4. QUATERNION ALGEBRAS

§4.1. Hamilton and His Quaternions

Historically, quaternions were the step between complex numbers and matrices. Hamilton sought in vain to find a 3-dimensional analogue of the way complex numbers represent rotations in 2-dimensional space. His 8 year old son would ask him after breakfast, “Well Papa, can you multiply triplets?” whereupon his father sadly shook his head and said, “no, I can only add and subtract them.”

Eventually, in 1843, while walking along beside a canal in Dublin, he realized that he had to consider not triplets but quadruplets, or “quaternions”. He took out a penknife and carved in Brougham Bridge the key to the problem:

\[ i^2 = j^2 = k^2 = ijk = -1. \]

Here \( i, j, k \) represent 90° degree rotations about three mutually orthogonal axes. The other basic relationships:

\[
\begin{align*}
ij &= k = -ji; \\
jk &= i = -kj; \\
ki &= j = -ik
\end{align*}
\]

can be deduced from them, assuming the associative law.

A typical quaternion has the form:

\[ x_0 + x_1 i + x_2 j + x_3 k. \]

Addition and multiplication are defined in the obvious way, assuming the associative and distributive laws.

Example 1: Writing a typical quaternion as an element \((\lambda, v)\) of \(F \times V\), where \(i, j, k\) are a basis for \(V\), the operation of multiplication becomes:

\[
(\lambda_1, v_1). (\lambda_2, v_2) = (\lambda_1 \lambda_2 - v_1 \cdot v_2, \lambda_1 v_2 + \lambda_2 v_1 + v_1 \times v_2).
\]

§4.2. Quaternion Algebras

If \(a, b \in F\) then we define \([a, b]_F\) to be a vector space over \(F\) of dimension 4 with basis \(1, i, j, k\) (with \(F\) identified with the subspace spanned by 1) made into an \(F\)-algebra by defining multiplication as follows:

\[
\begin{array}{cccc}
1 & i & j & k \\
i & 1 & i & j \\
j & i & a & k \\
k & j & -k & b \\
\end{array}
\]

Example 2:

\([-1, -1]_\mathbb{R}\) is Hamilton’s quaternion algebra.

\([1, -1]_F \cong M_2(F)\), the algebra of \(2 \times 2\) matrices over \(F\), for any field \(F\).

Here \(1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ i \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ j \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ k \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.\)
§4.3. Quaternion Algebras and Quadratic Forms

If \( x = x_0 + x_1i + x_2j + x_3k \) is an element of the quaternion algebra \( A \), then the conjugate of \( x \) is defined by:

\[
\bar{x} = x_0 - x_1i - x_2j - x_3k.
\]

We define \( x \) to be a pure quaternion if \( x_0 = 0 \), that is, if \( \bar{x} = -x \).

**Notation:** \( A_0 \) denotes the set of pure quaternions in \( A \).

We make \( A \) into a quadratic space by defining:

\[
\langle x \mid y \rangle = \frac{1}{2} (x \bar{y} + y \bar{x}).
\]

Note that \( F \) and \( A_0 \) are orthogonal complements of one another and so \( A = F \oplus A_0 \) as quadratic spaces.

**Theorem 1:** If \( A = [a, b]_F \) then \( A \cong \langle 1, -a, -b, ab \rangle, F \cong \langle 1 \rangle \) and \( A_0 \cong \langle -a, -b, ab \rangle \).

**Proof:** Take the basis \( 1, i, j, k \).

**Corollary:** \( \det A \equiv 1 \).

**Theorem 2:** \([a_1, a_2]_F \cong [b_1, b_2]_F\) as \( F \)-algebras if and only if \( \langle -a_1, -a_2, a_1a_2 \rangle \cong \langle -b_1, -b_2, b_1b_2 \rangle \).

**Proof:** Let \( A = [a_1, a_2]_F \) and \( B = [b_1, b_2]_F \). Let \( \varphi: A \rightarrow B \) be an \( F \)-isomorphism.

1. \( \varphi(A_0) = B_0 \):
   - It is sufficient to show that \( \varphi(i), \varphi(j), \varphi(k) \in B_0 \).
   - Suppose \( \varphi(i) = x_0 + x_1i + x_2j + x_3k \).
   - Then \( a_1 = a_1\varphi(1) = \varphi(a_1) = \varphi(i^2) = \varphi(i)^2 \)
     \[= (x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_3^2) + 2x_0(x_1i + x_2j + x_3k).\]
   - Equating pure parts, \( x_0(x_1i + x_2j + x_3k) = 0. \)
   - If \( x_1i + x_2j + x_3k = 0 \) then \( \varphi(i) = x_0 = \varphi(x_0) \), a contradiction since \( \varphi \) is 1-1.
   - Hence \( x_0 = 0 \) and so \( \varphi(i) \in B_0 \). Similarly for \( \varphi(j) \) and \( \varphi(k) \).

2. \( \overline{\varphi(x)} = \varphi(\bar{x}) \):
   - Let \( x = y + z \) where \( y \in F \) and \( z \in A_0 \).
   - Then \( \varphi(x) = \varphi(y) + \varphi(z) = \varphi(y) - \varphi(z) = \varphi(y - z) = \varphi(\bar{x}) \).

3. \( \varphi \) is an isometry:
   - \( \langle \varphi(x) \mid \varphi(x) \rangle = \varphi(x)\overline{\varphi(x)} = \varphi(x)\varphi(\bar{x}) = \varphi(x\bar{x}) = x\bar{x} = \langle x \mid x \rangle \), since \( x\bar{x} \in F \).

Hence \( A_0, B_0 \) are isomorphic as quadratic spaces.

Now suppose that \( A_0 \cong B_0 \).

Then \( \langle -a_1, -a_2, a_1a_2 \rangle \cong \langle -b_1, -b_2, b_1b_2 \rangle \).

Let \( \varphi: A_0 \rightarrow B_0 \) be an isometry.

Then
\[
-\varphi(i)^2 = \varphi(i)\overline{\varphi(i)} = \langle \varphi(i) \mid \varphi(i) \rangle = \langle i \mid i \rangle = -i^2 = -a_1.
\]

Hence \( \varphi(i)^2 = a_1 \). Similarly \( \varphi(j)^2 = a_2 \) and \( \varphi(i)\varphi(j) = -\varphi(j)\varphi(i) \).

Since \( 1, \varphi(i), \varphi(j), \varphi(k) \) is a basis for \( B, B \cong [a_1, a_2]_F \) as \( F \)-algebras.
Corollary: Quaternion algebras are isomorphic if and only if they are isometric as quadratic spaces.

Proof: This follows from the fact that $A \cong B$ if and only if $A_0 \cong B_0$ (using the Witt Uniqueness Theorem).

Theorem 3: Either $[a, b]_F$ is a division ring or it is isomorphic to $M_2(F)$.

Proof: Suppose $A = [a, b]_F$ is not a division ring.

1. **A is isotropic as a quadratic space:**
   There exists $0 \neq x \in A$ with no multiplicative inverse.
   
   Now if $x \neq 0$ then $x \frac{x}{x} = 1$, a contradiction.
   
   Hence $\langle x \mid x \rangle = x \frac{x}{x} = 0$.

2. **A is hyperbolic as a quadratic space:**
   By Theorem 8 of chapter 2, $A \cong \langle 1, -1 \rangle \oplus \langle c, d \rangle$ for some $c, d \cong \langle 1, -1 \rangle \oplus \langle 1, -1 \rangle$ by Theorem 5 of chapter 2.

3. **A$_0$ is isotropic as a quadratic space:**
   A contains two linearly independent elements $x + x_0$ and $y + y_0$, with $x, y \in F$ and $x_0, y_0 \in A_0$ which are orthogonal and have zero length.
   We may assume without loss of generality that $x = y = 1$. (If $x$ or $y = 0$ we are done, otherwise we may divide.)
   Clearly $x_0 \neq y_0$. From $\langle 1 + x_0 \mid 1 + x_0 \rangle = \langle 1 + x_0 \mid 1 + y_0 \rangle = \langle 1 + y_0 \mid 1 + y_0 \rangle = 0$ we conclude that $\langle x_0 \mid x_0 \rangle = \langle x_0 \mid y_0 \rangle = \langle y_0 \mid y_0 \rangle = -1$ and hence $\langle x_0 - y_0 \mid x_0 - y_0 \rangle = 0$.

4. **A $\cong M_2(F)$ as F-algebras:**
   By Theorem 8 of chapter 2, $A_0 \cong \langle -a, -b, ab \rangle \cong \langle 1, -1 \rangle \oplus \langle -1 \rangle$.
   Hence by Theorem 2 above, $A_0 \cong [1, -1]_F \cong M_2(F)$.

Example 3:
Over $C$ the only possible quaternion algebras is $M_2(C)$.

Example 4:
Over $R$ the possible quaternion algebras are:

<table>
<thead>
<tr>
<th>Quaternion algebra</th>
<th>As a QS</th>
<th>Isomorphic to</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[1, 1]_R$</td>
<td>$\langle 1, -1, -1, 1 \rangle$</td>
<td>$M_2(R)$</td>
</tr>
<tr>
<td>$[1, -1]_R$</td>
<td>$\langle 1, -1, 1, -1 \rangle$</td>
<td>$M_2(R)$</td>
</tr>
<tr>
<td>$[-1, -1]_R$</td>
<td>$\langle 1, 1, 1 \rangle$</td>
<td>Hamilton’s quaternion algebra</td>
</tr>
</tbody>
</table>

Example 5: There are infinitely many Quaternion algebras over $Q$. In fact, if $p, q$ are distinct primes of the form $4n + 3$ then $[-1, p]_Q$ is not isomorphic to $[-1, q]_Q$. Dirichlet’s Theorem ensures that there are infinitely many such primes.
§4.4. The Witt Ring of a Finite Field

**Theorem 4:** There is only one quaternion algebra over a finite field, namely $M_2(F)$.

**Proof:** If $F$ is a finite field and $Q$ is a quaternion algebra over $F$ then $|Q| = |F|^4 < \infty$. By a theorem of Wedderburn every finite division ring is a field. Since $Q$ is non-commutative it must be isomorphic to $M_2(F)$.

**Theorem 5:** If there is only one quaternion algebra over the field $F$ then $W(F) = \{ \langle x \rangle \} + \{ \langle x \rangle \mid x \in F^#F^\# \} + \{ \langle 1, x \rangle \mid x \in F^#F^\# \}$.

Addition and multiplication is defined by:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>\langle x \rangle</th>
<th>\langle 1, x \rangle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>\langle x \rangle</td>
<td>\langle 1, x \rangle</td>
</tr>
<tr>
<td>\langle y \rangle</td>
<td>\langle y \rangle</td>
<td>\langle 1, xy \rangle \text{ if } x \neq -y</td>
<td>\langle -xy \rangle</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>\langle 1, x \rangle</td>
<td>\langle -xy \rangle</td>
</tr>
<tr>
<td>\langle 1, y \rangle</td>
<td>\langle 1, y \rangle</td>
<td>\langle 1, -xy \rangle \text{ if } x \neq y</td>
<td>0 \text{ if } x = y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>\langle x \rangle</th>
<th>\langle 1, x \rangle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>\langle y \rangle</td>
<td>0</td>
<td>\langle xy \rangle</td>
<td>\langle 1, x \rangle</td>
</tr>
<tr>
<td>\langle 1, y \rangle</td>
<td>0</td>
<td>\langle 1, y \rangle</td>
<td>0</td>
</tr>
</tbody>
</table>

**Proof:** Let $x, y, z \in F^\#$. Putting $a_1 = -\frac{1}{yz}$, $a_2 = -\frac{1}{xz}$, $b_1 = b_2 = 1$ in Theorem 2 we conclude that

$\langle yz, 1/xz, 1/xy \rangle \cong \langle -1, -1, 1 \rangle \cong \langle -1 \rangle \oplus H$.

Multiplying by $xyz$, $\langle x, y, z \rangle \cong \langle -xyz \rangle \oplus H$.

Hence every non-isotropic quadratic form has degree $\leq 2$.

Now, putting $z = -1$ we conclude that

$\langle x, y, -1 \rangle \cong \langle xy, 1, -1 \rangle$

whence, by Witt’s Cancellation Theorem, $\langle x, y \rangle \cong \langle 1, xy \rangle$.

Hence every element of $W(F)$ can be written in the form stated.

The addition and multiplication tables can be easily checked.

**Corollary:** Suppose there is only one quaternion algebra over $F$.

If $-1 \not\in F^\#_2$ then $W(F)$ has exponent 4.

If $-1 \in F^\#_2$ then $W(F)$ has exponent 2.

**Proof:** Every element of the form $\langle 1, x \rangle$ has order 2.

$\langle x \rangle \oplus \langle x \rangle \cong \langle 1, 1 \rangle$.

Hence $\langle x \rangle$ has order $\begin{cases} 4 & \text{if } -1 \not\in F^\#_2 \\ 2 & \text{if } -1 \in F^\#_2 \end{cases}$.

**Theorem 5:** If $F$ is a finite field of odd characteristic, $|F^\#/F^\#_2| = 2$.

**Proof:** $\{ \pm x \} \leftrightarrow x^2$ is a 1-1 correspondence.
Theorem 6: If $F$ is a finite field, $|W(F)| = 4$ and
\[
W(F) \cong \begin{cases} 
Z_4 & \text{if } -1 \not\in F^{#2} \\
Z_2(C_2) & \text{if } -1 \in F^{#2}.
\end{cases}
\]

Proof: If $-1 \not\in F^{#2}$, $W(F) = \{\langle 0 \rangle, \langle 1 \rangle, \langle -1 \rangle, \langle 1, 1 \rangle\} \cong Z_4$.
If $-1 \in F^{#2}$ and $s \not\in F^{#2}$, $W(F) = \{\langle 0 \rangle, \langle 1 \rangle, \langle s \rangle, \langle 1, s \rangle\} \cong Z_2(C_2)$. 