1965

Classes of Binary Quadratic Forms Over Polynomial Rings.

Dennis Ray Estes
Louisiana State University and Agricultural & Mechanical College

CLASSES OF BINARY QUADRATIC FORMS OVER POLYNOMIAL RINGS

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
Dennis Ray Estes
B.S., East Central State College, 1961
M.S., Louisiana State University, 1963
August, 1965

ACKNOWLEDGMENT

The author wishes to express his appreciation to Professor Gordon Pall, under whose direction this dissertation was written, for his advice and encouragement.

TABLE OF CONTENTS

CHAPTER		PAGE
	ACKNOWLEDGMENT	ii
	ABSTRACT	iv
I	INTRODUCTION AND NOTATION	1
II	IDEALS IN K_{Δ} AND THEIR ASSOCIATED BINARY QUADRATIC FORMS	7
III	DEFINITE QUADRATIC FORMS	15
IV	INDEFINITE QUADRATIC FORMS	33
V	DETERMINANTS DIFFERING BY SQUARE FACTORS.	54
	SELECTED BIBLIOGRAPHY	62
	BIOGRAPHY	63

ABSTRACT

This paper is a study of classes of primitive quadratic forms with coefficients from K[t], the domain of polynomials in the indeterminate t over a field K whose characteristic is different from 2. Two quadratic forms are said to be equivalent if there is a linear transformation with coefficients in K[t] and having determinant 1 taking one into the other. The equivalence classes of primitive binary quadratic forms having determinant $\Delta(t)$ constitute an abelian group Q_Δ. The primary concern of this paper is to obtain structure theorems pertaining to the group Q_Δ.

It is shown, in Chapter II, that to each primitive binary quadratic form having determinant $\Delta(t)$ there belongs an associated invertible ideal in $K[t,\theta]$, θ a solution of the equation $X^2 + \Delta(t)Y^2 = 0$. A necessary and sufficient condition is given for an ideal in $K[t,\theta]$ to be invertible. Two invertible ideals A, B in $K[t,\theta]$ are said to be equivalent if there are elements η, γ in $K[t,\theta]$ such that $\eta A = \gamma B$. The equivalence classes of invertible ideals form an abelian group G_Δ and the above association of ideals with quadratic forms is shown to give rise to a homomorphism from Q_Δ onto G_Δ.

to give rise to a homomorphism from Q_Δ onto

The third chapter deals with definite binary quadratic forms, the forms whose determinants have odd degree or have leading coefficient d such that $d = k^2$ for any k in K. It is shown that in every class of Q_Δ there is an essentially unique reduced form; therefore, only in special cases is the group Q_Δ finite. In order to obtain results similar to the classical case over the rational integers where such groups are finite, we restrict our attention to the elements of Q_Δ having finite order. It is shown for algebraically closed fields that the elements having order less than some positive integer are finite in number. This result exhibits a class of rings with out torsion; that is, rings which contain a prime ideal no power of which is principal.

Of concern in the fourth chapter is the study of indefinite forms, the forms having determinant $\Delta(t)$ of even degree and whose leading coefficient $d = -k^2$ for some k in K. Reduced forms are defined and shown to lie in chains in the classes of Q_Δ. The condition that such chains are periodic is shown to be equivalent to the existence of a non-trivial solution of the Pell equation $X^2 + \Delta(t)Y^2 = 1$. Examples are given for which the Pell equation has only the trivial solutions $X = \pm 1$, $Y = 0$. Necessary and sufficient conditions for the Pell equation to have a non-trivial solution are also given in terms of the number of properly ambiguous forms, forms having second

coefficient zero, in the identity class. It is shown that the properly ambiguous forms in an ambiguous class, a class having order 1 or 2, constitute a vector space over K having dimension 2 whenever the Pell equation has a non-trivial solution and 1 otherwise. The paper is concluded by studying the relationship between the groups Q_{Δ} and $Q_{p^2(t)\Delta}$, where p(t) is an irreducible polynomial in K[t].

CHAPTER I

INTRODUCTION AND NOTATION

INTRODUCTION 1.0. So much is known today about class groups of binary quadratic forms over the rational integers that it is of interest to try to extend the results to corresponding groups of quadratic forms over polynomial rings. Artin [1][1] has, in fact, made such extensions for the case of quadratic forms with polynomials over finite fields as coefficients. The purpose of this paper will be to investigate what theorems carry over for forms with coefficients from polynomial rings over arbitrary fields of characteristic not 2.

The methods used in this paper will, in general, parallel classical methods used for integral forms; however, some of the more desirable results, such as finite class number, remain valid only in special cases. Nevertheless, these groups of infinite order are of particular interest for they provide examples of domains without torsion as given in [3]. It is interesting to note how we verify these

---

[1]Pairs of numbers in brackets refer to correspondingly numbered references in Selected Bibliography and page numbers, respectively. A single number in a bracket refers to the correspondingly numbered reference in the Selected Bibliography.

examples without, as in [8], resorting to the theory of algebraic curves.

NOTATION 1.1. Throughout this work, K will denote a field whose characteristic is not 2, and K[t] will denote the set of polynomials f(t), g(t),..., in the indeterminate t with coeficients in K. Elements from K will be called constants and will be represented by lower case English letters. $|f(t)|$ will designate the degree of f(t), for $f(t) \neq 0$ and $-\infty$, for $f(t) = 0$. A binary quadratic form $F = a(t)X^2 + 2b(t)XY + c(t)Y^2$ will be represented by the symbol $[a(t), 2b(t), c(t)]$ or simply as F.

DEFINITION 1.2. A polynomial is said to be monic if its leading coefficient is 1. The greatest common divisor of a finite set of polynomials in K[t] will be the monic polynomial of largest degree which divides each member of the set. The divisor of a quadratic form $[a(t), 2b(t), c(t)]$ is defined to be the greatest common divisor of its coefficients a(t), 2b(t), c(t), and the form is called primitive if its divisor is 1. The expression $-b^2(t) + a(t)c(t)$ will denote the determinant of the form $[a(t), 2b(t), c(t)]$. If the variables of a form $F = [a(t), 2b(t), c(t)]$ undergo a linear transformation $X = r(t)X' + s(t)Y'$, $Y = u(t)X' + v(t)Y'$ then the form obtained is $F' = [a'(t), 2b'(t), c'(t)]$ where

$$a'(t) = a(t)r^2(t)+2b(t)r(t)u(t)+c(t)u^2(t)$$

$$(1)\quad b'(t) = a(t)r(t)s(t)+c(t)u(t)v(t)+b(t)\{r(t)v(t)+s(t)u(t)\}$$

$$c'(t) = a(t)s^2(t)+2b(t)s(t)v(t)+c(t)v^2(t).$$

Such a transformation will be represented by the matrix

$$T = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

and $FT = F'$ will signify that T takes F into F'. T is said to be <u>unimodular</u> if its determinant is 1. Two forms F and F' are said to be <u>equivalent</u>, written $F \sim F'$, if there is a unimodular transformation taking F into F'.

It is easily verified that the determinant and the divisor of a form F are left invariant under a unimodular transformation of F, hence the set of primitive binary quadratic forms of determinant $\Delta(t)$ is divided into classes of equivalent forms. Q_Δ will be used to denote this set of equivalence classes and {F} will represent the class containing F. It is possible, by extending the results of [6], to obtain a group structure for Q_Δ. Since the results and proofs carry over without change, we shall state, without proof, the principal results of [6]. They are the following:

<u>Gauss Criterion 1.3.</u> The forms $F = [a(t), 2b(t), c(t)]$ and $F_1 = [a_1(t), 2b_1(t), c_1(t)]$, with $a_1(t) \neq 0$, are equivalent if and only if their determinants are equal and there exist two elements r(t), u(t) in K[t] satisfying

(2) $a_1(t) = a(t)r^2(t) + 2b(t)r(t)u(t) + c(t)u^2(t)$ and

(3) $a(t)r(t) + [b(t) + b_1(t)]u(t) \equiv 0 \mod a_1(t)$

$[b(t) - b_1(t)]r(t) + c(t)u(t) \equiv 0 \mod a_1(t)$.

Indeed, if we set $-s(t) = [\{b(t) - b_1(t)\}r(t) + c(t)u(t)]/a_1(t)$ and $v(t) = [a(t)r(t) + \{b(t) + b_1(t)\}u(t)]/a_1(t)$ then

$$T = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

takes F into F_1.

Lemma 1.4. For any primitive binary quadratic forms $F_1,\ldots,F_q$ of the same determinant $\Delta(t)$, there can be found polynomials $b(t)$, $c(t)$, $a_1(t),\ldots,a_q(t)$ such that

$$F_i \sim [a_i(t),\ 2b(t),\ c(t)a_1(t)\ldots a_q(t)/a_i(t)].$$

Furthermore, these polynomials can be chosen so that $a_1(t),\ldots,a_q(t)$, and $\Delta(t)$ are coprime in pairs.

By the preceding lemma, there can be constructed within any two primitive classes $\{F\}$ and $\{F'\}$, not necessarily distinct, of binary quadratic forms of the same determinant, united forms of the type

$$(4) \qquad \begin{aligned} F_1 &= [a_1(t),\ 2b(t),\ a_2(t)c(t)] \text{ in } \{F\} \text{ and} \\ F_2 &= [a_2(t),\ 2b(t),\ a_1(t)c(t)] \text{ in } \{F'\}. \end{aligned}$$

Theorem 1.5. For all choices of united forms (4), the form $[a_1(t)a_2(t),\ 2b(t),\ c(t)]$ belongs to a unique class.

We shall interpret $\{F_1\}\{F_2\}$, the composition of $\{F_1\}$ and $\{F_2\}$, to be the class $\{[a_1(t)a_2(t),\ 2b(t),\ c(t)]\}$. It is easily seen from lemma 1.4 and theorem 1.5 that composition is a well defined, associative operation. Further, the class containing $[1,\ 0,\ \Delta(t)]$ is the identity and $\{[c(t),\ 2b(t),\ a(t)]\}$ is the inverse of $\{[a(t),\ 2b(t),\ c(t)]\}$.

Hence Q_Δ is an abelian group under composition.

Unless otherwise specified, we shall now assume that $-\Delta(t)$ is a non-constant polynomial which is not a square. Denote by K_Δ the integral domain $K[t,\theta]$, θ a solution of the equation $Y^2 + \Delta(t) = 0$.

Definitions 1.6. The conjugate, written $\overline{f(t) + g(t)\theta}$, of an element $f(t) + g(t)\,\theta$ in K_Δ is defined to be $f(t) - g(t)\theta$ and the norm, $N(f(t) + g(t)\theta)$, of $f(t) + g(t)\theta$ is defined to be $f^2(t) + g^2(t)\,\Delta(t)$. The conjugate $\overline{A}$, of an ideal in K_Δ is defined to be the ideal generated by conjugates of the elements of A, and the norm, N(A), of A is defined to be $A\overline{A}$. An ideal A of K_Δ is said to be invertible if there is an ideal B of K_Δ such that AB is principal. Two ideals A and B are said to be equivalent if there exist principal ideals (π) and (μ) such that $(\pi)A = (\mu)B$.

The invertible ideals are divided into classes of equivalent ideals which we shall denote by G_Δ. Let {A} represent the class containing the ideal A and define {A}{b}, the product of {A} and {B}, to be the class {AB}. If {A} is an element of G_Δ then A is invertible and there is an ideal A^{-1} such that AA^{-1} is principal. Thus $\{A\}\{A^{-1}\} = \{(1)\}$. It follows that G_Δ is an abelian group with {(1)} as its identity.

Using methods similar to those given by Landau in [4], we exhibit a homomorphism between the groups Q_{Δ} and G_{Δ} so that any result obtained for Q_{Δ} gives rise to a corresponding result for G_{Δ}.

CHAPTER II

IDEALS OF K_Δ AND THEIR ASSOCIATED BINARY QUADRATIC FORMS

Theorem 2.1. The proper ideals of K_Δ are those modules over $K[t]$ having a basis of the form

(1). $f(t)c(t)$, $g(t)c(t) + c(t)\theta$ where

(2). $f(t) \mid N(g(t) + \theta)$.

PROOF: A proper ideal A of K_Δ contains a nonzero element α and hence a nonzero polynomial $N(\alpha)$. Denote by $a(t)$ a nonzero polynomial in A with least degree. Since $a(t)\theta$ is in A, among the elements of A there is one of the form $b(t) + c(t)\theta$ with $c(t) \neq 0$ and $c(t)$ of least degree. Clearly the elements $a(t)$, $b(t) + c(t)\theta$ are independent over $K[t]$. For any element $r(t) + s(t)\theta$ in A choose $m(t)$, $n(t)$ such that $s(t) = m(t)c(t) + n(t)$ and $|n(t)| < |c(t)|$. We have $r(t) + s(t)\theta = m(t)(b(t) + c(t)\theta) + \{r(t) - m(t)b(t)\} + n(t)\theta$, hence $\{r(t) - m(t)b(t)\} + n(t)\theta$ is in A. Thus $n(t) = 0$. Using the same proceedure, we have $a(t) \mid r(t) - m(t)b(t)$; therefore $a(t)$, $b(t) + c(t)\theta$ is a module basis of A over $K[t]$.

Since $a(t)\theta$ and $b(t)\theta - c(t)\,\Delta(t)$ are elements of A, $c(t) \mid a(t)$ and $c(t) \mid b(t)$. Let $a(t) = c(t)f(t)$ and $b(t) = c(t)g(t)$. Also, $c(t)N(g(t) + \theta)$ is A whence $f(t) \mid N(g(t)+\theta)$.

Conversely, let A be a module over K[t] having a basis as given in (1) and (2). To prove A is an ideal in K_Δ, it is sufficient to show that the products of the basis elements of A by the basis elements 1, θ of K_Δ are elements of A. This being evident for 1 we need consider only θ. On multiplication by θ, we have

$$f(t)c(t)\theta = f(t)\{g(t)c(t) + c(t)\theta\} - g(t)f(t)c(t) \text{ and}$$

$$\{g(t)c(t) + c(t)\theta\}\theta = f(t)c(t)\{N(g(t) + \theta)/-f(t)\} + g(t)\{g(t)c(t) + c(t)\theta\}.$$

Since the above elements are evidently in A, the theorem follows.

Theorem 2.2. An ideal A of K_Δ having a basis as given in (1) and (2) of theorem 1.1 is invertible if and only if the greatest common divisor of f(t), g(t), and $N(g(t) + \theta)/f(t)$ is a constant.

PROOF: Let A' be the K[t]-module generated by f(t), g(t) + θ. By theorem 1.1, A is an ideal in K_Δ. Evidently A = (c(t))A'. If A is invertible then there is an ideal B of K_Δ such that AB is principal; therefore, A'{(c(t))B} is principal and A' is invertible. Conversely, if A'B is principal for some ideal B of K_Δ then AB is principal. Hence A is invertible if and only if A' is invertible.

Let d(t) denote the greatest common divisor of f(t) g(t), and $N(g(T) + \theta)/f(t)$. Since f(t), g(t) - θ is a module basis of $\overline{A}'$,

$$N(A') = (f(t))(f(t),\ g(t) + \theta,\ g(t) - \theta,\ N(g(t) + \theta)/f(t))$$
$$= (f(t))(f(t),\ g(t),\ N(g(t) + \theta)/f(t),\ \theta)$$
$$= (f(t))(d(t),\ \theta).$$

It follows that A' is invertible if d(t) is a constant.

Since $N(g(t) + \theta) = g^2(t) + \Delta(t),\ d^2(t) \mid \Delta(t)$ and

$$(d(t),\ \theta)^2 = (d^2(t),\ d(t)\theta,\ \Delta(t))$$
$$= (d(t))(d(t),\ \theta).$$

If A' is invertible then $(d(t),\ \theta)$ is invertible. Choose B such that $B(d(t),\ \theta)$ is principal. We have

$$B(d(t),\ \theta)(d(t),\ \theta) = (d(t))B(d(t),\ \theta), \text{ hence}$$
$$(d(t),\ \theta) = (d(t)).$$

Therefore, $\theta = d(t)\{m(t) + n(t)\theta\}$ for some m(t) and n(t) in K[t]. Equating coefficients, we have d(t) is a constant.

Corollary 2.3. If $A = (c(t))(f(t),\ g(t) + \theta)$ and A is invertible then $N(A) = (c^2(t)f(t))$.

PROOF: The corollary follows immediately from the proof of theorem 1.2.

Definition 2.4. A polynomial f(t) is said to be semiprime to a polynomial g(t) if and only if $p(t) \mid f(t)$ and $p^2(t) \mid g(t)$ implies p(t) is a constant.

Corollary 2.5. If $A = (c(t))(f(t),\ g(t) + \theta)$ is a proper ideal in K_Δ and c(t)f(t) is semiprime to $\Delta(t)$ then A is invertible and uniquely expressible as a product of a finite number of maximal ideals.

PROOF: If $d(t)$ is any common factor of $f(t)$, $N(g(t)+\theta)/f(t)$, and $\Delta(t)$ then $d(t)$ divides $f(t)$ and $d^2(t)$ divides $\Delta(t)$. Since $f(t)$ is semiprime to $\Delta(t)$, $d(t)$ is a constant. By theorem 1.2, A is invertible. The theorem being evident for A maximal we may assume A is properly contained in a maximal ideal M_1. A polynomial of least degree in M_1 must be a divisor of $c(t)f(t)$ and thus semiprime to $\Delta(t)$. From the above comment, we see that M_1 is invertible. Since M_1 contains A, $M_1\overline{M}_1$ contains $\overline{M}_1 A$. Thus $\overline{M}_1 A$ is contained in the principal ideal $(N(M_1))$. It follows that there is an ideal B_1 such that $\overline{M}_1 A = (N(M_1))B_1$. Multiplying both sides by M_1, we obtain $A = M_1 B_1$. Clearly B_1 is invertible and $N(A) = N(M_1)N(B_1)$. Since B_1 contains A, B_1 satisfies the same conditions as A, hence B_1 can be factored as $M_2 B_2$ where M_2 is maximal. The equation $N(A) = N(M_1)N(B_1)$ implies $|N(B_1)| < |N(A)|$. Thus, the process of factoring will terminate after a finite number of steps; that is, A can be expressed as a product of a finite number of maximal ideals. For uniqueness see [10;227].

Theorem 1.1 allows primitive binary quadratic forms of determinant $\Delta(t)$ to be associated with invertible ideals of K_Δ. Let $F = [f(t), 2g(t), h(t)]$ be a form of determinant $\Delta(t)$. Since $-\Delta(t)$ is not a square, $f(t) \neq 0$; hence, by theorem 1.1, $(f(t), g(t) + \theta)$ is an ideal in K_Δ. We call $(f(t), g(t) + \theta)$ the <u>associated ideal</u> of F. In view of theorem 1.2, F is primitive if and only if its

associated ideal is invertible. Define $\phi: Q_\Delta \longrightarrow G_\Delta$ by $\phi(\{F\}) = \{A\}$ where A is the associated ideal of F. We have,

Theorem 2.6. ϕ is a homomorphism of Q_Δ onto G_Δ.

PROOF: To show ϕ is well defined let $F_1 = [f_1(t), 2g_1(t), h_1(t)]$ and $F_2 = [f_2(t), 2g_2(t), h_2(t)]$ be two equivalent forms with

$$T = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

a unimodular transformation taking F_2 into F_1. By the Gauss criterion,

(1). $f_1(t)v(t) = f_2(t)r(t) + \{g_1(t) + g_2(t)\}u(t)$

(2). $-f_1(t)s(t) = \{g_2(t) - g_1(t)\}r(t) + h_2(t)u(t) =$
$\{g_2(t) - g_1(t)\}r(t) + \{g_2^2(t) + \Delta(t)\}u(t)/f_2(t).$

From (1) and (2) we have

(3). $f_2(t)f_1(t)s(t) + g_2(t)f_1(t)v(t) =$
$u(t)g_1(t)g_2(t) + u(t)\theta^2 + r(t)g_1(t)f_2(t).$

Equations (1) and (3) give

$u(t)(g_1(t) + \theta)(g_2(t) + \theta) + r(t)\, f_2(t)(g_1(t) + \theta) =$
$v(t)f_1(t)(g_2(t) + \theta) + s(t)f_1(t)f_2(t)$. Hence,

$$(4). \quad (g_1(t) + \theta)/f_1(t) = \frac{v(t)\{g_2(t)+\theta)/f_2(t)\}+s(t)}{u(t)\{(g_2(t)+\theta)/f_2(t)\}+r(t)}$$

Let $\pi = f_2(t)r(t) + (g_2(t) + \theta)u(t)$, $\mu = f_1(t)$. From (4), we have

(5). $\pi f_1(t) = \{r(t)f_2(t) + (g_2(t) + \theta)u(t)\}\mu$
$\pi(g_1(t) + \theta) = \{s(t)f_2(t) + v(t)(g_2(t) + \theta)\}\mu$.

Since the determinant of T is 1, it follows that

$$(\pi)(f_1(t),\ g_1(t) + \theta) = (\mu)(f_2(t),\ g_2(t) + \theta).$$

Therefore the associated ideals of F_1 and F_2 are equivalent.

The fact that $\emptyset$ is onto is an immediate consequence of theorems 1.1 and 1.2.

To see that $\emptyset$ preserves multiplication let $\{F_1\}$ and $\{F_2\}$ be elements of Q_Δ such that F_1 and F_2 are the united forms $[f_1(t),\ 2g_1(t),\ c_1(t)f_2(t)]$ and $[f_2(t),\ 2g_1(t),\ c_1(t)f_1(t)]$ respectively. We have $\emptyset(\{F_1\}\{F_2\}) = (f_1(t)f_2(t),\ g_1(t) + \theta)$ and $\emptyset(\{F_1\})\emptyset(\{F_2\}) = (f_1(t),\ g_1(t) + \theta)(f_2(t),\ g_1(t) + \theta)$. Clearly $\emptyset(\{F_1\}\{F_2\})$ contains $\emptyset(\{F_1\})\emptyset(\{F_2\})$. Since $(g_1(t) + \theta)^2 = 2g_1(t)(g_1(t) + \theta) - N(g_1(t) + \theta) = 2g_1(t)(g_1(t) + \theta) - f_1(t)f_2(t)\ N(g_1(t) + \theta)/f_1(t)f_2(t)$ we have $g_1(t)(g_1(t) + \theta)$, $f_1(t)(g_1(t) + \theta)$, and $f_2(t)(g_1(t) + \theta)$ are elements of $\emptyset(\{F_1\})\emptyset(\{F_2\})$. Now F_1 is primitive hence the greatest common divisor $d(t)$ of $f_1(t)$, $g_1(t)$, $f_2(t)$ is a constant. Since $d(t)$ is a linear combination of $f_1(t)$, $g_1(t)$, $f_2(t)$ with polynomials from $K[t]$, it follows that $g_1(t) + \theta$ is in $\emptyset(\{F_2\})$. Therefore $\emptyset(\{F_1\}\{F_2\}) = \emptyset(\{F_1\})\emptyset(\{F_2\})$ and $\emptyset$ is a homomorphism of Q_Δ onto G_Δ.

Theorem 2.7. If the associated ideal $A = (f(t),\ g(t) + \theta)$ of $F = [f(t),\ 2g(t),\ h(t)]$ is principal then F is equivalent to $F_k = [k,\ 0,\ \Delta(t)/k]$ for some k in K.

PROOF: If μ is a generator of A then there are elements r(t) and s(t) in K[t] such that

$$\mu = r(t)f(t) + s(t)(g(t) + \theta) \text{ and}$$

$$N(\mu) = r^2(t)f^2(t) + 2r(t)s(t)g(t)f(t) + s^2(t)N(g(t) + \theta).$$

By corollary 1.3, $N(A) = (N(\mu)) = (f(t))$. Thus $N(\mu) = kf(t)$ for some k in K and $k = r^2(t)f(t) + 2r(t)s(t)g(t) + s^2(t)N(g(t) + \theta)/f(t)$.

Choose u(t) and v(t) so that $r(t)v(t) - s(t)u(t) = 1$ and let

$$T = \begin{bmatrix} r(t), & u(t) \\ s(t), & v(t) \end{bmatrix} .$$

It follows that $FT = [k, 2g_1(t), h_1(t)]$. If

$$T_1 = \begin{bmatrix} 1, & -g_1(t)/k \\ 0, & 1 \end{bmatrix} ,$$

then TT_1 takes F into $[k, 0, \Delta(t)/k]$ completing the proof of the theorem.

If H_Δ denotes the kernel of $\emptyset$ then, by theorem 1.7, H_Δ consists of the classes $\{F_k\}$, for k in K. Hence $\emptyset$ is an isomorphism if and only if $\{F_k\} = \{F_1\}$, the identity class, for each k in K; that is, if and only if F_k is equivalent to F_1 for each k in K. It is easily verified that the equivalence of F_k and F_1 is the same as the existence of polynomials $X = u_k(t)$, $Y = v_k(t)$ satisfying the equation $X^2 + \Delta(t)Y^2 = k$. In case $|\Delta(t)|$ is odd, we have $v_k(t) = 0$ and $k = u_k^2(t)$. Thus,

Corollary 2.8. A necessary and sufficient condition for

$\emptyset$ to be an isomorphism is that the equation $X^2 + \Delta(t)Y^2 = k$ have a solution in $K[t]$. In particular for $\Delta(t)$ of odd degree, $\emptyset$ is an isomorphism if and only if every element of K is a square.

CHAPTER III

DEFINITE QUADRATIC FORMS

Definition 3.0. A binary quadratic form $[a(t), 2b(t), c(t)]$ is said to represent $f(t)$ primitively if there are relatively prime polynomials $r(t)$, $s(t)$ such that $a(t)r^2(t) + 2b(t)r(t)s(t) + c(t)s^2(t) = f(t)$.

Lemma 3.1. For any polynomial $f(t)$ primitively represented by a quadratic form F, there is a form F' equivalent to F having leading coefficient $f(t)$.

PROOF: Let $r(t)$, $s(t)$ be a primitive representation of $f(t)$ by $F = [a(t), 2b(t), c(t)]$. Since $r(t)$ and $s(t)$ are relatively prime, there exist $u(t)$, $v(t)$ in $K[t]$ such that $r(t)v(t) - s(t)u(t) = 1$. If we set

$$T = \begin{bmatrix} r(t), & u(t) \\ s(t), & v(t) \end{bmatrix},$$

then $FT = F'$ is the required form.

Lemma 3.2. Every primitive binary quadratic form having determinant $\Delta(t)$ represents primitively a non-zero polynomial of degree $\leq |\Delta(t)|/2$.

PROOF: For a primitive form F having determinant $\Delta(t)$ denote by $a(t)$ a non-zero polynomial of minimal degree represented by F. It is obvious that any representation of $a(t)$ by F is primitive hence, by lemma 3.1, there is a

form $F' = [a(t), 2b(t), c(t)]$ equivalent to F. Now $a(t)F' = [a(t)X + b(t)Y]^2 + \Delta(t)Y^2$. Choose $n(t)$ in $K[t]$ so that $|a(t)n(t) + b(t)| < |a(t)|$ and let $X = n(t)$, $Y = 1$. Then $g(t) = [[a(t)n(t) + b(t)]^2 + \Delta(t)]/a(t)$ is a non-zero polynomial represented by F'. Since any polynomial represented by F' must also be represented by F, we have

$$2|a(t)| \leq \max\{2|a(t)n(t) + b(t)|, |\Delta(t)|\} = |\Delta(t)|.$$

Corollary 3.3. Let K^* denote the multiplicative group of K. Then, for $\Delta(t)$ of degree one, Q_Δ is isomorphic to K^*/K^{*2}.

PROOF: By lemmas 3.1 and 3.2, a class $\{F\}$ contains a form $[k, 2b(t), c(t)]$ for some k in K. Define $\psi : Q \longrightarrow K^*/K^{*2}$ by $\psi(\{F\}) = k$. The fact that ψ is an isomorphism follows from the proofs of theorem 1.7 and corollary 1.8.

Corollary 3.4. If K is a finite field then Q_Δ is finite.

PROOF: By lemmas 3.1 and 3.2, there are in each class forms $F = [a(t), 2b(t), c(t)]$ with $|a(t)| \leq |\Delta(t)|/2$. Choose $n(t)$ so that $|b(t) + n(t)a(t)| < |a(t)|$ and let

$$T = \begin{bmatrix} 1, & n(t) \\ 0, & 1 \end{bmatrix}.$$

Then $FT = [a(t), 2b'(t), c'(t)]$ satisfies

$$(1) \quad |b'(t)| < |a(t)| \leq |\Delta(t)|/2.$$

Since K is finite there are at most a finite number of polynomials satisfying (1). Hence Q_Δ is a finite group.

Denote by sg[f(t)] the leading coefficient of a polynomial f(t) and set

$$\chi(\Delta) = \begin{cases} 1 \text{ if } |\Delta(t)| \text{ is even and } -sg[\Delta] \text{ is a square,} \\ 0 \text{ if } \Delta(t) = 0, \text{ and} \\ -1 \text{ otherwise.} \end{cases}$$

Definition 3.5. A binary quadratic form having determinant $\Delta(t)$ is said to be definite (indefinite) if $\chi(\Delta) = -1 (\chi(\Delta) = 1)$.

Definition 3.6. A definite binary quadratic form $F = [a(t), 2b(t), c(t)]$ having determinant $\Delta(t)$ is said to be reduced if

$$(2) \quad |b(t)| < |a(t)| \leq |\Delta(t)|/2.$$

We say that F is properly (improperly) reduced if (2) holds with inequality (equality).

If F is properly reduced, then the forms FT_k,

$$T_k = \begin{bmatrix} k, & 0 \\ 0, & 1/k \end{bmatrix}$$

for k a non-zero constant in K, are properly reduced forms equivalent to F. For F improperly reduced, $sg[a(t)]sg[c(t)] = sg[\Delta]$, hence for r, s in K with not both r and s zero, $sg[a(t)]r^2 + sg[a(t)]s^2 \neq 0$ It is easy to verify that the forms $FT_{r,s}$,

$$T_{r,s} = \begin{bmatrix} r, & -sg[c(t)]s/(sg[a(t)]r^2 + sg[c(t)]s^2) \\ s, & sg[a(t)]r/(sg[a(t)]r^2 + sg[c(t)]s^2) \end{bmatrix}$$

are improperly reduced forms equivalent to F. We now show that these are exactly the reduced forms equivalent to F.

Theorem 3.7. In every class of Q_Δ, $\chi(\Delta) = -1$, there is a reduced form F. Moreover, if F is properly(improperly) reduced and F' is any reduced form equivalent to F then F' is properly(improperly) reduced and there exists $k \neq 0$ in K(r, s, with not both r and s zero, in K) such that $F' = FT_k$ ($F' = FT_{r,s}$).

PROOF: The proof of the first statement is identical to (1) of corollary 3.4. To verify the second statement, let

$$T = \begin{bmatrix} r(t), & u(t) \\ s(t), & v(t) \end{bmatrix}$$

be a unimodular transformation taking $F = [a(t), 2b(t), c(t)]$ into $F' = [a'(t), 2b'(t), c'(t)]$. By the Gauss criterion, we have

(3) $a'(t) = a(t)r^2(t) + 2b(t)r(t)s(t) + c(t)s^2(t)$ and

(4) $$\begin{aligned} a'(t)v(t) &= a(t)r(t) + [b(t) + b'(t)]s(t), \\ -a(t)u(t) &= [b(t) - b'(t)]r(t) + c(t)s(t). \end{aligned}$$

We now consider the case in which F is properly reduced. Completing squares in (3), we obtain

(5) $a'(t) = [[a(t)r(t) + b(t)s(t)]^2 + \Delta(t)s^2(t)]/a(t)$.

Hence $|a'(t)| = |m^2(t) + \Delta(t)s^2(t)| - |a(t)|$, $m(t) = a(t)r(t) + b(t)s(t)$; therefore, $|\Delta(t)| > |a'(t)| + |a(t)| =$

$|m^2(t) + \Delta(t)s^2(t)|$. Since the coefficient of t $|\Delta(t)| + 2|s(t)|$ in $m^2(t) + \Delta(t)s^2(t)$ cannot vanish unless $s(t) = 0$, it follows that $s(t) = 0$ and $a'(t) = a(t)r^2(t)$. Now

$$T^{-1} = \begin{bmatrix} v(t), & -u(t) \\ -s(t), & r(t) \end{bmatrix}$$

takes F' into F, hence $a(t) = a'(t)v^2(t)$ and we deduce that $r(t)$ is a constant. If we set $r(t) = k$, then $a'(t) = a(t)k^2$ and $|a(t)| = |a'(t)|$. Thus F' is also properly reduced. Equating degrees in the last equation of (4), we see that $|a'(t)| + |u(t)| = |b(t) - b'(t)| \leq \max\{|b(t)|, |b'(t)|\}$. Since $|a'(t)|$ exceeds both $|b(t)|$ and $|b'(t)|$, it follows that $u(t) = 0$, whence $T = T_k$.

Assume now that F is improperly reduced. Since T^{-1} takes F' into F, it follows from the preceeding proof that F' must be improperly reduced. From (5), we have $|\Delta(t)| \geq |a'(t)| + |a(t)| = |m^2(t) + \Delta(t)s^2(t)|$, thus $s(t)$ is a constant. Comparing degrees in equation (3) and (4) and noticing that $|a(t)| = |c(t)|$, we see that $r(t)$, $u(t)$, and $v(t)$ are constants. Set $r(t) = r$, $s(t) = s$, $u(t) = u$, and $v(t) = v$. Hence, from (3) and (4), we have $v = sg[a(t)]r/sg[a'(t)]$, $u = -sg[c(t)]s/sg[a'(t)]$, and

$$sg[a'(t)] = sg[a(t)r^2 + sg[c(t)]s^2.$$

This concludes the proof of the theorem.

Corollary 3.8. If $K^{*2} = K^*$ then Q_{Δ} is infinite for $\Delta(t)$ of odd degree greater than one.

PROOF: The forms $F_a = [t-a, 2b, \{\Delta(t) + b^2\}/(t-a)]$, where $b^2 = -\Delta(a)$ and $\Delta(a) \neq 0$, are reduced and primitive. By theorem 3.7, the classes $\{F_a\}$ are distinct for distinct values of a. The condition $K^{*2} = K^*$ implies K is infinite, hence there are an infinite number of values a in K for which $\Delta(a) \neq 0$; therefore, there are an infinite number of distinct classes $\{F_a\}$ in Q_{Δ}.

Lemma 3.9. A primitive binary quadratic form represents primitively polynomials prime to any given polynomial.

PROOF: Let $F = [a(t), 2b(t), c(t)]$ be a primitive form and $f(t)$ be any given polynomial. Suppose $f(t) = \prod_{i=1}^{n} p_i^{e_i}(t)$ is a factorization of $f(t)$ into powers of irreducible polynomials $p_i(t)$. Let $X_i = 1$, $Y_i = 0$ whenever $(a(t), p_i(t)) = 1$; $X_i = 0$, $Y_i = 1$ whenever $(a(t), p_i(t)) = p_i(t)$ and $(c(t), p_i(t)) = 1$; and $X_i = 1$, $Y_i = 1$ whenever $(a(t), c(t) = p_i(t)$. Since F is primitive, $a(t)X_i^2 + 2b(t)X_iY_i + c(t)Y_i^2$ is prime to $p_i(t)$. By the Chinese remainder theorem, there are polynomials $r(t)$, $s(t)$ such that $r(t) \equiv X_i \bmod p_i^{e_i}(t)$ and $s(t) \equiv Y_i \bmod p_i^{e_i}(t)$, $i = 1,\ldots,n$. Hence $r(t)/(r(t),s(t))$, $s(t)/(r(t), s(t))$ is a primitive representation of a polynomial prime to $f(t)$.

Definition 3.10. A class $\{F\}$ of Q_Δ is said to be prime if F represents an irreducible polynomial.

Lemma 3.11. Every class of Q_Δ is the product of prime classes.

PROOF: Let $\{F\}$ be any class of Q_Δ. By lemma 3.9, F represents primitively a polynomial $a(t)$ prime to $\Delta(t)$. If $|a(t)| = 0$, then there exist k in K such that $F \sim F_k = [k, 0, \Delta(t)/k]$. It is evident that F_k represents primitive non-constant polynomials prime to $\Delta(t)$, thus we may assume $|a(t)| > 0$. Let $F' = [a(t), 2b(t), c(t)]$ be a form equivalent to F with leading coefficient $a(t)$ and let $a(t) = \prod_{i=1}^{n} p_i^{e_i}(t)$ be a factorization of $a(t)$ into powers of irreducible polynomials. Since the united forms $F_i = [p_i(t), 2b(t), c(t)p_1^{e_1}(t)\ldots p_n^{e_n}(t)/p_i(t)$ are each primitive, $\prod_{i=n}^{n} \{F_i\}^{e_i}$ is a factorization of $\{F'\} = \{F\}$ into prime classes.

Lemma 3.12. Let $h(t)$, $f(t)$, $a(t)$ be polynomials in $K[t]$ such that $(f(t), a(t)) = 1$ and $h(t) \equiv f^2(t) \bmod a(t)$. The congruence $h(t) \equiv [\sum_{i=0}^{n-1} X_i a^i(t)]^2 \bmod a^n(t)$ has a solution $X_i = f_i(t)$ with $f_0(t) \equiv f(t) \bmod a(t)$. Furthermore, $f_i(t)$ may be chosen so that $|f_i(t)| < |a(t)|$, $i = 0,\ldots,n-1$.

PROOF: Let $X_0 = f(t)$ and assume the existence of polynomials $X_i = f_i(t)$, $1 \le i \le j$, such that $h(t) \equiv$

$[\sum_{i=0}^{j-1} X_i a^i(t)]^2$. If we set $g(t) = \{h(t) - [\sum_{i=0}^{j-1} X_i a^i(t)]^2\}/a^j(t)$, then $h(t) - [\sum_{i=0}^{j} X_i a^i(t)]^2 \equiv g(t)a^j(t) - 2X_jX_0a^j(t) \mod a^{j+1}(t)$. Since $X_0 = f(t)$ is prime to $a(t)$, there exists $X_j = f_j(t)$ such that $2X_jX_0 \equiv g(t) \mod a(t)$. Thus, $h(t) \equiv [\sum_{i=0}^{j} f_i(t)\, a^i(t)]^2 \mod a^{j+1}(t)$. By induction, the congruence has a solution for any positive integer n. The fact that $f_i(t)$ may be chosen so that $|f_i(t)| < |a(t)|$ is an immediate consequence of the preceding statements.

Theorem 3.13. If K is algebraically closed then every class of Q_Δ is a square.

PROOF: In view of lemma 3.11, it is sufficient to show that the classes $\{c(t-a), 2b, (\Delta(t) + b^2)/c(t-a)]$, where $b^2 = -\Delta(a)$ and $\Delta(a) \neq 0$, are squares. Let $\Delta(t) = sg[\Delta] \prod_{i=1}^{n} (t-d_i)^{e_i}$ be a factorization of $\Delta(t)$ in K[t]. Since $c(d_i-a) = r_i^2$ for some r_i in K, and $c(t-a) \equiv r_i^2 \mod t-d_i$, it follows from lemma 3.12 that there exist polynomials $u_i(t)$, $i = 1,\ldots,n$, such that $c(t-a) \equiv u_i^2(t) \mod (t-d_i)^{e_i}$. By the Chinese remainder theorem, there is a polynomial u(t) such that $c(t-a) \equiv u^2(t) \mod \Delta(t)$. Let $u^2(t) + v(t)\,\Delta(t) = c(t-a)$. Then $[-\Delta(t), 2u(t), v(t)]$ is a primitive form having determinant $-c(t-a)$. By corollary 3.3, $Q_{-c(t-a)}$ contains only the identity class $\{1, 0, -c(t-a)]\}$, hence $[-\Delta(t), 2u(t), v(t)] \sim [1, 0, -c(t-a)]$. Let

$$T = \begin{bmatrix} r(t), & m(t) \\ s(t), & n(t) \end{bmatrix}$$

be a unimodular transformation taking the second form into the first. We have $r^2(t) - c(t-a)s^2(t) = -\Delta(t)$, hence $[c(t-a) \pm 2r(t), s^2(t)]$ and $[c(t-a)s(t), \pm 2r(t), s(t)]$ are primitive forms having determinant $\Delta(t)$. Since $\{[c(t-a), \pm 2r(t), s^2(t)]\} = \{[c(t-a)s(t), \pm 2r(t), s(t)]\}^2$, it suffices to show $[c(t-a), 2b, (\Delta(t) + b^2)/c(t-a)]$ is equivalent to one of the two forms $[c(t-a), \pm 2r(t), s^2(t)]$. By a translation, we may assume $r(t)$ is reduced modulo $c(t-a)$; thus, $r(t)$ is some constant r in K. Now $-\Delta(a) \equiv r^2 \equiv b^2 \bmod c(t-a)$. Hence $b = r$ or $-r$ and, by choice of sign, $[c(t-a), 2b, (\Delta(t) + b^2)/c(t-a)]$ is equivalent to one of the forms $[c(t-a), \pm 2r(t), s^2(t)]$.

Corollary 3.14. If K is algebraically closed, $\Delta(t)$ has odd degree greater than one and is not a power of a linear polynomial, then there are elements of Q_Δ of order 2^n, n any positive integer.

PROOF: If $t-a$ is a linear polynomial such that $(t-a)^n$ exactly divides $\Delta(t)$, then the form $[(t-a)^n, 0, \Delta(t)/(t-a)^n]$ is primitive and has determinant $\Delta(t)$. Since $[(t-a)^n, 0, \Delta(t)/(t-a)^n]$ and $[\Delta(t)/(t-a)^n, 0, (t-a)^n]$ are equivalent forms, the class $\{F_1\} = \{[(t-a)^n, 0, \Delta(t)/(t-a)^n]\}$ has order ≤ 2. Now $\Delta(t)$ has odd degree > 1, hence $n < |\Delta(t)|/2$ or $|\Delta(t)| - n < |\Delta(t)|/2$. It follows that one of the above forms is reduced. By

theorem 3.7, $\{F_1\} \neq \{F_0 = [1, 0, \Delta(t)]\}$, hence $\{F_1\}$ has order 2. Now suppose $\{F_n\}$ is a class having order 2^n, $n \geq 1$. By theorem 3.13, there is a class $\{F_{n+1}\}$ such that $\{F_{n+1}\}^2 = \{F_n\}$. It is apparent that the order of $\{F_{n+1}\}$ is a divisor, 2^j, of 2^{n+1}. Since $\{F_n\}^{2^{j-1}} = \{F_{n+1}\}^{2^j} = \{F_0\}$, 2^n divides 2^{j-1}. Hence $j = n+1$ and the corollary follows by induction.

Corollary 3.15. Given the same hypothesis as that of corollary 3.14, the prime classes do not have bounded orders.

PROOF: Let $\{F_n\}$ be a class of Q_Δ having order 2^n and $\prod_{i=1}^{m} \{P_i\}^{e_i}$ be a factorization of $\{F_n\}$ into prime classes. Let p_i denote the order of $\{P_i\}$ and p be the least common multiple of the set of p_i, $i = 1,\ldots,m$. Since $\{F_n\}^p$ is the identity class, 2^n divides p. It follows that at least one p_i must be divisible by 2^n.

Definition 3.16. For η in $K(t, \theta)$ define $d\eta/dt$, the derivative of η with respect to t, to be $-f'_t(t,\eta)/f'_y(t,\eta)$, where $f(t,y)$ is the irreducible polynomial η satisfies over $K(t)$ and $f'_t(t,y)$, $f'_y(t,y)$ denote the partial derivatives of $f(t,y)$ with respect to t and y.

It is shown in [9] that the usual rules for sums, products, and quotients hold for $d\eta/dt$. In particular, if the i-th derivative of η is denoted by $\eta^{(i)}$ then $\theta^{(i)} = d_i(t)/\theta^{2i-1}$ where $d_i(t)$ is a polynomial in $K[t]$. Let $\theta(a)$

denote a solution of the equation $Y^2 + \Delta(a) = 0$, for a in K, and let $\theta(a)^{(i)} = d_i(a)/\theta(a)^{2i-1}$ whenever $\Delta(a) \neq 0$.

Lemma 3.17. If A is an ideal in K_Δ and η is an element of A^n, $n \geq 2$, then $\Delta(t)d\eta/dt$ is in A^{n-1}.

PROOF: A has a module basis over K[t] of the form $a(t)c(t)$, $b(t)c(t) + c(t)\theta$, hence A^n is generated by $c^n(t)a^i(t)(b(t) + \theta)^j$, $i+j = n$. For η in A^n, there are polynomials $r_{ij}(t)$ such that

$$\eta = \sum_{i,j=0}^{n} r_{ij}(t)c^n(t)a^i(t)(b(t) + \theta)^j.$$

Since the derivatives of the terms appearing on the right, when multiplied by $\Delta(t)$, are elements of A^{n-1}, $\Delta(t)d\eta/dt$ is in A^{n-1}.

Lemma 3.18. If $\theta(a)$ is an element and K and $\Delta(a) \neq 0$ then

$$-\Delta(t) \equiv [\sum_{i=0}^{n-1} \theta(a)^{(i)}(t-a)^i/i!]^2 \bmod (t-a)^n.$$

PROOF: By lemma 3.12, there are constants $c_0, \ldots, c_{n-1}$, with $c_0 = \theta(a)$, in K such that $-\Delta(t) \equiv [\sum_{i=0}^{n-1} c_i(t-a)^i]^2 \bmod (t-a)^n$.

Let P be the ideal in K_Δ generated by $t-a$, $-\theta(a) + \theta$. It is clear that P is a prime ideal in K_Δ and $P\overline{P} = (t-a)$. Now $-\Delta(t) - [\sum_{i=0}^{n-1} c_i(t-a)^i]^2$ has for factors, $\eta =$

$\theta - \sum_{i=0}^{n-1} c_i(t-a)^i$ and $\eta' = \sum_{i=0}^{n-1} c_i(t-a)^i + \theta$. Since $c_0 = \theta(a)$, η' is prime to P, hence η is in P^n. By lemma 3.17, $\Delta^i(t)\eta^{(i)}$ is an element of P^{n-i}, $1 \leq n-i \leq n$. We have

$$-\Delta^i(t)\eta^{(i)} \equiv \Delta^i(t)\theta^{(i)} - \Delta^i(t)i!c_i \equiv$$
$$(-1)^i d_i(t)\theta - \Delta^i(t)i!c_i \equiv$$
$$(-1)^i d_i(t)(-\theta(a)+\theta)+(-1)^i d_i(t)\theta(a) - \Delta^i(t)i!c_i$$

modulo P. Thus $(-1)^i d_i(t)\theta(a) - \Delta^i(t)i!c_i$ is divisible by P, hence is in (t-a). It follows that $(-1)^i d_i(a)\theta(a) - \Delta^i(a)i!c_i = 0$, therefore $c_i = (-1)^i d_i(a)\theta(a)/\Delta^i(a)i! = d_i(a)/i!\theta(a)^{2i-1} = \theta(a)^{(i)}/i!$.

Lemma 3.19. Let $-\Delta(t) \equiv f^2(t) \bmod p(t)$ where $p(t)$ is an irreducible polynomial in $K[t]$ prime to $\Delta(t)$. The class $\{[p(t), 2f(t), g(t)]\}$, $-f^2(t) + g(t)p(t) = \Delta(t)$, has order q if and only if q is the least positive integer for which the form $[1, 0, \Delta(t)]$ primitively represents $p^q(t)$.

PROOF: The hypothesis of the lemma implies the existence of polynomials $g_0(t),\ldots,g_{n-1}(t)$, $g_0(t) \equiv f(t) \bmod p(t)$, such that $-\Delta(t) \equiv [\sum_{i=0}^{n-1} g_i(t)p^i(t)]^2 = u^2(t) \bmod p^n(t)$. Since the forms $[p(t), 2f(t), g(t)]$ and $[p(t), 2u(t), v(t)p^{n-1}(t)]$, $-u^2(t) + p^n(t)v(t) = \Delta(t)$, are equivalent, we have

$\{[p^n(t), 2u(t), v(t)]\} = \{[p(t), 2u(t), v(t)p^{n-1}(t)]\}^n = \{[p(t), 2f(t), g(t)]\}^n$.

If $\{[p(t), 2f(t), g(t)]\}$ has order q then $\{p^q(t), 2u(t), v(t)]\} = \{[1, 0, \Delta(t)]\}$. Evidently, the equivalence of $[p^q(t), 2u(t), v(t)]$ and $[1, 0, \Delta(t)]$ implies $p^q(t)$ is primitively represented by $[1, 0, \Delta(t)]$.

Conversely, assume $p^k(t)$ to be primitively represented by $[1, 0, \Delta(t)]$. By lemma 3.1, there is a form $[p^k(t), 2b(t), c(t)]$ equivalent to $[1, 0, \Delta(t)]$. Since $\{[p(t), \pm 2b(t), c(t)p^{k-1}(t)]\}^k = \{[p^k(t), \pm 2b(t), c(t)]\} = \{[1, 0, \Delta(t)]\}$, the classes $\{[p(t), \pm 2b(t), c(t)p^{k-1}(t)]\}$ have orders which divide k. From the condition $b^2(t) \equiv f^2(t) \bmod p(t)$, $b(t) \equiv f(t) \bmod p(t)$ or $b(t) \equiv -f(t) \bmod p(t)$. It follows that $[p(t), f(t), g(t)]$ is equivalent to one of the forms $[p(t), \pm 2b(t), c(t)p^{k-1}(t)]$; therefore, the order of $\{[p(t), 2f(t), g(t)]\}$ is a divisor of k. Thus $\{[p(t), 2f(t), g(t)]\}$ has order q, the least integer for which $[1, 0, \Delta(t)]$ primitively represents $p^q(t)$.

Remark 3.20. If $r^2(t) + \Delta(t)s^2(t) = p^h(t)$ and $q = h|p(t)|$, then for $\Delta(t)$ of odd degree

$q \geq |\Delta(t)|$, $|r(t)| = q/2$, and $2|s(t)| < q - |\Delta(t)|$ whenever q is even,

$q \geq |\Delta(t)|$, $|r(t)| < q/2$, and $2|s(t)| = q - |\Delta(t)|$ whenever q is odd.

Theorem 3.21. Let $\Delta(t) = 2r+1$ with $r > 0$ and $\theta(a) \neq 0$ be in K. For the prime class $\{[t-a, 2\theta(a), \{\Delta(t) - \Delta(a)\}/(t-a)]\}$ to have order $2n+\epsilon$, $\epsilon = 0$ or 1, it is necessary

for the equations

$$(7)\qquad \sum_{j+k=i} c_k X_j = 0, \text{ where } c_k = \theta(a)^{(k)}/k!,$$
$$i = n+1,\ldots,q-1, \text{ and } j = 0,\ldots,n+\epsilon-r-1,$$

to have a non-trivial solution in K. Moreover, the order of the prime class is $\leq 2q$ whenever such solutions exist.

PROOF: Assume $[[t-a, 2\theta(a), \{\Delta(t) - \Delta(a)\}/(t-a)]]$ has order q and let u(t), v(t) be a primitive representation of $(t-a)^q$. From (6), we have $q \geq n$, $|\Delta(t)|$, $|v(t)| \leq n+\epsilon-r-1$, and $|u(t)| \leq n$. Let $u(t) = \sum_{i=0}^{n} u_i(t-a)^i$, $u_i = 0$ for $i > |u(t)|$; $v(t) = \sum_{i=0}^{n+\epsilon-r-1} v_i(t-a)^i$, $v_i = 0$ for $i > |v(t)|$; and $\Delta_{q,a} = \sum_{i=0}^{q-1} c_i(t-a)^i$. We have $u^2(t) + v^2(t)\Delta(t) \equiv u^2(t) - v^2(t)\Delta_{q,a}^2 \equiv 0 \bmod (t-a)^q$. It follows that one of the factors $u(t) - v(t)\Delta_{q-a}$ or $u(t) + v(t)\Delta_{q-a}$ is divisible by $(t-a)^q$. By changing the sign of v(t), we may assume $u(t) - v(t)\Delta_{q-a} \equiv 0 \bmod (t-a)^q$. Thus

$$u_i = \sum_{j+k=i} c_k v_j, \; i = 0,\ldots,n, \text{ and}$$

$$\sum_{j+k=i} c_k v_j = 0, \; i = n+1,\ldots,q-1, \; j = 0,\ldots,n+\epsilon-r-1.$$

Since $v(t) \neq 0$, the equations given in (7) have a non-trivial solution in K.

Now assume $v_0,\ldots,v_{n+\epsilon-r-1}$ to be a non-trivial solution of (7) and let $u_i = \sum_{j+k=i} c_k v_j$, $i = 0,\ldots,n$. If we set $u(t) = \sum_{i=0}^{n} u_i(t-a)^i$ and $v(t) = \sum_{i=0}^{n+\epsilon-r-1} v_i(t-a)^i$ then

$u(t) - v(t)\Delta_{q,a} \equiv 0 \bmod (t-a)^q$. Hence

$u^2(t) - v^2(t)\Delta_{q,a} \equiv u^2(t) + v^2(t)\Delta(t) \equiv 0 \bmod (t-a)^q$. Let $u^2(t) + v^2(t)\,\Delta(t) = c(t)(t-a)^q$. Since $|u^2(t) + v^2(t)\Delta(t)|$ cannot exceed q, c(t) is some constant c in K. Set $(u(t), v(t)) = (t-a)^s$. Since $v_i \neq 0$ for some $0 \leq i \leq n+\epsilon-r-1$, $v(t) \neq 0$ whence $s \leq |v(t)| < q/2$. Thus $u(t)/(t-a)^s$, $v(t)/(t-a)^s$ is a primitive representation of $c(t-a)^{q-2s}$ by $[1, 0, \Delta(t)]$. By lemma 3.19, the order of $\{[c(t-a), 2\theta(a), \{\Delta(t) - \Delta(a)\}/c(t-a)]\}$ is a divisor of q-2s. Since $\{[c, 0, \Delta(t)/c]\}$ has order a divisor of 2, $\{[(t-a), 2\theta(a), \{\Delta(t) - \Delta(a)\}/(t-a)]\}$ has order less than or equal to 2q.

Let $\Delta(t)$ be a polynomial of odd degree in K[t], K' a field containing K, and Q'_Δ the class group of primitive binary quadratic forms over K'[t] having determinant $\Delta(t)$. If F is any primitive form over K[t] then F is primitive with respect to K'[t]; therefore, for each class {F} of Q_Δ there is a corresponding class $\{F\}' = \emptyset\{F\}$ in Q'_Δ.

Lemma 3.22. $\emptyset$ is a homomorphism of Q_Δ into Q'_Δ with kernel $H_\emptyset$, the classes $\{[c, 0, \Delta(t)/c]\}$ such that c is a square in K'.

PROOF: Since $\emptyset$ is evidently a homomorphism, we need only show that $H_\emptyset$ is the kernel of $\emptyset$. Suppose $\emptyset\{F\} = \{[1, 0, \Delta(t)]\}'$ the identity of Q'_Δ, and let F_1 be a

reduced form in $\{F\}$. Now F_1 is, by definition, reduced with respect to $K'[t]$ hence F_1 and $[1, 0, \Delta(t)]$ are two reduced forms in $\phi\{F\}$. By theorem 3.7, the leading coefficient of F_1 must be a square in K'. Thus $F_1 \sim [c, 0, \Delta(t)/c]$ for some c in K which is a square in K'. Conversely, the forms $[k^2, 0, \Delta(t)/k^2]$ and $[1, 0, \Delta(t)]$ are equivalent for each k in K'. Thus H_ϕ is the kernel of ϕ.

Theorem 3.23. Let $\Delta(t)$ be a polynomial of degree $2r+1$, $r > 0$, which is not a power of a linear polynomial in $K[t]$. The number of prime classes $\{t-a, 2\theta(a), \{\Delta(t) - \Delta(a)\}/(t-a)]\}$, with $\theta(a)$ in K, having order $q = 2n+\epsilon$, $\epsilon = 0$ or 1, is finite.

PROOF: In view of lemma 3.22, it is sufficient to prove the theorem for K algebraically closed. From theorem 3.7, none of the above prime classes have order 1 and have order 2 if and only if $t-a$ exactly divides $\Delta(t)$. Hence we may assume $q > 2$.

Since the equations (7) must have a non-trivial solution in K whenever $\{[t-a, 2\theta(a), \{\Delta(t) - \Delta(a)\}/(t-a)]\}$ has order q, it follows that the rank of the coefficient matrix

$$A_a = \left(\theta(a)^{(i+j)}/(i+j)!\right), \text{ where}$$

$j = 1, \ldots, n+\epsilon-1$ and $i = r+1-\epsilon, \ldots, n$,

is less than $m = n-r+\epsilon$, the number of columns of A_a. Hence all the minor determinants of A_a having order m

must be zero. Let $A_{j,a}$, $j = 1,\ldots,s$, denote the minor determinants of A_a having order m. Substituting $d_i(a)/\theta(a)^{2i-1}$ for $\theta(a)^{(i)}$, we have $\theta(a)\, A_{j,a} = f_j(a)/c_j \Delta^{e_j}(a)$ where $f_j(t)$ is a polynomial in K[t] independent of the choice of a and c_j, e_j are rational integers. Hence the rank of A_a is less than m whenever $f_j(a) = 0$, $1 \leq j \leq s$. Since a non-zero polynomial can have at most a finite number of roots in K, the theorem will follow if we can exhibit a j for which $f_j(t)$ is not identically zero. If we assume $f_j(t)$ to be identically zero for $1 \leq j \leq s$, then the rank of A_a is less than m for each a in K such that $\Delta(a) \neq 0$. Thus the equation (7) have a non-trivial solution for each a in K such that $\Delta(a) \neq 0$. From theorem 3.21, the order of $\{[t-a,\ 2\theta(a),\ \{\Delta(t) - \Delta(a)\}/(t-a)]\}$ is $\leq 2q$. Hence the prime classes have bounded orders and we have obtained a contradiction of corollary 3.15.

Corollary 3.24. Let the hypothesis be the same as given in theorem 3.22. If K is algebraically closed and uncountable then the number of prime classes having infinite order is uncountable.

PROOF: Since the forms $[t-a,\ 2\theta(a),\ \{\Delta(t) - \Delta(a)\}/(t-a)]$ are reduced, they are in distinct prime classes of Q_Δ. Therefore, the number of prime classes in Q_Δ is uncountable. By theorem 3.23, there are at most a countable

number of prime classes having finite order; therefore, the number of prime classes having infinite order is uncountable.

CHAPTER IV

INDEFINITE QUADRATIC FORMS

Lemma 4.0. If $\chi(\Delta) = 1$ then there is a polynomial $u(t)$, unique except for sign, such that $|u^2(t) + \Delta(t)| < |\Delta(t)|/2$.

PROOF: Let $\Delta(t) = \sum_{i=0}^{2k}{}' d_i t^i$ and consider the equations

$$X_k^2 = -d_{2k}$$

$$X_k X_{k-1} + X_{k-1} X_k = -d_{2k-1}$$

$$X_k X_0 + X_{k-1} X_1 + \ldots\ldots + X_0 X_k = -d_k.$$

Since $-d_{2k}$ is a square, the equations have a solution $u_0, \ldots, u_k$ in K. It is apparent that $u(t) = \sum_{i=0}^{k}{}' u_i t^i$ satisfies the condition $|u^2(t) + \Delta(t)| < k$. If $v(t)$ is any polynomial such that $|v^2(t) + \Delta(t)| < k$, then $|u^2(t) - v^2(t)| = |u(t) + v(t)| + |u(t) - v(t)| < k$. Now $|u(t)| = |v(t)| = k$, hence $|u(t) + v(t)| = k$ or $|u(t) - v(t)| = k$. Thus $v(t) = \pm u(t)$.

Notation 4.1. Denote by $D(t)$ a polynomial satisfying the condition $|D^2(t) + \Delta(t)| < |\Delta(t)|/2$.

Definition 4.2. A form $[a(t), 2b(t), c(t)]$ having determinant $\Delta(t), \chi(\Delta) = 1$, is said to be reduced if

(1) $|D(t) - b(t)| < |a(t)| < |D(t) + b(t)|$.

Lemma 4.3. If $F = [a(t), 2b(t), c(t)]$ satisfies the conditions of definition 4.2 then

(2) $|b(t)| = |\Delta(t)|/2$, $|a(t)| < |\Delta(t)|/2$,

(3) no other form obtained from F be a translation is reduced,

(4) $[c(t), 2b(t), a(t)]$ is reduced.

PROOF: (2) Since $|D(t) - b(t)| \neq |D(t) + b(t)|$, $|b(t)| = |D(t)| = |\Delta(t)|/2$.

(3) If $b(t)$ is replaced by $b'(t) = b(t) + h(t)a(t)$, $h(t) \neq 0$, then $|D(t) - b'(t)| = |h(t)| + |a(t)| \geq |a(t)|$.

(4) We have $\{D(t) + b(t)\}\{D(t) - b(t)\} = D^2(t) + \Delta(t) - a(t)c(t)$. If $D(t) - b(t) \neq 0$ then $|D(t) + b(t)| + |D(t) - b(t)| = |a(t)| + |c(t)|$, hence $|D(t) - b(t)| < |c(t)| < |D(t) + b(t)|$. If $D(t) - b(t) = 0$ then $D^2(t) + \Delta(t) = a(t)c(t)$, hence $|c(t)| < |D(t) + b(t)|$.

Let $F = [a(t), 2b(t), c(t)]$ have determinant $\Delta(t)$, $\chi(\Delta) = 1$. Choose $q(t)$, $s(t)$ in $K[t]$ so that $D(t) + b(t) = q(t)c(t) + s(t)$ and $|s(t)| < |c(t)|$. The form $F_1 = [c(t), 2b_1(t), a_1(t)]$ obtained from F by the transformation

$$\begin{bmatrix} 0, & -1 \\ 1, & q(t) \end{bmatrix}$$

is called the right neighbor of F.

Lemma 4.4. If $|c(t)| < |\Delta(t)|/2$ then F_1 is reduced.

PROOF: Since $b_1(t) = c(t)q(t) - b(t)$, $D(t) - b_1(t) = s(t)$. Hence $|D(t) - b_1(t)| < |c(t)| < |\Delta(t)|/2 =$

$|D(t) + b_1(t)|$.

Lemma 4.5. If $|c(t)| \geq |\Delta(t)|/2$ then $|a_1(t)| < |c(t)|$.

PROOF: Since $a_1(t)c(t) = \Delta(t) + b_1^2(t) = \Delta(t) + D^2(t) - 2D(t)s(t) + s^2(t)$,

$$|a_1(t)| + |c(t)| \leq \max\{|\Delta(t)+D^2(t)|, |\Delta(t)|/2+|s(t)|, 2|s(t)|\}$$
$$\leq \max\{|\Delta(t)|/2+|s(t)|, 2|s(t)|\}.$$

If $|a_1(t)| + |c(t)| \leq |\Delta(t)|/2 + |s(t)|$ then $|a_1(t)| < |\Delta(t)|/2$. If $|a_1(t)| + |c(t)| \leq 2|s(t)|$ then $|a_1(t)| < |s(t)| < |c(t)|$.

By lemmas 3.4 and 3.5, a succession of right neighbors F, F_1, F_2, ... ultimately gives a reduced form, and thereafter only reduced forms, these forming a chain, say

$$[a_1(t), 2b_1(t), a_2(t)], [a_2(t), 2b_2(t), a_3(t)],...$$

Since $[c(t), 2b(t), a(t)]$ is reduced with $[a(t), 2b(t), c(t)]$, the chain can be extended backwards, each reduced from F_i having a reduced left neighbor F_{i-1} such that F_i is the right neighbor of F_{i-1}.

Theorem 4.6. If

$$T = \begin{bmatrix} r_1(t), & r_2(t) \\ r_3(t), & r_4(t) \end{bmatrix}$$

is a unimodular transformation taking a reduced indefinite form into a reduced indefinite form then exactly one of the following is true:

(5) $|r_1(t)| > |r_2(t)|$, $|r_3(t)| > |r_4(t)|$,

(6) $|r_4(t)| > |r_2(t)|$, $|r_3(t)| > |r_1(t)|$, or

(7) $r_2(t) = r_3(t) = 0$.

Let $F_1 = [a_1(t), 2b_1(t), c_1(t)]$ be the given form and $FT = F_2 = [a_2(t), 2b_2(t), c_2(t)]$. By the Gauss criterion, applied in both directions, we obtain

$$(8)\quad \begin{aligned} a_2(t) &= a_1(t)r_1^2(t) + 2b_1(t)r_1(t)r_3(t) + c_1(t)r_3^2(t) \\ a_1(t) &= a_2(t)r_4^2(t) - 2b_2(t)r_3(t)r_4(t) + c_2(t)r_3^2(t), \end{aligned}$$

$$(9)\quad \begin{aligned} a_2(t)r_4(t) &= a_1(t)r_1(t) + [b_1(t) + b_2(t)]r_3(t) \\ a_1(t)r_1(t) &= a_2(t)r_4(t) - [b_1(t) + b_2(t)]r_3(t), \text{ and} \end{aligned}$$

$$(10)\quad \begin{aligned} -a_2(t)r_2(t) &= [b_1(t) - b_2(t)]r_1(t) + c_1(t)r_3(t) \\ a_1(t)r_2(t) &= [b_2(t) - b_1(t)]r_4(t) - c_2(t)r_3(t). \end{aligned}$$

If $r_3(t) = 0$ then T is a translation. It follows from lemma 3.4 that $r_2(t) = 0$. Since

$$T_1 = \begin{bmatrix} r_4(t), & r_3(t) \\ r_2(t), & r_4(t) \end{bmatrix}$$

takes $[c_1(t), 2b_1(t), a_1(t)]$ into $[c_2(t), 2b_2(t), a_2(t)]$, $r_2(t) = 0$ implies $r_3(t) = 0$. Thus we may assume $r_2(t)r_3(t) \neq 0$.

If $r_1(t) = 0$ then $r_1(t)r_4(t) - r_2(t)r_3(t) = -r_2(t)r_3(t) = 1$, hence $|r_2(t)| = |r_3(t)| = 0$. By comparing degrees in the second equation of (8), we see that $|r_4(t)| > 0$. In a similar manner, we obtain $|r_1(t)| > |r_2(t)|$, $|r_3(t)| > |r_4(t)|$ whenever $r_4(t) = 0$.

Now assume $r_1(t)r_2(t)r_3(t)r_4(t) \neq 0$. Since $b_1(t)$, $b_2(t)$ have the same leading coefficient as $D(t)$, $|b_1(t) + b_2(t)| = |\Delta(t)|/2$. From (9), it follows that $|r_3(t)|$ cannot exceed both $|r_1(t)|$ and $|r_4(t)|$. Replacing T by T_1, we

see that $|r_2(t)|$ likewise cannot exceed both $|r_1(t)|$ and $|r_4(t)|$.

If $|r_4(t)| \geq |r_1(t)|$ then $|r_4(t)| \geq |r_2(t)|, |r_3(t)|$. We see from (8) that $|r_4(t)| \neq |r_3(t)|$ and, replacing T by T_1, $|r_2(t)| \neq |r_4(t)|$. Since $r_1(t)r_4(t) - r_2(t)r_3(t) = 1$, $|r_1(t)| + |r_4(t)| = |r_2(t)| + |r_3(t)|$ hence (6) holds.

If $|r_1(t)| \geq |r_4(t)|$ then, as in the preceding manner, (5) holds.

Theorem 4.7. If $F = [a(t), 2b(t), c(t)]$ and $F' = [a'(t), 2b'(t), c'(t)]$ are equivalent indefinite reduced froms then there is an element k in K such that FT_k,

$$T_k = \begin{bmatrix} k, & 0 \\ 0, & 1/k \end{bmatrix},$$

is in the chain of reduced forms containing F'.

PROOF: Let

$$T = \begin{bmatrix} r_1(t), & r_2(t) \\ r_3(t), & r_4(t) \end{bmatrix}$$

be a unimodular transformation taking F into F'. Now T must satisfy one of the three conditions of theorem 4.6. The theorem being evident in case (7) holds, we need consider only (5) and (6).

Suppose (5) holds for T and let

$$N_i = \begin{bmatrix} 0, & -1 \\ 1, & q_i(t) \end{bmatrix}$$

be the transformation taking F_i, the i^{th} right neighbor of F', into its right neighbor F_{i+1}. If

$$M = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

is any matrix satisfying (5) then $|s(t)|, |u(t)| > |v(t)|$, hence

$$MN_i = \begin{bmatrix} s(t), & -r(t) + s(t)q_i(t) \\ v(t), & -u(t) + v(t)q_i(t) \end{bmatrix}$$

must satisfy either (5) or (7) whenever MN_i takes a reduced form into a reduced form. Since the degree coefficients of $TN_0 \ldots N_i$ decend with increasing i, after a finite number of steps we obtain a matrix $TN_0 \ldots N_n$ satisfying (7). That is, $TN_0 \ldots N_n = T_k$ for some k in K. Hence $FTN_0 \ldots N_n = F'N_0 \ldots N_n = FT_k$ so that FT_k is the $n+1^{th}$ right neighbor of F'.

Now let T satisfy (6) and

$$T^* = \begin{bmatrix} r_4(t), & r_3(t) \\ r_2(t), & r_1(t) \end{bmatrix},$$

the matrix taking $[c(t), 2b(t), a(t)]$ into $[c'(t), 2b'(t), a'(t)]$. Clearly (5) holds for T*; therefore, as in the preceding proof, $[k^2c(t), 2b(t), a(t)/k^2]$ is in the chain of right neighbors of $[c'(t), 2b'(t), a'(t)]$ for some k in K. By definition, $[a(t)/k^2, 2b(t), k^2c(t)]$ is in the chain of left neighbors of F'.

Definition 4.8. T is said to be an integral automorph of a form F if T is a unimodular transformation with coefficients in K[t] which takes F into itself.

Lemma 4.9. The integral automorphs of a primitive form F, $\Delta(t)$ the determinant of F, are the transformations

$$(11)\quad \begin{bmatrix} f(t) - b(t)g(t), & -c(t)g(t) \\ a(t)g(t), & f(t) + b(t)g(t) \end{bmatrix}$$

where $f^2(t) + g^2(t)\,\Delta(t) = 1$.

PROOF: By the Gauss criterion,

$$T = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

is an integral automorph of F if and only if

$$\begin{aligned} a(t) &= a(t)r^2(t) + 2b(t)r(t)u(t) + c(t)u^2(t) \\ a(t)v(t) &= a(t)r(t) + 2b(t)u(t) \\ -a(t)s(t) &= c(t)u(t). \end{aligned} \qquad (12)$$

Since F is primitive, a(t) divides u(t). If we set $u(t) = a(t)g(t)$ then

$$\begin{aligned} 1 &= r^2(t) + 2b(t)r(t)g(t) + c(t)g^2(t) \\ &= [r(t) + b(t)g(t)]^2 + g^2(t)\,\Delta(t). \end{aligned}$$

Letting $f(t) = r(t) + b(t)g(t)$, we have $r(t) = f(t) - b(t)g(t)$, $s(t) = -c(t)g(t)$, $u(t) = a(t)g(t)$ and $v(t) = f(t) + b(t)g(t)$. Since it is apparent that any matrix of the form (11) satisfies (12), the proof of the lemma is complete.

Definition 4.10. A chain C of indefinite reduced forms is said to be periodic if for F in C there is an integer n and a k in K such that FT_k,

$$T_k = \begin{bmatrix} k, & 0 \\ 0, & 1/k \end{bmatrix},$$

is the n^{th} right neighbor of F.

Theorem 4.11. A necessary and sufficient condition for a chain C of indefinite reduced forms of determinant $\Delta(t)$

to be periodic is for the Pell equation $X^2 + \Delta(t)Y^2 = 1$ to have a non-trivial solution in K[t].

PROOF: To show necessity, let F be a form in C and F_n, the n^{th} right neighbor of F, be obtained from F by T_k. If N_i denotes the matrix taking F_i, the i^{th} right neighbor of F, into its right neighbor F_{i+1} then $N = N_0 \cdots N_{n-1}$ takes F into F_n. Since NT_k^{-1} is an integral automorph of $F = [a(t), 2b(t), c(t)]$,

$$NT_k^{-1} = \begin{bmatrix} f(t) - b(t)g(t), & -c(t)g(t) \\ a(t)g(t), & f(t) + b(t)g(t) \end{bmatrix}$$

where $f^2(t) + \Delta(t)g^2(t) = 1$. It follows easily by induction that NT_k^{-1} satisfies (6) of theorem 4.6, hence $|f(t) + g(t)b(t)| > |f(t) - g(t)b(t)|$. Therefore $g(t) \neq 0$ and $X = f(t)$, $Y = g(t)$ is a non-trivial solution of the Pell equation.

Now let f(t), g(t) be a non-trivial solution of the Pell equation and

$$T = \begin{bmatrix} f(t) - g(t)b(t), & -c(t)g(t) \\ a(t)g(t), & f(t) + g(t)b(t) \end{bmatrix}$$

be an integral automorph of the reduced form $[a(t), 2b(t), c(t)]$. We may assume $|f(t) - g(t)b(t)| > |f(t) + g(t)b(t)|$ since g(t) can be replaced by -g(t). Since F is reduced, T must satisfy (5) of theorem 4.6. By theorem 4.7, there is a k in K such that $FTT_k = FT_k$ is in the chain of right neighbors of F.

Definition 4.12. An ambiguous form is a form of the type

$[a(t), 2b(t), c(t)]$ where $a(t)$ divides $b(t)$.

Definition 4.13. An ambiguous class of Q_Δ is one whose square is the identity.

Theorem 4.14. A class of Q_Δ is ambiguous if and only if it contains an ambiguous form.

PROOF: If a class contains an ambiguous form then it contains a form of the type $[a(t), 0, \Delta(t)/a(t)]$ where $a(t)$ divides $\Delta(t)$. Clearly $\{[a(t), 0, \Delta(t)/a(t)]\}^2 = [[1, 0, \Delta(t)]]$.

To show the condition is necessary, we make use of a method divised by Cantor[2],[7]. Let $\{F\}^2 = [[1, 0, \Delta(t)]]$ with $F = [a(t), 2b(t), c(t)]$. Then $F \frown [a(t), -2b(t), c(t)]$ hence there are polynomials $r(t)$, $s(t)$, $u(t)$, and $v(t)$ in $K[t]$ such that $r(t)v(t) - s(t)u(t) = 1$, $a(t) = a(t)r^2(t) + 2b(t)r(t)u(t) + c(t)u^2(t)$, $a(t)v(t) = a(t)r(t)$, $-a(t)s(t) = 2b(t)r(t) + c(t)u(t)$. Thus $r(t) = v(t)$ and $-r^2(t) + s(t)u(t) = -1$. Hence $F' = [s(t), 2r(t), u(t)]$ is a primitive form having determinant -1. By lemma 3.2, F' represents a constant $k \neq 0$ in K; therefore, F' can be transformed into $[k, 0, -1/k]$. Since

$$\begin{bmatrix} 1, & -1/2k \\ k, & 1/2 \end{bmatrix}$$

takes $[k, 0, -1/k]$ into $[0, -2, 0]$, $F' \frown [0, -2, 0]$. Let

$$T = \begin{bmatrix} s_1(t), & s_2(t) \\ s_3(t), & s_4(t) \end{bmatrix}$$

be a unimodular transformation taking F' into $[0,-2,0]$.

Then $s(t) = -2s_1(t)s_3(t)$, $r(t) = -s_1(t)s_4(t) - s_2(t)s_3(t)$, and $u(t) = -2s_2(t)s_4(t)$, hence

$$F\begin{bmatrix} s_1(t), & s_3(t) \\ s_2(t), & s_4(t) \end{bmatrix} = [a'(t), 2b'(t), c'(t)] \text{ with}$$

$-2b'(t) = -2a(t)s_1(t)s_3(t) - 2b(t)\{s_1(t)s_4(t)+s_2(t)s_3(t)\}$
$-2c(t)s_2(t)s_4(t) = a(t)s(t) + 2b(t)r(t) + c(t)u(t) = 0.$
Therefore $[a'(t), 2b'(t), c'(t)]$ is an ambiguous form in $\{F\}$.

Definition 4.15. A properly ambiguous form will be a primitive form of the type $[a(t), 0, \Delta(t)/a(t)]$ where $a(t)$ divides $\Delta(t)$.

Let A_Δ denote the set of properly ambiguous forms having determinant $\Delta(t)$. For $F_1 = [a_1(t), 0, \Delta(t)/a_1(t)]$ and $F_2 = [a_2(t), 0, \Delta(t)/a_2(t)]$ in A_Δ define F_1F_2, the product of F_1 and F_2, to be the form $F_3 =$ $[a_1(t)a_2(t)/(a_1(t), a_2(t))^2, 0, b(t)]$ where $b(t)a_1(t)a_2(t)/(a_1(t), a_2(t))^2 = \Delta(t)$. Since F_1 and F_2 are primitive, a prime divisor of $a_1(t)$ or $a_2(t)$ must be prime to $(a_1(t), a_2(t))$ or appear to the same power in both $a_1(t)$ and $a_2(t)$. It follows that F_3 is primitive and multiplication is closed and associative. Now $[1, 0, \Delta(t)]$ acts as an identity element and each form is its own inverse. Hence A_Δ is an abelian group.

Lemma 4.16. There is a homomorphism ϕ from A_Δ onto C_Δ, the ambiguous classes of Q_Δ, such that the kernel of ϕ is the set of forms in A_Δ equivalent to $[1, 0, \Delta(t)]$.

PROOF: The lemma follows immediately by letting $\emptyset(F) = \{F\}$.

An element $\eta = f(t) + g(t)\theta$ in K_Δ will be called a unit if $N(\eta) = f^2(t) + \Delta(t)g^2(t)$ is a non-zero constant. If η is a unit then $sg^2[f(t)] - sg^2[g(t)]d^2 = 0$, where d denotes a solution of the equation $X^2 + sg[\Delta] = 0$. We say that η is positive(negative) if $sg[f(t)] = sg[g(t)]d(-sg[g(t)]d)$. Let $|\eta| = |f(t)|$. If the Pell equation has a non-trivial solution choose $\eta_1 = f_1(t) + g_1(t)\theta$ such that $|\eta_1|$ is minimal among the units with $g(t) \neq 0$.

Lemma 4.17. If $\mu = r(t) + s(t)\theta$ is any unit in K_Δ then there is an integer n such that $\mu = k\eta_1^n$ for some k in K.

PROOF: Let μ be as above and $\nu = u(t) + v(t)\theta$, $v(t) \neq 0$, be any other unit in K_Δ. Then $\nu\mu = [r(t)u(t) - s(t)v(t)\Delta(t)] + [s(t)u(t) + r(t)v(t)]\theta$ is a unit in K_Δ. We consider the respective cases:

(a). ν, μ are positive.

Since $|u(t)| = |v(t)| + |\Delta(t)|/2$ and $|r(t)| = |s(t)| + |\Delta(t)|/2$,

$$\begin{aligned} sg[r(t)u(t) - s(t)v(t)\Delta(t)] &= \\ &= sg[r(t)]\ sg\ [u(t)] - sg[s(t)]sg[v(t)]sg[\Delta] \\ &= sg[s(t)\ sg[u(t)]d + sg[r(t)]sg[v(t)]d \\ &= sg[s(t)u(t) + r(t)v(t)]d. \end{aligned}$$

Hence $\nu\mu$ is positive and $|\nu\mu| = |\nu| + |\mu|$.

(b). μ , $\nu\mu$ are positive.

If ν is positive then the case reduces to (a). For ν negative, $N(\nu)\mu = \overline{\nu}(\nu\mu)$. Therefore $|\overline{\nu}| + |\nu\mu| = |N(\nu)\mu| = |\mu|$ hence $|\nu\mu| = |\mu| - |\nu|$.

(c). μ is positive, $\nu\mu$ is negative.

Then $\nu N(\mu) = (\nu\mu)\overline{\mu}$. By taking conjugates in (a), we have $|\overline{\mu}| + |\nu\mu| = |\nu|$. Therefore $|\nu\mu| = |\nu| - |\mu|$.

All other cases may be obtained by taking conjugates in (a), (b), and (c); thus,

$$|\nu\mu| = \begin{cases} |\nu| + |\mu| & \text{when } \nu \text{ and } \mu \text{ are of the same type and} \\ \\ \big||\nu| - |\mu|\big| & \text{when } \nu \text{ and } \mu \text{ are of different types.} \end{cases}$$

Now let $|\mu| = |\eta_1|n + m$ with $0 < m < n$. We may assume η_1 is positive since η_1 may be replaced with $\overline{\eta}_1$. For μ positive we have $|\overline{\mu}\eta_1^n| = \big|n|\eta_1| - |\overline{\mu}|\big| = m$. Since $\overline{\mu}\eta_1^n$ is a unit satisfying $|\overline{\mu}\eta_1^n| < |\eta_1|$, $\overline{\mu}\eta_1^n$ is a non-zero constant in K. Therefore $\mu = k\eta_1^n$ for some $k \neq 0$ in K.

In a similar manner, $\mu = k'\eta_1^{-n}$ when μ is negative.

Definition 4.18. We say two forms F and F' are scalar equivalent if there is a k in K such that

$$T_k = \begin{bmatrix} k, & 0 \\ 0, & 1/k \end{bmatrix} \quad \text{or} \quad T_k^* = \begin{bmatrix} 0 & , & -k \\ 1/k, & & 0 \end{bmatrix}$$

takes F into F'.

Lemma 4.19. For any non-trivial solution $f(t)$, $g(t)$ of the Pell equation $X^2 + \Delta(t)Y^2 = 1$ there corresponds a properly ambiguous form $F = [-2sg[f(t)](1-f(t), \Delta(t)), 0, \Delta(t)/-2sg[f(t)](1-f(t), \Delta(t))]$ in the principal class. Furthermore, if F' is any properly ambiguous form equivalent but not scalar equivalent to $[1, 0, \Delta(t)]$ then there is a constant c and a non-trivial solution $f(t)$, $g(t)$ of the Pell equation such that $F' = FT_c$.

PROOF: Let $f(t)$, $g(t)$ be a non-trivial solution of the Pell equation and let $1 - f(t) = -sg[f(t)]r^2(t)a(t)$, $1 + f(t) = g^2(t)\Delta(t)/-sg[f(t)]a(t)r^2(t)$ where $a(t) = (1 - f(t), \Delta(t))$ and $f^2(t) = (1 - f(t), g^2(t))$. It follows that $(r(t), g(t)/r(t)) = 1$ and $(a(t), \Delta(t)/a(t)) = 1$. Hence $[a(t), 0, \Delta(t)/a(t)]$ is properly ambiguous and we have $a(t)\{-sg[f(t)]r(t)\}^2 + \Delta(t)\{g(t)/r(t)\}^2/a(t) = -2sg[f(t)]$. Therefore $[a(t), 0, \Delta(t)/a(t)] \sim [-2sg[f(t)], 0, \Delta(t)/-2sg[f(t)]]$. Multiplying both sides by the latter form, we obtain the equivalence of F and $[1, 0, \Delta(t)]$.

Now let $F' = [a(t), 0, \Delta(t)/a(t)]$ be an ambiguous form in the principal class which is not scalar equivalent to $[1, 0, \Delta(t)]$. Since F' and $[1, 0, \Delta(t)]$ are equivalent there are relatively prime polynomials $r(t)$, $s(t)$ such that $a(t)r^2(t) + s^2(t)\Delta(t)/a(t) = 1$. If $f(t) = s^2(t)\Delta(t)/a(t) - a(t)r^2(t)$ then $1 - f(t) = 2a(t)r^2(t)$

and $1 + f(t) = 2s^2(t)\Delta(t)/a(t)$, hence $f^2(t) + \Delta(t)[2r(t)s(t)]^2 = 1$. Since F' is not scalar equivalent to $[1, 0, \Delta(t)]$, neither a(t) or $\Delta(t)/a(t)$ is the square of some constant in K; therefore, $r(t)s(t) \neq 0$. Let F be the ambiguous form corresponding to the solution f(t), 2r(t)s(t) of the Pell equation. Then $F = [-2sg[f(t)](1-f(t), \Delta(t)), 0, \Delta(t)/-2sg[f(t)](1-f(t), \Delta(t))]$ $= [-2sg[f(t)]a(t)/sg[a(t)], 0, \Delta(t)sg[a(t)]/-2sg[f(t)]a(t)]$ $= [4sg^2[r(t)]a(t), 0, \Delta(t)/4sg^2[r(t)]a(t)]$.
Therefore $FT_c = F'$ where $c = 1/2sg[r(t)]$.

Theorem 4.20. If the Pell equation $X^2 + \Delta(t)Y^2 = 1$ has a non-trivial solution then there is an ambiguous form F, equivalent but not scalar equivalent to $[1, 0, \Delta(t)]$, such that every properly ambiguous form in the principal class is scalar equivalent to either F or $[1, 0, \Delta(t)]$.

PROOF: From lemma 4.17, there is a unit η in K_Δ with the property that given any unit μ having norm 1 there is an integer n such that $\mu = \eta^n$ or $-\eta^n$. Let $f_n(t)$, $g_n(t)$ be the solution of the Pell equation corresponding to η^n.

Since $|\eta^n| < |\eta^{n+1}|$, $g_n(t) = 0$ if and only if $n = 0$; therefore, there is a properly ambiguous form F_n corresponding to each solution $f_n(t)$, $g_n(t)$ with $n \neq 0$. If $-F_n$ denotes the form corresponding to $-f_n(t)$, $-g_n(t)$, $n \neq 0$, then $-F_n$ has leading coefficient $2sg[f_n(t)](1+f_n(t), \Delta(t))$

$= 2sg[f_n(t)]\Delta(t)/sg[\Delta](1 - f_n(t), \Delta(t)) =$ $\{2sg[g_n(t)]\}^2\Delta(t)/-2sg[f_n(t)](1 - f_n(t), \Delta(t))$. It follows that $-F_n = F_nT_1^*/sg[g(t)]$. Now $f_{-n}(t) = f_n(t)$, hence $F_{-n} = F_n$. Therefore, by lemma 4.19, any properly ambiguous form in the ambiguous class is scalar equivalent to either $[1, 0, \Delta(t)]$ or F_n for some positive integer n.

We now show that the forms F_n, $n > 0$, are scalar equivalent to either F_1 or $[1, 0, \Delta(t)]$. Without loss of generality, we may assume η to be positive. Since $\eta^{n+1} = (f_n(t) + g_n(t)\theta)(f_1(t) + g_1(t)\theta) =$ $[f_n(t)f_1(t) - g_n(t)g_1(t)\Delta(t)] + [f_n(t)g_1(t) +$ $f_1(t)g_n(t)]\theta$, we have $f_{n+1}(t) \equiv f_n(t)f_1(t) \bmod \Delta(t)$ and $sg[f_{n+1}(t)] = 2sg[f_n(t)sg[f_1(t)]$. By induction, we have $f_n(t) \equiv f_1^n(t) \bmod \Delta(t)$ and $sg[f_n(t)] = 2^{n-1}sg^n[f_1(t)]$. Since $1 - f_1^2(t) \equiv 0 \bmod \Delta(t)$, $f_n(t) \equiv 1 \bmod \Delta(t)$ for n even and $f_n(t) \equiv f_1(t) \bmod \Delta(t)$ for n odd. Thus, $(1 - f_n(t), \Delta(t)) = \Delta(t)/sg[\Delta]$ for n even and $(1 - f_1(t), \Delta(t))$ for n odd. Since the leading coefficient of F_{2n} is $-2^{2n}sg^{2n}[f_1(t)]\Delta(t)/-d^2$, where $d^2 = -sg[\Delta]$, F_{2n} and $[1, 0, \Delta(t)]$ are scalar equivalent. Now the leading coefficient of F_{2n+1} is $-2^{2n+1}sg^{2n+1}[f_1(t)](1 - f_1(t), \Delta(t))$; in which case, F_1 and F_{2n+1} are scalar equivalent.

It remains to show that F_1 and $[1, 0, \Delta(t)]$ are not scalar equivalent. If F_1 and $[1, 0, \Delta(t)]$ are scalar equivalent then there is a k in K such that $F_1 =$

$[k^2, 0, \Delta(t)/k^2]$ or $[\Delta(t)/k^2, 0, k^2]$. Since the two cases may be handled in similar ways, assume $F_1 = [k^2, 0, \Delta(t)/k^2]$. Then $-2sg[f_1(t)] = k^2$ and $(1 - f_1(t), \Delta(t)) = 1$; therefore, $1 - f_1(t) = k^2r^2(t)/2$ and $1 + f_1(t) = 2\Delta(t)g_1^2(t)/k^2r^2(t)$ where $r^2(t) = (1 - f_1(t), g_1^2(t))$. From the two equations, we have $1 = \{kr(t)/2\}^2 + \Delta(t)\{g_1(t)/kr(t)\}^2$. Therefore, $\mu = kr(t)/2 + \theta g_1(t)/kr(t)$ is a unit in K_Δ having norm 1. Since $|\mu| \geq |\eta|$, $|r(t)| \geq |f_1(t)|$; in which case, $f_1(t)$ and $r(t)$ are constants. Since $\Delta(t)$ is not a constant, $1 - f_1^2(t) = 0 = g_1(t)$. Hence the only units in K_Δ having norm 1 are ± 1, a contradiction to the assumption of the existance of a non-trivial solution of the Pell equation. This completes the proof of the theorem.

Corollary 4.21. If the Pell equation has a non-trivial solution then in each ambiguous class there are two properly ambiguous forms F and F' such that (13) F and F' are not scalar equivalent and (14) any properly ambiguous form in the class is scalar equivalent to F or F'. If the Pell equation has only trivial solutions then all properly ambiguous forms in an ambiguous class are scalar equivalent.

PROOF: The corollary follows immediately from lemmas 4.16-4.19 and theorem 4.20.

Corollary 4.22. If K is algebraically closed, $|\Delta(t)| =$

$2n$, $n > 1$, and $\Delta(t)$ is not a power of a polynomial of degree 2, then there are classes of order 2^n for every positive integer n.

PROOF: Let $\Delta(t) = sg[\Delta] \prod_{i=1}^{r} (t-d_i)^{e_i}$ be a prime factorization $\Delta(t)$ in $K[t]$. Since $\Delta(t)$ is not a power of a polynomial of degree 2, the forms $[(t-d_1)^{e_1}, 0, \Delta(t)/(t-d_1)^{e_1}] = F$ and $[(t-d_2)^{e_2}, 0, \Delta(t)/(t-d_2)^{e_2}] = F'$ are properly ambiguous forms which are not scalar equivalent. Since F and F' are not scalar equivalent to $[1, 0, \Delta(t)]$, we see by theorem 4.20 that one of the classes $\{F\}$, $\{F'\}$ is not the principal class. Since each of the classes is ambiguous, there is a class of order 2. The existence of classes having order 2^n, $n > 1$, follows from the proof of corollary 3.14.

Lemma 4.23. Let $F = [a(t), 2b(t), c(t)]$ be an indefinite reduced form having determinant $\Delta(t)$ and K' be a subfield of K containing the coefficients of $a(t)$, $b(t)$, $c(t)$ and $D(t)$. If $F' = [a'(t), 2b'(t), c'(t)]$ is any form in the chain of reduced forms containing F then $a'(t)$, $b'(t)$, and $c'(t)$ are elements of $K'[t]$.

PROOF: The right neighbor of F is obtained by the transformation

$$T = \begin{bmatrix} 0, & -1 \\ 1, & q(t) \end{bmatrix}$$

where $q(t)$ satisfies $|D(t) + b(t) - q(t)c(t)| < |c(t)|$.

Clearly $q(t)$ is unique and $q(t)$ is an element of $K'[t]$. Therefore, the right neighbor of F has coefficients in $K'[t]$. In a similar manner, we see that the left neighbor of F has coefficients in $K'[t]$. The lemma follows by induction.

Lemma 4.24. The following are equivalent:

(14) the Pell equation has a solution in $K[t]$,

(15) the Pell equation has a solution in $K'[t]$ where K' is the least field containing the coefficients of $\Delta(t)$ and $(sg[\Delta])^{1/2}$, and

(16) the Pell equation has a solution in $\overline{K}[t]$, the algebraic closure of K.

PROOF: Evidently the equivalence of the first two statements implies the equivalence of all three. By lemma 4.23, the coefficients of the polynomials appearing in the chain $[1, 2D(t), \Delta(t) + D^2(t)]$ are elements of $K'[t]$. If we assume (14) then the chain is periodic with respect to $K[t]$, hence there exists k in K such that $[k^2, 2D(t), \{\Delta(t) + D^2(t)\}/k^2]$ is in the chain of right neighbors of $[1, 2D(t), \Delta(t) + D^2(t)]$. It follows from the proof of 4.11 that the equation $X^2 + \Delta(t)Y^2 = k^2$ has a solution $f(t)$, $g(t)$ in $K'(t)$ with $g(t) \neq 0$. Therefore $\{f^2(t) - \Delta(t)g^2(t)\}$, $2f(t)g(t)/k^2$ is a non-trivial solution of the Pell equation in $K'[t]$.

Theorem 4.25. If the Pell equation $X^2 + \Delta(t)Y^2 = 1$

has a solution in K[t], there exists k in K such that $\Delta(t)$ is reducible in $K(k^{1/2})[t]$.

PROOF: Let $\eta_1 = f(t) + g(t)\theta$ be a unit in $\overline{K}_\Delta$, $\overline{K}$ the algebraic closure of K, such that η_1 is minimal among the units μ with $|\mu| > 0$. Since $N(\eta_1)$ is a square in $\overline{K}$, we may assume $N(\eta_1) = 1$. Therefore

$$T = \begin{bmatrix} f(t) - D(t)g(t), & -\Delta(t)g(t) - D^2(t)g(t) \\ g(t) \quad , & f(t) + D(t)g(t) \end{bmatrix}$$

is an automorph of $[1, 2D(t), \Delta(t) + D^2(t)]$. By changing signs of g(t), we may assume T to satisfy (6) of theorem 4.6. It follows from theorem 4.7 that $T = T_k \prod_{i=0}^{n} N_i$ where

$$T_k = \begin{bmatrix} k, & 0 \\ 0, & 1/k \end{bmatrix}$$

for some k in $\overline{K}$ and N_i is the transformation taking the i^{th} right neighbor F_i of $[1, 2D(t), \Delta(t) + D^2(t)]$ into its right neighbor F_{i+1}. By lemma 4.23, TT_k^{-1} has coefficients in K[t]; hence, f(t)/k, g(t)/k, and k^2 are elements of K[t]. Now $\Delta(t)g^2(t)/k^2 = (1/k - f(t)/k)(1/k + f(t)/k)$. From the proof of theorem 4.20, there is a proper divisor of $\Delta(t)$ in $\overline{K}[t]$ which divides $1/k - f(t)/k$. Therefore, there is a proper divisor of $\Delta(t)$ in K(k)[t] which divides $1/k - f(t)/k$.

Example 4.26. Theorem 4.25 exhibits a class of polynomials $\Delta(t), \chi(\Delta) = 1$, for which the Pell equation has only trivial solutions. For example, let K be the

rational numbers and $\Delta(t) = -t^4 + 2t + 2$. By Eisenstein's criterion, $\Delta(t)$ is irreducible in $K[t]$. We now show that $\Delta(t)$ is irreducible in $K(r^{1/2})[t]$ for every rational number r which is not a square. If $-\Delta(t) = f(t)g(t)$ is a proper factorization in $K(r^{1/2})[t]$ then $f(t)$, $g(t)$ are irreducible and $|f(t)| = |g(t)| = 2$. Let $\emptyset$ be the K-automorphism of $K(r^{1/2})$ which sends $r^{1/2}$ onto $-r^{1/2}$. Without loss of generality, we may assume $f(t)$, $g(t)$ are monic. Since $\emptyset(f(t))\emptyset(g(t)) = f(t)g(t)$, $\emptyset(f(t)) = f(t)$ or $g(t)$. Now $f(t)$ is not in $K[t]$, hence $\emptyset(f(t)) = g(t)$. Let $f(t) = t^2 + at + b$, $g(t) = t^2 + ct + d$. Then $d = -2/b$ and $a(b + 2/b) = -2$. Since $\emptyset(b) = -2/b$, $2b = b - 2/b + (b + 2/b)r^{1/2}$; therefore $b + 2/b = (b + 2/b)r^{1/2}$. Since $b + 2/b \neq 0$, $r^{1/2} = 1$ which contradicts the assumption that r is not a square.

Theorem 4.27. Let K be algebraically closed, $x = 1/t$, and $\Delta_1(x) = \Delta(t)/t^{2n}$ where $2n = |\Delta(t)|$. A necessary and sufficient condition for the Pell equation $X^2 + \Delta(t)Y^2 = 1$ to have a non-trivial solution in $K[t]$ is for there to be a positive integer $m \geq n$ such that the rank of

$$\begin{bmatrix} c_{m+1}, \ldots\ldots, c_{n+1} \\ \vdots \qquad\qquad \vdots \\ c_{2m-1}, \ldots\ldots, c_{m+n-1} \end{bmatrix}$$

$c_k = \theta_1(0)^{(k)}/d!$, is less than $m+1-n$.

PROOF: Let $f(t)$, $g(t)$ be a non-trivial solution of the

Pell equation with $|f(t)| = m$ and set $f_1(x) = f(t)/t^m$, $g_1(x) = g(t)/t^{m-n}$ and $\Delta_1(x) = \Delta(t)/t^{2n}$. It follows that $f_1(x)$, $g_1(x)$ is a primitive representation of x^{2m} by $[1, 0, \Delta_1(x)]$. Let $f_1(x) = \sum_{i=0}^{m} f_i x^i$, $g_1(x) = \sum_{i=0}^{m-n} g_i x^i$, and $\Delta_2(x) = \sum_{i=0}^{2m-1} c_i x^i$, $c_i = \theta_1(0)^{(i)}/i!$. Since $f_1^2(x) + g_1^2(x)\,\Delta_1(x) \equiv f_1^2(x) - g_1^2(x)\Delta_2^2(x) \equiv 0 \bmod x^{2m}$, $f_1(x) - g_1(x)\Delta_2(x)$ or $f_1(x) + g_1(x)\Delta_2(x)$ is divisible by x^{2m}. By changing signs of $g_1(x)$, we may assume $f_1(x) - g_1(x)\Delta_2(x)$ is divisible by x^{2m}. Therefore, the equations

(17) $\sum_{j+k=1} c_k X_j = 0$ for $i = m+1,\ldots,2m-1$ and $j = 0,\ldots,m-n$

have a non-trivial solution $g_0, g_1, \ldots, g_{m-n}$ in K. It follows that the rank of A is less than m-n+1. Conversely, if the rank of A is less than m-n+1 then the equations (17) have a non-trivial solution in K. It follows that there exist polynomials $f_1(x)$, $g_1(x)$ in K[x] such that $|g_1(x)| \leq m-n$, $|f_1(x)| \leq m$, $g_1(x) \neq 0$, and $f_1^2(x) + \Delta_1(x)g_1^2(x) \equiv 0 \bmod x^{2m}$. Since $-\Delta(t)$ is not a square, $-\Delta_1(x)$ is not a square; therefore, $f_1^2(x) + \Delta_1(x)g_1^2(x) \neq 0$ and has degree at most 2m. Hence $f_1^2(x) + \Delta_1(x)g_1^2(x) = rx^{2m}$ for some $r \neq 0$ in K. Multiplying by t^{2m}, we obtain a non-trivial representation of r, hence r^2, hence of 1 by $[1, 0, \Delta(t)]$. Therefore, the Pell equation has a non-trivial solution.

CHAPTER V

DETERMINANTS DIFFERING BY SQUARE FACTORS

Let $p(t)$ be an irreducible polynomial in $K[t]$ and $Q_{p^2(t)\Delta}$, Q_{Δ} denote the groups of classes of primitive binary quadratic forms with determinants $p^2(t)\Delta(t)$ and $\Delta(t)$ respectively. In this chapter, it is our purpose to extend the results of [5] in order to obtain a relationship between the groups $Q_{p^2(t)\Delta}$ and Q_{Δ} .

Lemma 5.0. A primitive form F having determinant $p^2(t)\Delta(t)$ primitively represents a polynomial divisible by $p^2(t)$.

PROOF: Let $F = [a(t), 2b(t), c(t)]$. If $p(t)$ divides $a(t)$, $p^2(t)$ divides $a(t)$ and $X = 1$, $Y = 0$ is a primitive representation of a polynomial $(a(t))$ divisible by $p^2(t)$. If $(a(t), p(t)) = 1$ then $(a(t), b(t), p(t)) = 1$. Let $X = -b(t)/d(t)$, $Y = a(t)/d(t)$ where $d(t) = (a(t), b(t))$. We have

$$a(t)X^2 + 2b(t)XY + c(t)Y^2 = a(t)\{-b^2(t) + a(t)c(t)\}/d^2(t)$$
$$= a(t)p^2(t)\Delta(t)/d^2(t).$$

Since $d^2(t)$ divides $a(t)\Delta(t)$, $X = -b(t)/d(t)$ and $Y = a(t)/d(t)$ is a primitive representation of a polynomial divisible by $p^2(t)$.

By lemma 5.0, every class of $Q_{p^2(t)\Delta}$ contains a form of the type

$$(1)\quad F = [p^2(t)a(t),\ 2p(t)b(t),\ c(t)].$$

Since F is primitive, the form $\emptyset F = [a(t),\ 2b(t),\ c(t)]$ is primitive and has determinant $\Delta(t)$. Define $\emptyset: Q_{p^2(t)\Delta} \longrightarrow Q_{\Delta}$ by $\emptyset(\{F\}) = \{\emptyset F\}$ where F is a form of type (1).

Theorem 5.1. $\emptyset$ is a homomorphism from $Q_{p^2(t)\Delta}$ onto Q_{Δ}.

PROOF: To show $\emptyset$ is well-defined, let $F = [p^2(t)a(t),\ 2p(t)b(t),\ c(t)]$ and $F' = [p^2(t)a'(t),\ 2p(t)b'(t),\ c'(t)]$ be equivalent primitive forms having determinant $p^2(t)\Delta(t)$ and

$$T = \begin{bmatrix} r(t), & s(t) \\ u(t), & v(t) \end{bmatrix}$$

be a unimodular transformation taking F onto F'. By the Gauss criterion,

$$p^2(t)a'(t)=p^2(t)a(t)r^2(t)+2p(t)b(t)r(t)u(t)+c(t)u^2(t)$$

$$(2)\quad p^2(t)v(t)a'(t)=p^2(t)a(t)r(t)+\{b(t)+b'(t)\}p(t)u(t)$$

$$-p^2(t)s(t)a'(t)=\{b(t)-b'(t)\}p(t)r(t)+c(t)u(t).$$

Since $(p(t),\ c(t)) = 1$, $p(t)$ divides $u(t)$. Therefore,

$$a'(t) = a(t)r^2(t)+2b(t)r(t)u(t)/p(t)+c(t)u^2(t)/p^2(t)$$

$$(3)\quad a'(t)v(t)=a(t)r(t)+\{b(t)+b'(t)\}u(t)/p(t)$$

$$-a'(t)s(t)p(t)=\{b(t)-b'(t)\}r(t)+c(t)u(t)/p(t).$$

In which case,

$$T' = \begin{bmatrix} r(t), & p(t)s(t) \\ u(t)/p(t), & v(t) \end{bmatrix}$$

is a unimodular transformation taking $\emptyset F$ onto $\emptyset F'$.

To show that $\emptyset$ is a homomorphism, let C_1 and C_2 be two classes of $Q_{p^2(t)\Delta}$. By lemma 1.4, we can find united forms $F = [p^2(t)a(t),\ 2p(t)b(t),\ 2p(t)b(t),\ c(t)a'(t)]$ in C_1 and $F' = [a'(t),\ 2p(t)b(t),\ c(t)a(t)p^2(t)]$ in C_2. We have

$$\emptyset(C_1) = \{[a(t),\ 2b(t),\ c(t)a'(t)]\} \text{ and}$$

$$\emptyset(C_1C_2) = \{[a(t)a'(t),\ 2b(t),\ c(t)]\}.$$

Since $F' \sim [c(t)a(t)p^2(t),\ -2p(t)b(t),\ a'(t)]$,

$$\emptyset(C_2) = \{[c(t)a(t),\ -2b(t),\ a'(t)]$$

$$= \{[a'(t),\ 2b(t),\ c(t)a(t)]; \text{ therefore,}$$

$$\emptyset(C_1)\emptyset(C_2) = \{[a(t)a'(t),\ 2b(t),\ c(t)]\} = \emptyset(C_1C_2).$$

Let $\{F\}$ be any class of Q_Δ with $F = [a(t),\ 2b(t),\ c(t)]$. Since F primitively represents polynomials prime to $p(t)$, we may assume $(c(t),\ p(t)) = 1$. Now $[a(t)p^2(t), 2b(t)p(t), c(t)]$ is a primitive form having determinant $p^2(t)\ \Delta(t)$. Since $\emptyset(\{[a(t)p^2(t),\ 2b(t)p(t),\ c(t)]\}) = \{F\}$, $\emptyset$ is onto.

<u>Theorem 5.2.</u> A necessary and sufficient condition for a primitive class to be in the kernel of $\emptyset$ is that it contain one of the following forms:

$$(4)\quad \begin{matrix}[p^2(t),\ 2h(t)p(t),\ h^2(t) + \Delta(t)], \text{ where} \\ p(t) \nmid h^2(t) + \Delta(t),\ |h(t)| < |p(t)|,\end{matrix}$$

or

$$(5)\quad [1,\ 0,\ p^2(t)\ \Delta(t)].$$

PROOF: If $\emptyset(\{[a(t)p^2(t), 2b(t)p(t), c(t)]\}) = \{[1, 0, \Delta(t)]\}$ then $[a(t), 2b(t), c(t)] \sim [1, 0, \Delta(t)]$, therefore there are relatively prime polynomials $r(t)$, $s(t)$ such that $1 = a(t)r^2(t) + 2b(t)r(t)s(t) + c(t)s^2(t)$. If $(p(t), r(t)) = 1$ then $r(t), p(t)s(t)$ is a primitive representation of $p^2(t)$ by $F = [a(t)p^2(t), 2b(t)p(t), c(t)]$. Hence F is equivalent to a form $F' = [p^2(t), 2h(t)p(t), h^2(t) + \Delta(t)]$. By a translation, we can reduce $h(t)$ modulo $p(t)$ so that F' is one of the forms (4). If $(p(t), r(t)) \neq 1$ then $r(t)/p(t), s(t)$ is a primitive representation of 1 by F; in which case, $[1, 0, p^2(t)\ \Delta(t)]$ is in the class containing F. Since it is apparent that any class containing one of the forms (4) or (5) maps on to the identity class of Q_Δ, the theorem follows.

Definition 5.3. Let $\pm\eta^n = \pm(f_n(t) + g_n(t)\theta)$ be the units in K_Δ having norm 1 and define the symbol ϵ to be

(6) 0 if $\eta = \pm 1$, i.e. ± 1 are the only units,

(7) ∞ if $g_n(t) \equiv 0 \bmod p(t)$ for every integer $n \neq 0$,

(8) m if $g_1(t) \neq 0$ and m is the least positive integer among the integers n for which $g_n(t) \equiv 0 \bmod p(t)$.

Theorem 5.4.

I. If $\epsilon = 0$, no form in (4) is equivalent to (5).

II. If $0 < \epsilon < \infty$, there are exactly $\epsilon - 1$ primitive forms (4) equivalent to (5).

III. If $\epsilon = \infty$, there is a unique form in (4) equivalent to (5) corresponding to each solution $f_n(t)$ $g_n(t)$, $n \neq 0$, of the Pell equation. (Accordingly, a denumerable infinity of the forms in (4) are equivalent to (5).)

PROOF: The forms $F = [1, 0, p^2(t)\,\Delta(t)]$ and $F' = [p^2(t), 2h(t)p(t), h^2(t)\,\Delta(t)]$ are equivalent if and only if there exist relatively prime polynomials $r(t)$, $g(t)$ such that

$$r^2(t) + g^2(t)p^2(t)\Delta(t) = p^2(t),$$

$$r(t) + h(t)\,p(t)g(t) \equiv 0 \bmod p^2(t), \text{ and}$$

$$-h(t)p(t)r(t) + p^2(t)\Delta(t)g(t) \equiv 0 \bmod p^2(t).$$

Since $p(t)$ must divide $r(t)$, let $r(t) = p(t)f(t)$. It follows that the above forms are equivalent if and only if $f(t)$, $g(t)$ is a solution of the Pell equation and $f(t) + h(t)g(t) \equiv 0$ modulo $p(t)$. Now $(f(t), g(t), p(t)) = 1$, hence $g(t) \equiv 0$ modulo $p(t)$. Conversely, any solution $f(t)$, $g(t)$ with $g(t) \equiv 0 \bmod p(t)$ gives rise to a polynomial $h(t)$, $|h(t)| < |p(t)|$, such that $f(t) + h(t)g(t) \equiv 0 \bmod p(t)$. Since $f^2(t) - h^2(t)g^2(t) \equiv 0 \not\equiv 1 \equiv f^2(t) + \Delta(t)g^2(t)$ modulo $p(t)$, $(h^2(t) + \Delta(t), p(t)) = 1$; thus, $[p^2(t), 2h(t)p(t), h^2(t), \Delta(t)]$ is a primitive form equivalent to $[1, 0, p^2(t)\,\Delta(t)]$.

I. If $\epsilon = 0$, the only solutions $f(t)$, $g(t)$ of the Pell equation are $f(t) = \pm 1$ and $g(t) = 0$. Therefore, no form in (4) is equivalent to (5).

II. If $0 < \epsilon < \infty$, there is a primitive form (4) equivalent to (5) corresponding to each solution $f(t)$, $g(t)$ of the Pell equation with $g(t) \equiv 0 \bmod p(t)$. Since the solutions $f(t)$, $g(t)$ and $-f(t)$, $-g(t)$ give rise to the same form in (4), we need consider only the solutions $f_n(t)$, $g_n(t)$, $n \neq 0$, given in definition 5.3. We have

$$f_n(t) \equiv f_{n-\epsilon}(t)f_\epsilon(t) + g_{n-\epsilon}(t)g_\epsilon(t)\,\Delta(t) \equiv \pm f_{n-\epsilon}(t)$$

modulo $p(t)$,

$$g_n(t) \equiv -f_{n-\epsilon}(t)g_\epsilon(t) + g_{n-\epsilon}(t)f_\epsilon(t) \equiv \pm g_{n-\epsilon}(t)$$

modulo $p(t)$.

In a similar manner, we have $f_n(t) \equiv \pm f_{n+\epsilon}(t) \bmod p(t)$ and $g_n(t) \equiv \pm g_{n+\epsilon}(t) \bmod p(t)$. It follows that we need consider only the solutions $f_n(t)$, $g_n(t)$ such that $0 < n < \epsilon$. If

$h_m(t) = h_n(t)$ for $0 < m,n < \epsilon$ then

$$\begin{aligned} f_m(t) + h_m(t)g_m(t) &\equiv f_n(t) + h_n(t)g_n(t) \\ &\equiv [f_m(t) + h_m(t)g_m(t)]f_{n-m}(t) - \\ &\qquad g_{m-n}(t)g_m(t)[h_m^2(t) + \Delta(t)] \\ &\equiv g_{m-n}(t)g_m(t)[h_m^2(t) + \Delta(t)] \\ &\equiv 0 \text{ modulo } p(t). \end{aligned}$$

Therefore, $g_{m-n}(t) \equiv 0 \bmod p(t)$ hence $m = n$. Thus, there are exaclty $\epsilon - 1$ forms in (4) equivalent to (5).

III. The proof of III follows immediately from II.

<u>Theorem 5.5.</u> Let $F = [p^2(t), 2h(t)p(t), h^2(t) + \Delta(t)]$ be a primitive form in (4) which is not in the primcipal class.

I. If $\epsilon = 0$, F is the only form in (4) equivalent to F.

II. If $0 < \epsilon < \infty$, there are exaclty ϵ forms in (4) equivalent to F.

III. If $\epsilon = \infty$, there is a unique form in (4) equivalent to F corresponding to each solution $f_n(t)$, $g_n(t)$ of the Pell equation.

PROOF: The forms F and $F_1 = [p^2(t), 2h_1(t)p(t), h_1^2(t) + \Delta(t)]$ are equivalent if and only if there exist relatively prime polynomials $r(t)$, $s(t)$ such that $p^2(t)r^2(t) + 2h(t)p(t)r(t)s(t) + \{h^2(t) + \Delta(t)\}s^2(t) = p^2(t)$, $p^2(t)r(t) + \{h(t) + h_1(t)\}p(t)s(t) \equiv 0 \bmod p^2(t)$ and $\{h(t) - h_1(t)\}p(t)r(t) + \{h^2(t) + \Delta(t)\}s(t) \equiv 0 \bmod p^2(t)$. Since $p(t)$ divides $s(t)$, let $s(t) = p(t)g(t)$ and $f(t) = r(t) + h(t)g(t)$. It follows that F and F_1 are equivalent if and only if $f^2(t) + g^2(t)\,\Delta(t) = 1$ and $h(t)f(t) + \Delta(t)g(t) \equiv h_1(t)\{f(t) - h(t(g(t)\} \bmod p(t)$. Conversely, for any solution $f(t)$, $g(t)$ of the Pell equation $f(t) - h(t)g(t) \not\equiv 0 \bmod p(t)$ since F is not in the principal class; therefore, there is a polynomial $h_1(t)$, $|h_1(t)| < |p(t)|$, such that $h(t)f(t) + \Delta(t)g(t) \equiv h_1(t)\{f(t) - h(t)g(t)\} \bmod p(t)$. The form $[p^2(t), 2h_1(t)p(t), h_1^2(t) + \Delta(t)]$ must be primitive, for if $\Delta(t) \equiv -h_1^2(t) \bmod p(t)$ then $\{h(t) - h_1(t)\}f(t) \equiv -h_1(t)\{h(t) - h_1(t)\}\, g(t) \bmod p(t)$. Therefore, $f(t) \equiv -h_1(t)g(t) \bmod p(t)$. Since $f^2(t) + g^2(t)\,\Delta(t) \equiv$

$f^2(t) - h_1^2(t)g^2(t) \equiv 1 \bmod p(t)$, $f(t)$ and $-h_1(t)g(t)$ cannot be congruent mod $p(t)$. Thus, there is a primitive form in (4) equivalent of F corresponding to each solution of the Pell equation. The remainder of the proof follows from the proof of theorem 5.4.

SELECTED BIBLIOGRAPHY

1. Artin, E. ''Quadratische Körper in Gibiete der höhen Kongruenzen,'' Mathematische Zeitschrift, vol 19 (1924), 207-246.

2. Cantor, G. ''Zwei Sätze aus der Theorie der Binary Quadratischen Formen,'' Zeitschrift für Mathematik and Physik, vol 13(1868), 259-261.

3. Gilmer, R. and Ohm, J. ''Integral Domains with Quotient Over Rings,'' Mathematic Annelen, vol 153(1964), 97-103.

4. Landau, E. Vorlesungen über Zahlentheorie Leipzig, 1927. vol. 3.

5. Pall, Gordon. ''Binary Quadratic Discriminants differing by Square Factors,'' American Journal of Mathematics, LVII(1935).

6. _____. ''Composition of Binary Quadratic Forms,'' Bulletin of the American Mathematical Society, vol. 54(1948).

7. _____. ''Representation of Discriminantal Divisors by Binary Quadratic Forms,'' (To appear).

8. Rees, D. ''On a Probelm of Zariski,'' Illinois Journal of Mathematics, vol 2(1958).

9. Van der Waerden, B. L. Modern Algebra. New York: Frederick Ungar Publishing Company, 1953. vol. 1.

10. Zariski, Oscar and Samuel, Pierre. Commutative Algebra. Princeton: D. Van Nostrand Company, Inc., 1958. vol. I.

BIOGRAPHY

Dennis Ray Estes was born on June 18, 1941, in Stradford, Oklahoma. He attended the public schools of Center, Vanoss, and Ada, Oklahoma. After graduation from high school he attended East Central State College in Ada, Oklahoma, where he received the degree of Bachelor of Science in August, 1961.

He entered Louisiana State University in September, 1961, as a Graduate Assistant and obtained The Master of Science Degree in Mathematics in August, 1963. He is currently a candidate for the degree of Doctor of Philosophy in The Department of Mathematics.

EXAMINATION AND THESIS REPORT

Candidate: Dennis Ray Estes,

Major Field: Mathematics

Title of Thesis: Classes of Binary Quadratic Forms over Polynomial Rings

Approved:

Gordon Pall
Major Professor and Chairman

Max Goodrich
Dean of the Graduate School

EXAMINING COMMITTEE:

Haskell Cohen

H. S. Butts

Ronald Bgoch

L. J. Wade

Gordon Pall

Date of Examination:

July 14, 1965