## §2.2. Orders in Quaternion Algebras.

$R$ : a Dedekind domain

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

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

**Def. 2.2.1** If $V$ is a vector space over $k$, an **$R$-lattice** $L$ in $V$ is a finitely generated $R$-module contained in $V$. Furthermore, $L$ is a **complete $R$-lattice** if $L \otimes_R k \cong V$.
("complete" means that the generators of $L$ form a $k$-basis of $V$).

**Lemma 2.2.2** $L$ : a complete lattice in $V$.
$M$ : an $R$-submodule of $V$.
$\Rightarrow$ $M$ is a complete $R$-lattice if and only if there exists $a \in R$ s.t. $aL \subset M \subset a^{-1}L$.

Proof) ($\Rightarrow$) Let $\{x_1, \cdots, x_n\}$, $\{y_1, \cdots, y_n\}$ be generating sets of $L$, $M$ respectively. Since both $L$ and $M$ are complete, each generating set of them forms a $k$-basis of $V$.
$\Rightarrow$ We have the following relations

$$y_i = \sum_{j=1}^{n} a_{ij} x_j \quad , \ 1 \le i \le n, \ {}^{\forall} a_{ij} \in k.$$

$\Rightarrow$ We can make the fractional ideal (= say $I$) in $k$ which is generated by the elements $\{a_{ij}\}_{1 \le i,j \le n}$.

$\Rightarrow$ $\exists$ nonzero $\alpha \in R$ s.t. $\alpha I \subseteq R$. (Check : p.12. Def 0.3.3)

$\Rightarrow \forall y_i$, $\alpha y_i = \sum_{j=1}^{n} \alpha \cdot (a_{ij} \cdot x_j) = \sum_{j=1}^{n} (\alpha \cdot a_{ij}) x_j \in L$

since $\alpha \cdot a_{ij} \in R$ for $\forall i, j$.

Then, $\alpha \cdot M \subseteq L$.

Similarly, we also have the relations

$$x_i = \sum_{j=1}^{n} b_{ij} y_j$$

$\Rightarrow$ Let $J$ be the frac. ideal in $k$ generated by $\{b_{ij}\}$.

$\Rightarrow \exists\ \beta \neq 0 \in R$ s.t. $\beta \cdot J \subseteq R$.

$\Rightarrow \forall x_i$, $\beta x_i = \sum_{j=1}^{n} \beta (b_{ij} y_j) = \sum_{j=1}^{n} (\beta \cdot b_{ij}) y_j \in M$.

$\Rightarrow \beta \cdot L \subseteq M$.

Hence, if we put $a = \alpha\beta$, we can obtain

$$aL \subseteq M \subseteq a^{-1}L.$$

( $a \cdot L = (\alpha\beta) \cdot L = \alpha \cdot (\beta \cdot L) \subseteq \alpha \cdot M \subseteq M$

& $a \cdot M = (\alpha\beta) \cdot M = \beta \cdot (\alpha \cdot L) \subseteq \beta \cdot L \subseteq L$

since $L, M$ are $R$-modules. ).

($\Leftarrow$) $aL \subset M \Rightarrow L \subset \frac{1}{a} \cdot M$.

$\Rightarrow V = L \otimes_R k \subset (\frac{1}{a} \cdot M) \otimes_R k$.

$= M \otimes_R k$. (since $\frac{1}{a} \in k$).

$\subseteq V$

$\therefore M \otimes_R k = V$. $\Rightarrow M$ is complete. ▨

Def. 2.2.3 Let $A$ be a quaternion algebra over $k$. An element $\alpha \in A$ is an integer (over $R$) if $R[\alpha]$ is an $R$-lattice in $A$.

**Lemma 2.2.4** An element $\alpha \in A$ is an integer if and only if the reduced trace $tr(\alpha)$ and the reduced norm $n(\alpha)$ lie in $R$.

Proof) ($\Leftarrow$) Any $\alpha \in A$ satisfies the polynomial

$$x^2 - tr(\alpha)\,x + n(\alpha) = 0.$$

$\Rightarrow$ If $tr(\alpha)$, $n(\alpha)$ lie in $R$, then $R[\alpha]$ is generated by $1, \alpha$ as an $R$-module.

$\Rightarrow$ $\alpha$ is an integer.

($\Rightarrow$) Suppose that $\alpha$ is an integer. & $\alpha \in k$.

$\Rightarrow$ $R[\alpha]$ is a finitely generated $R$-module. So, $\alpha$ satisfies some monic polynomial over $R$.

$\Rightarrow$ $\alpha$ is integral over $R$. & since $R$ is integrally closed, $\alpha \in R$.

$\Rightarrow$ $tr(\alpha) = 2\alpha$, $n(\alpha) = \alpha^2$ lie in $R$.

Now suppose that $\alpha \in A \setminus k$. If $A$ is a division algebra so that $k(\alpha)$ is an integral domain, then $k(\alpha)$ is a quadratic extension of $k$, and say $k(\alpha) = L$.

Note that $\bar{\alpha}$ is the conjugate of $\alpha$ in $L/k$. i.e, $\bar{\alpha}$ is the image of $\alpha$ of the unique nontrivial automorphism of $L$ which is trivial on $k$.

Now $\alpha, \bar{\alpha} \in R_L$, the integral closure of $R$ in $L$.

($\because$ $\alpha$ is integral over $R$ since $R[\alpha]$ is fin. generated.

$\Rightarrow$ $\exists$ a monic poly. $f(x) \in R[x]$ s.t. $f(\alpha) = 0$.

$\Rightarrow$ $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$ (here, $R \subset k$ is invariant under the conjugation).

So, $\bar{\alpha} \in R_L$. //)

Note the fact that $R_L$ is also a Dedekind ring.

( [Janusz] "Algebraic Number Fields" §I.6. Thm 6.1.

$R$ : a Dedekind domain with quotient field $K$.

$L/K$ : a finite dim. ext. of $K$.

$\Rightarrow$ The integral closure of $R$ in $L$ is a Dedekind domain. ).

Then, $tr(\alpha), n(\alpha) \in R_L \cap k = R$.

( $tr(\alpha) = \alpha + \bar{\alpha} \Rightarrow tr(\alpha) \in R_L$, $n(\alpha) = \alpha\bar{\alpha} \Rightarrow n(\alpha) \in R_L$.

& We already saw that $tr(\alpha), n(\alpha) \in k$ for $\alpha \in A$ )

If $A$ is not a division algebra, then $A \cong M_2(k)$.

Let $\hat{k}$ be the algebraic closure of $k$. In $M_2(\hat{k})$, every matrix has the eigenvalues & using those of $\alpha$, we can write

$$\alpha = u \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot u^{-1} \quad \cdots (*)$$

for some unitary matrix $u$ over $\hat{k}$ and $a, b, c \in \hat{k}$.

Then $\alpha^n = u \cdot \begin{pmatrix} a^n & * \\ 0 & c^n \end{pmatrix} u^{-1}$ and if $f(\alpha) = 0$ for some $f(x) \in R[x]$, then $f(a) = f(c) = 0$. So, $a, c \in R$.

From $(*)$, we know that $tr(\alpha) = tr\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $n(\alpha) = n\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.

$$\Rightarrow tr\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \overline{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a+c & 0 \\ 0 & a+c \end{pmatrix}$$

$$= (a+c) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longmapsto (a+c) \cdot 1 \text{ in } A.$$

$$n\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & ac \end{pmatrix} = ac \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longmapsto ac \cdot 1 \text{ in } A.$$

Hence, $tr(\alpha), n(\alpha) \in R$. //



Remark In contrast to the case of integers in number fields, it is not always true that the sum and product of a pair of integers

In a quaternion algebra are necessarily integers.

example) $A = \left(\frac{-1,3}{\mathbb{Q}}\right)$. $k = \mathbb{Q}$, $R = \mathbb{Z}$ case.

$\{1, i, j, ij\}$ : the standard basis for $A$.

$\Rightarrow \alpha = j$, $\beta = \frac{3j+4ij}{5}$ are integers, but neither $\alpha+\beta$ nor $\alpha\beta$ are integers.

(Using Lemma 2.2.4 : $tr(\alpha) = tr(\beta) = 0$, $n(\alpha) = n(\beta) = -3$.
but, $tr(\alpha\beta) = \frac{18}{5} \notin \mathbb{Z}$ & $n(\alpha+\beta) = -\frac{48}{5} \notin \mathbb{Z}$. )

The role played by the ring of integers $R$ in a number field is replaced by that of an order in a quaternion algebra. //

Def. 2.2.5 $A$ : a quaternion algebra.

- An ideal $I$ in $A$ is a complete $R$-lattice.
- An order $\mathcal{O}$ in $A$ is an ideal which is also a ring with 1.
- An order $\mathcal{O}$ is maximal if it is maximal w.r.t. inclusion.

Examples 2.2.6

1. $\{x_1, x_2, x_3, x_4\}$ : a $k$-base of $A$.
→ the free module $R[x_1, x_2, x_3, x_4]$ is an ideal in $A$.

2. $A \cong \left(\frac{a,b}{k}\right)$, using $\left(\frac{ax^2, by^2}{k}\right) \cong \left(\frac{a,b}{k}\right)$, we may assume $a, b \in R$.
$\Rightarrow$ the free module $R[1, i, j, ij]$, where $\{1, i, j, ij\}$ is a standard basis, is an order in $A$.

3. $M_2(R)$ is an order in $M_2(k)$ & it is maximal.
(If it is not maximal, $\exists$ an order $\mathcal{O}$ properly containing $M_2(R)$

and $\mathcal{O}$ must contain an element $\alpha = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, where $a \notin R$.
$\Rightarrow R[\alpha]$ is not finitely-generated, as an $R$-submodule of $\mathcal{O}$.
$\Rightarrow$ It is impossible. // )

4. $I$: an ideal in $A$.
$\Rightarrow$ the order on the left of $I$ and the order on the right of $I$, defined respectively by

$$\mathcal{O}_l(I) = \{\alpha \in A \mid \alpha I \subset I\}, \quad \mathcal{O}_r(I) = \{\alpha \in A \mid I\alpha \subset I\}$$

are orders in $A$.

Lemma 2.2.7
1. $\mathcal{O}$ is an order in $A$ if and only if $\mathcal{O}$ is a ring of integers in $A$ which contains $R$ and is such that $k\mathcal{O} = A$.
2. Every order is contained in a maximal order.

Proof) 1. ($\Rightarrow$) $\alpha \in \mathcal{O}$, $\mathcal{O}$ : an order in $A$.
$\Rightarrow \mathcal{O}$ is an $R$-lattice $\Rightarrow R[\alpha]$ is an $R$-lattice
$\Rightarrow \alpha$ is an integer.
($\Leftarrow$) Choose a basis $\{x_1, x_2, x_3, x_4\}$ of $A$ s.t. each $x_i \in \mathcal{O}$.
Now the reduced trace defines a non-singular symmetric bilinear form on $A$.
( If $A$ is defined over $k$, consider the map

$$B' : A \times A \longrightarrow k, \quad \text{defined by } B'(\alpha, y) = \mathrm{tr}(\alpha y).$$

$\Rightarrow B'(x,y) = B'(y,x)$, $B'(x+y, z) = B'(x,z) + B'(y,z)$
$B'(x, y+z) = B'(x,y) + B'(x,z)$, $B'(\alpha x, y) = \alpha \cdot B'(x,y)$
$\Rightarrow$ symmetric, bilinear.

This bilinear form is said to be nonsingular when the matrix representing the quadratic form $Q(x) = B'(x,x)$ is nonsingular.

Set $A = \left(\frac{a,b}{k}\right)$, $\{1, i, j, ij=k\}$ the standard basis of $A$.

$\Rightarrow$ The matrix assoc. to $B'$ :

$$\begin{pmatrix} tr(1\cdot 1) & tr(1\cdot i) & \cdots & tr(1,k) \\ \vdots & & & \vdots \\ tr(i\cdot 1) & \cdots & & tr(k,k) \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2a & 0 & 0 \\ 0 & 0 & 2b & 0 \\ 0 & 0 & 0 & -2ab \end{pmatrix}, \text{ nonsingular.}$$

& The matrix $(tr(x_i x_j))$ is conjugate to the above matrix. )

Thus, $d = \det(tr(x_i x_j)) \neq 0$. Let $L = \{\sum a_i x_i \mid a_i \in R\}$.

$\Rightarrow L \subset \mathcal{O}$. Now suppose $\alpha \in \mathcal{O}$ so that $\alpha = \sum b_i x_i$ with $b_i \in k$.

For each $j$, $\alpha x_j \in \mathcal{O}$ and so $tr(\alpha x_j) = \sum b_i\, tr(x_i x_j) \in R$ by Lemma 2.2.4.

$\Rightarrow b_i \in (1/d) R$

( $\because$ $lb = (b_1\ b_2\ b_3\ b_4) \Rightarrow lb \cdot (tr(x_i x_j)) = lr$ for some $lr = (r_1\ r_2\ r_3\ r_4)$, $\forall r_i \in R$.

$\Rightarrow lb = lr \cdot (tr(x_i x_j))^{-1}$

& $(tr(x_i x_j))^{-1} = \frac{1}{d} \cdot$ ( some matrix with all entries are poly. in $r_i$'s ) ).

$\therefore \mathcal{O} \subset (1/d) \cdot L$

$\Rightarrow \mathcal{O}$ is finitely generated. ▨

Let us consider the special cases where $A = M_2(k)$. If $V$ is a 2-dimensional v.s. over $k$, then $A$ can be identified with $\mathrm{End}(V)$.

$L$ : a complete $R$-lattice in $V$

$\Rightarrow$ define $\mathrm{End}(L) = \{ \sigma \in \mathrm{End}(V) \mid \sigma(L) \subset L \}$.

Let $\{e_1, e_2\}$ be a basis for $V$. $\Rightarrow L_0 = Re_1 + Re_2$ is a complete $R$-lattice and $\mathrm{End}(L_0)$ is identified with $M_2(R)$. For any complete $R$-lattice $L$, $\exists\ a \in R$ s.t. $aL_0 \subset L \subset a^{-1}L_0$. It follows that $a^2\,\mathrm{End}(L_0) \subset \mathrm{End}(L) \subset a^{-2}\,\mathrm{End}(L_0)$

( For any $\sigma \in \mathrm{End}(L_0)$,

$a^2\sigma(L) \subset a^2 \cdot \sigma(a^{-1}L_0) \subset a \cdot \sigma(L_0) \subset aL_0 \subset L$.

$\Rightarrow a^2 \cdot \sigma \in \mathrm{End}(L) \Rightarrow a^2 \cdot \mathrm{End}(L_0) \subset \mathrm{End}(L)$. // ).

Thus each $\mathrm{End}(L)$ is an order //

**Lemma 2.2.8** $\mathcal{O}$ : an order in $\mathrm{End}(V)$.

$\Rightarrow \mathcal{O} \subset \mathrm{End}(L)$ for some complete $R$-lattice $L$ in $V$.

Proof) Let $L = \{ l \in L_0 \mid \mathcal{O}l \subset L_0 \}$. Then $L$ is an $R$-submodule of $L_0$. Also, if $a\,\mathrm{End}(L_0) \subset \mathcal{O} \subset a^{-1}\,\mathrm{End}(L_0)$ for some $a$, then $aL_0 \subset L$.

$\Rightarrow L$ is a complete $R$-lattice and $\mathcal{O} \subset \mathrm{End}(L)$. ▨

**Theorem 2.2.9** Let $L$ be a complete $R$-lattice in $V$. Then $\exists$ a basis $\{x, y\}$ of $V$ and a fractional ideal $J$ s.t. $L = Rx + Jy$.

**Corollary 2.2.10** If $R$ is a PID, all maximal orders in $M_2(k)$ are conjugate : //

## §2.3. Quaternion Algebras and Quadratic forms.

$A$: a quaternion algebra over $F$.

$\Rightarrow$ From the norm map on $A$, define a symmetric bilinear form $B$ on $A$ by

$$B(x,y) = \frac{1}{2}[n(x+y) - n(x) - n(y)] = \frac{1}{2}[x\bar{y} + y\bar{x}]$$

so that $A$ becomes a quadratic space. //

(Recall $V$: a fin-dim. v.s. / $k$. $B: V \times V \to k$ a symm. bilinear map.
$\Rightarrow (V, B)$ is a quadratic space.)

If $\{1, i, j, ij\}$ is a standard basis of $A$, then these vectors make an orthogonal basis of $A$.

(i.e. for each pair of distinct vectors of $\{1, i, j, ij\}$, $B$ vanishes.)

If $A = \left(\frac{a,b}{F}\right)$, then the quadratic form of this quadratic space $(A, B)$ is $B(x,x) = \frac{1}{2}[x\bar{x} + x\bar{x}] = n(x)$

$$= x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 \to \boxed{\text{norm form}}$$

& the assoc. matrix $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 \\ 0 & 0 & -b & 0 \\ 0 & 0 & 0 & ab \end{pmatrix}$, clearly nonsingular.

$\Rightarrow$ the quadratic space $(A, B)$ is regular.

If we restrict $n$, or $B$, to the pure quaternions $A_0$, then $A_0$ becomes a regular three dimensional quad. space.

$\Rightarrow$ On $A_0$, the forms $n$ and $B$ have particularly simple descriptions on $A_0$ since, for $x \in A_0$, $\bar{x} = -x$.

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

Recall a quad. space $V$ with a quad. form $q: V \to F$ is said to be isotropic if $\exists\, v \neq 0 \in V$ s.t. $q(v) = 0$.
(Otherwise, the space, or the form is said to be anisotropic)

Thm 2.3.1 $A = \left(\frac{a,b}{F}\right)$. TFAE :
(a) $A \cong \left(\frac{1,1}{F}\right)$ $(\cong M_2(F))$
(b) $A$ is not a division algebra.
(c) $A$ is isotropic as a quad. space with the norm form.
(d) $A_0$ " " "
(e) The quad. form $ax^2+by^2=1$ has a sol. with $(x,y) \in F \times F$.
(f) If $E = F(\sqrt{b})$, then $a \in N_{E|F}(E)$.

Proof) (a)$\Leftrightarrow$(b) : Theorem 2.1.7.
(b)$\Rightarrow$(c) : If $A$ is not a division algebra, it contains a nonzero noninvertible element $x$. $\Rightarrow n(x)=0$ for $x \neq 0$ & $A$ is isotropic.
(c)$\Rightarrow$(d) : Supp. $x = a_0 + a_1 i + a_2 j + a_3 k$, $k = ij$, is such that $n(x)=0$. If $a_0 = 0$, then $x \in A_0$ and $A_0$ is isotropic.
Thus assume that $a_0 \neq 0$ so that at least one of $a_1, a_2$ and $a_3$ must be nonzero.
$\Rightarrow$ Without loss, assume that $a_1 \neq 0$.
Now from $n(x) = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2 = 0$, we obtain
$$a_0^2 - ba_2^2 = a(a_1^2 - ba_3^2)$$
$\Rightarrow$ Let $y = b(a_0a_3 + a_1a_2)i + a(a_1^2 - ba_3^2)j + (a_0a_1 + ba_2a_3)k$.
$\Rightarrow$ A straightforward calculation gives $n(y)=0$.
Now suppose that $A_0$ is anisotropic.
$\Rightarrow y=0$ and, in particular, $a \cdot a_1^2 - aba_3^2 = 0$.

$\Rightarrow n(z)=0$ where $z=a_1 i+a_3 k$.

$\Rightarrow$ Again, if $A$ is anisotropic, $z$ must be $0 \Rightarrow a_1=0$, contradict to our assumption. $\therefore A_0$ is isotropic.

(d) $\Rightarrow$ (e). $A_0$ is isotropic $\Rightarrow n(x)=0$ for some $x=a_1 i+a_2 j+a_3 k$.

$\Rightarrow n(x)=-aa_1^2-ba_2^2+aba_3^2=0$. Observe that at least two of $a_1, a_2$ and $a_3$ non-zero.

$$a\cdot a_1^2+b\cdot a_2^2=aba_3^2$$

$\Rightarrow$ If $a_3\neq 0$, $\dfrac{a_1^2}{ba_3^2}+\dfrac{a_2^2}{aa_3^2}=b\cdot\left(\dfrac{a_1}{ba_3}\right)^2+a\cdot\left(\dfrac{a_2}{aa_3}\right)^2=1$.

$\Rightarrow\left(x=\dfrac{a_2}{aa_3},\ y=\dfrac{a_1}{ba_3}\right)$ is a solution for $ax^2+by^2=1$.

If $a_3=0$, then $a\cdot a_1^2+b\cdot a_2^2=0 \Rightarrow$ If we set

$x=(1+a)/2a$, $y=a_2(1-a)/2aa_1$

$\Rightarrow ax^2+by^2=1$ using $a\cdot a_1^2=-ba_2^2$. //

(e) $\Rightarrow$ (f): Let $ax_0^2+by_0^2=1$. If $x_0=0$, then $b=\left(\dfrac{1}{y_0}\right)^2$

$\Rightarrow \sqrt{b}\in F$ and $E=F$, in which case the result is obvious.

$\Rightarrow$ Assume that $x_0\neq 0$.

$$\Rightarrow a=\frac{1-by_0^2}{x_0^2}=\left(\frac{1-\sqrt{b}y_0}{x_0}\right)\left(\frac{1+\sqrt{b}y_0}{x_0}\right)$$

$$=N_{E|F}\left(\frac{1+\sqrt{b}y_0}{x_0}\right) \ \&\ \frac{1+\sqrt{b}y_0}{x_0}\in E=F(\sqrt{b}).$$

(f) $\Rightarrow$ (b) If $\sqrt{b}=c\in F$, then $c^2=b=j^2$.

$\Rightarrow (c+j)(c-j)=0$ and $A$ has zero divisors.

Now supp. that $\sqrt{b}\in F$. Then $a\in N_{E|F}(E)$ shows that $\exists\, x_1, y_1\in F$, not both zero, such that $a=N_{E|F}(x_1+\sqrt{b}y_1)=x_1^2-by_1^2$.

$\Rightarrow n(x_1+i+y_1 j)=x_1^2-a-by_1^2=0$ & $x_1+i+y_1 j\neq 0$ so that

A has non-zero non-invertible elements. ▨

**Definition 2.3.2** If the quaternion algebra A over F is such that $A \cong M_2(F)$, then A is said to be split over F.

**Remark** In §0.9, we introduced a Hilbert symbol $(a,b)$ which takes the values $\pm 1$ according as the quad. form $ax^2+by^2$ represents 1 or not.
⇒ The above thm relates the two definitions of Hilbert symbol.
Thus, $\left(\frac{a,b}{F}\right)$ splits if and only if $(a,b)=1$. //

**Corollary 2.3.3** The quaternion algebras $\left(\frac{1,a}{F}\right)$ and $\left(\frac{a,-a}{F}\right)$ are isomorphic to $M_2(F)$.

Proof) 1. $\left(\frac{1,a}{F}\right)$ : $x^2+ay^2=1$ has a sol. $(1,0)$ in $F\times F$.

2. $\left(\frac{a,-a}{F}\right)$ : the norm form on the pure quaternions is $-ax^2+ay^2+a^2z^2$ &
$i+j \neq 0$ $\leftrightarrow$ $n(i+j) = -a+a = 0$ where $\{1, i, j, ij\}$ is a standard basis of $\left(\frac{a,-a}{F}\right)$.
⇒ isotropic. ▨

**Example** (which are not iso. to 2×2 matrix algebra)
Let k be a number field and $A = \left(\frac{a,b}{k}\right)$. ⇒ We can assume that $a, b \in R_k$, the ring of integers in k.
Now the form $ax^2+by^2=1$ has a sol. in k iff $ax^2+by^2=z^2$ has a sol. in $R_k$.
⇒ For any ideal I of $R_k$, there will be a solution in the finite ring $R_k/I$. ⇒ We are enable to make examples $\not\cong M_2(k)$.

Take $A = \left(\frac{-1,p}{\mathbb{Q}}\right)$, where $p$ is a prime $\equiv -1 \pmod 4$.

$\Rightarrow$ Choosing $I = p\mathbb{Z}$, the congruence $-x^2 + py^2 \equiv z^2 \pmod p$ clearly has no solution. ($z \neq 0$)

$\Rightarrow \left(\frac{-1,p}{\mathbb{Q}}\right) \not\cong M_2(\mathbb{Q})$ by Thm 2.3.1 (e).

On the other hand, noting that Pell's equation

$$x^2 - py^2 = -1$$

has an int. solution if $p \equiv 1 \pmod 4$; $\Rightarrow \left(\frac{1,p}{\mathbb{Q}}\right) \cong M_2(\mathbb{Q})$. //

Thm 2.3.4 $A, A'$ : quaternion algebras over $F$.

$\Rightarrow A$ and $A'$ are isomorphic if and only if the quad. space $A_0$ and $A_0'$ are isometric.

Proof) Note with norm forms $n$ and $n'$ for $A_0, A_0'$, the last statement means that $\exists$ a linear isomorphism $\phi : A_0 \longrightarrow A_0'$ s.t.

$$n'(\phi(x)) = n(x) \quad \text{for all } x \in A_0.$$

($\Rightarrow$) Supp. that $\psi : A \longrightarrow A'$ is an algebra isomorphism. Since $x \in A_0 \iff x \notin Z(A) \,\&\, x^2 \in Z(A)$, $\psi$ must map $A_0$ to $A_0'$. Then for $x \in A_0$,

$\psi(x) \in A_0' \Rightarrow n'(\psi(x)) = -\psi(x)^2$ (for $x \in A_0'$, $\bar{x} = -x$)

$= \psi(-x^2) = \psi(n(x)) = n(x)$.

Thus $A_0$ and $A_0'$ are isometric.

($\Leftarrow$) Suppose $\phi : A_0 \longrightarrow A_0'$ is an isometry with $\{1, i, j, ij\}$ a standard basis of $A$. We will show that $\{\phi(i), \phi(j), \phi(i)\phi(j)\}$ is a basis of $A_0'$. Let $A = \left(\frac{a,b}{F}\right)$.

First note that $\phi(i)^2 = -n'(\phi(i)) = -n(i) = i^2 = a$

$\& \; \phi(j)^2 = b$.

Since $\bar{i}$ and $\bar{j}$ are orthogonal in $A_0$, $\phi(\bar{i})$ and $\phi(\bar{j})$ are orthogonal

(i.e. $B(\bar{i},\bar{j}) = \frac{1}{2}(\bar{i}\cdot(-\bar{j}) + \bar{j}(-\bar{i})) = 0$)

in $A_0'$. $\Rightarrow \phi(\bar{i})\phi(\bar{j}) + \phi(\bar{j})\phi(\bar{i}) = 0$.

Now $\phi(\bar{i})(\phi(\bar{i})\phi(\bar{j})) = -\phi(\bar{i})(\phi(\bar{j})\phi(\bar{i})) = -(\phi(\bar{i})\phi(\bar{j}))\phi(\bar{i})$.

$\Rightarrow \phi(\bar{i})\phi(\bar{j}) \notin Z(A')$ & $(\phi(\bar{i})\phi(\bar{j}))^2 = -ab \in Z(A')$.

Thus $\phi(\bar{i})\phi(\bar{j}) \in A_0'$. Now consider $a_1\phi(\bar{i}) + a_2\phi(\bar{j}) + a_3\phi(\bar{i})\phi(\bar{j}) = 0$.

$\Rightarrow \phi(\bar{i})(a_1\phi(\bar{i}) + a_2\phi(\bar{j}) + a_3\phi(\bar{i})\phi(\bar{j}))$ $\quad a_1 a + a_2\phi(\bar{i})\phi(\bar{i}) + a_3\phi(\bar{i})^2\phi(\bar{j})$

$= a_1 a^2 + (a_3 - a_2)\phi(\bar{i})\phi(\bar{j}) = 0$. $\quad a a_1 + a(a_2 + a_3)\phi(\bar{i}) = 0$

$\Rightarrow a_1 = 0$ & $a_2 = a_3$ $\quad \downarrow$ $a \neq 0 \Rightarrow a_1 = 0$ similarly $a_2 = a_3 = 0$

& in the same way, $a_2 = a_3 = 0$.

Thus, $\{1, \phi(\bar{i}), \phi(\bar{j}), \phi(\bar{i})\phi(\bar{j})\}$ forms a standard basis of $A'$,

so that $A' \cong \left(\frac{a,b}{F}\right) = A$. ▨

**Corollary 2.35** $A = \left(\frac{a,b}{F}\right)$, $A' = \left(\frac{a',b'}{F}\right)$

$\Rightarrow$ $A$ and $A'$ are isomorphic if and only if the quadratic forms $ax^2 + by^2 - abz^2$ and $a'x^2 + b'y^2 - a'b'z^2$ are equivalent over $F$.

Proof) The norm forms on $A_0$, $A_0'$ w.r.t. the standard basis are

$-ax^2 - by^2 + abz^2$. $\quad -a'x^2 - b'y^2 + a'b'z^2$.

$\Rightarrow$ Since $A_0, A_0'$ are isometric iff these two forms are equivalent, the statement follows. ▨

**Remark** We can use the equivalence classes of quadratic forms to distinguish quaternion algebras. //