Chapter III
Quarternion Algebras and norm forms

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

August 15 2013

1 Construction or Definition

Definition 1.1. *Let F be any field with $char(F) \neq 2$ and $a, b \in \dot{F}$. Define quarternion algebra $A = \left(\frac{a,b}{F}\right)$ as follows:*

A is generated, as an algebra, by two generators i, j. with relations

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

1. *Also let $k := ij \in A$. Then,*

$$k^2 = -ab, \quad ik = -ki = aj, \quad kj = -jk = bi$$

2. *So, i, j, k anticommute.*

3. *When $F = \mathbb{R}$, the usual quaternion is $\mathcal{H} := \left(\frac{-1,-1}{\mathbb{R}}\right)$.*

4. *A is spanned by $1, i, j, k$ as a VS over F.*

Lemma 1.2 (Construction)**.** $A = \left(\frac{a,b}{F}\right)$ is constructed as follows:

1. Let $P = F[[X, Y]]$ be the non-commutative polynomial algebra. This is also called the "free algebra" over F, generated by X, Y. In fact,

$$P = F[[X, Y]] = \bigoplus_{w \in \Omega} F \cdot w = F \cdot 1 \oplus \oplus F \cdot X \oplus F \cdot Y \oplus F \cdot XY \oplus F \cdot YX \cdots$$

where Ω is the set of all words in X, Y.

2. Let $\mathcal{I}$ be the two sided ideal of $F[[X, Y]]$ generated by

$$\{X^2 - a, Y^2 - b, XY + YX\}$$

3. Then,

$$A = \left(\frac{a, b}{F}\right) = \frac{F[[X, Y]]}{\mathcal{I}}$$

4. We write

$$i := \overline{X}, \quad j := \overline{Y}, \quad k := ij = \overline{XY}$$

Proposition 1.3 (1.0)**.** *$\{1, i, j, k\}$ is a basis for $A = \left(\frac{a,b}{F}\right)$. So,* $\dim A = 4$.

Proof. We use the construction. Write $i = \overline{X}, j = \overline{Y}$ and $k = ij$. It is clear that A is generated by $\{1, i, j, k\}$ spans A.

Linear Independence: Let E be the algebraic closure of F. Fix $\alpha, \beta \in E$ such that $\alpha^2 = -a, \beta^2 = b$. Let

$$i_0 = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} \quad j_0 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} \in \mathbb{M}(E).$$

Define

$$\varphi_0 : F[[X, Y]] \longrightarrow \mathbb{M}(E) \quad by \quad \varphi_0(X) = i_0, \quad \varphi_0(Y) = j_0.$$

Now,

$$\varphi_0(X^2 - a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - a = 0.$$

Similarly,

$$\varphi_0(Y^2 - a) = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} - b = 0.$$

Also,

$$\varphi(XY+YX) = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}\begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix} + \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}\begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{pmatrix} + \begin{pmatrix} -\alpha\beta & 0 \\ 0 & \alpha\beta \end{pmatrix} = 0.$$

So, φ_0 factors through as follows:

$$\begin{array}{ccc} F[[X,Y]] & \longrightarrow & \frac{F[[X,Y]]}{\mathcal{I}} \\ & \searrow^{\varphi_0} & \downarrow \varphi \\ & & \mathbb{M}(E) \end{array}$$

So, φ_0 factors as follows:

$$\varphi(k) = \varphi(ij) = \varphi_0(XY) = \begin{pmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{pmatrix}$$

Clearly,

$$1, i_0 = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}, j_0 = \begin{pmatrix} 0 & \beta \\ \beta & 0 \end{pmatrix}, \begin{pmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{pmatrix}$$

are linealry independent over E. Hence $1, i, j, k$ are linearly independent. The proof is complete. ■

Linear Independence: Possible Proof. Suppose $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k = 0$. This means, $\alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 XY \in \mathcal{I}$. Write

$$\alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 XY$$

$$= \sum f_1(X,Y)^k (X^2 - a) g_1^k(X,Y) + \sum f_2^k(X,Y)(Y^2 - b) g_2^k(X,Y)$$

$$+ \sum f_3^k(X,Y)(XY+YX) g_3^k(X,Y)$$

In fact

$$X^2 Y = X(XY+YX) - XYX = X(XY+YX) - (XY+YX)X + YX^2$$

or

$X^2Y \equiv YX^2$ *mod* $(XY+YX)$. *Similarly* $Y^2X = XY^2$ *mod* $(XY+YX)$.

Using this, we can write

$$\begin{aligned}\alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 XY \\ = f_1(X,Y)(X^2-a) + f_2(X,Y)(Y^2-b) \\ + \sum f_3^k(X,Y)(XY+YX)g_3^k(X,Y)\end{aligned}$$

One should be able to equate coefficients and complete the proof. I did not spend enough time on it. I live it as an exercise.

Lemma 1.4. *Two observations:*

1. *Symmetry:*
$$\left(\frac{a,b}{F}\right) = \left(\frac{b,a}{F}\right)$$

2. *Functoriality:*
$$If \quad F \hookrightarrow K \; is\; a\; field\; extension \quad K_F \otimes_F \left(\frac{a,b}{F}\right) \xrightarrow{\sim} \left(\frac{a,b}{K}\right) \quad as \;\; K\!-\!algebras.$$

Proof. Follows from construction. ∎

Proposition 1.5. *Let* $a, b \in \dot{F}$. *Then,*

1. $$\left(\frac{a,b}{F}\right) \xrightarrow{\sim} \left(\frac{ax^2, by^2}{F}\right) \quad \forall\; x,y \in \dot{F}.$$

2. $$\left(\frac{-1,1}{F}\right) \xrightarrow{\sim} \mathbb{M}_2(F)$$

3. $$CENTER\left(\frac{a,b}{F}\right) = F.$$

4. *$\left(\frac{a,b}{F}\right)$ has no nontrivial ideals (a simple algebra).*

5. **Remark**. Because of (3, 4), $\left(\frac{a,b}{F}\right)$ is a central simple algebra over F, which will be discussed in chapter IV.

Proof. Write $A = \left(\frac{a,b}{F}\right)$ and $A' = \left(\frac{ax^2,by^2}{F}\right)$. As usual let $1, i, j, k = ij$ be the "standard" basis of A. and $1, i', j', k' = i'j'$ be the "standard" basis of A'.

$$Then, \quad i^2 = a, j^2 = b, (i')^2 = ax^2, (j')^2 = by^2.$$

Define a map

$$\varphi_0 : F[[X, Y]] \longrightarrow \left(\frac{a,b}{F}\right) \quad by \quad \varphi(X) = xi, \quad \varphi(Y) = yj.$$

Consider the two sided ideal

$$\mathcal{J} = GeneratedBy\left(X^2 - ax^2, Y^2 - by^2, XY + YX\right)$$

Then, $\varphi(\mathcal{J}) = 0$. So, φ_0 factors as

$$\begin{array}{ccc} F[[X,Y]] & \xrightarrow{\varphi_0} & \left(\frac{a,b}{F}\right) \\ \downarrow & \nearrow_{\varphi} & \\ \left(\frac{ax^2,by^2}{F}\right) & & \end{array} \quad sending \quad i' \mapsto xi, j' \mapsto yj.$$

Since φ is $F-$algebra map, it is also a $F-$linear map. So, $1, \varphi(i') = xi, \varphi(j') = yj, \varphi(k') = xyk$ is also a basis. Therefore, φ is an isomorphism.

Proof of (2): In the proof of (1.3), take $a = -1, b = 1$ and $\alpha = \beta = 1$. That means, take

$$i_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad j_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad Note, \quad i_0 j_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

It is easy to check that $I_2, i_0, j_0, i_0 j_0$ is a basis of $\mathbb{M}_2(F)$. So, $i \mapsto i_0, j \mapsto j_0$ defines the isomophism needed.

Proof of (3): Let E be the algebraic closure of F. Then,

$$E\otimes_F\left(\frac{a,b}{F}\right)\approx\left(\frac{a,b}{E}\right)\approx\left(\frac{-\sqrt{-a}^2,\sqrt{b}^2}{E}\right)\approx\left(\frac{-1,1}{E}\right)\approx\mathbb{M}_2(E).$$

1. Center of $\mathbb{M}_2(E)$ is E (as EI_2). **Proof.** Exercise.
2. Claim: Center of $A := \left(\frac{a,b}{F}\right)$ is F.

   Proof. Note, for $x\in A$,

   $x\in Center(A)\iff xi=ix, xj=jx\iff x\in Center(\mathbb{M}_2(E))\iff x\in E.$

   So, $x\in A\cap E$. So, $x\in F$. So, (3) is established.
3. **Proof of (4)**: Suppose A has a nontrivial ideal I. Write $\mathcal{I}=I\otimes E$. So, $\dim_F I<4$ and hence $\dim_E\mathcal{I}<4$. Note $iI\subseteq I, jI\subseteq I, Ii\subseteq I, Ij\subseteq I$. Hence, $i\mathcal{I}\subseteq\mathcal{I}, j\mathcal{I}\subseteq\mathcal{I},\mathcal{I}i\subseteq\mathcal{I},\mathcal{I}j\subseteq\mathcal{I}$. Therefore, $\mathcal{I}$ is a nontrivial ideal of $\left(\frac{a,b}{F}\right)\approx\mathbb{M}_2(E)$, which is a contradiction.

■

1.1 Pure Quarternions

Definition 1.6. A quaternion $v=\alpha+\beta i+\gamma j+\delta k\in A:=\left(\frac{a,b}{F}\right)$ is called a pure quaternion if $\alpha=0$. The $F-$linear space of all pure quaternions is denoted by A_0.

Proposition 1.7. *Let $0\neq v\in A$. Then*

$$v\in A_0\iff v\notin F \quad and \quad v^2\in F.$$

Proof. Let $v=\alpha+\beta i+\gamma j+\delta k$. Then,

$$v^2=(\alpha^2+a\beta^2+b\gamma^2-ab\delta^2)+2\alpha(\beta i+\gamma j+\delta k).$$

The corollary follows form this identity. ■

Corollary 1.8. *If $A=\left(\frac{a,b}{F}\right)$ and $A'=\left(\frac{a',b'}{F}\right)$. Let $\varphi: A\xrightarrow{\sim} A'$ be a $F-$algebra isomorphism. The $\varphi(A_0)=A'_0$.*

Proof. Follows from (1.6). ■

1.2 The Real Quarternion

By (1.5), we have only three quartenion algebras:

$$\left(\frac{1,1}{\mathbb{R}}\right), \quad \left(\frac{-1,1}{\mathbb{R}}\right) \approx \mathbb{M}_2(\mathbb{R}), \quad and \quad \mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right).$$

We will study the third one, known as The Real Quarternion Algebra.

1. First, $\mathbb{C} = \mathbb{R} + \mathbb{R}i \subseteq \mathcal{H}$.

2. $\mathbb{C}$ is not in the center of $\mathcal{H}$. In this sense, $\mathcal{H}$ is not a $\mathbb{C}-$algebra.

3. $\mathcal{H}$ is a right $\mathbb{C}$ vector space with basis $\{1, j\}$. Any $v = x + yi + zj + wk$ can ne written as
$$v = (x + yi) + j(z - wi) = \alpha + j\beta \qquad for\ some \quad \alpha, \beta \in \mathbb{C}.$$

4. For $v \in \mathcal{H}$ define
$$L_v : \mathcal{H} \longrightarrow \mathcal{H} \quad by \quad L_v(z) = vz. \quad Then, \quad L_{vv'} = L_v o L_{v'}.$$

5. L_v is a $\mathbb{C}-$linear endomorphism of $\mathcal{H}$. To see this we check
$$L_v(z_1\alpha + z_2\beta) = v(z_1\alpha + z_2\beta) = L_v(z_1)\alpha + L_v(z_2)\beta.$$

6. L defines, $\mathbb{R}-$algebra homomorphism
$$L : \mathcal{H} \longrightarrow End_{\mathbb{C}}(\mathcal{H}) = \mathbb{M}_2(\mathbb{C}) \qquad wrt \quad basis \quad 1, j.$$

7. We have
$$L_i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad L_j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad L_k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \in \mathbb{M}_2(\mathbb{C}).$$
Needs care, because scalar multiplication comes from right:
$$\begin{pmatrix} L_i(1) \\ L_i(j) \end{pmatrix}^t = \begin{pmatrix} i \\ ij \end{pmatrix}^t = \begin{pmatrix} i \\ -ji \end{pmatrix}^t = \begin{pmatrix} 1 & j \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$
Note entries in the square matrix are scalars and the basis elements are from $\mathcal{H}$. Also
$$\begin{pmatrix} L_k(1) \\ L_k(j) \end{pmatrix}^t = \begin{pmatrix} k \\ kj \end{pmatrix}^t = \begin{pmatrix} -ji \\ -i \end{pmatrix}^t = \begin{pmatrix} 1 & j \end{pmatrix} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

8. This is left regular representation of $\mathcal{H}$ in $End(\mathcal{H})$.

9. We can compute $L_{x+iy}, L_{\alpha+j\beta}$ where $x, y \in \mathbb{R}$ and $\alpha, \beta \in \mathbb{C}$, by composition:

$$L_{x+yi} = L_x + L_y L_i = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} x+yi & 0 \\ 0 & \overline{x+yi} \end{pmatrix}$$

Use this to compute

$$L_{\alpha+j\beta} = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$$

10. L is a faithful representation:

$$L_v = 0 \Longrightarrow L_v(1) = v = 0.$$

11. So, $\mathcal{H}$ is isomorphic to the real subalgebra of $\mathbb{M}_2(\mathbb{C})$, consisting of matrices of the form:

$$L_{\alpha+j\beta} = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \qquad with \quad \alpha, \beta \in \mathbb{C}.$$

Recall the following:

Definition 1.9. Recall the following:

1. A matrix in $U \in \mathbb{M}_n(\mathbb{C})$ is called a unitary matix, if $UU^* = I_n = U^*U$.

2. The group $U(n)$ of all unitary matrices is called the unitary group.

3. The special unitary group $SU(n)$ is defined to be

$$SU(n) = \{U \in U(n) : \det(U) = 1\}.$$

Lemma 1.10. *We have*

$$SU(2) = \left\{ \sigma = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C} \ and \ \det(\sigma) = 1 \right\}$$

Proof. Omitted. Write down the equations and solve. ■

Corollary 1.11. The group of unit quaternions

$$U_0 = \{x + yi + zj + wk : x^2 + y^2 + z^2 + w^2 = 1\} \xrightarrow{\sim} SU(2)$$

Proof. Under the representation L, image of L is exactly $SU(2)$, by (1.10). More precisely,

$$L_{\alpha+\beta j} \begin{pmatrix} 1 & j \end{pmatrix} = \begin{pmatrix} 1 & j \end{pmatrix} \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}$$

■

Conjugation

Definition 1.12. For

$$v = x + yi + zj + wk \in \mathcal{H} \quad define \quad \overline{v} := x - yi - zj - wk$$

We say $\overline{v}$ is the conjugate of v.

1. If we write

$$v = (x + yi) + j(z - wi) = \alpha + j\beta \quad then \quad \overline{v} = \overline{\alpha} - j\beta$$

2. The representation $L : \mathcal{H} \longrightarrow \mathbb{M}_2(\mathbb{C})$ preserves the conjugation (involution) in the sense

$$(L_v)^* = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix}^* = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix} = L_{\overline{v}}.$$

2 Quaternions and Quadratic Spaces

Let $A := \left(\frac{a,b}{F}\right)$. In this section, we define a quadratic structure on the quaternion algebra A.

1. For $x = \alpha + \beta i + \gamma j + \delta k$, define $\overline{x} := \alpha - \beta i - \gamma j - \delta k$.
2. It follows, for $x, y \in A$ and $r \in F$
$$\overline{x+y} = \overline{x} + \overline{y}, \quad \overline{xy} = \overline{y} \cdot \overline{x}, \quad \overline{\overline{x}} = x, \quad \overline{rx} = r\overline{x}.$$
3. The map $x \mapsto \overline{x}$ is called the bar involution on A.
4. For $x \in A$ define, Norm Nx and Trace Tx of x as follows:
$$Nx := x\overline{x}, \quad Tx := x + \overline{x}.$$
5. In fact, $Nx \in F$ and $Tx \in F$. This is because
$$\overline{Nx} = \overline{x\overline{x}} = Nx, \quad \textit{and similarly}, \quad \overline{Tx} = Tx.$$
So,
$$\text{the norm maps} \quad N : A \longrightarrow F, \quad \textit{and} \quad \text{the trace maps} \quad T : A \longrightarrow F.$$
6. Define the bilinear form
$$B : A \times A \longrightarrow F \quad \textit{by} \quad B(x, y) := \frac{T(x\overline{y})}{2} = \frac{x\overline{y} + y\overline{x}}{2}$$
7. The quadratic map associated with B is
$$q_B(x) = B(x, x) = x\overline{x} = Nx.$$
This quadratic form is called the Norm form.
8. We claim: $\{1, i, j, k\}$ forms an orthogonal basis of A, which is checked easily:
$$B(1, i) = \frac{Ti}{2} = 0, \quad B(i, j) = \frac{T(ij)}{2} = \frac{T(k)}{2} = 0 \quad \textit{and so on}.$$

Corollary 2.1. The quadratic space (A, B) has an orthogonal basis and isometric to

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a\rangle \otimes \langle 1, -b\rangle$$

Proof. We saw $\{1, i, j, k\}$ is an orthogonal basis of A. We have

$$q(1) = N(1) = 1, \quad q(i) = N(i) = -i^2 = -a,$$

$$q(j) = N(j) = -j^2 = -b, q(k) = N(k) = -k^2 = ab.$$

The proof is complete. ∎

Observations and a Question:

1. $\det(A) = \det(\langle 1, -a, -b, ab\rangle) = 1$.
2. $1 \in D(A)$.
3. Lam comments: these $\langle 1, -a, -b, ab\rangle$ are precisely the four dimensional quadratic forms satifying condition (1, 2). (Give a proof).

Corollary 2.2. *For $x = \alpha + \beta i + \gamma j + \delta k$ we have*

$$Nx = \alpha^2 - \beta^2 a - \gamma^2 b + \delta^2 ab.$$

Proof. Use orthogonality. The proof is complete. ∎

Remarks.

1. For $x \in A$, we have $Nx = N\overline{x}$.
2. So, $x \mapsto \overline{x}$ is an isometry.
3. So, $B(x, y) = B(\overline{x}, \overline{y})$ for all x, y. Ofcourse

$$B(x, y) = \frac{T(x\overline{y})}{2} = \frac{T(\overline{x}y)}{2} = B(\overline{x}, \overline{y}).$$

4. For any $x \in A$ we have

$$x^2 - T(x)x + N(x) = 0.$$

5. For $x = \alpha + \beta i + \gamma j + \delta k \in \mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, we are not surprized

$$N(x) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

6. Exercise. If we use the model $L(\mathcal{H})$, then norm and trace corresponds exactly to that of matrices (over $\mathbb{C}$).

Proposition 2.3. *We have*

1. $x, y \in A \Longrightarrow N(x, y) = Nx \cdot Ny$.

2. $x \in A$ *is invertible if and only if* $Nx \neq 0$ *(which means* x *is anisotropic).*

Proof. $N(xy) = xy\overline{xy} = x(y \cdot \overline{y})\overline{x} = Nx \cdot Ny$. To prove (2), suppose x^{-1} exists. Then

$$1 = N(1) = N(x \cdot x^{-1}) = N(x)N(x^{-1}).$$

So, $Nx \neq 0$. Conversely, If $Nx \neq 0$ then

$$x \cdot \frac{\overline{x}}{Nx} = \frac{x \cdot \overline{x}}{Nx} = 1. \qquad So, \qquad x^{-1} = \frac{\overline{x}}{Nx}.$$

■

Contrast: To inner product spaces, with involution (like $\mathbb{C}$),

$$x^{-1} = \frac{\overline{x}}{\langle x, \overline{x} \rangle} = \frac{\overline{x}}{\| x \|^2}.$$

Corollary 2.4. *skip Corollary 2.4*

Theorem 2.5. Let $A = \left(\frac{a,b}{F}\right)$ and $A' = \left(\frac{a',b'}{F}\right)$. The following are equivalent:

1. A and A' are isomorphic as $F-$algebars.

2. A and A' are isometric as quadratic spaces.

3. A_0 and A'_0 are isometric as quadratic spaces.

Proof. (2) $\iff$ (3) by cancellation thoerem.

((1) $\Longrightarrow$ (2)): Let $\varphi : A \xrightarrow{\sim} A'$ be an $F-$algebra homomorphism. By corollary 1.8, $\varphi(A_0) = A'_0$. Let $x = \alpha + x_0 \in A$, with $\alpha \in F, x_0 \in A_0$. We prove $Nx = N(\varphi(x))$. We have $\varphi(x) = \alpha + \varphi(x_0)$. It follows $\overline{\varphi(x)} = \alpha - \varphi(x_0) = \varphi(\overline{x})$. So,

$$N(\varphi(x)) = \varphi(x) \cdot \overline{\varphi(x)} = \varphi(x \cdot \overline{x}) = x \cdot \overline{x} = Nx.$$

((3) $\Longrightarrow$ (1)): Let $\sigma : A_0 \xrightarrow{\sim} A'_0$ be an isometry. We have

$$-a = N(i) = N(\sigma(i)) = \sigma(i)\overline{\sigma(i)} = -\sigma(i)^2, \qquad So, \quad \sigma(i)^2 = a.$$

Similalrly, $\sigma(j)^2 = b$. Also,

$$i \perp j \Longrightarrow \sigma(i) \perp \sigma(j) \longrightarrow \sigma(i)\sigma(j) = -\sigma(j)\sigma(i).$$

This shows there is $F-$algebra homomorphism:

$$\tilde{\sigma} : A \longrightarrow A' \qquad i \mapsto \sigma(i), \; j \mapsto \sigma(j).$$

So, $\tilde{\sigma}(k) = \tilde{\sigma}(i)\tilde{\sigma}(j) = \sigma(i)\sigma(j)$.

One can see for $u, v \in A'$ the producs uv, vu have same constant term. Since, $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i)$, it follows $\omega := \sigma(i)\sigma(j) \in A'_0$.

Also $\sigma(i), \sigma(j), \sigma(k)$ is a basis os A'_0. Claim: $\omega \notin F\sigma(i) + F\sigma(j)$. If not, write $\sigma(i)\sigma(j) = \alpha\sigma(i) + \beta\sigma(j)$. Multiply by $\sigma(i)$ from left, we have

$$a\sigma(j) = \alpha a + \beta\sigma(i)\sigma(j)$$

Since, $1, \sigma(i), \sigma(j), \sigma(k)$ a basis, we have the constant term $\alpha a = 0$ and hence $\alpha = 0$. Similarly, $\beta = 0$. So, the claim is proved.

So, $1, \sigma(i), \sigma(j), \tilde{\sigma(k)} = \sigma(i)\sigma(j)$ is a basis. So, $\tilde{\sigma}$ is an isomorphism. ∎

Corollary 2.6.

$$\left(\frac{a,a}{F}\right) \xrightarrow{\sim} \left(\frac{a,-1}{F}\right) \quad and \quad \left(\frac{a,a}{F}\right) \cong \left(\frac{a,-1}{F}\right)$$

Proof. He wrote only $\cong$. Two quaternion algebras have the norm forms (see (2.1))

$$\langle 1, -a, -a, a^2 \rangle, \quad \langle 1, -a, 1, -a \rangle$$

But

$$\langle 1, -a, 1, -a \rangle \cong \langle 1, -a, -a, 1 \rangle \cong \langle 1, -a, -a, a^2 \rangle$$

Now, by (2.5), they are isomorphic. The proof is complete. ∎

Theorem 2.7. Let $A = \left(\frac{a,b}{F}\right)$. Then, the following are equivalent:

1. $A \cong \left(\frac{1,-1}{F}\right)$ (which is $\cong \mathbb{M}_2(F)$).
2. A is not a division algebra.
3. A is isotropic as a quadratic space.
4. A is hyperboloc as a quadratic space.
5. A_0 is isotropic as a quadratic space.
6. $(\langle a\rangle - 1)(\langle b\rangle - 1) = 0$ in $\widehat{W}(F)$ (or in $W(F)$).
7. The binary form $\langle a, b\rangle$ represents 1.
8. $a \in N_{E/F}(E)$, where $E = F(\sqrt{b})$ and $N_{E/F}$ is a field.

Note, by (2.5), $\cong$ may mean isomorphism or isometry. If any of these conditions hold, we say A splits over F.

Proof. ((1) $\iff$ (4)): (1) means Hyperabolic space (the RHS) as $F-$algebra. So, this is established by (2.5).

((4) $\implies$ (6))**:** In fact, A is isometric to $(\langle a\rangle - 1)(\langle b\rangle - 1)$, hence zero in $\widehat{W}(F)$.

((6) $\implies$ (4))**:** Following isometries follows from (6):

$$\langle 1, ab\rangle \cong \langle a, b\rangle \implies \langle 1, -a, -b, ab\rangle \cong \langle a, b\rangle \perp \langle -a, -b\rangle$$

which is hyperpolic.

((6) $\implies$ (7))**:** We have

$$\langle ab\rangle \perp \langle 1\rangle = \langle a\rangle \perp \langle b\rangle \quad \in \widehat{W}(F).$$

Hence

$$\langle ab, 1\rangle \cong \langle a, b\rangle$$

Since LHS represents 1, so does the RHS.

((7) $\Longrightarrow$ (6)): Since, $\langle a, b\rangle$ represents 1, $\langle a, b\rangle \cong \langle 1, ab\rangle$. So, $\langle 1, -a, -b, ab\rangle = 0 \in \widehat{W}(F)$. Therfore, we have

$$(1) \Longleftrightarrow (4) \Longleftrightarrow (6) \Longleftrightarrow (7)$$

((3) $\Longleftrightarrow$ ((4)): Clearly, (4) $\Longrightarrow$ (3). Now suppose A is isotropic. Then, $A \cong \mathbb{H} \perp q$, for some q. In any case, the determinant of the Norm form is $= a^2b^2 = 1$. So, $1 = \det(\mathbb{H}) \det q$. So, $\det q = -1$. So, $q \cong \mathbb{H}$, by (I.5.1). So, (4) follows.

((4) $\Longleftrightarrow$ ((5)): If A_0 has Witt index zero, then Witt indesx of A would be at most one. So, (4) $\Longrightarrow$ (5) $\Longrightarrow$ 3 $\Longrightarrow$ (4).

((1) $\Longrightarrow$ ((2)): Obvious, because the former is not a division algebra.

((2) $\Longrightarrow$ ((3)): Suppose A is ansotropic. Then, by (2.3), A would be a division algebra.

The proof is complete. ■