The Class-Group in Binary Quadratic-Orders.

John Wayne Matherne

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/2414

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 material 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 thru 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 photoing at the upper left hand corner of a large sheet and to continue photoing 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.

5. PLEASE NOTE: Some pages may have indistinct print. Filmed as received.

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106
MATHERNE, John Wayne, 1944-
THE CLASS GROUP IN BINARY QUADRATIC ORDERS.
The Louisiana State University and Agricultural and Mechanical College, Ph.D., 1973
Mathematics

University Microfilms, A XEROX Company, Ann Arbor, Michigan
THE CLASS GROUP IN BINARY QUADRATIC 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

John W. Matherne
B.S., Louisiana State University, 1966
M.S., Louisiana State University, 1968
May, 1973
ACKNOWLEDGMENT

The author wishes to express his appreciation to Professor Gordon Pall under whose direction this work was done.

Also, the author wishes to thank his wife, Nancy, and son, Christopher, for their patience and understanding during his graduate study.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>I</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>8</td>
</tr>
<tr>
<td>III</td>
<td>30</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>38</td>
</tr>
<tr>
<td>VITA</td>
<td>40</td>
</tr>
</tbody>
</table>
ABSTRACT

In this work the Gaussian theory of composition of binary quadratic forms is studied in an attempt to discover the structure of certain class groups of primitive binary quadratic forms. In their article "Modules and Binary Quadratic Forms" [2], H. S. Butts and Gordon Pall describe the abelian semigroup $\mathcal{J}$ of primitive classes of binary quadratic forms with discriminants in $\mathcal{D} = \{ d_0 s^2 | s = 1, 2, \ldots \}$, where $d_0$ is a fundamental discriminant. The semigroup $\mathcal{J}$ can be partitioned into subgroups consisting of the primitive classes of each discriminant $d$ in $\mathcal{D}$. The subgroup of primitive classes of discriminant $d \in \mathcal{D}$ will be denoted by $\mathcal{C}_d$, and $I_d$ will denote the principal class of $\mathcal{C}_d$.

The mapping $h: \mathcal{C}_{ds^2} \to \mathcal{C}_d$ defined by $h(C) = C \ast I_d$, the product under composition of $C$ and $I_d$, defines a homomorphism of $\mathcal{C}_{ds^2}$ onto $\mathcal{C}_d$ [2, p. 26].
results given in Chapter II determine the structure of the kernel of the homomorphism $h: \mathcal{C}_{ds^2} \to \mathcal{C}_d$. Thus if the structure of the group $\mathcal{C}_{ds^2}$ is known, then the structure of $\mathcal{C}_d$ is determined since $\mathcal{C}_d \cong \mathcal{C}_{ds^2}/\ker(h)$.

A more challenging question is whether the structure of $\mathcal{C}_{ds^2}$ is determined if the structure of $\mathcal{C}_d$ is known. Although this question was not completely settled, Theorem 3.4 does give an affirmative answer in case the group $\mathcal{C}_d$ has a single class in each genus.
INTRODUCTION

The problem investigated in this thesis is that of the structure of the class group in an arbitrary quadratic order. The methods used are mainly special cases of Gaussian composition by means of suitable bilinear substitutions. Both the problem and the methods originated in Gauss's Disquisitiones Arithmeticae (1801). The structure of the class group has, at least in the case of the maximal order, and in the corresponding case in algebraic fields, been of much interest to mathematicians in the subsequent 172 years, while the method of Gaussian composition has languished, and been considered much too difficult, until it was recently reconsidered by two of my professors at L.S.U., Hubert S. Butts and Gordon Pall.

One of the main features of interest in this thesis is how nicely Gaussian composition applies to the problem, while the alternative methods of composition by Dirichlet and Dedekind - which have long been considered simpler.
It has been conjectured (many times, it seems) that the Gaussian class groups provide realizations of any desired finite abelian group. This conjecture was actually proved a few years ago for the class groups of an arbitrary algebraic field by Luther Claborn - a young man who was killed in an automobile accident on his way to a position at Rice University. Whether it is true for quadratic fields, or perhaps quadratic orders, remains unknown, and it is partly with the hope of making applications to proving the conjecture in the case of quadratic orders that this thesis was initiated. It is curious that, although Gauss was already interested in the ratio of the number of classes in a quadratic order to the number in the maximal order, that the question of precisely how the structures of the two class groups are related has not hitherto been investigated.
CHAPTER I

We will follow the treatment of Gaussian composition given by Gordon Pall [9]. Let \( f, f', f'' \) be integral binary quadratic forms with non-zero discriminants \( d, d', d'' \) and the variables \( x_1, y_1, z_1 \) respectively. Further, take \( f \) and \( f' \) primitive. If the bilinear substitution,

\[
\begin{align*}
Z_1 &= P_{11}x_1y_1 + P_{12}x_1y_2 + P_{21}x_2y_1 + P_{22}x_2y_2 \\
Z_2 &= q_{11}x_1y_1 + q_{12}x_1y_2 + q_{21}x_2y_1 + q_{22}x_2y_2
\end{align*}
\]

which has matrix,

\[
M = \begin{bmatrix}
P_{11} & P_{12} & P_{21} & P_{22} \\
q_{11} & q_{12} & q_{21} & q_{22}
\end{bmatrix}
\]

makes \( f'' = ff' \), then \( f'' \) is also primitive since the \( x_i \) and \( y_i \) can be chosen to make \( ff' \) prime to
any desired integer. The bilinear substitution (1.1) expresses the linear transformation,

\[ z_1 = (p_{11}y_1 + p_{12}y_2)x_1 + (p_{21}y_1 + p_{22}y_2)x_2 \]

(1.3)

\[ z_2 = (q_{11}y_1 + q_{12}y_2)x_1 + (q_{21}y_1 + q_{22}y_2)x_2 \]

which sends \( f \) into \( f' \) and has determinant,

\[ \Delta' = \begin{vmatrix} p_{11}y_1 + p_{12}y_2 & p_{21}y_1 + p_{22}y_2 \\ q_{11}y_1 + q_{12}y_2 & q_{21}y_1 + q_{22}y_2 \end{vmatrix} . \]

Also, (1.1) expresses the linear transformation,

\[ z_1 = (p_{11}x_1 + p_{21}x_2)y_1 + (p_{12}x_1 + p_{22}x_2)y_2 \]

(1.5)

\[ z_2 = (q_{11}x_1 + q_{21}x_2)y_2 + (q_{12}x_1 + q_{22}x_2)y_2 \]

which sends \( f' \) into \( (f)f' \) and has determinant,

\[ \Delta = \begin{vmatrix} p_{11}x_1 + p_{12}x_2 & p_{12}x_1 + p_{22}x_2 \\ q_{11}x_1 + q_{12}x_2 & q_{12}x_1 + q_{22}x_2 \end{vmatrix} . \]

Let \( h \) and \( h' \) denote the divisors of the forms

\[ \Delta = [D_{12}, D_{14} - D_{23}, D_{34}] \quad \text{and} \quad \Delta' = [D_{13}, D_{14} + D_{23}, D_{24}] \]

where \( D_{ij} \) is the determinant of the \( i \)th and \( j \)th columns of \( M \). Then the bilinear substitution (1.1) is Gaussian.
If $\Delta = hf$, $\Delta' = h'f'$, and $M$ is primitive. To say $M$ is primitive means the six determinants $D_{12}$, $D_{13}$, $D_{14}$, $D_{23}$, $D_{24}$ and $D_{34}$ are coprime. We call $f''$ the product of $f$ and $f'$ under Gaussian composition and write $f'' = f*f'$.

It is shown in [9] that the following three properties are equivalent:

(i) $M$ is primitive.

(1.7) (ii) $(h,h') = 1$.

(iii) $d'' = (d,d')$.

Also in [9] we find that $d = h'd''$ and $d' = h^2d''$ so that if the forms $f$, $f'$, $f''$ have the same discriminant $d = d' = d''$, then $h = h' = 1$ and the bilinear substitution (1.1) is Gaussian if $\Delta = f$ and $\Delta' = f'$.

Finally, if $C_1$ and $C_2$ are primitive classes of integral binary quadratic forms, we define the product of $C_1$ and $C_2$ under composition to be the class of $f_1*f_2$ where $f_1 \in C_1$ and $f_2 \in C_2$. We will denote this product by $C_1* C_2$. The uniqueness of the product class $C_1* C_2$ is shown in [9].

In this paper we will deal with primitive classes of integral binary quadratic forms having discriminants in the set $\mathcal{D} = \{d_0s^2|s=1,2,\cdots\}$ where $d_0$ is a fundamental discriminant.
Theorem 1.8. Associated with any primitive classes $C_1$ and $C_2$ with discriminants in $\mathcal{D}$ there is a unique primitive class $C$ which is their product under composition. If the discriminants of $C_1$ and $C_2$ are $d_0s_1^2$ and $d_0s_2^2$, then the discriminant of $C$ is $d_0s^2$ where $s = (s_1, s_2)$. Under composition the set of all primitive classes of discriminants in $\mathcal{D}$ form an abelian semigroup $\mathcal{J}$, which can be partitioned into subgroups consisting of the primitive classes of each discriminant in $\mathcal{D}$. The identities $I_d$ in these subgroups are the only idempotents of $\mathcal{J}$.

Proof. [2, p. 25]

We will adopt the notation $C_d$ for the subgroup of $\mathcal{J}$ consisting of the primitive classes having discriminant $d$. It is the structure of the groups $C_d$ for $d$ in $\mathcal{D}$ that is investigated in this paper.

Theorem 1.9. The mapping $h: C_{ds^2} \rightarrow C_d$ defined by $h(C) = C \ast I_d$ maps the group $C_{ds^2}$ homomorphically onto the group $C_d$.

Proof. [2, p. 26]

Theorem 1.10. The class $C \ast I_d$ onto which a primitive
class $C$ of discriminant $ds^2$ is mapped can be characterized as the unique primitive class of discriminant $d$ which can be carried into $C$ by some integral transformation $T$ of determinant $|s|$. 

Proof. [2, p. 27]

From this theorem we see that if $h:C_{ds^2} \to C_d$, then $h^{-1}(C)$ consists of those primitive classes which are derivable from $C$ by integral transformations of determinant $|s|$. Also, it is clear that the kernel of $h$ consists of those primitive classes derivable from $I_d$ by integral transformations of determinant $|s|$. 
We begin this section with the following theorem about the forms derivable from a primitive form of discriminant \( d \).

**Theorem 2.1.** Let \( f = [a, b, c] \) be primitive, \( b^2 - 4ac = d \neq 0 \). Every form derivable from \( f \) by integral transformations of prime determinant \( p \) is equivalent to one of the \( p+1 \) forms,

\[
T^\alpha = [a p^2, (2a \alpha + b)p, a \alpha^2 + b \alpha + c], \alpha = 0, 1, \ldots, p-1
\]

\[
f^\infty = [a, pb, p^2c]
\]

where \( T^\infty = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \) and \( T_\alpha = \begin{bmatrix} p & \alpha \\ 0 & 1 \end{bmatrix} \) for \( \alpha = 0, 1, \ldots, p-1 \). Exactly \( p - (d/p) \) of these forms are primitive.

**Proof.** [7, p. 791].

**Theorem 2.2.** If in Theorem 2.1, \( f \) is replaced by an equivalent form \( g \), the classes of \( g^\infty, g^0, \ldots, g^{T^p_l} \) constitute a permutation of the classes of...
Proof. [7, p. 792].

In view of the above theorem we see that the classes derived from a given class $C$ of binary quadratic forms, are precisely the classes derived from any form in $C$. These classes need not be distinct, in fact, the number of distinct primitive classes is, if $d < 0$,

$$p - \left(\frac{d}{p}\right)$$

where $\sigma = 1$ if $d < -4$, $\sigma = 2$ if $d = -4$, and $\sigma = 3$ if $d = -3$ [6, p. 790].

Let $I_d$ denote the principal class of discriminant $d$, and for the moment assume $d = -4m$ with $m > 1$. In $I_d$ select the principal form $[1,0,m]$ and consider the primitive classes derived from $[1,0,m]$ by integral transformations of determinant $p$, an odd prime. Denote these classes by $[1,0,m]_T^{\infty}$, $[1,0,m]_T^0$, ..., $[1,0,m]_T^{p-1}$ where it is understood that any improper classes are disregarded. In this case there will be exactly $p - \left(\frac{d}{p}\right)$ distinct primitive classes. We recall from the discussion in Chapter I that these classes constitute the kernel of the homomorphism $h: C_{dp^2} \to C_d$, and thus form a group under composition. The class of $[1,0,m]_T^{\infty}$ is the principal class of discriminant $dp^2$.
and thus,

\[(2.3) \quad [1,0,m]^T_\alpha \ast [1,0,m]^T_\beta = [1,0,m]^T_\gamma \quad \text{for} \quad \alpha = 0,1,\ldots,p-1.
\]

In case \(\alpha \neq \infty\) and \(\beta \neq \infty\) we must have

\[ [1,0,m]^T_\alpha \ast [1,0,m]^T_\beta = [1,0,m]^T_\gamma \]

which means there is a Gaussian substitution which takes

\[ [1,0,m]^T_\alpha = (pz_1 + \gamma z_2)^2 + mz_2^2 \]

into the product of

\[ [1,0,m]^T_\alpha = (px_1 + \alpha x_2)^2 + mx_2^2 \]

and

\[ [1,0,m]^T_\beta = (py_1 + \beta y_2)^2 + my_2^2 \]

In an attempt to find the Gaussian substitution we equate the form factors,

\[(2.4) \quad (px_1 + \alpha x_2 + \theta x_2)(py_1 + \beta y_2 + \theta y_2) = pz_1 + \gamma z_2 + \theta z_2 , \]

where \(\theta = \sqrt{-m}\). Equating real and imaginary parts in the above gives the following bilinear substitution:

\[(2.5) \quad z_1 = px_1 y_1 + (\beta - \gamma) x_1 y_2 + (\alpha - \gamma) x_2 y_1 +
\]

\[ + \frac{\alpha \beta - m - \gamma (\alpha + \beta)}{p} x_2 y_2 \]

\[ z_2 = px_1 y_2 + px_2 y_1 + (\alpha + \beta) x_2 y_2 \]

which is integral if and only if \(\gamma \equiv \frac{\alpha \beta - m}{\alpha + \beta} \pmod{p}\).

It is straightforward to check that the bilinear substitution (2.5) does take the form \([1,0,m]^T_\gamma\) into the product of the forms \([1,0,m]^T_\alpha\) and \([1,0,m]^T_\beta\).
Finally, to see that (2.5) is Gaussian, we write it as:

\[
(2.6) \quad z_1 = [py_1 + (\beta - \gamma)y_2]x_1 + [(\alpha - \gamma)y_1 + \frac{\alpha\beta - m - \gamma(\alpha + \beta)}{p} y_2]x_2
\]

\[
z_2 = [py_2]x_1 + [py_1 + (\alpha + \beta)y_2]x_2
\]

considering it as a transformation in terms of the \( x \)'s, with the \( y \)'s held constant. The determinant of the transformation given in (2.6) is then,

\[
(2.7) \quad \Delta_y = p^2 y_1^2 + 2p\beta y_1 y_2 + (\beta^2 + m)y_2^2 = [l, 0, m]^T \beta.
\]

Likewise, if we consider the bilinear substitution as a transformation in terms of the \( y \)'s with the \( x \)'s held constant, then

\[
(2.8) \quad z_1 = [px_1 + (\alpha - \gamma)x_2]y_1 + [(\beta - \gamma)x_1 + \frac{\alpha\beta - m - \gamma(\alpha + \beta)}{p} x_2]y_2
\]

\[
z_2 = [px_2]y_1 + [px_1 + (\alpha + \beta)x_2]y_2
\]

and the determinant is,

\[
(2.9) \quad \Delta_x = p^2 x_1^2 + 2\alpha p x_1 x_2 + (\alpha^2 + m)x_2^2 = [l, 0, m]^T \alpha.
\]

Thus, (2.5) is a Gaussian substitution under which 

\[
[l, 0, m]^T \gamma
\]

is taken into the product of 

\[
[l, 0, m]^T \alpha
\]

and 

\[
[l, 0, m]^T \beta.
\]

Hence, we have shown that in case \( \alpha + \beta \neq 0 \ (\text{mod} \ p) \), 

\[
[l, 0, m]^T \alpha * [l, 0, m]^T \beta = [l, 0, m]^T \gamma
\]

where \( \gamma = \frac{\alpha\beta - m}{\alpha + \beta} \ (\text{mod} \ p) \).
In case \( \alpha + \beta \equiv 0 \pmod{p} \) then

\[
[l,0,m]^T_\alpha \ast [l,0,m]^T_\beta = [l,0,m]^T_\infty;
\]

that is, the classes of \([l,0,m]^T_\alpha\) and \([l,0,m]^T_\beta\) are inverses provided \(\alpha + \beta \equiv 0 \pmod{p}\). To see this we simply observe that,

\[(2.10) \quad z_1 = p^2x_1y_1 + p\beta x_1y_2 + px_2y_1 + (\alpha\beta - m)x_2y_2
\]

is a Gaussian substitution which takes the form

\[
[l,0,m]^T_\infty = z_1^2 + mp^2z_2^2
\]

into the product of the forms

\[
[l,0,m]^T_\alpha = (px_1 + \alpha x_2)^2 + mx_2^2 \quad \text{and} \quad [l,0,m]^T_\beta = (py_1 + \beta y_2)^2 + my_2^2.
\]

It should be noted that the substitution (2.10) is obtained in the same manner used for (2.5).

Summarizing the results of this discussion we have,

\[
[l,0,m]^T_\gamma, \gamma = \frac{\alpha\beta - m}{\alpha + \beta}
\]

if \(\alpha + \beta \not\equiv 0 \pmod{p}\)

\[
[1,0,m]^T_{\alpha \ast [1,0,m]^T_\beta} = \begin{cases} [l,0,m]^T_\infty, & \text{if } \alpha + \beta \equiv 0 \pmod{p} \end{cases}
\]

Theorem 2.12. Let \( d = -4m \) with \( m > 1 \). The primitive classes of binary quadratic forms derivable from the principal class of discriminant \( d \) by integral
transformations of an odd prime determinant \( p \), form a cyclic group under composition having order \( p - \left(\frac{d}{p}\right) \).

**Proof.** We have already observed that these classes form a group having order \( p - \left(\frac{d}{p}\right) \). Now we must see that this group is cyclic. Let \( I = [1, 0, m] \) so that any of the derived classes can be expressed as the class of

\[ I^\alpha \]

for some \( \alpha = \infty, 0, 1, \ldots, p-1 \). From formula (2.11),

\[ [I^\alpha]^2 = I^\alpha * I^\alpha = I^\gamma \]

where \( \gamma = \frac{\alpha^2 - m}{2\alpha} \), and in general we have the following formula, with \( \theta = \sqrt{-m} \):

\[ (2.13) \quad [I^\alpha]^n = I^\gamma, \quad \text{where} \quad \gamma = \frac{(\alpha+\theta)^n + (\alpha-\theta)^n}{(\alpha+\theta)^n - (\alpha-\theta)^n} \cdot \theta \pmod{p} \]

and of course \( \gamma = \infty \) if \( (\alpha+\theta)^n - (\alpha-\theta)^n \equiv 0 \pmod{p} \).

To verify (2.13) we use induction on \( n \). It is clear that this formula holds when \( n = 2 \). If we take

\[ [I^\alpha]^{n-1} = I^\beta \]

where \( \beta = \frac{(\alpha+\theta)^{n-1} + (\alpha-\theta)^{n-1}}{(\alpha+\theta)^{n-1} - (\alpha-\theta)^{n-1}} \cdot \theta \pmod{p} \),

then equation (2.11) gives \( [I^\alpha]^n = I^\alpha * I^\beta = I^\gamma \) with

\[ \gamma = \frac{\alpha\beta - m}{\alpha + \beta} \pmod{p} \]. Substituting for \( \beta \) gives,

\[ \gamma = \frac{(\alpha+\theta)^n + (\alpha-\theta)^n}{(\alpha+\theta)^n - (\alpha-\theta)^n} \cdot \theta \pmod{p} \]. The important thing to notice is that in this expression for \( \gamma \) the denominator is a polynomial in \( \alpha \) whose degree will be \( n-1 \), and thus has at most \( n-1 \) roots modulo \( p \). This means that
for any \( n \), the number of classes \( I_a^n \), such that \([I_a^n]\) is the principal class, is less than \( n \). The group is thus cyclic and the theorem is proved.

We now turn our attention to those classes of binary quadratic forms which are derivable from the principal class of discriminant \( d \) by transformations of determinant \( p^n \), for an odd prime \( p \) and positive integer \( n \). Again, by repeated application of Theorem 2.1, we find that the classes derivable from the principal class of discriminant \( d = -4m \) are the classes of the forms,

\[
I(p^n,p^n,a) \quad \text{for} \quad \alpha = 0,1,\ldots,p^n-1
\]
\[
I(p^n,p^{n-1},\beta) \quad \text{for} \quad \beta = 0,1,\ldots,p^{n-1} - 1
\]
\[
I(p^n,p,\gamma) \quad \text{for} \quad \gamma = 0,1,\ldots,p-1
\]
\[
I(p^n,1,0)
\]

(2.14)

where \( I(p^n,p^k,\alpha) \) denotes the form obtained by applying the transformation \[
\begin{bmatrix}
p^k & \alpha \\
0 & p^{n-k}
\end{bmatrix}
\]
to the principal form \( I = [1,0,m] \). We will adopt this notation for the remainder of this chapter.

Theorem 2.15. If \( d = -4m \) with \( m > 1 \) and \( p \) is an
odd prime, then the primitive classes among

\[ I(p^n, p^k, \alpha), \quad \alpha = 0, 1, \ldots, p^k - 1 \]
\[ I(p^n, p^{k-1}, \beta), \quad \beta = 0, 1, \ldots, p^{k-1} - 1 \]
\[ \vdots \]
\[ I(p^n, p^1, \gamma), \quad \gamma = 0, 1, \ldots, p - 1 \]
\[ I(p^n, 1, 0) \]

where \( k < n \), form a cyclic group, under composition, having order \( p^k \). Further, each primitive class of the type \( I(p^n, p^k, \alpha) \) has order \( p^k \).

**Proof.** We first notice that the classes of the type \( I(p^n, p^k, \alpha) \) compound as follows,

\[
I(p^n, p^k, \alpha) \ast I(p^n, p^k, \beta) = \begin{cases} 
I(p^n, p^k, \gamma) \\
\text{where } \gamma = \frac{\alpha \beta - 2p(n-k)}{\alpha + \beta} \pmod{p^k}, \\
\text{if } \alpha + \beta \neq 0 \pmod{p}
\end{cases}
\]

\[
I(p^n, p^{k-1}, \gamma) \\
\text{where } \gamma = \frac{\alpha \beta - 2p(n-k)}{\alpha + \beta} \pmod{p^{k-1}},
\]

\[
\text{if } \alpha + \beta = 0 \pmod{p} \\
\text{but } \alpha + \beta \neq 0 \pmod{p^2}
\]
This formula is obtained by observing that in case \( \alpha + \beta \neq 0 \pmod{p} \),

\[
z_1 = p^k x_1 y_1 + (\beta - \gamma)x_1 y_2 + (\alpha - \gamma)x_2 y_1 + \frac{\alpha \beta - 2p^{2(n-k)-\gamma} + \gamma(\alpha + \beta)}{p^k} x_2 y_2
\]

\[
z_2 = p^k x_1 y_1 + p^k x_2 y_1 + (\alpha + \beta)x_2 y_2
\]
is a Gaussian substitution taking \( I(p^n, p^k, \gamma) \) into the product of \( I(p^n, p^k, \alpha) \) and \( I(p^n, p^k, \beta) \) where the \( x \)'s, \( y \)'s and \( z \)'s are the variables associated with the forms \( I(p^n, p^k, \alpha) \), \( I(p^n, p^k, \beta) \) and \( I(p^n, p^k, \gamma) \) respectively.

Also in case \( \alpha + \beta = 0 \pmod{p} \) but \( \alpha + \beta \neq 0 \pmod{p^2} \),

\[
z_1 = p^{k+1} x_1 y_1 + (p \beta - \gamma)x_1 y_2 + (p \alpha - \gamma)x_2 y_1 + \frac{\alpha \beta - 2p^{2(n-k)} - \gamma(\alpha + \beta)}{p^{k-1}} x_2 y_2
\]

\[
z_2 = p^{k-1} x_1 y_2 + p^{k-1} x_2 y_1 + (\frac{\alpha + \beta}{p})x_2 y_2
\]
is a Gaussian substitution taking \( I(p^n, p^{k-1}, \gamma) \) into the product of \( I(p^n, p^k, \alpha) \) and \( I(p^n, p^k, \beta) \), where the \( x \)'s, \( y \)'s and \( z \)'s are the variables associated with the forms \( I(p^n, p^k, \alpha) \), \( I(p^n, p^k, \beta) \) and \( I(p^n, p^{k-1}, \gamma) \) respectively.

It should be noted that formula (2.16) does not cover all cases; however, it will suffice for the proof of this theorem.

We proceed with the proof of Theorem 2.15 by induction on \( k \). If \( k = 1 \), this group consists of the
primitive classes among \( I(p^n, 1, 0), I(p^n, p, \alpha) \), for \( \alpha = 0, 1, \ldots, p-1 \). These classes are exactly those derivable from the principal class of discriminant \( dp^{2(n-1)} \) by integral transformations of determinant \( p \). Thus, from Theorem 2.12, the group is cyclic of order \( p \).

Now take \( k < n \) and assume the theorem is true for \( k-1 \). There will be \( p^{k-1} + (p^k - p^{k-1}) = p^k \) primitive classes. Hence, the group will have order \( p^k \). From formula (2.16) we find that the \( n \)th power of the class \( I(p^n, p^k, 1) \) under composition is given by

\[
[I(p^n, p^k, 1)]^n = I(p^n, p^k, \gamma), \quad \gamma = \frac{A}{n-B} \pmod{p}
\]

where \( A \) and \( B \) are polynomials in \( p \), and of course, assuming \( n-B \neq 0 \pmod{p} \). It is also clear that \( p \mid B \), and thus \( n = p \) is the least power of \( I(p^n, p^k, 1) \) which gives a class of the type \( I(p^n, p^{k-1}, \alpha) \). Hence, \( [I(p^n, p^k, 1)]^p \) has order \( p^{k-1} \) and from this it follows that \( I(p^n, p^k, 1) \) has order \( p^k \), the order of the group.

Finally there are \( p^{k-1}(p-1) = \phi(p^k) \) primitive classes of the type \( I(p^n, p^k, \alpha) \), and since there are \( \phi(p^k) \) generators of this group, it follows that each primitive class of the type \( I(p^n, p^k, \alpha) \) has order \( p^k \). This completes the proof of Theorem (2.15).

**Theorem 2.17.** Let \( d = -4m \), \( m > 1 \), and \( p \) an odd
prime such that \( p \nmid d \). The primitive classes of binary quadratic forms derivable from the principal class of discriminant \( d \) by integral transformations of determinant \( p^n \), form a cyclic group under composition. The order of this group is \( p^{n-1}(p - \left(\frac{d}{p}\right)) \).

**Proof.** With the notation previously introduced we are considering the group of primitive classes among,

\[
I(p^n, p^n, \alpha), \quad \alpha = 0, 1, \ldots, p^n - 1
\]
\[
I(p^n, p^{n-1}, \beta), \quad \beta = 0, 1, \ldots, p^{n-1} - 1
\]
\[
\vdots
\]
\[
I(p^n, p, \gamma), \quad \gamma = 0, 1, \ldots, p - 1
\]
\[
I(p^n, 1, 0)
\]

It follows by repeated application of Theorem (2.1) that the order of this group is \( p^{n-1}(p - \left(\frac{d}{p}\right)) \).

From Theorem (2.15) we know that the primitive classes among,
\[ I(p^n, p^{n-1}, \alpha), \quad \alpha = 0, 1, \ldots, p^{n-1} - 1 \]

\[ I(p^n, p^{n-2}, \beta), \quad \beta = 0, 1, \ldots, p^{n-2} - 1 \]

\[ \vdots \]

\[ I(p^n, p, \gamma), \quad \gamma = 0, 1, \ldots, p-1 \]

\[ I(p^n, 1, 0) \]

form a cyclic group of order \( p^{n-1} \), and that each class of the type \( I(p^n, p^{n-1}, \alpha) \) has order \( p^{n-1} \).

Following the procedure used before, we find that the product under composition of classes of the type \( I(p^n, p^n, \alpha) \) is given by,

\[
I(p^n, p^n, \alpha) \ast I(p^n, p^n, \beta) = \begin{cases} 
I(p^n, p^n, \gamma) \\
\text{where } \gamma = \frac{\alpha \beta - m}{\alpha + \beta} \pmod{p^n} \\
\text{if } \alpha + \beta \neq 0 \pmod{p} 
\end{cases}
\]

\[
I(p^n, p^{n-1}, \gamma) \\
\text{where } \gamma = \frac{\alpha \beta - m}{\alpha + \beta} \pmod{p^{n-1}} \\
\text{if } \alpha + \beta = 0 \pmod{p} \\
\text{but, } \alpha + \beta \neq 0 \pmod{p^2}.
\]

(2.18)

To verify (2.18) we simply notice that in case \( \alpha + \beta \neq 0 \pmod{p} \) the bilinear substitution,
\[ z_1 = p^n x_1 y_1 + (\beta - \gamma)x_1 y_2 + (\alpha - \gamma)x_2 y_1 + \frac{a\beta - m - \gamma(a+\beta)}{p^n} x_2 y_2 \]

\[ z_2 = p^n x_1 y_2 + p^n x_2 y_1 + (\alpha + \beta)x_2 y_2 \]

is a Gaussian substitution which takes \( I(p^n, p^n, \gamma) \) into the product of \( I(p^n, p^n, \alpha) \) and \( I(p^n, p^n, \beta) \). Likewise, if \( \alpha + \beta \equiv 0 \pmod{p} \) but \( \alpha + \beta \not\equiv 0 \pmod{p^2} \), then the bilinear substitution,

\[ z_1 = p^{n-1} x_1 y_1 + (\beta - \gamma)x_1 y_2 + (\alpha - \gamma)x_2 y_1 + \frac{a\beta - m - \gamma(a+\beta)}{p^{n-1}} x_2 y_2 \]

\[ z_2 = p^{n-1} x_1 y_2 + p^{n-1} x_2 y_1 + \frac{\alpha + \beta}{p} x_2 y_2 \]

is a Gaussian substitution which takes \( I(p^n, p^{n-1}, \gamma) \) into the product of \( I(p^n, p^n, \alpha) \) and \( I(p^n, p^n, \beta) \).

We will now use (2.18) to show that the \( j \)th power under composition of a class of the type \( I(p^n, p^n, \alpha) \) is given by the formula,

\[ [I(p^n, p^n, \alpha)]^j = I(p^n, p^n, \gamma), \]

\[ \gamma \equiv \frac{(\alpha + \theta)^j + (\alpha - \theta)^j}{(\alpha + \theta)^j - (\alpha - \theta)^j} \cdot \theta \pmod{p^n} \]

provided \( (\alpha + \theta)^j - (\alpha - \theta)^j \not\equiv 0 \pmod{p} \). To verify this formula we use induction on \( j \). If \( j = 2 \),

\[ [I(p^n, p^n, \alpha)]^2 = I(p^n, p^n, \gamma) \]
\[ Y = \frac{a^2 - m}{2\alpha} = \frac{(a+\theta)^2 + (a-\theta)^2}{(a+\theta)^2 - (a-\theta)^2} \cdot \theta \pmod{p^n}. \]

Taking (2.19) to be true for \( j = 1 \), we see that

\[ [I(p^n, p^n, a)]^j = I(p^n, p^n, a) \times [I(p^n, p^n, a)]^{j-1} = I(p^n, p^n, \gamma) \]

where

\[ \gamma = \frac{(a+\theta)^j - (a-\theta)^j}{(a+\theta)^j - (a-\theta)^j} \cdot \theta \]

Thus 2.19 holds. Also, from (2.18) and (2.19) it follows that \([I(p^n, p^n, a)]^j\) will be of the type \(I(p^n, p^{n-1}, a)\) when \((a+\theta)^j - (a-\theta)^j = 0 \pmod{p}\). With this in mind, we would like to find a class of the type \(I(p^n, p^n, a)\) whose \([p - (\frac{d}{p})]^{th}\) power under composition is of the type \(I(p^n, p^{n-1}, \gamma)\), but no smaller power is.

Case \((\frac{d}{p}) = 1\). In this case the congruence \(x^2 = d \pmod{p}\) has a solution and thus \(x^2 = -m \pmod{p}\) is also solvable.

Let \(p\) be such an integer, i.e., \(p^2 = -m \pmod{p}\).

Select a primitive root \(\sigma\) of \(p\) with the property that \(\sigma^{p-1} \neq 1 \pmod{p^2}\), i.e., \(\sigma^{p-1} = 1 \pmod{p}\) but \(\sigma^{p-1} \neq 1 \pmod{p^2}\), see [4, p. 19]. Let
\[ \alpha_0 = \frac{\sigma + 1}{\sigma - 1} \cdot \rho \mod p , \]  
then
\[ (\alpha_0 + \rho)^{p-1} - (\alpha_0 - \rho)^{p-1} = (\frac{\sigma + 1}{\sigma - 1} \cdot \rho + \rho)^{p-1} - (\frac{\sigma + 1}{\sigma - 1} \cdot \rho - \rho)^{p-1} = 0 \mod p \]
\[ \neq 0 \mod p^2 . \]

Also, since \( \sigma \) was selected as a primitive root of \( p \), it follows that \( (\alpha_0 + \rho)^k - (\alpha_0 - \rho)^k \neq 0 \mod p \) for \( k < p-1 \). Hence \([I(p^n, p^n, \alpha_0)]^{p-1}\) is of the type \( I(p^n, p^n-1, \gamma) \) and has order \( p^{n-1} \). Further, \( (p-1) \) is the smallest power of \( I(p^n, p^n, \alpha_0) \) which has order \( p^{n-1} \), thus the order of \( I(p^n, p^n, \alpha_0) \) is \( p^{n-1}(p-1) = p^{n-1}(p - (\frac{d}{p})) \).

Case \( (\frac{d}{p}) = -1 \). In this case we need to make use of the following lemma.

**Lemma 2.17.1.** In the quadratic field \( Q(\theta) \), where \( \theta = \sqrt{-m} \), \( d = -4m \), and \( (\frac{d}{p}) = -1 \), there exist elements \( \beta \), with \( N(\beta) = 1 \), such that \( p+1 \) is the least exponent where \( \beta^{p+1} \equiv 1 \mod p \).

**Proof of lemma.** Since \( (\frac{d}{p}) = -1 \), then \( (p) \) is a prime ideal in the ring of integers \( J \) of \( Q(\theta) \). Thus \( J/(p) \) is a field containing \( p^2 \) elements, and the multiplicative group \( [J/(p) - (0)] \) is cyclic of order \( p^2 - 1 \).
Let $a$ be a generator of this group and set $\beta = a^{p-1}$.

Then $\beta$ has order $p+1$, and $N(\beta) = N(a^{p-1}) = [N(a)]^{p-1}$.

Since $(N(a), p) = 1$ Fermat's theorem gives

$$N(\beta) = [N(a)]^{p-1} \equiv 1 \pmod{p},$$

which proves the lemma.

Let $\beta$ be chosen as in the lemma above, and require that $\beta^{p+1} \not\equiv 1 \pmod{p^2}$. This can be done, since, if $\beta^{p+1} \equiv 1 \pmod{p^2}$, replacing $\beta$ with $\beta+p$ gives the desired properties. Choose $\alpha_0 \equiv \frac{\beta^{p+1}-1}{\beta-1} \cdot \Theta \pmod{p}$.

Expressing $\beta = b_0 + b_1\Theta$, where $b_0$ and $b_1$ are rational integers, we find,

$$\alpha_0 = \frac{2mb_1}{N(\beta-1)} + \frac{N(\beta)-1}{N(\beta-1)} \cdot \Theta \pmod{p}.$$

Since $N(\beta)-1 \equiv 0 \pmod{p}$, then $\alpha_0$ is a rational integer modulo $p$. This case now follows in the same manner as the previous one, i.e., we find that $I(p^m, p^n, \alpha_0)$ has order $p^{n-1}(p+1) = p^{n-1}(p - \left(\frac{d}{p}\right))$. This completes the proof of Theorem 2.17.

In the previous theorem we considered only the case where $p \nmid d$. We now remove this restriction and examine the situation of Theorem 2.17 when $p \mid d$. First, the order of the group is $p^{n-1}(p+1) = p^n$. Also, since equations (2.18) and (2.19) hold when $p \mid d$ we have,
\[ [I(p^n,p^n,1)]^j = I(p^n,p^n,y) \]

(2.20)

\[ \gamma = \frac{(1+\theta)^j + (1-\theta)^j}{(1+\theta)^j - (1-\theta)^j} \cdot \theta \pmod{p} \]

provided \((1+\theta)^j - (1-\theta)^j \neq 0 \pmod{p}\). Of particular interest is the denominator in the above expression for \(Y\) when \(j = p\). In fact, if \(j = p\) we get,

\[ \gamma = \frac{\binom{p}{0} + \binom{p}{2}(\theta)^2 + \cdots + \binom{p}{p-1}(\theta)^{p-1}}{\binom{p}{1} + \binom{p}{3}(\theta)^2 + \cdots + \binom{p}{p}(\theta)^{p-1}} \pmod{p}. \]

The denominator in this expression for \(\gamma\) is clearly congruent to zero modulo \(p\); hence, \([I(p^n,p^n,1)]^p\) will be of the type \(I(p^n,p^{n-1},y)\), except in the case

\[ \binom{p}{1} + \binom{p}{3}(\theta)^2 + \binom{p}{5}(\theta)^4 + \cdots + \binom{p}{p}(\theta)^{p-1} = 0. \]

If this happens, then

\[ p = \binom{p}{3}m - \binom{p}{5}m^2 - \cdots - \binom{p}{p-2}(-m)^{\frac{p-3}{2}} - \binom{p}{p}(-m)^{\frac{p-1}{2}}, \]

which implies that \(m \mid p\), or that \(m = p\) is the only possible solution. However, if \(m = p > 3\), then the above equation yields a non-trivial factorization of a prime. Thus, the only solution is \(m = p = 3\). In this case \([I(3^n,3^n,1)]^2 = I(3^n,3^n,-1)\) and \([I(3^n,3^n,1)]^3 = \quad = I(3^n,l,0)\), the principal class, so that \(I(3^n,3^n,1)\)
has order 3 and the group is the direct product of a cyclic group of order 3 and a cyclic group of order $3^{n-1}$. Summarizing the results of this discussion gives the following theorem:

**Theorem 2.21.** Let $d = -4m$, $m > 1$, and $p$ an odd prime such that $p | d$. Except in the case $m = p = 3$, the primitive classes of binary quadratic forms derivable from the principal class of discriminant $d$ by integral transformations of determinant $p^n$, form a cyclic group having order $p^n$. In the exceptional case $m = p = 3$, the group is the direct product of a cyclic group of order 3 and a cyclic group of order $3^{n-1}$.

Up to this point we have considered only the odd primes. If we take $p = 2$ and apply transformations of determinant 2 to $I = [1,0,m]$ with $m > 1$, the derived classes are,

- $I(2,1,0) = [1,0,4m]$
- $I(2,2,0) = [4,0,m]$
- $I(2,2,1) = [4,4,m+1]$.

In case $m$ is even, then $I(2,1,0)$ and $I(2,2,1)$ are primitive classes. If $m$ is odd, then $I(2,1,0)$ and $I(2,2,0)$ are primitive classes. Thus in either case,
the primitive derived classes form a cyclic group of order 2. If we apply integral transformations of determinant $2^n$ we find that the argument of Theorem 2.21 applies, so that the derived classes form a cyclic group having order $2^n$. Combining this with Theorems 2.17 and 2.21 we have the following:

**Theorem 2.22.** Let $d = -4m$ with $m > 1$. The group of primitive classes of binary quadratic forms derivable from the principal class of discriminant $d$ by integral transformations of determinant $p^n$ for any prime $p$, is given by one of the following:

(i) The direct product of a cyclic group of order 3 and a cyclic group of order $3^{n-1}$ in case $m = p = 3$.

(ii) A cyclic group of order $2^n$ if $p = 2$.

(iii) A cyclic group of order $p^{n-1}(p - (\frac{d}{p}))$.

Finally we consider the primitive classes of binary quadratic forms derivable from the principal class of discriminant $d$ by integral transformations of determinant $s = p_1^{e_1} \cdot p_2^{e_2} \cdots \cdot p_n^{e_n}$. Again we impose the restriction $d = -4m$ with $m > 1$. As before we will use the notation $I(s, p^k, \alpha)$ to represent the class obtained when the transformation
\[ \begin{bmatrix} p^k & a \\ s^k & pj \end{bmatrix} \] is applied to \( I = [1,0,m] \). To discover the

order of the group of primitive classes derivable from

\( I \) by transformations of determinant

\( s = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n} \), we picture first applying

to \( I \) integral transformations of determinant \( p_1^{e_1} \); then to each one of these primitive derived classes apply

integral transformations of determinant \( p_2^{e_2} \); etc.

Thus, the number of primitive classes derivable from \( I \)

by transformations of determinant \( s = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n} \)

will be,

\[ \cdot \left[ p_1^{e_1-1} \left( p_1 - \left( \frac{d}{p_1} \right) \right) \right] \cdot \left[ p_2^{e_2-1} \left( p_2 - \left( \frac{dp_1}{p_2} \right) \right) \right] \cdot \ldots \cdot \left[ p_n^{e_n-1} \left( p_n - \left( \frac{dp_1 \ldots dp_{n-1}}{p_n} \right) \right) \right] = \]

\[ \cdot \left[ p_1^{e_1-1} \left( p_1 - \left( \frac{d}{p_1} \right) \right) \right] \cdot \left[ p_2^{e_2-1} \left( p_2 - \left( \frac{d}{p_2} \right) \right) \right] \cdot \ldots \cdot \left[ p_n^{e_n-1} \left( p_n - \left( \frac{d}{p_n} \right) \right) \right]. \]

Included in the primitive classes derivable from \( I \)

by integral transformations of determinant \( s \) will be

the primitive classes of the following:
\[
\begin{align*}
\mathbb{T} - u_\theta^d \cdots \mathbb{T}_0 &= g \\
\left[ \begin{array}{cc}
1 & 0 \\
0 & 1
\end{array} \right] \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I &= \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I = (s' u_\theta^d s) I \\
\vdots \\
\mathbb{T} - u_\theta^d \cdots \mathbb{T}_0 &= a \\
\left[ \begin{array}{cc}
u_\theta^d & 0 \\
0 & 1
\end{array} \right] \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I &= \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I = (a' u_\theta^d s) I \\
\vdots \\
\mathbb{T} - \mathbb{T}_0 &= g \\
\left[ \begin{array}{cc}
u_\theta^d & 0 \\
0 & 1
\end{array} \right] \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I &= \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I = (s' \mathbb{T}_d s) I \\
\vdots \\
\mathbb{T} - \mathbb{T}_0 &= a \\
\left[ \begin{array}{cc}
u_\theta^d & 0 \\
0 & 1
\end{array} \right] \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I &= \left[ \begin{array}{cc}
u_\theta^d/s & 0 \\
0 & u_\theta
\end{array} \right] I = (a' \mathbb{T}_d s) I
\end{align*}
\]
Each $c(p_i)$ is in fact the subgroup of primitive classes derivable from the principal class of discriminant
\[ d(s/p_i^2) \] by integral transformations of determinant $p_i^{e_i}$.

Thus $c(p_i)$ has order $p_i^{e_i-1}(p_i - (d(s/p_i^2)/p_i)) = p_i^{e_i-1}(p_i - (d/p_i))$, and its structure is given by

Theorem 2.22. It is clear that if $i \neq j$,
$\mathcal{C}(p_i) \cap \mathcal{C}(p_j) = I(s,l,0)$ which is the principal class, thus we get the following theorem:

**Theorem 2.25.** Let $d = -4m$ with $m > 1$. The group of primitive classes of binary quadratic forms derivable from the principal class of discriminant $d$ by integral transformation of determinant $s = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$ is the direct product $c(p_1) \otimes c(p_2) \otimes \ldots \otimes c(p_n)$, where the groups $c(p_i)$ are given by equation 2.24.
CHAPTER III

As discussed in Chapter I we will let $C_d$ denote the group of primitive classes of binary quadratic forms having discriminant $d$. Also, with $h: C_{ds^2} \to C_d$ defined as before, we recall that the $\ker (h)$ is the group of primitive classes derivable from the principal class of discriminant $d$ by integral transformations of determinant $s$. Thus in case $d = -4m$ with $m > 1$, the structure of $\ker (h)$ is given by Theorem 2.25.

In this section we will consider the entire class group $C_d$ and again make restriction that $d = -4m$ with $m > 1$. We find that the other cases can be reduced to this case. Let $C_d$ and $C_{4d}$ denote the class groups of discriminant $d$ and $4d$ respectively, and let $h: C_{4d} \to C_d$ be the homomorphism described in Chapter I. We know that $\ker (h)$ consists of the primitive classes derived from the principal class of discriminant $d$ by integral transformations of determinant $2$. If $d \equiv 1 \pmod{4}$ it follows that $\ker (h)$ is a cyclic
group of order 1 or 3 according as $d \equiv 1$ or 5 (mod 8). Further $C_d \cong C_{4d}/\ker(h)$, thus it is sufficient to consider only the case $d \equiv 0$ (mod 4). In fact, if $d = -4$ we have $C_{-16} \rightarrow C_{-4}$ and the ker $(h)$ consists of the primitive classes derivable from the class of $[1,0,1]$ by integral transformations of determinant 2. The derived classes are those of the forms, $[1,0,4]$, $[4,0,1]$, and $[4,4,2]$. But, $[1,0,4] \sim [4,0,1]$ and $[4,4,2]$ is imprimitive, thus ker $(h)$ is trivial and $C_{-4} \cong C_{-16}$. Therefore, we need only consider the case $d = -4m$ with $m > 1$.

It is interesting to notice that if the structure of the class group $C_{d2}$ is known, then from the homomorphism $h:C_{d2} \rightarrow C_d$ we get $C_d \cong C_{d2}/\ker(h)$, with the structure of ker $(h)$ given by Theorem 2.25. From this we have the following theorem.

**Theorem 3.1.** If $d = -4m$ with $m > 1$, and the structure of $C_{d2}$ is known, then $C_d \cong C_{d2}/\ker(h)$ with the structure of ker $(h)$ given by Theorem 2.25.

At this point, I want to give a couple of results about finite abelian groups.

**Theorem 3.2.** Let $A$ and $B$ be finite abelian groups
and \( h: A \to B \), a homomorphism onto \( B \). Further, let 
\[ \{ \beta_1, \ldots, \beta_n \} \] be a set of independent elements in \( B \) and 
\[ \{ a_1, \ldots, a_n \} \] a set of elements in \( A \) such that 
\[ h(a_i) = \beta_i \] for \( i = 1, \ldots, n \) and order \( (a_i) = \text{order}(\beta_i) \) for 
\( i = 1, \ldots, n-1 \). Then, \( \{ a_1, \ldots, a_n \} \) is an independent set in \( A \).

**Proof.** If 
\[ a_1^{r_1} \cdots a_n^{r_n} = e_A, \] the identity of \( A \),
then 
\[ h(a_1^{r_1} \cdots a_n^{r_n}) = \beta_1^{r_1} \cdots \beta_n^{r_n} = e_B, \] the identity of \( B \). Since the set of \( \beta \)'s are independent, it follows that \( r_i \) is a multiple of the order of \( \beta_i \) for each \( i = 1, \ldots, n \). Also, order \( (a_i) = \text{order}(\beta_i) \) for \( i = 1, \ldots, n-1 \) so that \( r_i \) is a multiple of the order of \( a_i \) for \( i = 1, \ldots, n-1 \). It now follows that 
\[ a_n^{r_n} = e_A \] and thus \( \{ a_1, \ldots, a_n \} \) is an independent set.

**Theorem 3.3.** If \( G \) is a finite abelian group, then the structure of \( G \) is determined if the order of \( G \) is known and the structure of the subgroup of \( p \)-th powers is known, for some prime \( p \).

**Proof.** Let 
\[ G \cong (p_1^{e_1}) \otimes \cdots \otimes (p_n^{e_n}) \] be the cyclic decomposition of \( G \), where \( (p_i^{e_i}) \) denotes the cyclic group of order \( p_i^{e_i} \). The subgroup of \( p \)-th powers will
be, \( G^p \approx (p_1^e_1)^p \otimes \cdots \otimes (p_n^e_n)^p \) where we notice that
\[
(p_1^e_1) \approx (p_1^{e_1}) \text{ if } p \neq p_1 \quad \text{and} \quad (p_1^e_1) \approx (p_1^{e_1-1}) \text{ if } p = p_1.
\]
It now follows that
\[
G^p \approx (p_1^{e_1-1}) \otimes \cdots \otimes (p_k^{e_k-1}) \otimes (p_{k+1}^{e_{k+1}}) \otimes \cdots \otimes (p_n^{e_n})
\]
where we have arranged the factors so that
\( p = p_1 = \cdots = p_k \) and \( p \neq p_i \) for \( i > k \). It is now clear that knowing the order of \( G \) and the cyclic decomposition of \( G^p \) gives the cyclic decomposition of \( G \).

It should be noted that in the group \( \mathcal{C}_d \), of primitive classes of binary quadratic forms of discriminant \( d \), the classes that constitute the principal genus are the squares of the classes in \( \mathcal{C}_d \); thus, in view of Theorem 3.3 the structure of \( \mathcal{C}_d \) will be determined if and only if the structure of the principal genus is determined.

The problem now is to determine the structure of the class group \( \mathcal{C}_{ds^2} \), assuming the structure of the group \( \mathcal{C}_d \) is known. Let us consider the case of \( \mathcal{C}_{dp^2} \) for an odd prime \( p \) and of course assuming \( d = -4m \) with \( m > 1 \). If we are able to make the step from \( \mathcal{C}_d \) to \( \mathcal{C}_{dp^2} \), we can continue to add one prime at a time until
we finally reach $c_{ds^2}$.

For the moment consider the case where $c_d$ has a single class in each genus. This means that the principal genus consists of only the principal class $I$. Also, we know that the primitive classes among $I(p,1,0)$ and $I(p,p,a)$ for $a = 0,1,\ldots,p-1$, form a cyclic subgroup of $c_{dp^2}$ having order $p - (\frac{d^p}{p})$.

Case $p | d$. In this case, $c_{dp^2}$ has the same number of genera as $c_d$, and thus each genus of $c_{dp^2}$ must contain $p - (\frac{d^p}{p}) = p$ classes. This implies that the principal genus in $c_{dp^2}$ contains exactly those primitive classes derived from the principal class $I$. The principal genus of $c_{dp^2}$ is thus cyclic of order $p$.

Case $p \nmid d$. In this case $c_{dp^2}$ has twice as many genera as $c_d$, and each genus of $c_{dp^2}$ contains $p - (\frac{d^p}{p})$ classes. Let $I(p,p,a)$ denote a generator of the cyclic subgroup of primitive classes derived from $I$. Then $[I(p,p,a)]^2$ will be in the principal genus of $c_{dp^2}$ and has order $\frac{p - (\frac{d^p}{p})}{2}$. Therefore, the principal genus of $c_{dp^2}$ in this case is cyclic of order $\frac{p - (\frac{d^p}{p})}{2}$.

We have proved the following.
Theorem 3.4. If $C_d$ has a single class in each genus, then the principal genus of $C^2_{dp}$ is a cyclic group having order $p$ or $\frac{1}{2}(p - (\frac{d}{p}))$ according as $p|d$ or $p \nmid d$, where $p$ is any odd prime.

In view of the discussion following Theorem 3.3, we see that this theorem actually determines the structure of the class group $C^2_{dp}$.

Removing the restriction on the number of classes in a genus, we return to the problem of finding the structure of $C^2_{dp}$ if the structure of $C_d$ is known. We proceed to study the relation between the product, under composition, of classes in $C_d$ and the corresponding derived classes in $C^2_{dp}$.

Theorem 3.5. Let $f$ and $g$ be primitive binary quadratic forms of discriminant $d$, and $p$ any prime. Then given $\alpha$ and $\beta$, there exist $Y$ such that

$$T^\alpha \ast g^\beta = (f \ast g)^Y$$

where $T_\infty = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ and

$$T^\alpha = \begin{bmatrix} p^\alpha & 0 \\ 0 & 1 \end{bmatrix}, \; \alpha = 0, \ldots, p-1.$$

Proof. For any form $f$ we will denote the class of $f$ by $[f]$. Then using the homomorphism $h:C^2_{dp} \rightarrow C_d$ described in Chapter I we have, $h([f^\alpha \ast g^\beta]) =$
\[ h([f^T \alpha] \ast [g^T \beta]) = h([f^T \alpha]) \ast h([g^T \beta]) = [f] \ast [g] = [f \ast g]. \] Thus \([f^T \alpha \ast g^T \beta] \in h^{-1}([f \ast g]),\] from which it follows that there is a \(\gamma \in \{\omega, 0, 1, \ldots, p-1\}\) such that \(f^T \alpha \ast g^T \beta = (f \ast g)^T \gamma.\)

**Theorem 3.6.** If \([f]\) is a class in \(C_d\) with \([f^T \alpha]\), a class in \(C_{\text{dp}^2}\), then the order of \([f^T \alpha]\) is a multiple of the order of \([f]\).

**Proof.** Let \(m\) denote the order of the class \([f^T \alpha]\). Then from the homomorphism \(h:C_{\text{dp}^2} \to C_d\) we have,

\[ [I] = h([f^T \alpha]^m) = h([f^T \alpha])^m = [f]^m \] and thus \(m\) is a multiple of the order of \([f]\).

With these tools it was hoped that given the structure of \(C_d\) we could determine the structure of \(C_{\text{dp}^2}\); however, with the exception of the special case of Theorem 3.4, this remains unsolved. In view of Theorem 3.3 it seems natural to concentrate on the principal genus; and, based on the examples I have considered, I close with the following.

**Conjecture.** Let \([[f_1], \ldots, [f_n]]\) be an independent set
of generators for the principal genus of the class group \( C_d \), with \( e_i \) the order of \([f_1]\), and selected so that \( e_i | e_{i+1} \). Then there exist integral transformations \( T_1, \ldots, T_n \) of determinant \( p \) such that \([f_1 \ T_1]\) is in the principal genus of \( C_{dp^2} \) where the order of \([f_1]\) equals \( e_i \) for \( i = 1, \ldots, n-1 \) and the order of \([f_n \ T_n]\) is \( e(n(p - (d/p))) \) or \( \frac{e_n}{2} (p - (d/p)) \) according as \( p | d \) or \( p \nmid d \). This will imply that

\[
([f_1], \ldots, [f_n])
\]

is an independent set of generators for the principal genus of \( C_{dp^2} \), and thus determines the structure of \( C_{dp^2} \).
BIBLIOGRAPHY

1. Hubert S. Butts and Dennis Estes, 'Modules and Binary Quadratic Forms over Integral Domains,' Linear Algebra and its Applications, 1(1968), 153-180.

2. Hubert S. Butts and Gordon Pall, 'Modules and Binary Quadratic Forms,' Acta Arithmetica, XV(1968), 23-44.


VITA

John W. Matherne was born on December 8, 1944 in Vivian, Louisiana. He graduated from Franklinton High School, Franklinton, Louisiana in June, 1962. In the fall of 1962, he entered Louisiana State University and graduated in August, 1966 with a Bachelor of Science degree in Physics. In September, 1966, he began graduate study in the Department of Mathematics at Louisiana State University supported by a National Science Foundation Traineeship. He received the Master of Science degree in Mathematics in May, 1968.

In July, 1968, he began a two year tour of duty with the U.S. Army assigned to the U.S. Army Mobility Equipment Research and Development Center. In September, 1970, he returned to graduate school at Louisiana State University where he is now a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.
Candidate: John W. Matherne

Major Field: Mathematics

Title of Thesis: The Class Group in Binary Quadratic Orders

Approved:

Gordon Hall
Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

N.S. Beth

R.E. Anderson

H. Collins

Bernard Modrson

Date of Examination:

April 27, 1973