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 48108
MADDEN, Daniel Joseph, 1948-
THE EXPONENT OF CLASS GROUPS IN CONGRUENCE
FUNCTION FIELDS.
The Ohio State University, Ph.D., 1975
Mathematics

Xerox University Microfilms, Ann Arbor, Michigan 48106

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED.
THE EXPONENT OF CLASS GROUPS
IN CONGRUENCE FUNCTION FIELDS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

Daniel J. Madden, B.A., M.S.

* * * * *

The Ohio State University
1975

Reading Committee:
Manohar L. Madan
James R. Leitzel
Robert Gold

Approved By
Manohar L. Madan
Advisor
Department of Mathematics
ACKNOWLEDGMENTS

My thanks go first to my parents for their support and encouragement. I would also like to thank my advisor Professor Manohar Madan, not only for his time and his many suggestions, but also for his friendship and understanding.
VITA

July 29, 1948 .................. Born - Philadelphia, Pennsylvania

1970 ....................... B.A., La Salle College, Philadelphia, Pennsylvania

1970-1971 ..................... Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

1971 ......................... M.S., The Ohio State University, Columbus, Ohio

1971-1975 ..................... Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

FIELDS OF STUDY

Major Field: Mathematics

Studies in Number Theory ........ Professor M. L. Madan, Professor A. C. Woods, Professor B. B. Divis

Studies in Algebra ............... Professor J. C. Ferrar
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>ii</td>
</tr>
<tr>
<td>Vita</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Chapter</td>
<td></td>
</tr>
<tr>
<td>I. The General Theory of Congruence Function Fields</td>
<td>6</td>
</tr>
<tr>
<td>- Primes in Congruence Fields</td>
<td>6</td>
</tr>
<tr>
<td>- Divisors and the Riemann-Roch Theorem</td>
<td>9</td>
</tr>
<tr>
<td>- Extensions of Congruence Function Fields</td>
<td>13</td>
</tr>
<tr>
<td>- The Noninvariant Theory</td>
<td>17</td>
</tr>
<tr>
<td>- The Zeta Function</td>
<td>19</td>
</tr>
<tr>
<td>II. Cyclic Extensions of ( k(x) ) of Prime Power Degree</td>
<td>21</td>
</tr>
<tr>
<td>- For Primes Other Than the Characteristic</td>
<td></td>
</tr>
<tr>
<td>- Poles of Integral Functions</td>
<td>24</td>
</tr>
<tr>
<td>- The Main Result in a Special Case</td>
<td>36</td>
</tr>
<tr>
<td>III. Artin-Schreier Extensions and the Main Result</td>
<td>43</td>
</tr>
<tr>
<td>- The Main Result</td>
<td>58</td>
</tr>
<tr>
<td>IV. Quadratic Extensions with Exponent Two</td>
<td>66</td>
</tr>
<tr>
<td>- Introduction</td>
<td>66</td>
</tr>
<tr>
<td>- Norms of Integral Elements in Imaginary Extensions</td>
<td>69</td>
</tr>
<tr>
<td>- Proof of Theorem 16</td>
<td>76</td>
</tr>
<tr>
<td>Bibliography</td>
<td>85</td>
</tr>
</tbody>
</table>

iv
INTRODUCTION

For a finitely generated extension $K$ of a field $k$ with transcendence degree 1, the divisor class group (which will be introduced in Chapter 1) is infinite and the null class group (the subgroup of divisors of degree 0) is, in general, also infinite. However, if $k$ is finite, it is a consequence of the Riemann-Roch theorem that the number of classes of degree 0 is finite. In this, the case of congruence function fields, the order of the null class group is called the class number of the field. This null class group is analogous to the ideal class group in the case of algebraic number fields, and it plays an important role in all algebraic, arithmetic, and geometric studies of congruence function fields.

In the theory of congruence function fields, the "Riemann Hypothesis" plays an essential role. This "hypothesis" determines the real part of the zeros of the zeta function of a congruence function field. It was proved in complete generality by Andre Weil [15] after H. Hasse [8] had given a proof in the elliptic case. This result gives bounds on the class number of a congruence function field; however, while there are bounds on the order of the null class group, not much is known about its structure. The purpose here is to study the exponent of this group for congruence
function fields of a particular type. These are fields $K$ which are abelian extensions of $k(x)$, the rational function field over $k$, for which $\text{GAL}(K/k(x))$ has order $n_0 p^{r_0}$, where $p$ is the characteristic of the field and $n_0$ is relatively prime to $p$; and for which the $p$-primary part of $\text{GAL}(K/k(x))$ is elementary abelian. The main object of this paper is to give a lower bound for the exponent of the null class group of a field of this type. A consequence of this will be that for a fixed finite field $k$ and a fixed degree $n_0 p^{r_0}$, the exponent will approach infinity as the genus of the field goes to infinity.

It is well-known that there is a strong similarity between the theory of congruence function fields and the theory of algebraic number fields; the two together form the class of global fields, and class field theory holds for them. It would be interesting to obtain analogous results for some special class of algebraic number fields. No such definitive result is known; for the class of imaginary quadratic number fields, H. Heilbronn [9] proved that the class number becomes infinitely large with the absolute value of the discriminant. In fact, C. L. Siegel [14] proved that for imaginary quadratic fields,

$$\lim_{|d| \to \infty} \frac{\log h}{\log \sqrt{|d|}} = 1$$

as $|d|$ tends to infinity (where $h$ is the class number and $d$ is the discriminant). Attempting to improve upon this result,
D. Boyd and H. Kisilevsky [2] and P. Weinberger [16] proved that the exponent of the class group becomes infinitely large with the absolute value of the discriminant if one assumes the truth of the extended Riemann Hypothesis. This is analogous to the result of this work because the Hurwitz genus formula for extensions of fixed degree gives that the genus grows infinitely large with the degree of the discriminant.

Chapter I of this paper is mostly expository. The object here is to set the notation, to introduce the fundamental concepts of the theory of congruence function fields, and to state the main results of the theory that are used in the main body of the paper. The restriction that the constant field is finite is unnecessary for many of the statements in this chapter, but this assumption is made for the sake of uniformity. Chapter II deals with cyclic extensions of $k(x)$ of prime power degree for primes other than the characteristic of the field; Chapter III deals with Artin-Schreier extensions of $k(x)$, i.e., extensions of degree $p$, where $p$ is the characteristic. Also in Chapter III the results of Chapter II and the first part of Chapter III are combined to give the main result. This is accomplished by studying the relationship between the null class group of a field whose Galois group is the direct product of two groups and the null class groups of the two subfields associated with the factors. Chapter IV contains an application of those results to quadratic extensions.
of \( k(x) \).

In his dissertation Emil Artin [1] developed the arithmetic and analytic theory of quadratic extensions \( K \) of the rational function field \( k(x) \), where \( k \) is a prime field of odd characteristic. One of his results concerns the problem of classifying all imaginary quadratic extensions for which there is one ideal class per Geschlecht, i.e., the ideal class group has exponent 2. Artin showed that there were only finitely many such fields. In particular, he showed that, if \( K \) is such a quadratic extension of \( k(x) \) in which the infinite prime of \( k(x) \) ramifies and in which the ideal class group has exponent 2, then the order of the field of constants must be 3, 5 or 7 and that (in the terminology of this paper) the genus of \( K \) is at most 9724, 9 and 13 respectively. His methods give larger bounds in these three cases when the infinite prime of \( k(x) \) is inert in \( K \).

Although the methods developed in this paper can be used in either case, for the sake of simplicity they are applied only to the case where the infinite prime ramifies. In this paper it is shown that there are only finitely many imaginary quadratic extensions of \( k(x) \) in which the infinite prime of \( k(x) \) ramifies and which have ideal class exponent 2. In fact, it is shown that the order of the constant field is necessarily 2, 3, 4, 5, 7, or 9 and that the genus is at most 8, 4, 2, 2, 1 and 1, respectively. In the case where the infinite prime is inert, these methods yield
bounds on the genus which are roughly double those in the ramified case.

Finally, while the methods and results of this paper are completely arithmetic and algebraic, there is a natural geometric interpretation of the results. If $K$ is a congruence function field over the field of constants $k$, let $\overline{K}$ be the constant field extension of $K$ which has the algebraic closure $\overline{k}$ of $k$ as its field of constants. There is a one-to-one morphism from the Jacobian Variety of $\overline{K}$ onto the divisor classes of degree 0 of $\overline{K}$. Through this morphism there is a one-to-one morphism from the $k$-rational points on the variety onto the null class group of $K$. 
CHAPTER I

THE GENERAL THEORY OF CONGRUENCE FUNCTION FIELDS

The object of this chapter is to set the notation, to introduce

the fundamental concepts of the theory of congruence function

fields, and to state the main results of the theory that are used

in the main body of the paper. Let $k$ be a finite field with

$q$ elements, and let $K$ be a finitely generated extension of $k$

with transcendence degree $1$. The field $K$ is then called a

congruence function field defined over $k$. The set $k'$ of all

elements of $K$ which are algebraic over $k$ is a subfield which

is algebraically closed in $K$. Throughout this work it is

assumed, unless stated otherwise, that $k = k'$, i.e., that $k$ is

the exact field of constants of $K$. If $x$ is an element of $k$

which is transcendental over $k$, then $K$ is a finite extension of

$k(x)$. The field $k$ is perfect, and so, by a theorem of F. K.

Schmidt [see 13, pp. 1-3], there exists a transcendental element $x$

such that $K/k(x)$ is separable. In this case the theorem of the

primitive elements gives $K = k(x,y)$ for some $y \in K$.

Primes in Congruence Fields

In order to develop an arithmetic theory for congruence function
fields, it is necessary to introduce the notion of a prime. To that purpose a normed valuation is defined.

**Definition:** A normed valuation on the congruence function field $K/k$ is a map $v$ from the multiplicative subgroup $K^*$ of $K$ onto the integers $\mathbb{Z}$ satisfying:

1. For $a, b \in K^*$, $v(ab) = v(a) + v(b)$,
2. For $a, b \in K^*$, $v(a + b) \geq \min\{v(a), v(b)\}$,
3. There exists an $a \in K$ such that $v(a) = 1$,
4. For all $a \in k$, $v(a) = 0$.

It is possible to extend a valuation $v$ to the whole field $K$ by assigning $v(0) = \infty$ and by giving the usual arithmetic to the set $\mathbb{Z} \cup \{\infty\}$. This will preserve the four conditions of the definition. Also, there is an easy consequence of the definition which strengthens condition 2; if $v(a) < v(b)$, then

$$v(a + b) = \min\{v(a), v(b)\} = v(a).$$

For a normed valuation $v$, let $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$. Then $\mathcal{O}_v$ is a ring contained in $K$ and is called the valuation ring of $v$; $\mathcal{O}_v$ contains a unique maximal ideal, $I_v = \{x \in K \mid v(x) > 0\}$. The residue field $\mathcal{O}_v/I_v$ is a finite extension of an isomorphic copy of $k$. There is a correspondence between valuations, valuation rings, and places of a congruence function field [see 5, pp. 1-19]. From this correspondence
the places can be considered as the primes of the field. It is sufficient, in this paper, to assume that to each normed valuation of a congruence function field, there is exactly one prime divisor of \( K \). The degree of the extension \( \mathbb{Q}_v / \mathbb{I}_v \) over the isomorphic copy of \( k \) is called the degree of the prime divisor associated with the valuation \( v \).

The rational function field over \( k \) in one variable is a congruence function field. Each element \( f(x) \) in \( k(x) \) can be written uniquely as a product of prime polynomials from \( k[x] \), the polynomial ring:

\[
f(x) = \prod p(x)^{r_p(x)}, \text{ where } r_p(x) \in \mathbb{Z}
\]

and where the product is taken over all prime polynomials of \( k[x] \). It can be easily shown that there are only two types of normed valuations on \( k(x) \), and that they are:

1. valuations associated with prime polynomials, i.e.,

\[
\nu_p(x)(f(x)) = r_p(x).
\]

The degree of the prime divisor associated with \( \nu_p(x) \) is the polynomial degree of \( p(x) \).

2. The "infinite" valuation,

\[
\nu_{1/\infty}(f(x)) = -\deg f(x).
\]
The prime divisor associated with this valuation has degree 1.

Every congruence function field can be considered as a finite extension of a rational function field, and its prime divisors are then extensions of the prime divisors of this subfield.

Divisors and the Riemann-Roch Theorem

Let $D(K)$ be the free group formed on the prime divisors of $K$. The elements of this group are called the divisors of $K$, and $D(K)$ is called the divisor group. If $\mathcal{U} \in D(K)$, then

$$\mathcal{U} = \prod_{p} v_p(\mathcal{U}), \quad v_p(\mathcal{U}) \in \mathbb{Z},$$

and where the product is taken over all prime divisors $p$ of $K$. A divisor is integral if $v_p(\mathcal{U}) \geq 0$ for all $p$; $\mathcal{U}$ divides $\mathcal{V}$ if $\mathcal{U} \mathcal{V}^{-1}$ is an integral divisor. Now, since $D(K)$ is a free group, $v_p(\mathcal{U}) = 0$ for all but finitely many primes $p$. Thus it is possible to define the degree of a divisor by:

$$\deg_K(\mathcal{U}) = \sum v_p(\mathcal{U}) \deg_K(p),$$

where the sum is taken over all prime divisors of $K$. It is clear from this definition that

$$\deg_K(\mathcal{U} \mathcal{V}) = \deg_K \mathcal{U} + \deg_K \mathcal{V},$$

and, therefore, that the set $D_0(K)$ of all divisors of degree 0 is a subgroup of $D(K)$.

If $x \in K$, it can be shown that $v_p(x) = 0$ for all but
finitely many prime divisors \( p \). Then to each element \( x \in K \), there is a divisor in \( D(K) \) given by:

\[
(x) = \prod p^{v_p(x)}.
\]

This divisor can be further decomposed into the numerator \( \mathfrak{g}_x \) and the denominator \( \mathfrak{r}_x \) by:

\[
\mathfrak{g}_x = \prod_{v_p(x) > 0} p^{v_p(x)} \quad \text{and} \quad \mathfrak{r}_x = \prod_{v_p(x) < 0} p^{-v_p(x)}.
\]

There is a well-known generalization of the theorem on the equality of the number of poles and of zeros of an algebraic function over complex numbers.

**Theorem:** If \( x \in K \) and \( x \notin k \), then

\[
[K: k(x)] = \deg_K \mathfrak{g}_x = \deg_K \mathfrak{r}_x,
\]

and consequently, \( \deg(x) = 0 \) for all \( x \in K \).

Let \( E(K) = \{(x) \in D(K) \mid x \in K\} \) be the group of principal divisors of \( K \). By the previous theorem, \( E(K) \) is a subgroup of \( D_0(K) \). This leads to the two main groups of the arithmetic theory of congruence function fields. Let the divisor class group, \( C(K) \), be the factor group \( D(K)/E(K) \); and the null class group, \( C_0(K) \), be \( D_0(K)/E(K) \). Since principal divisors have degree 0, the degree of a class of \( C(K) \) is well-defined, and \( C_0(K) \) can be
characterized as the classes of degree zero.

For any divisor \( \mathfrak{m} \in D(K) \), the set
\[ L(\mathfrak{m}) = \{ x \in K \mid \mathfrak{m} \text{ divides } (x) \} \]
is a finite dimensional vector space over \( k \); let \( l(\mathfrak{m}) \) denote the dimension of this space.

It can be easily seen that if \( \mathfrak{m} \) and \( \mathfrak{m}' \) are divisors which are in the same class, then \( l(\mathfrak{m}) = l(\mathfrak{m}') \). There is a well-defined dimension of a class of divisors; the dimension of a class \( C \) will be denoted by
\[ N(C) = l(\mathfrak{m}^{-1}) \text{, where } \mathfrak{m} \in C. \]

There is another characterization of the dimension of a class \( C \); it is the maximum number of linearly independent integral divisors \( \mathfrak{m}_1 \) in \( C \). If \( \mathfrak{m} \) is any element of \( C \), then the divisors \( \mathfrak{m}_1 \) in \( C \) are linearly independent if the elements of \( K \) associated with the principal divisors \( \mathfrak{m}_1 \mathfrak{m}^{-1} \) are linearly independent over \( k \).

This leads to one of the most useful results in the theory of congruence function fields, the Riemann-Roch theorem.

**Theorem:** If \( K \) is a congruence function field over \( k \), a finite field, then there exists an integer \( G \geq 0 \) and a divisor class \( W \), such that, for all classes \( C \in C(K) \),
\[ N(C) = \deg_K(C) - G + 1 + N(W^{-1}). \]

\( G \) is called the genus of the field, and \( W \) is called the canonical class (or the class of differentials).
A number of important results follow immediately from this theorem.

**Corollary 1:** If \( \deg C < 0 \), or \( \deg C = 0 \) and \( C \neq E \), then \( N(C) = 0 \).

This follows from the alternate interpretation of \( N(C) \); for, if \( N(C) > 0 \), there must be an integral divisor in the class \( C \). An integral divisor must have degree greater than or equal to zero, and can have degree zero only if it is the null divisor.

**Corollary 2:** If \( \deg(C) > 2G - 2 \) or \( \deg C = 2G - 2 \) and \( C \neq W \), then

\[
N(C) = \deg C - G + 1.
\]

This is just an application of Corollary 1 to the class \( W^{c-1} \); for, \( N(E) = 1 \) and \( \deg E = 0 \) implies \( N(W) = G \), and, therefore, \( \deg W = 2G - 2 \). It is in this form that the Riemann-Roch theorem will be used in this paper.

**Corollary 3:** The order of \( C_o(K) \) is a finite number;

\[
h = |C_o(K)|
\]

is called the class number of the field \( K \).

This is a consequence of the fact that there are only finitely many primes of degree \( m \) or less for any fixed number \( m \). For, if \( E \) is any integral divisor of \( K \) with degree greater than \( 0 \), then for any class \( C \) of degree \( 0 \),
\[ N(C \mathfrak{W}) \geq \deg(\mathfrak{W}) - G + 1 \geq 1, \]

where \( C \mathfrak{W} \) denotes the product of \( C \) and the class to which \( \mathfrak{W} \) belongs. Thus \( C \mathfrak{W} \) contains an integral divisor \( \mathfrak{B} \) with \( \deg \mathfrak{B} = \deg(C \mathfrak{W}) = \deg \mathfrak{W} \). There are only finitely many such \( \mathfrak{B} \), so there can be at most finitely many classes of degree 0.

**Extensions of Congruence Function Fields**

**Definition**: Let \( L \) and \( K \) be congruence function fields over the constant fields \( l \) and \( k \) respectively. Then \( L/l \) is an extension of \( K/k \) if \( K \subseteq L \) and \( K \cap l = k \).

An extension \( L/l \) over \( K/k \) is a constant field extension if \( L \) is the composite extension of \( K \) and \( l \); when \( [L:K] \) is finite, this is equivalent to \( [L:K] = [l:k] \). The extension is geometric when the constant field is unchanged in the extension; that is, \( l = k \). In this paper all extensions will be assumed to be finite and separable unless stated otherwise.

If \( \mathfrak{P} \) is a prime of \( L \), then the set \( v_{\mathfrak{P}}(K) \) is an additive subgroup of \( \mathbb{Z} \). Thus \( v_{\mathfrak{P}}(K) = e_{\mathfrak{P}} \mathbb{Z} \), for some integer \( e_{\mathfrak{P}} \).

\((e_{\mathfrak{P}} \neq 0 \text{ since the extension is assumed to be finite.})\) This gives a valuation on \( K \) defined by

\[ v_{\mathfrak{P}}(x) = \frac{1}{e_{\mathfrak{P}}} v_{\mathfrak{P}}(x). \]

The prime \( p \) of \( K \) associated with this valuation is said to be under \( \mathfrak{P} \) in \( K \), and \( e_{\mathfrak{P}} \) is called the ramification index of \( \mathfrak{P} \).
over $K$. It can be shown that the field $\mathcal{O}_\mathfrak{P}/I_\mathfrak{P}$ is a finite extension of an isomorphic copy of $\mathcal{O}_p/I_p$. The degree of this extension is the relative degree of $\mathfrak{P}$ over $K$ and is denoted by $\deg_{L/K}(\mathfrak{P})$. The connection between the degree of a prime $\mathfrak{P}$ of $L$ and the degree of the prime $p$ under it in $K$ is given by the equation

$$\deg_L(\mathfrak{P})[l:k] = \deg_{L/K}(\mathfrak{P}) \deg_K(p).$$

There are only finitely many primes of $L$ that lie over one fixed prime of $K$. If $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are all the primes of $L$ over a fixed prime $p$ of $K$, then

$$[L:K] = \sum_{i=1}^{g} \deg_{L/K}(\mathfrak{P}_i) e_{\mathfrak{P}_i}.$$  

Further, if $L$ is a normal extension of $K$, the Galois group is transitive on the primes $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ through the action given by

$$v_\sigma(\mathfrak{P})(x) = v_\mathfrak{P}(\sigma(x)).$$

A consequence of this is that, in a normal extension, all the primes above a fixed prime of $K$ have the same ramification index and the same relative degree. Also this action can be extended linearly to define an action on the whole group $D(K)$.

There is an injection of $D(K)$ into $D(L)$ defined on the primes by
where $p_1, p_2, \ldots, p_g$ are all the primes of $L$ over $p$. Throughout this paper $D(K)$ will be identified through this injection with a subgroup of $D(L)$. In the case of normal extensions, the action of $\text{GAL}(L/K)$ on $D(L)$ can be used to define a norm map;

$$N(u) = \prod_{\sigma \in \text{GAL}(L/K)} \sigma(u).$$

This norm is a group homomorphism of $D(L)$ to $D(K)$.

The injection of $D(K)$ into $D(L)$ induces, in a canonical way, a homomorphism of $C(K)$ into $C(L)$ and, consequently, of $C^0(K)$ into $C^0(L)$. This homomorphism, called the conorm, plays an important part in the study of algebraic number fields as well as congruence function fields. While in the case of algebraic number fields the results in this direction are incomplete, in congruence function fields the kernel of this map can be characterized [see 12, p. 68]. In fact,

$$|\ker(\text{conorm})| \text{ divides } [K:L].$$

If $L/l$ is a Galois extension of $K/k$, the decomposition group $G_{p_l}$ and the ramification groups $G_i$, $i = 0, 1, 2, \ldots$ of a prime $p$ of $L$ are given by:
$G_{-1}(\mathfrak{p}) = \{ \sigma \in \text{GAL}(L/K) | \sigma(\mathfrak{p}) = \mathfrak{p} \}$,

$G_1(\mathfrak{p}) = \{ \sigma \in \text{GAL}(L/K) | \sigma(\pi) = \pi(\text{mod } \mathfrak{p}^{1+1}) \}$,

where $\pi$ is an element of $L$ with $v_{\mathfrak{p}}(\pi) = 1$. Then

$$G \geq G_{-1}(\mathfrak{p}) \geq G_0(\mathfrak{p}) \geq G_1(\mathfrak{p}) \geq \cdots \geq G_m(\mathfrak{p}) \geq \cdots$$

The prime $\mathfrak{p}$ is tamely ramified if $G_1(\mathfrak{p}) = \{1\}$ and is wildly ramified otherwise. For normal extensions these groups can be used to define the different, $\delta_{L/K}$, of $L$ over $K$:

$$\delta_{L/K} = \prod \mathfrak{p}^{d(\mathfrak{p})}, \text{ where } d(\mathfrak{p}) = \sum_{i=0}^{\infty} (|G_i| - 1).$$

It is clear by this definition that a prime divides the different if and only if it is ramified. There are only finitely many ramified primes in a finite extension; thus, $\delta_{L/K} \in D(L)$, and is an integral divisor. The discriminant $\Delta_{L/K}$ of the extension $L$ over $K$ is the norm of the different: $\Delta_{L/K} \in D(K)$.

Another important result in the theory of congruence function fields is the:

**Hurwitz Genus Formula**

If $L/k$, with genus $G_L$, is a finite, separable, geometric extension of $K/k$, with genus $G_K$, then

$$2G_L - 2 = [L:K](2G_K - 2) + \deg_L(\delta_{L/K})$$

In the context of this formula, it is useful to note that
Extensions of the field of constants of a congruence function field play an important role even if the extension under study is a geometric extension. The importance of constant field extensions is due in a large part to the following:

**Theorem:** If $L/k$ is a constant field extension of $K/k$ of finite degree, then:

1. $G_K = G_L$, i.e., the genus is unchanged in a constant field extension,
2. $N_K(\mathfrak{m}) = N_L(\mathfrak{m})$, for any divisor $\mathfrak{m}$ of $K$,
3. $\deg_K(\mathfrak{m}) = \deg_L(\mathfrak{m})$, for any divisor $\mathfrak{m}$ of $K$.

The decomposition of a prime in a constant field extension is given by:

**Theorem:** If $L/k$ is a constant field extension of $K/k$ of degree $n$, then for any prime $p$ of $K$:

1. $p$ is unramified,
2. there are exactly $(n, \deg_K(p))$ primes above $p$ in $L$.

**The Noninvariant Theory**

Let $K$ be a congruence function field with constant field $k$. If $x$ is an element of $K$ such that $K$ is a separable extension of $k(x)$, then the results of the previous section can be applied. This approach is particularly interesting because the genus of a rational function field is $0$, and because the primes of $k(x)$ are
so easily characterized. There is, however, another approach to this type of extension. The polynomial ring \( k[x] \) is a unique factorization domain, and so there is an arithmetic theory of ideals in finite extensions of \( k(x) \). While this approach parallels the invariant theory given above, it does not take into account the prime divisors of \( k(x) \) which lie over the infinite prime of \( k(x) \). Thus the ideal theory of congruence function fields depends upon \( x \).

Let \( \mathfrak{O}(K) \) be the integral closure of \( k[x] \) in \( K \); \( \mathfrak{O}(K) \) is a Dedekind domain. Let \( \mathfrak{J}(K) \) be the group of fractional ideals of \( \mathfrak{O} \); since prime ideals of \( \mathfrak{O} \) give rise to valuations on \( K \), there is a natural homomorphism of \( \mathfrak{J}(K) \) into \( D(K) \), which will be denoted by \( I \mapsto (I) \). This is an isomorphism of \( \mathfrak{J}(K) \) onto the subgroup of \( D(K) \) containing all divisors relatively prime to the infinite prime of \( k(x) \). Let \( \mathfrak{S}(K) \) be the principal ideals of \( K \), and \( \mathfrak{C}(K) = \mathfrak{J}(K)/\mathfrak{S}(K) \) be the ideal class group of \( K \). The order \( h_x \) of \( \mathfrak{C}(K) \) is finite and is called the ideal class number of \( K \). F. K. Schmidt [13] gave a connection between the class number of \( K \) and the ideal class number.

**Theorem:** With the notation as above:

\[ h_x r_x = h n_x, \]

where \( r_x = |D_{o}(x)/E(x)| \) and \( n_x \) is the greatest common divisor of the degrees of the primes in \( K \) above the infinite prime of \( k(x) \). Here \( D_{o}(x) \) is the group of divisors of
K of degree 0 which are made up only of primes above the infinite prime of \( k(x) \); \( E(x) = D_0(x) \cap E(K) \).

In the theory of Dedekind rings, the different and the discriminant of extensions are defined. These ideals have a very close relationship with the divisors defined in Section 2. If \( \delta_x \) is the ideal different of the extension \( K \) over \( k(x) \), and \( \delta \) the divisor different, then

\[ (\delta_x)^\mathbb{U} = \delta, \text{ where } \mathbb{U} \text{ is that part of } \delta \text{ made up of primes above } p_{1/x} \text{ the infinite prime of } k(x). \]

Similarly, if \( \Delta_x \) is the ideal discriminant of the extension,

\[ (\Delta_x)^{\lambda_\infty} p_{1/x}^{\lambda_\infty} = \Delta, \text{ for suitable } \lambda_\infty \in \mathbb{Z}. \]

The Zeta Function

The zeta function of a congruence function field \( K \) over the constant field \( k \) is a function of a complex variable \( s \) and is defined by the equation:

\[ \zeta(s,K) = \sum \frac{1}{\mathfrak{N}(\mathbb{U})^s}, \text{ where } \mathfrak{N}(\mathbb{U}) = q^{\deg_K(\mathbb{U})}, \]

where the sum is taken over all integral divisors \( \mathbb{U} \) of \( K \). This series converges for all complex \( s \) with \( \Re(s) > 1 \). Like the Riemann zeta function, \( \zeta(s,k) \) has a simple pole at \( s = 1 \), but does have an analytic continuation to the rest of the complex plane. The zeta function of \( K \) can also be written as
where \( L(u) \) is a polynomial with rational integral coefficients.

In fact,

\[
L(u) = \frac{2G}{\prod_{i=0}^{2G} a_i^i} = \prod_{i=1}^{2G} (1 - \omega_i u)
\]

where \( a_{2G-i} = q^{G-i}a_i \), for \( i > G \). Also \( a_0 = 1 \), and

\[
a_1 = N_1 - (1 + q)
\]

where \( N_1 \) is the number of primes of degree 1 of \( K \). The zeta function in this form has a very strong connection with the arithmetic theory of the field; in fact \( L(1) = h \).

The Riemann hypothesis as applied to this zeta function states that all the zeros of \( \zeta(s,K) \) with real part greater than zero have real part equal to \( 1/2 \). This is equivalent to the two statements:

1. \( |a_1| = |N_1 - (1 + q)| \leq 2G\sqrt{q} \)
2. \( |\omega_1| = q^{1/2} \)

Andre Weil [15] proved that the Riemann hypothesis is valid for congruence function fields. A consequence of this is that there are bounds on the class number, \( h \), of \( K \):

\[
(1 - q^{1/2})^{2G} \leq h = L(1) \leq (1 + q^{1/2})^{2G}.
\]
CHAPTER II

CYCLIC EXTENSIONS OF \( k(x) \) OF PRIME POWER DEGREE

FOR PRIMES OTHER THAN THE CHARACTERISTIC

Let \( k \) be a finite field with \( q \) elements, and let \( Z \) be a cyclic extension of \( k(x) \) of degree \( p^n \), where \( p \) is a prime other than the characteristic. Then \( Z \) is a congruence function field over the exact field of constants \( k \). Further, if \( p^n \) divides \( q - 1 \), then \( k \) contains the \( p^n \)-th roots of \( 1 \). This type of extension, a cyclic Kummer extension\(^*\), can be realized as \( Z = k(x, y) \) where

\[
y^{p^n} = f(x) = \prod_{i=1}^{\ell} p_i(x)^{\lambda_i}, \quad \lambda_i \in \mathbb{Z}.
\]

However, if \( \lambda_i < 0 \) or \( \lambda_i \geq p^n \), then a transformation

\[
y' = y \cdot p_i(x)^{\gamma}, \quad \text{for a suitable } \gamma \in \mathbb{Z},
\]

can be used to put this generating equation into a standard form in which

\(^*\) Hasse's paper [7] contains a very clear presentation of the arithmetic theory of Kummer extensions and of Artin-Schreier extensions. For the convenience of the reader and in order to fix notation, the principal results about the decomposition of primes in these extensions are stated here and in the beginning of Chapter III.
The decomposition of a prime divisor of $k(x)$ in $\mathbb{Z}$ can be easily computed using the following two theorems:

**Theorem 1**: If, with the notation as above, $\mathbb{Z} = k(x,y)$, where the generating equation is in standard form, then for a prime $p(x)$ which does not divide $f(x)$:

1. The prime divisor of $k(x)$ associated with $p(x)$ is unramified.

2. If the polynomial $y^p - f(x)$ modulo $p(x)$ decomposes into $g$ factors each of degree $f$ (this is the only possible type of decomposition since $k$ contains the $p^n$-th roots of 1), then the prime $p_p(x)$ of $k(x)$, associated with $p(x)$, decomposes in $\mathbb{Z}$ as

$$p_p(x) = \mathcal{T}_1 \mathcal{T}_2 \ldots \mathcal{T}_g$$

where $\deg_{\mathbb{Z}/k(x)}(\mathcal{T}_1) = f$.

**Theorem 2**: With the notation as above, if $p_1(x)$ is a prime polynomial which divides $f(x)$, then the prime $p_{p_1}(x)$ of $k(x)$ associated with $p_1(x)$:

1. ramifies in $\mathbb{Z}$ and has ramification index $e_1$, where

$$e_1 = \frac{p^n}{(p^n, x^n)}$$

2. is unramified in the subfield $\mathbb{Z}' = k(x, y^{e_1})$. 

$$0 < \lambda_i < p^n, \quad i = 1, 2, \ldots, \ell.$$
(3) Further, if \( \mathfrak{p}_1 \) is any prime of \( Z \) which lies over \( p_{p_1}(x) \), the contribution of \( p_1 \) to the different of \( Z/k(x) \) is

\[
\delta(p_1) = \frac{e_1 - 1}{e_1}.
\]

The decomposition of a ramified prime \( p_{p_1}(x) \) of \( k(x) \) can be completely determined by applying Theorem 1 to the extension \( Z' = k(x, y^{e_1}) \) over \( k(x) \).

There is, of course, one prime of \( k(x) \) which is not explicitly covered in these two theorems. However, the decomposition of this infinite prime is exactly the decomposition of the prime associated with \( x \) in the extension generated by the equation

\[
y^p = f\left(\frac{1}{x}\right).
\]

The extension generated by this equation is \( Z \), and, for this reason, the infinite prime of \( k(x) \) is often called the prime divisor associated with \( \frac{1}{x} \). It is useful, however, to give the decomposition of this prime directly from the standard form of the generating equation.

**Corollary:** With the notation as above, let \( \lambda_\infty = -\deg f(x) \),

\[
e_\infty = \frac{n}{(p^n, \lambda_\infty)}.
\]
(1) If $e_\infty = 1$, then $\mathfrak{p}_{1/x}$ is unramified in $\mathbb{Z}$, and its decomposition into primes is determined by the decomposition of the polynomial $y^p - \alpha$ in $k[x]$, where $\alpha$ is the leading coefficient of $f(x)$.

(2) If $e_\infty > 1$, then $\mathfrak{p}_{1/x}$ is ramified in $\mathbb{Z}$ with ramification index $e_\infty$; the contribution to the different of any prime $\mathfrak{p}_\infty$ of $\mathbb{Z}$ over $\mathfrak{p}_{1/x}$ is given by

$$\delta(\mathfrak{p}_\infty) = \frac{e_\infty - 1}{\mathfrak{p}_\infty}.$$

The precise decomposition of $\mathfrak{p}_{1/x}$ is obtained by considering the field $Z' = k(x^e_\infty)$ in which $\mathfrak{p}_{1/x}$ is unramified.

**Poles of Integral Functions**

The object now is to show that a primitive integral element of a cyclic extension $Z/k(x)$ of degree $p^n$ must have some infinite prime as a pole of large order if the genus of $Z$ is large. To that end a special type of integral basis is constructed for cyclic Kummer extensions of prime power degree which can be used to determine the values of an integral element at an infinite valuation in terms of the coefficients in its representation.

With the notation of the previous section, let $\mathfrak{G}$ be the integral closure of $k[x]$ in $Z$. A basis of $Z$ over $k(x)$ is called an integral basis if it is also a basis of the module $\mathfrak{G}$ over $k[x]$. If $B = \{\theta_1, \theta_2, \ldots, \theta_p\}$ is a basis of $Z$ in
which every element $\theta_i$ is integral over $k[x]$, then the ring

$$\mathfrak{O}(B) = k[x]^n \oplus \cdots \oplus k[x] \oplus k[x] \otimes \cdots \otimes k[x] \theta_1 \otimes \cdots \otimes k[x] \theta_n$$

is called the order generated by the basis $B$. Clearly $\mathfrak{O}(B) \subseteq \mathfrak{O}$; and so $\mathfrak{O}$ is the maximum order of $Z$ over $k[x]$. The discriminant of the order $\mathfrak{O}(B)$ (or of the basis $B$) is given by

$$\Delta_x(B) = \det(S(\theta_i \theta_j)),$$

where $S$ is the trace of $Z$ to $k(x)$. Thus $\Delta_x(B) = \Delta_x$ (the Dedekind discriminant of the field) if and only if $B$ is an integral basis. Also, for any basis $B$, $(\Delta_x(B)/\Delta_x)^{1/2}$ is an element of $k[x]$ called the index of $\mathfrak{O}(B)$ in $\mathfrak{O}$.

A special type of integral basis is now constructed for cyclic Kummer extensions of $k(x)$ of prime power degree.

Theorem 3: Let $Z$ be a cyclic geometric extension of $k(x)$ of degree $p^n$, where $p$ is not the characteristic of $k$ and where $k$ contains the $p^n$-th roots of 1. Further, let $Z = k(x, y)$ where

$$y^{p^n} = f(x) = \prod_{i=1}^{\ell} p_i(x)^{\lambda_i}, \quad 0 < \lambda_i < p^n, \quad i = 1, 2, \ldots, \ell.$$

Then $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{p^n-1}\}$ is an integral basis of $Z$ over $k(x)$, where
\[ \theta_j = \frac{y^j}{\prod_{i=1}^{g} p_i(x)^{r_{ij}}} \text{, for } r_{ij} = \left\lfloor \frac{j \lambda_i}{p^n} \right\rfloor, \text{ the greatest integer not exceeding } \frac{j \lambda_i}{p^n}. \]

Proof: If \( p_i \) is any prime of \( Z \) lying over the prime divisor of \( k(x) \) associated with \( p_i(x) \), then

\[ v_{p_i}(\theta_j) = v_{p_i}\left( \frac{y^j}{\prod_{h=1}^{g} p_h(x)^{r_{ij}}} \right) \]

\[ = j v_{p_i}(y) - r_{ij} v_{p_i}(p_i(x)) \]

\[ = \frac{j}{p^n} v_{p_i}(y^{p^n}) - e_i r_{ij} \]

\[ = \frac{j e_i \lambda_i}{p^n} - e_i \left\lfloor \frac{j \lambda_i}{p^n} \right\rfloor \]

\[ \geq 0; \]

so this basis consists of elements that are integral with respect to all prime divisors of \( Z \) except those that lie over the infinite prime of \( k(x) \). Thus, the elements \( \theta_i \) are integral over \( k[x] \).

Consider the field basis \( \{1, y, y^2, \ldots, y^{p^n-1}\} \). Up to multiplication by a constant, the discriminant of such a basis is the discriminant of the minimal polynomial of \( y \) over \( k[x] \). Disregarding the constant the discriminant of this
basis is, therefore,

\[ \Delta_{x}(1, y, y^2, \ldots, y^{p^n-1}) = f(x)p^n - 1. \]

Let \( M \) be the matrix,

\[
M = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
0 & \frac{1}{\prod_{i=1}^{\ell} p_i(x)^{r_i,1}} & 0 & \cdots & 0 \\
0 & 0 & \frac{1}{\prod_{i=1}^{\ell} p_i(x)^{r_i,2}} & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \frac{1}{\prod_{i=1}^{\ell} p_i(x)^{r_i,p^n-1}}
\end{pmatrix}.
\]

Then,
\[
\begin{pmatrix}
1 \\
y \\
y^2 \\
\vdots \\
y^{p^n-1}
\end{pmatrix}
M
\begin{pmatrix}
\theta_0 \\
\theta_1 \\
\theta_2 \\
\vdots \\
\theta_{p^n-1}
\end{pmatrix}
\]

And so the discriminant of the basis \( \{ \theta_i \} \) is given by

\[
\Delta_x(\theta_i) = (\det M)^2(\Delta_x(y^i))
\]
\[
= (\det M)^2 f(x)p^n - 1
\]

(1)
\[
= \prod_{i=1}^{p_n} \lambda_i(p^n - 1) - 2 \sum_{j=0}^{p_n-1} r_{ij} .
\]

Now, evaluating the sum:

\[
\sum_{j=0}^{p_n-1} r_{ij} = \sum_{j=0}^{p_n-1} \left[ \frac{j \lambda_i}{p^n} \right]
\]
\[
= \frac{p_n-1}{2} \frac{\lambda_i}{p^n} - \sum_{j=0}^{p_n-1} \left\{ \frac{j \lambda_i}{p^n} \right\} , \quad \text{(the fractional part)}.
\]

Let \( d_i = (\lambda_i, p^n) \) and \( \lambda_1 = d_1 \lambda_i \). Then

\[
\sum_{j=0}^{p_n-1} r_{ij} = \frac{1}{2} \lambda_i(p^n - 1) - \sum_{j=0}^{p_n-1} \left\{ \frac{j \lambda_i}{p^n} \right\} .
\]
But \( \lambda_i' \) is relatively prime to \( \frac{p^n}{d_1} \), and so

\[
\{ j \mid 0 \leq j < \frac{p^n}{d_1} \} \text{ is a complete residue system modulo } \frac{p^n}{d_1}.
\]

\[
\sum_{j=0}^{p^n-1} r_{ij} = \frac{1}{2} \lambda_i (p^n - 1) - d_1 \sum_{j=0}^{\frac{p^n}{d_1} - 1} \frac{d_1}{d_1} \frac{p^n}{d_1} - 1 = \frac{1}{2} \lambda_i (p^n - 1) - d_1 \cdot \frac{d_1}{p^n} \cdot \frac{1}{2} (\frac{p^n}{d_1} - 1) \frac{p^n}{d_1}
\]

\[
= \frac{1}{2} \lambda_i (p^n - 1) - \frac{1}{2}(p^n - d_1).
\]

Substituting (2) into (1) yields

\[
\Delta_x(\theta_i) = \prod_{i=1}^{\ell} p_i(x)^{\lambda_i (p^n - 1) - \lambda_i (p^n - 1) + (p^n - d_1)}
\]

\[
= \prod_{i=1}^{\ell} p_i(x)^{p^n - d_1}.
\]

However, this (after being converted to an ideal and then injected into the divisor group) is exactly that part of the divisor discriminant of the extension which is based on the finite primes, \( \Delta_x \). For consider the contribution of \( p_i(x) \) to the discriminant,

\[
\Delta_x(p_i(x)) = N(\prod_{n=1}^{\mathfrak{p}_n} \delta_x(\mathfrak{p}_n))
\]
where $\mathfrak{P}_h$ are the primes of $Z$ above the divisor associated with $p_1(x)$ and where $N$ denotes the norm of $Z$ to $k(x)$.

Thus

$$\Delta_x(p_1(x)) = N\left( \prod_{h=1}^{g} \mathfrak{P}_h \right)^{e_1-1}$$

$$= \prod_{h=1}^{g} (N(\mathfrak{P}_h))^{e_1-1}$$

$$= (p_1(x))^{d_1(e_1-1)}$$

This completes the proof of Theorem 3.

**Theorem 4:** Let $Z$ be a congruence function field as in Theorem 3. Then, for any $\alpha \in \mathfrak{G}$ which is a primitive element for the extension $Z/k(x)$, there is a prime $\mathfrak{P}_\infty$ lying over the infinite prime of $k(x)$, $p_{1/x}$, such that

$$v_{\mathfrak{P}_\infty}(\alpha) \leq \frac{e_\infty - 1}{p^n - 1} - \frac{2e}{p^n} - \frac{2G}{p^n(p^n - 1)}$$

where $G$ is the genus of $Z$ and $e_\infty$ is the ramification index of $\mathfrak{P}_\infty$.

**Proof:** Let the decomposition of $p_{1/x}$ in $Z$ be given by

$$p_{1/x} = (\mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g)^{e_\infty}, \deg_{Z/k(x)}(\mathfrak{P}_1) = f.$$
\[ \alpha = a_0(x) \theta_0 + a_1(x) \theta_1 + \ldots + a_{p^n-1}(x) \theta_{p^n-1}, \]
\[ a_i(x) \in k[x], \]
and then, for all the primes \( \mathfrak{p}_i \),

\[ v_{\mathfrak{p}_i}(\alpha) \geq \min_{0 \leq j < p^n} \{ v_{\mathfrak{p}_i}(a_j(x) \theta_j) \}. \]

By the definition of \( \theta_j \), it is clear that

\[ v_{\mathfrak{p}_i}(\theta_j) = v_{\mathfrak{p}_h}(\theta_j) \]

for all possible \( h, i \) and \( j \); so there is only one minimum as in \((3)\). Let \( m \) denote this minimum, and let \( j_o \) be an index such that

\[ v_{\mathfrak{p}_i}(a_{j_o}(x) \theta_{j_o}) = m. \]

Let \( \sigma \) be a generating automorphism in \( \text{GAL}(Z/k(x)) \). The action of the Galois group on \( \theta_j \) is given by

\[ \sigma^i \theta_j = \zeta^{ij} \theta_j \]

where \( \zeta \) is a primitive \( p^n \)-th root of 1 in \( k \). Consider, then, the system of equations:

\[ \sigma^i \alpha = \sum_{j=0}^{p^n-1} a_j(x) \sigma^i \theta_j = \sum_{j=0}^{p^n-1} a_j(x) \zeta^{ij} \theta_j, \]

where \( 0 \leq i < p^n \). Now multiplying the \( i \)-th equation by
these equations become:

$$\zeta^{\text{th}} \sigma \alpha = \sum_{i=0}^{p^n-1} a_j(x) \zeta^{i-j_0} \theta_j.$$  

For any $p^n$-th root of $1$, $\zeta'$, not equal to $1$ 

$$\sum_{i=0}^{p^n-1} (\zeta')^i = 0.$$  

Thus adding these equations yields 

$$p^n a_j(x) \theta_j = \sum_{i=0}^{p^n-1} (\zeta')^i \theta_j.$$  

And then taking the valuation $v_{\mathfrak{P}_1}$ of both sides gives 

$$m = v_{\mathfrak{P}_1} (p^n a_j(x) \theta_j) = v_{\mathfrak{P}_1} (\sum_{i=0}^{p^n-1} (\zeta')^i \theta_j) \geq \min_{0 \leq i < p^n} \{v_{\mathfrak{P}_1} (\zeta')^i \theta_j\}.$$  

Thus there is a prime $\mathfrak{P}_m$ lying over $p_1/x$ such that
Consider now $v_{p_{\infty}}(a_j(x)e_j)$ for any prime $p_{\infty}$ over $p_{1/x}$. If $a(x)$ is any non-zero polynomial over $k$, then $v_{p_{\infty}}(a_j(x)) \leq 0$, and so

$$v_{p_{\infty}}(a_j(x)e_j) \leq v_{p_{\infty}}(e_j)$$

$$\leq v_{p_{\infty}}(y^j) - v_{p_{\infty}}\left(\prod_{i=1}^{\ell} p_i(x)^{r_{ij}}\right)$$

$$\leq \frac{j}{n} v_{p_{\infty}}(y^{p_n}) - \frac{\ell}{n} r_{ij} \sum_{i=1}^{\ell} v_{p_{\infty}}(p_i(x))$$

(5)

$$\leq \frac{j}{n} e_{p_{\infty}} p_{1/x} \sum_{i=1}^{\ell} p_i(x)^{\lambda_i} - \sum_{i=1}^{\ell} r_{ij} e_{p_{\infty}} p_{1/x} (p_i(x))$$

$$\leq - e_{p_{\infty}} \sum_{i=1}^{\ell} \left(\frac{j\lambda_i}{p_n} - \left\lfloor \frac{j\lambda_i}{p_n} \right\rfloor \right) \deg p_i(x)$$

Since $\alpha$ is also a primitive element in the extension $k$ over $k(x)$, there must be an index $j$ relatively prime to $p$ such that $a_j(x) \neq 0$, otherwise $\alpha$ would be contained in the subfield $k(x,y^p)$. But then, if $(j,p) = 1$,

$$\frac{j\lambda_i}{p_n}$$

is not an integer, and so
Thus (4) and (5) imply, for some prime $\mathfrak{p}_\infty$ lying over $p_1/x$, 

$$v_{\mathfrak{p}_\infty}(\alpha) = \min \{v_{\mathfrak{p}_\infty}(a_j(x)\theta_j)\}$$

$$0 \leq j < p^n$$

$$\leq -\frac{e_\infty}{p^n} \sum_{i=1}^{\ell} \deg p_i(x)$$

$$\leq -\frac{e_\infty}{p^n} \sum_{i=1}^{\ell} \frac{p^n - d_i}{p^n - 1} \deg p_i(x), \text{ where } d_i = (p^n, \lambda_i),$$

$$\leq -\frac{e_\infty}{p^n(p^n - 1)} \deg(\prod_{i=1}^{\ell} p_i(x)^{p^n - d_i})$$

$$\leq -\frac{e_\infty}{p^n(p^n - 1)} \deg(\Delta_x), \text{ where } \Delta_x \text{ is the Dedekind discriminant},$$

$$\leq -\frac{e_\infty}{p^n(p^n - 1)}(\deg_k(x)(\Delta) - (p^n - \frac{p^n}{e_\infty})), \text{ (7)}$$

where $\Delta$ is the divisor discriminant of the extension $Z/k(x)$. By the Hurwitz genus formula this gives:

$$v_{\mathfrak{p}_\infty}(\alpha) \leq -\frac{e_\infty}{p^n(p^n - 1)} (2G + 2(p^n - 1) - (p^n - \frac{p^n}{e_\infty}))$$

$$\leq \frac{e_\infty}{p^n - 1} - \frac{2e_\infty}{p^n} - \frac{2G}{p^n(p^n - 1)} \leq \frac{e_\infty - 1}{p^n} \text{ ....}$$
for some \( \pi \) of \( Z \) lying over \( \mathfrak{p}_{1/x} \). Thus Theorem 4 is proved.

Next, Theorem 4 is generalized to include cyclic extensions of \( k(x) \) of degree \( p^n \) in which \( p^n \)-th roots of 1 are not necessarily present:

**Theorem 5:** Let \( Z \) be a cyclic geometric extension of \( k(x) \) of degree \( p^n \), where \( p \) is a prime other than the characteristic of \( k \). Then, for any \( \alpha \) integral over \( k[x] \), which is a primitive element of the extension \( Z/k(x) \), there is a prime \( \mathfrak{p} \) of \( Z \) lying over the infinite prime of \( k(x) \) such that

\[
\nu_{\mathfrak{p}}(\alpha) < \frac{e_{\infty} - 1}{p^n - 1} - \frac{2e_{\infty}}{p^n} - \frac{2G}{p'(p^n - 1)}
\]

where \( G \) is the genus of \( Z \) and \( e_{\infty} \) is the ramification index of \( \mathfrak{p} \).

**Proof:** Let \( k' \) be the smallest extension of \( k \) which contains the \( p^n \)-th roots of 1, and let \( Z' \) be the constant field extensions of \( Z \) with constant field \( k' \). Any primitive element \( \alpha \) for the extension \( Z/k(x) \) satisfies a \( p^n \)-th degree polynomial that is irreducible over \( k[x] \). Since \( Z/k(x) \) is geometric and has \( k \) for its exact field of constants, the polynomial is also irreducible in \( k'[x] \). Thus \( \alpha \) is also a primitive element for the extension.
Z'/k'(x). If \( \alpha \) is integral over \( k[x] \), it is also integral over \( k'[x] \). Finally \( Z'/Z \) is a constant field extension so the genus of \( Z' \) is the genus of \( Z \). Thus by Theorem 4 there is a prime \( \mathfrak{p}'_1 \) of \( Z' \) which lies over the infinite prime \( p'_{1/x} \) of \( k'(x) \) such that

\[
v_{\mathfrak{p}'_1}(\alpha) \leq \frac{e'_{\infty} - 1}{p - 1} - \frac{2e'_1}{p^2} - \frac{2G}{p^n(p^n - 1)},
\]

where \( e'_{\infty} \) is the ramification index of \( \mathfrak{p}'_{1/x} \) over \( k'(x) \).

Now \( \mathfrak{p}'_{1/x} \) lies over some \( \mathfrak{p}_1 \) in \( Z \), and, since \( Z'/Z \) is unramified, the ramification index of \( \mathfrak{p}_1 \) over \( p_{1/x} \) is \( e'_{\infty} \). Thus

\[
v_{\mathfrak{p}_1}(\alpha) = v_{\mathfrak{p}'_1}(\alpha) \leq \frac{e_{\infty} - 1}{p - 1} - \frac{2e_{\infty}}{p^n} - \frac{2G}{p^n(p^n - 1)},
\]

completing the proof of Theorem 5.

The Main Result in a Special Case

To prove the main result for cyclic extensions of \( k(x) \), it is necessary to estimate the minimum degree of a prime of \( k(x) \) that splits in \( Z \). Such an estimate is given by:

**Theorem 6**: If \( Z \) is a cyclic geometric extension of \( k(x) \) of degree \( p^n \) where \( p \) is any prime (including the characteristic of \( k \)), then there exists a prime divisor in \( k(x) \) which splits completely in \( Z \) and which has degree less
than or equal to $m_o$, where $m_o = m_\perp + 2$ for any $m_\perp$ which satisfies

$$q^{\frac{m_\perp}{2}} - 2Gq^{\frac{m_\perp}{2}} - 2m_\perp(G + p^n) \geq 0.$$

**Lemma 1:** Let $\mathbb{Z}_m$ be the constant field extension of $\mathbb{Z}$ of degree $m$ for $m$ relatively prime to $p$. If $\mathfrak{p}_m$ is a prime divisor of $\mathbb{Z}_m$ of degree 1, and if $\mathfrak{p}$ is the prime under $\mathfrak{p}_m$ in $\mathbb{Z}$, then

$$\deg_{\mathbb{Z}/k(x)}(\mathfrak{p}) = 1.$$

**Proof of Lemma:** Suppose $\deg_{\mathbb{Z}/k(x)}(\mathfrak{p}) \neq 1$. Let $\mathfrak{p}$ lie over $p_p(x)$ in $k(x)$. Then since the degree of the extension $\mathbb{Z}/k(x)$ is $p^m$, $\deg_{\mathbb{Z}/k(x)}(\mathfrak{p}) = p^f$ for some $f \geq 1$. This follows from the fact that in a normal extension the relative degree of any prime divides the degree of the extension. And therefore,

$$\deg_{\mathbb{Z}}(\mathfrak{p}) = p^f \deg_{k(x)}(p_p(x)) = p^f \deg p(x).$$

And then,

$$\deg_{\mathbb{Z}/m}(\mathfrak{p}_m) \cdot m = \deg_{\mathbb{Z}_m/Z}(\mathfrak{p}_m) \deg_{\mathbb{Z}}(\mathfrak{p}) = \deg_{\mathbb{Z}_m/Z}(\mathfrak{p}_m) \cdot p^f \cdot \deg p(x).$$

But $(m,p) = 1$, so $p$ must divide $\deg_{\mathbb{Z}/m}(\mathfrak{p}_m)$; thus it cannot be 1.
Proof of Theorem 6: A prime $p$ in $Z$ can have relative
degree 1 in only two ways:

(1) the prime $p_{p(x)}$ lying under $p$ in $k(x)$ is ramified
in $Z$;

(2) the prime $p_{p(x)}$ lying under $p$ in $k(x)$ is split
completely in $Z$.

Thus if $m$ is chosen large enough to ensure that there are
more primes of degree 1 in $Z_m$ than could lie over ramified
primes of $k(x)$, then there must be a prime of degree 1
in $Z_m$ which lies over a prime $p_{p(x)}$ of $k(x)$ which is
split completely in $Z$. Now the degree of $p_{p(x)}$ cannot
exceed $m$, for it lies under a prime of degree 1 in
$k'(x)$, a degree $m$ constant extension of $k(x)$. Thus,
it is only necessary to choose the proper $m$.

First, let $N_m$ be the number of primes of degree 1
in $Z_m$. $N_m$ can be estimated using the Riemann hypothesis;

$$|N_m - (q^m + 1)| \leq 2Gq^{m/2}.$$ 

And so,

$$N_m \geq q^m - 2Gq^{m/2} + 1.$$  (3)

Next, the number of primes of $Z$ that have ramified from
$k(x)$ is less than or equal to the degree of the different
of the extension $Z/k(x)$. By the genus formula, this
degree is
Now each of these primes of $\mathbb{Z}$ that have ramified from $k(x)$ can have at most $m$ primes over it in $\mathbb{Z}_m$. Thus the number of primes of $\mathbb{Z}_m$ which lie over primes of $k(x)$ that ramify in $\mathbb{Z}$ is at most

$$2m(G + p^n - 1).$$

Thus if $m$ is chosen such that $(m,p) = 1$ and

$$q^m - 2Gq^{m/2} + 1 > 2m(G + p^n - 1),$$

then there is a prime of $k(x)$ which splits completely in $\mathbb{Z}$ and has degree at most $m$. Such an $m$ can be chosen less than or equal to the $m_0$ in the statement of the theorem.

It is now possible to prove the main result of the paper in a special case.

**Theorem 7**: Let $\mathbb{Z}$ be a cyclic geometric extension of $k(x)$ of degree $p^n$, where $p$ is a prime other than the characteristic of $k$. If $G$ is the genus of $\mathbb{Z}$, $e_\infty$ is the ramification index of a prime of $\mathbb{Z}$ over the infinite prime of $k(x)$, $m = m_0$ of Theorem 6, and $E$ is the exponent of the null class group of $\mathbb{Z}$, then
Proof: Let \( p \) be a prime divisor of \( k(x) \) of smallest degree which splits completely in \( \mathbb{Z} \). Then by Theorem 6,

\[
\deg_{k(x)} p \leq m.
\]

Let \( \mathfrak{p}_1 \) be any prime of \( \mathbb{Z} \) which lies over \( p \); then \( \mathfrak{p}_1 \) has \( p^n \) distinct conjugates under the action of the Galois group. If \( \mathfrak{p}_\infty \) is any prime of \( \mathbb{Z} \) (other than \( \mathfrak{p}_1 \)) which lies over the infinite prime of \( k(x) \), then

\[
\frac{\deg_{\mathbb{Z}} \mathfrak{p}_\infty}{\deg_{\mathbb{Z}} \mathfrak{p}_1} \in D_0(\mathbb{Z}).
\]

Therefore, since \( E \) is the exponent of \( D_0(\mathbb{Z})/E(\mathbb{Z}) \),

\[
\frac{E \deg_{\mathbb{Z}} \mathfrak{p}_1}{E \deg_{\mathbb{Z}} \mathfrak{p}_1} = (\alpha) \in E(\mathbb{Z}), \quad \alpha \in \mathbb{Z}.
\]

The function \( \alpha \) has its only pole at a prime over the infinite prime of \( k(x) \); so \( \alpha \) is integral over \( k(x) \). Also \( \alpha \) has \( p^n \) distinct conjugates under the action of the Galois group of \( \mathbb{Z}/k(x) \); thus, \( \alpha \) is a primitive element for this extension. By Theorem 5
\[-E \deg_Z(n_1) \leq \frac{e_\infty - 1}{p^n - 1} - \frac{2e_\infty}{p^n} - \frac{2G}{p^n(p^n - 1)}.
\]

But \(\deg_Z(n_1) = \deg_k(x)p \leq m\). Therefore

\[E \geq \frac{1}{m}(\frac{2G}{p^n(p^n - 1)} + \frac{2e_\infty}{p^n} - \frac{e_\infty - 1}{p^n - 1}), \text{ Q.E.D.}
\]

Corollary: In the class of finite, cyclic, geometric extensions \(Z\) of \(k(x)\) of fixed degree \(p^n\), where \(p\) is a prime other than the characteristic of the finite field \(k\), the exponent of the null class group approaches infinity as the genus of \(Z\) goes to infinity.

Proof: Since \(e_\infty \geq 1\),

\[\frac{2e_\infty}{p^n} - \frac{e_\infty - 1}{p^n - 1} = \frac{p^n e_\infty - 2e_\infty + p^n}{p^n(p^n - 1)} \geq \frac{p^n - 2 + p^n}{p^n(p^n - 1)} \geq \frac{2}{p^n},
\]

and so

\[(10) \quad E \geq \frac{1}{m}(\frac{2G}{p^n(p^n - 1)} + \frac{2}{p^n}).
\]

For \(G\) large enough, the \(m\) in Theorem 6 can be taken as
This is easily seen since

\[(q^{1/2} - 2G) = G^3 - 2G > 1,\]

for \(G\) large enough. Thus,

\[q^{1/2}(q^{1/2} - 2G) - 2m_1(G + p^n) > q^{1/2} - 2m_1(G + p^n),\]

or, after plugging in the value suggested for \(m_1\),

\[q^{1/2}(q^{1/2} - 2G) - 2m_1(G + p^n) > G^3 - \frac{12}{\log q} (\log G)(G + p^n)\]

If \(G\) is large enough, this is positive; so \(m_1 = \frac{6 \log G}{\log q}\)
satisfies the inequality of Theorem 6. Now,

\[m = m_0 = m_1 + 2 = \frac{6 \log G}{\log q} + 2 \leq \frac{7 \log G}{\log q},\]

if \(G\) is large enough.

Putting this in (10) gives

\[E \geq \frac{\log q}{7 \log G} \left( \frac{2G}{p(n^n)} + \frac{2}{p^n} \right).\]

Therefore,

\[\lim_{G \to \infty} E = \infty.\]
CHAPTER III

ARTIN-SCHREIER EXTENSIONS AND THE MAIN RESULT

In this chapter results analogous to those proved in Chapter II for extensions of prime power degree are obtained for Artin-Schreier extensions. In the second part of the chapter, these results are combined to give the main result of the paper.

Let $Z$ be a cyclic geometric extension of $k(x)$ of degree $p$ where $p$ is the characteristic of $k$; then $Z$ is a congruence function field over the exact field of constants $k$, if $k$ is finite. Let $k$ be finite and $|k| = q$; this type of extension, an Artin-Schreier extension, can be realized as $Z = k(x, y)$ where

$$y^p - y = f(x) = \prod_{i=1}^{l} p_i(x)^{\gamma_i}, \quad \gamma_i \in \mathbb{Z}.$$ 

There is a standard form of such an equation that can be reached through the transformation $y = y' + a(x)$ for suitable $a(x)$; it can be assumed that the generating equation of $Z$ over $k(x)$ is
\[ y^p - y = f(x), \text{ where } (f(x)) = \frac{\Omega}{\lambda_1 \lambda_2 \ldots \lambda_L}, \]

\[ (\lambda_i, p) = 1 \text{ for } i = 1, 2, \ldots, L. \]

Also \( \Omega \) is an integral divisor of \( k(x) \) and relatively prime to the denominator of \( f(x) \). Note that the standard form of an Artin-Schreier extension treats all the prime divisors of \( k(x) \) equally, unlike the standard form of a Kummer extension.

**Theorem 8:** If, with the notation as above, \( Z = k(x, y) \), where the generating equation is in standard form, then

\[ y^p - y = f(x) = \frac{q(x)}{p_1(x) \lambda_1 p_2(x) \lambda_2 \ldots p_L(x) \lambda_L}, \]

\[ (\lambda_1, p) = 1; \]

and, in keeping with the standard form of \( f(x) \),

\[ \lambda_\infty = \begin{cases} 
\deg f(x), & \text{if } \deg f(x) > 0 \\
0, & \text{if } \deg f(x) \leq 0.
\end{cases} \]

Thus \( (\lambda_\infty, p) = 1 \), if \( \lambda_\infty \neq 0 \). Further, for any prime divisor \( p \) of \( k(x) \):

1. \( p \) is ramified if and only if \( p \) divides the (divisor) denominator of \( f(x) \). The contribution of the prime \( \Phi \) of \( Z \) above \( p \) to the different is
(a) \( \delta(p) = \frac{\lambda_1 + 1)(p - 1)}{p - 1} \), if \( p \) is not the infinite prime,

(b) \( \delta(p) = \frac{\lambda_\infty + 1)(p - 1)}{p - 1} \), if \( p \) is the infinite prime.

(2) If \( p \) is an unramified prime, then

\[ y^p - y - f(x) \]

is an integral polynomial with respect to \( p \). The decomposition of \( p \) in \( \mathbb{Z} \) mirrors the decomposition of this polynomial modulo \( p \). That is, \( p \) is inert if \( y^p - y - f(x) \) is irreducible in \( \mathbb{Z}/p \mathbb{Z} \) and is split if the polynomial factors there.

In any Artin-Schreier extension, there is an automorphism \( \sigma \) which generates \( \text{GAL}(\mathbb{Z}/k(x)) \) such that

\[ \sigma(y) = y + 1. \]

With the notation in Theorem 8, let \( \mathcal{O} \) be the integral closure of \( k[x] \) in \( \mathbb{Z} \). If \( \{w_1, w_2, \ldots, w_p\} \) is a basis of \( \mathbb{Z} \) over \( k(x) \), the discriminant of this basis \( \Delta_x(w_1) \) can be defined regardless of whether the elements of that basis are integral. Also, if \( y \) is a primitive element of the extension \( \mathbb{Z} \) over \( k(x) \), the discriminant of the basis \( \{1, y, y^2, \ldots, y^{p-1}\} \) is the discriminant of the minimum polynomial of \( y \).
Theorem 9: Let \( Z \) be an Artin-Schreier extension of \( k(x) \), and let

\[
y^p - y = f(x) = \frac{q(x)}{p_1(x)^{\lambda_1} p_2(x)^{\lambda_2} \cdots p_g(x)^{\lambda_g}}
\]

be the generating equation in standard form (the notation as in Theorem 3). Then \( \{\theta_0, \theta_1, \theta_2, \ldots, \theta_{p-1}\} \) is an integral basis of \( Z \) over \( k(x) \), where

\[
\theta_j = y^j \prod_{i=1}^g p_i(x)^{r_{ij}}, \text{ for } r_{ij} = \begin{cases} 
1 + \left[ \frac{j\lambda_i}{p} \right], & \text{if } j \neq 0 \\
0, & \text{if } j = 0.
\end{cases}
\]

Proof: \( \theta_j \) is clearly integral for all the primes of \( Z \) except possibly those lying over ramified primes or the infinite prime. If \( \mathfrak{p}_1 \) is a prime of \( Z \) lying over \( \mathfrak{p}_{p_1}(x) \), the prime divisor of \( k(x) \) associated with \( p_1(x) \), then

\[
\nu_{\mathfrak{p}_1}(y) < 0.
\]

Therefore,

\[
\nu_{\mathfrak{p}_1}(y) = \nu_{\mathfrak{p}_1}(y+1) = \nu_{\mathfrak{p}_1}(y+2) = \ldots = \nu_{\mathfrak{p}_1}(y+p-1).
\]

This gives immediately

\[
\nu_{\mathfrak{p}_1}(y) = \nu_{\mathfrak{p}_1}(y+1) = \nu_{\mathfrak{p}_1}(y+2) = \ldots = \nu_{\mathfrak{p}_1}(y+p-1).
\]
\[ v_{\mathfrak{p}_1}(y) = \frac{1}{p} v_{\mathfrak{p}_1}(y^p - y) = -\lambda_1 \]

and, using the definition,

\[ v_{\mathfrak{p}_1}(\theta_j) = v_{\mathfrak{p}_1}(y^j \prod p_h(x)^{r_{hj}}) = -j\lambda_1 + r_{ij}p. \]

Therefore, \( v_{\mathfrak{p}_1}(\theta_j) \geq 0 \) for all the primes \( \mathfrak{p}_1 \) that have ramified from \( k(x) \) and which are associated with polynomials in \( k(x) \). In fact, if \( j \neq 0 \), then \( v_{\mathfrak{p}_1}(\theta_j) > 0 \). This gives that the elements of the basis \( \{\theta_1\} \) are integral over \( k[x] \).

To compute the discriminant of the basis \( \{\theta_1\} \), let \( M \) be the matrix:

\[
M = \begin{pmatrix}
1 & 0 & 0 & \ldots & 0 \\
0 & \prod_{i=1}^l p_i(x)^{r_{i,1}} & 0 & \ldots & 0 \\
0 & 0 & \prod_{i=1}^l p_i(x)^{r_{i,2}} & \ldots & 0 \\
0 & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \prod_{i=0}^{d-1} p_i(x)^{r_{i,d-1}}
\end{pmatrix}
\]
Thus

\[
M \begin{pmatrix}
1 \\
y \\
y^2 \\
\vdots \\
y^{p-1}
\end{pmatrix}
= \begin{pmatrix}
\theta_0 \\
\theta_1 \\
\theta_2 \\
\vdots \\
\theta_{p-1}
\end{pmatrix},
\]

and, therefore,

\[\Delta_x(\theta_i) = [\det M]^2 \Delta_x(y^i).\]

But \(\Delta_x(y^i)\) is the discriminant of the polynomial \(y^p - y - f(x)\), which is 1. So,

\[
(13) \quad \Delta_x(\theta_i) = \prod_{i=1}^p p_1(x)^2 \sum_{j=0}^{p-1} r_{ij}. \]

Now,

\[
\sum_{j=0}^{p-1} r_{ij} = \sum_{j=1}^{p-1} \left(1 + \left\lfloor \frac{j\lambda_1}{p} \right\rfloor \right)
= (p - 1) + \frac{\lambda_1}{2} (p - 1) - \frac{1}{2}(p - 1)
= \frac{1}{2} (\lambda_1 + 1)(p - 1).
\]

Then (13) and (14) together give
\[ \Delta_x(\theta_1) = \prod_{i=1}^{\ell} p_i(x)^{(\lambda_i+1)(p-1)}. \]

However, this (after being made an ideal and then a divisor) is exactly the finite part of the norm of the different as given by (12). So

\[ \Delta_x(\theta_1) = \Delta_x(z), \]

where \( \Delta_x(z) \) is the Dedekind discriminant of \( Z \) over \( k(x) \). Thus \( \{\theta_1\} \) is an integral basis and the theorem is proved.

**Theorem 10:** Let \( Z \) be an Artin-Schreier extension with the notation as in Theorems 8 and 9; then, for any \( \alpha \in \Theta \) which is a primitive element of the extension \( Z \) over \( k(x) \), there is a prime divisor \( \mathfrak{p} \) of \( Z \) lying over the infinite prime \( p_{1/x} \) of \( k(x) \) such that

\[ v_{\mathfrak{p}}(\alpha) \leq -e_\infty \left( \frac{2G}{p(p - 1)} + \frac{1}{p} \right), \]

where \( e_\infty \) is the ramification index of \( \mathfrak{p} \) and \( G \) is the genus of \( Z \).

**Proof:** If \( \alpha \in \Theta \), then by the previous theorem \( \alpha \) can be written as
\[ \alpha = a_0(x)\theta_0 + a_1(x)\theta_1 + a_2(x)\theta_2 + \ldots + a_{p-1}(x)\theta_{p-1} \]
\[ = b_0(x) + b_1(x)y + b_2(x)y^2 + \ldots + b_{p-1}(x)y^{p-1}, \]
where \( a_j(x) \in k[x] \) and \( b_j(x) = a_j(x) \prod_{i=1}^{l} p_i(x)^{r_{ij}}. \) As in the proof of Theorem 4, it is necessary to evaluate \( v_{x_\infty}(\alpha) \) for some \( x_\infty \) lying over \( p_{1/x}. \) It is convenient to do this in the form of

**Lemma 2:** For \( \alpha \) as in the theorem, there is a \( x_\infty \) lying over the infinite prime \( p_{1/x} \) of \( k(x) \) such that

\[ v_{x_\infty}(\alpha) = m, \]

where

\[ m = \begin{cases} 
\min_{0 \leq j < p} \{v_{x_\infty}(b_j(x)y^j)\}, & \text{if } p_{1/x} \text{ is ramified in } Z \\
\min_{0 \leq j < p} \{v_{p_{1/x}}(b_j(x))\}, & \text{if } p_{1/x} \text{ is unramified in } Z.
\end{cases} \]

**Proof of Lemma:** The proof is given in two parts. First, if \( p_{1/x} \) is ramified in \( Z, \) then there is only one prime \( x_\infty \) of \( Z \) over \( p_{1/x}, \) and \( v_{x_\infty}(y) = x_\infty. \) Now,

\[ v_{x_\infty}(b_j(x)y^j) = v_{x_\infty}(b_j(x)) + v_{x_\infty}(y^j) \]
\[ = pv_{p_{1/x}}(b_j(x)) - jx_\infty \]
However, since \( p_{1/x} \) is ramified, \( \lambda_{\infty} \neq 0 \) (mod p), and so the set

\[
\{ v_{\mathfrak{p}_{\infty}}(b_j(x)y^j) | 0 \leq j < p \}
\]

is a complete residue system modulo \( p \). Therefore, this set has a distinct minimum, and so,

\[
v_{\mathfrak{p}_{\infty}}(\alpha) = m.
\]

Next is the case where \( p_{1/x} \) is unramified in \( \mathbb{Z} \). If \( \mathfrak{p}_{1} \) is any prime of \( \mathbb{Z} \) over \( p_{1/x} \), then

\[
v_{\mathfrak{p}_{1}}(y) \geq 0.
\]

Thus for all the primes \( \mathfrak{p}_{1} \) over \( p_{1/x} \)

\[
v_{\mathfrak{p}_{1}}(\alpha) = v_{\mathfrak{p}_{1}}(b_0(x) + b_1(x)y + \ldots + b_{p-1}(x)y^{p-1})
\]

\[
\geq \min_{0 \leq j < p} \{ v_{\mathfrak{p}_{1}}(b_j(x)y^j) \}.
\]

\[ (15) \]

\[
\geq \min_{0 \leq j < p} \{ v_{\mathfrak{p}_{1}}(b_j(x)) + jv_{\mathfrak{p}_{1}}(y) \}
\]

\[
\geq \min_{0 \leq j < p} \{ v_{\mathfrak{p}_{1}}(b_j(x)) \}
\]

\[
\geq m.
\]

Notice here, that there is some prime \( \mathfrak{p}_{1} \) over \( p_{1/x} \) such that \( v_{\mathfrak{p}_{1}}(y) = 0 \). For suppose \( v_{\mathfrak{p}_{1}}(y) > 0 \), then
\( v_{p_{1/x}}(f(x)) > 0 \), and so \( p_{1/x} \) must split over \( Z \). Then
\[
v_{p_{1/x}}(y) = v_{p_{1/x}}(y + 1) = \min(v_{p_{1/x}}(y), 0) = 0.
\]

Let \( j_o \) be an index such that \( v_{p_{1/x}}(b_{j_o}(x)) = m \). It can be assumed that \( j_o \neq 0 \); for if \( o \) is the only index where this minimum occurs, it follows immediately that
\[
v_{p_{1/x}}(\alpha) = \min_{0 \leq j < 0} \{v_{p_{1/x}}(b_j(x)y^j)\} = m\]
for that prime \( p_{1/x} \) over \( p_{1/x} \) for which \( v_{p_{1/x}}(y) = 0 \).

Consider then
\[
(16) \quad y^{p-1-j_o} = b_0(x)y^{p-1-j_o} + b_1(x)y^{p-1-j_o} + \ldots + b_{j_o}(x)y^{p-1-j_o} + \ldots + b_{p-1}(x)y^{2(p-1)-j_o}.
\]

Now since \( j_o \neq 0 \), the highest power of \( y \) that can occur in this sum is \( 2p - 3 \). By Newton's formulae [see 3, p. 437], it is easy to see that the trace from \( Z \) to \( k(x) \) (denoted by \( \text{Tr}(\alpha) \)) acts on these powers of \( y \) in the following way:
\[
\text{Tr}(y^h) = \begin{cases} 
0, & \text{if } 0 \leq h < 2p-1 \text{ and } h \neq p-1 \\
-1, & \text{if } h = p-1.
\end{cases}
\]

Therefore, (16) gives, for any prime \( p_{1/x} \) above \( p_{1/x} \),
\[
m = v_{\mathfrak{p}_1/x}(b_j(x)) = v_{\mathfrak{p}_1}(b_j(x)) = v_{\mathfrak{p}_1}(\text{Tr}(y^{-1}j_0\alpha)) \\
\geq \min_{\sigma \in \text{GAL}(\mathbb{Z}/k(x))} \{v_{\mathfrak{p}_1}(\sigma(y^{-1}j_0\alpha))\} \\
\geq \min_{\mathfrak{p}_1 \text{ above } p_{1/x}} \{v_{\mathfrak{p}_1}(y^{-1}j_0\alpha)\} \\
\geq \min_{\mathfrak{p}_1 \text{ above } p_{1/x}} \left((p^{-1}j_0)v_{\mathfrak{p}_1}(y) + v_{\mathfrak{p}_1}(\alpha)\right).
\]

(17)

But \(v_{\mathfrak{p}_1}(y) \geq 0\), \((p^{-1}j_0) \geq 0\), and \(v_{\mathfrak{p}_1}(\alpha) \geq m\) for all the primes \(\mathfrak{p}_1\) of \(\mathbb{Z}\) above \(p_{1/x}\), and this together with (15) gives

\[
m \geq \min_{\mathfrak{p}_1 \text{ above } p_{1/x}} \left((p^{-1}j_0)v_{\mathfrak{p}_1}(y) + v_{\mathfrak{p}_1}(\alpha)\right) \geq m.
\]

Thus, there is a prime \(\mathfrak{p}_\infty\) in \(\mathbb{Z}\) above \(p_{1/x}\) such that \(v_{\mathfrak{p}_\infty}(\alpha) = m\), and this proves the lemma.

**Proof of Theorem 10:** It remains to estimate the value of \(m\) in the lemma. For a primitive element \(\alpha\) in the extension \(Z/\mathbb{k}(x)\), there is an index \(j_1\) such that \(a_{j_1}(x) \neq 0\) and \(j_1 \neq 0\). When \(p_{1/x}\) is ramified this gives
\[ m = \min_{0 \leq j < p} \{ v_{\|_{\infty}}(b_j(x)y^j) \} \]
\[ \leq v_{\|_{\infty}}(b_{j_1}(x)y^{j_1}) \]
\[ \leq v_{\|_{\infty}}(a_{j_1}(x)) + v_{\|_{\infty}}\left( \prod_{i=1}^{l} p_i(x)^{r_{ij_1}} \right) - j_1 \lambda_{\infty} \]
\[ \leq p v_{p_{l/x}}\left( \prod_{i=1}^{l} p_i(x)^{r_{ij_1}} \right) - \lambda_{\infty} \]

When \( p_{l/x} \) is unramified,

\[ m = \min_{0 \leq j < p} \{ v_{p_{l/x}}(b_j(x)) \} \]
\[ \leq v_{p_{l/x}}(b_{j_1}(x)) \]
\[ \leq v_{p_{l/x}}(a_{j_1}(x)) + v_{p_{l/x}}\left( \prod_{i=1}^{l} p_i(x)^{r_{ij_1}} \right) \]
\[ \leq v_{p_{l/x}}\left( \prod_{i=1}^{l} p_i(x)^{r_{ij_1}} \right) \]

In both cases it is necessary to approximate

\[ v_{p_{l/x}}\left( \prod_{i=1}^{l} p_i(x)^{r_{ij}} \right), \text{ for } j \neq 0; \]
\[ v_{p_1/x} ( \prod_{i=1}^{\ell} p_i(x)^{r_{ij}} ) = -\deg(\prod_{i=1}^{\ell} p_i(x)^{r_{ij}}) \]

\[ = - \sum_{i=1}^{\ell} r_{ij} \deg p_i(x) \]

\[ = - \sum_{i=1}^{\ell} (1 + \left\lfloor \frac{j \lambda_i}{p} \right\rfloor) \deg p_i(x) \]

\[ \leq - \sum_{i=1}^{\ell} \left( \frac{j \lambda_i}{p} + \frac{1}{p} \right) \deg p_i(x) , \quad \therefore p \nmid \lambda_i \]

\[ \leq - \frac{1}{p} \sum_{i=1}^{\ell} (j \lambda_i + 1) \deg p_i(x) \]

\[ \leq - \frac{1}{p} \sum_{i=1}^{\ell} (\lambda_i + 1) \deg p_i(x) \]

\[ \leq - \frac{1}{p(p-1)} \sum_{i=1}^{\ell} (\lambda_i + 1)(p-1) \deg p_i(x) \]

\[ \leq - \frac{1}{p(p-1)} \deg(\prod_{i=1}^{\ell} p_i(x)(p-1)(\lambda_i + 1)) \]

\[ \leq - \frac{1}{p(p-1)} \deg(\Delta_x) , \]

where \( \Delta_x \) is the ideal discriminant of \( Z \). When \( p_1/x \) is unramified

\[ \deg \Delta_x = \deg_k(x) \Delta , \]

where \( \Delta \) is the divisor discriminant, and so, by the genus formula, (19), and (21),
\[ m \leq - \frac{1}{p(p-1)} \deg \Delta = - \frac{2G}{p(p-1)} - \frac{2}{p}. \]

When \( p_{1/x} \) is ramified,

\[ \Delta = (\Delta_x) p_{1/x}^{(p-1)(\lambda_\infty + 1)}, \]

and so

\[ \deg \Delta_x = \deg \Delta - (p - 1)(\lambda_\infty + 1). \]

Using the genus formula, it follows from (18) and (21) that

\[ m \leq -p\left( \frac{\deg \Delta - (p - 1)(\lambda_\infty + 1)}{p(p-1)} \right) - \lambda_\infty \]

\[ \leq \frac{1}{p-1}(2G - 2(p-1) - (p-1)(\lambda_\infty + 1) + \lambda_\infty(p-1)) \]

\[ \leq -\frac{2G}{p-1} - 1. \]

In either case there is a prime \( \mathfrak{p}_\infty \) of \( \mathbb{Z} \) lying over \( p_{1/x} \) such that

\[ v_{\mathfrak{p}_\infty}(\alpha) \leq m \leq -e_\infty\left( \frac{2G}{p(p-1)} + \frac{1}{p} \right), \]

where \( e_\infty \) is the ramification index of \( \mathfrak{p}_\infty \). This completes the proof of Theorem 10.
Since Theorem 6 holds for all cyclic extensions of $k(x)$ of prime power degree, there is a bound on the minimum degree of a prime of $k(x)$ which splits completely in an Artin-Schreier extension. This, together with the bound given by Theorem 10, gives the following:

**Theorem 11:** Let $Z$ be an Artin-Schreier extension of $k(x)$. If $G$ is the genus of $Z$, $e_\infty$ is the ramification index of a prime over the infinite prime, $m = m_0$ of Theorem 6, and $E$ is the exponent of the null class group of $Z$, then

$$E \geq \frac{e_\infty}{m} \left( \frac{2G}{p(p - 1)} + \frac{1}{p} \right).$$

**Corollary:** In the class of Artin-Schreier extensions of $k(x)$ for a fixed finite field $k$, the exponent of the null class group approaches infinity as the genus of the field goes to infinity.

The proof of Theorem 11 parallels the proof of Theorem 7, and the approximation for $m$ used in the proof of the corollary of that theorem gives

$$E \geq \frac{\log a}{7 \log G} \left( \frac{2G}{p(p - 1)} + \frac{1}{p} \right).$$

Thus

$$\lim_{G \to \infty} E = \infty.$$
The Main Result

Let \( k \) be a finite field with \( q \) elements and with characteristic \( p \). The next step is to combine the results of Chapter II with the results of the first part of this chapter to show that, for a special class of extensions of \( k(x) \), the exponent of the null class group approaches infinity as the genus of the field goes to infinity. This special class of extensions consists of these geometric abelian extensions \( Z \) of \( k(x) \) of fixed degree where the \( p \)-primary part of the Galois group is elementary abelian. These are exactly those extensions of \( k(x) \) whose Galois group is the direct product of cyclic groups of prime power order for primes other than the characteristic and groups of order equal to the characteristic.

Let \( K/k(x) \) be an extension as described above, and let \( G \) be its genus. Then,

\[
\text{GAL}(K/k(x)) = C_1 \times C_2 \times C_3 \ldots \times C_n
\]

where each \( C_i \) is a cyclic group of the proper type. There is a subfield \( Z_i \) corresponding to each \( C_i \) such that

\[
\text{GAL}(Z_i/k(x)) = C_i
\]

These subfields are, therefore, either cyclic geometric extensions of \( k(x) \) of prime power degree for primes other than the characteristic or are Artin-Schreier extensions of \( k(x) \). Thus,
the result has been established for all of the subfields $Z_i$ of $K$. The first step in extending this result to $K$ is to show that, if $G$ is large, then the genus $G_i$ of some $Z_i$ is also large. To this purpose a lemma and Theorem 12 are proved.

**Lemma 3:** Let $Z_1$, $Z_2$, and $K$ be extensions of $k(x)$ such that $Z_i \subset K$, for $i = 1, 2$, and such that

$$\text{GAL}(K/k(x)) = \text{GAL}(Z_1/k(x)) \times \text{GAL}(Z_2/k(x)).$$

Then, as divisors of $K$,

$$\delta(K/Z_1) \text{ divides } \delta(Z_2/k(x))$$

and

$$\delta(K/Z_2) \text{ divides } \delta(Z_1/k(x)),$$

where $\delta$ denotes the different of the proper extension.

**Proof:** Let $\mathcal{O}_1$, $\mathcal{O}_2$, and $\mathcal{O}$ be the respective integral closures of $k[x]$ in $Z_1$, $Z_2$, and $K$. Also let $\delta_x(K/Z_1)$ and $\delta_x(Z_2/k(x))$ be the Dedekind differentials in the respective extension. It is well-known that $\delta_x(Z/k(x))$ is the greatest common divisor of the differentials of all the elements of $\mathcal{O}_2$. However,

$$\text{GAL}(K/Z_1) \cong \text{GAL}(K/k(x))/\text{GAL}(Z_1/k(x)) \cong \text{GAL}(Z_2/k(x)),$$

and $\mathcal{O}_2 \subset \mathcal{O}$. Thus the different of an element of $\mathcal{O}_2$ in the
extension $Z_2/k(x)$ can also be considered as the different of an element of $\mathfrak{G}$ in the extension $K/Z_1$. Therefore,

$$\delta_x(K/Z_1) \text{ divides } \delta_x(Z_2/k(x)).$$

This completes the proof for all prime divisors of $K$ that do not lie over the infinite prime of $k(x)$. For the complete proof of the lemma, it is necessary to extend the divisibility to include the infinite primes. This is done by observing that $k(x) = k(\frac{1}{x})$ and that the global different is the product of the local different. Therefore,

$$\delta(K/Z_1) \text{ divides } \delta(Z_2/k(x)).$$

**Theorem 12:** Let $K$ and $Z_i$, $i = 1, 2, \ldots, h$, be geometric extensions of $k(x)$ such that:

1. $[K: k(x)] = n$ and $[Z_i: k(x)] = n_i$, $i = 1, 2, \ldots, h$;
2. $K$ has genus $G$, and $Z_i$ has genus $G_1$, $i = 1, 2, \ldots, h$;
3. $Z_i \subset K$, for $i = 1, 2, \ldots, h$;
4. $\text{GAL}(K/k(x)) = \text{GAL}(Z_1/k(x)) \times \text{GAL}(Z_2/k(x)) \times \ldots \times \text{GAL}(Z_h/k(x)).$

Then for some field $Z_i$, say $Z_1$,

$$G_1 \geq \frac{1}{n^2}(G - (h - 1)n + \sum_{i=1}^{h} \frac{n}{n_i} - 1).$$
Proof: For the purposes of this proof, $Z_{i_1} Z_{i_2} \cdots Z_{i_s}$ will denote the smallest subfield of $K$ containing the fields $Z_{i_1}, Z_{i_2}, \ldots, Z_{i_s}$. In this particular case,

$$\text{GAL}(Z_{i_1} Z_{i_2} \cdots Z_{i_s} / k(x)) = \text{GAL}(Z_{i_1} / k(x)) \times \text{GAL}(Z_{i_2} / k(x)) \times \cdots \times \text{GAL}(Z_{i_s} / k(x)).$$

Now in the tower of fields $K > Z_1 \geq k(x)$,

$$\delta(K/k(x)) = \delta(Z_1/k(x)) \delta(K/Z_1),$$

considered as divisors of $K$. Now, by the lemma,

$$\delta(K/Z_1) \text{ divides } \delta(Z_2 Z_3 \cdots Z_h / k(x)),$$

and so

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2 Z_3 \cdots Z_h / k(x)).$$

Similarly,

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2/k(x)) \delta(Z_3 Z_4 \cdots Z_h / k(x)).$$

This can be continued until

$$\delta(K/k(x)) \text{ divides } \delta(Z_1/k(x)) \delta(Z_2/k(x)) \cdots \delta(Z_h/k(x)).$$

Taking degrees in $K$ gives:
\[ \deg_K(\delta(K/k(x))) \leq \sum_{i=1}^{h} \deg_K(\delta(Z_i/k(x))) \]

\[ \leq \sum_{i=1}^{h} n_i^* \deg_{Z_i}(\delta(Z_i/k(x))) \]

where \( n_i^* = \frac{n}{n_i} \), \( i = 1, 2, ..., h \). After applying the genus formula, this gives

\[ 2G + 2(n - 1) \leq \sum_{i=1}^{h} n_i^*(2G_i + 2(n_i - 1)), \]

and so,

\[ \sum_{i=1}^{h} n_i^* G_i \geq G - (h - 1)n + \sum_{i=1}^{h} n_i^* - 1. \]

Since \( n \geq n_i^* \), there must be some \( G_i \), say \( G_1 \), such that

\[ G_1 \geq \frac{1}{n^2}(G - (h - 1)n + \sum_{i=1}^{h} n_i^* - 1) \]

and this completes the proof.

**Theorem 13:** In the class of abelian geometric extensions of \( k(x) \) of fixed degree \( n \), where \( k \) is a fixed finite field with characteristic \( p \), in which the \( p \)-primary part of the Galois group is elementary abelian, the exponent of the null class group approaches infinity as the genus of the field approaches infinity. In fact if \( K \) is a field in this class with genus \( G \) large enough, the exponent \( E \) of the null
The class group is bounded by

\[ E \geq C \frac{\frac{G}{n} + M}{\log \left( \frac{G}{n} + M \right)} \],

where \( C \) and \( M \) are constants.

**Proof:** Let

\[ \text{GAL}(K/k(x)) = C_1 \times C_2 \times \cdots \times C_h, \]

where each \( C_i \) is a group of prime power order, and let \( Z_i \) be the subfield of \( K \) for which

\[ \text{GAL}(Z_i/k(x)) = C_i, \quad i = 1, 2, \ldots, h. \]

Then by Theorem 12, \( C_1 \) can be chosen such that its genus \( G_1 \) is bounded by

\[ G_1 \geq \frac{1}{n} (G - (h - 1)n + \sum_{i=1}^{h} \frac{n}{n_i} - 1) \]

where \( n = [K: k(x)] \) and \( n_i = [Z_i: k(x)] \), \( i = 1, 2, \ldots, h \).

Since \( n \geq h \) this can be written as

\[ G_1 \geq \frac{G}{n^2} + M, \quad \text{for some constant } M. \]

Now \( Z_1 \) must be either a cyclic geometric extension of prime power degree or an Artin-Schreier extension of \( k(x) \). Thus by Theorems 7 and 11 (in particular (11) and (22)),
However, if \( G \) is large enough, \( \frac{G}{\log G} \) is an increasing function, and so,

\[
E_1 \geq \frac{2 \log q}{7 n_1(n_1 - 1)} \left( \frac{\log \left( \frac{G}{2} + M \right)}{n} \right). 
\]

Also since \( n \geq n_1 \),

\[
E_1 \geq \frac{2 \log q}{7 n(n - 1)} \left( \frac{\log \left( \frac{G}{2} + M \right)}{n} \right). 
\]

Thus, when the genus of \( K \) is large, there is a subextension \( Z_1 \) of \( k(x) \) whose null class group \( C_0(Z_1) \) has equally large exponent. The group \( C_0(Z_1) \) is mapped in a canonical way into \( C_0(K) \). This map (called the conorm) has the following property [4]

\[
|\text{Ker(conorm)}| \text{ divides } [K: Z_1].
\]

In this particular case,

\[
|\text{Ker(conorm)}| < [K: k(x)] = n.
\]

But then the null class group of \( K, C_0(K) \), contains a
subgroup,

\[ C_0(\mathbb{Z}_1)/|\text{ker(conorm)}|, \]

whose exponent is greater than or equal to \( \frac{E_1}{n} \). Thus by (23),

\[
E \geq \frac{E_1}{n} \geq \frac{2 \log q}{7 n^2(n - 1)} \cdot \frac{\frac{G^2}{n^2} + M}{\log(\frac{G^2}{n^2} + M)}.
\]

This completes the proof of the main theorem.
Introduction

The main object of this chapter is to use the techniques and
the results of Chapters II and III in a study of quadratic
extensions of $k(x)$. In his dissertation Emil Artin studied
the arithmetic and analytic theory of quadratic extensions of
$k(x)$ where $k$ is a field of prime order. His approach to this
subject is a complete analogy to the theory of algebraic number
fields, and, for this reason, he separated these extensions into
two classes, real and imaginary, depending upon (in the terminology
of this paper) the decomposition of the infinite prime of $k(x)$
in the extension. This distinction can be extended to arbitrary
extensions of $k(x)$.

Definition: If $K$ is an extension of $k(x)$ for which there
is only one prime divisor that lies over the infinite prime
of $k(x)$, then $K$ is called an imaginary extension of
$k(x)$; otherwise $K$ is a real extension of $k(x)$.

Notice that any prime of $k(x)$ of degree 1 may act as the
infinite prime since

\[ k(x) = k\left(\frac{1}{x + a}\right), \text{ for any } a \in k. \]

A field \( K \) is said to be a totally imaginary extension of \( k(x) \) if no prime of degree 1 in \( k(x) \) splits in \( K \).

In the course of his study of quadratic extensions of \( k(x) \), Artin discussed the problem of classifying all imaginary extensions of \( k(x) \) which have one class per Geschlecht, i.e., in which the ideal class group has exponent 2. He proved that the number of such fields is finite; more precisely, he showed that in any such field \( |k| = q = 3, 5, \text{ or } 7 \) and that (in the terminology of this paper) the genus is bounded. The techniques developed in the present paper can be used to remove the condition that \( k \) be a prime field and to substantially improve the bounds on the genus. However, for the sake of simplicity, this chapter will, for the most part, be confined to those imaginary extensions in which the infinite prime ramifies. In this case the methods of Artin give that when \( |k| = q = 3, 5 \text{ and } 7 \) the genus of the extension must be less than or equal to \( 9724, 9 \text{ and } 13 \) respectively. The results obtained through the methods of this paper are given in the form of

**Theorem 14:** If \( K \) is a quadratic imaginary extension of \( k(x) \) of genus \( G \), where \( k \) is a finite field of order \( q \), in which the infinite prime of \( k(x) \) ramifies, and if the ideal class group of \( K \) has exponent 2, then:
(i) $q = 9$, $G = 1$;
(ii) $q = 7$, $G = 1$;
(iii) $q = 5$, $G \leq 2$;
(iv) $q = 4$, $G \leq 2$;
(v) $q = 3$, $G \leq 4$;
or (vi) $q = 2$, $G \leq 8$.

The study of congruence function fields with ideal class exponent 2 is made by first considering those fields with null class exponent 2. If $K$ is a quadratic imaginary extension of $k(x)$ in which the ideal class group has exponent 2, then, since the null class group of an imaginary extension is a subgroup of the ideal class group [see 10, pp. 246-247], the null class group must either have exponent 2 or be of order 1. M. L. Madan and C. S. Queen [11] have shown that there are only 2 cases in which a quadratic extension of $k(x)$ has class number 1. In both of these cases, $q = 2$ and $G = 2$. Since it is assumed that the infinite prime of $k(x)$ ramifies, the connection is even simpler; for then, the ideal class group and the null class group are identical. Therefore, Theorem 14 follows immediately from the following two theorems.

Theorem 15: If $K$ is a quadratic extension of $k(x)$ for which the null class group has exponent 2, then $K$ is an imaginary extension of $k(x)$ for a suitable choice of $x$. 
In fact, if \( K \) has genus greater than or equal to 2, then \( K \) is a totally imaginary extension of \( k(x) \).

**Theorem 16**: Let \( K \) be a quadratic extension of \( k(x) \) with genus \( G \), where \( k \) is a finite field with \( q \) elements and in which not all the primes of degree 1 in \( k(x) \) are inert. If the null class group of \( K \) has exponent 2, then

1. \( q = 9 \), \( G = 1 \);
2. \( q = 7 \), \( G = 1 \);
3. \( q = 5 \), \( G \leq 2 \);
4. \( q = 4 \), \( G \leq 2 \);
5. \( q = 3 \), \( G \leq 4 \);
6. or \( q = 2 \), \( G \leq 8 \).

The restriction in Theorem 16 that not all the primes of degree 1 in \( k(x) \) are inert in \( K \) is imposed only for the sake of convenience and, as we shall see, is redundant for \( q = 7 \) and \( q = 9 \). Without this restriction, the methods used here give bounds on the genus that are roughly double those in Theorem 16. This also is a substantial improvement over the bounds obtained through Artin's method.

**Norms of Integral Elements in Imaginary Extensions**

With the definition of imaginary extensions, Theorems 4, 5 and 10 take on a special meaning. In an imaginary extension \( K \) of \( k(x) \), there is only one prime \( P \) which lies over the
infinite prime $p_{1/x}$ of $k(x)$. Then

$$ \deg N(\alpha) = -v_{p_{1/x}}(N(\alpha)) $$

$$ = -\frac{1}{e_\infty} v_{p_\infty}(\prod_{\sigma \in \text{GAL}(K/k(x))} \sigma(\alpha)), \text{ where } e_\infty \text{ is the ramification index of } p_\infty, $$

$$ (24) $$

$$ = -\frac{1}{e_\infty} \sum_{\sigma \in \text{GAL}(K/k(x))} v_{\sigma p_\infty}(\alpha) $$

$$ = -\frac{p}{e_\infty} v_{p_\infty}(\alpha), \quad p^n = [K: k(x)]. $$

Thus, in imaginary extensions, Theorems 4, 5 and 10 can be used to give bounds on the degrees of norms of primitive integral elements. In particular this gives

**Theorem 17:** Let $k$ be a finite field of order $q$, and let $K$ be an imaginary extension of $k(x)$ with genus $G$.

(A) If $K$ is a cyclic geometric extension of $k(x)$ of prime power degree for a prime other than the characteristic, then, for any $\alpha \in K$ which is both a primitive element for the extension $K/k(x)$ and integral over $k[x],$

$$ \deg N(\alpha) \geq \deg(\prod p_1(x)), $$

where the product is taken over all the ramified polynomial primes of $k(x).$
(B) If \( K \) is a geometric Artin-Schreier extension of \( k(x) \), then, for any \( \alpha \in K \) which is both a primitive element for the extension \( K/k(x) \) and integral over \( k[x] \),

\[
\deg N(\alpha) \geq \deg \left( \prod P_i(x) \right) + \max\{\deg n(x), \deg d(x)\},
\]

where the product is taken over all the ramified polynomial primes of \( k(x) \) and where \( n(x) \) and \( d(x) \) are defined by the generating equation of \( K \),

\[
y^p - y = \frac{n(x)}{d(x)}.
\]

(C) If \( K \) is a geometric quadratic extension of \( k(x) \), then, for any \( \alpha \in K \) which is integral over \( k[x] \) but not in \( k[x] \),

\[
\deg N(\alpha) \geq 2G + 1.
\]

Proof:

(A) If \( \{\theta_i\} \) is the fundamental basis constructed in Theorem 3, then

\[
\alpha = a_0(x)\theta_0 + a_1(x)\theta_1 + \ldots + a_{p^n-1}(x)\theta_{p^n-1},
\]

and

\[
v_{\Pi_\infty}(\alpha) = \min_{0 \leq j < p^n} (v_{\Pi_\infty}(a_j(x)\theta_j)) \leq \min_{0 \leq j < p^n} (v_{\Pi_\infty}(\theta_j)).
\]
Then by (6), this gives

\[ v_{\mathfrak{p}_\infty}(\alpha) \leq -\frac{e}{\ell} \sum \deg p_i(x), \]

where the sum is taken over all the ramified primes of \( k(x) \). Thus, plugging this into (24) gives

\[ \deg N(\alpha) \geq \deg(\prod p_i(x)). \]

But this proves the theorem only when \( k \) contains the \( p^n \)-th roots of 1; however, just as Theorem 4 extends to Theorem 5, it is possible to drop this condition on the roots of unity.

(B) Since \( K \) is an imaginary extension, (24) gives

\[ \deg N(\alpha) = -\frac{D}{e_{\alpha}} v_{\mathfrak{p}_\infty}(\alpha). \]

Then, by (18), (19) and (20), in the notation of Theorem 10,

\[ v_{\mathfrak{p}_\infty}(\alpha) \leq -\frac{e}{\ell} \left( \sum_{i=1}^{\ell} (\lambda_i + 1) \deg p_i(x) + \lambda_\infty \right). \]

Thus

\[ \deg N(\alpha) \geq \sum_{i=1}^{\ell} (\lambda_i + 1) \deg p_i(x) + \lambda_\infty. \]

However, by definition,
\[ d(x) = \prod_{i=1}^{\ell} p_i(x) \lambda_i ; \]

\[ \lambda_\infty = \begin{cases} 
\deg n(x) - \deg d(x), & \text{if } \deg n(x) - \deg d(x) > 0 \\
0, & \text{if } \deg n(x) - \deg d(x) \leq 0
\end{cases} \]

This gives,

\[ \deg N(\alpha) \geq \begin{cases} 
\deg(\prod p_i(x)) + \deg n(x), & \text{if } \deg n(x) - \deg d(x) > 0 \\
\deg(\prod p_i(x)) + \deg d(x), & \text{if } \deg n(x) - \deg d(x) \leq 0
\end{cases} \]

This proves part \((B)\).

\((C)\) This is simply an application of Theorems 4 and 10, when \( p^n = 2 \) to \((24)\);

\[ \deg N(\alpha) = -\frac{2}{e_\infty} v_{\mathbb{F}_p}(\alpha) \geq 2G + 1. \]

This part of the theorem is stated separately only because it is in this form that the theorem will be used.

This completes the proof of Theorem 15.

**Corollary:** If \( K \) is an imaginary quadratic extension of \( k(x) \) for which the null class group has exponent 2, then, for any prime \( p \) of \( k(x) \) which splits in \( K \),

\[ \deg_{k(x)} p > \frac{G}{f_\infty} \]
where $G$ is the genus of $K$ and $f_{\infty}$ is the degree of the prime of $K$ over the infinite prime of $k(x)$.

**Proof:** Let $p(x)$ be the polynomial prime of $k[x]$ associated with the divisor prime $p$, and let $\mathfrak{p}$ be either prime of $K$ which lies over $p$. Thus,

$$\frac{\deg \mathfrak{p}}{\deg p} \in D_0(K).$$

Now since the exponent of the null class group is 2,

$$\left(\frac{f_{\infty}}{\frac{\deg \mathfrak{p}}{\deg p}}\right)^2 = (\alpha), \alpha \in K.$$

Taking norms of both sides gives

$$\left(\frac{f_{\infty}}{\frac{\deg \mathfrak{p}}{f_{\infty} \deg p}}\right)^2 = (N(\alpha)).$$

But then,

$$N(\alpha) = a \cdot p(\alpha)^{2f_{\infty}}$$

for some $a \in k$. By part (c) of the theorem,

$$2f_{\infty} \deg p(x) \geq 2G + 1.$$
Thus

\[ \deg p > \frac{G}{F_\infty}. \]

This proves the corollary.

This leads to the proof of Theorem 15.

Proof: Now, \( K \) is a quadratic extension of \( k(x) \) for which the null class group has exponent 2. Suppose there is a prime of degree 1 in \( k(x) \) which splits in \( K \); let it be the infinite prime of \( k(x) \). Then, if \( \mathfrak{P}_1 \) and \( \mathfrak{P}_2 \) are 2 primes of \( K \) which lie over the infinite prime of \( k(x) \),

\[ \frac{\mathfrak{P}_1 \cdot \mathfrak{P}_2}{\mathfrak{P}_0} \in D_0(K). \]

Therefore,

\[ \frac{\mathfrak{P}_1 \cdot \mathfrak{P}_2}{\mathfrak{P}_0} = (\alpha), \]

and, by Theorems 4 and 10,

\[ 2 > G + \frac{1}{2}, \]

\[ \therefore G < \frac{3}{2}. \]

Thus, if a prime of degree 1 splits in such a \( K \), \( K \) has genus 1.
Next, suppose all the primes of degree 1 in \( k(x) \) split in \( K \); then \( K \) has genus 1 and has \( 2q + 2 \) primes of degree 1, where \( |k| = q \). However, by the Riemann hypothesis,

\[
| (2q + 2) - (q + 1) | \leq 2\sqrt{q},
\]

or equivalently,

\[
q - 2\sqrt{q} + 1 \leq 0.
\]

This cannot happen for \( q > 1 \). So some prime of degree 1 in \( k(x) \) must not split in \( K \), and this concludes the proof.

**Proof of Theorem 16**

The first step in the proof of Theorem 16 is to establish an upper bound on the order of constant field of a congruence function field with null class exponent 2. This bound is furnished by a well-known result in algebraic geometry. From algebraic geometry, it is known that the p-rank of the null class group of an algebraic function field over an algebraically closed field of constants is \( 2G \), if \( p \) is not the characteristic, and is at most \( G \) when \( p \) is the characteristic. Thus in a congruence function field the 2-rank of the null class group is at most \( 2G \) when 2 is not the characteristic and at most \( G \) when 2 is the characteristic. This gives immediately,

**Lemma 4**: If \( K/k \) is a congruence function field in which
the null class group has exponent 2, then

\[ |k| = q = 2, 3, 4, 5, 7, \text{ or } 9. \]

**Proof:** If \( k \) has odd characteristic, then for \( h \), the class number of \( K \),

\[
(25) \quad h \leq 2^{2G},
\]

since \( C_0(K) \) is at most the product of \( 2G \) copies of \( \mathbb{Z}_2 \). However, by the Riemann hypothesis,

\[
(q^{1/2} - 1)^{2G} \leq h \leq 2^{2G}.
\]

This implies

\[ q \leq 9. \]

If \( k \) has characteristic 2, then

\[
(q^{1/2} - 1)^{2G} \leq h \leq 2^d,
\]

or, equivalently

\[ q \leq 6. \]

This proves the lemma.

Now, returning to the proof of Theorem 16, if \( K \) is an extension of \( k(x) \) which has null class exponent 2, then by Theorem 15, there is some prime of degree 1 in \( k(x) \) which does
not split in \( K \). If, further, \( K \) is such that not all the primes of degree 1 of \( k(x) \) are inert in \( K \) and such that the genus \( G > 1 \), then some prime of degree 1 must ramify. Thus it can be assumed that the \( K \) in Theorem 16 is imaginary and that the infinite prime of \( k(x) \) ramifies in \( K \). Now under this assumption, the corollary to Theorem 17 says that no prime of degree \( G \) or less can split in \( K \). However, this fact together with the techniques employed in the proof of Theorem 6 gives that if the genus of \( K \) is odd and

\[
q^G - 2q^{G/2} + 1 > GR,
\]

where \( R \) is the number of primes of \( k(x) \) that ramify in \( K \), then there is a prime of degree at most \( G \) which splits in \( K \). Thus \( K \) could not have genus \( G \).

Case i: \( q = 9 \). The number of primes of \( k(x) \) which ramify in \( K \) is less than or equal to \( 2G + 2 \) (the degree of the discriminant by the genus formula). Thus the genus \( G \) cannot be odd and satisfy

\[
g^G - 2 \cdot G \cdot 3^G + 1 > G(2G + 2).
\]

Thus, if the genus of \( K \) is odd it must be 1; for, when \( G = 3 \),

\[
g^3 - 2 \cdot 3 \cdot 3^3 + 1 = 568 > 24 = 3(6 + 2).
\]
If $G$ is even it cannot satisfy the inequality

$$9^{G-1} - 2 \cdot G \cdot 3^{G-1} + 1 > (G - 1)(2G + 2),$$

and then it must be $2$; for if $G = 4$

$$9^3 - 2 \cdot 4 \cdot 3^3 + 1 = 514 > 30 = 3(8 + 2).$$

Thus, if $q = 9$, the genus of $K$ must be $1$ or $2$. Further analysis rules out the case of genus $2$; for by (25) the class number of $K$ with genus $2$ is $2, 4, 8$ or $16$. Also by Lemma 4, there can be no prime of degree $1$ or $2$ which splits in $K$. Let $M_i$ be the number of primes of $K(x)$ of degree $i$ which ramify in $K$, and let $N_i$ be the number of primes of $K$ of degree $i$. By the genus formula for $G = 2$,

(26) \[ 0 \leq M_1 + 2M_2 \leq \deg \delta = 6. \]

Also, since no prime of degree $1$ or $2$ splits in $K$,

(27) \[ N_1 = M_1; \]

(28) \[ N_2 = M_2 + (q + 1) - M_1. \]

The zeta function $L(u)$ of $K$ is given by [see 11, p. 427],

$$L(u) = 1 + (N_1 - (q + 1))u + \frac{1}{2}(N_1^2 - N_1 - 2qN_1 + 2N_2 + 2q)u^2$$

$$+ q(N_1 - (q + 1))u^3 + qu^4,$$
and plugging (27) and (28) into $L(1)$ gives

$$h = 1 + \frac{1}{2}(M_1^2 - M_1) + M_2$$

which is independent of $q$.

In this particular case where $q = 9$, the Riemann hypothesis gives

$$(1 - q^{1/2})^4 = 16 \leq h.$$ 

Thus $h$ must be 16. There is however only one simultaneous solution for (26) and (29) for $h = 16$; this is, $M_1 = 6$ and $M_2 = 0$. In this case the zeta function must be

$$L(u) = 1 - 4u - 26u^2 - 36u^3 + 81u^4.$$ 

However, by the Riemann hypothesis the reciprocals of the roots of $L(u)$ are $3e^{i\theta_1}$, $3e^{i\theta_2}$, and thus

$$L(u) = (1 - 3e^{i\theta_1}u)(1 - 3e^{-i\theta_1}u)(1 - 3e^{i\theta_2}u)(1 - 3e^{-i\theta_2}) =$$

$$= (1 - 6 \cos \theta_1 u + 3u^2)(1 - 6 \cos \theta_2 u + 3u^2).$$

Therefore,

$$\cos \theta_1 + \cos \theta_2 = \frac{2}{3},$$

$$\cos \theta_1 \cos \theta_2 = -\frac{11}{9},$$
and so \( \cos \theta_1 \) and \( \cos \theta_2 \) are roots of the equation

\[
x^2 - \frac{2}{3}x - \frac{11}{9} = 0.
\]

The roots of this equation are not both between \(-1\) and \(1\). There is no field of the proper type with \( q = 9, \ G = 2 \).

Case ii: \( q = 7 \). Again if \( G \) is the genus of \( K \), there are at most \( 2G + 2 \) primes of \( k(x) \) that ramify in \( K \). Thus \( G \) cannot be odd and satisfy

\[
7^G - 2G7^{G/2} + 1 > G(2G + 2).
\]

Then if \( G \) is odd, it must be 1, for \( G = 3 \) satisfies this inequality. If \( G \) is even it must be 2 because \( G = 4 \) satisfies

\[
7^G - 1 - 2G7^{G-1/2} + 1 > (G - 1)(2G + 2).
\]

Now in this case where \( q = 7 \), the Riemann hypothesis gives

\[
h \geq (1 - 7^{1/2})^4 \sim 7.1,
\]

and so \( h = 8 \) or 16. There is only one simultaneous solution of (26) and (29) each for \( h = 8 \) and \( h = 16 \). These solutions and the zeta functions they imply are:

\begin{align*}
\ h = 16; & \ M_1 = 6, \ M_2 = 0; \ L(u) = 1 - 2u - 18u^2 - 14u^3 + 49u^4 \\
\ h = 8; & \ M_1 = 4, \ M_2 = 1; \ L(u) = 1 - 4u - 10u^2 - 28u^3 + 49u^4 .
\end{align*}
However, the same methods used above show that these cannot be the zeta functions of congruence function fields. Thus if \( q = 7 \), then \( G = 1 \).

Case iii: \( q = 5 \). There are at most \( 2G + 2 \) primes of \( k(x) \) that ramify in \( K \). If \( G \) is odd, it cannot satisfy

\[
5^G - 2 \cdot G \cdot 5^{G/2} + 1 > G(2G + 2),
\]

and must therefore be 1. Similarly if \( G \) is even it must be 2. Thus if \( q = 5 \), then \( G \leq 2 \).

Case iv: \( q = 4 \). In this case \( K/k(x) \) is an Artin-Schreier extension, and so all ramification must be wild. This allows a better estimate on the number of primes of \( k(x) \) that ramify in \( K \). If \( G = 3 \), the degree of the discriminant is 8. Now since the ramification is wild, each prime that appears in the discriminant has a power of at least 2. Thus, there are at most 4 primes of \( k(x) \) that ramify in \( K \). But,

\[
4^3 - 2 \cdot 3 \cdot 2^3 + 1 = 17 > 12 = 3 \cdot 4.
\]

And so there is no congruence function field of the proper type of odd genus larger than 1.

If \( G \) is even, consider \( G = 6 \). The degree of the discriminant is 14, and thus there are at most 6 primes of \( k(x) \) which ramify in \( K \) (6 since there are only 5 primes of degree 1
in \( k(x) \). Then

\[ 4^5 - 2 \cdot 6 \cdot 2^5 + 1 > 5 \cdot 6. \]

Both of these facts together give that, when \( q = 4 \), \( G \) must be 1, 2, or 4. Further analysis of the type used in the case of \( q = 9 \), \( G = 2 \) rules out \( G = 4 \). There are 13 possible combinations of ramified primes which give a power of 2 for the class number. These can all be eliminated by studying the zeta functions they imply. And so, \( q = 4 \) implies \( G = 1 \) or 2.

Case v: \( q = 3 \). In this case a more accurate approximation of the number of primes that ramify is needed. If \( G = 5 \), then the degree of the discriminant is 12. There are however only 4 primes of degree 1 in \( k(x) \). Thus there are at most 8 primes of \( k(x) \) that ramify in \( K \), 4 of degree 1 and 4 of degree 2. However,

\[ 3^5 - 2 \cdot 5 \cdot 3^{5/2} + 1 > 5 \cdot 9. \]

Thus if \( q = 3 \), then \( G \leq 4 \).

Case iv: \( q = 2 \). This is an Artin-Schreier case, so all the ramification is wild. In this case a similar procedure gives \( G \leq 8 \). This completes the proof of Theorem 16.

The restriction on the primes of degree 1 in the statement of Theorem 16 is redundant when \( q = 7 \) and \( q = 9 \). In a
quadratic extension $K$ of $k(x)$ in which the null class group has exponent 2, all the classes in this group are ambiguous, i.e., they are fixed by the action of the Galois group of $K/k(x)$. Thus the class number $h$ of $K$ is equal to the ambiguous class number $h_0$. There is a well-known theorem of F. K. Schmidt [see 12, p. 69] which can be used to calculate the ambiguous class number of $K$. In particular, when $K$ is a geometric quadratic extension of $k(x)$ which has null class exponent 2 and in which all the primes of degree 1 of $k(x)$ are inert, 

$$h = h_0 \leq 2^{\ell - 1},$$

where $\ell$ is the number of primes in $k(x)$ which ramify in $K$. If $G$ is the genus of $K$, the genus formula shows that the degree of the discriminant is $2G + 2$. Since no prime of degree 1 in $k(x)$ ramifies in $K$,

$$\ell \leq G + 1;$$

$$\therefore h \leq 2^G.$$

Now, by the Riemann hypothesis,

$$(1 - q^{1/2})2^G \leq h \leq 2^G,$$

or equivalently,

$$q \leq 3 + \sqrt{8} < 6.$$
BIBLIOGRAPHY


