Topics in Quadratic and Cubic Forms.

Richard Marshall Caron
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/2270

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.
INFORMATION TO USERS

This dissertation was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photographing at the upper left hand corner of a large sheet and to continue photographing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again – beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106
A Xerox Education Company
CARON, Richard Marshall, 1944-  
TOPICS IN QUADRATIC AND CUBIC FORMS.  
The Louisiana State University and Agricultural and Mechanical College, Ph.D., 1972  
Mathematics  

University Microfilms, A XEROX Company, Ann Arbor, Michigan  

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED.
TOPICS IN QUADRATIC AND CUBIC 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

Richard Marshall Caron
B.A., Florida Atlantic University, 1966
August, 1972
PLEASE NOTE:

Some pages may have
indistinct print.

Filmed as received.

University Microfilms, A Xerox Education Company
ACKNOWLEDGMENTS

The author wishes to thank his advisor, Professor Gordon Pall, for his guidance in the preparation of this dissertation. In addition, he wishes to express his gratitude to his former teachers, J. M. Freeman (Florida Atlantic University) and H. P. McKean (Courant Institute, New York University) for their encouragement and foresight through the years. He extends special thanks to his family for their patience and help through often difficult times.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>PART I UNIMODULAR QUADRATIC FORMS VIA SKew</td>
<td></td>
</tr>
<tr>
<td>ORTHOGONAL MATRICES</td>
<td></td>
</tr>
<tr>
<td>CHAPTER I FORMS IN ( n ) VARIABLES, ( n \leq 16 )</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER II FORMS IN ( 2^4 ) VARIABLES</td>
<td>13</td>
</tr>
<tr>
<td>PART II ORDERS OF TERNARY CUBIC FORMS</td>
<td></td>
</tr>
<tr>
<td>CHAPTER III LEFT DIVISORS OF ORDERS</td>
<td>23</td>
</tr>
<tr>
<td>CHAPTER IV IDEALS OF ORDERS</td>
<td>36</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>45</td>
</tr>
<tr>
<td>VITA</td>
<td>47</td>
</tr>
</tbody>
</table>
ABSTRACT

In Part I, the construction of unimodular quadratic forms (i.e. forms having an integral matrix of determinant 1) is discussed. The technique yields n-ary forms \( f \) with matrix

\[
(1) \quad f = \begin{bmatrix}
aI & cI+dV \\
cI-dV & bI
\end{bmatrix}
\]

where \( V \) is a skew orthogonal matrix of order \( m = \frac{n}{2} \), \( I \) is the identity matrix of order \( m \), and \( a, b, c, d \in \mathbb{Z} \). The main result of Chapter I shows that, for \( n = 16 \), four of the eight possible classes are represented: the sum of 16 squares and the three classes of minimum 2. In Chapter II, the forms (1) are studied by means of their connection with binary Hermitian forms. An equivalence criterion for the latter, analogous to the familiar Gauss criterion for binary quadratic forms given by L. E. Dickson, is established. Then a procedure is described by which the coefficients of such a form are minimized, with an eye toward classification. The results are applied to the case \( n = 24 \), with \( V \) a skew orthogonal matrix of order 12 satisfying \( VV' = 111 \). In particular for the quadratic residue matrix of Paley, we show that five classes (under proper or improper equivalence of
binary Hermitian forms) are represented, including the
two of minima 3 and 4, respectively.

In Part II, factorable ternary cubic forms are viewed
as norm forms of 3-dimensional modules in the \( \mathbb{Z} \)-algebra
\( A = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \). An order is defined to be a 3-dimensional
subring of \( A \) with identity. In Chapter III a bi-unique
correspondence between the set of orders of determinant
\( n = p_1^{a_1} \cdots p_k^{a_k} \) (\( p_i \) distinct primes) and the set of
collections of orders of respective determinants
\( p_i^{a_i} \), \( i = 1, \ldots, k \), is established. The association is by
means of left Hermite matrix divisors, which also serve in
Chapter IV to give a similar correspondence among invertible
ideals. As an application, class numbers of the orders are
calculated.
PART I
UNIMODULAR QUADRATIC FORMS VIA SKEW ORTHOGONAL MATRICES

CHAPTER I
FORMS IN n VARIABLES, n ≤ 16

I. Introduction. An n-ary quadratic form will be called unimodular if it is positive definite and has an integral matrix of determinant 1. The prime example is the form \( f_n = x_1^2 + \ldots + x_n^2 \), a sum of \( n \) squares. Recently, there has been some interest in studying the classes of such forms, with particular interest in those classes having minimum larger than 1. In [6], Kneser counted the number of classes in \( n \) variables for \( n ≤ 16 \). In particular, he showed that, for \( n = 16 \), there are eight classes, five of minimum 1 and three of minimum 2. Beyond \( n = 16 \), the number of classes increases very rapidly (there are more than \( 10^8 \) for \( n = 32 \), according to Conway [7]) and the study becomes correspondingly difficult. In this chapter we present a method by which certain families of classes may be constructed and even studied in some measure as if they were binary forms. The families so constructed consist mainly of classes of higher minimum. The technique derives from an idea used by Pall and O'Connor in [5] to construct the first known unimodular form of minimum 3 (in 24 variables). It will turn out that,
for $n \leq 16$, our construction yields precisely $f_n$ and all forms of minimum greater than 1.

II. The Construction. All matrices in Chapter 1 are integral. An $m \times m$ matrix $V$ is called skew orthogonal if it satisfies $VV' = -V^2 = kI$ for some positive integer $k$, called the norm of $V$. It is well-known that such matrices exist only for $n$ even and subject to the necessary condition that $n \equiv 0 \pmod{4}$ unless $k$ is a square. Paley in [8] gave an important class of these matrices: if $p$ is a prime $\equiv 3 \pmod{4}$, there is a skew orthogonal matrix of order $p + 1$ and norm $p$, defined by

a) $a_{ii} = 0$

b) $a_{i j} = 1$, $j > 1$

c) $a_{i j} = \left( \frac{j-i}{p} \right)$ for $j > i > 1$, where $\left( \frac{a}{p} \right)$ denotes the Legendre symbol, and

d) $a_{i j} = -a_{j i}$ for $j < i$

In this chapter we use the Paley matrices for $p = 3$ and $p = 7$. They are

\begin{equation}
\begin{bmatrix}
0 & 1 & 1 & 1 \\
-1 & 0 & 1 & -1 \\
-1 & -1 & 0 & 1 \\
-1 & 1 & -1 & 0
\end{bmatrix}
\end{equation}

$P = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & -1 & 0 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 0 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}

Q = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & -1 & 0 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 & 1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 0 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 0 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\
-1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}
An important feature of a skew orthogonal matrix $V$ of norm $k$ is that a matrix of the type $A = cI + dV$ (where $c$ and $d$ are integers and $I$ is the identity of the same order as $V$) is orthogonal of norm $c^2 + kd^2$, i.e. $AA' = (c^2 + kd^2)I$. As will be seen below, it is this property that makes our construction work.

Now let $V$ be as above, let $a, b, c, d$ be integers and let $n = 2m$ (m is the order of $V$). We construct an $n \times n$ symmetric matrix

$$f_Y(a, b, c, d) = \begin{bmatrix} aI & cI + dV \\ 0 & bI \end{bmatrix}$$

where all blocks are of order $m$. This is therefore the matrix of an $n$-ary quadratic form $f$, which we henceforth use interchangeably with its matrix, setting $f = f_Y(a, b, c, d)$.

We prove the following lemmas about the forms $f_Y(a, b, c, d)$:

**LEMMA 1:** The form $f_Y(a, b, c, d)$ is unimodular if and only if

$$a > 0 \text{ and } ab = c^2 + kd^2 + 1.$$ 

**PROOF:** Apply to $f_n = x_1^2 + \ldots + x_n^2$ the linear transformation $T$ with matrix

$$T = \begin{bmatrix} aI & cI + dV \\ 0 & I \end{bmatrix}.$$
Then $a_n$ becomes (using (3) for the second equality)

$$T'T = \begin{bmatrix} a^2 I & a(cI+dV) \\ a(cI-dV) & c^2 + kd^2 + 1 \end{bmatrix} = \begin{bmatrix} aI & cI+dV \\ cI-dV & bI \end{bmatrix} = af,$$

where now clearly $f$ has an integral matrix of determinant 1. Also, since $a_n$ is positive definite and $af$ is a transformation of $a_n$, $a > 0$ implies that $af$ is positive definite. Thus $f$ is positive definite.

Conversely, if $f$ is unimodular, since all blocks in the matrix (2) commute, we have that $(ab-c^2-kd^2)^m = 1$. Thus $ab - c^2 - kd^2 = \pm 1$. If -1, then $f$ is equivalent to

$$\begin{bmatrix} -bI & cI+dV \\ cI-dV & -aI \end{bmatrix} \begin{bmatrix} aI & cI+dV \\ cI-dV & bI \end{bmatrix} \begin{bmatrix} -bI & cI+dV \\ cI-dV & -aI \end{bmatrix} = \begin{bmatrix} -bI & cI+dV \\ cI-dV & -aI \end{bmatrix},$$

a contradiction to the positive character of $f$. //

**Lemma 2:** If $f_V(a,b,c,d)$ is unimodular, then $f_V(a,b,c,d) \sim f_V(a,b,|c|,|d|) \sim f_V(b,a,|c|,|d|)$.

**Proof:** First equivalence: if $c,d \leq 0$, then
\[
\begin{bmatrix}
-I & 0 \\
0 & I
\end{bmatrix}
\begin{bmatrix}
ai & cI+DV \\
cl-dV & bi
\end{bmatrix}
\begin{bmatrix}
-I & 0 \\
0 & I
\end{bmatrix}
= 
\begin{bmatrix}
ai & -cI-dV \\
-cI+DV & bi
\end{bmatrix}
\]

If \( c \leq 0, d \geq 0 \), then
\[
\begin{bmatrix}
-cI+DV & ai \\
bI & -cI-dV
\end{bmatrix}
\begin{bmatrix}
ai & cI+DV \\
cl-dV & bi
\end{bmatrix}
\begin{bmatrix}
-cI-dV & bi \\
ai & -cI+DV
\end{bmatrix}
= 
\begin{bmatrix}
ai & -cI+DV \\
-cI-dV & bi
\end{bmatrix}
\]

Second equivalence:
\[
\begin{bmatrix}
bI & cI+DV \\
-cI+DV & ai
\end{bmatrix}
\begin{bmatrix}
ai & cI+DV \\
cl-dV & bi
\end{bmatrix}
\begin{bmatrix}
bI & cI+DV \\
cl-dV & ai
\end{bmatrix}
= 
\begin{bmatrix}
bI & cI+DV \\
cl-dV & ai
\end{bmatrix}
. //
\]

In view of Lemma 2, we note we may assume in \( f_V(a,b,c,d) \) that \( 0 \leq c,d \) and \( a \leq b \). Note also that by applying one or more translations
\[
(4) \quad \tau_k = \begin{bmatrix} I & kI \\ 0 & I \end{bmatrix}, \quad \tau_j = \begin{bmatrix} I & jV \\ 0 & I \end{bmatrix}
\]

we may secure
\[
(5) \quad 0 \leq c,d \leq \frac{1}{2}a \leq \frac{1}{2}b .
\]

Henceforth, unless otherwise specified, it will be supposed that every form \( f_V(a,b,c,d) \) satisfies (3) and (5).

Note that for \( n = 8 \), the matrix \( P \) of (1) yields the form \( B = \begin{bmatrix} P & I \\ P & 2I \end{bmatrix} \) which, since all its coefficients are even, has minimum 2. It is well-known that no unimodular
form in fewer than eight variables has minimum 2, and that there are precisely two classes of unimodular forms in eight variables, represented by $f_8$ and $B$. Similar results can be obtained with our construction for the three classes in $n = 12$ variables using the skew orthogonal matrix.

\[
W = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & -1 & 0 & 1 \\
1 & 1 & 0 & 0 & -1 & -1 \\
1 & -1 & 0 & 0 & 1 & -1 \\
1 & 0 & -1 & 1 & 0 & 1 \\
0 & -1 & 1 & 1 & -1 & 0 \\
\end{bmatrix}
\]

3. The case $n = 16$. The first non-trivial case is that of 16 variables. We show in Theorem 1 that, in addition to the class of $f_{16}$, our construction using the Paley matrices (1) yields exactly the classes of minimum 2. The heart of the proof is

**Lemma 3** (Reduction): Let $Q$ be the Paley matrix of (1). If a unimodular form $f = f_Q(a, b, c, d)$ satisfies (5) and if $d \geq 2$, then one of the expressions $3a + 2b - 14d$, $4a + 4b - 3c - 21d$ is strictly negative.

**Proof:** Case 1. If $c \leq \frac{1}{2}d$, we show $3a + 2b - 14d < 0$. Let $a = rd$, $b = sa$, where $r \geq 2$, $s \geq 1$. Then $b = sr'd$. We observe $r < 3$: for if $r \geq 3$, then $9d^2 \leq a^2 \leq ab = c^2 + 7d^2 + 1 \leq \frac{29d^2}{4} + 1$, but this is
Impossible since \( d \geq 2 \). Note also that, since 
\[
sr^2d^2 = ab \leq \frac{a^2d^2}{4} + 1,
\]
we have \( sr^2 \leq \frac{1}{2} \).

Thus if \( 1/\sqrt{2} \leq d \leq 3a + 3b \), then \( 1/\sqrt{2} \leq 3ad + 3br \) or
\[
1/\sqrt{2} \leq 3r^2 + 2sr^2 \leq 3r^2 + 1.5.
\]
Thus \( 3r^2 - 1.5r + 1.5 \geq 0 \).

But since the zeros of \( 3r^2 - 1.5r + 1.5 \) are at \( r = \frac{1}{3} \) and \( r = 3 \), and since \( 0 \leq r < 3 \), this is impossible.

Case 2. If \( 1/2d < c \leq d \), we show \( 4a + 4b - 3c - 21d < 0 \).

Observe that \( b < 4d \): for if \( b \geq 4d \), then, setting \( a = 2d + r \)
and \( b = 4d + s \), where \( r, s > 0 \), we have
\[
ab = (2d + r)(4d + s) = c^2 + 7d^2 + 1 \leq 8d^2 + 1,
\]
or
\[
4dr + 2ds + rs \leq 1.
\]
Since \( r, s \) are integers in this case, this implies \( r = s = 0 \), and therefore \( 2d^2 + c^2 + 7d^2 + 1 \), or \( d^2 - c^2 = 1 \), a contradiction to \( d \geq 2 \). We therefore set
\[
\begin{align*}
    a &= 2d + r, \\
    b &= 4d - s, \quad \text{and} \\
    c &= d - t,
\end{align*}
\]
where \( r \geq 0, s > 0 \) and \( 0 \leq t < 1/2d \). Then
\[
(2d + r)(4d - s) = (d - t)^2 + 7d^2 + 1,
\]
or
\[
4dr + 2dt - t^2 - 1 = 2ds + rs.
\]
Thus
\[
(6) \quad s = \frac{4dr + 2dt - t^2 - 1}{2d + r}.
\]

We wish to show \( 4a + 4b - 3c - 21d < 0 \), or \( 4r - 4s + 3t < 0 \).

By (6), this is
\[
4r + 3t < \frac{16dr + 8dt - 4t^2 - 4}{2d + r},
\]
or, equivalently,

\[(4) \quad 4r^2 + (3t - 3d)r + 4t^2 - 2dt + 4t > 0.\]

Now observe that, if \( r \geq d \), then \( 9d^2 \leq a^2 \leq ab \leq 8d^2 + 1 \), which is impossible. Thus \( r < d \). Note also that, since \( 2t \leq d - 1 \), we have \( 4t^2 \leq 2dt - 2t \), so that \( 4t^2 - 2dt + 4t \geq 2t \).

Therefore, \( 4r^2 + (3t - 3d)r + 4t^2 - 2dt + 4 \)
\[< \frac{4}{2} rd + \frac{3}{2} rd = 2rd + (4t^2 - 2dt + 4)\]
\[\leq -\frac{5}{2} rd + 4 - 2t \leq 0\]

for \( r > 0 \), or for \( r = 0 \) and \( t > 1 \). Thus (7) is established except for the two cases \( r = 0, t = 1 \) and \( r = 0, t = 0 \). We now settle these. First, suppose \( r = 0, t = 1 \).

Then \( 2d(4d - s) = 8d^2 - 2d + 2 \), which implies \( s = 1 - \frac{1}{d} \), but \( s \) is integral and \( d > 2 \), so this is impossible. If \( r = 0 \) and \( t = 0 \), then \( 2d(4d - s) = 8d^2 + 1 \), or \(-2ds = 1\), but \( s \) was assumed positive. Case 2 is therefore completed.

Case 3: If \( d < c \), we again show that \( 4a + 4b - 3c - 21d < 0 \).

Note that, by (5), we have

\[(8) \quad 4c^2 \leq c^2 + 7d^2 + 1 \quad \text{or} \quad c \leq \frac{7d^2 + 1}{3} < 2d.\]

We set

\[c = d + t,\]
\[a = 2d + 2t + r, \quad \text{and} \]
\[b = 4d - s,\]

where \( r \geq 0 \) and, by (8), \( 0 < t < d \). We assert that \( s \geq 0 \): for
\[(2d + t)(2d - s) \leq ab = d^2 + 2dt + t^2 + 7d^2 + 1 ,\]

which says \[-c \leq \frac{-6dt + t^2 + 1}{2d + 2t} \leq 0 \quad \text{for} \quad 0 < t < d .\]

Case 3 now proceeds much as Case 2, and the details will be omitted. //

We now consider two transformations, T_1 and T_2, whose matrices are

\[
T_1 = \begin{bmatrix} Q & 3I \\ -2I & -Q \end{bmatrix}, \quad T_2 = \begin{bmatrix} 3I & -I-Q \\ -I+Q & 3I \end{bmatrix}
\]

The effects of T_1 and T_2 on a form \( f = f_Q(a,b,c,d) \) is as follows:

\[
T_1 f T_1 = \begin{bmatrix} (7a + 4b - 28d)I & -cI + (3a + 3b - 13d)Q \\ -cI - (3a + 3b - 13d)Q & (9a + 7b - 42d)I \end{bmatrix}
\]

and

\[
T_2 f T_2 = \begin{bmatrix} (9a + 8b - 6c - 42d)I & (-3a - 3b + 3c + 14d)I + \\ (-3a - 3b + 3c + 14d)I & (8a + 9b - 6c - 42d)I + \\ (3a + 3b - 2c - 15d)Q & (3a + 3b - 2c - 15d)Q \end{bmatrix}
\]

We note especially that, upon application of T_1, the diagonal coefficients a and b undergo a change of

\( c(3a + 2b - 14d) \) and \( 3(3a + 2b - 14d) \), resp., while application of T_2 changes both diagonal coefficients by

\( 2(4a + 4b - 3c - 21d) \). Thus if the unimodular form

\( f = f_Q(a,b,c,d) \) satisfies (5) and if \( d \geq 2 \), then, by Lemma 3, application of T_1 or T_2 yields a (unimodular) form \( f' \)
with strictly smaller diagonal coefficients. If \( f' \) does not satisfy (5), note that it can be made to do so while leaving the smaller of the diagonal coefficients unchanged. This process must terminate in finitely many steps, leaving a form with \( d = 0 \) or \( 1 \). We now easily establish

**Theorem 1.** Every unimodular form \( f = f_Q(a,b,c,d) \), where \( Q \) is the Paley matrix of order 8, is equivalent to one of \( f_{16} (= f_Q(1,1,0,0)) \), \( f_Q(2,4,0,1) \) or \( f_Q(3,3,1,1) \).

**Proof:** In view of the above remarks, it suffices to show that the three forms listed are the only ones satisfying (5) with \( d = 0 \) or \( 1 \). We seek solutions of \( ab = c^2 + 7d^2 + 1 \). Let \( d = 0 \). Then \( ab = c^2 + 1 \), with \( 0 \leq c \leq \frac{1}{2} a \leq \frac{1}{2} b \). Thus \( 4c^2 \leq ab = c^2 + 1 \) and \( c = 0 \). This forces \( a = b = 1 \) and yields \( f_{16} \). Now let \( d = 1 \). Then \( ab = c^2 + 8 \), again with \( 4c^2 \leq ab \). Thus \( c^2 \leq \frac{8}{3} \), so that \( c = 0 \) or \( 1 \). If \( c = 0 \), then \( a = 2 \) and \( b = 4 \) is the only solution consistent with (5), yielding \( f_Q(2,4,0,1) \). If \( c = 1 \), the only possibility is \( a = b = 3 \), giving \( f_Q(3,3,1,1) \).

That these three forms represent distinct classes follows when one shows that \( f_Q(3,3,1,1) \) has minimum 2, which is easily done using the technique described in [5]. Since \( f_Q(2,4,0,1) \) represents only even numbers, it is obviously not equivalent to either of the others.
To complete our study for \( n = 16 \), we consider now the Paley matrix \( P \) of (1) and construct from it a skew orthogonal matrix

\[
\tilde{R} = \begin{bmatrix} P & 0 \\ 0 & P \end{bmatrix}
\]

of order 8 and norm 3. By Lemma 1, a form \( f_R(a,b,c,d) \) is unimodular if and only if \( a > 0 \) and

\[
ab = c^2 + 3d^2 + 1.
\]

**THEOREM 2.** Every unimodular form \( f = f_R(a,b,c,d) \), where \( R \) is the compound Paley matrix (10), is equivalent to one of \( f_{16} \) or \( f_R(2,2,0,1) \).

**PROOF:** We show first that (11) has no (integral) solution consistent with (5) for \( d > 2 \). Since \( 0 \leq 2c, 2d \leq a \leq b \), we have \( 4c^2 \leq ab = c^2 + 3d^2 + 1 \) or \( c^2 \leq d^2 + \frac{1}{3} \). Thus \( c \leq d \). On the other hand, \( 4d^2 \leq ab = c^2 + 3d^2 + 1 \), giving \( d^2 \leq c^2 + 1 \), or, since \( d \geq 2 \), \( d \leq c \). Thus \( d = c \) if \( d \geq 2 \). But \( a \) and \( b \) are both at least \( 2d \), so that \( ab = 4d^2 + 1 \) is impossible in integers. Thus \( d = 0 \) or \( 1 \).

Now if \( d = 0 \), we have \( 4c^2 \leq ab = c^2 + 1 \), or \( c = 0 \), \( a = b = 1 \). This gives \( f_{16} \). If \( d = 1 \), we see \( 4c^2 \leq ab = c^2 + 4 \). Thus \( c^2 \leq \frac{4}{3} \), yielding only \( a = b = 2 \), \( c = 0 \), or the form \( f_R(2,2,0,1) \) (which, incidentally, is
equivalent to \( 3 \pm x \).

Notice that the form \( f_R(2,2,0,1) \) represents only even numbers. It is not clear a priori that it is not equivalent to \( f_Q(2,4,0,1) \), encountered in Theorem 1. That it is not follows upon counting representations of \( \mathbb{Z} \) by both forms. Once again using techniques developed in [5], one shows without great difficulty that \( f_Q(2,4,0,1) \) represents 2 exactly 144 times, whereas \( f_R(2,2,0,1) \) has at least 203 representations that can be found immediately. This remark, along with Theorems 1 and 2, combine to yield

**THEOREM 3.** For \( n = 16 \), using the Paley matrices (1), four classes of unimodular forms (2) appear: the class of \( f_{16} \) and the three classes of minimum 2.
CHAPTER II
FORMS IN $2^b$ VARIABLES

1. After $n = 16$, the next interesting case for our constructive techniques is $n = 2^b$ (although there are limited possibilities also for $n = 20$). We have at our disposal the Paley matrix of order 12 and norm 11:

$$U = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\
-1 & -1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
-1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\
-1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\
-1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 & -1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & -1 & 1 \\
-1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 & 1 \\
-1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & 0 & 1 \\
-1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 \\
-1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 0
\end{bmatrix}$$

The total number of classes of unimodular forms in $2^4$ variables is very large. However, it has been shown by Niemeier ([9]) that there are $2^4$ even classes (an even form is one that represents only even numbers), of which 23 have minimum 2 and one has minimum 4 (the famous Leech form). Of the odd classes, it is known that only one has minimum 3 and the others have minimum 1 or 2.
As before, we ask which classes are represented by the forms \( f_V(a,b,c,d) \) (see Chapter I for definitions). Unfortunately, the methods employed for the case of 16 variables become far too cumbersome in 2^4 variables. We present in this chapter progress on an alternate approach to this problem. We are able to answer most efficiently questions concerning what we call Hermite equivalence of forms.

**DEFINITION.** Let \( V \) be a skew orthogonal matrix of order \( m \) and norm \( k \) (here again all matrices are integral). We call two forms \( f = f_V(a,b,c,d) \) and \( f' = f_V(a',b',c',d') \) Hermite-equivalent (or \( H \)-equivalent) if there are integers \( a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \) and a transformation \( T \) of determinant 1 with matrix

\[
T = \begin{bmatrix}
  a_1I + b_1V & a_2I + b_2V \\
  a_3I + b_3V & a_4I + b_4V
\end{bmatrix}
\]

such that \( T'fT = f' \).

Obviously, if two forms are \( H \)-equivalent, then they are equivalent. The converse fails in general, but the author believes that, for certain special matrices \( V \) (like the Paley matrices), the converse holds. This seems, however, to be a difficult question and no proof has been found.
The reason for the terminology in the definition is the connection between our forms $f_V(a,b,c,d)$ and the so-called binary Hermitian forms (see [10]). We discuss this connection briefly.

Let $k$ be a positive integer and define $j$ to be the complex number $j = \sqrt{-k}$. A binary quadratic form in the ring $\mathbb{Z}[j]$ is called Hermitian if its matrix is Hermitian. Such a form looks like $\phi = ax\bar{x} + cy\bar{y} + \bar{y}x\bar{y} + by\bar{y}$, where $\gamma \in \mathbb{Z}[j]$ and $a,b \in \mathbb{Z}$. Setting $\gamma = c + dj$, the matrix of $\phi$ is

$$
\phi_k(a,b,c,d) = \begin{bmatrix}
 a & c+dj \\
 c-dj & b
\end{bmatrix}
$$

(3)

It is not hard to see that a form (3) is positive definite with determinant 1 (i.e. unimodular) if and only if $a > 0$ and $ab - c^2 - kd^2 = 1$. Further, a transformation (2) corresponds in the obvious way to a transformation (4)

$$
\tau = \begin{bmatrix}
 \alpha_1 + \beta_1 j & \alpha_2 + \beta_2 j \\
 \alpha_3 + \beta_3 j & \alpha_4 + \beta_4 j
\end{bmatrix}
$$

and it is clear that $\tau' \phi_k(a,b,c,d) \tau = \phi_k(a',b',c',d')$ if and only if $T f_V(a,b,c,d) T = f_V(a',b',c',d')$, where $V$ is skew orthogonal of norm $k$ and $T$ is the transformation (2) corresponding to (4). We need to know when $T$ of (2) and
\( \tau \) of (4) have determinant 1. Note that the determinant of \( \Gamma \) can be calculated as follows. If we define
\[
\Delta = a_1a_4 - a_2a_3 + k\beta_2\beta_3 - k\beta_1\beta_4 \quad \text{and} \quad \Gamma = a_1\beta_4 + a_4\beta_1 - a_2\beta_3 - a_3\beta_2,
\]
then \(|\Gamma| = |\Delta I + \Gamma V|\). Since \((\Delta I + \Gamma V)(\Delta I - \Gamma V)' = \)
\((\Delta I + \Gamma V)(\Delta I - \Gamma V) = (\Delta^2 + k\Gamma^2)I\) (where \( I \) is of order \( m \), the order of \( V \)), we have \(|\Delta I + \Gamma V|^2 = (\Delta^2 + k\Gamma^2)^m\), and this \(|\Gamma| = (\Delta^2 + k\Gamma^2)^{m/2}\). Since \( m \) is even, \(|\Gamma| = 1\) says (for \( k > 1 \))
\[
|\Delta| = |a_1a_4 - a_2a_3 + k\beta_2\beta_3 - k\beta_1\beta_4| = 1 \quad \text{and} \quad (4')
\]
\[
\Gamma = a_1\beta_4 + a_4\beta_1 - a_2\beta_3 - a_3\beta_2 = 0
\]

On the other hand, the determinant of \( \tau \) is \( \Delta + \Gamma j \). Thus a transformation (2) of determinant 1 corresponds to a transformation (4) of determinant \( \pm 1 \). We call two forms \( \varphi \) and \( \varphi' \) semi-equivalent if there is a transformation \( \tau \) over \( \mathbb{Z}[j] \) of determinant \( \pm 1 \) such that \( \tau' \varphi \tau = \varphi' \). Thus two forms \( f \) and \( f' \) are \( H \)-equivalent if and only if the corresponding forms \( \varphi \) and \( \varphi' \) are semi-equivalent over \( \mathbb{Z}[j] \).

Now the analogy between the n-ary forms \( f_V(a,b,c,d) \) and the binary Hermitian forms \( \varphi_k(a,b,c,d) \) is complete, and any results we can obtain for the latter (with semi-equivalence over \( \mathbb{Z}[j] \)) will be valid for the former (with \( H \)-equivalence). For the slightly briefer notation, we study the binary Hermitian forms in this chapter.
Our first result is of a general nature, and, while its counterpart for binary quadratic forms over the rational integers is quite well-known (see [11]), we believe this generalization to be new. It gives a criterion for equivalence over $\mathbb{Z}[j]$ ($j^2 = -k$, $k$ a positive integer) for two forms $\varphi_k(a,b,c,d)$ and $\varphi_k(A,B,C,D)$.

**Theorem 1.** Let $j = \sqrt{-k}$, where $k$ is a positive integer. Two binary Hermitian forms $\varphi = \varphi_k(a,b,c,d)$ and $\tilde{\varphi} = \varphi_k(A,B,C,D)$ (with $A \neq 0$) are equivalent over $\mathbb{Z}[j]$ (by a transformation of determinant 1) if and only if they have the same determinant and there exist four rational integers $\alpha_1, \alpha_2, \beta_1, \beta_2$ satisfying:

(5) $A = a(a_1^2 + k\beta_1^2) + b(a_2^2 + k\beta_2^2) + 2c(a_1a_2 + k\beta_1\beta_2) + 2kd(a_1^2 - a_2^2 - a_1\beta_2)$

and the congruences

(6) $a_1a_1 + (c + C)a_2 - k(d + D)\beta_3 = 0 \pmod{A}$
(7) $ba_2 + (c - C)a_1 + k(d + D)\beta_1 = 0 \pmod{A}$
(8) $a\beta_1 + (c - C)\beta_3 + (d - D)a_3 = 0 \pmod{A}$
(9) $b\beta_3 + (c + C)\beta_1 - (d - D)a_1 = 0 \pmod{A}$

**Proof:** First suppose that $\varphi$ and $\tilde{\varphi}$ are equivalent. Then their determinants are the same and there is a transformation $\tau$ of determinant 1 such that

(10) $\tau' \varphi \tau = \tilde{\varphi}$.
Let the matrix of \( T \) be

\[
T = \begin{bmatrix}
\alpha_1 + \beta_1 \iota & \alpha_2 + \beta_2 \iota \\
\alpha_3 + \beta_3 \iota & \alpha_4 + \beta_4 \iota
\end{bmatrix}
\]

(10')

where, from (4'), \( \Gamma = \alpha_1 \beta_1 + \beta_1 \alpha_1 - \alpha_2 \beta_2 - \alpha_2 \beta_2 = \Delta \) and \( |\Delta| = \Delta = \alpha_1 \alpha_4 - \alpha_2 \alpha_3 + k \beta_2 \beta_3 - k \beta_1 \beta_4 = 1 \). We must show \( \alpha_1, \beta_1, \alpha_3, \beta_3 \) satisfy (5)-(9). After multiplying the matrices of (10), we see (5) and

\[
C = a(\alpha_1 \alpha_2 + k \beta_1 \beta_2) + b(\alpha_3 \alpha_4 + k \beta_3 \beta_4) + c(\alpha_1 \alpha_4 + d \beta_3) + k \beta_1 \beta_4)
\]

and

\[
D = a(\alpha_1 \beta_2 - a_2 \beta_1) + b(\alpha_3 \beta_4 - a_4 \beta_3) + c(\alpha_3 \beta_2 - a_2 \beta_3 - a_4 \beta_1 + a_1 \beta_4) + d(a_1 \alpha_2 - a_2 \beta_3 - k \beta_2 \beta_3 + k \beta_1 \beta_4).
\]

To prove (6), we use (4'), (11) and (12) to get

\[
a \alpha_1 + (c + C) \alpha_3 - k(d + D) \beta_3 = A \alpha_4
\]

Similarly, (7), (8) and (9) come from

\[
(b \alpha_3 + (c - C) \alpha_1 + k(d + D) \beta_1 = -A \alpha_2,
\]

\[
a \beta_1 + (c - C) \beta_3 + (d - D) \alpha_3 = -A \beta_4 \] and

\[
b \beta_3 + (c + C) \beta_1 - (d - D) \alpha_1 = A \beta_2.
\]

To prove the converse, let the quotients in the congruences (6) - (9) be called, respectively, \( \alpha_4, -\alpha_2, -\beta_4 \) and \( \beta_2 \). This gives back equations (13) - (16). Now
consider the transformation $\tau$ whose matrix is as in (10').

We show $\tau$ has determinant 1. Multiplying (13) - (16) by $a_1$, $a_3$, $k_1$ and $k_3$, resp., we get, upon addition of the resulting equations, $A = A \Delta$. Since $A \neq 0$, $\Delta = 1$. Further, multiplying (13) - (16) by $k_2$, $k_5$, $-a_2$, $-a_3$, resp., we get, upon addition, $C = A \Delta$. Thus $\tau = C$. Now let $\varphi' = \tau' \varphi \tau$. We show $\varphi' = \varphi$. To see this, multiply (13) - (16) by $a_2$, $a_4$, $k_2$, $k_4$, resp. Upon addition the result is (11). Similarly, multiplying by $k_2$, $k_1$, $a_2$, $a_4$, resp., addition gives (12). Here we use (4') in both cases. Now $\varphi' = \varphi_k(A, b', C, D)$, where $b'$ has yet to be determined. But since the determinants are the same, $b' = B$. Thus $\varphi' = \varphi$. //

This theorem has the effect of reducing six equations in eight unknowns to one equation and four congruences in two unknowns. The author is currently employing this result in an attempt to classify the (unimodular) automorphs of a form $\varphi_k(a, b, c, d)$.

We now present a procedure by which any unimodular form $\varphi_k(a, b, c, d)$ may be reduced (by equivalence) to a form in which $a$ is minimal. The method is derived from the techniques developed in [5].

We begin with a unimodular form $\varphi_k(a, b, c, d)$. As in the proof of Lemma 1, Chapter I, we apply the transformation
\[ \tau \text{ with matrix} \]
\[ \tau = \begin{bmatrix} a & c + dj \\ 0 & 1 \end{bmatrix} \]

to the form \( \tilde{\phi} = x\tilde{x} + y\tilde{y} \). The result is
\[ \tilde{\tau}'\tau = \begin{bmatrix} a & 0 \\ c-dj & 1 \end{bmatrix} \begin{bmatrix} a & c+dj \\ 0 & 1 \end{bmatrix} = a \begin{bmatrix} a & c+dj \\ c-dj & b \end{bmatrix} = a\phi. \]

We would like to know if \( \phi \) represents a number \( r \) smaller than \( a \) (indeed, we are looking for the smallest such), and if so, whether the representation can be used to produce a unimodular transformation of \( \tilde{\phi} \) which gives a form having \( r \) as a diagonal coefficient. So suppose \( \xi \) is a representation of \( r \) by \( \phi \), i.e. \( \tilde{\xi}'\phi \xi = r \). Then \( \tilde{\xi}'(a\phi)\xi = ar \), or \( \tilde{\xi}'\tilde{\tau}'\tau \xi = ar \). Thus \( \eta = \tau\xi \) is a representation of \( ar \) by \( \tilde{\phi} \). Conversely, given such an \( \eta \), we ask when \( \xi = \tau^{-1}\eta \) is integral. Since
\[ \tau^{-1} = \begin{bmatrix} 1/a & -1/a(c+dj) \\ 0 & 1 \end{bmatrix} \]
this says (setting \( \eta = (s,t), s,t \in \mathbb{Z}[j] \))
\[ (17) \quad s = t(c+dj) \pmod{a}. \]
Thus we seek solutions to the system
Now let $\xi = \tau^{-1}(s, w) = (z, w)$. In order that the required unimodular transformation exist, it is necessary and sufficient that there exist elements $z_o, w_o \in \mathbb{Z}[j]$ satisfying $zz_o + ww_o = 1$. Then the transformation $\sigma$ with matrix

$$
\sigma = \begin{bmatrix}
z & z_o \\
w & w_o
\end{bmatrix}
$$

will transform $\varphi$ to a form having $r$ as a diagonal coefficient. We may summarize the above this way:

**THEOREM 2:** Let $\varphi = \varphi_k(a, b, c, d)$ be unimodular. Then $\varphi$ is $H$-equivalent to a form $\varphi' = \varphi_k(r', b', c', d')$ if and only if there exist elements $s, t \in \mathbb{Z}[j]$ satisfying (18) and $z_o w_o \in \mathbb{Z}[j]$ satisfying $\frac{1}{a}[s - t(c + dj)]z_o + tw_o = 1$.

This process will clearly produce a form equivalent over $\mathbb{Z}[j]$ to $\varphi$ in which the smaller of the diagonal coefficients can not be reduced.

We return now to the case $j = \sqrt{-11}$, which corresponds to the unimodular forms $f_U(a, b, c, d)$, where $U$ is (for example) the Paley matrix (1). After applying the above procedure to all forms $\varphi_{11}(a, b, c, d)$ satisfying
0 \leq c,d \leq \tfrac{a}{2} \leq \tfrac{b}{2} \text{ with } d \geq 7, \text{ the author has found that five classes (under semi-equivalence) appear, represented by } \varphi_1 = \varphi_{11}(1,1,0,0), \varphi_{11}(2,0,0,1), \\
\varphi_3 = \varphi_{11}(3,1,0,1), \varphi_4 = \varphi_{11}(4,2,1) \text{ and } \varphi_5 = \varphi_{11}(5,3,1,1). \\
\text{While it has not been shown, it seems doubtful that any further classes will appear for } d > 7. \\
\text{We note that } \varphi_3 \text{ is the unique class of minimum } \delta \text{ and } \varphi_4 \text{ is the unique class of minimum } \lambda \text{ (both shown by Pall).} \\
\text{Finally, it should be noted that there exist other skew orthogonal matrices of order 12 and norm 11. By Theorem 1, the class structure (under H-equivalence) for the forms } f_Y(a,b,c,d) \text{ is identical to that in the above example. Whether the corresponding forms are equivalent (H-equivalence does not apply) seems to be a difficult question in general, but one that should be studied.}
I. **Introduction.** We discuss here the structure of orders of ternary cubic forms which are a product of three integral linear factors. Although this is a situation much simpler than the most general, it is hoped that the results obtained in this concrete example will be of help in later studies.

Though the work is primarily self-contained, the author is indebted to both G. Pall and H. Butts (both Louisiana State University), for discussions concerning some of their as yet unpublished work in this area.

II. We study the associative-commutative $\mathbb{Z}$-algebra $A = \mathbb{Z}[j_1, j_2, j_3]$, where $j_i^2 = j_i$, $j_i j_k = 0$ for $i \neq k$, and $j_1 + j_2 + j_3 = 1$. As a $\mathbb{Z}$-module, $A$ is 3-dimensional and we will take the set $\{j_1, j_2, j_3\}$ as a (ordered) $\mathbb{Z}$-basis, representing the elements of $A$ as $a_1 j_1 + a_2 j_2 + a_3 j_3$ or, alternatively, as a column in a $3 \times m$ matrix. Thus a $\mathbb{Z}$-module $M$ with basis $\{a_1 j_1 + a_2 j_2 + a_3 j_3, b_1 j_1 + b_2 j_2 + b_3 j_3, c_1 j_1 + c_2 j_2 + c_3 j_3\}$ may be written

$$M = \{a_1 j_1 + a_2 j_2 + a_3 j_3, b_1 j_1 + b_2 j_2 + b_3 j_3, c_1 j_1 + c_2 j_2 + c_3 j_3\}$$
For $\alpha = a_1j_1 + a_2j_2 + a_3j_3$, we define the conjugates of $\alpha$ by:

$$\alpha' = a_1j_2 + a_2j_3 + a_3j_1, \quad \alpha'' = a_1j_3 + a_2j_1 + a_3j_2$$

Then $N(\alpha)$, the norm of $\alpha$, is:

$$N(\alpha) = \alpha \cdot \alpha' \cdot \alpha'' = a_1a_2a_3$$

Likewise, if $(\alpha, \beta, \gamma)$ is any ordered triple of elements of $A$, we define the norm form of this triple by:

$$f = (x\alpha + y\beta + z\gamma)(x\alpha' + y\beta' + z\gamma')(x\alpha'' + y\beta'' + z\gamma'').$$

Thus we have associated with a module $M = [\alpha, \beta, \gamma]$ a collection of forms, the norm forms of the various Z-bases of $M$.

The determinant, $|M|$, of a module $M = [\alpha, \beta, \gamma]$ will be the absolute value of the determinant of the matrix of $M$, while classically the discriminant of the norm form of the triple $(\alpha, \beta, \gamma)$ is $|M|^2$.

By an order we will mean a subring of $A$ with identity which is 3-dimensional as a Z-module (thus the norm forms will be of non-zero discriminant). We will habitually confuse an order with its matrix.

We begin the study of these orders with:
LEMMA 1: Every order can be given a \( Z \)-basis of the form 
\[ \{a_1 l_1, b_1 l_1 + c j_2, 1\} \], where \( a, c > 0 \), \( 0 \leq b < a \), and \( a \mid b^2 - bc \).
Conversely, any module with such a \( Z \)-basis is an order of determinant \( ac \).

PROOF: Let
\[
\theta = \begin{pmatrix}
a_1 & b_1 & c_1 \\
a_2 & b_2 & c_2 \\
a_3 & b_3 & c_3 \\
\end{pmatrix}
\]

To maintain a basis, we must restrict ourselves to unit-modular column operations: column permutations, column translations and column negations. Using these, and by repeated application of the Euclidean algorithm, we can produce a 1 in the \((3, 3)\) position (since \( g.c.d.(a_3, b_3, c_3) = 1 \)), and then by subtracting a multiple of column 3 from each of the others, reduce to:
\[
\hat{\theta} = \begin{pmatrix}
a'_1 & b'_1 & c'_1 \\
a'_2 & b'_2 & c'_2 \\
0 & 0 & 1 \\
\end{pmatrix}
\]

Now since 1 \( \in \hat{\theta} \), we may replace \( c'_1 \) and \( c'_2 \) by 1. Again by the Euclidean algorithm, we replace \( b'_2 \) by \( g.c.d.(b'_2, a'_2) \) and subtract a multiple of column 2 from column 1 to get:
\[
\theta = \begin{pmatrix}
a'' & b'' & 1 \\
0 & b'' & 1 \\
0 & 0 & 1 \\
\end{pmatrix}
\]
By negating $a_1''$ if necessary and reducing $b_1''$ modulo $a_1''$, we get the required form. Now since $(b_1j_1 + c_1j_2)^2 \equiv 0$, we have:

$$b_1^2j_1 + c_1^2j_2 = r(b_1'j_1 + c_1'j_2) + sa_1 \quad (r, s \in \mathbb{Z})$$

which forces $r = c$ and $sa = b_1^2 - bc$. Thus $a \mid b_1^2 - bc$.

The converse is trivial. //

Thus every order takes the form

$$\theta = \begin{bmatrix} a & b & 1 \\ 0 & c & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad a, c > 0, \quad 0 \leq b < a$$

with the additional property

$$a \mid b_1^2 - bc.$$  

We now present the main theorems of this section (Theorems 1 and 2). Using them, many questions concerning orders and their class groups (ideals of orders will be discussed later) may be reduced to those concerning orders of prime-power determinants only. The theorems establish a bi-unique association between the set of orders $\theta$ of determinant $n = p_1^{\delta_1} \cdots p_k^{\delta_k}$ and the set of collections of orders $\theta_i, i = 1, 2, \ldots, k$ with respective determinants $p_1^{\delta_i}$. The association is by means of left matrix divisors, where an integral matrix $L$ is said to be a left divisor of an integral matrix $M$ if there is an integral matrix $R$ such that $M = LR$. 
**THEOREM 1.** (Factorization): for each order

\[
\begin{bmatrix}
  a & b & 1 \\
  0 & c & 1 \\
  0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\text{with } |\mathcal{G}| = n = p_1^{\delta_1} \cdots p_k^{\delta_k},
\]

there is a unique collection of orders \( \mathcal{G}_i \) with

\[
|\mathcal{G}_i| = p_i^{\delta_i} \quad (i = 1, \ldots, k)
\]

such that each \( \mathcal{G}_i \) is a left divisor of \( \mathcal{G} \). In this case, the \( \mathcal{G}_i \) are called the factors of \( \mathcal{G} \).

**PROOF:** Let

\[
\begin{bmatrix}
  a & b & 1 \\
  0 & c & 1 \\
  0 & 0 & 1 \\
\end{bmatrix}
= \begin{bmatrix}
  a_i & \beta_i & b_i & 1 \\
  p_i & p_i & b_i & 1 \\
  0 & \gamma_i & c_i & 1 \\
  0 & 0 & 1 \\
\end{bmatrix}
\]

\[
i = 1, \ldots, k
\]

with \((a_i, p_i) = (c_i, p_i) = 1, a_i + \gamma_i = \delta_i, \) and \((b_i, p_i) = 1\)

for \( b > 0, b_i = 0 \) for \( b = 0 \). We first establish the existence of \( \mathcal{G}_i \) for each \( i \).

**Case 1:** \( b > 0 \) and \( \beta_i < a_i \). Then

\[
\begin{bmatrix}
  a_i & \beta_i & 1 \\
  p_i & p_i & k & 1 \\
  0 & \gamma_i & 1 \\
  0 & 0 & 1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
  a_i & -k' & 0 \\
  a_i & -k' & 0 \\
  0 & c_i & 0 \\
  0 & 0 & 1 \\
\end{bmatrix}
\]

where \( k \) is the unique solution \( \text{mod } p_i^{\beta_i} \) to

\[
p_i^{\beta_i} c_i = p_i^{\beta_i} b_i + k' p_i^{\alpha_i}.
\]
Case 2: \( b > 0 \) and \( \beta_1 \geq \alpha_1 \); or \( b = 0 \). Then

\[
\begin{bmatrix}
\alpha_1 & \beta_{1-a_1} & b_1 \\
p_1 & 0 & 1 \\
p_1 & 1 & 1 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
\gamma_1 \\
p_1 & 1 \\
1 & 1 \\
0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
n_1 & p_1^{\beta_{1-a_1-b_1}} & 0 \\
p_1 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

Uniqueness: For all uniqueness arguments we note that:

a) the right divisor in each case must be upper triangular; and

b) the determinant conditions force the values of the diagonal entries of each matrix. This leaves only the \((1,2)\) entry of the left divisor in question.

Case 1: Since \( k \) was unique \( \text{(mod } p_i^{\alpha_i}) \), then \( kp_i^{\beta_i} \) is unique \( \text{(mod } p_i^{\alpha_i}) \).

Case 2: If

\[
\begin{bmatrix}
\alpha_1 & \beta_{1-a_1} & b_1 \\
p_1 & 0 & 1 \\
p_1 & 1 & 1 \\
0 & 0 & 1
\end{bmatrix}
= \begin{bmatrix}
\alpha_1 & d & 0 \\
p_1 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
a_1 & e & f \\
c_i & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

then \( p_i^{\beta_{1-b_1}} = p_i^{a_i}e + dc_i \)

and \( p_i^{a_i}|d \). But \( d \) is assumed to be reduced \( \text{(mod } p_i^{\alpha_i}) \).

Thus \( d = 0.//\)

**THEOREM 2** (Composition): Given any collection of orders

\( \gamma_i \) with \( |\gamma_i| = p_i^{\delta_i} \) \((i = 1, \ldots, k)\), there is a unique order \( \gamma \) with \( |\gamma| = p_1^{\delta_1} \cdots p_k^{\delta_k} \) for which each \( \delta_i \) is a left
divisor. In this case we call $\theta$ the composition of the $\theta_i$ and write $\theta = \theta_1 \circ \theta_2 \circ \ldots \circ \theta_k$.

**Proof:** We begin with existence. Let there be given orders

$$\theta_i = \begin{bmatrix} \alpha_i & 0 & 1 \\ p_i & \gamma_i & 1 \\ 0 & p_i & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad i = 1, \ldots, j \quad j \geq 0$$

and

$$\theta_i = \begin{bmatrix} \alpha_i & \beta_i & 1 \\ p_i & p_i & 1 \\ 0 & \gamma_i & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad i = j+1, \ldots, k$$

where $\alpha_i + \gamma_i = \delta_i$ and $(d_i, p_i) = 1$

Define

$$S_1 = \begin{bmatrix} m_1 & 0 & 1 \\ 0 & n_1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad m_1 = p_1 \ldots p_j$$

and

$$S_2 = \begin{bmatrix} m_2 & b & 1 \\ 0 & n_2 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad m_2 = p_{j+1} \ldots p_k$$

where $c$ is determined by the Chinese Remainder Theorem and the congruences:

$$d_i \{_{l=j+1}^{k} \frac{1}{p_l} \} \equiv c \{_{l=j+1}^{k} \frac{1}{p_l} \} \pmod{p_i}$$

for $j+1 \leq i \leq k$

where $\{ \}$ indicates that the $i^{th}$ term is to be omitted from
the product. Then \( c \) is uniquely determined
\[
\left( \prod_{i=j+1}^{k} a_i - a_i \right) \pmod{n_p},
\]
and we may assume \( 0 \leq c < \prod_{i=j+1}^{k} a_i - a_i \).

Thus \( 0 < c \leq \prod_{i=j+1}^{k} p_i \).

\( S_1 \) is clearly an order and we now verify that \( S_2 \)
is. We must show
\[
c \left( \prod_{i=j+1}^{k} p_i \right) c = c \left( \prod_{i=j+1}^{k} p_i \right) \pmod{p_i}.
\]

Since \( S_i \) is an order for each \( i \), we have
\[
p_i^i d_i = p_i \pmod{p_i}.
\]

Thus
\[
c \prod_{i=j+1}^{k} p_i d_i = c \prod_{i=j+1}^{k} p_i \pmod{p_i}.
\]

But from (3) we see
\[
c d_i \prod_{i=j+1}^{k} p_i \pmod{p_i} = c^2 \prod_{i=j+1}^{k} p_i \pmod{p_i}.
\]

and substituting this in (4) yields
\[
c^2 \prod_{i=j+1}^{k} p_i \pmod{p_i} = c \prod_{i=j+1}^{k} p_i \pmod{p_i}.
\]

Now multiplying the congruence and the modulus by \( p_i \), and
multiplying the congruence only by \( \prod_{i=j+1}^{k} p_i \), we have as
desired,
\[
c^2 \left( \prod_{i=j+1}^{k} p_i \right) \pmod{p_i} = c \prod_{i=j+1}^{k} p_i \pmod{p_i}.
\]

Thus both \( S_1 \) and \( S_2 \) are orders.
Now let \( k \) be defined by

\[(i) \quad m_1^k \equiv n_1 \pmod{m_2}\]

Then, for \( 0 \leq h < m_1 m_2 \), and \( h \equiv km_1 b \pmod{m_1 m_2} \),

\[
\begin{bmatrix}
  m_1 m_2 & h & 1 \\
  0 & n_1 n_2 & 1 \\
  0 & 0 & 1
\end{bmatrix}
= \begin{bmatrix}
  m_2 b & 1 \\
  0 & n_2 & 1 \\
  0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
  m_1 & 0 & 0 & 0 & 1 \\
  0 & n_1 & 0 & 0 & 1 \\
  0 & 0 & 1
\end{bmatrix}
\]

where \( \ell \) is defined by \( km_1b = n_1b + \ell m_2 \) and \( t \) is defined by \( h = km_1b + tm_1 m_2 \). This \( \theta \) clearly has \( S_1 \) and \( S_2 \) as left divisors and we now show that \( \theta \) is an order. It is this \( \theta \) that is the composition of the \( \theta_i \), \( \theta = \theta_1 \circ \theta_2 \circ \ldots \circ \theta_k \).

\( \theta \) is an order: Since \( S_2 \) is an order, we have

\[b^2 \equiv bn_2 \pmod{m_2}, \text{ thus}\]

\[kn_1b^2 \equiv kn_1bn_2 \pmod{m_2}, \]

which, using \((5)\), becomes

\[k^2m_1b^2 \equiv kn_1bn_2 \pmod{m_2}.
\]

Multiplying by \( m_1 \), we have, as required, since

\[h \equiv km_1b \pmod{m_1 m_2}, \]

\[k^2m_1^2b^2 \equiv km_1bn_1n_2 \pmod{m_1 m_2}.
\]

To complete the proof of existence, we need only show that \( \theta_i \) is a left divisor of \( S_1 \) for \( 1 \leq i \leq j \) and of \( S_2 \) for
\[ j + 1 \leq i \leq k. \]

If \( 1 \leq i \leq j \),
\[
\begin{bmatrix}
\prod_{\ell=1}^{i} p_{\ell}^{a_{\ell}} & 0 & 1 \\
0 & \prod_{\ell=1}^{i} p_{\ell}^{\beta_{\ell}} & 0 \\
0 & 0 & 1
\end{bmatrix}
= \begin{bmatrix}
p_{i}^{a_{i}} & 0 & 1 \\
0 & p_{i}^{\beta_{i}} & 1 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
\prod_{\ell=1}^{i} p_{\ell}^{a_{\ell}} & 0 & 1 \\
0 & \prod_{\ell=1}^{i} p_{\ell}^{\beta_{\ell}} & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

and if \( j + 1 \leq i \leq k \)
\[
\begin{bmatrix}
\prod_{\ell=j+1}^{k} p_{\ell}^{a_{\ell}} & 0 & 1 \\
0 & \prod_{\ell=j+1}^{k} p_{\ell}^{\beta_{\ell}} & 0 \\
0 & 0 & 1
\end{bmatrix}
= \begin{bmatrix}
p_{i}^{a_{i}} & 0 & 1 \\
0 & p_{i}^{\beta_{i}} & 1 \\
0 & 0 & 1
\end{bmatrix}
\begin{bmatrix}
\prod_{\ell=j+1}^{k} p_{\ell}^{a_{\ell}} & 0 & 1 \\
0 & \prod_{\ell=j+1}^{k} p_{\ell}^{\beta_{\ell}} & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

where \( h \) is defined as the quotient of the congruence
\[
\prod_{i=1}^{j} p_{i}^{a_{i}} \prod_{\ell=j+1}^{k} p_{\ell}^{\beta_{\ell}} = c \prod_{\ell=j+1}^{k} p_{\ell}^{\beta_{\ell}} \pmod{p_{i}^{a_{i}}}
\]

which is (3) multiplied by \( \frac{\beta_{i}}{p_{i}} \).

Thus there is at least one order satisfying the conditions of the theorem. We now prove that there is at most one. As in Theorem 1, we need only be concerned with the \((1,2)\) entry.

First, we note that if each \( \theta_{i} \) has its \((1,2)\) entry equal to 0, then so does \( \theta \), by Theorem 1. Also by Theorem 1, if \( \theta \) has its \((1,2)\) entry 0, then so do the \( \theta_{i} \). Now suppose some \( \theta_{i} \) has a non-zero \((1,2)\) entry.
Suppose further that
\[
\alpha = \begin{bmatrix}
  a & b & 1 \\
  0 & c & 1 \\
  0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
  p_i a_i & p_i b_i & 1 \\
  0 & p_i c_i & 1 \\
  0 & 0 & 1
\end{bmatrix}
\]
i = 1, \ldots, k

and
\[
\alpha' = \begin{bmatrix}
  a' & b' & 1 \\
  0 & c & 1 \\
  0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
  p_i a_i & p_i b_i & 1 \\
  0 & p_i c_i & 1 \\
  0 & 0 & 1
\end{bmatrix}
\]
i = 1, \ldots, k

with \( bb' \neq 0 \), are orders with \(|\alpha| = |\alpha'| = p_1 \cdots p_k \), where
\[
\delta_i = a_i + \gamma_i .
\]
We will show that if \( b \neq b' \), then \( \alpha \) and \( \alpha' \) differ in at least one factor. This, along with the above comments, will establish the uniqueness of the composition. Suppose, then, that \( b \neq b' \). Since \( b < a \), there is at least one prime, say \( p_j \), with \( \beta_j < a_j \). Then, by the proof of Theorem 1,
\[
\alpha_j = \begin{bmatrix}
  a_j & \beta_j & 1 \\
  p_j & p_j k & 1 \\
  0 & p_j & 1 \\
  0 & 0 & 1
\end{bmatrix}
\]
is the \( j \)th factor of \( \alpha \), where
\[
k = c_j^{-1} b_j \pmod{p_j} \frac{a_j - \beta_j}{p_j} .
\]
Let us now examine the \( j \)th factor of \( \alpha' \):
If $\beta_j = \beta'_j$, then $\beta_j \neq \beta'_j$ and, in fact, 
$\beta_j \neq \beta'_j \pmod{p_j}$ and therefore $\alpha_j \neq \alpha'_j$. If $\beta_j \neq \beta'_j$, 
then $p_j^\beta_j \neq p_j^\beta'_j$ and since $(k,p_j) = (k',p_j) = 1$. Thus 
again $\alpha_j \neq \alpha'_j$.

We have thus established a kind of unique factoring 
and composition among our orders, which should provide an 
opportunity for numerous applications.

Before proceeding, we present an example. We form 
the composition of the orders

\[
\alpha_1 = \begin{bmatrix} 5 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \alpha_2 = \begin{bmatrix} 4 & 2 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \alpha_3 = \begin{bmatrix} 27 & 12 & 1 \\ 0 & 3 & 1 \\ 0 & 0 & 1 \end{bmatrix}
\]

using the constructive methods of Theorem 2, whose notation 
we also retain. Note here $j = 1$.

Thus

\[
S_1 = \begin{bmatrix} 5 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad S_2 = \begin{bmatrix} 108 & b & 1 \\ 0 & 6 & 1 \\ 0 & 1 \end{bmatrix}
\]
where $b = c \cdot 2 \cdot 3$. By (3), $c$ is determined by the congruences:

$1 \cdot 3 = c \cdot 3 \pmod{2}$, $4 \cdot 2 = c \cdot 2 \pmod{9}$.

Thus $c = 1 \pmod{2}$ and $c = 4 \pmod{9}$, or $c = 13 \pmod{10}$, $c = 13$. Thus $b = 78$. To get $s$, we form $k = 5 \cdot 76c$, where $k = m_1^{-1}n_1 \pmod{m_2}$ or $k = e^{-1} \cdot 1 \pmod{10}$. By the Chinese Remainder theorem, we find $k = 65$. Reducing $65 \cdot 5 \cdot 78 = 25, 350 \pmod{540}$, we get $\theta = \begin{bmatrix} 540 & 510 & 1 \\ 0 & 6 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

One shows easily using the constructive techniques of Theorem 1 that $\theta$ has factors $\mathfrak{o}_1, \mathfrak{o}_2, \mathfrak{o}_3$.

We conclude this chapter by noting an alternate characterization of order: a 3-dimensional module $M$ contained in $\mathcal{A}$ is an order if and only if $M^2 = M$. This can be established by arguments similar to those already used, or is easily deduced from the following fact from commutative ring theory: Let $R$ be a commutative ring and $T$ a commutative $R$ algebra, both with identity. If $M \subseteq T$ is a finitely generated $R$-module with $T$-annihilator 0 and $M^2 = M$, then $M$ contains the identity of $T$. This can be proven easily by means of Cramer's rule.
CHAPTER IV
IDEALS OF ORDERS

I. We discuss in particular the class of invertible fractional ideals of a specified order $\theta \subset A$. We work as usual in the total quotient ring of $A$, which in this case is simply $T(A) = \mathbb{Q}[j_1, j_2, j_3]$. If $\theta$ is an order, we note that $T(\theta) = T(A)$.

DEFINITION: We call a subset $M \subset T(\theta)$ a fractional ideal of $\theta$ if $\theta M \subset M$. Further a fractional ideal $M$ is called invertible in $\theta$ (or for $\theta$) if there is another fractional ideal $N$ such that $MN = \theta$.

We note the following:

LEMMA 1: A fractional ideal is invertible in at most one order.

PROOF. Let $M$ be invertible in both $\theta$ and $\theta'$. Then there are ideals $N$ and $N'$ such that $MN = \theta$ and $MN' = \theta'$. Therefore $\theta = \theta \theta' = \theta MN' \subset MN' = \theta'$ and $\theta' \subset \theta \theta' = \theta' MN \subset MN = \theta$. Thus $\theta = \theta'$.

Now let

$$\theta = \begin{bmatrix} a & b & 1 \\ 0 & c & 1 \\ 0 & 0 & 1 \end{bmatrix}$$
be an order. The following characterization of invertible ideals for \( \mathfrak{O} \) is due to Pall and Butts:

**Theorem 1:** If \( \mathfrak{O} \) is the order in \( (1) \), then every invertible ideal \( \mathfrak{J} \) in \( \mathfrak{O} \) can be given an integral \( \mathbb{Z} \)-basis

\[
\mathfrak{J} = \begin{bmatrix} a & d & e \\ 0 & c & f \\ 0 & 0 & 1 \end{bmatrix}
\]

where \( 0 \leq d < a \)

\( 0 \leq e < a \)

and \( 0 \leq f < c \)

with the properties:

(2) \( (a,d,e) = 1 \)

(3) \( (c,f) = 1 \)

(4) \( d = \tilde{d} \cdot b \pmod{a} \) for some \( \tilde{d} \in \mathbb{Z} \).

(5) \( e = d \cdot f \pmod{a'}, a' = a/(a,b) \).

Conversely, any \( \mathbb{Z} \)-module \( (1') \) satisfying (2)-(5) is an invertible ideal for \( \mathfrak{O} \).

Note in particular that every invertible ideal is 2-dimensional as a \( \mathbb{Z} \)-module. Henceforth the term "invertible ideal" will mean an Hermite matrix \( (1') \) satisfying (2)-(5).

The main theorems of this chapter are analogous to Theorems 1 and 2 of Chapter 3, in that we establish a bi-unique correspondence between invertible ideals \( \mathfrak{J} \) and
sets of invertible ideals \( J_1 \) of prime-power determinants. First, however, we pause to discuss some properties of Hermite matrices developed by Pall in [1].

A square, integral \( n \times n \) matrix \( M = [m_{ij}] \) will be called Hermite if

\begin{enumerate}
  \item \( m_{ii} > 0 \)
  \item \( m_{ij} = 0 \) for \( i > j \), and
  \item \( \sum m_{ij} < m_{ii} \) for \( i < j \).
\end{enumerate}

Note that our invertible ideals \((1')\) are Hermite. From Lemma 6 of [1], we deduce:

**Lemma 2:** (a) Let \( M \) be Hermite with \( |M| = m_1 m_2, (m_1, m_2) = 1 \).

Then \( M \) has a unique Hermite left divisor of determinant \( m_1 \).

(b) Let \( M_1, \ldots, M_k \) be Hermite matrices with determinants coprime in pairs. Then there is a unique Hermite matrix \( M \) with \( |M| = \prod_{i=1}^{k} |M_i| \) having \( M_1, \ldots, M_k \) as left divisors.

We now establish

**Theorem 2:** Let \( \theta \) be the composition of the orders \( \theta_1, \ldots, \theta_k \), with \( |\theta_i| = p_1^i \), and suppose \( J \) is invertible in \( \theta \). Define \( J_1, \ldots, J_k \) to be the (unique) Hermite left divisors of \( J \) of respective determinants \( p_1^1, \ldots, p_k^k \).

Then for each \( i \), \( J_i \) is an invertible ideal for \( \theta_i \).
PROOF: The notation is from Chapter 3.

Let \( n = \sigma_1 \cdots \sigma_k \), where

\[
\sigma = \begin{bmatrix} a & b & 1 \\ 0 & c & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \iota = \begin{bmatrix} \alpha_i & \beta_i & k_i \\ p_i & p_i & 1 \\ 0 & p_i & 1 \end{bmatrix}
\]

with \( \alpha_i + \gamma_i = \delta_i \), \( k_i = 0 \) for \( 1 \leq i \leq j \) and \( j \geq 0 \).

Further, suppose that \( J \) is an invertible ideal of \( \mathfrak{a} \). By Lemma 2, for each \( i \), \( J \) has a unique Hermite left divisor of determinant \( p_i^{\delta_i} \). Call it \( J_1^{\delta_i} \). Then

\[
(J') \quad J = \begin{bmatrix} a & d & e \\ c & f & \gamma_i \\ 1 & p_i & 1 \end{bmatrix} = \begin{bmatrix} \alpha_i & \beta_i & k_i \\ p_i & p_i & 1 \\ 0 & p_i & 1 \end{bmatrix} = J_1^{\delta_i} S_i
\]

where, as before, the diagonal entries are fixed by the determinant condition. Note also that \( d_i = 0 \) if and only if \( k_i = 0 \) if and only if \( \beta_i \geq \alpha_i \). We must prove (2)-(5), which in this case read:

(7) \( (p_i^{\alpha_i}, d_i, e_i) = 1 \)

(8) \( (p_i^{\gamma_i}, f_i) = 1 \)

(9) \( d_i = \tilde{d}_i p_i^{\beta_i} (\text{mod } p_i^{\alpha_i}) \text{ for some } \tilde{d}_i \in \mathbb{Z} \).

(10) \( e_i = \tilde{d}_i f_i (\text{mod } p_i^{\alpha_i-\beta_i}) \)

(7) and (8) are clear since the analogous properties hold in
To prove \((\alpha)\), note that, from \((h)\), \((\gamma)\) and \((\gamma')\), we have
\[
p_i\alpha_1 x_1 + d_1 c_1 = \tilde{a}(\alpha p_i k_1' + p_i k_1 c_1) + ta \quad (t \in \mathbb{Z}).
\]
Thus \(d_1 c_1 = \tilde{a} p_i k_1 c_1 \pmod{p_i}\); but this is \((9)\) since \((c_1, p_i) = 1\). To get \((10)\), we use \((\tilde{a})\) and \((\gamma')\) to show
\[
p_i a_i y_1 + d_1 z_1 + e_1 = \tilde{a}(p_i y_1 z_1 + f_1) + sa' \quad (s \in \mathbb{Z}).
\]
Thus \(e_1 - \tilde{a} f_1 = -(d_1 - \tilde{a} p_i y_1) z_1 \pmod{p_i}\). But since \(\gamma_1\) is an order, we have that
\[
p_i y_1 = p_i k_1 \pmod{p_i}.
\]
This and \((9)\) give \((10)\).

The converse of Theorem 2 is

THEOREM 3: Let \(J_1, \ldots, J_k\) be invertible ideals for the orders \(\theta_1, \ldots, \theta_k\), resp., where \(|\theta_i| = |J_1| = p_i\) for \(i = 1, \ldots, k\), and let \(\theta = \theta_1 \circ \cdots \circ \theta_k\). Then there is a unique ideal \(J\) with \(|J| = |\theta|\) which is invertible in \(\theta\) and has the \(J_1\) as (Hermite) left divisors.

PROOF: Let
\[
J_i = \begin{bmatrix}
\alpha_i \\
p_i & d_i & e_i \\
0 & y_i & f_i \\
0 & 0 & 1
\end{bmatrix}
\]
d_1 = 0 for \(1 \leq i \leq j\).
and let

\[
(a) = \begin{bmatrix}
    a & b & 1 \\
    0 & c & 1 \\
    0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
    a_i & b_i & k_i & 1 \\
    0 & c_i & 1 \\
    0 & 0 & 1
\end{bmatrix} = \begin{bmatrix}
    n_i & -k_i' & 1 \\
    c_i & 0 & 1
\end{bmatrix}
\]

with \(k_i = 0\) for \(1 \leq i \leq j\) and \(j \geq 0\). The proof consists of constructing an Hermite matrix \(J\) of determinant \(\alpha\) with the \(J_i\) as left divisors. By Lemma 2 it will be unique. We then show \(J\) is invertible in \(\mathbb{Q}\).

We set \(J = \begin{bmatrix}
    a & d & e \\
    0 & c & f \\
    0 & 0 & 1
\end{bmatrix}\) and describe \(d, e,\) and \(f\).

Using the Chinese Remainder Theorem (CRT), we define \(d\) to be the unique solution to the system

\[
(d) \quad d \equiv d_i c_i \pmod{p_i^a} \quad i = 1, \ldots, k,
\]

with \(0 \leq d < a\). Also using CRT, define \(f\) by

\[
(f) \quad f \equiv f_i \pmod{p_i^a} \quad i = 1, \ldots, k,
\]

with \(0 \leq f < c\). Using CRT again, define \(e\) by

\[
(1^4) \quad e \equiv d_i z_i + e_i \pmod{p_i^a}
\]

where \(\{z_i\}\) are the quotients in (13), and \(0 \leq e < a\).

Thus \(J\) is Hermite. Now let \(\{x_i\}\) be the quotients in (12) and \(\{y_i\}\) be the quotients in (14).

Then
Thus each \( J_i \) is a left divisor of \( J \).

We now verify (2)-(5) for \( J \). If \( p_i | (a, d, c) \), then by (12) and (14) \( p_i | d_i \) and \( p_i | e_i \). Thus \( p_i | (p_i^{a_i}, d_i, e_i) \), a contradiction. This gives (2) and a similar argument gives (3). Now since \( J_i \) is invertible in \( \theta_i \), (9) gives \( p_i^a | d_i \) for \( j + 1 \leq i \leq k \). Thus, from (12), \( p_i^a | d \). Let \( d_i' = d / p_i^a \) and define \( \tilde{d} \) to be the solution of the system

\[
d_i' \equiv \tilde{d} b (\mod p_i^a) \quad \text{with} \quad j + 1 \leq i \leq k.
\]

In addition, note from (11) and (12) that, for \( 1 \leq i \leq j \),

\[
d_i' \equiv \tilde{d} b (\mod p_i^a) \quad \text{for} \quad j + 1 \leq i \leq k.
\]

Combining (16) and (17) gives (4). To prove (5), we first note that \( \tilde{d} \) may be substituted for \( \tilde{d}_i \), \( i = 1, \ldots, k \), in (9) and (10). To see this, use (4), (6) and (12) to get

\[
d_i c_i = -p_i x_i + \tilde{d}(-p_i k_i + p_i k_i c_i) + t p_i^a,
\]

which, since \( (c_i, p_i) = 1 \), yields

\[
d_i' \equiv \tilde{d} p_i^a k_i (\mod p_i^a).
\]

Thus, by (18), \( \tilde{d} \equiv \tilde{d}_i (\mod p_i^{a_i}) \), and

\[
(d_i' \equiv \tilde{d} f_i (\mod p_i^{a_i - \theta_i})). \quad \text{We now have}
\]
c = d_1 z_1 + e_1 \pmod{p_1^{\alpha_i - \beta_i}}
= d_1 z_1 + \tilde{d} f_i
= d_1 z_1 + \tilde{d} (f - z_1 p_1^{\gamma_i})
= z_1 (d_1 - \tilde{d} p_1^{\beta_i}) + \tilde{d} f
= d f \pmod{p_1^{\alpha_i - \beta_i}}.

2. As an application of Theorems 2 and 3, we calculate the order of the class group of an order $\mathcal{O}$. We first observe

**Lemma 3:** The only principal invertible ideal of $\mathcal{O}$ is $\mathcal{O}$ itself.

**Proof:** If there is an element $a = r_1 j_1 + s j_2 + t j_3 \in J$ such that $\mathfrak{p} a = J$, i.e.

$$
\begin{bmatrix}
a & b & 1 \\
0 & c & 1 \\
0 & 0 & 1 
\end{bmatrix}
\begin{bmatrix}
r \\
s \\
t 
\end{bmatrix}
= 
\begin{bmatrix}
a & d & e \\
0 & c & f \\
0 & 0 & 1 
\end{bmatrix},
$$

then clearly $t = 1$. Also $a = \ell a r$ for some $\ell \in \mathbb{Z}$, so $r = 1$. Likewise $c = \ell ' s c$, so that $s = 1$.//.

Therefore, to count the class group, we simply count the number of matrices (1') satisfying (2) - (5). We may suppose by Theorems 2 and 3 that $|\mathfrak{p}| = p^\delta$, $p$ a prime. Therefore, let
Case 1: \( k = d = 0 \). We need only choose \( c \) and \( f \) so that (2) and (3) hold. Thus there are \( \phi(p^\alpha) \) choices for \( c \) and \( \phi(p^\gamma) \) choices for \( f \), where \( \phi \) is the Euler \( \phi \)-function. Since the choices are independent ( (3) and (4) are satisfied automatically), the order of the group in this case is \( \phi(p^\alpha) \cdot \phi(p^\gamma) \).

Case 2: \( k, d \neq 0 \) (here \( \beta < \alpha \)). Here again we have \( \phi(p^\gamma) \) choices for \( f \). Now we must choose a \( \tilde{d} \) in one of \( p^{\alpha-\beta} - 1 \) ways (\( \tilde{d} = 0 \) is excluded) and \( e \) is determined \( \pmod{p^{\alpha-\beta}} \). However, \( e \) must only be reduced \( \pmod{p^\alpha} \), so there are \( p^\beta \) choices for \( e : e + mp^{\alpha-\beta}, 0 \leq m \leq p^\beta \). Thus there are \( (p^{\alpha-\beta} - 1) \cdot p^\beta \cdot \phi(p^\gamma) \) choices.

Now by the theorems, to calculate the order of the class group of \( \Theta \) with \( |\Theta| = p_1^{\delta_1} \ldots p_k^{\delta_k} \), one simply multiplies the orders of the class groups of the factors of \( \Theta \).
BIBLIOGRAPHY

3. L. E. Dickson, "La Composition des Polynomes", Comptes Rendues, 1921.

VITA

Richard Marshall Caron was born on 20 July 1944 in Calais, Maine. He attended elementary and secondary schools in Massachusetts and Florida, graduating from Seacrest High School in Delray Beach, Florida, in 1962. He graduated from Palm Beach Junior College in 1964 and received his B. A. in mathematics from Florida Atlantic University in 1966. He continued his study of mathematics at the Rockefeller University prior to moving to Louisiana State University, where he is now a candidate for the degree of Doctor of Philosophy in mathematics.

He is married to the former Lynne Marie Apsley and they have two children, Lisa, age 9, and Ricky, age 6.
EXAMINATION AND THESIS REPORT

Candidate: Richard Marshall Caron

Major Field: Mathematics

Title of Thesis: TOPICS IN QUADRATIC AND CUBIC FORMS

Approved:

[Signatures]

Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

[Signatures]

Date of Examination:

July 14, 1972