K$ is a quad. ext. Thus we need to choose α s.t. the max. prime ideal P of R is inert in the quad. ext.

To do this, we show that O/Q is a non-trivial finite field ext. of R/P.

For any $x \in A$, $n(\pi^m x) = \pi^{2m} n(x)$ lies in R for m large enough so that $\pi^m x \in O$. $\left(w(\pi^m x) = v(\pi^{2m} \cdot n(x)) \right.$
$\left. = 2m\, v(\pi) + v(n(x)) . \right)$

It follows that $A = K \cdot O$ and we choose a basis $\{x_1, x_2, x_3, x_4\}$ of A with $x_i \in O$. If we define B' by $B'(x,y) = n(x+y) - n(x) - n(y)$, then (A, B') is a regular quad. space.

$\Rightarrow$ There is a dual basis $\{x_1^*, x_2^*, x_3^*, x_4^*\}$ of $\{x_1, x_2, x_3, x_4\}$ w.r.t. B'. $\left(B'(x_i, x_j^*) = \delta_{ij} \right)$.

Let $x \in O$ and write $x = \sum a_i x_i^*$.

Then since $n(O) \subset R$, $a_i = B'(x, x_i)$
$= n(x + x_i) - n(x) - n(x_i) \in R$.

Thus $R[x_1, x_2, x_3, x_4] \subset O \subset R[x_1^*, x_2^*, x_3^*, x_4^*]$
and O is a (necessarily free) R-module of rank 4.

$\Rightarrow O/\pi O$ is a $\bar{K}$-space of dim. $= 4$, where $R/P = \bar{K}$.

Note $Q^2 \subset \pi O \subset Q$ & O/Q and Q/Q^2 are $\bar{K}$-spaces.

Indeed, O/Q, Q/Q^2 have the same dimension, for if we let $q \in Q$ be such that $w(q)$ is minimal, then for $y_i \in O$ chosen such that $\{y_i + Q\}$ is a $\bar{K}$-basis of O/Q, then $\{q y_i + Q^2\}$ is a $\bar{K}$-basis of Q/Q^2. $\Rightarrow \dim_{\bar{K}}(O/Q) = \dim_{\bar{K}}(Q/Q^2) > 1$.

However, $\mathcal{O}/Q$ is a field, for if $x \in \mathcal{O} \setminus Q$, then $w(x) = 0$. Hence $0 = w(1) = w(x \cdot x^{-1}) = w(x) + w(x^{-1}) \Rightarrow w(x^{-1}) = 0 \Rightarrow x^{-1} \in \mathcal{O} \setminus Q$. Thus $\mathcal{O}/Q$ is a division ring. However, as it is finite-dim. over the finite field $\bar{K}$, it is a finite division ring and so is a field, by a theorem of Wedderburn.

$\Rightarrow$ We choose $\alpha \in \mathcal{O}$ s.t. $\alpha + Q = \bar{\alpha}$ generates $\mathcal{O}/Q$ over $\bar{K}$.

$\Rightarrow F = K(\alpha)$ is a quad. ext. of K and by construction, it is unramified since $\bar{K}(\bar{\alpha})/\bar{K}$ is nontrivial. Thus by the uniqueness of such extensions (see Theorem 0.7.13), we can take $F = K(\alpha)$, where $\alpha^2 = u$ with $u \in R^*$.

$\Rightarrow$ The two roots $\pm\alpha$ of $x^2 - u$ give two embeddings of F in A and so by the Skolem Noether Thm. (Thm 2.9.8), $\exists\ \beta \in A^*$ s.t. $\beta\alpha\beta^{-1} = -\alpha \Rightarrow \{1, \alpha, \beta, \alpha\beta\}$ is a basis of A. Since β^2 commutes with α, ($\because \beta\alpha\beta^{-1} = -\alpha \Rightarrow \beta(\beta\alpha\beta^{-1})\beta^{-1} = -(-\alpha)$
$\Rightarrow \beta^2 \cdot \alpha \beta^{-2} = \alpha \Rightarrow \beta^2\alpha = \alpha\beta^2$.)

β^2 lies in the center of $A = K$. ($\because \beta^2$ commutes with all of basis elts) $\Rightarrow \{1, \alpha, \beta, \alpha\beta\}$ is a standard basis of A.

Let $\beta^2 = \pi^m u'$, where $u' \in U$ (unit group of K). Since we can remove squares $A = \left(\frac{u, \pi^\varepsilon u'}{K}\right)$ with $\varepsilon = 0$ or 1.

Now every unit $u' \in U$ is a norm of an elt in F.
(In Thm 0.7.13, $R^* \subset N_{F|K}(R_F^*)$, R_F : ring of ints of F).

$\Rightarrow \left(\frac{u, u'}{K}\right)$ splits over F. i.e. $\left(\frac{u, u'}{K}\right) \cong M_2(K)$ by Thm 2.3.1.

Thus $\varepsilon = 1$ and $\exists\ a, b \in K$ s.t. $a^2u + b^2u' = 1$ by Thm 2.3.1 (e).

$\Rightarrow b \neq 0$ ($\because$ If not, $a^2u = 1 \Rightarrow \left(\frac{u, \pi u'}{K}\right) \cong \left(\frac{a^2u, \pi u'}{K}\right) \cong \left(\frac{1, \pi u'}{K}\right)$
$\Rightarrow$ split. //)

We let $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b^{-1} & ub^{-1} \\ 0 & ab^{-1} & b^{-1} \end{pmatrix}$.

Under M, the forms $ux^2+\pi y^2-u\pi z^2$ and $ux^2+\pi u'y^2-u\pi u'z^2$ are equivalent.

$\Rightarrow$ By Cor. 2.3.5, $A \cong \left(\frac{u,\pi}{K}\right)$ ▨

Corollary 2.6.4 A : a quaternion algebra over P-adic K.
$\Rightarrow A$ is iso. to exactly one of $M_2(K)$ or the unique division algebra $\left(\frac{\pi,u}{K}\right)$.

Theorem 2.6.5 $A=\left(\frac{\pi,u}{K}\right)$. & L/K : a quad. ext.
Then A splits over L.

Recall (Definition) a P-adic field k_P is called dyadic if $N(P) = |R_P/P|$ is a power of 2. and otherwise non-dyadic. //

Theorem 2.6.6 Let K be a non-dyadic P-adic field. with integes R and maximal ideal P. Let $A=\left(\frac{a,b}{K}\right)$, where $a,b \in R$.

1. If $a,b \notin P$, then A is splits.
2. If $a \notin P$, $b \in P \setminus P^2$, then A splits iff a is a square mod P.
3. If $a,b \in P \setminus P^2$, then A splits iff $-a^{-1}b$ is a square mod P. //