Topics in Quadratic and Quaternion Orders.

Bart Francis Rice

Louisiana State University and Agricultural & Mechanical College

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

Recommended Citation
https://repository.lsu.edu/gradschool_disstheses/1686

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
This dissertation has been microfilmed exactly as received 70-9086

RICE, Bart Francis, 1943-
TOPICS IN QUADRATIC AND QUATERNION ORDERS.
The Louisiana State University and Agricultural and Mechanical College, Ph.D., 1969
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan
TOPICS IN QUADRATIC AND QUATERNION ORDERS

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
Bart Francis Rice
B.A., Rice University, June, 1965
B.S., Louisiana State University, May, 1967
August, 1969
ACKNOWLEDGEMENT

The author wishes to express his appreciation to Dr. Gordon Pall, under whose direction this dissertation was written, for his advice and encouragement. Special thanks go also to Dr. Dennis Estes, University of Southern California, for his interest and counsel.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>I</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>II</td>
<td>MODULES OVER ORDERS AND TRANSFORMATIONS OF QUADRATIC FORMS</td>
</tr>
<tr>
<td>(2.1) The Quadratic Case</td>
<td>8</td>
</tr>
<tr>
<td>(2.2) The Four-Dimensional Case</td>
<td>10</td>
</tr>
<tr>
<td>(2.3) The Lipschitz Ring</td>
<td>15</td>
</tr>
<tr>
<td>(2.4) Remarks on Rings of Transformations - The n-Dimensional Case</td>
<td>20</td>
</tr>
<tr>
<td>III</td>
<td>RINGS OF INTEGRAL QUATERNIONS</td>
</tr>
<tr>
<td>IV</td>
<td>QUATERNIONS AND BINARY QUADRATIC FORMS</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>50</td>
</tr>
<tr>
<td>VITA</td>
<td>52</td>
</tr>
</tbody>
</table>
ABSTRACT

This paper is a study of several subjects concerning integral orders in composition algebras of dimensions 2 and 4 over the rational numbers.

Chapter I consists of preliminaries. In the second chapter we examine transformations carrying certain binary and quaternary quadratic forms into multiples of themselves. In the quadratic case, nothing new is done, but a slightly novel and generalizable approach is used. In the 4-dimensional case, an interesting factorization theorem (2.2.3) is obtained, and this and other results are used to find an essentially unique factorization of 4 x 4 matrices T such that T'T = ml as T = RLU, where U is a permutation matrix and R,L are right, left "quaternion matrices" respectively. This chapter is concluded with a few remarks on special automorphic transformations of n-ary quadratic forms.

In the third chapter we introduce the notion of "m-maximal" quaternion orders R; to wit, those for which \( R_p \) is a maximal \( Z_p \) order for each prime p in m. A characterization of these rings is obtained, and the following theorem is proved: (1) Suppose R is p-maximal and \( c_p = +1 \). Then there are, in R, \( p + 1 \) primitive left ideals of norm p.

Next we develop the concept of an "ideal divisor" of a quaternion, and generalize a theorem due to Lipschitz, the earliest known result on factorization of quaternions. This along with
(1) allows us, in certain prescribed instances, to count primitive representations of an integer by certain quaternary quadratic forms.

In the fourth chapter, the integral order \( R \) associated with \( f = x^2 - yz \) is studied, and it is shown how purely primitive quaternions correspond to binary quadratic forms. In particular, composition of primitive binary quadratic forms may be achieved by simply factoring and multiplying quaternions in a natural way.
CHAPTER I

INTRODUCTION

A composition algebra over a field $K$, of characteristic not $2$, is a pair $(\mathcal{A}, N)$ where $\mathcal{A}$ is an algebra over $K$, and $N$ is a function, $N: \mathcal{A} \to K$, such that, for $\alpha, \beta \in \mathcal{A}$, $c \in K$,

(i) $N(\alpha\beta) = (N\alpha)(N\beta)$;

(ii) $N(\alpha c) = c^2 N\alpha$;

(iii) the inner product $(\alpha, \beta) = N(\alpha + \beta) - N\alpha - N\beta$ is bilinear;

(iv) $N$ is non-degenerate; that is, if $(\alpha, \beta) = 0$ for each $\beta \in \mathcal{A}$, then $\alpha = 0$; and

(v) $\mathcal{A}$ has an identity element $1$; $\alpha = \alpha 1 = \alpha$ for all $\alpha \in \mathcal{A}$.

We'll denote "$(\mathcal{A}, N)$" simply by "$\mathcal{A}$", since no ambiguity will arise by so doing. For $\alpha \in \mathcal{A}$, $N\alpha$ will be called the norm of $\alpha$. The conditions (i) - (v) imply the following useful identities:

(a) $(\alpha\beta, \alpha'\beta') = (\beta\alpha, \beta'\alpha') = (N\beta)(\alpha, \alpha')$

(b) $(\alpha, \alpha')(\beta, \beta') = (\alpha\beta', \alpha'\beta) + (\alpha\beta, \alpha'\beta')$

(c) $N1 = 1$

(d) $N\alpha = (1/2)(\alpha, \alpha)$

We notice that $K\mathcal{L}$ is a vector subspace of $\mathcal{A}$, and we may then derive $\mathcal{A} = K\mathcal{L} \oplus (K\mathcal{L})^\perp$. An element $\alpha \in \mathcal{A}$ will be called pure if $\alpha \in (K\mathcal{L})^\perp$; that is, if $(\alpha, l) = 0$. Thus if $\gamma \in \mathcal{A}$, we may write $\gamma$ uniquely as $\gamma = c_l + \alpha$, where $c \in K$ and $\alpha$ is pure. We define the conjugate $\bar{\gamma}$ of $\gamma$ by $\bar{\gamma} = c_l - \alpha$. Then $\gamma - \bar{\gamma}$ is a linear mapping of
period 2 in $a$. We may conclude that $(\alpha\beta, \gamma) = (\alpha, \gamma\overline{\beta}) = (\beta, \overline{\alpha}\gamma)$, $(\alpha, \beta) = (\overline{\alpha}, \overline{\beta})$, and $(\alpha\overline{\beta}, \gamma) = (\overline{\alpha}, \alpha, \gamma)$. Thus, in view of (iv), 
\[\overline{\alpha}\beta = \beta \overline{\alpha} .\] Also, then, $\alpha\overline{\alpha} = \overline{\alpha}\alpha = \alpha\overline{\alpha}$, whence the map $\gamma \rightarrow \gamma$ leaves $\alpha\overline{\alpha}$ fixed. Therefore, $\alpha\overline{\alpha} \in K_{\ell}$, and so $(1/2)(\alpha\overline{\alpha}, 1) = (1/2)(\alpha, \alpha) = N\alpha$ implies $\alpha\overline{\alpha} = (N\alpha)_{\ell}$. We also have $\alpha + \overline{\alpha} = (\alpha, 1)_{\ell} = T\alpha$, the \textit{trace} of $\alpha$, where $T\alpha \in K_{\ell}$ and $\alpha \rightarrow T\alpha$ is a linear mapping. We may further deduce (cf. [4], p. 58) that $\alpha^2\beta = \alpha(\alpha\beta), \beta\alpha^2 = (\beta\alpha)\alpha$, which are the defining conditions for an alternative algebra.

A composition algebra is, then, an alternative algebra with an involution $\alpha \rightarrow \overline{\alpha}$ such that $\alpha\overline{\alpha} = (N\alpha)_{\ell}, \alpha + \overline{\alpha} = T\alpha$, and such that $\alpha^2 - (T\alpha)\alpha + (N\alpha)_{\ell} = 0$, as may be verified. The study of composition algebras was prompted by interest in the "Hurwitz problem;" to wit, given a field $K$ and a vector space $\mathcal{A}$ over $K$, determine the quadratic forms $N$ for which there is a bilinear composition $\alpha \beta$ in $\mathcal{A}$ such that $(N\alpha)(N\beta) = N(\alpha\beta)$. Jacobson in [4], a classic, showed that a composition algebra admitted such composition (and a converse statement as well), and he actually determined all of them, showing in the process that the dimension of $\mathcal{A}$ over $K$ is 1, 2, 4, or 8. Those of dimension 8 were found to be non-associative, and this condition precluded continuation of the algorithm which Jacobson showed had to yield all composition algebras over $K$.

Now suppose that $D$ is an integral domain such that the quotient field $K$ of $D$ has characteristic different from 2. Let $(\mathcal{A}, N)$ be a composition algebra over $K$. An element $\alpha \in \mathcal{A}$ will be called \textit{integral} if $N\alpha_{\ell}$ and $T\alpha$ are elements of $D_{\ell}$. Assume that $R$ is a
D-module such that \( R \subseteq D \). Let \( R^\ast = \{ c\alpha : c \in K, \alpha \in R \} \). \( R \) is a D-order, or integral order, of \( D \) provided:

(i) \( D \subseteq R \subseteq R^\ast = D \)

(ii) \( R \) is closed under multiplication; and

(iii) \( R \) contains only integral elements.

The condition \( D \subseteq R \) allows us to write \( l = 1 \) without ambiguity.

Henceforth we will restrict ourselves to the case \( D = \mathbb{Z} \), the integers, and \( K = \mathbb{Q} \), the rational numbers.

(1.1) Lemma: Let \( M \subseteq \mathcal{A} \) be a \( \mathbb{Z} \)-module such that \( M \) contains \( n \) linearly independent elements, where \( n = \dim \mathcal{A}/\mathbb{Q} \). Then \( M \) has a \( \mathbb{Z} \)-basis.

proof: (Estes) Let \( \beta_1, \ldots, \beta_n \) be linearly independent elements of \( M \). Since \( c\beta_1, \ldots, c\beta_n \) are again linearly independent for \( c \neq 0 \), \( c \in \mathbb{Q} \), we may assume that \( \beta_1, \ldots, \beta_n \) are chosen to be integral elements; chosen, in fact, so that \( |\det((\beta_i, \beta_j))| \) is minimal with respect to this property. For \( \gamma_1 \neq 0 \) in \( M \) there is a rational integer \( c \neq 0 \) such that \( c\gamma_1 = c_1\beta_1 + \cdots + c_n\beta_n \), with \( c_i \in \mathbb{Z} \) and \( (c_1, \ldots, c_n) = 1 \). Let \( T \) be an integral matrix of determinant 1 and first column \( \xi \), where \( \xi' = (c_1, \ldots, c_n) \), and let \( (c\gamma_1, \gamma_2, \ldots, \gamma_n) = (\beta_1, \ldots, \beta_n) T \). Then \( \gamma_1, \ldots, \gamma_n \) are integral elements of \( M \), and \( |\det((\gamma_i, \gamma_j))| = (1/c^2)|\det((\beta_i, \beta_j))| \) (see (2.2.1)). Hence \( c = \pm 1 \), and \( \beta_1, \ldots, \beta_n \) is a \( \mathbb{Z} \)-basis for \( M \). q.e.d.

Henceforth we will assume that all modules \( M \) satisfy the hypotheses of (1.1). We define the norm of \( M \) to be the least positive integer in \( M \). Let \( \beta_1, \ldots, \beta_n \) be a basis for \( M \). We will
sometimes write \( \mathcal{M} = [\beta_1, \ldots, \beta_n] \). \( N(\sum_k x_k \beta_k) \) is a quadratic form

\[
\psi = \sum_{i,j} b_{ij} x_i x_j, \quad b_{ij} \in \mathbb{Q},
\]
called the norm form of \( \mathcal{M} \) for the basis \( \beta_1, \ldots, \beta_n \). We may extract a rational number \( q \) and write \( \psi = q \psi' \), where \( \psi' \) is a primitive \( n \)-ary quadratic form with coefficients in \( \mathbb{Z} \), called a primitive norm of \( \mathcal{M} \) for the basis \( \beta_1, \ldots, \beta_n \). We verify easily that \( |q| \) is an invariant of the choice of basis, and that equivalent bases give rise to equivalent norm forms.

In this paper we will concentrate on \( \mathbb{Z} \)-orders in composition algebras of dimensions 2 and 4 over \( \mathbb{Q} \), the quadratic and quaternion algebras, respectively.

A composition algebra of order 2 over \( \mathbb{Q} \) is a field \( F_j = \mathbb{Q}(j) \), where \( j^2 \neq 1 \) is a square free integer, or, if \( j \) is a symbol such that \( j^2 = 1 \), \( F_j \) is the commutative associative algebra over \( \mathbb{Q} \) with basis \( 1, j \). If \( \alpha = a_0 + a_1 j, \quad \overline{\alpha} = a_0 - a_1 j \), and \( N_\alpha = a_0^2 - j a_1^2 \), and thus if \( j^2 \neq 1 \), \( N_\alpha = 0 \) if and only if \( \alpha = 0 \). Set \( d_\alpha = j^2 \) or \( 4j^2 \) according as \( j^2 \equiv 1 \) or \( \not\equiv 1 \) (mod 4). Let \( \mathcal{D} = \{d_\alpha : s = 1, 2, 3, \ldots\} \).

To each \( d \in \mathcal{D} \) corresponds an order \( R_d \) in \( F_j \) given by

\[
R_d = \{x_0 + x_1 \omega : x_0, x_1 \in \mathbb{Z}\},
\]
where

\[
(1.2) \quad \omega = \omega_d = (\epsilon + \sqrt{d})/2, \quad \epsilon = 0 \text{ or } 1 \quad \text{according as } d \equiv 0 \text{ or } 1 \text{ (mod 4)}.
\]

It follows that \( N(x + y \omega) = x^2 + \epsilon xy + (\epsilon - d)y^2/4 \), the norm form of \( R_d \) for the basis 1, \( \omega \).

The four dimensional composition algebras over \( K \) were shown by Jacobson to be the quaternion algebras, 4-dimensional central algebras which are isomorphic to either a division algebra or the
the algebra of $2 \times 2$ matrices over $K$. O'Meara in [7] gives what is probably the best known definition of a quaternion algebra. However, for our purposes, a more suitable definition is the one which follows, first given by Pall in [9].

Let $f$ be an integral ternary form, $(a_{ij})$ the matrix of $f$. Let $(A_{ij}) = \text{adj}(a_{ij})$ [If $K$ is an $n \times n$ matrix, by "adj $K$" we mean the transpose of the matrix of cofactors of $K$], and let adj $f$ be the ternary form with matrix $(A_{ij})$. The quaternion algebra $\mathcal{Q}(f)$ pertaining to the form $f$ has $Q$-basis $1, i_1, i_2, i_3$, where

$$i_k^2 = -A_{kk}, \quad k = 1, 2, 3,$$

$$i_k i_l = -A_{kl} + \sum_k a_{lk} i_k,$$

$$i_s i_r = -A_{sr} - \sum_k a_{rk} i_k,$$

where $(r,s,t)$ is a cyclic permutation of $(1,2,3)$. If $\alpha = x_1 i_1 + x_2 i_2 + x_3 i_3 \in \mathcal{Q}(f)$ such that $x_1, x_2, x_3 \in \mathbb{Z}$, then $\alpha$ is said to be purely integral. If, in addition, $(x_1, x_2, x_3) = 1$, then $\alpha$ is termed purely primitive.

The norm-form of $\mathcal{Q}$ for the basis $1, i_1, i_2, i_3$ is

$$N(x_0 + \sum_k x_k i_k) = x_0^2 + \text{adj} f (x_1, x_2, x_3) = x_0^2 + \sum_{k,j} A_{ij} x_i x_j,$$

which need not always be an integral form. However, it is found (cf.[9]), for

$\{i,j,k\} = \{1,2,3\}$, that if $\epsilon_k = 0$ or 1 according as $2a_{ij}$ is even or odd, then the "Brandt norm-form" $F = (x_0 + (1/2) \sum_k \epsilon_k x_k)^2 + \text{adj} f (x_1, x_2, x_3)$, has integral coefficients. Accordingly, if we let $j_k = i_k + \epsilon_k/2$, $k = 1, 2, 3$, then the norm form of $\mathcal{Q}$ for the basis $1, j_1, j_2, j_3$ is $F$. Further, it may be verified that

$$R(f) = \{x_0 + \sum_k x_k i_k : x_k \in \mathbb{Z}\}$$

is a $\mathbb{Z}$-order, which will be called the integral order "associated with", or "obtained from", $f$. When
it is convenient, we will write simply \( \mathcal{A} \) and \( R \) for \( \mathcal{A}(f) \) and \( R(f) \).

An element \( \alpha = x_0 + \sum x_k j_k \in R \) will be termed primitive if \( 1 = (x_0, x_1, x_2, x_3); \) primitive (mod \( m \)) if \( (x_0, x_1, x_2, x_3, m) = 1 \); pure (mod \( m \)) if \( (\alpha, 1) \equiv 0 \pmod{m} \). If \( \alpha \) is pure and primitive, \( \alpha \) will sometimes be called "pure-primitive" (as distinguished from "purely primitive").

The most familiar quaternion algebra is the Hamilton algebra \( \mathcal{A}(f) \) obtained from the form \( f = x^2 + y^2 + z^2 \). The corresponding order \( R_o = R(f) \) is the "Lipschitz ring" of integral quaternions. This system is not maximal; for if \( g = x^2 + y^2 + z^2 + xy + xz + yz \), then the Hurwitz ring, \( R(g) \), contains \( R_o \). In fact, we can write \( R(g) = \{ (x_0 + x_1i + x_2i_2 + x_3i_3)/2 : x_0 \equiv x_1 \equiv x_2 \equiv x_3 \pmod{2} \} \), where \( R_o = \mathbb{Z}[i_1, i_2, i_3] \). In general, it is well known (cf.[9]) that an integral order \( R(f) \) is maximal if and only if \( \text{adj } f \) is fundamental, in the sense that \( \text{adj } f \) cannot be obtained by an integral linear transformation of determinant greater than 1 from the adjoint of an integral ternary form. For, if \( d = 4 \det(a_{ij}) \), \( \text{adj } f \) is fundamental if and only if \( d \) is square free and \( c_p = -1 \) for each prime in \( d \), \( c_p \) denoting the Hasse symbol.

We remark in closing that no generality is lost by studying the rings \( R(f) \); for Estes* has shown that every ring \( R \) of integral quaternions containing four linearly independent elements such that

\*Dennis R. Estes, USC, in several letters to the author and to Professor Gordon Pall, LSU, communicated a number of (heretofore unpublished) ideas and results which have been utilized in this paper. Accordingly, the author wishes to acknowledge Professor Estes' contribution. Several ensuing results owe their inception, or are directly due, to him.
$1 \in \mathbb{R}$ is isomorphic to a quaternion order associated with an integral ternary form.
2.1 The Quadratic Case

Suppose $\alpha_1, \alpha_2$ are elements of the quadratic order $R_d = [1, \omega]$ such that $\alpha_1, \alpha_2$ are linearly independent over $\mathbb{Q}$. Let $\mathcal{M}$ be the two-dimensional $\mathbb{Z}$-module $[\alpha_1, \alpha_2]$. Then we may select a $\mathbb{Z}$-basis $k[a, r + so]$ for $\mathcal{M}$, where $a, r, s \in \mathbb{Z}$, $(a, r, s) = 1$, $k \in \mathbb{Q}$. In the $\mathbb{Z}$-module $[a, r + so]$, $s$ is the least positive integer coefficient of $\omega$ among the elements of the module, $a$ is the norm of the module, and $r$ is unique (mod $a$).

Now $[a, r + so]$ with $(a, r, s) = 1$ is an ideal in $R_d$ if and only if $s = 1$ and $a | N(r + so)$ (cf. [2], p. 32). We may then set

$$r + so = \frac{b + \sqrt{d}}{2}, \quad N(r + so) = \frac{b^2 - d}{4} = ac,$$

whence $b = (r + so, 1)$, the trace of $r + so$. Thus with the $\mathbb{Z}$-module $\mathcal{M} = [a, r + so]$ we may associate the form $\psi = [a, b, c]$. Notice that if $(a, 2d) = 1$, or if $d$ is fundamental, then $\psi$ is primitive; for if $p | (a, b, c)$, then $p^2 | b^2 - 4ac = d$, and $(b^2 - 4ac)/p^2$ is a discriminant.

Let $A$ denote the matrix of $\psi$, and suppose $\alpha \in \mathbb{F}_j$ such that $\alpha \mathcal{M} \subset \mathcal{M}$ or $\alpha \overline{\mathcal{M}} \subset \mathcal{M}$. Then we may select integers $t_1, t_2, t_3, t_4$ such that
\[ a = t_1 a + t_3 (r + \omega); \quad \text{and} \]

\[(2.1.1) \quad \alpha (r + \omega) = t_2 a + t_4 (r + \omega), \quad \text{or} \]

\[\alpha (r + \bar{\omega}) = t_2 a + t_4 (r + \omega).\]

One verifies easily that if

\[(2.1.2) \quad T = \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix},\]

then \(T'^T A T = (N_{\alpha}) A\). Also, \(\det T = N_{\alpha}\) or \(-N_{\alpha}\) according as \((2.1.1)_2\)
or \((2.1.1)_3\) is the case.

Conversely, suppose \(\psi = [a, b, c]\) is a binary quadratic form of
discriminant \(d\) with matrix \(A\), and that \(T\) is a \(2 \times 2\) integral
matrix such that \(T'^T A T = e A\). If \(T\) is given by \((2.1.2)\), then
\[\det T = t_1 t_4 - t_2 t_3 = \pm e.\]

Choose \(r\) so that \(r + \omega_d = (b + \sqrt{d})/2\),
and let \(\alpha_1 = t_1 a + t_3 (r + \omega), \alpha_2 = t_2 a + t_4 (r + \omega)\).

Assume \(\det T = e\). Then from the Gauss Lemma (cf \([1]\), p. 160)
we obtain the equations \(-at_2^2 = ct_3^2, bt_3 = at_4 - at_1\), whence
\[\alpha = (1/\phi) \alpha_1 = (r + \omega)^{-1} \alpha_2\]
satisfies \(N_{\alpha} = e\) and
\(\alpha([a, r + \omega]) \subseteq [a, r + \omega]\). If \(\det T = -e\), the Gauss Lemma yields
\(bt_1 = at_2 - ct_3, t_4 = -t_1\), whence \(\alpha_1 (r + \bar{\omega}) = \alpha_2 a\). Hence if
\(\alpha = (1/a) \alpha_1\), then \(N_{\alpha} = e\) and \(\alpha ([a, r + \omega]) \subseteq [a, r + \omega]\).

\[(2.1.3) \quad \text{Theorem:} \quad \text{Let} \ A \text{ be the matrix of a binary quadratic form} \]
\(\psi = [a, b, c]\) of discriminant \(d\), \(r + \omega = r + \omega_d = (b + \sqrt{d})/2\),
and \(m = [a, r + \omega]\). Then to each \(2 \times 2\) matrix \(T\) such that
\(T'^T A T = e A\) corresponds an \(\alpha \in F\) such that \(\alpha m \subseteq m\) or \(\alpha \bar{m} \subseteq m\).
Specifically, $\alpha = (1/a)\alpha_1$ and $N\alpha = \pm e$, where $(\alpha_1,\alpha_2) = (a, r + \omega)T$.

If $\psi$ is primitive, those $T$'s such that $T: \alpha M \rightarrow M$ form a ring $R$, isomorphic with $R_d$. Conversely, if $\alpha M$ or $\alpha \bar{M} \subset M$, $\alpha \in F_j$, there is an integral $2 \times 2$ matrix $T_\alpha$ satisfying $T_\alpha^T \alpha T_\alpha = (Na)A$.

Clearly $\alpha M \subset M$, $\beta M \subset M$ imply $(\alpha + \beta) M \subset M$, $\alpha \beta M \subset M$,

and we easily verify that $T_\alpha + \beta = T_\alpha + T_\beta$, $T_\alpha \beta = T_\alpha T_\beta = T_\beta T_\alpha = T_{\alpha \beta}$.

Also, $R' = \{\alpha \in F_j: \alpha M \subset M\} \supset R_d$, surely. And if $\psi$ is primitive, $R_d$ is the largest order within which $M$ is an ideal (cf [2]). Thus $R' = R_d$.

2.2. The Four-Dimensional Case

Let $A = (a_{ij})$ be a primitive $4 \times 4$ semi-integral matrix in the rational class of the matrix $B$ of a Brandt norm-form $G$ (whence $\det A \neq 0$), and let $\mathcal{O} = Q[1, i_1, i_2, i_3]$ be the quaternion algebra over $Q$ associated with $G$. Let $1, j_1, j_2, j_3$ be the $\mathbb{Z}$-basis for the integral order $R$ obtained from $G$, so that $N(x_0 + x_1 j_1 + x_2 j_2 + x_3 j_3) = G(x_0, x_1, x_2, x_3)$. Let $U$ be a rational matrix such that $U^T B U = A$,

and $k$ a non-zero integer such that $kU$ is integral. Then if $V = kU$, $V^T B V = k^2 A$. Hence if $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1, j_1, j_2, j_3)V$, then for $x' = (x_1, x_2, x_3, x_4)$, $x'^T A x = (1/k)^2 (N(\sum_i x_i \alpha_i))$.

Therefore $\mathcal{O}$ contains a four dimensional $\mathbb{Z}$-module $M = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ with norm form $N(\sum_i x_i \alpha_i) = m F(x_1, x_2, x_3, x_4)$ and having $A$ as the matrix of its primitive norm $F$.

Suppose that $\sigma, \rho \in \mathcal{O}$ satisfy $\rho M \sigma \subset M$. Then we can find integers $t_{ij}$, $1 \leq i, j \leq 4$, such that $\rho \alpha_i \sigma = \sum_j t_{ij} \alpha_j$. 


Let $T = (t_{ij})$. Now $(1/2)(\alpha_i, \alpha_j) = m a_{ij}$, so that $(\rho \alpha_i, \rho \alpha_j) = (Np)(N\sigma)(\alpha_i, \alpha_j) = 2m (Np)(N\sigma) a_{ij}$. But also, $(\rho \alpha_i, \rho \alpha_j) = (\sum r_{ri} \alpha_r, \sum s_{sj} \alpha_j) = \sum r_{ri} (\alpha_r, \alpha_s) t_{sj} = 2m \sum r_{ri} a_{rs} t_{sj}$, which is $2m$ times the $(i,j)$ entry in $T'AT$. Hence $T'AT = (Np)(N\sigma)A$.

Virtually identical reasoning yields this same result if we assume instead that $\rho \in M \subseteq N$.

The following useful lemma was essentially proved above:

(2.2.1) Lemma: Let $M$, $A$ be as above, and suppose that $S$ is a non-singular $4 \times 4$ matrix. Let $\beta_j$, $1 \leq j \leq 4$, be given by

$$(\beta_1, \beta_2, \beta_3, \beta_4) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)S.$$ Then $S'AS = (1/2m)((\beta_1, \beta_j))$.

(2.2.2) Lemma: (Estes): Let $1, \rho_1, \rho_2, \rho_3$ be linearly independent elements of $\mathcal{A}$ such that $(\rho_i, 1) = 0$, $i = 1,2,3$. Let

$$A = 1/2((\rho_1, \rho_j)) = (A_{ij}).$$ Then $\det A$ is the square of a rational number $d$, and, for a cyclic permutation $(i,j,k)$ of $(1,2,3),\rho_i \rho_j = -A_{ij} + \sum_n a_{nk} \rho_n,$ where $(a_{ij}) = (\text{adj } A)/d$.

Proof: Let $\rho_i \rho_j = r_0 + r_1 \rho_1 + r_2 \rho_2 + r_3 \rho_3$, $i \neq j$. Since $(\rho_i, \rho_j, 1) = -2A_{ij}$, we have that $r_0 = -A_{ij}$. Now $(\rho_i, \rho_j, \rho_i) = (\rho_i, \rho_j, \rho_j) = 0$, hence $(0,0,0) = 2(r_1, r_2, r_3)A$, $k \neq i,j$. Since $1, \rho_1, \rho_2, \rho_3$ are linearly independent, $\det A \neq 0$, and

$$(r_1, r_2, r_3) = (1/2 \det A)(0,0,0) \text{ adj } A.$$ Expanding the three terms $N(\rho_i \rho_j + A_{ij})$, $(\rho_i \rho_1 \rho_j, \rho_k)$, and $(\rho_i \rho_j \rho_j, \rho_k)$, we obtain the three equations.
Since one of $a_{kk}$, $a_{ik}$, $a_{jk}$ is not zero, $(\rho_1 \rho_j, \rho_k)^2 = 4 \det A$.

Choose $d = \pm \sqrt{\det A}$ so that $(\rho_1 \rho_2, \rho_3) = 2d$. Then $\rho_1 \rho_2 =$ 

$-A_{12} + a_{13} \rho_1 \rho_2 + a_{23} \rho_2 + a_{33} \rho_3$. Since $(\rho_1 \rho_2, \rho_3) = (\rho_3 \rho_1, \rho_2) = (\rho_2 \rho_3, \rho_1)$, the lemma follows. q.e.d.

Now suppose that $T$ is a $4 \times 4$ non-singular matrix such that $T'AT = eA$ (whence $e \neq 0$), and let $(\beta_1, \beta_2, \beta_3, \beta_4) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$.

Assume further that $\alpha_1$ is of non-zero norm. Then from (2.2.1) we conclude that $(\beta_1, \beta_j) = e(\alpha_1, \alpha_j)$, $1 \leq i, j \leq 4$. Thus $N\beta_1 \neq 0$. Also, $(1, \beta_1, \beta_j) = e(1, \alpha_1, \alpha_j)$, so that $(N\beta_1)(1, \beta_1^{-1}\beta_j) = (1, \beta_1^{-1}\beta_j) = e(1, \alpha_1, \alpha_j) = eN\alpha_1(1, \alpha_1^{-1}\alpha_j)$. Therefore, $(1, \beta_1^{-1}\beta_j) = (1, \alpha_1^{-1}\alpha_j)$, $1 \leq j \leq 4$.

Thus we may apply a transformation

$$
U = \begin{bmatrix}
1 & u_1 & u_2 & u_3 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix},
$$

so that if $(1, \gamma_1, \gamma_2, \gamma_3) = (1, \alpha_1^{-1}\alpha_2, \alpha_1^{-1}\alpha_3, \alpha_1^{-1}\alpha_4)U$ and $(1, \delta_1, \delta_2, \delta_3) = (1, \beta_1^{-1}\beta_2, \beta_1^{-1}\beta_3, \beta_1^{-1}\beta_4)U$, then each $\gamma_1, \delta_j$ is pure. Therefore

$$
U'AU = (N\alpha_1/2m) \begin{bmatrix}
1 & 0 \\
0 & ((\gamma_1, \gamma_j))
\end{bmatrix}.
$$
But also, $eU'AU = U'T'ATU$, and $(1, \delta_1, \delta_2, \delta_3) = \beta_1^{-1}(\beta_1, \beta_2, \beta_3, \beta_4)U = \beta_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)TU$. Hence

$$eU'AU = (N\beta_1/2m)\begin{bmatrix} 1 & 0 \\ 0 & \langle(\delta_i, \delta_j)\rangle \end{bmatrix} = e(N\alpha_1/2m)\begin{bmatrix} 1 & 0 \\ 0 & \langle(\delta_i, \delta_j)\rangle \end{bmatrix}.$$ 

Consequently, $((\gamma_i, \gamma_j)) = ((\delta_i, \delta_j))$, and so by (2.2.2) the $\gamma_i$'s have the same multiplication table as either the $\delta_j$'s or the $\overline{\delta}_j$'s. Hence we can find a quaternion $\xi$ and a sign $\tau = \pm 1$ such that $\tau \delta_j = \xi \gamma_j \xi^{-1}$, $1 \leq j \leq 3$ (cf. [9], p. 285).

If $\tau = +1$, then $(1, \delta_1, \delta_2, \delta_3)$ equals both $\beta_1^{-1}(\beta_1, \beta_2, \beta_3, \beta_4)$ and $\xi(1, \gamma_1, \gamma_2, \gamma_3)\xi^{-1} = \xi \alpha_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\xi^{-1}U$. Thus, taking $\rho = \beta_1 \xi \alpha_1^{-1}$, $\sigma = \xi^{-1}$, we have $\rho \alpha_i \sigma = \beta_1$, $1 \leq i \leq 4$.

If $\tau = -1$, we observe that $\xi \alpha_1^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\xi^{-1}U = (1, \delta_1, \delta_2, \delta_3) = (\beta_1, \beta_2, \beta_3, \beta_4)\beta_1^{-1}U$. Letting $\rho = \beta_1 \xi^{-1}$, $\sigma = \overline{\alpha}_1^{-1} \overline{\xi}$, it follows that $\beta_i = \rho \overline{\alpha}_1 \sigma$, $1 \leq i \leq 4$.

We've proved:

(2.2.3) Theorem: Let $\mathfrak{m} = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ be a four dimensional $\mathbb{Z}$-module in a quaternion algebra $\mathcal{A}$ such that $N\alpha_1 \neq 0$, and let $F$ be the primitive norm form of $\mathfrak{m}$, $A$ the matrix of $F$. Suppose $T$ is a $4 \times 4$ integral matrix such that $T'AT = eA$, $e \neq 0$. Then we can find quaternions $\rho, \sigma \in \mathcal{A}$ satisfying

(i) $(N\rho)(N\sigma) = e$

(ii) $\rho \mathfrak{m} \sigma \subset \mathfrak{m}$, $\rho(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\sigma = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$, or $\rho \overline{\mathfrak{m}} \sigma \subset \mathfrak{m}$, $\rho(\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3, \overline{\alpha}_4)\sigma = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T$.

Conversely, if $\rho \mathfrak{m} \sigma$ or $\rho \overline{\mathfrak{m}} \sigma \subset \mathfrak{m}$, then the matrix $T$ determined by (ii) satisfies $T'AT = (N\rho)(N\sigma)A$. 
Thus (2.2.3) establishes an essentially unique association between pairs \((\rho, \sigma) \in A \times A\) such that \(\rho \cdot \sigma \in \mathcal{M}\), or \(\rho \cdot \overline{\sigma} \in \mathcal{M}\), with \((N\rho)(N\sigma) \neq 0\), and 4 x 4 integral matrices \(T: \rho \cdot \sigma \rightarrow \mathcal{M}\), or \(T: \rho \cdot \overline{\sigma} \rightarrow \mathcal{M}\), such that \(T'AT = eA\), \(e \neq 0\); "essentially unique" in the sense that \((\rho, \sigma)\) and \((\rho q, \rho^{-1} \sigma)\) gives rise to the same \(T\) for any non-zero rational number \(q\). Those matrices \(T: \rho \cdot \sigma \rightarrow \mathcal{M}\) form a (non-commutative) multiplicative semigroup, and those associated with pairs \((\rho, 1)\) form a ring \(R^1\), as is easily verified; for if \(T: \rho \cdot \sigma \rightarrow \mathcal{M}\), then we may identify \(T\) and \(\rho\). A necessary and sufficient condition that \(R^1\) be isomorphic with \(R = [1, i_1, i_2, i_3]\) is evidently that \(\mathcal{M}\) be an ideal in \(R\) and not in any larger ring. Clearly the same remarks apply for those \(T\)'s associated with pairs \((1, \sigma)\).

If \(T_1: \rho \cdot \sigma \rightarrow \mathcal{M}\), \(T_2: \sigma \rightarrow \mathcal{M}\), then \(T_1T_2 = T_2T_1: \rho \cdot \sigma \rightarrow \mathcal{M}\), since \((\alpha_1, \alpha_2, \alpha_3, \alpha_4)T_1T_2 = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)T_2T_1 = \rho(\alpha_1, \alpha_2, \alpha_3, \alpha_4)\sigma\).

We are thus led to the following questions: Which matrices \(T\) satisfying \(T'AT = eA\) may be written \(T = T_1T_2\), where \(T_1: \rho \cdot \sigma \rightarrow \mathcal{M}\), \(|U| = \pm 1\), \(T_2: \sigma \rightarrow \mathcal{M}\) ? And, when such a factorization is possible, what about uniqueness? We observe the following with these questions in mind:

Let \(k\) be a positive integer, \(\mathcal{M} = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]\) as above. With any 4 x \(k\) rational matrix \(V = (v_{ij})\) we may associate a \(k\)-tuple of quaternions \((\beta_1, \ldots, \beta_k) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)V\). Hence we may write \(V = [\beta_1, \ldots, \beta_k]_{\mathcal{M}}\). Conversely, for any particular \(Z\)-basis \(\alpha_1, \alpha_2, \alpha_3, \alpha_4\) of \(\mathcal{M}\), we may associate with any \(k\) vectors \(\beta_1, \ldots, \beta_k\)
a 4 x k matrix $V = [\beta_1 \ldots \beta_k]$ since $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ may serve as a basis for $\mathcal{A}$ over $Q$. If $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1, j_1, j_2, j_3)$, write $V = [\beta_1 \ldots \beta_k]$, and call $\beta_s$ the "s-th column quaternion of $V". Similarly we may discuss "row quaternions" of any k x 4 matrix.

(2.2.4) Lemma: $[\alpha \mu \alpha \zeta \alpha \rho \alpha \sigma] = [\alpha \alpha j_1 \alpha j_2 \alpha j_3][\mu \zeta \rho \sigma]$, $[\mu \alpha \zeta \alpha \rho \alpha \sigma \alpha] = [\alpha j_1 \alpha j_2 \alpha j_3 \alpha][\mu \zeta \rho \sigma]$. The proof is easy. Also, a matrix $[\alpha \alpha j_1 \alpha j_2 \alpha j_3]$ may be termed a "right quaternion matrix," $[\alpha j_1 \alpha j_2 \alpha j_3 \alpha]$ a "left quaternion matrix". The following has already been observed:

(2.2.5) Corollary: $[\alpha \alpha j_1 \alpha j_2 \alpha j_3][\beta j_1 \beta j_2 \beta j_3 \beta] = $ $[\beta j_1 \beta j_2 \beta j_3 \beta][\alpha \alpha j_1 \alpha j_2 \alpha j_3 \beta]$. These are matrices $\alpha R \rightarrow R$, $R \beta \rightarrow R$.

Thus our question about factorization of matrices seems to be one about factorization of quaternions; and hence the question of uniqueness may be settled in part by (3.3). We answer these questions in the instance that $\mathfrak{m} = [1, i_1, i_2, i_3]$, the order of Lipschitz quaternions.

2.3 The Lipschitz Ring

Let $R_0 = [1, i_1, i_2, i_3]$ denote the Lipschitz ring of integral quaternions, and suppose that $m$ is a positive integer, 1 the $4 \times 4$ identity matrix, and $T = (t_{ij})$ a $4 \times 4$ integral matrix satisfying $T'T = mI$. We assume with no loss of generality that
T is primitive. Notice that $T'T = mI$ implies that $TT' = mI$. Let $\alpha_s, \beta_s$ denote the $s$th column quaternion, row quaternion of $T$, respectively. It follows from (2.2.1) that $\frac{1}{2}(\alpha_i, \alpha_j) = \frac{1}{2}(\beta_i, \beta_j) = m \delta_{ij}$, where $\delta_{ij}$ is the Kronecker symbol.

Since $T$ is primitive, if $p$ is an odd prime dividing $m$, then at least two of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are primitive (mod $p$); for if three are imprimitive (mod $p$), so must be the fourth. We may assume $\alpha_1, \alpha_2$ are primitive (mod $p$). Because $N\alpha_1 = m$, $1 \leq i \leq 4$, $\alpha_1, \alpha_2$ have either the same right divisors, or the same left divisors (or both) of norm $p$, and such divisors certainly exist (cf. [8]). Thus $\alpha_1$ and $\alpha_2$ have a common right (say) divisor $\gamma$ or norm $p$.

If $\alpha_k, k = 3$ or $4$, is also primitive, then $\alpha_1$ and $\alpha_k$ have $\gamma$ as a common left or right divisor. If $\gamma$ is a right divisor of $\alpha_1$ and $\alpha_k$, then all three of $\alpha_1, \alpha_2, \alpha_k$ have $\gamma$ as a right divisor.

If $\alpha_1$ and $\alpha_k$ have $\gamma$ as a left divisor, we consider $\gamma$ as a factor of $\alpha_2$ and $\alpha_k$, then $\gamma$ is a right [left] divisor of all three of $\alpha_1, \alpha_2, \alpha_k$. If the fourth $\alpha_j$ is also primitive (mod $p$), the above argument may be reapplied to yield the result that $\gamma$ is a common left divisor or a common right divisor of each of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

Further, if a quaternion $\mu$ satisfies $\mu \equiv 0$ (mod $p$), then any quaternion of norm $p$ is both a left and a right divisor of $\mu$.

Also, the above reasoning applies if the words "right" and "left" are interchanged. Hence:

(2.3.1) Lemma: Suppose $T$ is a primitive $4 \times 4$ non-singular integral matrix such that $T'T = mI$, and that $p$ is an odd prime dividing $m$. 
Let \( \alpha_1, \alpha_2, \alpha_3, \alpha_4 \) be the column quaternions of \( T \). Then there exists a quaternion \( \gamma \in R_0 \) of norm \( p \) such that \( \gamma \) is a common left or right divisor of \( \alpha_1, \alpha_2, \alpha_3, \alpha_4 \).

Suppose \( \alpha_i = \alpha_i \gamma, \) \( 1 \leq i \leq 4 \). Then from (2.2.3) we conclude that \( T = US = [\gamma \ y_1 \gamma \ y_2 \gamma \ y_3 \gamma][\alpha_1 \ \alpha_2 \ \alpha_3 \ \alpha_4 \gamma] \). Now \( U^T U = (Ny)I \), so that \( T'T = mI \) implies \( S'S = (m/Ny)I \). A similar result holds if \( \gamma \) is a common left divisor of \( \alpha_i, \) \( 1 \leq i \leq 4 \), only then
\[
T = VS = [\gamma \ y_1 \gamma \ y_2 \ y_3 \gamma][\alpha_1 \ \alpha_2 \ \alpha_3 \ \alpha_4 \gamma].
\]
Hence, in view of (2.3.1), we may take \( Ny = p \) for any odd prime factor \( p \) of \( m \), repeat the process with \( S \), and so on until the supply of such factors is exhausted. We thus obtain a factorization \( T = LRE = RLE \), where
\[
(2.3.2) \quad R = [\mu \ \mu_1 \ \mu_2 \ \mu_3], \quad L = [\xi \ i_1 \xi \ i_2 \xi \ i_3 \xi],
\]
det \( L = m_1^2 \), det \( R = m_2^2 \), where \( (2, m_1 m_2) = 1 \) and \( 2^\lambda = m/m_1 m_2 \) is such that \( E'E = 2^\lambda I \). Further, \( \lambda = 0, 1, \) or \( 2 \), since \( T \) is primitive, and if \( 8 \) divides a sum of four squares, each term must be even.

Suppose \( \delta_i \) is the \( i \)-th column quaternion of \( E \), \( 1 \leq i \leq 4 \). Assume \( \lambda = 2 \). Then \( N\delta_i = 4 \) implies \( \delta_i(1 - i_k) \equiv (1 - i_k)\delta_i \equiv 0 \) (mod 2), \( 1 \leq k \leq 3 \), since \( N(\delta_i(1 - i_k)) = 8 \). Hence \( 1 + i_k \) is both a left and right divisor of each \( \delta_i \), and so we may write \( E = RE_1 = LE_2 \), \( R, L \) as in (2.3.2), each of determinant \( 4 \), and \( E_1'E_1 = E_2'E_2 = 2I \). Thus the case \( \lambda = 2 \) may be reduced to the case \( \lambda = 1 \).

If \( \lambda = 1 \), then we see that \( \delta_1, \delta_2, \delta_3, \delta_4 \) must in some order be given by \( \pm i, \pm i_j \), \( \pm i, \pm i_k, \pm i_j \), \( \pm i, \pm i_k \), with \( j, k, n \) distinct. Now
$1 + i_k$ and $1 - i_k$ are divisors (left and right) of $1 \pm i_k$, and, if $j, n \neq k$, $i_j \pm i_n$ is equal to $i_j(1 + i_k) = (1 - i_k)i_j$, or to $i_j(1 - i_k) = (1 + i_k)i_j$. Hence we may write $E = RW_1 = LW_2$, where $R, L$ are given by (2.3.2), and each is of determinant 4. $W_1, W_2$ have determinants $\pm 1$.

(2.3.3) Theorem: Suppose $T'T = mI, T$ primitive. Then there exists a factorization $T = RLW = LRW$, $W$ unit-modular (i.e., det $W = \pm 1$), det $R = m_1^2$, det $L = m_2^2$, $m = m_1m_2$, with $R, L$ as in (2.3.2). Further, if $m$ is odd, the factorization $m = m_1m_2$ is unique.

Everything has been shown but uniqueness. We need several lemmas:

(2.3.4) Lemma: Suppose $\rho_1, \rho_2, \rho_3 \in R_0$ such that $(\rho_k, 1) = 0$, and such that $\rho_1, \rho_2, \rho_3$ have the same multiplication as $i_1, i_2, i_3$. Then there exists a sign $\sigma = \pm 1$ and a unit $\xi \in R_0$ such that

$$\sigma \rho_k = \xi i_k \overline{\xi}, \quad k = 1, 2, 3$$

This follows from the proof of Lemma 1 in [9], p. 285.

(2.3.6) Lemma: Suppose $R, L$ are right, left quaternion matrices respectively, and det $U = \pm 1$. Then if $RL = qU$, $q$ rational and not zero, then $R$ and $L$ are within unimodular factors of a diagonal matrix.

proof: Let $U = [\theta_0 \theta_1 \theta_2 \theta_3]$, $N\theta_k = 1, 0 \leq k \leq 3$. Let $\rho_k = \overline{\theta_0}\theta_k$, $k = 1, 2, 3$. Since $U'U = I$, it follows that $\rho_1, \rho_2, \rho_3$ satisfy the
hypothesis of (2.3.4). Choose $\sigma = \pm 1$ and $\xi \in R_0$ as in (2.3.5). Then $U = R_1 L_1 J$, where $R_1 = [\Theta_0 \xi \quad \Theta_0 \xi i_1 \quad \Theta_0 \xi i_2 \quad \Theta_0 \xi i_3]$, $L_1 = [\xi i_1 \xi i_2 \xi i_3; \quad J = [1 \quad \sigma_1 \quad \sigma_2 \quad \sigma_3]$. Further, $\sigma = 1$, since $\sigma^2 = \det J = \det U = (1/q^4)(\det R)(\det L) > 0$. Hence $J = I$, and $R_1'R = L_1'L$ is thus both a left and right quaternion matrix. Consequently, $R_1'R$ is a scalar multiple of $I$. q.e.d.

proof of (2.3.3): Suppose $T = R_1 L_1 W_1 = R_2 L_2 W_2$, $R_1, R_2$ right quaternion matrices, $L_1, L_2$ left quaternion matrices, and $W_1, W_2$ unit-modular. Since $T$ is primitive, so are $L_1$ and $R_1$. Let $U = W_2 W_1'$. Then $(R_2'R_1)(L_2'L_1) = mU$, and hence we can find integral unimodular matrices $V, W$, and integers $q, s$ such that $R_2'R_1 = qV, L_2'L_1 = sW$. Let $R_1'R_1 = r_1 I$, $R_2'R_2 = r_2 I$, $L_1'L_1 = t_1 I$, $L_2'L_2 = t_2 I$. If follows that $q^2 = r_1 r_2$, $s^2 = t_1 t_2$, and that $L_1 = (s/t_2)L_2 W$, $R_1 = (q/r_2)R_2 V$. Since $R_1$ and $L_1$ are primitive, $s|t_2$ and $q|r_2$. Hence $(r_2/q)r_1 = q$, $(t_2/s)t_1 = s$, so $r_1|q$, $t_1|s$. Also, $q^2 s^2 = r_1 r_2 t_1 t_2 = m^2 = r_1^2 t_1^2 = |\det T|$, so $r_1 t_1 = qs$. Thus $r_1 = q$, $t_1 = s$. Similarly, $r_2 = q$, $t_2 = s$. Consequently, the factorization $T = R_1 L_1 W_1$ is essentially unique. q.e.d.

(2.3.7) Corollary: Let $R$ and $L$ be as in (2.3.2). Then $RL$ is primitive if and only if $R$ and $L$ are.

proof: In the proof of (2.3.3) just above, we obtained essential uniqueness using only the fact that $R_1$ and $L_1$ were primitive. Clearly essential uniqueness does not follow if $T$ is imprimitive. q.e.d.
We remark in passing that, if \( m \) is even, the factorization \( T = RLU, |\det T| = (\det R)(\det L) \) is not unique, even if \( T \) is primitive; for the quaternion matrices of determinant \( 4 \) may be taken as left or right, as has been shown.

(2.4) **Remarks on Rings of Transformations - The \( n \)-Dimensional Case**

Let \( A \) be an \( n \times n \) positive-definite symmetric matrix over the reals \( \mathbb{R} \), and let \( \mathcal{J} \) be a set of matrices over \( \mathbb{R} \) such that:

(a) \( \mathcal{J} \) is an \( \mathbb{R} \)-module and a ring containing the identity matrix;

(b) If \( S \in \mathcal{J} \), then there is an \( r \in \mathbb{R} \) such that \( S'AS = rA \); and

(c) If \( S \in \mathcal{J} \) satisfies \( S^2 = 0 \), then \( S = 0 \).

For \( S \in \mathcal{J} \), define the norm of \( S \) by \( N(S) = r \), where \( S'AS = rA \).

It follows that if \( S, S_1 \in \mathcal{J}, \lambda \in \mathbb{R} \), then \( N(SS_1) = (NS)(NS_1) \), and \( N(\lambda S) = \lambda^2 N(S) \). Define the inner product \( (S, T) \) by

\[
(S, T) = N(S + T) - NS - NT.
\]

Then \( (S, T) = (T, S) \), and \( N(S + T)A = (S' + T')A(S + T) = (NS)A + (NT)A + S'AT + T'AS \). Therefore \( S'AT + T'AS = (S, T)A \). From this follows \( (\lambda_1 S_1 + \lambda_2 S_2, S) = \lambda_1(S_1, S) + \lambda_2(S_2, S) \), so the inner product is bilinear.

Suppose that \( S_0 \in \mathcal{J} \) such that \( (S_0, S) = 0 \) for each \( S \in \mathcal{J} \). Then, in particular, \( (S_0, 1) = 0 \), so \( S_0'1A = -A^{-1}S_0'1A = S_0 \).

Thus \( S_0^2 = 0 \), so \( S_0 = 0 \).

Therefore \( \mathcal{J} \) is a non-degenerate, associative composition algebra over \( \mathbb{R} \). Hence \( \dim \mathcal{J}:\mathbb{R} = 1, 2, \) or \( 4 \) (cf. \([4]\))

Suppose that \( \dim \mathcal{J}:\mathbb{R} = 4 \). Then \( \mathcal{J} \) has a basis \( 1, E_1, E_2, E_3 \)
over $\mathbb{R}$ with norm form $x^2 + y^2 + z^2 + w^2$ or $x^2 + y^2 - z^2 - w^2$ (the determinant of the norm form must be a square, thus precluding index 1 or 3). Since $A$ is positive definite, the former must be the case, since for $S \in \mathcal{J}$, $NS$ is represented by the $n$-ary quadratic form with matrix $A$. Also, it follows easily that $(E_j, I) = (E_j, E_k) = 0$ if $1 \leq j, k \leq 3$, $j \neq k$, and hence that $E_j A = -AE_j$. Thus $A = E_j AE_j = -AE_j^2$, $E_j^2 = I$. Further, if $i \neq j$, $0 = (E_i, E_j)A = E_i AE_j + E_j AE_i = -A(E_i E_j + E_j E_i)$.

Therefore, $E_1, E_2, E_3$ satisfy

$$(2.4.1) \quad E_j^2 = -I, \quad E_i E_j + E_j E_i = 0, \quad i \neq j.$$ 

Accordingly, we recall two theorems of M.H.A. Newman in [6]:

$(2.4.2)$ Theorem: If $n = 2^q p$ where $p$ is odd, and $\{E_1, E_2, \ldots, E_M\}$ is a set of $n \times n$ matrices satisfying $(2.4.1)$, then $M \leq 2q + 1$; and this maximum is attained.

A set satisfying $(2.4.1)$ Newman calls an "E-set". A "maximal" E-set has the obvious meaning. It is easily shown that a maximal E-set contains an odd number of elements.

$(2.4.3)$ Theorem: If all members of a maximal E-set are real or pure imaginary, say $R$ real and $I$ imaginary, then $R - I = -1$ or $7$.

Therefore we may conclude that $\{E_1, E_2, E_3\}$ is not a maximal E-set, and that if $n = 2^q p$, $p$ odd, then $2q + 1 \geq 5$, $q \geq 2$. Hence $n \equiv 0 \pmod{4}$.

Now suppose that $\dim \mathcal{J} : \mathbb{R} = 2$. Then $\mathcal{J}$ has a basis $1, E$ over $\mathbb{R}$.
with norm form \( x^2 + y^2 \). From (2.4.2) and (2.4.3) we conclude

\[ 2q + 1 \geq 3, \; n \text{ even}. \]

Thus if \( n \) is odd, \( \dim \mathcal{A} : \mathcal{R} = 1 \). We remark in passing that, if we remove the restriction that \( A \) be definite, we can still conclude that \( n \) is even when \( \dim \mathcal{A} : \mathcal{R} = 4 \).
CHAPTER III
RINGS OF INTEGRAL QUATERNIONS

Let $f$ be an integral ternary quadratic form with matrix $(a_{ij})$, and let $\mathcal{A} = \mathbb{Q}[1,i_1,i_2,i_3]$ and $R = \mathbb{Z}[1,j_1,j_2,j_3]$ be respectively the quaternion algebra and the integral order obtained from $f$. Let $F = (x_o + \frac{1}{2} \sum_k x_k \epsilon_k)^2 + \text{adj } f$ be the associated Brandt norm-form, and suppose $d = 4 \det (a_{ij}) \neq 0$.

Let $c_p = c_p(f)$ denote the Hasse symbol. An ideal $A$ (left or right) of $R$ will be called primitive if $AC \subseteq aR$ for some $a \in \mathbb{Z}$ implies $a = \pm 1$. If $S$ is a set such that $S \subseteq R$, $(S)$ will denote the left ideal generated by $S$, and $[S]$ the right ideal generated by $S$. Also, we will sometimes write $x_o + \sum_k x_k j_k = x_o' + \sum_k x_k i_k$, where $x_o' = x_o + (1/2) \sum_k \epsilon_k x_k$.

We insert here a needed theorem on form residues (cf. [9]).

(3.1) Theorem: If $p$ is an odd prime not dividing $d$ or dividing $d$ at most once, we can assume

$$f \equiv a_1 x_1^2 + a_2 x_2^2 + p x_3^2 \mod p^r,$$

$r$ arbitrary, where $(a_1 a_2 a_3, p) = 1$, and $\alpha$ is 0 or 1; if $\alpha = 1$,

$$c_p = \frac{(-a_1 a_2)}{p}.$$ If $d$ is odd, $f$ is equivalent $(\mod 2^r)$ to the form

$$f \equiv x_1 x_2 + a_3 x_3^2,$$

$a_3$ odd; and if $d \equiv 2(\mod 4)$ and $c_2 = -1$, then $f$ is equivalent $(\mod 2^r)$ to the form
Form residues for coprime moduli may be achieved simultaneously.

(3.2) Corollary: If $\alpha$ is primitive and $m|N\alpha$, then if $p$ is a prime dividing $d$ precisely once and satisfying $c_p = -1$, $m$ cannot be divisible by $p^2$.

Pall in [9] applied (3.1) to prove the following useful theorems:

(3.3) Theorem: Let $\alpha \in R$ be primitive. If $N\beta = m$, and $\beta$ is a right divisor of $\alpha$, then the only right divisors of $\alpha$ with norm $m$ are the left associates $\theta\beta$, $N\theta = 1$, provided

\[ m \text{ is not divisible by any prime } p \text{ such that } p^2|d \text{ or such that } p|d \text{ and } c_p = +1. \]

(3.5) Theorem: Let $m$ be a non-zero integer represented by some form in the genus of $F$ such that $m$ satisfies (3.4). Suppose $\alpha \in R$ is primitive, $m|N\alpha$. Then every factorization $\alpha = \gamma\beta$ in which $N\theta = m$ may be associated with a representation of the number 1 by a certain quaternary quadratic form in the genus of $F$. Hence, unless the genus of $F$ contains a class of forms which do not represent 1, there exists a right divisor $\beta$ of norm $m$ of $\alpha$, and necessarily (by (3.3)) unique up to a left unit factor.

The following theorem is another useful application of (3.1), embodying facts needed later.
(3.6) Theorem: Suppose that \( (m,d) = 1 \) and that \( \beta \) is primitive \( (\mod m) \), \( m \mid N \beta \). Then if \( \gamma \) is both a left and right divisor of \( \beta \) of norm \( m \), \( \gamma \) is a left and right divisor of \( \alpha \) if and only if \( \alpha \equiv s \beta \pmod{m} \) for some integer \( s \).

Proof: The sufficiency is clear. Suppose \( \gamma = t_o + \sum_{k} t_k j_k \) is a right and left divisor of both \( \beta \) and \( \alpha = x_o + \sum_{k} x_k j_k \), and that \( N \gamma = m \). Since \( \beta \) is primitive, so is \( \gamma \).

Let \( p > 2 \) be a prime such that \( p^r \mid m \). Using form residues (3.1), the congruences \( \overline{\alpha \gamma} = \overline{\gamma \alpha} = 0 \pmod{p^r} \) imply the existence of integers \( a_1, a_2, a_3 \) satisfying \( (a_1 a_2 a_3, p) = 1 \) and

\[
\begin{align*}
&x_0 t_o' + a_2 a_3 x_1 t_1 + a_3 a_1 x_2 t_2 + a_1 a_2 x_3 t_3 \equiv 0 \\
&x_1 t_o' - x_0 t_1 + a_1 x_3 t_2 - a_1 x_2 t_3 \equiv 0 \\
&x_2 t_o' - a_2 x_3 t_1 - x_0 t_2 + a_2 x_1 t_3 \equiv 0 \\
&x_3 t_o' + a_3 x_2 t_1 - a_3 x_1 t_2 - x_0 t_3 \equiv 0 \\
&x_1 t_o' - x_0 t_1 - a_1 x_3 t_2 + a_1 x_2 t_3 \equiv 0 \\
&x_2 t_o' + a_2 x_3 t_1 - x_0 t_2 - a_2 x_1 t_3 \equiv 0 \\
&x_3 t_o' - a_3 x_2 t_1 + a_3 x_1 t_2 - x_0 t_3 \equiv 0 \pmod{p^r}.
\end{align*}
\]

The congruences (3.7) imply that, \( \pmod{p^r} \), \( x_1 t_o' \equiv x_0 t_1' \), \( x_3 t_2 \equiv -x_2 t_3 \), \( x_2 t_o' \equiv x_0 t_2' \), \( x_3 t_o' \equiv x_0 t_3' \), \( x_1 t_3' \equiv x_3 t_1' \), \( x_2 t_1' \equiv x_1 t_2' \). Since \( \gamma \) is primitive \( (\mod m) \), \( t_o' \neq 0 \pmod{p} \), or \( (t_k'p) = 1 \) for some \( k = 1, 2, 3 \). Let \( u \) be the unique residue \( (\mod p^r) \) such that \( ut_k' \equiv 1 \pmod{p^r} \), or \( ut_o' \equiv 1 \pmod{p^r} \), and let \( s = ux_k' \), or \( s = ux_o' \). Then \( \alpha \equiv sy \pmod{p^r} \).
If \( d \) is odd, we can use the residue \( f \equiv x_1 x_2 + a_3 x_3^2 \pmod{2^k} \), \( a_3 \) odd, whence \( \alpha \bar{\gamma} = \bar{\gamma} \alpha \equiv 0 \pmod{m} \) implies

\[
\begin{align*}
x_0 t_0 - a_3 x_2 t_1 + x_0 t_3 & \equiv 0 \\
x_1 t_0 - (x_0 + x_3) t_1 + x_1 t_3 & \equiv 0 \\
x_2 t_0 - x_0 t_2 & \equiv 0 \\
x_3 t_0 + a_3 x_2 t_1 - a_3 x_1 t_2 - x_0 t_3 & \equiv 0
\end{align*}
\tag{3.8}
\]

From (3.8) we obtain \( x_0 t_0 = x_1 t_1 \pmod{2^r} \), \( k, \ell = 0, 1, 2, 3 \). Hence \( \alpha \) is proportional to \( \gamma \pmod{2^r} \). Using the Chinese Remainder Theorem, \( \alpha \) is proportional to \( \gamma \pmod{m} \). \( \text{q.e.d.} \)

(3.9) Corollary: If \( \alpha, \beta \) are purely integral, \( \gamma \) primitive such that \( N \gamma = m, (m, d) = 1 \), and if \( m \) is odd, or if \( R \) is a maximal order, then the equation \( \gamma \alpha \bar{\gamma} = m \beta \) implies the existence of an integer \( x_0 \) such that \( x_0/2 + \alpha = \delta \gamma \) (whence \( \beta = \gamma \delta - x_0/2 \)).

Proof: There is a unique integer residue \( u \pmod{2} \) such that \( u/2 + \alpha \) is integral. \( \gamma \alpha \bar{\gamma} = m \beta \) and \( N \gamma = m \) imply

\( \gamma(u/2 + \alpha) \bar{\gamma} = m(u/2 + \beta) \). Thus \( N(u/2 + \alpha) = N(u/2 + \beta) \in \mathbb{Z} \), and

\( (u/2 + \alpha, 1) = (u/2 + \beta, 1) = u \in \mathbb{Z} \). Hence \( u/2 + \alpha, u/2 + \beta \) are integral, and thus, if \( R \) is maximal, \( u/2 + \alpha, u/2 + \beta \in R \). Further,

\( \gamma(u/2 + \alpha) = (u/2 + \beta) \gamma \in R \) have \( \gamma \) (primitive) as a left and right
divisor of norm $m$. Hence we may select an integer $s$ such that $\gamma(u/2 + \alpha) = s\gamma \pmod{m}$. Let $x_0 = 2s - u$. Then $(x_0/2 + \alpha)\gamma = \gamma - (u/2 + \alpha)\gamma = s\gamma - s\gamma = 0 \pmod{m}$. Therefore $(x_0/2 + \alpha)\gamma = m\delta$, $x_0/2 + \alpha = \delta\gamma$.

If $m$ is odd, then we see easily that $u/2 + \alpha \in R$ if and only if $u/2 + \beta \in R$, so the restriction that $R$ be maximal is, in this case, unnecessary. q.e.d.

We will call $R$ "m-maximal" if, for $\alpha \in R$, the conditions

\begin{align*}
(i) \quad N\alpha &\equiv 0 \pmod{m^2}, \text{ and} \\
(ii) \quad (\alpha, R) &\equiv 0 \pmod{m}
\end{align*}

(3.10)

imply $\alpha \equiv 0 \pmod{m}$, where $(\alpha, R) = \{(\alpha, \beta): \beta \in R\}$. Notice that if $n|m$ and $R$ is m-maximal, then $R$ is n-maximal. A characterization of m-maximal orders will be given later (see (3.13), p. 28). We first derive some properties of these rings.

(3.11) Theorem: Suppose that $R$ is m-maximal, $\alpha$ a primitive element of $R$ such that $m|N\alpha$. Then we can find an element $\gamma \in R$ such that $(m, N(\alpha + m\gamma)/m) = 1$.

proof: (Estes) Let $N\alpha = mq$, $n = \prod[p: p \text{ is prime, } p|m, (p, q) = 1]$, and suppose $p$ is a prime such that $p|(m, q)$. Now $N\alpha \equiv 0 \pmod{p^2}$ and $\alpha \not\equiv 0 \pmod{p}$, so there is an element $\delta \in R$ such that $(\alpha, \delta) \not\equiv 0 \pmod{p}$. Now $N(\alpha + nm\delta) = m(q + n^2 m\delta + n(\alpha, \delta))$,

and $q + n^2 m\delta + n(\alpha, \delta) \not\equiv 0 \pmod{p}$, nor is it divisible by any prime which divides $m$ but does not divide $q$. If this process
is continued, we obtain the required $y$. q.e.d.

(3.12) Corollary: Let $R$ be $m$-maximal, $B$ a primitive left ideal of $R$ of norm $m$. Then we can find $\beta \in B$ such that $B = (m, \beta]$.

proof: (Estes) By (3.11), there exists $\beta \in B$ such that $(m, N\beta/m) = 1$. Let $N\beta = qm$. Since $(q, m) = 1$, $B = (m, qB]$.

Suppose $y \in B$. Then $N\gamma\beta \equiv 0 \pmod{m^2}$, and, for $\delta \in R$,

$$
(y\beta, \delta) = (y, \delta\beta) = N(y + \delta\beta) - N\gamma - N(\delta\beta) \equiv 0 \pmod{m},
$$

since $y + \delta\beta, \gamma, \text{ and } \delta\beta \in B$. Thus $\gamma\beta \equiv 0 \pmod{m}$, $\gamma\beta = m\xi$.

$qy = \xi\beta$. Therefore $B = (m, qB] \subseteq (m, \beta] \subseteq B$, $B = (m, \beta]$. q.e.d.

(3.13) Theorem: Let $Z_p = \{r/s : r, s \in Z, (p, s) = 1\}, R_p = Z_p R$.

The following are equivalent:

(i) $R$ is $m$-maximal;

(ii) $m$ satisfies (3.4);

(iii) $R_p$ is a maximal $Z_p$-order for each prime $p$ in $m$.

proof: (i) $\Rightarrow$ (ii). Suppose $p^2 | (m, d)$, or $p \parallel d$ and $c_p = +1$. Then $\text{adj } f$ is not fundamental, so there exists a ternary form $g$ and an integral matrix $T$ of determinant $e > 1$ such that $(\text{adj } g)^T = \text{adj } f$.

Further, $\text{adj } g$ may be assumed to be fundamental, so that $p | e$ ($c_p$ is invariant under rational transformations). Let $(B_{ij})$ be the matrix of $\text{adj } f$, $k_1, k_2, k_3$ the basal elements of $G(f)$, and $i_1, i_2, i_3$ the basal elements of $G(g)$. Then $(k_1, k_2, k_3) = (i_1, i_2, i_3)T$, and the transformation replacing the norm form $G = (x_0 + \frac{1}{2} \sum_k \varepsilon_k x_k^2 + \text{adj } g$ by the norm form $F = (y_0 + \frac{1}{2} \sum_k \varepsilon_k^* y_k^2 + \sum_{i,j} B_{ij} y_i y_j$ is the integral.
transformation $X = TY$, $x'_0 = y'_0 + \frac{1}{2}(\epsilon'^* - \epsilon'T)Y$, where

$$X' = (x'_1, x'_2, x'_3), \quad Y' = (y'_1, y'_2, y'_3), \quad \epsilon'^* = (\epsilon'_1, \epsilon'_2, \epsilon'_3),$$

Now we may replace $f, g$ by equivalent forms $V'fV, U'gU$, 

$$\det U = \det V = 1, \text{ whence } T \text{ is replaced by } U'T \text{ adj } V'.$$

Thus with $U$ and $V$ at our disposal, we may assume that $T$ is diagonal, say

$$T = \begin{bmatrix} t_1 & 0 & 0 \\ 0 & t_2 & 0 \\ 0 & 0 & t_3 \end{bmatrix}.$$ 

Thus, $p|t_1 t_2 t_3$, $p|t_k$ for some $k = 1, 2, 3$. If, say, $p|t_2$, then

$$4B_{22} = 4 \text{ adj } g (0, t_2, 0) \equiv 0 \pmod{p^2}.$$ 

Thus integers $y'_0, y'_1, y'_2, y'_3$ not all zero $\pmod{p}$ may be chosen so that $y'_0 \equiv 0 \pmod{p}$ if $p$ is odd, $\Sigma \epsilon_k \epsilon' \equiv 0 \pmod{p}$ if $p = 2$, since

$$4(B_{ij}) = \epsilon' \epsilon' \pmod{2} \quad \text{(cf. [9])}, \text{ and so that } Ny = y'_0 + \Sigma B_{ij} y'_i y'_j \equiv 0 \pmod{p^2}.$$ 

(Specifically, $y'_k B'_{kk} \equiv 0 \pmod{p}$ if $p$ is odd, or, if $p = 2$, $y'_k \equiv 0 \pmod{2}$ or $B'_{kk} \equiv 0 \pmod{1}$). Hence $(y, k_1) = -2y'_1 k_1 \equiv 0 \pmod{p}$. Therefore, if $\delta = w'_o + \Sigma w'_i k'_i \in R$, $(y, \delta) = (y, w'_0) + \Sigma y'_i k'_i = y'_o (y, 1) + \Sigma y'_i (y, k'_i) \equiv 0 \pmod{p}$.

Consequently, $R$ is not $p$-maximal.

(ii) $\Rightarrow$ (i). This implication follows easily from (3.1) and (3.2).

(i) $\Rightarrow$ (iii). Suppose $D$ is a $Z_p$-order properly containing $R_p$.

Then we can find $\alpha \in D - R_p$ such that $N\alpha \in Z_p$ and $Z_p \supset (\alpha, D) \supset (\alpha, R_p)$. We may write $\alpha = (a/b) \xi$, where $\xi$ is a primitive element of $R$, $a, b \in Z$, $(a, b) = 1$. Now $\alpha \notin R_p$ implies $p|b$. Thus

$$p^2|a^2 N\xi, \quad N\xi \equiv 0 \pmod{p^2},$$

and, for $\beta \in R,$
$(\xi, \beta) = (b/a)(\alpha, \beta) \in (b/a)Z_p \cap Z \subseteq pZ$. Thus $(\xi, R) \equiv 0 \pmod{p}$, $N\xi \equiv 0 \pmod{p^2}$, and yet $\xi \not\equiv 0 \pmod{p}$. Thus $R$ is not $p$-maximal.

(iii) $\Rightarrow$ (ii). Suppose that $R_p$ is a maximal $Z_p$-order, and that $D$ is an integral order containing $R$. Let $g$ be the ternary form associated with $D$, $T$ an integral matrix such that $T'\text{adj} g T = \text{adj} f$. Now $D_p \supseteq R_p$, so $D_p = R_p$. Thus $\det T$ is a unit in $Z_p$; that is, $(\det T, p) = 1$.

This completes the proof of (3.13). q.e.d.

Suppose $\alpha \in R$ is primitive $\pmod{m}$, and that $m|N\alpha$. We define

$$B_m(\alpha) = \{\gamma \in R : \alpha \sim \gamma \equiv 0 \pmod{m}\}.$$ 

It is clear that $B_m(\alpha)$ is a primitive left ideal of $R$ of norm $m$.

(3.15) Lemma: Suppose that $p$ is a prime and that $R$ is $p$-maximal. Let $A$ and $B$ be primitive left ideals of $R$ of norm $p$. Then either $A = B$ or $A \cap B = (p)$.

proof: The proof of (3.12) shows that if $A \cap B$ contains an element $\xi$ which is primitive $\pmod{p}$, then $A = B = A \cap B = (p, \xi]$. If not, $A \cap B \subseteq (p)$, and clearly $(p) \subseteq A \cap B$. q.e.d.

We remark in passing that if $p\|d$, $c_p = -1$, then $R$ contains exactly one primitive left ideal $A$ of norm $p$, and $A$ is two sided; for if $\xi$ is primitive such that $p|N\xi$, then $\xi\eta \equiv \eta\xi \equiv 0 \pmod{p}$ for every $\eta \in R$ such that $p|N\eta$, a fact easily verified using form residues. Thus $A = (p, \xi)$. If, however, $(p, d) = 1$, the situation is more interesting:
(3.16) Theorem: Suppose that \((p,d) = 1\). Then there are \(p + 1\) primitive left ideals in \(R\) of norm \(p\).

The proof involves some interesting lemmas:

(3.17) Lemma: (Pall, [9], p. 291) Suppose \(p\) is a prime. If \(p \not| d\) and \(\alpha\) is primitive, we can find an integral quaternion residue \(\mu \pmod{p^5}\), \(s\) given not less than zero, such that \((N\mu, p) = 1\) and \(\mu \alpha\) is pure \(\pmod{p^5}\).

(3.18) Lemma: If \(\alpha \equiv \beta \pmod{m}\), \((N\mu, m) = 1\), then \(B_m(\alpha) = B_m(\beta) = B_m(\mu \alpha)\).

proof: An easy verification.

Thus, for \((m, d) = 1\), we may take the ideals \(B_m(\alpha)\) to satisfy:
\(\alpha\) pure-primitive \(\pmod{m}\), \((m, Na/m) = 1\). For \((p, d) = 1\) we may assume

\[
\begin{cases}
\text{for } p \text{ odd, } f \equiv a_1x^2 + a_2y^2 + a_3z^2 \pmod{p}, (a_1a_2a_3, p) = 1; \\
\text{for } d \text{ odd, } f \equiv x^2 - yz \pmod{2}.
\end{cases}
\]

(3.19)

(3.20) Lemma: Suppose that \((p, d) = 1\), and that \(\alpha\) is pure-primitive \(\pmod{p}\). Then we can find \(p^2\) distinct left multiples of \(\alpha \pmod{p}\).

proof: Write \(\alpha \equiv \sum_k t_k i_k \pmod{p}\). Suppose that \(p\) is odd such that \(p \not| t_k\). Then we may verify, using (3.19), that the \(p^2\) residues \((e + fi_k)\alpha, 0 \leq e, f \leq p - 1\) are distinct \(\pmod{p}\). For example, if \(k = 1\), \((e + fi)\alpha \equiv -ft_1a_2a_3 + (et_2 - ft_3)i_2 + (et_3 + ft_2a_3)i_3 \pmod{p}\).

If \(p = 2\), then \(\alpha\) pure \(\pmod{2}\) implies \(t_1 \equiv 0 \pmod{2}\). Then
\[(e + fj_2)\alpha \equiv (et_0 - ft_3) + ft_3j_1 + (e + f)t_2j_2 + et_3 \pmod{2},\]
\[(e + fj_3)\alpha \equiv et_0 - ft_2j_1 + et_2j_2 + (et_3 + ft_0)j_3 \pmod{2}.

Thus if \(2 \nmid t_2 \quad [2 \nmid t_3]\), the four residues \((e + fj_3)\alpha\) \([\alpha = (e + fj_2)\alpha]\), 
\(e, f = 0 \text{ or } 1,\) are distinct \(\pmod{2}\). Also if \(t_1 \equiv t_2 \equiv t_3 \pmod{2}\), 
\(t_0 \text{ odd,}\) the four residues \((e + fj_3)\alpha,\) \(e, f = 0 \text{ or } 1,\) are distinct 
\(\pmod{2}\).

q.e.d.

(3.21) Lemma: Let \(\alpha\) be pure-primitive \(\pmod{p}\), where \(p \nmid d\).
Then \(\mu \alpha\) represents precisely \(p^2\) residues \(\pmod{p}\), each residue 
for \(p^2\) residues \(\mu \pmod{p}\).

proof: (Pall, [8], p. 489) Let \(a\) denote the number of solutions \(\beta\) of \(\beta \alpha \equiv 0 \pmod{p}\), and \(b\) the number of residues \(\mu \alpha \pmod{p}\).
The number of solutions \(\beta\) of \(\beta \alpha \equiv \gamma \alpha\), for a given \(\gamma\), is the same 
as that of \((\beta - \gamma)\alpha \equiv 0\), hence equals \(a\); that is, every residue 
\(\mu \alpha\) is represented for \(a\) residues \(\mu\), whence \(ab = p^4\), the total 
number of residues \(\pmod{p}\). By (3.20), \(b \geq p^2\). Let 
\(\mu = (e + fj_k)\alpha\) if \(p\) odd, \((e + fj_k)\alpha\) if \(p = 2\), as in the proof 
of (3.20). Then \(\mu \alpha \equiv 0 \pmod{p}\), so \(a \geq p^2\). Thus 
\(a = b = p^2\). q.e.d.

(3.22) Corollary: In (3.21), precisely \(p\) of the \(p^2\) left multiples 
of \(\alpha\) are pure \(\pmod{p}\), and all are proportional \(\pmod{p}\).

proof: Since \(\alpha\) is pure, the pure multiples \(\pmod{p}\) are \((e + fj_k)\alpha\) 
with \(f = 0, 0 \leq e \leq p - 1\). q.e.d.

proof of (3.16): By (3.22) there are \(p\) pure quaternions \(\pmod{p}\)
in each of the sets $B_p(\alpha)$, and, in view of (3.15), only the zero residue overlaps. Denote by $\lambda$ the number of sets $B_p(\alpha)$ [$\alpha$ roams]. Then there are $\lambda(p - 1)$ pure-primitive residues in $\cup B_p(\alpha)$. Of course there are $p^3 - 1$ pure-primitive residues (mod $p$). We proceed to find $\lambda$ by counting the number $c_0$ of pure quaternion residues $\beta \in \cup B_p(\alpha)$, and then writing

$$\lambda(p - 1) = p^3 - 1 - c_0.\]$$

The quaternions $\beta \in R$ such that $\beta \notin \cup B_p(\alpha)$ are precisely those satisfying $N\beta \neq 0$ (mod $p$). For if $\beta \in B_p(\alpha)$, $\alpha\beta = 0$ (mod $p$) implies $\alpha N\beta = 0$ (mod $p$), and thus $p | N\beta$, since $\alpha$ is primitive. Conversely, if $N\beta = 0$ (mod $p$), $\beta$ primitive (mod $p$), and $(p, N(\beta + yr)/p) = 1$, then $\beta \in B_p(\beta + py)$. Thus we wish to count those pure-primitive residues $\beta$ of norm prime to $p$.

Assume that $p$ is odd, and that $f$ is as in (3.19)\(1\). Let $\beta = x_1 i_1 + x_2 i_2 + x_3 i_3$ (mod $p$). The condition $\beta \beta \neq 0$ (mod $p$) is then

$$a_2 a_3 x_1^2 + a_3 a_1 x_2^2 + a_1 a_2 x_3^2 \quad \text{(mod } p\text{).}$$

Let $\varphi(x, y) = a_3 a_2 x_2^2 + a_1 y^2$. Then $\varphi(x, y)$ represents every residue (mod $p$), and so we wish to count the number of triples (mod $p$) satisfying

$$-a_1 a_2 x_3^2 \neq \varphi(x_1, x_2) \quad \text{(mod } p\text{).}$$

Suppose that $\left(\frac{-a_1 a_2}{p}\right) = 1$. Then we may replace (3.23) by

$$x_3^2 \neq \varphi(x_1, x_2) \quad \text{(mod } p\text{).}$$

Let $\langle x, y \rangle = a_3 (a_2 x_2^2 + a_1 y^2)$. Then $\langle x, y \rangle$ represents every residue (mod $p$), and so we wish to count the number of triples (mod $p$) satisfying

$$\langle x_1, x_2 \rangle \neq \varphi(x_1, x_2) \quad \text{(mod } p\text{).}$$

Let $\psi(x, y) = a_3 a_2 x_2^2 + a_1 y^2$. Then $\psi(x, y)$ represents every residue (mod $p$), and so we wish to count the number of triples (mod $p$) satisfying

$$\psi(x_1, x_2) \neq \varphi(x_1, x_2) \quad \text{(mod } p\text{).}$$

Let $\varphi(x, y) = a_3 a_2 x_2^2 + a_1 y^2$. Then $\varphi(x, y)$ represents every residue (mod $p$), and so we wish to count the number of triples (mod $p$) satisfying

$$\varphi(x_1, x_2) \neq \psi(x_1, x_2) \quad \text{(mod } p\text{).}$$
case 1: \( \varphi(x_1, x_2) \equiv 0 \pmod{p} \).

There are \( p - 1 \) choices for \( x_3 \). Fix \( x_1 \). Then \( \varphi(x_1, x_2) \equiv 0 \pmod{p} \) implies \( x_2^2 \equiv -(a_2/a_1)x_1^2 \pmod{p} \). Hence there are two possible choices for \( x_2 \), unless \( x_1 \equiv 0 \pmod{p} \), when \( x_2 \equiv 0 \) is the only possibility. Thus there are \( 2(p-1) + 1 = 2p - 1 \) choices for \( (x_1, x_2) \), and hence \( (p-1)(2p-1) \) possibilities for \( (x_1, x_2, x_3) \).

case 2: \( \left( \frac{\varphi(x_1, x_2)}{p} \right) = -1 \). There are \( p \) choices for \( x_3 \).

case 3: \( \left( \frac{\varphi(x_1, x_2)}{p} \right) = 1 \). There are \( p - 2 \) choices for \( x_3 \), since for fixed \( x_1, x_2 \), there are two values, \( z \) and \( -z \), such that \( z^2 \equiv \varphi(x_1, x_2) \pmod{p} \).

It is convenient to combine cases 2 and 3: For \( \sigma = \pm 1 \), the number of pairs \( (x_1, x_2) \) for which \( \left( \frac{\varphi(x_1, x_2)}{p} \right) = \sigma \) may be easily shown to be the same as the number of pairs satisfying

\[
\left( \frac{x_1^2 - 2x_2}{p} \right) = \sigma \left( \frac{a_2a_3}{p} \right).
\]

Fix \( x_1 \), \( 1 \leq x_1 \leq p - 1 \). Then there are \( (p-1)/2 \) choices for \( x_1^2 - 2x_2 \), and hence for \( x_2 \). Therefore, in cases 2 and 3, there are \( (p-1)^2/2 \) possible pairs \( (x_1, x_2) \pmod{p} \). Hence in case 2 there are \( p(p-1)^2/2 \) possible triples \( (x_1, x_2, x_3) \), and in case 3 there are \( (p-2)(p-1)^2/2 \).

Combining the above for \( \left( \frac{-a_1a_2}{p} \right) = 1 \), the triples satisfying (3.24) are in number \( (p-1)(2p-1) + p(p-1)^2/2 + (p-2)(p-1)^2/2 = p^2(p-1) \).

Now suppose that \( \left( \frac{-a_1a_2}{p} \right) = -1 \).

case 1: \( \varphi(x_1, x_2) \equiv 0 \pmod{p} \).

In this instance \( x_1 \equiv x_2 \equiv 0 \pmod{p} \). Thus there are \( p - 1 \)
triples \((x_1, x_2, x_3) \pmod{p}\) satisfying (3.23) (namely, \((0,0,x_3)\), \(1 \leq x_3 \leq p - 1\)).

**Case 2:** \(\left(\frac{\varphi(x_1, x_2)}{p}\right) = 1\). There are \(p\) choices for \(x_3 \pmod{p}\), since 

\[-a_1a_2x_3^2\] 

is not a quadratic residue for \((x_3, p) = 1\), and clearly \((3.23)\) is satisfied if \(x_3 \equiv 0 \pmod{p}\).

**Case 3:** \(\left(\frac{\varphi(x_1, x_2)}{p}\right) = -1\). There are \(p - 2\) possibilities for \(x_3 \pmod{p}\).

Again we combine cases 2 and 3: There are \(p^2 - 1\) pairs \((x_1, x_2) \pmod{p}\) such that \(\left(\frac{\varphi(x_1, x_2)}{p}\right) = \pm 1\), with only \((0,0) \pmod{p}\) excluded. Also, \(a_2x^2 + a_1y^2\) represents every residue \(\pmod{p}\), and thus so does \(x^2 - dy^2\), where \(d = -a_1a_2\), each non-zero residue represented equally often; for suppose \((u_1, v_1), (u_2, v_2), \ldots, (u_{p-1}, v_{p-1})\) are fixed pairs satisfying \(u_k^2 - dv_k^2 \equiv h \pmod{p}\), \(1 \leq k \leq p - 1\), and let \(q, r\) be non-zero residues \(\pmod{p}\).

Suppose \((x_1, x_2)\) is a pair such that \(x_1^2 - dx_2^2 \equiv q \pmod{p}\), and let \(k\) be the unique integer \(\pmod{p}\) satisfying \(qk \equiv r \pmod{p}\). Then \(r \equiv qk \equiv (x_1^2 - dx_2^2)(u_k^2 - dv_k^2) \equiv (x_1u_k - dx_2v_k)^2 - d(x_1v_k - x_2u_k)^2\) \(\pmod{p}\) such that \(x_1^2 - dx_2^2 \equiv q \pmod{p}\), we may associate a unique pair \((y_1, y_2) \equiv (x_1u_k - dx_2v_k, x_1v_k - x_2u_k) \pmod{p}\) such that \(y_1^2 - dy_2^2 \equiv r \pmod{p}\); and conversely.

Hence, for \((p^2 - 1)/2\) pairs \((x_1, x_2) \pmod{p}\), \(\left(\frac{\varphi(x_1, x_2)}{p}\right) = 1\).

Therefore, for \(\left(\frac{-a_1a_2}{p}\right) = -1\), the number of triples \((x_1, x_2, x_3)\) satisfying (3.23) is (again) \(p - 1 + p(p^2 - 1)/2 + (p - 2)(p^2 - 1)/2 = p^2(p - 1)\). Consequently \(c_0 = p^2(p - 1)\), \(\lambda(p - 1) = p^3 - 1 - c_0 = p^2 - 1\), \(\lambda = p + 1\).
The proof for the case 'd odd, $p = 2'$ remains. Let $f$ be as in (3.19). One verifies easily that the pure-primitive quaternions $\beta \equiv x_0 + x_1j_1 + x_2j_2 + x_3j_3 \pmod{2}$ such that $\beta \notin \bigcup B_2(\alpha)$ are precisely those satisfying $x_1 \equiv 0 \pmod{2}$, $x_0^2 \neq x_2x_3 \pmod{2}$. By direct count there are four of these (mod 2), and hence $\lambda = (2^3 - 1) - 4 = 3$.

This completes the proof of (3.16). q.e.d.

In [5], Lipschitz proved the first known theorem on factorization of quaternions:

(3.25) Theorem (Lipschitz): Let $R_\alpha = \mathbb{Z}[1,i,j,k]$ be the ring of Lipschitz quaternions, and suppose $\alpha \in R_\alpha$ is such that $\alpha$ is primitive and $1 < m = N\alpha \equiv 1 \pmod{2}$. Let $m = p_1 \cdots p_r$ be a factorization of $m$ as a product of primes. Then there exist quaternions $\alpha_i \in R_\alpha$, $1 \leq i \leq r$, of norm $N\alpha_i = p_i$, such that $\alpha = \alpha_1 \cdots \alpha_r$. Further, this factorization is unique apart from insertion of unit factors.

For years mathematicians have sought in vain a suitable analogue of (3.25) for arbitrary quaternion orders, and, more generally, a theory of divisors encompassing all composition algebras. A principal difficulty in the four dimensional case is that, in a generalized quaternion order $R$, elements of certain norms may not exist, and some ideals may have primitive norm forms in classes different from the Brandt norm-form of $R$, a class not representing 1 (cf. [9], Theorems 3 and 12). Mindful
of these remarks, we study further the ideals $B_m(\alpha)$.

Henceforth assume that

$$
\begin{cases}
\alpha \in R \text{ is primitive, } m | N\alpha, \\
R \text{ is } m\text{-maximal}
\end{cases}
$$

(3.26)

Let $A$ be an ideal of $R$ of norm $m$. $A$ may be termed an "ideal-right divisor of $\alpha$ of norm $m$" if $\alpha A \equiv 0 \pmod{m}$ (i.e.,

$\alpha \xi \equiv 0 \pmod{m}$ for each $\xi \in A$). Clearly $A = B_m(\alpha)$ is a left ideal which is maximal with respect to the property of being an ideal-right divisor of $\alpha$ of norm $m$; and, if $A$ is any primitive left ideal which is also an ideal-right divisor of $\alpha$ of norm $m$, then $A = B_m(\alpha)$. The following is easily proved.

(3.27) Lemma: $\alpha$ in (3.26) has a unique primitive ideal-right divisor of norm $m$. Also, if $\alpha \equiv \beta \pmod{m}$ and $(N\gamma, m) = 1$, then $\alpha, \beta$, and $\gamma \alpha$ have the same ideal-right divisor of norm $m$.

Let $m = p_1 \ldots p_r$ be a factorization of $m$ into primes. By (3.27) we can find unique primitive ideal-right divisors of $\alpha$ of respective norms $\Pi_{i=1}^{k} p_{r-i+1}$ for each $k, 1 \leq k \leq r$, and hence associated with each factorization $\pi$ is a unique set

$$
\Omega_\pi = \{B_{p_r}(\alpha), B_{p_{r-1}p_r}(\alpha), \ldots, B_m(\alpha)\}
$$

(3.28) of ideal-right divisors of $\alpha$ ($\pi$ may be viewed as a permutation of $\{1, \ldots, r\}$).

We may regard the existence of the sets $\Omega_\pi$ as our analogue of (3.25). The relationship will become clear as we gain a connection between "divisors" and "ideal divisors". The following
Lemma is helpful:

(3.29) Lemma (Estes): Assume (3.26). The following are equivalent:

(i) \( \alpha \) has a right divisor of norm \( m \);
(ii) \( B_m(\alpha) \) is principal;
(iii) A norm form of \( B_m(\alpha) \) is equivalent to \( mF \).

proof: (i) \( \Rightarrow \) (ii). Suppose \( \alpha = \gamma \beta, \ N\beta = m \). Then, easily,
\[ B_m(\alpha) = (\beta). \]

(ii) \( \Rightarrow \) (iii). Obvious. \[ ((\beta) = [\beta, j_1\beta, j_2\beta, j_3\beta]). \]

(iii) \( \Rightarrow \) (i). If a norm-form of \( (m,\alpha) \) is \( mF \), then \( (m,\alpha) \) contains an element \( \beta \) of norm \( m \). Then \( (m,\alpha) = (\beta), \alpha\beta = my \)
for some \( \gamma \in R, \alpha = \gamma\beta. \)

q.e.d.

(3.30) Corollary: Assume (3.26). Suppose that \( F \) resides in a genus consisting of a single class, and that \( F \) represents \( m \). Then \( \alpha \) has a right divisor of norm \( m \).

proof: Pall in [9] showed that the norm form of \( B_m(\alpha) \) is in the genus of \( F \), if the genus represents \( m \). q.e.d.

(3.31) Corollary: Assume (3.26), and assume further that \( F \) is in a genus of one class. Suppose that \( N\alpha = m \) and that \( F \) represents each prime factor of \( m \). Let \( m = p_1...p_r \) be a prime factorization of \( m \). Then we may factor \( \alpha \) as \( \alpha = \alpha_1...\alpha_r \), uniquely apart from unit factors, where \( \alpha_i \in R, N\alpha_i = p_i, 1 \leq i \leq r. \)
proof: \( \alpha \) has a right divisor \( \alpha_r \) of norm \( p_r \), by (3.30). Then 
\[
(1/p_r)\overline{\alpha \alpha_r} = \beta \text{ is primitive, and so we may repeat the process,}
\]
thereby obtaining the desired factorization. q.e.d.

Of course, the Lipschitz Theorem is a special case of (3.31). Notice also that, in the proof of (3.31), \( (\alpha_r) = B_{p_r}(\alpha) \), 
\( (\alpha_{r-1}\alpha_r) = B_{p_{r-1}p_r}(\alpha) \), and so on. Thus the concept of sets 
(3.28) of ideal divisors seems to include the notion of 
divisibility in the usual sense. Further applications are possible; for example:

(3.32) Theorem: Assume the hypotheses of (3.31), and suppose 
that \( (m,d) = 1 \). Let \( m = p_1^{e_1} \ldots p_r^{e_r} \) be a factorization of \( m \) 
into powers of distinct primes. Then the number of sets of 
primitive representations of \( m \) by \( F \) is given by 
\[
\nu^r(m) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i + 1).
\]

The proof requires the following result:

(3.33) Lemma: If \( \alpha_1, \ldots, \alpha_t \) are quaternions of norm \( p \), \( (p,d) = 1 \), 
then \( \alpha = \alpha_1 \ldots \alpha_t \) is primitive if and only if \( \alpha_j \alpha_{j+1} \) is primitive 
for \( j = 1, 2, \ldots, t - 1 \).

proof: (Pall, [8], pp. 490-491). The assertion is trivial if \( t = 2 \), 
and the necessity of \( \alpha_j \alpha_{j+1} \) being primitive is obvious for every \( t \). 
Assume for a given \( t \) that \( \alpha_j \alpha_{j+1} \) is primitive, \( 1 \leq j \leq t - 1 \), and 
\( \alpha \) is proper. Consider \( \beta = \alpha \alpha_{t+1} \). If \( \beta \) is not proper, \( \beta = \gamma p \), 
\( \gamma \in R \); and since \( p = \overline{\alpha_{t+1}} \alpha_{t+1} \), \( \alpha = \gamma \overline{\alpha_{t+1}} \). Hence \( \alpha_t = \theta \overline{\alpha}_{t+1} \),

\[ N\theta = 1, \text{ since both are right divisors of } \alpha \text{ of norm } p. \text{ Hence} \]
\[ \alpha \alpha_{t+1} = \theta p, \text{ completing the proof.} \quad \text{q.e.d.} \]

The proof of (3.32) now follows easily; for if \( \alpha \) is primitive such that \( N\alpha = m \), then by (3.16) there are \( p + 1 \) possible quaternions \( \gamma \) of norm \( p \) which are right divisors of \( \alpha \). But, if \( r > 1 \), there are only \( p \) of these which are possible right divisors of \( (1/p) \alpha \gamma \), by (3.33). Continuation of this reasoning yields (3.32). \quad \text{q.e.d.}
CHAPTER IV
QUATERNIONS AND BINARY QUADRATIC FORMS

Pall in [8] introduced a procedure, involving quaternions in the Lipschitz ring, to study the representations of a positive integer \( n \) as a sum of three squares. Similar methods using quaternions in other rings may be applied in order to count the representations of an integer by the adjoints of other ternary forms. A slight modification of these techniques enables the study of certain binary quadratic forms. We illustrate in the case that \( R \) is the integral order obtained from \( f = x^2 - yz \).

Since \( \text{adj} f = \frac{1}{4}(x^2 - 4yz) \), the Brandt norm-form of \( R \) is given by \( F = (x_0 + \frac{1}{2}x_1)^2 + \text{adj} f = x_0^2 + x_0x_1 + x_2x_3 \). \( F \) is indefinite and fundamental, and thus, according to Brandt and Latimer ([9], p. 293), \( F \) resides in a genus containing a single class. Because of this and the fact that \( d = -1 \), factorization as in (3.5) is always possible in \( R \). The multiplication in \( R \) is as follows: If \( \alpha = u_0 + \Sigma u_k^j k, \beta = v_0 + \Sigma v_k^j k, \) then
\[
\alpha \beta = u_0v_0 - u_2v_3 + (u_0v_1 + u_1v_0 + u_2v_3 - u_3v_2)j_1 + (u_0v_2 + u_2v_0 + u_2v_1)j_2 + (u_0v_3 + u_3v_0 + u_1v_3)j_3.
\]

Let \( \eta = x_1i_1 + x_2i_2 + x_3i_3 \) be a purely integral quaternion. Define \([\eta] = \{\theta \in \mathbb{R}: \theta \eta = \eta, \theta \in R\}\). Notice that \( \mu \in [\eta] \) implies \( N\mu = N\eta \), and if \( \eta \) is purely primitive, so is \( \mu \). Thus we will call \([\eta] \) "purely primitive of norm \( q \)" if \( \eta \) is purely primitive and \( N\eta = q \). Let \( \psi = [a,b,c] \) be a primitive binary quadratic form of
discriminant \( d = b^2 - 4ac = -n \). We now define a process by which
\( \psi \) carries each purely primitive \([\eta]\) of norm \( n/4(\neq 0) \) into a unique
purely primitive \([\zeta]\) of like norm:

\[
N(b/2 + \eta) = (b^2 + n)/4 = ac , \quad (b/2 + \eta, 1) = b , \text{ so } b/2 + \eta
\]
is integral. Hence \( b/2 + \eta \in \mathbb{R} \), so we may write \( b/2 + \eta = \sigma \tau \),
where \( N\sigma = c \), \( N\tau = a \), \( \sigma , \tau \in \mathbb{R} \). Let \( \zeta = (b/2 + \eta)/\sqrt{4ac} = \tau \sigma - b/2 \).

It follows easily that \( \zeta \) is purely integral. Also, \( \zeta \) is purely
primitive; for if \( \zeta = \sum y_k i_k \) and \( p|y_k \), \( k = 1,2,3 \), then \( p|a \)
since \( a\eta = \tau \zeta \tau \) and \( (x_1, x_2, x_3) = 1 \). Also, \( p|n \), since

\[
y_1^2 - 4y_2y_3 = -n .
\]

Because \( b^2 + n = 4ac \), \( p|b \). Further,
\( \sigma \zeta \sigma = c\eta \) implies \( p|c \). This contradicts the primitvity of \( \psi \).

Also, if \( \tau \) is replaced by \( \theta \tau \), \( N\theta = 1 \), \( \zeta \) is replaced by
\( \theta \sigma \theta \in [\zeta] \). If \( \eta \) is replaced by \( \theta \eta \theta \), \( N\theta = 1 \), then \( \zeta \) is unchanged,
since \( b/2 + \theta \eta \theta = \theta \sigma \tau \theta \), \( (1/N(\tau \theta)) \tau \theta \theta \sigma \tau \theta = (1/N\tau \theta) \tau \eta \theta = \zeta \).

(4.1) Lemma: The process associated with the primitive form
\( \psi = [a,b,c] \) is the same as that for the following forms equivalent
to \( \psi \):

\[
[a, b + 2ah, c + bh + ah^2], \quad [c, -b, a].
\]

proof: If \( b/2 + \eta = \sigma \tau \), then \( (b/2 + ah) + \eta = (\sigma + h\tau)\tau \), and
\( -b/2 + \eta = -(b/2 + \eta) = -\tau \sigma \); also, \( (1/N\sigma)\sigma \tau \sigma = \tau \sigma - b/2 = \zeta \). q.e.d.

(4.2) Corollary: Any two equivalent forms \( \psi \) determine the same
process.

Thus we may speak of a class \( C \) of primitive forms taking \([\eta]\)
to \([\zeta] \), "\( [\eta] \sim [\zeta] \)."
(4.3) Lemma: If \([\eta] \subseteq [\zeta], [\zeta] \supseteq [\xi]\), then \([\eta] \cap [\xi]\).

The proof involves united forms. The reader is referred to [8], p. 496.

(4.4) Lemma: There is at most one primitive class of discriminant \(-n\) carrying any given purely primitive \([\eta]\) of norm \(n/4\) into a given purely primitive \([\zeta]\) of the same norm.

proof: Suppose \(C,D\) take \([\eta]\) into \([\zeta]\). Then both \(C^{-1}D\) and the principal class \(E\) carry \([\eta]\) into \([\eta]\). Suppose \(m\) is primitively represented by \(C,D\). Then \(m\) can be made the first coefficient of a form \(\psi = [m,b,c] \in C^{-1}\). \(\psi\) takes \([\eta]\) into \([\eta]\), so there is an integral quaternion \(\tau \in \mathbb{R}\) satisfying \(N\tau = m\) and \(\tau\tau = m\eta\).

From this follows \(\tau\eta = \eta\tau\), an expansion of which yields
\[x_i t_j = x_j t_i, \quad i,j = 1,2,3,\]
where \(\eta = \sum_k x_k i_k\), \(\tau = t_0 i + \sum_k t_k i_k\).

Since \((x_1,x_2,x_3) = 1\), we can find an integer \(g\) such that \(t_k = gx_k\), \(k = 1,2,3\). Thus \(m = N\tau = t_0^2 + x_1 t_0 g + x_2 x_3 g^2\).

Clearly \([1, x_1,x_2,x_3]\) \(\in E\), and thus \(E\) represents every integer represented primitively by \(F = C\). Since \(E\) is ambiguous, \(F = E, C = D\). q.e.d.

(4.5) Lemma: Suppose \([\eta] \subseteq [\zeta], N\theta = -1\). Assume that the principal class \(E\) and \(C\) have discriminant \(-n = -4N\eta\). Then:

(i) \([\zeta] \subseteq [-\eta]\)

(ii) \([\eta] \xrightarrow{(-E)C} [-\eta]\)

(iii) \([-\eta\theta\eta\theta] \xrightarrow{(-E)C} [\zeta]\)
proof: An easy verification.

We now turn to the equation $\tau \alpha \tau = \beta$, where $\tau \in \mathbb{R}$, and $\alpha = \sum a_k i_k, \beta = \sum b_k i_k$ are purely integral. Pollak in [10] treated this equation more generally. The situation here is simpler. By direct computation,

\[
\begin{align*}
    b_1 &= 2t_1 t_2 a_3 - 2t_0 t_3 a_2 + t_0^2 a_1 + t_0 t_1 a_1 + 2t_0 t_2 a_3 - t_2 t_3 a_1; \\
    b_2 &= a_2 t_0^2 + a_1 t_0 t_2 + a_3 t_2^2; \\
    b_3 &= a_2 (-t_3)^2 + a_1 (-t_3)(t_0 + t_1) + a_3 (t_0 + t_1)^2.
\end{align*}
\]

Thus, for $\tau = t_0 + \sum t_k i_k$, the equations (4.6) imply that if $T = T(\tau) =$

\[
\begin{bmatrix}
    t_0 & -t_3 \\
    t_2 & t_0 + t_1
\end{bmatrix}, \quad \det T = N \tau,
\]

then $T^\top A T = B$, where $A, B$ are respectively the matrices of the forms $\varphi(\alpha) = [a_2, a_1, a_3], \varphi(\beta) = [b_2, b_1, b_3]$. Conversely, if

\[
S = \begin{bmatrix}
    s_1 & s_2 \\
    s_3 & s_4
\end{bmatrix}
\]

satisfies $S^\top A S = B$, then $\sigma = \sigma(S) = s_1 + (s_4 - s_1)j_1 + s_3 j_2 - s_2 j_3$ satisfies $\sigma \alpha \sigma = \beta$. Thus, in particular, a set $[\eta]$ "corresponds" to a class $C(\eta)$ in the sense that $\zeta \in [\eta]$ if and only if $\varphi(\zeta) \sim \varphi(\eta) \in C(\eta)$. Moreover, if $\psi = [a, b, c]$ is primitive of discriminant $-n$, then $\alpha(\psi) = bi_1 + ai_2 + ci_3$ is purely primitive of norm $n/4$. Also, $\alpha(\varphi(\eta)) = \eta, \varphi(\alpha(\psi)) = \psi, \sigma(T(\tau)) = \tau$. 
Let $\alpha(C)$ denote a representative of $[\alpha(\psi)]$, where $\psi \in C$.

As before, let $E$ denote the principal class of discriminant $-n = -4N\eta$, where $\eta = \sum_{k} x_k i_k$ is purely primitive. Then 

$$\eta' = x_1 i_1 + i_2 + x_2 x_3 i_3 \in [\alpha(E)],$$

since surely $[1, x_1, x_2 x_3] \in E$.

By direct computation, $x_1/2 + \eta' = \sigma \tau$, where $\sigma = x_1 i_1 + j_2 + x_3 j_3$ ($N\sigma = x_3$), and $\tau = x_2 + (1 - x_2) j_1 (N\tau = x_2)$, and $\tau \eta' \tau = x_2 \eta$.

Hence $C(\eta)$ takes $[\alpha(E)]$ into $[\eta]$.

(4.7) Theorem: There is a one-to-one correspondence between purely primitive sets $[\eta]$ of norm $n/4$ and classes of primitive binary quadratic forms of discriminant $-n$. Also, given any two such purely primitive sets, $[\eta]$ and $[\zeta]$, there is a unique class $C$ taking $[\eta]$ into $[\zeta]$. If $B$, $C$, $D$ are primitive classes of discriminant $-n$, then $BC = D$ if and only if $[\alpha(B)] C [\alpha(D)]$.

proof: The first statement has already been established as fact. From the preceding, $[\alpha(E)] \xrightarrow{C(\eta)} [\eta]$, $[\alpha(E)] \xrightarrow{C(\zeta)} [\zeta]$. Thus, $[\eta] \xrightarrow{C(\eta)^{-1} C(\zeta)} [\zeta]$. Uniqueness has already been established.

Suppose that $[\eta] C [\zeta]$. The commutativity of the diagram

$$\begin{array}{ccc}
[\eta] & \xrightarrow{C} & [\zeta] \\
\downarrow C(\eta) & & \downarrow C(\zeta) \\
[\alpha(E)] & & [\alpha(E)]
\end{array}$$

yields the validity of the last sentence in the theorem. q.e.d.

Thus composition of primitive binary quadratic forms may be achieved simply by multiplying quaternions! The correspondence
between this method and composition by united forms may be gleaned from the formulae
\[
\begin{align*}
\frac{b}{2} + bi_1 + a_1i_2 + a_2ci_3 &= (bj_1 + a_1j_2 + cj_3)(a_2 + (1 - a_2)j_1); \\
(a_2 + (1 - a_2)j_1)(bj_1 + a_1j_2 + cj_3) &= \frac{b}{2} + bi_1 + a_1a_2i_2 + c_j_3.
\end{align*}
\]
For the connection between this "quaternionic composition" and composition by bilinear substitution, we turn to Gauss. Specifically, we answer the question, "Given a quaternionic composition \( BC = D \) determined by \([\alpha(B)]^f'[\alpha(D)]\), \( f' \in C \), is there in evidence a Gaussian bilinear substitution which yields \( F = ff' \), \( f \in B \), \( F \in D \)?"...And the converse question as well.

Thus suppose that \( f = [a, b, c] \in B \), \( f_1' = [a', b', c'] \in C \).

Suppose further that \( b'/2 + \alpha(f) = a\tau, \quad N\tau = a', \quad N\sigma = c' \), \( \tau = t_0 + \sum t_kj_k, \quad \sigma = u_0 + \sum u_kj_k \), \( \zeta = (1/a') \tau\alpha(f)\tau = \tau\sigma - b'/2 \), and \( \varphi(\zeta) = F \). Then the equations \( \tau\zeta\tau = a'\alpha(f) \), \( \sigma\zeta\sigma = c'\alpha(f) \), and the famous equations [1] - [9] of article 235 of Gauss' Disquisitiones Arithmeticae ([3]), prompt use of the bilinear substitution with matrix
\[
T(\sigma, \tau) = \begin{bmatrix}
t_0 + t_1 & u_0 & t_3 & -u_3 \\
-t_2 & u_2 & t_0 & u_0 + u_1
\end{bmatrix}.
\]
Indeed, using this substitution, \( F \) is a composite of the forms \( f, f' \) in the Gauss sense.

Conversely, suppose \( F = ff' \) via the bilinear substitution
and that all three forms are primitive of discriminant d.

Butts and Estes in \([1]\) pointed out that \(pq'' - qp'' = a',\)
\(p'q''' - q'p''' = c'.\) And, in fact, if we choose \(\sigma, \tau\) by
\(T = T(\sigma, \tau),\) then \(N\sigma = c',\ N\tau = a',\ b'/2 + \alpha(f) = \sigma\tau,\) and
\(\tau\alpha(f)\tau^{-1} = a'\alpha(F).\) We remark in passing that, evidently,
quaternionic and Gaussian composition coincide over every
domain which admits composition in the Gauss sense. The
following lemma allows us to identify quaternion and Gaussian
composition even in the case when discriminants are not equal.

\[ (4.8) \text{Lemma: Let } p \text{ be a prime, } n \equiv 0 \text{ or } -1 \pmod{4}. \text{ Every}
\text{purely primitive } \zeta \text{ of norm } p^{2}n/4 \text{ is of the form } \zeta = \tau\eta\tau^{-1}, \text{ where}
N\tau = p \text{ and } N\eta = n/4. \text{ Further, } \tau \text{ and } \eta \text{ are unique apart from}
\text{insertion of unit factors. Thus every purely primitive } \left[\zeta\right]
\text{of norm } p^{2}n/4 \text{ is derivable from a unique purely primitive}
\left[\eta\right] \text{of norm } n/4. \]

**proof:** Suppose \(p\) is odd. Choose \(j = 0 \text{ or } 1\) such that \(pj/2 + \zeta\)
is integral. Then \(N(pj/2 + \eta) = p^{2}(j + n)/4.\) Hence
\(pj/2 + \zeta = \sigma\tau,\) where \(N\tau = p\), \(\sigma\) primitive \((\text{mod } p)\). Therefore,
\(\sigma \text{ and } pj/2 + \zeta = \tau(\tau(j) - \sigma)\) have the same left divisors of norm \(p.\)
Thus \(\sigma = \tau\eta\), \(pj/2 + \zeta = \tau\eta\tau, \zeta = \tau(\eta - j/2)\tau = \tau\eta\tau.\) We obtain
uniqueness readily from \((3.3)\). If \(p = 2,\) the above proof applies
with \( j \) chosen 0 or 1 according as \( n \equiv 0 \) or \(-1 \) (mod 4). q.e.d.

The techniques developed in this chapter may be applied to the study of the quadratic orders \( R_d \). We illustrate by using these methods to derive some results obtained by Butts and Pall in [2].

We can, in view of (4.8), map a given primitive class \( C \) of binary quadratic forms of discriminant \( dv^2 \) onto a unique primitive class \( D \) of discriminant \( d \); simply take \( D = C(\eta) \), where \( \alpha(C) = \tau \eta \), \( \eta = v > 0 \). An easy argument shows that this factorization is essentially unique. According to Theorem (2.5) in [2], this corresponds to the function \( C \rightarrow \text{Cl}_d \).

Now suppose that \( d_1 = dv^2 (v > 0) \), and that \( A', A \) are invertible fractional ideals in \( R_d', R_d \) respectively. To study the equation \( A = A'R_d \), we may assume \( A = [m, r + \omega], A' = k[m', r' + \omega'] \), \( k \) rational, \( m, m', r, r' \epsilon \mathbb{Z}, m|N(r + \omega), m'|N(r' + \omega') \), where \( \omega = \omega_d, \omega' = \omega_d \), as in (1.2). Associated with the invertible fractional ideals \( A, A' \) are the primitive norms \( \psi(A) = [m, 2r + \epsilon, N(r + \omega)/m], \psi(A') = [m', 2r' + \epsilon', N(r' + \omega')/m'] \) of discriminants \( d \) and \( dv^2 \) respectively. Hence we may associate with \( A, A' \) purely primitive sets \([\eta], [\eta']\), where \( \eta = \alpha(\psi(A)), \eta' = \alpha(\psi(A')) \), of norms \(-d/4, -dv^2/4 \) respectively. According to Theorem (5.1) of [2], \( A = A'R_d \) implies the existence of a matrix

\[
H = \begin{bmatrix}
e & h \\
0 & n_1
\end{bmatrix}, \quad en_1 = v,
\]
such that \( k(m', r' + \omega') = (m, r + \omega)H \). It follows that
\[ \Psi(A)^H = \Psi(A'), \]
and thus \( \tau\eta' = \eta' \), where \( \tau = e + (n_1 - e)j_1 \)
-\( h_j \) has norm \( en_1 = v \). Conversely, if \( A \) is an invertible ideal in
\( R_d \) and \( A' \) is an invertible ideal in \( R_d ' \) obtained from \( \tau\eta' = \eta' \),
\( N\tau = v \), then \( A' R_d = A \).

Now let \( p \) be a prime. Then there are \( p + 1 \) ideals \( \{\tau\} \)
of norm \( N\tau = p \) in \( R \), according to (3.16). Those for which
\( \tau\eta' \equiv 0 \pmod{p} \), \( N\eta = n/4 \), are, by (3.9), the right divisors of
\( x_0/2 + \eta \), where \( (x_0^2 + n)/4 \equiv 0 \pmod{p} \), and thus are \( 1 + \left(\frac{-n}{p}\right) \)
in number. Also, if \( \tau \) and \( \tau' \) are not left associates, then
\( \tau\eta' \) and \( \tau'\eta' \) are not in the same purely primitive set \( \{\xi\} \),
from the uniqueness feature of (4.8). Thus a given purely
primitive \( \{\eta\} \) of norm \( n/4 \) gives rise to \( (p + 1) - (1 + \left(\frac{-n}{p}\right)) = p(\left(\frac{-n}{p}\right) \)
purely primitive sets \( \{\xi\} \) of norm \( p^2n/4 \). We obtain easily, then, that
the number \( N \) of purely primitive sets \( \{\xi\} \) of norm \( nv^2/4 \), \( v > 0 \), obtainable from a given purely primitive set \( \{\eta\} \) of norm \( n/4 \) is given by

\[
N = \prod_{i=1}^{\pi} p_i^{e_i - 1} \left( p_i - \left(\frac{-n}{p_i}\right) \right),
\]
where \( v = p_1^{e_1} \cdots p_r^{e_r} \) is a factorization of \( v \) into distinct primes.
Hence we deduce Theorem 5.2 and Corollary 5.3.1 of [2], namely:

(4.10) Theorem: Suppose \( A \) is an invertible fractional ideal in
\( R_d \), where \( d = -n \), and \( d' = dv^2 \), \( v > 0 \). Let
\( v = p_1^{e_1} \cdots p_r^{e_r} \) be a factorization of \( v \) into distinct primes. Then the number of
invertible fractional ideals \( A' \) in \( R_d ' \) such that \( A'R_d = A \) is
given by (4.9).


VITA

Bart Francis Rice was born on March 12, 1943, in Miami Beach, Florida. He attended the public schools of Dade County, Florida. After graduation from high school he entered Rice University in Houston, Texas, where he received the degree of Bachelor of Arts in June, 1965.

He entered Louisiana State University in September, 1965, received the degree of Master of Science in May, 1967, and is now a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.
EXAMINATION AND THESIS REPORT

Candidate: Bart Francis Rice

Major Field: Mathematics

Title of Thesis: Topics in Quadratic and Quaternion Orders

Approved:

[Signatures]

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

[Signatures]

Date of Examination: July 15, 1969