1967

Modules of Quaternions and Their Related Quadratic Forms.

Charles Carter Waid
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
https://digitalcommons.lsu.edu/gradschool_disstheses/1368

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
This dissertation has been microfilmed exactly as received 67-17,351

WAID, Charles Carter, 1939-
MODULES OF QUATERNIONS AND THEIR RELATED QUADRATIC FORMS.

Louisiana State University and Agricultural and Mechanical College, Ph.D., 1967
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan
MODULES OF QUATERNIONS AND THEIR RELATED QUADRATIC FORMS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Charles Carter Waid
B.S., New Mexico Institute of Mining and Technology, 1961
M.S., Louisiana State University, 1964
August, 1967
ACKNOWLEDGMENT

The author wishes to express his appreciation to Dr. Gordon Pall, under whose direction this dissertation was written, for his advice and encouragement.
<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>I QUATERNION ALGEBRAS</td>
<td>1</td>
</tr>
<tr>
<td>II ORDERS, IDEALS, AND MODULES</td>
<td>10</td>
</tr>
<tr>
<td>III THE LOCAL CASE</td>
<td>19</td>
</tr>
<tr>
<td>IV THE GLOBAL CASE</td>
<td>32</td>
</tr>
<tr>
<td>SELECTED BIBLIOGRAPHY</td>
<td>45</td>
</tr>
<tr>
<td>AUTOBIOGRAPHY</td>
<td>46</td>
</tr>
</tbody>
</table>
ABSTRACT

This thesis is concerned with modules and ideals of integral quaternions. The first two chapters are primarily concerned with developing the general properties of quaternion algebras and their integral subrings.

A simple definition of quaternion algebras is given in Chapter I, and their basic properties are derived. Using these properties, Pall’s characterization of quaternion algebras in terms of ternary quadratic forms is obtained. The remainder of the chapter is devoted to proving various isomorphism theorems.

The notion of integrality is introduced in Chapter II, and the general properties of rings of integral quaternions over principal ideal domains are developed. The correspondence, first discovered by Pall, between classes of integral ternary forms and principal orders is derived. Using this, the following interesting decomposition theorem is proven:

Every principal quaternion order \( \Theta \) admits a decomposition
\[
\Theta = R \oplus S \cdot x
\]
where \( R \) is a quadratic subring of \( \Theta \), \( S \) is a primitive ideal in \( R \) whose norm is \( s \), and \( x \in \Theta \).

In Chapter III, the maximal orders over the \( p \)-adic integers are studied. If \( \Theta = \Theta(f) \) is a maximal local order, it is shown that
\[
\Theta \cong M_2(\mathbb{Z}_p) \quad \text{when} \quad c_p(f) = 1 \quad \text{and that} \quad \Theta \text{ is a non-commutative valuation ring when} \quad c_p(f) = -1.
\]
Both of these rings are principal ideal rings and extensive use is made of this fact in proving locally the global theorems of Chapter IV. The crucial result is that if \( \alpha, \beta \in \Theta \) and
Na = Nb = (α, β) = 0 mod p, then α and β are both contained in the same maximal right ideal or both contained in the same maximal left ideal.

Principal orders over the rational integers are studied by localizing to the p-adic case. The rules for going back and forth between the local and global cases are given, and a unique primary decomposition theorem for modules is proven. The good primes for an order Θ are defined to be those primes for which the local order Θ_p is maximal. The ideal theory for those ideals whose norms are products of good primes is developed, and the following theorem is proven:

Let A be a primitive \( \frac{n}{2} \)-dimensional submodule of \( \Theta(f) \),
\[ G_A = mF_A \]
where \( m \) is the product of good primes and
\[ \det F_A = \det F_\Theta. \]
Then there exists a unique triplet of integers \((a, b, c)\) and unique right, two-sided, and left ideals, \( R, I, \) and \( L \), respectively, such that

1. \( A = R \cdot I \cdot L \)

2. \( m = abc \) with \( b \) the largest factor of \( m \) that is the product of primes for which \( c_p(f) = -1 \).

3. \( n(R) = a, n(I) = b, n(L) = c. \)

As an application of this theorem it is shown that if \( T \) is a \( 4 \times 4 \) orthogonal matrix, that is, if \( T^T = mI \), \( m \) a positive odd integer, then there exist matrices

\[
M = \begin{bmatrix}
    x_0 & -x_1 & -x_2 & -x_3 \\
    x_1 & x_0 & -x_3 & x_2 \\
    x_2 & x_3 & x_0 & -x_1 \\
    x_3 & x_2 & x_1 & x_0
\end{bmatrix}, \quad
N = \begin{bmatrix}
    y_0 & -y_1 & -y_2 & -y_3 \\
    y_1 & y_0 & y_3 & -y_2 \\
    y_2 & -y_3 & y_0 & y_1 \\
    y_3 & y_2 & -y_1 & y_0
\end{bmatrix}
\]
with \( x_0^2 + x_1^2 + x_2^2 + x_3^2 = m_1 \), \( y_0^2 + y_1^2 + y_2^2 + y_3^2 = m_2 \), \( m = m_1 m_2 \),

and a unit modular matrix \( U \) such that \( T = MNU = NMU \).
CHAPTER I

QUATERNION ALGEBRAS

There are many different ways of defining a quaternion algebra. Since this thesis is primarily concerned with rings of integral quaternions and their ideals we shall define the algebra in a way that will allow the speedy development of the basic properties we need.

Let $k$ be a field of characteristic $\neq 2$ and $\mathcal{A}$ a 4-dimensional vector space over $k$ with basis $\rho_0, \rho_1, \rho_2, \rho_3$. Let $a, b \neq 0 \in k$ and define multiplication for the $\rho_k$ by the following table.

\[
\begin{array}{c|cccc}
  & \rho_0 & \rho_1 & \rho_2 & \rho_3 \\
\hline
\rho_0 & \rho_0 & \rho_1 & \rho_2 & \rho_3 \\
\rho_1 & \rho_1 & a & \rho_3 & a\rho_2 \\
\rho_2 & \rho_2 & -\rho_3 & b & -b\rho_1 \\
\rho_3 & \rho_3 & -a\rho_2 & b\rho_1 & -ab \\
\end{array}
\]

We extend the multiplication by linearity and obtain an associative algebra $\mathcal{A}$ called the quaternion algebra $(\frac{a, b}{k})$. As usual we will imbed $k$ in $\mathcal{A}$ by identifying 1 and $\rho_0$.

Let $\alpha = a_0 + a_1\rho_1 + a_2\rho_2 + a_3\rho_3 \in \mathcal{A}$, $a_i \in k$.

We define the conjugate of $\alpha$ to be the quaternion
\[ \overline{\alpha} = a_0 - a_1a_1 - a_2a_2 - a_3a_3. \]

It is easily seen for \( c \in k \), \( \alpha, \beta \in \mathcal{G} \) that

\[ c \overline{\alpha} = c \overline{a}, \quad \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha \beta} = \overline{\beta} \overline{\alpha}. \]

We define the **norm** \( N \) and **trace** \( T \) of \( \alpha \) by the equations

\[ N\alpha = \alpha \overline{\alpha}, \quad T\alpha = \alpha + \overline{\alpha}. \]

It follows that

\[ N\alpha = a_0^2 - a_1^2 - a_2^2 + a_3^2, \quad T\alpha = T\overline{\alpha}. \]

For any \( \alpha, \beta \in \mathcal{G} \), we have

\[ N(\alpha\beta) = N\alpha \cdot N\beta, \quad T(\alpha + \beta) = T\alpha + T\beta. \]

A quaternion \( \alpha \) is called **pure** if \( T\alpha = 0 \). Since

\[ 0 = (\alpha - \overline{\alpha})(\alpha - \overline{\alpha}) = \alpha^2 - (T\alpha)\alpha + N\alpha \]

we see that every quaternion is a root of a quadratic polynomial in \( k[x] \). The following lemmas are easily verified \([5;142]\).\(^1\)

---

\(^1\)Pairs of Arabic numerals in brackets refer to correspondingly numbered references in the Selected Bibliography and page numbers, respectively. A single Arabic numeral in a bracket refers to the correspondingly numbered reference in the Selected Bibliography.
(1.1) **Lemma.** \( \alpha \in \mathcal{A} \) is invertible if and only if \( N\alpha \neq 0 \). If this condition is satisfied, then \( \alpha^{-1} = (N\alpha)^{-1} \alpha \).

(1.2) **Lemma.** \( \mathcal{A} \) is central simple.

(1.3) **Lemma.** If \( \alpha \) and \( \beta \) are elements of an associative algebra \( \mathcal{J} \) over \( k \) such that \( \alpha^2 = a, \beta^2 = b, \alpha\beta = -\beta\alpha \) with \( a, b \neq 0 \in k \), then the subalgebra \( \theta = k + k\alpha + k\beta + k\alpha\beta \) is isomorphic to \( \left( \frac{a,b}{k} \right) \).

An important application of (1.3) is that \( \left( \frac{1,-1}{k} \right) \) is isomorphic to the algebra \( M_2(k) \) of \( 2 \times 2 \) matrices over \( k \). For let \( e_{11}, e_{12}, e_{21}, e_{22} \) be the defining matrices of \( M_2(k) \). Then \( e_{11} + e_{22} \) is the identity matrix of \( M_2(k) \). Now set \( \alpha = e_{21} + e_{12} \) and \( \beta = e_{21} - e_{12} \). Then \( \alpha^2 = 1, \beta^2 = -1, \) and \( \alpha\beta = -\beta\alpha \).

If \( \xi = x_0 + x_1\rho_1 + x_2\rho_2 + x_3\rho_3 \in \mathcal{A} \), we have seen that

\[
N\xi = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2.
\]

If the \( x_i \) are considered as indeterminates over \( k \), then \( F(x_0, x_1, x_2, x_3) = N\xi \) is a quaternary quadratic form over \( k \) with non-zero square determinant. The form \( F \) is called the **norm form** of \( \mathcal{A} \) for the basis \( 1, \rho_1, \rho_2, \rho_3 \). If \( \alpha, \beta \in \mathcal{A} \), then

\[
(\alpha, \beta) = \alpha \overline{\beta} + \beta \overline{\alpha} = T(\alpha \overline{\beta})
\]

is a symmetric bilinear form. It has the following useful properties.

(1.4) \( \quad (1) \ N\alpha = \frac{1}{2}(\alpha, \alpha), \quad T\alpha = (1, \alpha) \)
(ii) \((\alpha\beta, \alpha\gamma) = N\alpha\cdot(\beta, \gamma)\), \((\beta\alpha, \gamma\alpha) = N\alpha\cdot(\beta, \gamma)\)

(iii) \((\alpha\beta, \gamma) = (\beta, \overline{\alpha} \gamma) = (\alpha, \gamma \overline{\beta})\).

Now consider an arbitrary basis \(\lambda_0, \lambda_1, \lambda_2, \lambda_3\) for \(G\) over \(k\) and let
\[\xi = \sum x_1 \lambda_1.\]
Then \(G(x_0, x_1, x_2, x_3) = N\xi = \frac{1}{2}(\xi, \xi) = \frac{1}{2}(\sum x_1 \lambda_1, \sum x_j \lambda_j)\)
\[= \sum_{i,j} \frac{1}{2}(\lambda_i, \lambda_j) x_i x_j\]
is a quaternary quadratic form called the **norm form** for the basis \(\lambda_0, \lambda_1, \lambda_2, \lambda_3\). Let \(T = (t_{ij})\) be the \(4 \times 4\) matrix taking the \(\rho\) basis onto the \(\lambda\) basis. That is, \(\lambda_1 = \sum_k \rho_k t_{ki}\). Then
\[(\lambda_i, \lambda_j) = (\sum_k \rho_k t_{ki}, \sum_m \rho_m t_{mj}) = \sum_k \sum_m t_{ki}(\rho_k\rho_m) t_{mj}.\]
Thus \(G = F^T\) and \(\det(G) = \det(T)^2 \det(F)\).

A basis \(\theta_0 = 1, \theta_1, \theta_2, \theta_3\) for \(G\) over \(k\) with \(\theta_1, \theta_2, \theta_3\) pure will be called a **pure basis**. We shall determine the multiplication table for such a basis. Since each of \(\theta_1, \theta_2, \theta_3\) is pure, the matrix taking the \(\rho\) basis onto the \(\theta\) basis is of the form
\[
\begin{pmatrix}
1 & 0 \\
0 & T
\end{pmatrix}
\]
where \(T = (t_{ij})\) is a \(3 \times 3\) matrix of non-zero determinant \(t\). Moreover, the norm form for the \(\theta\) basis is \(G = x_0^2 + \sum_{i,j=1}^3 \frac{1}{2}(\theta_i, \theta_j) x_i x_j\).
Let $\Delta_{ij} = \frac{1}{2}(\theta_i^* \theta_j)$ and $\Delta = (\Delta_{ij})$. We have the equations

$$\begin{bmatrix}
-a & 0 & 0 \\
0 & -b & 0 \\
0 & 0 & ab
\end{bmatrix} = T' \begin{bmatrix}
-a & 0 & 0 \\
0 & -b & 0 \\
0 & 0 & ab
\end{bmatrix} \begin{bmatrix}
T \\
1
\end{bmatrix}, \quad \det(\Delta) = (ab)^2.
$$

Let $\omega = (\omega_{ij}) = (ab)^{-1} \text{adj}(\Delta)$. Then $\text{adj}(\omega) = \Delta$. We will denote the symmetric group on $\{1,2,3\}$ by $S_3$. If $\sigma \in S_3$ then $|\sigma| = +1$ or $-1$ according as $\sigma$ is an even or odd permutation.

(1.5) Lemma. If $\sigma = (i,j,k) \in S_3$

\begin{align*}
(1, \rho_i \rho_j \rho_k) &= -|\sigma|ab \text{ if } \sigma = (i,j,k) \in S_3 \\
&= 0 \text{ if two of } i,j,k \text{ are equal.}
\end{align*}

Proof: An easy verification.

(1.6) Lemma. If $\sigma = (i,j,k) \in S_3$, then $(1, \theta_{i,j} \theta_{j,k}) = -|\sigma|ab$.

Proof: By repeated application of property (1.4.iii) of the inner product we have $(1, \theta_{i,j} \theta_{j,k}) = |\sigma|(1, \theta_{i,j} \theta_{j,k})$. But $(1, \theta_{i,j} \theta_{j,k}) = (1, \sum_{i,j,k} \rho_i \rho_j \rho_k) = (1, \sum_{i,j,k} \rho_i \rho_j \rho_k t_{i1} t_{i2} t_{i3})$

\begin{align*}
&= (1, \sum_{i,j,k} \rho_i \rho_j \rho_k t_{i1} t_{i2} t_{i3}) \\
&= (1, \sum_{\sigma \in S_3} |\sigma|t_{\sigma(1)}t_{\sigma(2)}t_{\sigma(3)}) = -ab.
\end{align*}

Q.E.D.

Using (1.4) and (1.6), we have, for $(i,j,k) \in S_3$, that
For $\sigma = (i, j, k)$, $P(\sigma)$ will denote the $3 \times 3$ matrix whose first, second, and third rows are the $i$th, $j$th, and $k$th rows, respectively, of the $3 \times 3$ identity matrix. Note that $P(\sigma)^{-1} = P(\sigma)'$. We can now find the multiplication table for the pure basis $1, \theta_1, \theta_2, \theta_3$. We have

$$\theta_i \theta_j = x_0 + x_1 \theta_1 + x_2 \theta_2 + x_3 \theta_3 \text{ with } x_i \in k. \text{ Thus}$$

$$\begin{align*}
(1, \theta_i \theta_j) &= 2x_0 \\
(\theta_i, \theta_i \theta_j) &= x_1(\theta_i, \theta_1) + x_2(\theta_i, \theta_2) + x_3(\theta_i, \theta_3) \\
(\theta_j, \theta_i \theta_j) &= x_1(\theta_j, \theta_1) + x_2(\theta_j, \theta_2) + x_3(\theta_j, \theta_3) \\
(\theta_k, \theta_i \theta_j) &= x_1(\theta_k, \theta_1) + x_2(\theta_k, \theta_2) + x_3(\theta_k, \theta_3)
\end{align*}
$$

Equating (1.7) and (1.8) and putting in matrix form we have

$$x_0 = -\Delta_{ij}$$

$$\begin{pmatrix}
0 \\
0 \\
1
\end{pmatrix} = P(\sigma) \cdot \begin{pmatrix}
x_1 \\
x_2 \\
x_3
\end{pmatrix}.$$
Solving for the $x_i$ we have

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = (|a|abc) \cdot \Delta^{-1} \mathbf{F}(\sigma)^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = |a|abc\mathbf{F}(\sigma)^{-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Thus the multiplication table for the $\theta$ basis is given by

$$\theta^2 = -\Delta_{ij}$$

(1.9)

$$\theta_i \theta_j = -\Delta_{ij} + |a|(\alpha_{ik} \theta_k + \alpha_{2k} \theta_2 + \alpha_{3k} \theta_3) \text{ for } \sigma = (i,j,k) \in S_3.$$

Let $f$ be a non-singular ternary form over $k$ with matrix $\delta$ and let $\Delta = \text{adj}(\delta)$. $\mathcal{A}(f)$ will denote the $4$-dimensional algebra over $k$ with basis $\theta_0 = 1, \theta_1, \theta_2, \theta_3$ satisfying the multiplication table given by (1.9).

(1.10) **Theorem.** Every quaternion algebra is an $\mathcal{A}(f)$ algebra and conversely every $\mathcal{A}(f)$ algebra is a quaternion algebra. Moreover,

$$F \mathcal{A} = x_0^2 + \text{adj } f(x_1, x_2, x_3).$$

**Proof:** Let $f = -bx^2 - ay^2 + z^2$, $a, b \neq 0 \in k$. Clearly $\mathcal{A}(f) \cong \left( \frac{a, b}{k} \right)$. Now let $f$, $\delta$, $\Delta$ be given. By using the fact that $\det(\Delta) = \det(\delta)^2$ is a non-zero square, it is easy to see that there exist $a, b \neq 0 \in k$ and a $3 \times 3$ matrix $T$ of determinant $t \neq 0$ such that
Thus det(Δ) = ± abt. We choose T or -T so that det(Δ) = abt. Thus there exists a pure basis 1, θ = gT of \((\frac{a}{b}, \frac{c}{d})\) which has the same multiplication table as the basis for \(A(f)\). Therefore \(A(f) \cong (\frac{a}{b}, \frac{c}{d})\).

Clearly \(P_A = x_1^2 + \text{adj} f(x_1, x_2, x_3)\).

Q.E.D.

(1.11) Theorem. If \(\text{adj}(f^*) = \text{adj}(f)^T\) and if \(\theta = (\theta_1, \theta_2, \theta_3)\) and \(\theta^* = (\theta_1^*, \theta_2^*, \theta_3^*)\), then there is a sign \(e = \pm 1\) such that the map \(A(f^*) \rightarrow A(f)\) defined by \(\tau(1) = 1, \tau(\theta^*) = \theta(eT)\) is an isomorphism.

Proof: By (1.10) there exist a, b \(\neq 0\) \(\in k\) and an isomorphism \(\alpha(f) \rightarrow \frac{a}{b} \frac{c}{d}\) defined by \(\mu(1) = 1, \mu(\theta) = \rho U\) for \(U\) a 3 \(\times\) 3 matrix such that

\[
Δ = U^t \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} U.
\]

Thus \(Δ^* = T^t Δ T = T^t U^t\)

\[
\begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix} UT
\]

and hence
by (1.10) there exists a sign $e = \pm 1$ such that the map $\mathcal{A}(f^*) \xrightarrow{\eta} (\frac{a}{b})$

defined by $\tau(1) = 1$, $\tau(\theta^*) = \rho(eUT)$ is an isomorphism. Let $\tau = \mu^{-1}\eta$.

Then $\tau(1) = 1$ and $\tau(\theta^*) = \mu^{-1}(\rho(eUT)) = \theta U^{-1} U^*(eT) = \theta \cdot eT$.

Q.E.D.

(1.12) **Theorem.** If $f^* = f^U$ and $T' = \text{adj } U'$, then the map $\mathcal{A}(f^*) \xrightarrow{\eta} \mathcal{A}(f)$ defined by $\tau(1) = 1$, $\tau(\theta^*) = \theta T$ is an isomorphism.

**Proof:** We may assume $\mathcal{A}(f) = (\frac{a}{b})$ and thus $\theta = \rho S$ for some $S$ of determinant $s \neq 0$. Then we must have $\delta = (\text{abs})^{-1}\text{adj}(\Delta)$ and thus

$$\det(\delta) = (\text{abs})^{-1}(\text{abs})^4 = \text{abs}.$$ Let $\theta' = \theta T = \rho ST$. Then again

$$\det(\theta') = \text{abs} u^2$$

where $u = \det(U)$. But $\det(\delta^*) = u^2 \det(\delta) = \text{abs} u^2$

and $\Delta^* = \text{adj}(\delta^*) = \text{adj} U' \Delta' \text{adj} U = T' \Delta T = \Delta' = \text{adj}(\theta')$. Thus

$\delta^* = \delta'$ and $\tau$ is an isomorphism.

Q.E.D.
CHAPTER II

ORDERS, IDEALS, AND MODULES

Let \( R \) be a principal ideal domain whose quotient field is \( k \) and let \( \mathcal{A} \) be a quaternion algebra over \( k \). A quaternion \( \alpha \in \mathcal{A} \) will be called \( R \)-integral or simply integral if \( T\alpha, N\alpha \in R \). A subset \( \Theta \) of \( \mathcal{A} \) will be called an \( R \)-order or simply an order if \( \Theta \) satisfies the following axioms.

(i) \( \Theta \) is a ring.

(ii) If \( \alpha \in \mathcal{A} \), then there exists \( m \neq 0 \in R \) such that \( m\alpha \in \Theta \).

(iii) \( \Theta \) is a finitely generated \( R \)-module.

By (ii), \( \Theta \) contains a basis for \( \mathcal{A} \) over \( k \), and (iii) implies that is a free \( R \)-module since \( R \) is a principal ideal domain. Thus \( \Theta \) is a \( 4 \)-dimensional \( R \)-module. If \( \omega_0, \omega_1, \omega_2, \omega_3 \) is an \( R \)-basis for the order \( \Theta \), we write \( \Theta = R\omega_0 + R\omega_1 + R\omega_2 + R\omega_3 = R[\omega_0, \omega_1, \omega_2, \omega_3] \) or simply \( \Theta = [\omega_0, \omega_1, \omega_2, \omega_3] \).

(2.1) \( \textbf{Theorem.} \) An order \( \Theta = [\omega_0, \omega_1, \omega_2, \omega_3] \) consists entirely of integral quaternions.
Proof: We can choose an R basis for \( \Theta \) with \( w_0 \in k \). But \( w_0 \cdot w_0 \in \Theta \) and hence \( w_0 \in R \). Moreover, \( w_1^2 = -Nw_1 + (Tw_1)w_1 \in \Theta \) and thus \( Tw_1, Nw_1 \in R \). Therefore, \( \vec{w}_1w_j = (Tw_1 - w_1)w_j \in \Theta \) and hence \( (w_i, w_j) = T(\vec{w}_i w_j) \in R \). Now let \( \xi = \sum x_i w_i \in \Theta, x_i \in R \). Then

\[
T(\xi) = \sum x_i Tw_i \in R, \text{ and }
\]

\[
N(\xi) = \frac{1}{2}(\xi, \xi) = \frac{1}{2} \sum (w_i, w_j)x_i x_j = \sum (Nw_i)x_i^2 + \sum (w_i, w_j)x_i x_j \in R.
\]

Q.E.D.

(2.3) Theorem. If \( \Theta \subset \mathcal{O} \) satisfying (i) and (ii) of (2.1) and if also

(iii') Every member of \( \Theta \) is integral,

then \( \Theta \) is an order.

Proof: If \( \alpha, \beta \in \Theta \) then \( \alpha \beta \in \Theta \) and hence \( T(\alpha \beta) \in R \). But \( T(\alpha \beta) = (1, \alpha \beta) = (T\alpha - \alpha, \beta) = T\alpha \cdot T\beta = (\alpha, \beta) \). Therefore, since \( T\alpha, T\beta \in R \) we have \( (\alpha, \beta) \in R \). By (2.1.ii), there exists a basis \( \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \Theta \) for \( \mathcal{O} \) over \( k \). Thus if \( \xi \in \Theta \), there exist \( x_i \in k \) such that \( \xi = \sum x_i \alpha_i \). Moreover, \( r_j = (\xi, \alpha_j) = \sum x_i (\alpha_i, \alpha_j) \in R \). If we let \( A \) be the matrix \( ((\alpha_i, \alpha_j)) \), then solving for the \( x_i \)'s gives
Since $A$ has coefficients in $R$, $\text{adj} \ A$ has coefficients in $R$ and \det \ A \ is \ in \ R$. Thus, $\Theta \subset (\det A)^{-1} \cdot R[\alpha_0, \alpha_1, \alpha_2, \alpha_3]$ and therefore is a finitely generated $R$-module.

\underline{Q.E.D.}

An order containing the identity will be called a principal order.

If $\Theta$ is a principal order and $A \subset \Theta$ such that

(i) $A$ is closed under addition,

(ii) $A \Theta \subset A$,

(iii) There exists an $m \neq 0 \in R$ such that $mA \subset \Theta$,

then $A$ is called a fractional right ideal in $\Theta$. Fractional left and two-sided ideals in $\Theta$ are defined analogously.

If $A$ is a fractional ideal in $\Theta$ and if $A \subset \Theta$, then $A$ is called an integral ideal or simply an ideal in $\Theta$. If $A$ is a fractional ideal in $\Theta$, then $mA \subset \Theta$ for some $m \neq 0 \in R$. Thus $mA$, and therefore $A$, is a free $R$-module. We will be interested primarily in 4-dimensional $R$-modules. We will often use the notation $[A]$, $(A)$, $(A)$ for right, left, and two-sided ideals, respectively.
Now let \( \Theta = [w_0, w_1, w_2, w_3] \) be a principal order and \( A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3] \) be a 4-dimensional \( R \)-module contained in \( \Theta \). In the following, we will define the symbols \( l(A) \), \( N(A) \), and \( n(A) \) to be certain non-zero ideals of \( R \); in the special case \( R = \mathbb{Z} \) (the rational integers) the symbol will be taken as denoting the positive integer generating the ideal, and in the case \( R = \mathbb{Z}_p \) (the \( p \)-adic integers), the power of \( p \) generating the ideal.

(2.5) Let \( l(A) = R \cap A \). Note that \( A \) has an \( R \)-basis \( \alpha_0, \alpha_1, \alpha_2, \alpha_3 \) with \( \alpha_0 \in R \) and thus, \( l(A) = (\alpha_0) \). Let \( \alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \) and \( \omega = (w_0, w_1, w_2, w_3) \). There is a \( 4 \times 4 \) matrix \( T \) with coefficients in \( R \) such that \( \alpha = \omega T \). Since \( A \) is 4-dimensional \( \det T \neq 0 \).

(2.6) Let \( N(A) = (\det T) \cdot R \). \( N(A) \) is called the norm of the module \( A \). In the case \( R = \mathbb{Z} \) or \( \mathbb{Z}_p \), it is well known \([4; 5]\) that \( N(A) \) is the number of residue classes in the difference module \( \Theta / A \).

Solving \( \alpha = \omega T \) for \( \omega \) we obtain \( \omega = \alpha \frac{\text{adj } T}{\det T} \). We now cancel all factors of \( \det T \) that divide all of the coefficients of \( \text{adj } T \) and obtain \( \omega = \alpha \frac{S}{h} \) where \( S \) is a \( 4 \times 4 \) matrix with coefficients in \( R \), \( h \in R \), and no divisor of \( h \) divides all the coefficients of \( S \). In fact, \( S \) is primitive as can be seen by the equation \( T \cdot \text{adj } T = (\det T) \cdot \text{I} \), which gives \( T \cdot S = h \cdot \text{I} \).

(2.7) Let \( n(A) = h \cdot R \). \( n(A) \) is called the reduced norm of \( A \). \( n(A) \) is the maximal ideal \( (b) \) in \( R \) for which \( (b) \cdot \Theta \subseteq A \). For if the prime ideal
(p) divides $n(A)$, then $p \mid h$ and there is a coefficient $s_{ij}$ of $S$ for which $p \nmid s_{ij}$. Now let $p^n \mid h$ and suppose $(b) \cdot \Theta \subseteq A$. Then $b\omega_j \in A$ and hence $\frac{bs_{ij}}{h} \in R$. Thus $p^n \mid b$ and therefore $n(A) \subseteq (b)$. It is clear that $l(A)$, $N(A)$, and $n(A)$ are independent of choice of basis for $A$ and $\Theta$ and that $l(A) \supseteq n(A) \supseteq N(A)$.

Let $\xi = \sum x_1 g_1 \in A$. We define the quadratic form $G_A$ by the equation $G_A = N\xi$. $G_A$ has coefficients in $R$ and can be expressed as the product of an element $m$ of $R$ and a primitive quadratic form $F_A$. Thus, $G_A = mF_A$. $G_A$ and $F_A$ are determined up to an $R$-unit modular transformation. For any choice of basis for $A$ we call $G_A$ the norm form of $A$ and $F_A$ the primitive part of the norm form of $A$. If $T$ is the matrix carrying $\Theta$ onto $A$ then $G_A = G^T_\Theta$ and thus $\det G_A = (\det T)^2 \cdot \det G_\Theta = N(A)^2 \cdot \det G_\Theta$. Clearly, $G_\Theta = F_\Theta$ and if $\det G_A$ is a unit multiple of $\det F_\Theta$ then $A = \Theta$.

(2.8) A subset $A$ of $\Theta$ is said to be primitive if whenever $A \subseteq b \cdot \Theta$ with $b \in R$, then $b$ is a unit of $R$.

(2.9) **Theorem.** If $A = [a]$ is a primitive principal right ideal in $\Theta$, then

(i) $a$ is primitive,
(ii) $(N\alpha) \cdot R = l(A) = n(A),$
(iii) $N(A) = n(A)^2$. 

Proof: (i) is clear. Thus \( \bar{\alpha} \) is primitive. It is also clear that \( 1(A) = n(A) \). Now suppose \( n(A) = mR \). Then there is a \( \beta \in \Theta \) such that \( \alpha \beta = m \). Hence, \( (Na) \cdot \beta = \bar{\alpha} \cdot \bar{\beta} = m \cdot \bar{\alpha} \) and \( \beta = \frac{m}{Na} \cdot \bar{\alpha} \). Since \( \bar{\alpha} \) is primitive we have \( Na \mid m \). But \( Na = \alpha \cdot \bar{\alpha} \in A \) and thus \( Na \cdot R = n(A) \).

It is clear that \( G_A = (Na) \cdot F_0 \). Thus \( \det G_A = (Na)^4 \cdot \det F_0 = N(A)^2 \cdot \det F_0 \). Therefore, \( N(A) = (Na)^2 \cdot R = n(A)^2 \).

Q.E.D.

An order \( \Theta \) of \( \mathcal{A} \) is said to be maximal if it is not properly contained in any order of \( \mathcal{A} \). If \( \Theta(f') \) properly contains \( \Theta(f) \), then the transformation carrying \( \Theta(f') \) onto \( \Theta(f) \) has non-unit determinant. Thus, since \( 4 \cdot \det f \) is in \( R \) if \( f \) has coefficients in \( R \), we have \( (4 \cdot \det f') \cdot R \) properly contains \( (4 \cdot \det f) \cdot R \). It follows that every order is contained in a maximal order. A maximal order must be principal since \( R + \Theta \) is an order if \( \Theta \) is an order.

We will now study principal orders more closely. The first thing we shall do is develop the multiplication table for a principal order and in doing so derive Pall's characterization of principal orders \([6; 285]\) which will be used throughout this thesis.

Let \( \Theta = [1, w_1, w_2, w_3] \) be a principal order and for convenience let \( b_i = Tw_i \) and \( c_{ij} = \frac{1}{2}(w_i, w_j) \). Then \( F_\Theta = x_0^2 + \Sigma b_i x_0 x_i + \Sigma c_{ij} x_i x_j \).

If \( \theta_i = w_i - \frac{1}{2}b_i \), then \( 1, \theta_1, \theta_2, \theta_3 \) is a pure basis for \( \mathcal{A} \) over \( k \) with multiplication table given by (1.9). Moreover, \( \Delta_{ij} = \frac{1}{2} (\theta_i, \theta_j) = c_{ij} - \frac{b_i b_j}{4} \). Thus,
\[ w^2_i = -(A_{ii} + \frac{1}{4} b_i^2) + b_i w_i \]

and, for \( \sigma = (i,j,k) \in S_3 \),

\[
(2.10) \quad w_i w_j = -(A_{ij} + \frac{1}{4} b_i b_j + \frac{1}{2}|\sigma| \sum_{m \neq k} a_{km} b_m) \\
+ (|\sigma|a_{ik} + \frac{b_i}{2})w_i + (|\sigma|a_{jk} + \frac{b_j}{2})w_j + |\sigma|a_{kk} w_k.
\]

Since the coefficients of \( w_1 \), \( w_2 \), and \( w_3 \) in the product \( w_i w_j \) must lie in \( R \), we have \( a_{kk}, 2a_{ij} \in R \) and thus \( a \) is the matrix of a ternary quadratic form with coefficients in \( R \). Furthermore, \( 2a_{ik} \equiv b_j \mod 2 \).

Since \( A_{ij} = a_{ik} a_{jk} - a_{ij} a_{kk} \) we have

\[
A_{ij} + \frac{1}{4} b_i b_j + \frac{1}{2}|\sigma| \sum_{m \neq k} a_{km} b_m \\
= (a_{ik} + \frac{1}{2}|\sigma|b_i)(a_{jk} + \frac{1}{2}|\sigma|b_j) + a_{kk}(\frac{1}{2}|\sigma|b_k - a_{ij})
\]

which is always integral. If we let \( w'_i = \frac{1}{2}b_i + \theta_i \) with \( b_i \equiv b_i \mod 2 \), then it is clear that \([1, w'_1, w'_2, w'_3] = [1, w_1, w_2, w_3] \). Thus we have proven

\[(2.11) \quad \text{Theorem.} \quad \text{Let } f \text{ be a ternary form with coefficients in } R \text{ and matrix } a. \text{ Choose } e_i = 0 \text{ or } 1 \text{ according as } 2a_{jk} \equiv 0 \text{ or } 1 \mod 2. \text{ Let } w_i = \frac{1}{2}e_i + \theta_i. \text{ Then } [1, w_1, w_2, w_3] \text{ is a principal order. Moreover, every principal order can be obtained in such a manner.} \]

We shall denote the principal order of (2.11) by \( \Theta(f) \).
(2.12) **Theorem.** Let \( f \) and \( f^* \) be non-singular ternary forms with coefficients in \( R \) and \( T \) be a \( 3 \times 3 \) matrix with coefficients in \( R \) such that \( \text{adj} \, f^* = (\text{adj} \, f)^T \). If \( \Theta(f) = [1, w_1, w_2, w_3] \) and \( \Theta(f^*) = [1, w_1^*, w_2^*, w_3^*] \), then \( \Theta(f^*) \sim [1, wT] \) where \( w = (w_1, w_2, w_3) \).

**Proof:** Let \( \Theta_1 = w_1 - \frac{1}{2}e_1, \Theta_1^* = w_1^* - \frac{1}{2}e_1^*, \Theta = (\Theta_1, \Theta_2, \Theta_3), \)
\( \Theta^* = (\Theta_1^*, \Theta_2^*, \Theta_3^*), \) \( \epsilon = (e_1, e_2, e_3), \epsilon^* = (e_1^*, e_2^*, e_3^*), \) and \( w^* = (w_1^*, w_2^*, w_3^*) \).

Then we have \( w = \frac{1}{2} \epsilon + \Theta \) and \( w^* = \frac{1}{2} \epsilon^* + \Theta^* \). Moreover, \( [1, wT] = [1, w(-T)] \) so we may assume the map \( \mathcal{G}(f^*) \rightarrow \mathcal{G}(f) \) defined by \( \tau(1) = 1, \tau(\Theta^*) = \Theta T \) is an isomorphism. Thus \( \tau(\Theta^*) = \tau(\frac{1}{2} \epsilon^* + \Theta^*) \)
\( = \frac{1}{2} \epsilon^* + \Theta T = wT + \frac{1}{2}(\epsilon^* - \epsilon T) \). Hence, \( [1, \tau(\Theta^*)] = [1, wT] \) if and only if \( \epsilon^* = \epsilon T \mod 2 \). However, we know that
\( F_\Theta = x_0^2 + \sum e_i x_i x_i + \sum c_{ij} x_i x_j \) and \( F_\Theta^* = x_0^2 + \sum e_i^* x_i x_i + \sum c_{ij}^* x_i x_j \)
have coefficients in \( R \), and that \( 4\Delta = 4(c_{ij}) - \epsilon'\epsilon \) and \( 4\Delta^* = 4(c_{ij}) - \epsilon^*\epsilon^* \). Hence, \( \epsilon'\epsilon^* = 4\Delta^* \cdot T^* 4\Delta T = T^*\epsilon'\epsilon T \mod 2 \). It follows that \( \epsilon^* = \epsilon T \mod 2 \) and thus that \( \Theta(f^*) \sim [1, wT] \).

Q.E.D.

(2.13) **Corollary.** If the determinant of \( T \) is a unit in \( R \), then \( \Theta(f^*) \sim \Theta(f) \). In particular, if \( U \) is a \( 3 \times 3 \) unit modular matrix over \( R \), then \( \Theta(f) \sim \Theta(f^U) \).

We have an interesting decomposition theorem for principal orders.
(2.14) **Theorem.** There is a basis $1, \omega_1, \omega_2, \omega_3$ for $\Theta(f)$ such that

$$\Theta(f) = [1, \omega_1] \oplus [\alpha_{33}, \omega_1] \frac{w_2}{\delta_{33}}$$

where $[\alpha_{33}, \omega_1]$ is an integral ideal of the quadratic ring $[1, \omega_1]$.

**Proof:** Let $\omega_1 = -\alpha_{23} + \theta_1$, $\omega_2 = -\alpha_{13} + \theta_2$, $\omega_3 = \alpha_{12} + \theta_3$. Then $\Theta(f) = [1, \omega_1, \omega_2, \omega_3]$. But

$$\omega_1 \omega_2 = \alpha_{13} \alpha_{23} - \alpha_{13} \theta_1 - \alpha_{23} \theta_2 - \Delta_{12} + \alpha_{13} \theta_1 + \alpha_{23} \theta_2 + \alpha_{33} \theta_3$$

$$= \alpha_{13} \alpha_{23} - (\alpha_{13} \alpha_{23} - \alpha_{12} \alpha_{33}) + \alpha_{33} \theta_3$$

$$= \alpha_{33} \omega_3.$$ 

Thus $\Theta(f) = [1, \omega_1] \oplus [\alpha_{33}, \omega_1] \frac{w_2}{\delta_{33}}$. For $[\alpha_{33}, \omega_1]$ to be an ideal in $[1, \omega_1]$ it is necessary and sufficient that $\alpha_{33} \mid N(\omega_1)$. But

$$N(\omega_1) = \frac{1}{2} (-\alpha_{23} + \theta_1 - \alpha_{23} + \theta_1) = \alpha_{23}^2 + \Delta_{11}$$

$$= \alpha_{23}^2 + (\alpha_{22} \alpha_{33} - \alpha_{23}^2)$$

$$= \alpha_{22} \alpha_{33}.$$ 

Q.E.D.
CHAPTER III

THE LOCAL CASE

In the following \( \mathbb{Q} \) will denote the rational numbers, \( \mathbb{Z} \) the rational integers, and \( p \) a rational prime. \( \mathbb{Q}_p \) will denote the \( p \)-adic completion of the rationals, \( \mathbb{Z}_p \) the \( p \)-adic integers and \( \mathcal{O} = \mathcal{O}(\mathfrak{f}) \) a quaternion algebra over \( \mathbb{Q}_p \). We will study the theory of maximal \( \mathbb{Z}_p \)-orders in \( \mathcal{O} \).

(3.1) **Theorem.** Let \( c_p(\mathfrak{f}) \) denote the Hasse symbol. If \( c_p(\mathfrak{f}) = c_p(g) \), then \( \mathcal{O}(\mathfrak{f}) \sim \mathcal{O}(g) \).

**Proof:** It is easily shown that \( c_p(\mathfrak{f}) = c_p(\text{adj } \mathfrak{f}) \). Now suppose \( c_p(\mathfrak{f}) = c_p(g) \). Then \( c_p(\text{adj } \mathfrak{f}) = c_p(\text{adj } g) \) and moreover the determinants of \( \text{adj } \mathfrak{f} \) and \( \text{adj } g \) are squares. Thus \( \text{adj } \mathfrak{f} \) and \( \text{adj } g \) are equivalent over \( \mathbb{Q}_p \). Therefore, by (1.11), \( \mathcal{O}(\mathfrak{f}) \sim \mathcal{O}(g) \).

We must therefore separate the study of the local algebra into two cases according as \( c_p(\mathfrak{f}) = -1 \) or \( c_p(\mathfrak{f}) = +1 \).

A. The case \( c_p(\mathfrak{f}) = -1 \).

(3.2) **Theorem.** \( \mathcal{O}(\mathfrak{f}) \) is a skew field.

**Proof:** The norm form for \( \mathcal{O}(\mathfrak{f}) \) is \( F_\mathcal{O} = x_0^2 + \text{adj } \mathfrak{f} \). But
\[ c_p(F_\mathcal{A}) = c_p(\text{adj } f) = c_p(f) = -1 \] and \( \det F_\mathcal{A} \) is a square. Hence, \( F_\mathcal{A} \) does not represent zero in \( \mathbb{Q}_p \). This means that every non-zero element of \( \mathcal{A} \) has a non-zero norm and therefore has an inverse. \( \text{Q.E.D.} \)

(3.3) Let \( \Phi = px^2 - \varphi(y, z) \) where

\[ \varphi(y, z) = \begin{cases} -\varphi y^2 + z^2 & \text{for } p \text{ odd with } \varphi \text{ a fixed quadratic non-residue of } p \\ y^2 - yz + z^2 & \text{for } p = 2. \end{cases} \]

\( \Phi \) is an integral form and \( c_p(\Phi) = -1 \). Hence, \( \mathcal{O} = \Theta(\Phi) = \mathbb{Z}_p[1, w_1, w_2, w_3] \) is a principal order of \( \mathcal{A} \).

(3.4) \textbf{Theorem.} \( \Theta \) is the unique maximal order of \( \mathcal{A} \). Furthermore, \( \alpha \in \mathcal{A} \) is integral if and only if \( N\alpha \in \mathbb{Z}_p \).

\textbf{Proof:} For \( p \) odd, \( e_1 = e_2 = e_3 = 0 \) and \( w_1 = \theta_1 \). Thus,

\[ F_\Theta = x_0^2 + \text{adj } \Phi = x_0^2 - \varphi x_1^2 - p(x_2^2 - \varphi x_3^2). \] For \( p = 2, e_1 = 1, e_2 = e_3 = 0 \) and therefore \( w_1 = \frac{1}{2} + \theta_1, w_2 = \theta_2, w_3 = \theta_3 \). Thus,

\[ F_\Theta = x_0^2 + x_0^1 + \frac{1}{4} x_1^2 + \text{adj } \Phi = x_0^2 + x_0^1 + x_1^2 - 2(x_2^2 + x_2x_3 + x_3^2). \]

Combining these two cases, we have \( F_\Theta = \text{adj } \varphi(x_0^1x_1^1) - p \cdot \text{adj } \varphi(x_2^1x_3^1) \).

Notice that if \( \text{adj } \varphi(x, y) \equiv 0 \text{ mod } p \) for some \( x, y \in \mathbb{Z}_p \), then \( x \equiv y \equiv 0 \text{ mod } p \). Now let \( \xi = x_0^1 + \sum x_i w_i \in \mathcal{A}, x_i \in \mathbb{Q}_p \), and suppose \( N\xi = h \neq 0 \in \mathbb{Z}_p \). Pick \( s \not\equiv 0 \) such that \( y_1 = p^s x_1 \) is a \( p \)-adic integer.
for each $i$ and $y_j$ is a $p$-adic unit for some $j$. Let $\eta = y_0 + \sum y_i w_i = p^s g$. Then $\eta = \text{adj} (y_0, y_1) - p \cdot \text{adj} (y_2, y_3) = p^{2s} h$. If $s > 0$, we have $\text{adj} \varphi(y_0, y_1)\equiv 0 \mod{p}$ and, thus, $y_0 = py'_0$, $y_1 = py'_1$. Hence, $\eta = p^2 \cdot \text{adj} \varphi(y_0, y_1) - p \cdot \text{adj} \varphi(y_2, y_3) = p^{2s} h$, $s > 0$. It follows that $\text{adj} \varphi(y_2, y_3)\equiv 0 \mod{p}$ and again $y_2 = py'_2$, $y_3 = py'_3$. This contradicts the assumption that one of the $y_j$ is a unit. Therefore, $s = 0$ and each $x_i \in \mathbb{Z}/p$. Thus, $g \in \Theta$ and, hence, is integral. It follows immediately that $\Theta$ is the unique maximal order of $\mathcal{O}$.

Q.E.D.

Now let $\pi = w_2$ and $v$ be the $p$-adic valuation on $\mathbb{Q}_p$. We see that $\pi^2 = p$ and that $\pi$ is irreducible.

(3.5) Theorem. If $\alpha \neq 0 \in \mathcal{O}$, then $\alpha = e^\pi n = \pi^s e'$ for some integers $n$ and some $e, e' \in \mathcal{O}$ with $Ne$ and $Ne'$ $p$-adic units. Moreover,

(i) $\Theta = \{ \alpha \in \mathcal{O} \mid V(\pi \alpha) \geq 0 \}$

(ii) $U = \{ \alpha \in \mathcal{O} \mid V(\pi \alpha) = 0 \}$ is the set of units of $\Theta$.

(iii) $P = \{ \alpha \in \mathcal{O} \mid V(\pi \alpha) > 0 \}$ is the unique maximal two-sided ideal in $\Theta$.

The proof is obvious.

(3.6) Theorem. $P = \pi \cdot \Theta = (\pi)$, and the fractional ideals in $\Theta$ are two-sided and are the integral powers of $(\pi)$. 
Again the proof is easy.

(3.7) **Theorem.** \((\pi)\) is the only proper primitive ideal in \(\Theta\) and is 2-dimensional mod \(p\).

**Proof:** It is clear that \((\pi)\) is the only proper primitive ideal since \(\pi^2 = p\). Also \(\pi, \pi w_1, \pi w_2, \pi w_3\) is a \(Z_p\) basis for \((\pi)\). By using the multiplication tables we have, both for \(p = 2\) and \(p\) odd, that \(\pi = w_2, \pi w_1 = w_3, \pi w_2 = p, \pi w_3 = p w_1\). Thus \((\pi) = [p, p w_1, w_2, w_3]\) and is clearly 2-dimensional mod \(p\).

Q.E.D.

(3.8) **Theorem.** If \(A\) is a 4-dimensional submodule of \(\Theta\) such that \(G_A = p^h F_A\), where \(\det F_A\) is a unit multiple of \(\det F_\Theta\) then \(A = (\pi^h)\).

**Proof:** Since the norm of every element of \(A\) is divisible by \(p^h\) it is clear that every element of \(A\) is divisible by \(\pi^h\). Thus \(A = \pi^h B\) and \(G_B = F_A\). But \(\det G_B = N(B)^2 \cdot \det F_\Theta\). Thus \(N(B)\) is a \(p\)-adic unit and \(B = \Theta\). Therefore \(A = (\pi^h)\).

Q.E.D.

B. The case, \(c_p(f) = +1\).

(3.9) **Theorem.** \(\mathcal{A}(f) \cong M_2(Q_p)\).

**Proof:** Let \(g = x^2 - y^2 + z^2\). \(c_p(g) = +1\) and therefore \(\mathcal{A}(f) \cong \mathcal{A}(g) = \left(\frac{1 - 1}{Q_p}\right) \cong M_2(Q_p)\).

Q.E.D.
(3.10) Let $\Theta = M_2(\mathbb{Z}_p)$.

(3.11) **Theorem.** $\Theta$ is a maximal order of $\mathcal{O}$.

**Proof:** (Hasse) Suppose $\Theta^*$ is an order containing $\Theta$ and let $\alpha = \sum a_{ij}e_{ij} \in \Theta^*$, $a_{ij} \in \mathbb{Q}_p$. Then for any $i$ and $j$ we have

$$a_{ij} = a_{ij}e_{kk} = e_{ki}a_{ik} = e_{jk}a_{kj} \in \Theta^*$$

and, thus, $a_{ij}(e_{11} + e_{22}) = a_{ij} \in \Theta^* \cap \mathbb{Q}_p = \mathbb{Z}_p$.

Thus $\alpha \in \Theta$.

$\blacksquare$.

(3.12) **Lemma.** Let $R$ be a principal ideal ring, $I_r$ the lattice of right ideals in $M_n(R)$, $I_l$ the lattice of left ideals in $M_n(R)$, and $S$ the lattice of submodules of $\bigoplus_{1}^{n} R$. Define the mappings $\rho: I_r \rightarrow S$ and $\lambda: I_l \rightarrow S$ by letting $\rho(A)$ be the set of all vectors $(x_1, \ldots, x_n)$ occurring as a column of some matrix $\alpha$ in $A$ and by letting $\lambda(B)$ be the set of all vectors $(x_1, \ldots, x_n)$ occurring as a row of some matrix $\beta$ in $B$. Then

(i) $\rho$ and $\lambda$ are lattice isomorphisms,

(ii) the ideals in $M_n(R)$ are principal,

(iii) the two-sided ideals of $M_2(R)$ are of the form $r \cdot M_n(R)$ with $r \in R$.

The proof is well known [3; ]. However, the construction of a
generator of an ideal \( A \) is of interest. \( \varphi(A) \) or \( \lambda(A) \) is a free \n R module since \( R \) is a principal ideal ring and hence has an \( R \) basis, \n say \( x_1, \ldots, x_k \), \( k \leq n \) with \( x_i = (x_{i1}, \ldots, x_{in}) \). Now let \n \[
\alpha = \begin{bmatrix}
    x_{11} & \cdots & x_{1k} & 0 & \cdots & 0 \\
    \vdots & & \vdots & & \vdots & \\
    \vdots & & \vdots & & \vdots & \\
    x_{n1} & \cdots & x_{nk} & 0 & \cdots & 0 
\end{bmatrix}
\]

with enough columns of zeros so that \( \alpha \) is an \( n \times n \) matrix. If \( A \) is a \n right ideal then \( A = [\alpha] \). If \( A \) is a left ideal, then \( A = (\alpha') \), where \n \( \alpha' \) is the transpose of \( \alpha \). The ideals in \( M_2(Z_p) \) we are considering in \n this thesis are all \( 4 \)-dimensional and therefore are generated by matrices with non-zero determinant. The submodules of \( Z_p \oplus Z_p \) \n corresponding to these ideals are \( 2 \)-dimensional.

(3.13) \textbf{Theorem.} Let \( \alpha \in \mathcal{O} \) with \( N\alpha \neq 0 \). Then \( \alpha^{-1} \Theta \alpha \) is a maximal \n order of \( \mathcal{O} \) and every maximal order is one of these. All maximal orders \n have the same norm form \( F_\Theta \).

\textbf{Proof:} (Hasse) It is clear that \( \alpha^{-1} \Theta \alpha \) is a maximal order of \( \mathcal{O} \) and \n has the same norm form as \( \Theta \). Now let \( \Theta^* \) be a maximal order of \( \mathcal{O} \). \n Then \( \Theta \Theta^* \) is a fractional left ideal in \( \Theta \). Thus \( \Theta \Theta^* = \Theta \alpha \). \( \Theta \Theta^* \) is \n \( 4 \)-dimensional since \( \Theta^* \) is \( 4 \)-dimensional and \( 1 \in \Theta \). Thus \( N\alpha \neq 0 \). \n Now \( \Theta \Theta^* \) is also a fractional right ideal in \( \Theta^* \) and therefore
© a ©* c © a. Since l © θ we have α © θ © © θ and thus θ © © α © α. But α © θ is an order and θ © is maximal. Therefore, θ © © α © α.

Q.E.D.

(3.14) Theorem. There are \( \frac{p^{r+1} - 1}{p - 1} \) right ideals in \( \Theta = M_2(Z_p) \) of reduced norm \( p^r \). They are generated by the quaternions \( \rho \) of the form

\[
\begin{pmatrix}
p^{r-t} & 0 \\
 a & p^t
\end{pmatrix}
\]

where \( a \in Z \), \( 0 \leq a \leq p \), \( 0 \leq t \leq r \).

Proof: Every submodule \( A \) of \( \frac{Z_p \oplus Z_p}{p} \) has a triangular basis. That is, \( A = [(x,y),(0,z)] \). If

\[
\rho = \begin{pmatrix}
x & 0 \\
y & z
\end{pmatrix}
\]

and \( n(\rho \Theta) = p^r \), then \( N\rho = xz = p^r \). Thus we may write

\( A = [(p^{r-t},y),(0,p^t)] \). However, there is an \( a \in Z \), \( 0 \leq a \leq p^t \) such that \( a \equiv y^t \mod p^t \). Thus \( A = [(p^{r-t},a),(0,p^t)] \). For every choice of \( t \), \( 0 \leq t \leq r \), and for every choice of \( a \mod p^t \) we obtain a distinct module \( A \) which corresponds to a right ideal of reduced norm \( p^r \). Since there are \( p^t \) choices for \( a \) we see that there are \( \sum_{t=0}^{r} p^t = \frac{p^{r+1} - 1}{p - 1} \) such
modules $A$ and correspondingly \[ \frac{p^{r+1} - 1}{p - 1} \] distinct right ideals of reduced norm $p^r$.

Q.E.D.

(3.15) Corollary. There are $p^r + p^{r-1}$ primitive right ideals of $\Theta$ of reduced norm $p^r$.

Proof: Let

\[ \rho = \begin{bmatrix} p^{r-t} & 0 \\ a & p^t \end{bmatrix}, \quad 0 \leq a \leq p^t \text{ be primitive.} \]

If $t \neq 0, r$, then $a$ must be prime to $p$. There are $\varphi(p^t) = p^t - p^{t-1}$ such $a$'s. If $t = 0$, there is only one $\rho$. If $t = r$, then $\rho$ is primitive for every choice of $a$. Hence, there are

\[ 1 + p^r + \sum_{t=1}^{r-1} (p^t - p^{t-1}) = p^r + p^{r-1} \]

primitive $\rho$'s which generate distinct right ideals of reduced norm $p^r$.

Q.E.D.

(3.16) Theorem. The primitive right ideals in $\Theta$ of reduced norm $p^r$ are 2-dimensional mod $p^r$. Let

\[ \rho = \begin{bmatrix} p^{r-t} & 0 \\ a & p^t \end{bmatrix} = p^{r-t}e_{11} + ae_{21} + p^te_{22} \text{ be primitive.} \]
A basis for $p \Theta$ is $p e_{11} = p^r t e_{11} + a e_{21}$, $p e_{12} = p^r t e_{12} + a e_{22}$, $p e_{21} = p^r t e_{21}$, $p e_{22} = p^r t e_{22}$. If $t = 0$ or $r$, then $[p]$ is clearly 2-dimensional mod $p^r$. If $t \neq 0$, $r$, then $a$ is prime to $p$. Thus
\[
p e_{11}, p e_{12}, a p e_{21} - p^r t p e_{11} = p^r e_{11}, a p e_{22} - p^r t p e_{12} = p^r e_{22}\]
is a basis for $[p]$. Clearly, $[p]$ is 2-dimensional mod $p^r$.

Q.E.D.

(3.17) Let $M$ be the set of $p + 1$ quaternions
\[
\begin{bmatrix}
1 & 0 \\
0 & 1
\end{bmatrix},
0 < a < p, \text{ and }
\begin{bmatrix}
p & 0 \\
0 & 1
\end{bmatrix}.
\]
Let $M'$ be the set of transposes of the matrices in $M$. The elements of $M$ ($M'$) generate all of the $p + 1$ right (left) ideals of reduced norm $p$. If $\pi$ is in $M$ or $M'$, then $\pi$ is irreducible and $\pi^2 \equiv \pi \mod p$.

(3.18) Theorem. The ideals $[\pi]$ are the maximal right ideals in $\Theta$ and every proper right ideal in $\Theta$ is contained in one of them. Moreover, if $\pi_1, \pi_2 \in M$ and $\pi_1 \neq \pi_2$, then $[\pi_1] \cap [\pi_2] = (p)$. (Similarly for the left ideals $([\pi], \pi \in M')$)

Proof: $\Theta/p\Theta \cong M_2(\mathbb{Z}/p\mathbb{Z})$. By (3.12) the lattice of right ideals of $M_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to the lattice of submodules of $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. 


Since \( \mathbb{Z}/p\mathbb{Z} \) is a field, the only proper submodules of \( \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \) are 1-dimensional and are of the form \( [(1,a)] \). \( 0 \neq a \neq p \) or \( [(0,1)] \).

These are the submodules corresponding to the ideals \([\pi]\) mod \(p\).

The intersection of any two distinct 1-dimensional submodules is easily seen to be 0-dimensional. Thus, if \( \pi_1, \pi_2 \in M \) and \( \pi_1 \neq \pi_2 \), then \( [\pi_1] \cap [\pi_2] = (0) \) mod \(p\). But \( p \in [\pi_1] \cap [\pi_2] \) and therefore \( [\pi_1] \cap [\pi_2] = (p) \). If \( A \) is a proper right ideal in \( \Theta \), then \( A \) is contained in some \([\pi]\) mod \(p\). Thus \( A \subseteq [\pi] + (p) = [\pi] \). Therefore, the right ideals \([\pi]\) are maximal.

Q.E.D.

(3.19) **Corollary.** If \( A \) is a proper primitive right ideal in \( \Theta \), then there is a unique \( \pi \in M \) such that \( A \subseteq [\pi] \). Moreover, \([\pi] = A + (p)\).

(3.20) **Theorem.** If \( \alpha, \beta \in \Theta \), then \( \alpha \) and \( \beta \) belong to either the same maximal right ideal or the same maximal left ideal if and only if \( N\alpha = N\beta = (\alpha, \beta) = 0 \) mod \(p\).

**Proof:** If \( \alpha \) and \( \beta \) lie in the same maximal ideal, then clearly

\( N\alpha = N\beta = (\alpha, \beta) = 0 \) mod \(p\). Now suppose \( N\alpha = N\beta = (\alpha, \beta) = 0 \) mod \(p\).

If one of \( \alpha \) and \( \beta \) is not primitive, then obviously they both lie in some maximal right ideal. If both \( \alpha \) and \( \beta \) are primitive, then \([\alpha]\) and \([\beta]\) are primitive. Thus \([\alpha] = [\pi]\) mod \(p\) for some \( \pi \in M \). Hence,

\( \pi \equiv \alpha \theta \) mod \(p\) for some unit \( \theta \). Let \( \rho = \beta \theta \).
Then \( N \alpha = N \rho = (\alpha, \rho) \equiv 0 \mod p \) and, furthermore, \( \alpha \) and \( \rho \) lie in the same ideal \( \mod p \) if and only if \( \alpha \) and \( \beta \) lie in the same ideal \( \mod p \).

If \( (\alpha) \neq (\rho) \), then \( \Theta = (\alpha) \oplus (\rho) \) since both \( (\alpha) \) and \( (\rho) \) are 2-dimensional \( \mod p \) and \( (\alpha) \cap (\rho) = (0) \). If \( x \lambda = \pi \eta \mod p \) for some \( \lambda, \eta \in \Theta \), then \( x \lambda = x^2 \lambda = x \pi \eta \equiv 0 \mod p \). Thus \( (\alpha) \cap (\rho) = (0) \) and \( \Theta = (\alpha) \oplus (\rho) \). Hence, there exist \( \mu, \nu \in \Theta \) such that

\[
\bar{\rho} = x \mu + x \nu.
\]

Therefore, \( x \bar{\rho} = x^2 \mu + x \pi \nu = x \mu \mod p \). Adding \( \rho \pi \) to both sides we obtain \( 0 = (\rho, \pi) = x \bar{\rho} + \rho \pi = x \mu + \rho \pi \). But since the sum \( (\alpha) + (\rho) \) is direct \( \mod p \), we must have \( x \mu = 0 \).

Therefore \( \rho = x \pi \nu \mod p \) and hence \( \bar{\rho} = [\pi] \). Therefore, \( (\rho) = (\pi) \).

Q.E.D.

(3.21) **Lemma.** Let \( S \) be a set, \( A \subseteq S \), and \( R_1, R_2 \) be two symmetric, transitive, relations on \( S \). If \( A \times A \subseteq R_1 \cup R_2 \), then

\[
A \times A \subseteq R_1 \text{ or } A \times A \subseteq R_2.
\]

**Proof:** Let \( a, b, c, d \in A \) and suppose that \( (a, b) \notin R_1 \), \( (c, d) \notin R_2 \).

Then \( (a, b) \in R_2, (c, d) \in R_1 \). If \( (a, c) \in R_2 \), then \( (b, c) \in R_2 \) and therefore neither \( (a, d) \) nor \( (b, d) \) is in \( R_2 \). Therefore, \( (a, d) \),

\( (b, d) \in R_1 \) which contradicts the assumption that \( (a, b) \notin R_1 \). If \( (a, c) \notin R_2 \), then \( (a, c) \in R_1 \) and we reach a contradiction using the same argument with \( R_1 \) and \( R_2 \) interchanged. It follows that \( A \times A \subseteq R_1 \) or \( A \times A \subseteq R_2 \).

Q.E.D.
Theorem. If $A$ is a primitive $4$-dimensional submodule of $\Theta$ and if $G_A = p^r A$, then there exist quaternions $\rho$ and $\rho'$ in $\Theta$ and a $4$-dimensional submodule $B$ of $\Theta$ such that

(i) $A = \rho B \rho'$,

(ii) $N(\rho \rho') = p^r$,

(iii) $G_B = F_B = F_A$.

Proof: If $r = 0$, the theorem is trivially true.

Suppose $r > 0$ and let $A'$ be the set of all primitive quaternions in $A$. Let $R_1$ be the set of all $(\alpha, \beta)$ such that $\alpha, \beta \in A'$ and $\alpha$ and $\beta$ lie in the same maximal right ideal. Let $R_2$ be the set of all $(\alpha, \beta)$ such that $\alpha, \beta \in A'$ and $\alpha$ and $\beta$ lie in the same maximal left ideal. $R_1$, and similarly $R_2$, is an equivalence relation on $\Theta$. For it is clearly reflexive and symmetric, and if $(\alpha, \beta), (\beta, \gamma) \in R_1$, then $(\alpha, \gamma) \in R_1$ since $\beta$ is primitive and therefore belongs to a unique maximal right ideal. Since $r > 0$, we have $Na = Nb = (\alpha, \beta) = 0 \mod p$ for all $\alpha, \beta \in A$. Hence, by (3.20), $A' \times A' \subseteq R_1 \cup R_2$ and thus, by (3.21), $A' \times A' \subseteq R_1$ or $A' \times A' \subseteq R_2$. Suppose $A' \times A' \subseteq R_1$ and let $\alpha \in A'$. Then every element $\beta \in A'$ belongs to the same maximal right ideal $[\pi]$ that $\alpha$ belongs to. Thus $A' \subseteq [\pi]$ and hence $A \subseteq [\pi]$.

Therefore, $A = [\pi] A_1$ where $G_{A_1} = p^{r-1} F_{A_1}$. We proceed by induction and the theorem follows. Q.E.D.
(3.23) **Corollary.** If $A$ is a 4-dimensional submodule of $\Theta$,

$$G_A = \rho F_A^r$$

and $\det F_A$ is a unit multiple of $\det F_{\Theta}$, then there is a right ideal $R$ and a left ideal $L$ such that $A = R \cdot L$.

**Proof:** By (3.22), $A = \rho B \rho'$ where $G_B = F_B = F_A$. Therefore, $\det G_B$ is a unit multiple of $\det F_{\Theta}$ and thus $B = \Theta$. Hence,

$$A = \rho \Theta \rho' = [\rho](\rho')$$

Q.E.D.

(3.24) **Corollary.** If $A$ satisfies the conditions of (3.23) and if $A$ is primitive, then the decomposition $A = R \cdot L$ is unique.

**Proof:** Suppose $A = R' \cdot L' = R \cdot L$. Then $L$ and $L'$ must be primitive.

But then $L \cdot \Theta = \Theta$ and $L' \cdot \Theta = \Theta$ since the only primitive two-sided ideal in $\Theta$ is $\Theta$. Therefore, $R = R \cdot \Theta = R(L \cdot \Theta) = A \cdot \Theta = R'(L' \cdot \Theta) = R'$ and, similarly, $L' = L$.

Q.E.D.

(3.25) **Theorem.** If $R$ and $L$ are primitive right ideals, then

$A = R \cdot L$ is primitive and $N(A) = N(R) \cdot N(L)$.

**Proof:** If $A = R \cdot L = \rho^h \cdot B$, then $\rho^h \cdot \Theta \cdot B = \Theta \cdot R \cdot L = L$ and thus $h = 0$.

Also, $G_A = n(R) \cdot n(L) F_{\Theta}$. Hence, $F_A = F_{\Theta}$ and

$$\det G_A = N(A)^2 \cdot \det F_{\Theta} = n(R)^4 n(L)^4 \cdot \det F_{\Theta}.$$ 

Therefore, $N(A) = n(R)^2 n(L)^2 = N(R) \cdot N(L)$.

Q.E.D.
CHAPTER IV

THE GLOBAL CASE

Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$ with basis $\rho_0, \rho_1, \rho_2, \rho_3$. We define the local algebra $\mathcal{A}_p$ over $\mathbb{Q}_p$ in the following manner.

Let $\mathcal{A}_p$ be a 4-dimensional vector space over $\mathbb{Q}_p$ with the same basis $\rho_0, \rho_1, \rho_2, \rho_3$. Let the $\rho_k$ have the same multiplication table as they did in $\mathcal{A}$ and extend by linearity to a multiplication on all of $\mathcal{A}_p$. We can obviously consider $\mathcal{A}_p$ as a subset of $\mathcal{A}$ with the same multiplication as before. If $A = \sum_{i=0}^{3} \mathbb{Z} \alpha_i$ is a $\mathbb{Z}$-module in $\mathcal{A}$, we let $A_p = \mathbb{Z}_p \cdot A = \sum_{i=0}^{3} \mathbb{Z}_p \alpha_i$. If $A$ is a 4-dimensional $\mathbb{Z}$-module, then the rational transformation taking the $\rho$ basis onto the $\alpha$ basis is also a $p$-adic transformation and has non-zero determinant. Thus, $A_p$ is a 4-dimensional $\mathbb{Z}_p$-module and $G_{A_p} = G_A$. If $\Theta = \Theta(f)$ is a principal $\mathbb{Z}$-order in $\mathcal{A}$, then clearly $\Theta_p$ is a principal $\mathbb{Z}_p$-order in $\mathcal{A}_p$.

We call $d = -\frac{1}{2} \det f$ the discriminant of $f$ (and of $\Theta(f)$). It can be seen from (3.4) and (3.13) or from [6; 287] that a necessary and sufficient condition that $\Theta_p$ be maximal is that $p^2 \nmid d$ and if $p \mid d$, then $c_p(f) = -1$. Primes which satisfy this last condition will be called good; the other primes (of which there are only finitely many)
will be called bad.

The \( \mathbb{Z} \)-modules in \( \Theta \) will be denoted by \( A, B, \) etc., while the \( \mathbb{Z}_p \)-modules in \( \Theta_p \) will be denoted by \( A^{(p)}, B^{(p)}, \) etc., or by \( A_p, B_p, \) etc. We call \( A^{(p)c} = A^{(p)} \cap \Theta \) the contraction of \( A^{(p)} \) to \( \Theta \).

We need to know the rules for going back and forth between the global and local algebras.

(4.1) **Lemma.** Let \( A \) be a \( k \)-dimensional submodule of \( \Theta \). Then

\[
A^c_p = \{ a \in \Theta \mid sa \in A \text{ for some integer } s \text{ prime to } p \}
\]

**Proof:** If \( a \in \Theta \) and \( sa \in A \) for some integer \( s \) prime to \( p \), then \( a \in A_p \) since \( s \) is a \( p \)-adic unit and hence \( a \in A_p \cap \Theta = A^c_p \).

Now let \( A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3] \). If \( a \in \Theta \), then there exist unique \( x_i \in \mathbb{Q} \) such that \( a = \Sigma x_i \alpha_i \). But if \( a \) is also in \( A_p \), then each \( x_i \in \mathbb{Z}_p \). Thus, there is an integer \( s \), prime to \( p \), such that \( sx_i \in \mathbb{Z} \) for each \( i \) and therefore \( sa \in A \).

\( \square \) E.D.

(4.2) **Lemma.** If \( A \) and \( B \) are \( k \)-dimensional submodules of \( \Theta \) and \( A^{(p)} \) and \( B^{(p)} \) are \( k \)-dimensional submodules of \( \Theta_p \), then

\[
\begin{align*}
(1) & \quad A \subset A^{(p)c}_p \\
(1i) & \quad A_p = (A^c_p)_p \\
(1i) & \quad (A \cap B)_p = A_p \cap B_p \\
(1i) & \quad (A^{(p)} \cap B^{(p)})^c = A^{(p)c} \cap B^{(p)c}
\end{align*}
\]
(iv) \((A \cap B)_p = A_p \cap B_p \), \((A(p)_c \cdot B(p)_c)_p = A(p)_c \cdot B(p)_c\)

(v) \(A = A^c_p\) if and only if \(N(A)\) or \(n(A)\) is a power of \(p\).

(vi) \(A(p)_c = (A(p)_c)_p\) if and only if there exists a \(Z_p\) basis \(\alpha_0, \alpha_1, \alpha_2, \alpha_3\) for \(A(p)\) with each \(\alpha_i \in \Theta\).

(vii) \(A^p = \emptyset_p\) if and only if \(p \nmid N(A)\).

(viii) \(N(A) = \prod_{p|N(A)} N(A_p) = \prod_{p|N(A)} N(A_p), n(A) = \prod_{p|N(A)} n(A_p) = \prod_{p|N(A)} n(A_p)\)

\[1(A) = \prod_{p|N(A)} 1(A_p) = \prod_{p|N(A)} 1(A_p).\]

Proof: (i), (iii), (iv), (vii), and (viii) are trivial.

(ii) By (i), \(A_p \supseteq (A^c_p)_p\) and \(A \subseteq A^c_p\). Thus, \(A_p \subseteq (A^c_p)_p \subseteq A_p\).

Therefore, \(A_p = (A^c_p)_p\). Again by (i), \(A(p)_c \subseteq (A(p)_c)_p\) and \((A(p)_c)_p \subseteq A(p)\). Thus, \(A(p)_c \subseteq (A(p)_c)_p \subseteq A(p)_c\). Therefore,

\(A(p)_c = (A(p)_c)_p\).

(v) Let \(T\) be the transformation taking \(\Theta\) onto \(A\). By (2.6) and (2.7), we know \(N(A) = |\text{det } T|, n(A) \mid N(A)\), and \(T \cdot S = \pm n(A) \cdot I\) for some primitive matrix \(S\). Taking determinants gives \(N(A) \cdot \text{det } S = n(A)^4\).

Thus \(p \mid N(A)\) if and only if \(p \mid n(A)\). Suppose \(A = A^c_p\). We know
that $n(A)$ is the least positive integer $h$ such that $h \cdot \theta \subseteq A$.

If $n(A) = p^s$ with $s$ prime to $p$, then $sp^r \cdot \theta \subseteq A$. But by (4.1) and by the assumption that $A = A^c_p$, this means $p^r \cdot \theta \subseteq A$. Thus, $s = 1$ and $n(A)$ and $N(A)$ are powers of $p$. Now suppose $n(A) = p^r$ and $A = [a_0, a_1, a_2, a_3]$. If $a \in \Theta$, then $a = \frac{1}{p^r} \cdot a'$ for some $a' = \sum x_i a_i \in A$, since $p^r \theta \subseteq A$. Thus, if $sa \in A$ for some $s$ prime to $p$, then $p^r sa' = \sum p^r x_i a_i \in A$. Therefore, $p^r \mid x_i$ for each $i$ and $a \in A$. In view of (4.1), we see that $A = A^c_p$.

(vi) Suppose $A(p) = \mathbb{Z}_p[a_0, a_1, a_2, a_3]$ with $a_1 \in \Theta$. Let
\[ A = \mathbb{Z}[a_0, a_1, a_2, a_3]. \]
Then $A \subseteq A(p)^c \subseteq A(p)$. Hence, $A(p) = A_p \subseteq (A(p)^c)_p \subseteq A(p)$ and therefore $A(p) = (A(p)^c)_p$. Now suppose $A(p) = (A(p)^c)_p$.

Since $A(p)^c \subseteq \Theta$ and is a $\mathbb{Z}$-module, then $A(p)^c = \mathbb{Z}[a_0, a_1, a_2, a_3]$ for some $a_1 \in \Theta$. Thus $A(p) = (A(p)^c)_p = \mathbb{Z}_p[a_0, a_1, a_2, a_3]$ with $a_1 \in \Theta$.

Q.E.D.

(4.3) Lemma. If $A(p)$ is a 4-dimensional $\mathbb{Z}_p$-module in $\Theta_p$, then $A(p)$ has a basis $a_0, a_1, a_2, a_3$ with $a_1 \in \Theta$ and consequently $A(p) = (A(p)^c)_p$. 
\[ N(A(p)) = N(A(p)^c), \quad n(A(p)) = n(A(p)^c), \quad \text{and} \quad l(A(p)) = l(A(p)^c). \]

**Proof:** If \( A(p) \) is 4-dimensional, then \( n(A(p)) = p^r \) for some \( r \geq 0 \). If \( r = 0 \), then \( A(p) = \emptyset \) and the theorem is true. If \( r > 0 \), let \( A(p) = \mathbb{Z}_p[\alpha_0, \alpha_1, \alpha_2, \alpha_3] \). There exist \( \alpha'_1 \in \Theta \) such that

\[ \alpha'_1 \equiv \alpha_1 \pmod{p^r} \]

and thus, \( \alpha'_1 = \alpha_1 + p^r \gamma_1 \) for some \( \gamma_1 \in \Theta_p \).

Let \( A = \mathbb{Z}[\alpha'_1, \alpha'_2, \alpha'_3] + p^r \Theta = \mathbb{Z}[\beta_0, \beta_1, \beta_2, \beta_3] \). Then

\[ A_p = \mathbb{Z}_p[\alpha'_0, \alpha'_1, \alpha'_2, \alpha'_3] + p^r \Theta_p = \mathbb{Z}_p[\beta_0', \beta_1', \beta_2', \beta_3']. \]

Clearly, \( A_p \subseteq A(p) \), and since \( p^r \gamma_1 \in A_p \) for each \( i \), we have \( \alpha_1 \in A_p \). Thus \( A(p) = A_p = \mathbb{Z}_p[\beta_0', \beta_1', \beta_2', \beta_3'] \) with \( \beta_1 \in \Theta \). The rest of the theorem follows easily.

Q.E.D.

(4.4) **Theorem.** If \( A = [\alpha_0, \alpha_1, \alpha_2, \alpha_3] \) is a 4-dimensional submodule of \( \Theta \), then \( A = \bigcap_{p|N(A)} A_p^c \). Moreover, if \( A(p) \) is a 4-dimensional \( \Theta_p \)-module for each rational prime \( p \) and if \( A = \bigcap_{p} A(p)_c \), then \( A_p = A(p) \) for each prime \( p \).
Proof: By (4.2.1), we have \( \cap_{p} A_{p}^{c}. \) If \( \xi \in \cap_{p} A_{p}^{c}, \) then \( \xi \in \Theta, \)
and thus there exist unique \( x_{1} \in \mathbb{Q} \) such that \( \xi = \sum x_{1}q_{1}. \) But then
each \( x_{1} \in \mathbb{Z}_{p} \) for every prime \( p. \) Thus each \( x_{1} \in \mathbb{Z}, \) \( \xi \in A, \) and
therefore \( A = \cap_{p} A_{p}^{c}. \) Now if \( p \nmid N(A), \) then \( A_{p} = \Theta, \) and hence
\[ A_{p}^{c} = \Theta. \] Therefore, \( A = \cap_{p} A_{p}. \) Now suppose \( A = \cap_{p} A(\mathbb{P})^{c} \) with
each \( A(\mathbb{P}) \) 4-dimensional. Then \( A \subseteq A(\mathbb{P})^{c} \) for each \( p, \) and hence
\[ A_{p} \subseteq (A(\mathbb{P})^{c})_{p} = A(\mathbb{P}) \] for each \( p. \) Thus \( n(A(\mathbb{P})) \mid n(A_{p}) \) for each \( p. \)
Let \( h = \prod_{p} n(A(\mathbb{P})) = \prod_{p} n(A(\mathbb{P})^{c}) \) and \( h_{p} = \frac{h}{n(A(\mathbb{P}))}. \) We see that
\[ (h_{p}, p) = 1 \text{ and that } h_{p} \cdot \Theta \subseteq A(\mathbb{Q})^{c} \text{ for every prime } q \neq p. \] In particular,
we have \( h_{p} \cdot A(\mathbb{P})^{c} \subseteq A(\mathbb{Q})^{c} \text{ for every } q \neq p. \) However, \( h_{p} \cdot A(\mathbb{P})^{c} \subseteq A(\mathbb{P})^{c} \)
and therefore \( h_{p} \cdot A(\mathbb{P})^{c} \subseteq \bigcap_{q} A(\mathbb{Q})^{c} = A. \) Thus, \( h_{p} \cdot A(\mathbb{P}) = h_{p} \cdot (A(\mathbb{P})^{c})_{p} \subseteq A_{p}. \)
But \( h_{p} \) is a unit in \( \mathbb{Z}_{p} \) and thus \( A(\mathbb{P}) \subseteq A_{p} \subseteq A(\mathbb{P}). \) Therefore, \( A_{p} = A(\mathbb{P}). \)

Q.E.D.

(4.5) Corollary. If \( A(\mathbb{P}) \) is a 4-dimensional submodule of \( \Theta_{p} \) for
each prime \( p \) and if \( A(\mathbb{P}) = \Theta \) for all but a finite number of primes,
then $A = \bigcap A^{(p)}$ is a $\Delta$-dimensional submodule of $\Theta$. Furthermore,

$$N(A) = \prod_{p} N(A^{(p)}), \text{ and } n(A) = \prod_{p} n(A^{(p)}), \text{ and } l(A) = \prod_{p} l(A^{(p)}).$$

(4.6) **Theorem.** If $R$ is a primitive right ideal in $\Theta$ such that $n(R)$ is divisible by good primes only, then $N(R) = n(R)^2,$ $G_{r} = n(R)\cdot F_{r},$ and there exists a primitive $\xi \in R$ such that $R = [n(R), \xi]$ and the g.c.d. $(n(R), \frac{N_{\xi}}{n(R)}) = 1.$

**Proof:** Since $R$ is primitive, each $R^{p}$ is primitive. By (2.9), we have

$$N(R^{p}) = n(R^{p})^2 \text{ and thus } G_{r} = n(R^{p})\cdot F_{r}^{p}.$$ Thus,

$$N(R) = \prod_{p} N(R^{p}) = \prod_{p} n(R^{p})^2 = n(R)^2.$$ Now $G_{r} = m F_{r}$ for some positive integer $m.$ But $G_{r} = G_{r}^{p}$ for each $p.$ Thus, $n(R^{p}) \mid m$ for each $p$ and therefore $m = n(R)\cdot m'.$ However, $m'$ is a unit in $Z_{p}$ for each $p.$ Therefore, $m' = 1$ and $G_{r} = n(R)\cdot F_{r}.$ Now let $n(R) = p_{1}^{r_{1}} \cdots p_{u}^{r_{u}}$ and $R = a_{i}^{p_{i}}$ with $N_{a_{i}} = p_{i}^{j}$ so that $R = \bigcap_{i=1}^{u} R^{c}_{p_{i}}.$ For each $i$ there exists $\xi_{i} \in R_{p_{i}}^{c}$ such that $a_{i} = \xi_{i} \mod p_{i}.$ Let $h = n(R)^2$ and $h_{i} = h \cdot p_{i}^{-2r_{i}}.$ Then $h_{i}$ is prime to $p_{i}$ so there exists $k_{i} \in Z$
such that \( h_1 k_1 \equiv 1 \mod p_1 \). Finally, let \( \xi = \Sigma h_1 k_1 \xi_1 \), and consider the ideal \([n(R), \xi]\) in \( \Theta \). If \( p \not| n(R) \), then \([n(R), \xi])_p = \Theta_p \). If \( p = p_i \) divides \( n(R) \), then \( \xi - \xi_1 \equiv a_1 \mod p_1 \). Thus, \([n(R), \xi])_{p_i} = \frac{r_1}{p_i} a_1 \xi_1 \equiv \frac{r_1}{p_i} \xi_1 \mod p_i \). Therefore, \( R = [n(R), \xi] \). Moreover, \( N\xi = Na_1 = p_i^{r_1} \) mod \( p_i \) and therefore the \( \text{g.c.d.}(n(R), \frac{N\xi}{n(R)}) = 1 \).

From the construction of \( \xi \), it is clear that if \( p \mid n(R) \), then

\( p \not| \xi \) in \( \Theta \). Thus, if \( \xi = s\xi' \) with \( s \in \mathbb{Z} \) and \( \xi' \) primitive, then \( s \) is prime to \( n(R) \) and there exist integers \( a \) and \( b \) such that \( as + b\cdot n(R) = 1 \).

Hence, \( \xi' = as\xi' + b\cdot n(R)\xi' = a\xi' + b\cdot n(R)\xi' \in [n(R), \xi] \). Since \( a \) is prime to \( n(R) \), it is clear that \([n(R), \xi']) = (n(R), \xi) \). Furthermore, 

\[ N\xi' = a^2 N\xi + ab\cdot n(R)\cdot (\xi, \xi') + b^2 \cdot n(R)^2 N\xi'. \]

Since \( n(R) \mid (\xi, \xi') \) we have the \( \text{g.c.d.}(n(R), \frac{N\xi'}{n(R)}) = 1 \).

\( \Box \) \( \text{E.D.} \)

(4.7) **Theorem.** Let \( R \) be a primitive right ideal in \( \Theta(f) \) such that \( n(R) \) is divisible by good primes only. If \( n(R) = m_1 m_2 \) where \( m_1 \) is the largest factor of \( m \) divisible only by primes for which \( c_p(f) = -1 \), then the two-sided ideal \( I = \Theta \cdot R \) is the ideal \( \bigcap \frac{R^c}{p_{m_1}} \) and \( n(I) = m_1 \).
Proof: If \( c_p(f) = +1 \), then \( I_p = \Theta_p \cdot R_p = \Theta_p \) since \( R_p \) is primitive.

If \( c_p(f) = -1 \), then \( I_p = \Theta_p \cdot R_p = R_p \) since ideals are two-sided in this case. Therefore, \( I = \bigcap_{p|n(I)} R_p \) and \( n(I) = m_1 \).

Q.E.D.

(4.8) Theorem. The two-sided ideals in \( \Theta(f) \) whose reduced norms are divisible by good primes only commute. If \( I \) is a primitive such ideal, then \( I^2 = n(I) \cdot \Theta \).

Proof: The theorem is true if it is true for primitive two-sided ideals. Let \( I \) and \( J \) be primitive two-sided ideals whose reduced norms satisfy the conditions of the theorem. If \( c_p(f) = +1 \), then

\[
I_p = J_p = \Theta_p
\]
since \( I_p \) and \( J_p \) are primitive. If \( c_p(f) = -1 \), then

\[
(IJ)_p = I_p \cdot J_p = J_p \cdot I_p = (J \cdot I)_p
\]
Thus \( IJ =JI \). Again, if \( I \) is primitive, the only primes \( p \) that divide \( n(I) \) are those for which \( c_p(f) = -1 \).

If \( p \mid n(I) \), then \( I_p \) is a proper primitive ideal of \( \Theta_p \) and thus is the maximal ideal \((\pi)\). But \((\pi)^2 = (p)\). Hence, \( n(I_p) = p \) and

\[
(I_p)^2 = p \Theta_p.
\]
Therefore, \( I^2 = \bigcap_{p|n(I)} I_p^c = \bigcap_{p|n(I)} p \Theta = (\prod p) \cdot \Theta = n(I) \cdot \Theta.\)

Q.E.D.
Theorem. Let $A$ be a primitive, $4$-dimensional submodule of $\Theta$ with $G_A = mF_A$ and $\det F_A = \det F_\Theta$. If $m$ is divisible by good primes only, then there exists a unique triplet of integers $(a, b, c)$ and unique right, two-sided, and left ideals $R$, $I$, and $L$, respectively, such that

(i) $A = RIL$

(ii) $m = abc$ with $b$ the largest factor of $m$ divisible only by primes for which $c_p(f) = -1$

(iii) $n(R) = a$, $n(I) = b$, $n(L) = c$.

Proof: If $p \nmid m$, then $\det G_A$ is a $p$-adic unit times $\det F_\Theta$ and hence $A = \Theta$. If $p \mid m$, then $G_A = p^r m' F_A$ where $m'$ is a $p$-adic unit. Thus, $\det m' F_A$ is a unit multiple of $\det F_\Theta$. Hence by (3.8) if $c_p(f) = -1$, then $A$ is a two-sided ideal of $\Theta$, and by (3.23) if $c_p(f) = +1$, then $A$ is uniquely expressible as a product $R(p)_L(p)$ of a right and left ideal in $\Theta$. Now let $b$ be the largest factor of $m$ for which $c_p(f) = -1$ and let $m' = \frac{m}{b}$. Let $I = \bigcap_p A_p^c$, $R = \bigcap_p R(p)_c$, $L = \bigcap_p L(p)_c$, and $B = R \cdot I \cdot L$. Then $B = R \cdot I \cdot L$. Thus, $B = A$ if $p \mid m'$.
\[ p \mid b, B_p = R(p)_B \cdot L(p) = R(p)_L(p) = A_p \text{ if } p \mid m', \text{ and} \]

\[ B_p = \Theta_p = A_p \text{ if } p \nmid m. \text{ Thus, } A = B = R \cdot I \cdot L. \text{ Clearly, } n(I) = b. \]

Let \( n(R) = a, n(L) = c. \) If \( p \mid m' \) we know that \( G_p = n(R_p) \cdot n(L_p) F_{\Theta_p} \)

and if \( p \mid b \) we know that \( G_p = n(A_p) \cdot F_{\Theta_p}. \) Therefore,

\[ m = \prod_{p \mid m'} n(R_p) \cdot \prod_{p \mid b} n(A_p) \cdot \prod_{p \mid m'} n(L_p) = abc. \]

\[ \text{Q.E.D.} \]

Let \( \Theta = Z[w_0, w_1, w_2, w_3] \) be a principal order in \( \mathcal{C} \) and let

\[ \Omega = (w_0, w_1, w_2, w_3). \] For \( \alpha \in \mathcal{C} \) there exist unique matrices \( \varphi(\alpha), \psi(\alpha) \in M_4(Q) \) such that \( \alpha \cdot \Omega = \Omega \cdot \varphi(\alpha) \) and \( \Omega \cdot \alpha = \Omega \cdot \psi(\alpha). \) It is easily shown that \( \varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta), \psi(\alpha \beta) = \varphi(\alpha) \cdot \varphi(\beta), \) and that

\[ \psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta), \psi(\alpha \beta) = \psi(\beta) \cdot \psi(\alpha). \] Thus, \( \varphi \) is a \( Q \)-homomorphism and \( \psi \) is a \( Q \)-anti-homomorphism of \( \mathcal{C} \) into \( M_4(Q). \) \( \mathcal{C} \) is simple and therefore each of \( \ker \varphi \) and \( \ker \psi \) is either 0 or \( \mathcal{C}. \) But \( 1 \in \mathcal{C} \) and hence \( \varphi(1) = \psi(1) = I_4 \neq 0. \) Thus \( \ker \varphi = \ker \psi = 0 \) and therefore \( \varphi \) and \( \psi \) are monomorphisms. Now \( \alpha \Omega \beta = \alpha(\Omega \beta) = (\alpha \Omega) \psi(\beta) = \Omega \varphi(\alpha) \cdot \psi(\beta) \) on one hand, and on the other hand, \( \alpha \Omega \beta = (\alpha \Omega) \beta = \Omega \varphi(\alpha) \beta = (\Omega \beta) \varphi(\alpha) = \Omega \psi(\beta) \cdot \varphi(\alpha). \) Therefore, \( \varphi(\alpha) \cdot \psi(\beta) = \psi(\beta) \cdot \varphi(\alpha) \) for every \( \alpha, \beta \in \mathcal{C}. \) If we restrict \( \varphi \) and \( \psi \) to \( \Theta, \) they they are
monomorphisms from $\Theta$ into $M_4(Z)$. We can now apply (4.9) to derive an interesting result.

(4.10) **Theorem.** Let $T \in M_4(Z)$ be a primitive matrix such that $T'T = mI$ where $m$ is an odd positive integer. Then there is a unique pair of integers $(m_1, m_2)$ and there exist matrices

$$M = \begin{bmatrix} x_0 & -x_1 & -x_2 & -x_3 \\ x_1 & x_0 & -x_3 & x_2 \\ x_2 & x_3 & x_0 & -x_1 \\ x_3 & -x_2 & x_1 & x_0 \end{bmatrix} \quad , \quad N = \begin{bmatrix} y_0 & -y_1 & -y_2 & -y_3 \\ y_1 & y_0 & y_3 & -y_2 \\ y_2 & -y_3 & y_0 & y_1 \\ y_3 & y_2 & -y_1 & y_0 \end{bmatrix}$$

with $x_0^2 + x_1^2 + x_2^2 + x_3^2 = m_1$, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = m_2$, $m = m_1 m_2$, and a unit-modular matrix $U \in M_4(Z)$ such that $T = MNU = NMU$.

**Proof:** Let $f = x^2 + y^2 + z^2$. Then $\Theta(f)$ is the ring of Lipschitz quaternions with the usual basis 1, i, j, k. The norm form for this basis is $F_\Theta = x_0^2 + x_1^2 + x_2^2 + x_3^2$. The prime 2 is the only bad prime in this order and $c_p(f) = +1$ for odd primes. It is well known that the ideals of odd norm are all principal. Now let $\Omega = (1, i, j, k)$ and $A$ be the submodule whose basis is $\Omega T$. Then $A$ is primitive and $G_A = m(x_0^2 + x_1^2 + x_2^2 + x_3^2)$. Since $m$ is odd, $c_p(f) = +1$ for every prime dividing $m$. Thus, by (4.9) there exists a unique pair $(m_1, m_2)$ of integers and unique right and left ideals $R$ and $L$, respectively, such
that \( A = R \cdot L, \) \( n(R) = m_1, \) \( n(L) = m_2, \) and \( m = m_1 m_2. \) But \( m_1 \) and \( m_2 \)
are odd and thus \( R = [\xi], \) \( L = [\eta] \) for some \( \xi = x_0 + x_1 i + x_2 j + x_3 k \)
and \( \eta = y_0 + y_1 i + y_2 j + y_3 k. \) Moreover, \( x^2_0 + x^2_1 + x^2_2 + x^2_3 = N \xi = n(R) = m_1, \)
\( y^2_0 + y^2_1 + y^2_2 + y^2_3 = N \eta = n(L) = m_2, \) and, by direct computation, \( \varphi(\xi) = M, \)
\( \psi(\eta) = N. \) It is easily seen that \( \xi \cap \eta \) is a basis for \([\xi] \cdot [\eta] = A. \)

Thus, there is a unit-modular matrix \( U \in M_4(\mathbb{Z}) \) such that \( \Omega \cdot T = \Omega \cdot \varphi(\xi) \psi(\eta) U = \Omega \cdot \psi(\eta) \varphi(\xi) U. \) Therefore, \( T = MNU = NMU. \)

Q.E.D.

Notice that \( \xi \) and \( \eta \) can be written as the product of irreducible
quaternions of prime norm. That is \( \xi = \pi_1 \cdot \pi_2 \cdots \pi_h \) and \( \eta = \pi'_1 \cdot \pi'_2 \cdots \pi'_k \)
with \( N \pi_i \) and \( N \pi'_i \) primes for each \( i. \) Thus, \( M = \varphi(\xi) = \varphi(\pi_1) \cdot \varphi(\pi_2) \cdots \varphi(\pi_h) \)
and \( N = \psi(\eta) = \psi(\pi'_1) \cdots \psi(\pi'_2) \cdot \psi(\pi'_3) \) where \( \varphi(\pi_i) \) has the same form as \( M \)
and \( \psi(\pi'_i) \) has the same form as \( N. \)

Other applications of (4.9) and the theory developed in this
thesis should be possible. One such is the generalization of (4.10) to

\[ (4.11) \begin{align*}
\text{Conjecture.} & \quad \text{If } F \text{ is a norm form of some principal order } \Theta, \text{ and} \\
& \text{if } T \in M_4(\mathbb{Z}) \text{ is a primitive matrix such that } F^T = mF \text{ and } m \text{ is the} \\
& \text{product of good primes, then there exist matrices } M_i, N_j, P_k \in M_4(\mathbb{Z}), \\
& i = 1, \ldots, r, j = 1, \ldots, s, k = 1, \ldots, t, \text{ and a unit-modular matrix} \\
& U \in M_4(\mathbb{Z}) \text{ such that } T = (N_1 N_2 \cdots N_r) \cdot (M_1 \cdots M_s) \cdot (P_1 \cdots P_t), \text{ det } N_i, \text{ det } M_j, \\
& \text{det } P_k \text{ are primes, and } N_1 M_j = M_j N_1, N_1 P_j = P_j N_1, M_1 P_j = P_j M_1, P_1 P_j = P_j P_1.
\end{align*} \]
SELECTED BIBLIOGRAPHY


Charles Carter Waid, son of Dr. and Mrs. Guy N. Waid, was born February 27, 1939, in Okeene, Oklahoma. He graduated from Carlsbad High School in Carlsbad, New Mexico, in June, 1957. He entered New Mexico Institute of Mining and Technology in June, 1957, and received his Bachelor of Science degree in mathematics in June, 1961. He then taught for one year at East Junior High School, Roswell, New Mexico.

He enrolled in the Graduate School of Louisiana State University in September, 1962, and received a Master of Science degree in mathematics in June, 1964.

From September, 1962, through August, 1966, he held a Graduate Teaching Assistantship. In September, 1966, he was appointed Instructor of Mathematics. In March, 1963, he was married to Margaret Yvonne Cowsar who received her Master of Science degree in mathematics from Louisiana State University in August, 1963. They have two sons, James Bryan and Gordon Chester, who were born in April, 1964, and November, 1966, respectively.

He is presently a candidate for the degree of Doctor of Philosophy in Mathematics.
EXAMINATION AND THESIS REPORT

Candidate: Charles Carter Wald

Major Field: Mathematics

Title of Thesis: MODULES OF QUATERNIONS AND THEIR RELATED QUADRATIC FORMS

Approved:

[Signatures of Major Professor and Chairman, Dean of the Graduate School, and members of the examining committee]

EXAMINING COMMITTEE:

[Signatures of committee members]

Date of Examination:

July 14, 1967