INFORMATION TO USERS

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

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

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

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

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

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

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

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106
PAL, Sat, 1942-
ABELIAN VARIETIES, A CONJECTURE OF
R. M. ROBINSON AND CLASS NUMBER
RELATIONS IN ALGEBRAIC FUNCTION
FIELDS.

The Ohio State University, Ph.D., 1976
Mathematics

Xerox University Microfilms, Ann Arbor, Michigan 48106
ABELIAN VARIETIES, A CONJECTURE OF R. M. ROBINSON

AND

CLASS NUMBER RELATIONS IN ALGEBRAIC 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

Sat Pal, B.A. (Hons.), M.A., M.S.

* * * * *

The Ohio State University

1976

Reading Committee:

James R. C. Leitzel
Robert Gold
Arno Cronheim
Manohar L. Madan

Approved By

[Signature]
Advisor
Department of Mathematics
ACKNOWLEDGMENTS

I take great pleasure in expressing my deep gratitude and sincerest thanks to my advisor Dr. Manohar L. Madan for his invaluable guidance, help, constant encouragement and numerous discussions throughout the preparation of this dissertation. I also wish to express my deep gratitude to my parents and teachers, especially Professor Bhattacharya, Professor Shanti Narayan and Mr. G. D. Sharma for creating my interest in mathematics and guiding me through difficult times in my life. Finally, I would like to thank my wife, Rajni, who had to face a lot of difficult days during my graduate work at Ohio State. I am also thankful to Miss Dodie Huffman for doing an excellent job of typing.
VITA

July 11, 1942 .................................. Born - Hoti Mardan, India (now Pakistan)

1963 .................................. B.A. (Hons.) Math, University of Delhi, India (Gold Medalist)

1965 .................................. M.A. Math, University of Delhi, India (Gold Medalist)

1965-1970 .................................. Lecturer in Math, Hans Raj College, University of Delhi, India

1970-1972 .................................. Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

1972 .................................. M.S., The Ohio State University, Columbus, Ohio

1972-1976 .................................. Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

FIELDS OF STUDY

Major Field: Mathematics

Studies in Analysis. Professors B. Baishanski and Ranko Bojanic

Studies in Topology. Professors Norman Levine and Henry Glover

Studies in Algebra. Professors Robert Gold and Manohar Madan

Studies in Number Theory. Professors Alan Woods, Manohar Madan and Robert Gold
TABLE OF CONTENTS

Page

ACKNOWLEDGMENTS ........................................... 11

VITA .............................................................................. 111

INTRODUCTION ......................................................... 1

Chapter I

§1. ROBINSON'S CONJECTURE ................................. 5

§2. CLASSIFICATION OF ABELIAN VARIETIES .......... 19

§3. APPLICATIONS TO ALGEBRAIC FUNCTION FIELDS .... 29

§4. REMARKS .............................................................. 50

Chapter II

§1. PRELIMINARIES ..................................................... 52

§2. GALOIS COHOMOLOGY .......................................... 56

§3. A THEOREM OF E. ARTIN ....................................... 68

BIBLIOGRAPHY .......................................................... 73
INTRODUCTION

This dissertation consists of two parts.

In Chapter I, we are concerned with the classification, up to isogeny, of abelian varieties with one rational point over finite fields, partial results on a conjecture of R. M. Robinson and applications to algebraic function fields. For the classification problem, because of the Poincaré-Weil Theorem, it is enough to consider only the simple abelian varieties. By the Honda-Tate theory [6, 18], a simple abelian variety over a field with \( q \) elements is determined up to isogeny by a Weil number. A Weil number is an algebraic integer which, together with all its conjugates has absolute value \( q^{1/2} \), \( q \) denoting a prime power. It turns out that for \( q = 2 \), there are infinitely many isogeny classes of simple abelian varieties with one rational point. For \( q = 3 \) and \( q = 4 \), in each case, there is one isogeny class. For \( q \) larger than \( 4 \), there are no such varieties.

The problem of determining the minimal polynomials of the relevant set of Weil numbers is closely related to a conjecture [15] of R. M. Robinson which states that the polynomial

\[
G_m(y) = \prod_{0 \leq k \leq m/2} [y^2 - (4 + 2\cos \frac{2k\pi}{m})y + 1]_{(k,m)=1}
\]
is irreducible for all natural numbers $m$ except 2, 7 and 30. We prove this conjecture for the case when $m$ is a prime and also show that $G_m(Y)$ is almost always irreducible. As a consequence, it follows that an interval obtained from

$$J_1 = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$$

by shortening it at either end contains only finitely many conjugacy sets of algebraic units. Robinson deduced this result from his general theory of critical intervals for the problem of algebraic units. An interval is called critical, if by lengthening it at both ends we obtain an interval which has infinitely many algebraic units and by shortening it at both ends, the resulting interval has only finitely many units. The critical interval $J_1 = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ itself contains infinitely many algebraic units. It is, however, not known what the conjugacy classes of these units are. This is the content of Robinson's conjecture. Robinson proved the conjecture for some infinite classes of cases and also, using a computer, its validity was checked for all $m$ not exceeding 426.

The infinite set of Weil numbers mentioned above also arises in another context. Let $F/K$, $E/L$ be algebraic function fields over finite fields of constants such that $E/F$ is finite and separable. Let $\overline{F}, \overline{E}$ be the fields obtained by extending the fields of constants to the algebraic closure. Let $J(\overline{F}), J(\overline{E})$ be the Jacobian varieties of the non-singular projective curves associated to $\overline{F}, \overline{E}$. When do $J(\overline{F}), J(\overline{E})$ have the same number
of rational points? In other words, when do the function fields $F/K$, $E/L$ have the same class number? This question was studied in [8]. However, that study left the problem unresolved in the following cases: $K$ is the prime field of 3 elements and $E/F$ is geometric, (that is $L = K$), or constant extension of degree 2; $K$ is the prime field of 2 elements, $E/F$ is a geometric extension of degree 2 or $E/F$ is a constant extension of degree 2 or 3. The explicit description of Weil numbers enables us to substantially improve the results in these cases except when $|K| = |L| = 2$ and $[E:F] = 2$.

Chapter II is devoted to galois cohomology of function fields and a theorem of E. Artin. In his dissertation [1], Artin proved that there are only finitely many quadratic extensions $E/K(\mathfrak{x})$ for which the ideal class group of the integral closure of $K[\mathfrak{x}]$ has exponent 2, if $K$ is a prime field of odd characteristic and the infinite prime does not split. The inequalities, from which Artin drew the conclusion about the finiteness, give also upper bounds on the genera of such fields. D. Madden [13] gave a substantial improvement of these upper bounds. He also included the case of characteristic 2 and allowed $K$ to be any finite field. In §3, we give a further improvement of Artin's Theorem. The null class group has exponent 2 for such fields. Using the class number formula for the ambiguous classes and counting the number of integral divisors in a divisor class of
sufficiently large degree, an application of the Riemann Hypothesis gives a bound on the genus. If there is no ramified prime of degree one, these bounds are better than those obtained by Madden. In §2, we evaluate the galois cohomology for the null class group and the divisor class group associated with a cyclic extension $E/F$ of prime degree $\ell$, $F$ being an algebraic function field over a finite field of constants. The formula giving the number of ambiguous classes plays a key role in this evaluation. Knowing the ramification, one can calculate the ambiguous class number from the formula except in the case when the $\ell$-th roots of unity are contained in the field of constants and the degrees of all the ramified primes are divisible by $\ell$. In this case, the least positive degree of an invariant divisor class is 1 or $\ell$. Both the possibilities are realised. This answers affirmatively a question of Rosen [16].
CHAPTER I

§1. ROBINSON'S CONJECTURE

For a natural number \( m \), let \( Q(m) \) denote the field obtained from \( Q \), the field of rational numbers, by adjoining the \( m \)-th roots of unity. Let \( R(m) \) denote the maximal real subfield of \( Q(m) \). Let \( \eta = e^{2\pi i/m} \) and let

\[ \eta_1 = \eta, \eta_1^{-1}, \eta_2, \eta_2^{-1}, \ldots, \eta_{\varphi(m)/2}, \eta_{\varphi(m)/2}^{-1} \]

be its conjugates. Robinson's conjecture [15; p. 416] states that the polynomial

\[ g_m(y) = \prod_{0 \leq k \leq m/2 \atop (k,m) = 1} [y^2 - (4 + 2 \cos \frac{2\pi k}{m})y + 1] \]

is irreducible in \( \mathbb{Z}[y] \) except for \( m = 2, 7 \) and \( 30 \). Equivalently,

\[ (4 + 2 \cos \frac{2\pi}{m})^2 - 4 = (6 + \eta + \eta^{-1})(2 + \eta + \eta^{-1}) \]

is a square in \( Q(m) \) only for \( m = 2, 7 \) and \( 30 \).

Now,

\[ (6 + \eta + \eta^{-1})(2 + \eta + \eta^{-1}) = \eta^{-2}(6\eta + \eta^2 + 1)(2\eta + \eta^2 + 1). \]
Therefore, Robinson's conjecture reduces to the statement:
\[ \eta^2 + 6\eta + 1 \text{ is a square only for } m = 7 \text{ and 30}. \]

The following theorem gives a partial affirmative answer to Robinson's conjecture.

**Theorem 1.** Robinson's conjecture is true for almost all natural numbers.

**Proof:** Let

\[ (3) \quad \eta^2 + 6\eta + 1 = \beta^2 \]

where \( \beta \) is, necessarily, an algebraic integer in \( \mathbb{Q}(m) \).

Following Cassels [2], we denote by \( \mathcal{M}(\beta) \) the mean of the squares of the absolute values of the conjugates of \( \beta \). We separate the proof into two cases.

**Case 1.** Let \( m = 7m_1, (p,m_1) = 1 \). Then, \( \eta = \rho \xi \) where \( \xi \) and \( \rho \) are respectively, primitive \( p \)-th and \( m \)-th roots of unity. There is a representation [2; p. 114]

\[ (4) \quad \beta = \sum_{j=1}^{X} \gamma_j \xi_j^r, \quad 0 \leq r_j \leq p - 1 \]

where \( 0 \neq \gamma_j \) are integers in \( \mathbb{Q}(m_1) \) and \( r_j \) are incongruent modulo \( p \). The number \( X \) satisfies the inequality

\[ (5) \quad \mathcal{M}(\beta) \geq \frac{(p-X)X}{p-1}. \]
Further if \( m(\beta) < \frac{p + 3}{4} \), then, there is a representation (4) for which

\[
\text{(6)} 
X \leq \frac{p - 1}{2}.
\]

Now, (3) implies

\[
\text{(7)} 
m(\beta) \leq 8.
\]

We observe that \( X(p - X) \) is an increasing function in \((0, \frac{p}{2})\). Therefore, we see from (5), (6), and (7) that \( X \leq 8 \) if \( p > 73 \).

We consider, now, the following system of inequalities

\[
|L_j| = |x_j^u - pv_j| < \frac{p}{4}, \quad j = 1, \ldots, X,
\]

\[
|L_{X+1}| = |u| < 4^8 + 1 \leq \frac{p}{4}.
\]

The absolute value of the determinant of the matrix of coefficients is \( p^X \) and \( p^X < (p/4)^X(4^8 + 1) \). Therefore, by Minkowski's Theorem on linear forms, there exist rational integers \( u, v_1, \ldots, v_X \), not all zero, satisfying the above system. We can, clearly, assume that \( u \) is positive.

Turning, now, to (3), using (4), we rewrite it as

\[
\text{(8)} \quad p^2 x^2 + 6px + 1 = \left( \sum_{j=1}^{X} v_j^r x_j \right)^2.
\]
We observe that \((u,p) = 1\). Applying the automorphism of \(Q(m)/Q(m_1)\) defined by \(g \rightarrow g^u\), we obtain from (8),

\[
\rho g^{2u} + 6 \rho g^u + 1 = (\sum_{j=1}^{\Sigma} \gamma_j g^{s_j})^2
\]

\[= (\sum_{j=1}^{\Sigma} \gamma_j \frac{1}{p} J^{s_j})^2, \quad |s_j| = |r_j u - p v_j| < p/4,
\]

(9)

\[= \Sigma \gamma_t g^t, \quad |t| < p/2.\]

The total number of terms appearing in (9) does not exceed \(p - 1\), by our choice of \(p\). Therefore, (9) is an identity. Let

\(s_1 < s_2 < \ldots < s_\Sigma\). Comparing coefficients in (9), we obtain:

\[1 = \gamma_1^2 \gamma_1^{2s_1}, \quad \rho g^{2u} = \gamma_X^2 \gamma_X^{2s_X},\]

\[\therefore s_1 = 0, \quad |\gamma_1| = 1, \quad |\gamma_X| = |\rho| = 1, \quad s_X = u.\]

Therefore, (9) reduces to

\[\rho g^{2u} + 6 \rho g^u + 1 = (\gamma_1 + \gamma_X g^u)^2,\]

which implies

\[6 \rho = 2 \gamma_1 \gamma_X,\]

\[|6 \rho| = 6 = 2 \cdot |\gamma_1| |\gamma_X| = 2.\]
Thus, we have a contradiction for all $m$ which are divisible by a prime $p > 4^2 + 4$ and $p^2$ does not divide $m$.

We shall need the following lemma in the discussion of the second case.

**Lemma 1.** Let $g(m) =$ sum of the primitive $m$-th roots of unity. Then, $g(m) = \mu(m)$, where $\mu$ is the Möbius function.

**Proof:** Let $f(m) =$ sum of all the $m$-th roots of unity. Then,

$$f(m) = 0, \quad m > 1,$$

$$= 1, \quad m = 1.$$

Also, we have $f(m) = \sum_{d|m} g(d)$. Then, by Möbius inversion formula [4]

$$g(m) = \sum_{d|m} \mu(d) f\left(\frac{m}{d}\right)$$

$$= \mu(m).$$

**Q.E.D.**

**Case 2.** Let $m = p^N m_2$, $N \geq 2$. Then,

$$\beta^2 = \eta^2 + 6\eta + 1$$

implies

$$\beta^{2\eta^{-1}} = 6 + \eta + \eta^{-1},$$

(10) $\mathcal{M}(\beta) = 6$ by Lemma 1.
Let $\eta = \rho \xi$ where $\xi$ and $\rho$ are, respectively, $p^N$-th and $m_2$-th primitive roots of unity.

Let $L$ be any positive integer such that $2L \leq N$ and $m_1 = p^{N-L}m_2$. Then, $\beta$ has [2] a representation

\begin{equation}
\beta = \sum_{j=1}^{X} \gamma_j \xi^j, \quad 0 \leq r_j \leq p^L - 1
\end{equation}

where $0 \neq \gamma_j$ are algebraic integers in $Q(m_1)$. Then, (10) and [2; p. 115] imply that $X \leq 5$ in (11). As in Case 1, we consider, now, the system of inequalities

\begin{equation}
|I_j| = |r_ju - p^lv_j| < p^L/4, \quad j = 1, \ldots, X,
\end{equation}

\begin{equation}
|I_{X+1}| = |u| < 4^6 + 1 \leq p^L/4.
\end{equation}

The absolute value of determinant of the matrix of coefficients is $p^{IX}$ and $p^{IX} < (p^L/4)^X(4^6 + 1)$. Therefore, by Minkowski's Theorem on linear forms, there exists an integral solution $(u, v_1, v_2, \ldots, v_X)$ such that $u$ is positive. If $(u, p) = p^k$, $k > 0$, then let $u = p^ku'$. The system of inequalities (12) gives

\begin{equation}
|r_ju' - p^k v_j| < p^{L-k}/4, \quad j = 1, \ldots, X,
\end{equation}

\begin{equation}
|u'| < p^{L-k}/4, \quad (u', p) = 1.
\end{equation}
Replacing $L$ by $L' = L - k$, retaining the notation of (11), we can write

\[(13) \quad \beta = \sum_{j=1}^{X} \gamma_j \xi_j^r, \quad 0 \leq r_j \leq pL' - 1,\]

and the nonzero integers $\gamma_j$ are in $Q(p^n - L' m_2)$. From (3) and (13), we obtain

\[\rho^2 \xi^2 + 6\rho \xi + 1 = \left( \sum_{j=1}^{X} \gamma_j \xi_j^r \right)^2.\]

Applying the automorphism of $Q(m)/Q(m_2)$ given by $\sigma: \xi \mapsto \xi^{u'}$ to this equation, we get

\[\rho^{2u'} \xi^{2u'} + 6\rho \xi^{u'} + 1 = \left( \sum_{j=1}^{X} (\sigma \gamma_j) \xi_j^{u'} \right)^2 = \left( \sum_{j=1}^{X} \gamma_j \xi_j^{s_j} \right)^2, \quad |s_j| < pL'/4, \]

\[= \sum s_t \xi^t, \quad |t| < pL'/2.\]

This gives a contradiction as in Case 1, for all $m$ which are divisible by $p^N$, $N \geq 2$ and such that $p^{N/2} \geq 4L' + 4$. From Case 1 and Case 2 we see that Robinson's conjecture is almost always true.

**Corollary.** There are only finitely many natural numbers $m$ such that the maximal real subfield $R(m)$ of $Q(m)$ is generated by a unit which together with all its conjugates,
lies in the interval \([3 - 2\sqrt{2}, 3 + 2\sqrt{2}]\).

**Proof:** The polynomial \(G_m(Y)\) is either irreducible or it is a product of two irreducible factors of degree \(\frac{1}{2} \varphi(m)\), (see Lemma 3). The field \(R(m)\) is generated by a root of any of the irreducible factors of \(G_m(Y)\). The roots of \(G_m(Y)\) are units which lie in \([3 - 2\sqrt{2}, 3 + 2\sqrt{2}]\). Therefore, the polynomial is irreducible iff \(R(m)\) cannot be generated by a unit in \([3 - 2\sqrt{2}, 3 + 2\sqrt{2}]\).

**Theorem 2.** An interval obtained from \(J_\perp = [3 - 2\sqrt{2}, 3 + 2\sqrt{2}]\) by shortening it at either end contains only finitely many conjugacy classes of units.

**Proof:** The roots of the equation 

\[y^2 - (4 + 2 \cos \frac{2\pi}{m})y + 1 = 0\]

are 

\[
\frac{(4 + 2 \cos \frac{2\pi}{m}) \pm \sqrt{(6 + 2 \cos \frac{2\pi}{m})(2 + 2 \cos \frac{2\pi}{m})}}{2},
\]

For large values of \(m\), these roots are close to \(3 \pm 2\sqrt{2}\). Therefore, since the polynomial \(G_m(Y)\) is almost always irreducible, by shortening the interval at either end, it can contain only finitely many full conjugacy classes of algebraic units. Q.E.D.
The following theorem is, in general, weaker than Theorem 1. However, it contains a proof of Robinson's conjecture for prime values of \( m \). Moreover, for specific values, it gives more information than Theorem 1 depending upon the diophantine equation which occurs in the proof.

**Theorem 3.** Let \( k \) be a fixed natural number. Then,

\[
\text{Norm}_{R(kp)} \left( \eta + \eta^{-1} + 2 \right) \left( \eta + \eta^{-1} + 6 \right)
\]

is a square for only finitely many primes \( p \), where \( \eta \) is a primitive \( pk \)-th root of unity. For \( k = 1 \), the only primes are 2 and 7. For \( k = 2 \), there are no such prime.

We shall first prove a lemma.

**Lemma 2.** If \( p \) is a prime number, not dividing \( k \), then

\[
\varphi_{pk}(x) = \frac{\varphi_k(x^p)}{\varphi_k(x)}.
\]

**Proof:** Let \( \xi \) and \( \eta \) be respectively \( p \)-th and \( k \)-th roots of unity. The conjugates of \( \xi \) are \( \xi, \xi^2, \ldots, \xi^{p-1} \) and let \( \eta_1 = \eta, \eta_2, \eta_3, \ldots, \eta_h, h = \varphi(k) \) be the conjugates of \( \eta \). We note that \( \eta_1^p, \eta_2^p, \ldots, \eta_h^p \) is also a complete set of conjugates of \( \eta \). Then, \( \xi \eta \) is a primitive \( pk \)-th root of unity with \( \xi^i \eta_j, 1 \leq i \leq p-1, 1 \leq j \leq h \) as its conjugates. We have then
Proof: We, first discuss the case when $k > 2$. There are only finitely many primes which divide $k$. Therefore, we can assume $(p,k) = 1$, $p > 2$. Let

$$
\eta_1 = \eta, \eta_1^{-1}, \ldots, \frac{\eta_{\varphi(pk)}}{2}, \frac{\eta_{\varphi(pk)}^{-1}}{2}
$$

be the primitive $pk$-th roots of unity. The $pk$-th cyclotomic polynomial $\varphi_{pk}(x)$ satisfies, by Lemma 2,
\[(14) \quad \varphi_{pk}(x) = \frac{\varphi_k(x^p)}{\varphi_k(x)} \]

Now,

\[
\varphi_{pk}(x) = \prod_{j=1}^{\frac{\varphi(pk)}{2}} (x - \eta_j)(x - \eta_j^{-1})
\]

\[
= \prod_{j=1}^{\frac{\varphi(pk)}{2}} [x^2 - (\eta_j + \eta_j^{-1})x + 1].
\]

Therefore,

\[
\varphi_{pk}(-1) = \prod_{j=1}^{\frac{\varphi(pk)}{2}} (2 + \eta_j + \eta_j^{-1})
\]

\[(15) \quad = \frac{N_{R(pk)}}{Q(2 + \eta + \eta^{-1})}.\]

Since \( p \) is odd, (14) and (15) imply

\[(16) \quad \frac{N_{R(kp)}}{Q(2 + \eta + \eta^{-1})} = 1.\]

Also,
\[ \frac{\varphi(pk)}{2} \]
\[ \varphi_pk(-3 - 2\sqrt{2}) = \prod_{j=1} \left[ (3 + 2\sqrt{2})^2 + (\eta_j + \eta_j^{-1})(3 + 2\sqrt{2}) + 1 \right] \]
\[ = (1 + \sqrt{2})^{\varphi(pk)} \prod_{j=1} [3 + 2\sqrt{2} + \eta_j + \eta_j^{-1} + 3 - 2\sqrt{2}] \]
\[ = (1 + \sqrt{2})^{\varphi(pk)} N_{R(pk)}/Q(6 + \eta + \eta^{-1}). \]

From (14), we obtain

\[ (1 + \sqrt{2})^{\varphi(pk)} N_{R(pk)}/Q(6 + \eta + \eta^{-1}) = \frac{\varphi_k[-(1 + \sqrt{2})^2p]}{\varphi_k(-3 - 2\sqrt{2})}. \]

If \( N_{R(pk)}/Q(2 + \eta + \eta^{-1})(6 + \eta + \eta^{-1}) \) is a square of a rational integer \( u \), we see from (16) and (17)

\[ (1 + \sqrt{2})^{\varphi(pk)} u^2 = \frac{\varphi_k[-(1 + \sqrt{2})^2p]}{\varphi_k(-3 - 2\sqrt{2})}. \]

Let \( c = \varphi_k(-3 - 2\sqrt{2}) \), an integer in \( \mathbb{Z}[[\sqrt{2}] \), \( w = (1 + \sqrt{2})^p \), \( \varphi(pk) = 2n \), \( v = (1 + \sqrt{2})^n \). Then (18) reduces to

\[ c(vu)^2 = \varphi_k(-w^2). \]

Thus, \((vu, w)\) is an integral solution of the diophantine equation

\[ cs^2 = \varphi_k(-T^2) \]
in \( \mathbb{Z}[\sqrt{2}] \). Since \( \varphi_k(-T^2) \) has degree larger than 2, by Siegel's Theorem [7], this has only finitely many solutions in \( \mathbb{Z}[\sqrt{2}] \). This proves our theorem for \( k > 2 \).

Turning, now, to the exceptional cases, \( k = 2 \) has been considered by Robinson. He, in fact, proves that

\[
N_{R(m)/Q}(\eta + \eta^{-1} + 2)(\eta + \eta^{-1} + 6)
\]

is never a square for \( m = 2p^l, \ l \geq 1, \ p \) odd. For \( m = 2 \cdot 2 = 4 \), one sees directly that \( N_{R(4)/Q}(\eta + \eta^{-1} + 2)(\eta + \eta^{-1} + 6) = 12 \), which is not a square.

Finally, to prove that 7 is the only odd prime for which \( N_{R(p)/Q}(\eta + \eta^{-1} + 2)(\eta + \eta^{-1} + 6) \) is a square, we observe that \( \eta + \eta^{-1} + 2 \) is a square in \( R(p) \) and, therefore, we have to prove

\[
N_{R(p)/Q}(\eta + \eta^{-1} + 6) \text{ square implies } p = 7.
\]

Let

\[
\alpha = \eta + \eta^{-1} + 6 = \theta + 6.
\]

It is easy to check that the minimal equation for \( \theta \) is

\[
f(\theta) = \frac{1}{1 - \theta - \sqrt{\theta^2 - 4}} \frac{p-1}{2} \theta^{p-1} + \frac{1}{1 - \theta + \sqrt{\theta^2 - 4}} \frac{p-1}{2} \theta^{p-1} = 0
\]
Therefore,

\[ N_{R(p)}/Q(\alpha) = (-1)^\frac{p-1}{2} \varphi(2) \]

(19)

\[ = \frac{(1 - \sqrt{2})^{p-1}}{4 + \sqrt{8}} + \frac{(1 + \sqrt{2})^{p-1}}{4 - \sqrt{8}}. \]

We, also, have the identity

\[ \left[ \frac{(1 - \sqrt{2})^{p-1}}{4 + \sqrt{8}} + \frac{(1 + \sqrt{2})^{p-1}}{4 - \sqrt{8}} \right]^2 = \frac{1}{2}. \]

(20)

It is verified that

(21) \[ v = \sqrt{2} \left[ \frac{(1 - \sqrt{2})^{p-1}}{4 + \sqrt{8}} - \frac{(1 + \sqrt{2})^{p-1}}{4 - \sqrt{8}} \right] \in \mathbb{Z}. \]

Therefore, if \( N_{R(p)}/Q(\alpha) \) is square of a rational integer \( u \), we get from (19), (20), and (21) the equation

\[ 2u^4 - v^2 = 1. \]

It is a deep result of Ljunggren [10] that the only positive integral solutions of this equation are \( u = 1 = v \); \( u = 13 \), \( v = 239 \).

We see from (19) that \( u = 1 \) is not possible and that \( u = 13 \) corresponds to \( p = 7 \). This completes the proof of our theorem.
§2. ABELIAN VARIETIES WITH ONE RATIONAL POINT

In this section, we are concerned with the problem of explicit determination of minimal polynomials of Weil numbers which characterize the isogeny classes of simple abelian varieties of positive dimension over finite fields with one rational point. As we shall see, this is closely related to Robinson's conjecture discussed in the last section.

We collect below the most important definitions and results that we shall need. (The details can be found in [6, 18, 20].)

Definitions. Let $K$ be a finite field, $\overline{K}$ be its algebraic closure and let $\mathbb{P}^n(\overline{K})$ denote the projective $n$-space. An abelian variety $A$ defined over $K$ is an algebraic set in $\mathbb{P}^n(\overline{K})$ such that

1. $A$ is defined by polynomials with coefficients in $K$,
2. $A$ is irreducible,
3. there is a group law on $A$ for which the maps $a \times b \to ab$, $a \to a^{-1}$ of $A \times A \to A$ and $A \to A$, respectively, are morphisms.

Let $A$ and $B$ be abelian varieties defined over $K$. An isogeny $\varphi: A \to B$ is a surjective homomorphism which has a finite kernel. It turns out that isogeny is an equivalence
relation. We can, therefore, speak of isogeny classes. If $C$ is any subvariety of an abelian variety $A$, we say that $C$ is an abelian subvariety of $A$ if $C$ is also a subgroup of $A$. An abelian variety is called simple if it has no proper abelian subvarieties. The Frobenius endomorphism of an abelian variety $A$ defined over $K$ is the map which raises every coordinate to $q$-th power, $q$ being the number of elements in $K$. The characteristic polynomial $f_A$ of the Frobenius endomorphism of $A$ is a monic polynomial with rational integral coefficients of degree $2d$, where $d$ is the dimension of $A$. A Weil number $w$ for $q$ is an algebraic integer which, together with all its conjugates, has the absolute value $\sqrt{q}$. A point of an abelian variety is called rational over $K$ if its coordinates are in $K$.

**Results.**

I. Every abelian variety is isogenous to a product of powers of nonisogenous simple abelian varieties.

II. There is a bijection between isogeny classes of simple abelian varieties over $K$ and the conjugacy classes of Weil numbers for $q$. The characteristic polynomial $f_A$ for the isogeny class is equal to $P_A^e$, where $P_A$ is the minimal polynomial of the conjugacy class of Weil numbers and $e$ is a positive integer which is determined by $P_A$. Different isogeny classes have different characteristic polynomials.

III. Let $Q$ denote the field of rational numbers. A being
simple, the algebra $E = \operatorname{End} A \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra with center $\mathbb{Q}(w)$. Its local invariants are computed from the decomposition behavior of rational primes in $\mathbb{Q}(w)$. The local invariants determine the algebra uniquely [5]. Then, $e$ and the dimension of the simple abelian variety $A$ are given by

$$[E : \mathbb{Q}] = e^2[\mathbb{Q}(w) : \mathbb{Q}], \quad 2 \dim A = e[\mathbb{Q}(w) : \mathbb{Q}].$$

IV. The number of rational points of an abelian variety is $\mathcal{f}_A(1)$. The splitting of an abelian variety into simple abelian varieties corresponds to the factorization of $\mathcal{f}_A$ into irreducible factors.

Thus, to give a complete description of the isogeny classes of abelian varieties with one rational point, we have to give the minimal polynomials of the set of Weil numbers $w$ such that $\mathcal{f}_A(1) = 1$ for the polynomial $\mathcal{f}_A$ determined by $w$.

Consider, first, the case when the Weil number $w$ is real, i.e. $w = \pm \sqrt{q}$. In this case, $P(U) = U \pm \sqrt{q}$ or $U^2 - q$ according as $\sqrt{q}$ is rational or not. Thus, $|P(1)| = 1$ implies $q = 4$, $P(U) = U - 2$, or $q = 2$, $P(U) = U^2 - 2$. In each case $e = 2$ [19] and hence $E$ is a 4-dimensional algebra over $\mathbb{Q}(w)$. The variety $A$ has dimension one in the first case and two in the second case. The characteristic polynomials are $U^2 - 4U + 4$ and $U^4 - 4U^2 + 4$, respectively.

We turn, now, to the case when the Weil number $w$ is non-real.
In this case,

\[ P(U) = \prod_{j=1}^{g} (U - \sqrt{q} e^{\pm i \theta_j}) \]

\[ = \prod_{j=1}^{g} (U^2 - 2\sqrt{q} U \cos \theta_j + q). \]

Clearly, \( f_A(1) = 1 \) iff

\[ P(1) = \prod_{j=1}^{g} (q + 1 - 2\sqrt{q} \cos \theta_j) = 1. \]

(23)

The number \( \omega \) being non-real,

\[ q + 1 - 2\sqrt{q} \cos \theta_j > (\sqrt{q} - 1)^2. \]

(24)

From (23) and (24), we see that there are no non-real Weil numbers for \( q \geq 4 \) satisfying (23).

To deal with the cases \( q = 2 \) and \( q = 3 \), we consider the polynomial

\[ F(X) = \prod_{j=1}^{g} (X - \beta_j), \quad \beta_j = 2\sqrt{q} \cos \theta_j. \]

(25)

The polynomial \( F(X) \) is irreducible in \( \mathbb{Z}[X] \), has all its roots in the interval \((-2\sqrt{q}, 2\sqrt{q})\) and \( F(q + 1) = 1 \). Conversely, any such polynomial \( F(X) \) determines, uniquely, a polynomial...
P(U). We have, therefore, to determine the set of polynomials $F(X)$. For $q = 3$, we claim that $F(X) = X - 3$ is the only polynomial. Namely, $F(X) \neq X - 3$ implies

$$F(4) = \prod_{j=1}^{g} (4 - \beta_j) = \prod_{j=1}^{g} |4 - \beta_j| > \prod_{j=1}^{g} |3 - \beta_j| \neq 0.$$ 

But, $\prod_{j=1}^{g} (3 - \beta_j)$ is a rational integer. Thus $F(4) > 1$.

We shall need the following two lemmas for discussion of the case $q = 2$.

**Lemma 3.** Let $Q_m(Y) = \prod_{0 \leq k \leq m/2} [Y^2 - (4 + 2 \cos \frac{2\pi k}{m})Y + 1]$, $m \geq 1$, $D = \sqrt{\sigma^2 - 4}$ and $\sigma = 4 + 2 \cos \frac{2\pi}{m}$. Then

1. $D \notin R(m) = G_m(Y)$ is a product of two irreducible factors of same degree over $Z[Y]$.

2. $D \notin R(m) = G_m(Y)$ is irreducible in $Z[Y]$.

**Proof:** For $m = 1$ and 2, the assertion is clear.

For $m > 2$, let $K = Q(\sigma) = R(m)$, $\gamma = \frac{\sigma + D}{2}$ and we consider the extension $K(\gamma) = Q(D,\sigma)$. Now

$$\gamma \in Q(D,\sigma).$$

Also,
\[ \sigma - \sqrt{\frac{\sigma^2 - 4}{2}} = \frac{1}{\gamma} \in Q(\gamma). \]

Hence,

(27) \[ \sigma \in Q(\gamma) = Q(D, \sigma) \subset Q(\gamma). \]

Hence (26) and (27) \[ Q(\gamma) = Q(D, \sigma). \]

**Case 1.** \( D \in R(m) \). Then \( Q(\gamma) = Q(D, \sigma) = Q(\sigma) \). So
\[ Q(\gamma) = Q(\sigma) \] and hence minimal polynomial \( m(\gamma) \) of \( \gamma \) is of degree \( \frac{1}{2} \varphi(m) \). But all roots of \( G_m(\gamma) \) are of the type \( \gamma \) or \( \gamma_1 = \frac{\sigma - D}{2} = \gamma^{-1} \) and hence
\[ G_m(\gamma) = n(\gamma) \cdot n(\gamma_1), \] for some \( \gamma_1 \),

which proves 1.

**Case 2.** Now \( D \notin R(m) \). Then \( [Q(D, \sigma) : Q(\sigma)] = 2 \) implies
\[ [Q(\gamma) : Q] = [Q(D, \sigma) : Q] = \varphi(m) = G_m(\gamma) = m(\gamma), \] which proves 2.

**Lemma 4.** For \( m = 2, 7, \) and 30, \( G_m(\gamma) \) is reducible in \( Z(\gamma) \) and the corresponding Weil numbers are given by
\[ U^2 - 2U + 2, \]
\[ U^6 - 4U^5 + 9U^4 - 15U^3 + 18U^2 - 16U + 8, \]
\[ U^5 - 3U^4 + 2U^3 + U^2 - 12U + 8, \]
\[ U^8 - 4U^7 + 4U^6 + 7U^5 - 21U^4 + 14U^3 + 16U^2 - 32U + 16, \]
\[ u^8 - 5u^7 + 13u^6 - 25u^5 + 39u^4 - 50u^3 + 52u^2 - 40u + 16. \]

**Proof:** We have

\[ g_2(y) = (y - 1)^2 \]
\[ g_7(y) = (y^3 - 5y^2 + 6y - 1)(y^3 - 6y^2 + 5y - 1) \]
\[ g_{30}(y) = (y^4 - 8y^3 + 14y^2 - 7y + 1)(y^4 - 7y^3 + 14y^2 - 8y + 1). \]

Also, let

\[ \eta = e^{2\pi i/m}, \quad \xi = \eta + \eta^{-1}. \]

Then,

\[ D^2 = (\xi + 4)^2 - 4 = \xi^2 + 8\xi + 12. \]

For \( m = 2 \), \( D = 0 \).

For \( m = 7 \), \( \eta \) satisfies \( \eta^6 + \eta^5 + \eta^4 + \eta^3 + \eta^2 + \eta + 1 = 0 \)
and \( \xi \) satisfies \( \xi^3 + \xi^2 - 2\xi - 1 = 0 \) and then,
\[ D^2 = (2 - 3\xi - 2\xi^2)^2. \]

For \( m = 30 \), \( \eta \) satisfies \( \eta^8 + \eta^7 - \eta^6 - \eta^4 - \eta^3 + \eta + 1 = 0 \)
and \( \xi \) satisfies \( \xi^4 + \xi^3 - 4\xi^2 - 4\xi + 1 = 0 \) and then,
\[ D^2 = (4 - 5 - 2\xi^2)^2. \]

A simple calculation gives the above Weil numbers.

For \( q = 2 \), we show that there are infinitely many polynomials \( F(X) \). Substituting \( X = 3 - Y \) in (25), we obtain
\[ G(Y) = F(3 - Y) = \prod_{j=1}^{g} (3 - Y - \beta_j). \]

The irreducible polynomial \( G(Y) \) has all its roots in the interval \((3 - 2\sqrt{2}, 3 + 2\sqrt{2})\) and \( G(0) = 1 \). To give a description of all such polynomials \( G(Y) \), consider first, the set of polynomials

\[ G_m(Y) = \prod_{0 \leq k \leq m/2} [Y^2 - (4 + 2 \cos \frac{2\pi k}{m})Y + 1] \]

for \( m > 1 \). The roots lie in \((3 - 2\sqrt{2}, 3 + 2\sqrt{2})\), \( G_m(0) = 1 \).

By Lemma 3, \( G_m(Y) \) is either itself some \( G(Y) \) or is a product of two such \( G(Y) \).

Conversely, we claim that every polynomial \( G(Y) \) is obtained, as above, from some \( G_m(Y) \). If \( G(Y) \) is symmetric, let

\[ G(Y) = \prod_{j=1}^{g} (Y^2 - \sigma_j Y + 1). \]

The roots of the equation \( Y^2 - \sigma_j Y + 1 = 0 \) are

\[ \sigma_j \pm \sqrt{\sigma_j^2 - 4}. \]

Since the roots lie in the interval \((3 - 2\sqrt{2}, 3 + 2\sqrt{2})\) and \( G(Y) \) is irreducible, we have

\[ 2 < \sigma_j < 6. \]
Let
\[ \sigma_j - 4 = \eta + \eta^{-1}, \]
so that
\[ \eta^2 - \eta(\sigma_j - 4) + 1 = 0. \]
This gives
\[ \eta = \frac{(\sigma_j - 4) \pm \sqrt{(\sigma_j - 4)^2 - 4}}{2}. \]

Since \(|\sigma_j - 4| < 2\), we see that \(|\eta| = 1\). This is also true of all conjugates of \(\eta\). Therefore, \(\eta\) is a root of unity and \(G(Y) = G_m(Y)\) for some \(m\).

If \(G(Y) = (-Y)^g + a_{g-1}Y^{g-1} + \ldots + 1\) is not symmetric, the polynomial \(G(Y) \overline{G}(Y)\), where
\[ \overline{G}(Y) = Y^g + a_1Y^{g-1} + \ldots + a_{g-1}Y + (-1)^g, \]
is symmetric. The above argument shows that \(G(Y) \overline{G}(Y)\) is \(G_m(Y)\) for some \(m\) up to multiplication by \(-1\).

Thus, we have a description of the set of Weil numbers associated with isogeny classes of simple abelian varieties which have one rational point. Assuming the validity of Robinson's conjecture, we collect the results of the above discussion in the form of
Theorem 4. The conjugacy classes of Weil numbers determining the isogeny classes of simple abelian varieties with one rational point are the roots of the following set of irreducible polynomials

\[ u - 2, \quad u^2 - 3u + 3, \quad u^2 - 2, \quad u^2 - 2u + 2, \]

\[ u^6 - 4u^5 + 9u^4 - 15u^3 + 18u^2 - 16u + 8, \]

\[ u^6 - 3u^5 + 2u^4 + u^3 + 4u^2 - 12u + 8, \]

\[ u^8 - 4u^7 + 4u^6 + 7u^5 - 21u^4 + 14u^3 + 16u^2 - 32u + 16, \]

\[ u^8 - 5u^7 + 13u^6 - 25u^5 + 39u^4 - 50u^3 + 52u^2 - 40u + 16, \]

and

\[ \prod_{(k,m) = 1}^{\left(\frac{2 - 2 \cos \frac{2\pi k}{m}}{2} + \sqrt{\left(\frac{4 + 2 \cos \frac{2\pi k}{m}}{m}\right)^2 - 4}\right)} [u^2 - \left\{ \frac{2 - 2 \cos \frac{2\pi k}{m}}{2} + \sqrt{\left(\frac{4 + 2 \cos \frac{2\pi k}{m}}{m}\right)^2 - 4}\right\} u + 2] \]

for \( m \neq 2, 7, \text{ and } 30. \)
§3. APPLICATIONS TO ALGEBRAIC FUNCTION FIELDS

Let $E/L$ be a finite separable extension of $F/K$, the finite fields $K$ and $L$ are the exact fields of constants. When do the function fields $E/L$, $F/K$ have the same class number? This question was studied in [8]. In this section, we shall show how the results of [8] can be substantially improved by using some results from the theory of abelian varieties and the explicit description of Weil numbers obtained in the last section. Let $\overline{K}$ be the algebraic closure of $K$. The function field $\overline{F}/\overline{K}$, $\overline{F} = \overline{FK}$ determines a non-singular projective curve to which is associated its Jacobian variety which is an abelian variety. The numerator polynomial, $L_F(U)$, of the zeta function of $F/K$, (we shall call it, simply the zeta function), is the reciprocal polynomial of the characteristic polynomial of the Frobenius endomorphism of this variety.

**Theorem 5.** Let $E/K$ be a finite separable extension of $F/K$. Then $L_E(U) L_F(U)^{-1}$ is a polynomial of degree $2(g_E - g_F)$ with rational integral coefficients, $g_E$, $g_F$ denoting the genera.

**Proof:** Let $\overline{K}$ be the algebraic closure of $K$. Consider the function fields $\overline{E}/\overline{K}$ and $\overline{F}/\overline{K}$ where $\overline{F} = \overline{FK}$, $\overline{E} = \overline{EK}$. 29
Let \( \overline{C}_{OF} \) and \( \overline{C}_{OE} \) be the classes of degree zero of \( \overline{F} \) and \( \overline{E} \) which are considered identified with the corresponding Jacobians. Then, the map \( \overline{C}_{OF} \rightarrow \overline{C}_{OE} \) induced by the inclusion \( F \subset E \) has a finite kernel. Its image \( \overline{C}'_{OF} \) is an abelian variety and hence \( \overline{C}_{OF} \rightarrow \overline{C}'_{OF} \) is an isogeny defined over \( K \). Therefore [18], the characteristic polynomial of \( \overline{C}_{OF} \) is the characteristic polynomial of \( \overline{C}'_{OF} \) and this divides the characteristic polynomial of \( \overline{C}_{OE} \). This proves our theorem, because \( L_E(U) \) and \( L_F(U) \) have degrees \( 2g_E \) and \( 2g_F \), respectively, and the zeta function is the reciprocal of the characteristic polynomial.

**Corollary:** If \( g_F = 1 \), and \( E/K \) is unramified, then \( E \) and \( F \) have the same zeta function.

**Proof:** By the genus formula \( g_E = 1 \) and the degree of the zeta function is twice the genus.

**Theorem 6.** Let \( E/K \) be separable over \( F/K, g_F > 1, [E:F] = n \). Then,

(a) \( h_E > h_F \) in each of the following cases:

(i) \( q > 4 \),
(ii) \( q = 4, g_F \geq 9 \),
(iii) \( q = 3, g_F \geq 35 \),
(iv) \( q = 3, g_F \geq 4, n \geq 3 \),
(v) \( q = 2, g_F \geq 3, g_E \geq 5g_F \).
(b) If $F$ is hyperelliptic then $h_E > h_F$ except, possibly, in the following cases:

$q = 3, q = 4, e_F = 2, e_E = 3, 4$;
$q = 3, q = 4, e_F = 3, e_E = 5$.

**Proof:** (i) From Theorem 5, we have

$L_E(u) = L_F(u) R(u) .

So, $h_E = h_F \cdot R(1) \geq h_F(\sqrt{q - 1})^{2g_E - 2g_F} > h_F$ if $q \geq 5$. This proves (i).

(ii) Using the notation of [8], one has $h_E > h_F$ whenever

$$T(g, q, g_0) = T(g, q) = (q - 1)[q^{2g - 1} + 1 - 2g \cdot q^{2g - 1}]
- (2g - 1)(q^g - 1)(q^{1/2} + 1)^{2g_0}$$

is positive, $g = e_E, g_0 = e_F$. We have

$$T(g, h, g_0) = 3 \cdot 4^g[4^{g - 1} - g - (2g - 1)^3] + 3 + (2g - 1)^3 2g_0 .$$

By the genus formula, $g \geq 2g_0 - 1$.

Writing $g = 2g_0 - 1 + m$, it is sufficient to show

$$4^{2g_0 - 2 + m} - (2g_0 - 1 + m) - (4g_0 - 3 + 2m) \cdot 3 2g_0 - 1$$

is positive for $g_0 \geq 9, m \geq 0$. Equivalently, it is sufficient to show

$$T'(g_0, m) = 4^{3m} h^2 2g_0 - 2 - (2g_0 - 1 + m) \cdot 3 2g_0 - 2 - (12g_0 - 9 + 6m)$$
is positive for \( g_0 \geq 9, m \geq 0 \).

For any fixed \( g_0 \geq 9 \),

\[
T'(g_0, m) - T'(g_0, 0) = 0 \quad \text{for} \quad m = 0,
\]

\[
= m \left[ \frac{h^m}{m} \left( \frac{h}{3} \right)^2 g_0 - 2 - \frac{1}{3 (2g_0 - 2) - 6} \right],
\]

\( m > 0 \)

\[
\geq \left( \frac{h}{3} \right)^{16} - 7 > 0, \quad m > 0,
\]

and hence, for \( g_0 \geq 9, m \geq 0 \), \( T'(g_0, m) \geq T'(g_0, 0) \). We have \( T'(9, 0) = 0.7699996 > 0 \). Also

\[
\frac{d^2 T'}{dg_0^2} = \left( \frac{h}{3} \right)^2 2g_0 - 2 \cdot 2 \cdot (\ln \frac{h}{3}) + \frac{(2g_0 - 1)}{(2g_0 - 2) \cdot 2} \cdot 2 \cdot \ln 3 - \frac{2}{(2g_0 - 2) - 12}
\]

\[
\geq \left( \frac{h}{3} \right)^{16} \cdot 2(\ln \frac{h}{3}) - 14 > 0.
\]

Thus, \( T'(g_0, 0) \) is an increasing function of \( g_0, g_0 \geq 9 \). Since \( T'(9, 0) > 0 \), we get \( T'(g_0, 0) > 0 \) for \( g_0 \geq 9 \), which proves the required result.

(iii) We omit the proof which is similar to that of (ii).

(iv) We have, as in (i) and Theorem 4,

\[
1 + \overline{a}_1 U + \overline{a}_2 U^2 + \ldots = \]

\[
= (1 + a_1 U + a_2 U^2 + \ldots)(1 - 3U + 3U^2)^{g - g_0}
\]
and hence
\[ a_1 - 3(g - g_0). \]

So [11],
\[ N_1 = N_1 - 3(g - g_0) \]

where \( N_1 \) and \( N_1 \) are the number of primes of degree 1 of \( E \) and \( F \), respectively. Also, the Riemann Hypothesis implies
\[ N_1 \leq 4 + 2g_0\sqrt{3}. \]

And, so
\[ N_1 \leq 4 + (2\sqrt{3})g_0 - 3(g - g_0) \geq 0, \]

only if
\[ g \leq \frac{4 + (3 + 2\sqrt{3})g_0}{3}. \]

But, if \( n \geq 3, g \geq n(g_0 - 1) + 1 \geq 3g_0 - 2 \) and
\[ 3g_0 - 2 > \frac{4 + (3 + 2\sqrt{3})g_0}{3}, \]
if \( g_0 \geq 4 \). This proves (iv).

(v) This is proved in [8].

(b) Now, let \( F \) be hyperelliptic. Let \( q = 4 \). Then
\[ N_1 \leq 10 \] because \([ F : K(X)] = 2 \) and \( K(X) \) has 5 primes of degree one. We have by Theorems 4 and 5,
\[ L_{p}(U) = L_{p}(U)(1 - 4U + 4U^{2})^{g - g_0} \]

or

\[ 1 + \tilde{a}_1 U + \tilde{a}_2 U^2 + \ldots = (1 + a_1 U + a_2 U^2 + \ldots)(1 - 4U + 4U^{2})^{g - g_0}. \]

Comparing coefficients,

\[ \tilde{a}_1 = a_1 - 4(g - g_0) \]

and, hence,

\[ \tilde{N}_1 = N_1 - 4(g - g_0) \leq 10 - 4(g - g_0) \geq 0. \]

Therefore,

\[ g \leq g_0 + 2 \]

(28) i.e. \[ g - g_0 \leq 2 \]

Also, by the genus formula, \[ g \geq n(g_0 - 1) + 1 \] which gives

(29) \[ g - g_0 \geq (n - 1)(g_0 - 1). \]

Our assertion is obvious from (28) and (29).

For \( q = 3 \), the proof is similar.

Assuming Robinson's conjecture for part (c) of the following theorem, we give, now, a substantial improvement of Theorem 3 in [8]. The irreducibility of \( L_{p}(U) \) means that the algebra of
endormorphisms of the corresponding Jacobian variety is commutative [18].

**Theorem 7.** Let $E/L$ be a constant extension of $F/K$, $g_F > 1$, $|K| = q$, $E = FL$. Then, $h_E > h_F$ in each of the following cases:

(a) $q \geq 3$,
(b) $q = 2$, $[L:K] \geq 3$, $L_p(U)$ irreducible,
(c) $q = 2$, $[L:K] = 2$, $g_F > 3$, $L_p(U)$ irreducible.

**Proof:** (a) We have to consider [8] only the case $q = 3$, $[L:K] = 2$. Let $h_E = h_F$. Then [3], $L_E(U) = L_F(U)$ $L_F(-U)$ gives $L_F(-1) = 1$. Therefore, by Theorem 4,

$$1 - a_1 U + a_2 U^2 + \ldots = L_F(-U) = (1 - 3U + 3U^2) g_F.$$  

Comparing coefficients [11],

$$a_1 = N_1 - 4 = 3g_F,$$

$$2a_2 = N_1^2 - 7N_1 + 2N_2 + 6 = 9g_F^2 - 3g_F = (4 + 3g_F)^2 - 7(4 + 3g_F) + 2N_2 + 6.$$  

Hence, $2N_2 = -6(g_F - 1) < 0$, a contradiction.

**Proof (b):** We have to consider [8] only the case $[L:K] = 3$. We shall give the proof in the cases $g = 2$ and $3$ only, for the method of proof for $4 \leq g \leq 9$ is similar to that in the case $g = 3$. Before proving the theorem, we shall prove the following
proposition, which will be useful in restricting the number of cases to be considered for $3 \leq g \leq 9$.

**Proposition 1.** Let $\alpha$ be an algebraic integer. Let the minimal polynomial $m(\alpha, x)$ of $\alpha$ be of degree $2g$. Then, $m(\eta \alpha, x)$ is of degree $g$, $2g$ or $4g$, where $\eta$ is a complex cube root of unity.

**Proof:** We consider the following cases:

**Case (i).** Let $\eta \in Q(\alpha)$, $\eta \not\in Q(\eta \alpha)$. In this case $Q(\alpha) = Q(\eta \alpha, \eta)$. We have

$$2g = [Q(\alpha) : Q] = [Q(\eta, \eta \alpha) : Q(\eta \alpha)][Q(\eta \alpha) : Q]$$

$$= 2[Q(\eta \alpha) : Q]$$

$$= [Q(\eta \alpha) : Q] = g.$$ 

**Case (ii).** $\eta \not\in Q(\alpha), \eta \in Q(\eta \alpha)$. In this case, $Q(\eta, \alpha) = Q(\eta \alpha)$. So, we have

$$[Q(\eta \alpha) : Q] = [Q(\eta, \alpha) : Q] = 4g.$$ 

**Case (iii).** $\eta \in Q(\alpha), \eta \in Q(\eta \alpha)$. Here $Q(\alpha) = Q(\eta \alpha)$. So,

$$[Q(\eta \alpha) : Q] = 2g.$$ 

**Case (iv).** $\eta \not\in Q(\alpha), \eta \not\in Q(\eta \alpha)$. Then,
From the four cases considered above, we see that we have proved the proposition.

Proof of the Theorem: Let $h_E = h_F$. Then [3]

$$L_E(U) = L_F(U) L_F(\eta U) L_F(\eta^2 U)$$

gives

$$(30) \quad L_F(\eta) L_F(\eta^2) = 1.$$ 

Let

$$L_F(U) = 1 + a_1 U + a_2 U^2 + \ldots = \prod_{1}^{g} (1 - \alpha_i U)(1 - \bar{\alpha}_i U),$$

$\bar{\alpha}_i$ denoting the complex conjugates of $\alpha_i$.

Let

$$H(U) = L_F(\eta U) L_F(\eta^2 U)$$

$$= \prod_{1}^{g} [1 - (\alpha_i \eta + \alpha_i \eta^2) U + 2U^2][1 - (\bar{\alpha}_i \eta + \alpha_i \eta^2) U + 2U^2]$$

$$= \prod_{1}^{2g} (1 - \gamma_i U + 2U^2).$$
Hence, it corresponds to the polynomial (in the sense of Theorem 4),

\[ F(X) = \prod_{i=1}^{2g} (X - \gamma_i). \]

Also by (30),

\[ H(1) = L_F(\eta) L_F(\eta^2) = 1. \]

Hence, \( L_F(\eta) \) is a unit of \( \mathbb{Q}(\eta) \). So,

\[ L_F(\eta) = -1, 1, -\eta, \eta, 1 + \eta, -1 - \eta. \]

Now, because of the above proposition, the irreducible factors of \( H(U) \) are of degree \( g, 2g \) or \( 4g \). We consider the following two cases, according as \( H(U) \) has repeated factors or not.

**Case 1.** Suppose \( H(U) \) has repeated factors. The roots of \( H(U) \) are \( \frac{1}{\alpha_i \eta}, \frac{1}{\alpha_i \eta^2}, \) \( i = 1, \ldots, 2g \), if \( \frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_{2g}} \) are the roots of \( L_F(U) \). As \( L_F(U) \) is irreducible, \( \alpha_i \) are all different, and, therefore, there exist \( i, j, i \neq j \) such that

\[ \alpha_i \eta = \alpha_j \eta^2 \]

\[ = \alpha_i = \alpha_j \eta. \]

Then, \( L_F(U) \) and \( H(U) \) have a root in common. The polynomial \( L_F(U) \) being irreducible, it divides \( H(U) \). Therefore,
\[ L_F(1) = 1 = h_F. \]

So [9, 11], the only possibilities are

(i) \( g = 2, N_1 = 0, N_2 = 3, \) or \( N_1 = 1, N_2 = 2; \)

(ii) \( g = 3, N_1 = 0, N_3 = 1, N_2 = 0 \) or \( 1. \)

The corresponding zeta functions are:

(i) \( 1 - 3U + 5U^2 - 6U^3 + 4U^4 , \)

(ii) \( 1 - 2U + 4U^2 - 4U^3 + 4U^4 , \)

(iii) \( 1 - 3U + 2U^2 + U^3 + 4U^4 - 12U^5 + 8U^6 , \)

(iv) \( 1 - 3U + 3U^2 + 2U^3 + 6U^4 - 12U^5 + 8U^6 . \)

In each case \( L_F(\eta) \) is not a unit.

Case 2. Suppose \( H(U) \) has no repeated factors. We have seen that the irreducible factors of \( H(U) \) are of degrees \( g, 2g, \) and \( 4g \) only; and if \( g \) is odd, the irreducible factors are of degrees \( 2g \) and \( 4g \) only, because the corresponding polynomial \( F(X) \) has degree half that of \( H(U) \). So, we have

\[ H(U) = \prod_{1}^{2g} (1 - \gamma_1 U + 2U^2) , \]

\[ F(X) = \prod_{1}^{2g} (X - \gamma_1) , \]

in the sense of Theorem 4.
Case $g = 2$. We observe that a field of genus 2 is necessarily, hyperelliptic since the dimension, as well as the degree of the canonical class, is two. The quotient of two integral divisors in it determines an $X$ such that [3, p. 32]

$$[F : K(X)] = 2.$$ 

Here, we have $L_p(\eta) = A + B\eta$, where

$$\begin{align*}
A &= 1 + 2a_1 - a_2, \\
B &= 4 + a_1 - a_2.
\end{align*}$$ (33)

By (32),

$$A + B\eta = -1, 1, -\eta, \eta, 1 + \eta, -1 - \eta.$$ 

Suppose $A = -1, B = 0$. In this case,

$$a_1 = 2, a_2 = 6, N_1 = 5, N_2 = 4.$$ (34)

There are 3 primes of degree one in $K(X)$, so two of them decompose and one ramifies. There is only one prime of degree two, corresponding to $X^2 + X + 1$ in $K(X)$ which can, at the most, decompose. Hence, $N_2 \leq 2$. So, this case is not possible. The proofs in the other cases are similar.

Case $g = 3$. Here, we have

$$H(U) = 1 - a_1 U + (a_1^2 - a_2)U^2 + (2a_3 - a_1 a_2)U^3 + \ldots.$$
Also,

\[ H(U) = \frac{6}{1} (1 - \gamma_1 U + 2U^2) \]

\[ = 1 - s_1 U + (s_2 + 12)U^2 + U^3(-10s_1 - s_3) + \ldots \]

where

\[
\begin{align*}
    s_1 &= \Sigma \gamma_1, \\
    s_2 &= \Sigma \gamma_1 \gamma_2, \\
    s_3 &= \Sigma \gamma_1 \gamma_2 \gamma_3,
\end{align*}
\]

(35)

Comparing coefficients above, we have

\[
\begin{align*}
    a_1 &= s_1, \\
    a_2^2 - a_2 &= 12 + s_2, \\
    2a_3 - a_1 a_2 &= -10s_1 - s_3.
\end{align*}
\]

(36)

This gives

\[
\begin{align*}
    a_1 &= s_1, \\
    a_2 &= s_1^2 - s_2 - 12, \\
    2a_3 &= s_1^3 - s_1 s_2 - 22s_1 - s_3.
\end{align*}
\]

(37)

We observe the following:
\[ s_1 \text{ even, } s_3 \text{ odd } \Rightarrow 2a_3 = \text{ odd}, \]
\[ s_1, s_2, s_3 \text{ odd } \Rightarrow 2a_3 = \text{ odd}, \]
\[ s_1 \text{ odd, } s_2, s_3 \text{ even } \Rightarrow 2a_3 = \text{ odd}. \]

Now, \( H(U) \) is of degree 12 and \( g = 3 \) is odd, so the only irreducible factors of \( H(U) \) are of degrees 12 and 6. Hence, the irreducible factors of \( F(X) \) are of degree 6 and 3.

We list the possibilities below:

(i) \( x^6 - 5x^5 - 3x^4 + 43x^3 - 33x^2 - 59x + 43, \quad s_1 = 5, \quad s_2 = -3, \quad s_3 = -43; \)

(ii) \( x^6 - 6x^5 + 3x^4 + 39x^3 - 60x^2 - 33x + 73, \quad s_1 = 6, \quad s_2 = 3, \quad s_3 = -39; \)

(iii) \( x^6 - 6x^5 + 3x^4 + 41x^3 - 78x^2 + 21x + 19, \quad s_1 = 6, \quad s_2 = 3, \quad s_3 = -41; \)

(iv) \((x^3 - 4x^2 + 3x + 1)(x^3 - 3x^2 - 4x + 13) = \]
\[ x^6 - 7x^5 + 11x^4 + 21x^3 - 67x^2 - 35x + 13, \quad s_1 = 7, \quad s_2 = 11, \quad s_3 = -21. \]

By (38), none of the above is possible. We omit the proofs in all other cases, \( 4 \leq g \leq 9 \), as in each case, we get a contradiction of the above type or that \( L_F(\eta) \) is not a unit in \( \mathbb{Q}(\eta) \).

Before proving Case (c), we prove a lemma.
Lemma 5. Let \( \eta_1, \eta_1^{-1}, i = 1, \ldots, \frac{\varphi(m)}{2} \) be the primitive \( m \)-th roots of unity and let

\[
\varphi_m(x) = x^{\varphi(m)} + Ax^{\varphi(m)-1} + Bx^{\varphi(m)-2} + \ldots
\]

Then,

(i) \( A = -1, 0 \) or \( 1 \),

(ii) \( B = -1, 0 \) or \( 1 \), \( m \geq 3 \),

\[
^{(d)}\binom{n}{2}
\]

(iii) \( B = \sum (\eta_1 + \eta_1^{-1}) (\eta_j + \eta_j^{-1}) + d, m \geq 3, \varphi(m) = 2d \).

Proof: (i) This is obvious from the definition of the Möbius function and Lemma 1.

(ii) Let \( \sigma_1^{(m)} = s_1^{(m)} = \Sigma \eta_1 \);

\[
\sigma_2^{(m)} = \Sigma \eta_1 \eta_2;
\]

\[
s_2^{(m)} = \Sigma \eta_1^2.
\]

We first calculate \( s_2^{(m)} \).

Case (a). Let \( m \) be odd. Then it is clear that if \( \eta_1 \)
is a primitive \( m \)-th root of unity, so is \( \eta_1^2 \). So, in this case

\[
s_2^{(m)} = s_1^{(m)} = \sigma_1^{(m)}.
\]

Case (b). Let \( m = 2n, (n,2) = 1 \). In this case, \( \eta_1 \) is a primitive \( m \)-th root of unity iff \( \eta_1^2 \) is a primitive \( n \)-th root.
of unity. Hence

\[ s_2^{(m)} = s_1^{(\frac{m}{2})} = \sigma_1^{(\frac{m}{2})}. \]

**Case (c).** Let \( m = 4n \), where \( n \) is, not necessarily, odd. In this case, we observe that if \( \eta_i \) is a primitive \( m \)-th root of unity, \( -\eta_i \) is also a primitive \( m \)-th root of unity; for, we have \( (-\eta_i)^m = 1 \). Let \( (-\eta_i)^h = 1 \), \( h < m \). Now, if \( h \) is even, we have \( \eta_i^h = 1 \), a contradiction. And, if \( h \) is odd, we have

\[ \eta_i^h = -1 \]
\[ \Rightarrow \eta_i^{2h} = 1 \]
\[ \Rightarrow m = 4n \mid 2h \]
\[ \Rightarrow 2n \mid h, \]

a contradiction. Hence, \( -\eta_i \) is also a primitive \( m \)-th root of unity. As

\[ (\eta_i)^2 = (-\eta_i)^2, \]

we have

\[ s_2^{(m)} = 2s_1^{(\frac{m}{2})} = 2\sigma_1^{(\frac{m}{2})}. \]

From the three cases considered above, we have
\[ s_2^{(m)} = \begin{cases} 
\sigma_1, & m \text{ odd;} \\
\frac{\sigma_1}{2^m}, & 2 | m, \quad 4 \not| \ m; \\
2\sigma_1, & 4 | m.
\end{cases} \]

Now, \( \sigma_1 = -A = 0, -1 \text{ or } 1; \) so \( s_2^{(m)} = 0, 1, -1, 2 \text{ or } -2. \) Also, we have the formula

\[ s_2 - s_1\sigma_1 + 2\sigma_2 = 0. \]

Hence,

\[ 2\sigma_2 = \sigma_1^2 - s_2. \]

If \( \sigma_1 = 1 \text{ or } -1, \) \( 2\sigma_2 = 1 - s_2. \) Now, \( s_2 \) can be \( 1 \) or \( -1, \) so \( \sigma_2 = 0 \text{ or } +1. \) If \( \sigma_1 = 0, \) \( 2\sigma_2 = -s_2 = 0, 2 \text{ or } -2. \) So \( \sigma_2 = 0, 1 \text{ or } -1. \) Hence, \( B = 0, 1, \text{ or } -1. \)

(iii) Let \( \varphi(m) = 2d, \) then we have

\[
x^{2d} + Ax^{2d-1} + Bx^{2d-2} + \ldots + Ex^2 + AX + 1 \\
= \prod_{1}^{d} (x - \eta_1)(x - \eta_1^{-1}) = \prod_{1}^{d} (x^2 - (\eta_1 + \eta_1^{-1})x + 1) \\
= x^{2d} - \sum_{1}^{d} (\eta_1 + \eta_1^{-1})x^{2d-1} + \\
x^{2d-2} \left[ \sum_{1}^{d} (\eta_1 + \eta_1^{-1})(\eta_j + \eta_j^{-1}) + d \right] + \ldots
\]
Comparing coefficients, we have

\[ B = \sum_{1}^{2} (\eta_i + \eta_i^{-1})(\eta_j + \eta_j^{-1}) + d. \]

Q.E.D.

**Proof of Case (c):**

Case 1. The polynomial \( g_m(y) \) of degree \( g \) of Theorem 4 is irreducible. Let \( h_E = h_F \). Then [3],

\[ L_E(U) = L_F(U) L_F(-U) \]

\[ = L_F(-1) = 1. \]

Let

\[ L_F(U) = 1 + a_1 U + a_2 U^2 + ... + a_g U^g. \]

(39)

\[ = \prod_{i=1}^{g} (1 - \alpha_i U)(1 - \overline{\alpha_i} U), \]

\( \overline{\alpha_i} \) denoting the complex conjugate of \( \alpha_i \). Therefore,

(40)

\[ L_F(-U) = 1 - a_1 U + a_2 U^2 + ... \]

\[ = \prod_{i=1}^{g} (1 + \alpha_i U)(1 + \overline{\alpha_i} U) \]

\[ = \prod_{i=1}^{g} (1 - \gamma_i U + 2U^2), \quad \gamma_i = -(\alpha_i + \overline{\alpha_i}), \]

(41)

\[ = 1 - \Sigma \gamma_1 U + (\Sigma \gamma_1 \gamma_2 + 2g)U^2 + ... \]
Comparing coefficients in (40) and (41), we get

\begin{equation}
\begin{cases}
a_1 = \Sigma \nu_1 \\
a_2 = \Sigma \nu_1 \nu_2 + 2g.
\end{cases}
\end{equation}

As in Theorem 4, we consider the polynomial of which the roots are $\nu_i$. Let

\begin{equation}
F(X) = \prod_{l=1}^{d} (X - \nu_l) = X^g - \Sigma \nu_1 X^{2g-1} + \Sigma \nu_1 \nu_2 X^{2g-2} + \ldots
\end{equation}

We now calculate $N_1$ and $N_2$. Let $\xi_i = \eta_i + \eta_i^{-1}$, where $\eta_i$, $\eta_i^{-1}$, $i = 1, \ldots, \frac{\phi(m)}{2}$ are the primitive $m$-th roots of unity. Then,

\begin{equation}
F(X) = G_m(Y) = \prod_{l=1}^{d} (Y^2 - (\xi_1 + 4)Y + 1) \text{ where } Y = 3 - X, \ d = \frac{g}{2},
\end{equation}

\begin{align*}
&= \prod_{l=1}^{d} \left[ X^2 + X(\xi_1 - 2) + (-3\xi_1 - 2) \right] \\
&= X^{2d} + \sum_{l=1}^{d} (\xi_1 - 2) X^{2d-1} + \\
&\quad \quad + X^{2d} - \sum_{l=1}^{d} \left[ -\Sigma (3\xi_1 + 2) + \Sigma (\xi_1 - 2)(\xi_j - 2) \right] + \ldots
\end{align*}

Using Lemma 5,
(45) \[ F(X) = X^{2d} + (-A - 2d)X^{2d-1} + X^{2d-2}(A + B - 5d + 2dA + 2d^2) + \ldots \]

Comparing the coefficients in (43) and (45), we have

\[
\begin{align*}
\Sigma Y_1 &= A + 2d \\
\Sigma Y_1 Y_2 &= A + B - 5d + 2Ad + 2d^2.
\end{align*}
\]

From (42), (44), and (46), we have

\[
\begin{align*}
a_1 &= A + 2d \\
a_2 &= A + B - d + 2dA + 2d^2.
\end{align*}
\]

Again [11], we have

\[
\begin{align*}
a_1 &= N_1 - 3 \\
2a_2 &= N_1^2 - 5N_1 + 2N_2 + 4.
\end{align*}
\]

So, we have

\[2N_2 = 2a_2 - \frac{N_1^2}{2} + 5N_1 - 4\]

(49)

\[= 2a_2 - a_1^2 - a_1 + 2.\]

Using (44) and (47), we obtain

\[2N_2 = A + 2B - 2g - A^2 + 2 = -A(A - 1) + 2B - 2g + 2\]

\[\leq 4 - 2g, \text{ by Lemma 5,}\]

\[< 0, \text{ if } g \geq 3.\]
Hence, we have proved that $h_E > h_F$ for $g \geq 3$, when the polynomial $G_m(Y)$ of degree $g$ is irreducible.

Case 2. We now, turn to the case when $G_m(Y)$ factors into two polynomials. Since we are assuming Robinson's conjecture and $g > 3$, by Lemma 4, we have to consider only the following two possibilities corresponding to $m = 30$.

1. $1 + 4U + 4U^2 - 7U^3 - 21U^4 + 14U^5 + 16U^6 + 32U^7 + 16U^8$,

2. $1 + 5U + 13U^2 + 25U^3 + 39U^4 + 50U^5 + 52U^6 + 40U^7 + 16U^8$.

In each case, (49) implies that $N_2$ is negative, which gives a contradiction. Hence, we have proved that $h_E > h_F$ for $g > 3$. 
§4. REMARKS

I. In the notation of Section 2, the polynomial $F(x)$ is irreducible for all $m \leq 426$. This was shown by Robinson and Brillhart [15]. To cover all the cases $g \leq 9$ in (b) of Theorem 7, we, therefore, need polynomials $F(x)$ of degree $\leq 18$. These were written down and (b) of Theorem 7 verified in each case.

II. We have given, in Theorem 4, an elementary argument to show that for $q = 3$, $U^2 - 3U + 3$ is the only irreducible polynomial $P(U)$ of a Weil number such that $P(1) = 1$. Using this, we can give a simpler proof than that in [11] for the fact that $g_F > 1$ implies $h_F > 1$.

For, suppose that there exists such a function field $F/K$ with $h_F = 1$. Then

$$L_F(U) = (1 - 3U + 3U^2)^{g_F}$$

$$= 1 - 3g_FU + \ldots$$

$$= 1 + a_1U + \ldots$$

Therefore,

$$-3g_F = a_1 = N_1 - 4.$$
So, $N_1 = 4 - 3g_F < 0$, which is a contradiction for $g_F > 1$.

III. We have shown in Theorem 7(c), that $g_F > 3$ implies $h_{FL} > h_F$ if $L_F(U)$ is irreducible. For $g_F = 3$, the example in [8] shows that $h_{FL} = h_F$ is possible. We show, now, that the zeta function in that example is the only possibility.

For, suppose there is such a function field $F/K$. If $L_F(U)$ is irreducible, the only possible $L_F(U)$, with $L_F(-1) = 1$, are

(1) $1 + 4U + 9U^2 + 15U^3 + 18U^4 + 16U^5 + 8U^6$,

(2) $1 + 3U + 2U^2 + U^3 + 4U^4 + 12U^5 + 8U^6$,

corresponding to the polynomials

$F(X) = X^3 - 4X^2 + 3X + 1$,

$F(X) = X^3 - 3X^2 - 4X + 13$, respectively.

Case (1) corresponds to the above given example. In Case (2), one can verify that $N_2 < 0$; hence this case is not possible.

If however, $L_F(U)$ is reducible, the only possibilities are

(3) $L_F(U) = (1 + 2U + 2U^2)^3$,

(4) $L_F(U) = (1 - 2U^2)^2(1 + 2U + 2U^2)$.

In each case, one verifies, as before, that $N_2 < 0$. 
CHAPTER II

§1. PRELIMINARIES

In this expository section, we introduce the notations for this chapter and state the various results from the cohomology theory of finite groups and class field theory which we shall need.

Facts from the Cohomology Theory of Finite Cyclic Groups.
Let \( G \) be a finite cyclic group and \( M \) be a \( G \)-module, (that is, \( M \) is a \( \mathbb{Z}[G] \)-module). The cohomology groups \( H^r(G,M) \) are defined for all \( r \geq 0 \). However,

\[
H^r(G,M) \cong H^{r+2}(G,M), \quad r \geq 0.
\]

Moreover,

\[
H^0(G,M) \cong \frac{M^G}{\text{Norm}(M)},
\]

\[
H^1(G,M) \cong \frac{\text{Crossed Homomorphisms}}{\text{Principal Crossed Homomorphisms}},
\]

\[
H^{-1}(G,M) \cong \frac{\text{Kernel of the Norm Map}}{(1 - \sigma)M}
\]

where

\( M^G \) = the Submodule of Invariant Elements,
and

\[ \sigma \text{ is a generator of } g. \]

We shall frequently use the following:

I. Let \( 0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0 \) be an exact sequence of \( G \)-modules. This induces the exact cohomology sequences

\[ \cdots \rightarrow H^r(G, M_1) \rightarrow H^r(G, M_2) \rightarrow H^r(G, M_3) \rightarrow H^{r+1}(G, M_1) \rightarrow \cdots, \]

\[ 0 \rightarrow M_1^G \rightarrow M_2^G \rightarrow M_3^G \rightarrow H^1(G, M_1) \rightarrow \cdots. \]

II. Hilbert's Theorem 90. If \( E/F \) is a cyclic extension and \( G = \text{gal}(E/F) \), then

\[ H^1(G, E) \cong H^{-1}(G, E) = 1. \]

We use the same symbol to denote a field and its multiplicative group.

III. Herbrand's Lemma. If \( M \) is a finite \( G \)-module, then

\[ h^1(G, M) = h^0(G, M), \]

where \( h^r(G, M) \) denotes the order of \( H^r(G, M) \).

Results from Class Field Theory. Let \( F \) be a field of algebraic functions of one variable having a finite field \( K \) with \( q \) elements as its exact field of constants. Let \( E/K \)
be a cyclic extension of $F/K$ such that $[E:F] = \ell$, a prime.

Let

$$G = \text{gal}(E/F);$$

$$E_p = \text{the completion of } E \text{ at a prime } \overline{p} \text{ of } E;$$

$$I_E(I_{OE}) = \text{the group of idèles (idèles of degree zero) of } E;$$

$$J_E(J_{OE}) = \text{the group of idèles classes (idèle classes of degree zero) of } E;$$

$$D_E(D_{OE}) = \text{the group of divisors (divisor of degree zero) of } E;$$

$$C_E(C_{OE}) = \text{the group of divisor classes (divisor classes of degree zero) of } E;$$

$$P_E = \text{the group of principal divisors of } E.$$

The group $G$ operates in a natural way on all these groups.

We shall need the following results from class field theory:

I. $h^1(G,J_E) = 1$, $h^0(G,J_E) = \ell$.

II. Let $p$ be a prime of $F$ and $\overline{p}$ be a prime of $E$ lying over $p$. An element $c \in F$ is called a local norm if it is norm in the extension $E_p/F_p$.

Hasse's Norm Theorem states that an element is a norm in $E/F$ iff it is everywhere locally a norm.
III. If the extension $E/F$ is unramified, then every element of $K$ is a norm.

IV. Let $\overline{p}$ be a ramified prime. A generator of $K$ is a local norm at $\overline{p}$ iff the degree of $\overline{p}$ is divisible by $\lambda$. 
§2. GALOIS COHOMOLOGY

Let $E/K$ be a cyclic extension of prime degree $\ell$ of an algebraic function field $F/K$ having the finite field $K$ as its exact field of constants. We evaluate, now, the cohomology groups for the various $G$-modules which are associated with the extension $E/F$. In particular, we prove

Theorem 8. (a) If $E/F$ is unramified,

$$h^0(G, C_{OE}) = h^1(G, C_{OE}) = \begin{cases} \ell^2, & \text{if } K \text{ contains the } \ell \text{-th roots of unity;} \\ \ell, & \text{if } K \text{ does not contain the } \ell \text{-th roots of unity.} \end{cases}$$

(b) If $E/F$ is ramified,

$$h^0(G, C_{OE}) = h^1(G, C_{OE}) = \begin{cases} 6(E/F) \cdot \ell^t, & \text{if } K \text{ does not contain the } \ell \text{-th roots of unity;} \\ \ell^{t-1}, & \text{if } K \text{ contains the } \ell \text{-th roots of unity and } \delta(E/F) = 1; \\ \ell^t, & \text{if } K \text{ contains the } \ell \text{-th roots of unity and } \delta(E/F) = \ell. \end{cases}$$
\[ h^0(G, C_E) = \begin{cases} tf, & \text{if } K \text{ contains the } t\text{-th roots of unity and } \delta(E/F) = 1; \\ t+1, & \text{otherwise.} \end{cases} \]

where

\[ \delta(E/F) = \gcd \ell \text{ and the degrees of ramified primes; } \]

\[ \delta(E/F) = \text{also, the minimal positive degree of an invariant divisor; } \]

\[ c = \text{the minimal positive degree of an invariant class}; \]

\[ t = \text{the number of ramified primes.} \]

**Proof:** Since \( G \) is cyclic, \( H^1(G, M) \cong H^1+2(G, M) \). Further, if the module is finite, by Herbrand's lemma, \( h^1(G, M) = h^{1+1}(G, M) \).

Thus,

(50) \[ h^1(G, C_{OE}) = h^0(G, C_{OE}) = [C_{OE}^G : \text{Norm}(C_{OE})] \]

\[ = [C_{OE}^G : C_{OF}^G][C_{OF}^G : \text{Norm}(C_{OE})], \]

\( C_{OF}^G \) denoting the image of \( C_{OF} \) under the canonical conorm map \( C_{OF} + C_{OE} \) induced by the inclusion \( F \subset E \). We have the ambiguous class number formula [14]

(51) \[ h_E \cdot [\bar{C} : \eta] = \frac{h_{\bar{C}} \cdot [\eta : \eta]}{a[\xi : 1]} \]

where,
We also know [12]

\[
[h_F : l] = \begin{cases}
\frac{h_F}{l}, & \text{if } E/F \text{ unramified and } K \\
\frac{h_F}{l}, & \text{otherwise.}
\end{cases}
\]

From (51) and (52), we can calculate \([C_{OE} : C_{OF}]\).

To evaluate the second factor on the right-hand side in (50), consider the canonical exact sequence of G-modules

\[1 + E + I_E + J_E + 1.\]

In cohomology, it gives the exact sequence

\[1 + E^G + I_E^G + J_E^G + H^1(G, E).\]

The group \(H^1(G, E)\) is trivial by Hilbert's Theorem 90. Therefore,
every invariant idèle class contains an invariant idèle. Also, it follows from the definition that

\[ I_E^G = I_F^G, \quad I_{OE}^G = I_{OF}^G. \]

Thus,

\[ J_E^G = J_F^G, \quad J_{OE}^G = J_{OF}^G. \]

Consider the canonical map

\[ J_{OE} \to C_{OE}. \]

Restricted to \( J_{OE}^G \), it gives the epimorphism

\[ J_{OE}^G = J_{OF}^G + C_{OF}. \]

Norms correspond to norms. Therefore,

\[ h^0(G, J_{OE}) = [J_{OE}^G : \text{norm}(J_{OE})] = [C_{OF}^G : \text{norm}(C_{OE})]. \]

By F. K. Schmidt's Theorem [17], an algebraic function field \( F/K \), for \( K \) finite, has a divisor of degree one and hence of every degree. Also considering the rational integers \( Z \) as \( G \)-modules under trivial action, we have the exact sequence of \( G \)-modules

\[ 1 \to J_{OE} \to J_E \xrightarrow{\text{degree}} Z \to 0, \]

which gives in cohomology, the exact sequence
(55) \[ H^{-1}(G, Z) \to H^0(G, J_{OE}) \to H^0(G, J_E) \xrightarrow{\rho} H^0(G, Z) \to H^{-1}(G, J_{OE}) \to H^{-1}(G, J_E). \]

From class field theory, \( H^{-1}(G, J_E) \) is trivial, and \( H^0(G, J_E) \) has order \( \ell \). Also,

\[ H^{-1}(G, Z) \cong H^1(G, Z) \cong \frac{\text{Crossed Homomorphisms}}{\text{Principal Crossed Homomorphisms}} \cong 1. \]

\[ H^0(G, Z) \cong \frac{\text{Invariant Elements}}{\text{Norms}} \cong \frac{Z}{\ell Z}. \]

Idèle classes of \( F \) have their degrees multiplied by \( \ell \) when considered as idèle classes of \( E \). Therefore, the map \( \rho \) in (55) induced by the degree map is the zero map. Hence,

(56) \[ h^0(G, J_{OE}) = h^0(G, J_E) = h^{-1}(G, J_{OE}) = \ell. \]

From (50), (51), (52), (53), and (56), we have

(57) \[ h^0(G, C_{OE}) = \begin{cases} \frac{\ell^2 h_E}{h_F}, & \text{if } E/F \text{ is unramified and } K \text{ contains the } \ell-\text{th roots of unity;} \\ \ell \frac{h_E}{h_F}, & \text{otherwise.} \end{cases} \]

\[ \mathcal{L}[C_{OE} : C_{OF}] = \frac{\ell h_E}{h_F}. \]

As mentioned above, the degree of a divisor of \( F \) gets multiplied by \( \ell \) when considered as a divisor of \( E \). Therefore, by F. K. Schmidt's Theorem, \( a = \ell \) in (51). From (51) and (57), we have
\[ h^0(G, \mathcal{O}_E) = \begin{cases} 
\overline{c}[\overline{n} : \eta], & \text{if } E/F \text{ unramified and } K \text{ contains the } \ell\text{-th roots of unity;} \\
\overline{c}^\ell + \overline{c}[\overline{n} : \eta], & \text{otherwise.}
\end{cases} \]

Now, we separate the ramified and the unramified cases.

**E/F Unramified.** Let \( \overline{E/F} \) be the extension obtained by making a constant extension of degree \( \ell \). Let \( \Gamma = \text{gal}(\overline{E}/E) = \text{gal}(\overline{F}/F) \).

As in [12], consider the exact sequences of \( \Gamma \)-modules, induced by the inclusion \( \overline{F} \subset \overline{E} \),

\[ 1 \rightarrow \overline{N} \rightarrow \mathcal{O}_{\overline{F}} \rightarrow \mathcal{O}_{\overline{E}} \rightarrow 1 \]

where \( \overline{N} = \text{kernel of the conorm map } \mathcal{O}_{\overline{F}} \rightarrow \mathcal{O}_{\overline{E}} \). In cohomology, it gives

\[ 1 \rightarrow \overline{N}^\Gamma \rightarrow \mathcal{O}_{\overline{F}}^\Gamma \rightarrow (\mathcal{O}_{\overline{F}}^\ell)^\Gamma \rightarrow H^1(\Gamma, \overline{N}) \rightarrow H^1(\Gamma, \mathcal{O}_{\overline{F}}^\ell). \]

If \( K \) contains the \( \ell \)-th roots of unity,

\[ \ell = |(\overline{N})^\Gamma| = |\overline{N}|, \quad \mathcal{O}_{\overline{F}}^\Gamma = \mathcal{O}_{\overline{F}}, \quad h^1(\Gamma, \mathcal{O}_{\overline{F}}^\ell) = 1, \quad h^1(\Gamma, \overline{N}) = \ell. \]

Therefore,

\[ h_F = [\ell : 1]. \]
If $K$ does not contain the $\ell$-th roots of unity, then $N = 1$, $h^1(\Gamma, \overline{N}) = 1$ and the last equation is still valid. Clearly,
\[(c_{\text{OF}}')^\Gamma \subset c^G_{\text{OF}}.\]

Therefore, \[(59) \quad h_F \mid \overline{h_E}.\]

For an unramified extension, every unit is a norm. If $K$ does not contain the $\ell$-th roots of unity, this is trivial because, then, every unit is norm of a unit. If $K$ contains the $\ell$-th roots of unity, this is a result of class field theory. Thus in each case,
\[(60) \quad \frac{[\overline{E} : \mathbb{Q}]}{[\mathbb{Q} : \mathbb{Q}]} = 1.\]

From (51), (59), and (60),
\[(61) \quad \overline{c} = \ell, \quad \overline{h_E} = h_F.\]

Substitution in (57) or (58) gives
\[(62) \quad h^0(G, C_{\text{OE}}) = h^1(G, C_{\text{OE}}) = \begin{cases} \ell^2, & \text{if } K \text{ contains the } \ell\text{-th roots of unity;} \\ \ell, & \text{otherwise.} \end{cases}\]

To calculate $h^0(G, C_{\text{E}})$ and $h^1(G, C_{\text{E}})$, consider the exact sequence of $G$-modules
In cohomology, (63) gives

\[ 1 \rightarrow c_{OE}^G + c_E^G \rightarrow Z \rightarrow H^1(G, c_{OE}) \rightarrow H^1(G, c_E) \rightarrow 1. \]  

By (61), the image under \( \mu \) is \( \ell Z \). Therefore, (62) and (64) imply, if \( K \) contains the \( \ell \)-th roots of unity,

\[ h^1(G, c_{OE}) = \ell^2 = \ell h^1(G, c_E). \]  

By Herbrand's Lemma,

\[ \frac{h^0(G, c_E)}{h^1(G, c_E)} = \frac{h^0(G, Z)}{h^1(G, Z)} \frac{h^0(G, c_{OE})}{h^1(G, c_{OE})} \frac{h^0(G, Z)}{h^1(G, Z)} = \ell. \]  

Therefore, (65) gives

\[ h^0(G, c_E) = \ell^2. \]  

Similarly,

\[ h^1(G, c_E) = 1, \quad h^0(G, c_E) = \ell, \]  

if \( K \) does not contain the \( \ell \)-th roots of unity.

Before we study the ramified case, we evaluate \( H^1(G, P_E) \), in general. To that end, consider the exact sequence

\[ 1 + K + E + P_E + 1, \]
obtaining, in cohomology,

\[ H^{-1}(G, E) = 1 \rightarrow H^{-1}(G, P_E) \rightarrow H^0(G, K) \xrightarrow{\lambda} H^0(G, E) \rightarrow \ldots \]

Therefore,

\[ h^{-1}(G, P_E) = \text{order of the kernel of } \lambda. \]

If \( K \) does not contain the \( \ell \)-th roots of unity, \( h^0(G, K) = 1 \). If \( K \) contains the \( \ell \)-th roots of unity, \( h^0(G, K) = \ell \). In this case, a generator of \( K \) is a norm form \( E \) iff it is everywhere locally a norm iff the degrees of the ramified primes are all divisible by \( \ell \). This follows from Hasse's Norm Theorem. Therefore,

\[
(68) \quad h^{-1}(G, P_E) = h^1(G, P_E) = \begin{cases} 
\ell, & \text{if } K \text{ contains the } \ell\text{-th roots of unity and the degrees of the ramified primes are all divisible by } \ell; \\
1, & \text{otherwise.}
\end{cases}
\]

\( E/F \) Ramified. We assert that

\[
(69) \quad \overline{c} = \sigma(E/F),
\]

if \( K \) does not contain the \( \ell \)-th roots of unity. For, consider the exact sequence
\[ 1 + P_E + D_E + C_E - 1, \]

and the induced cohomology sequence

\[(70) \quad 1 + P_E^G + D_E^G + C_E^G + H^1(G, P_E) + \ldots \]

(68) and (70) imply that every invariant class contains an invariant divisor. Therefore, \( \overline{c} = \delta(E/F) \). Substitution in (58) gives

\[
\delta(E/F) l^t, \text{ if } K \text{ does not contain the } \ell\text{-th roots of unity;}
\]

\[
l^{t-1}, \text{ if } K \text{ contains the } \ell\text{-th roots of unity and } \delta(E/F) = 1;
\]

\[
\overline{c} l^t, \text{ if } K \text{ contains the } \ell\text{-th roots of unity and } \delta(E/F) = \ell.
\]

The orders \( h^0(G, C_E) \) and \( h^1(G, C_E) \) are calculated, as in the unramified case, by considering the exact sequence (63). The values are

\[
(72) \quad h^0(G, C_E) = \ell h^1(G, C_E) = \begin{cases} 
\ell^t, & \text{if } K \text{ contains the } \ell\text{-th roots of unity and } \\
\delta(E/F) = 1; \\
\ell^{t+1}, & \text{otherwise.}
\end{cases}
\]
From (62), (65), (66), (71), and (72), we see that the proof of the theorem is complete.

We observe that it is only the last case in (71) which involves $c$. Rosen [16] asked the question if $c = 1$ can, at all, occur in this case. An affirmative answer is provided by the following:

**Proposition 2.** Let characteristic $K \neq 2$ and $P(X)$ be an irreducible monic polynomial of degree $4n + 2$ in $K[X]$.

Then, $E = K(X)(\sqrt{P(X)})$ contains an invariant class of degree one.

**Proof:** Consider the quadratic constant extension $\overline{E}$. The polynomial $P(X)$ decomposes as the product of two monic irreducible polynomials over the extended field of constants. The formula (51) for the ambiguous class number shows that the class number of $\overline{E}$ is odd. Since $\text{gal}(E/E)$ operates on $C_{OE}$ and $C_{OE}$ is the invariant subgroup, it follows that $h_E$ is also odd. Now, the ambiguous class number formula applied to $E$ shows that it has an invariant class of degree one.

**Remark.** It was proved [12] that $h_F$ divides $h_E$ if $E/F$ is a normal extension. Rosen [16] gave another proof. We observe that the normality is an unnecessary restriction. Using results from the theory of abelian varieties, we have shown that the quotient of the zeta functions is a polynomial with rational
integral coefficients. To give an arithmetic proof for \( h_F \mid h_E \)
one can assume that there is no field strictly between \( F \) and \( E \),
and that the canonical map \( C_F + C_E \) has a non-trivial kernel. This
implies that \( E/F \) is a pure extension of degree \( \ell \), a prime. The
proof [12] for the divisibility is valid in this case. If \( E/F \)
is non-normal, a proof can also be given by considering a Hilbert
class field \( H \) of \( F \), i.e. a maximal abelian unramified extension
of \( F \) which has \( K \) as its exact field of constants. Then
\( H \cap E = F \) and \( EH/E \) is abelian and unramified. Also, \( K \)
is the exact field of constants of \( HE \). Namely, if \( \overline{K} \neq K \) is
the exact field of constants, let \( \overline{H} = HK \) be the constant
extension. Then,

\[
\overline{H} \cap E = F
\]

and

\[
\]

This is a contradiction since \( EH = E\overline{H} \). By the Reciprocity
Law,

\[
\text{gal}(H/F) \cong C_F \cong \text{gal}(EH/E)
\]

and \( \text{gal}(EH/E) \) is a subgroup of \( C_E \).

In particular \( h_F \) divides \( h_E \).
§3. A THEOREM OF E. ARTIN

Let $K$ be a finite field and $K(X)$ be the field of rational functions in one indeterminate. Following Artin, we call a quadratic extension $E/K(X)$ imaginary if the infinite prime of $K(X)$ does not split in $E$. Let $R$ be the integral closure of $K[X]$ in $E$. Then, $R$ is a Dedekind domain with finite class group. There are only finitely many imaginary quadratic extensions $E/K(X)$ for which the class group of $R$ has exponent 2. We wish to obtain bounds on the genera of such fields. We shall assume that the genus $g_E = g > 1$ and, hence [13], $|K| = q \leq 5$. If $h_X$ is the class number of $R$, one has the relation [17]

\[ h_X = fh_E, \]

where $f = 1$ or 2 according as the infinite prime ramifies or is inert. In each case, $C^E_{OE}$ is a subgroup of $R$. Therefore, its exponent is also 2. (We leave out of consideration the 5 fields [11] for which $h_E = 1$.) Now, $C^E_{OE}$ has exponent 2 iff it is equal to its subgroup of ambiguous classes, i.e.

\[ h_E = f_E = \pi \cdot 2^{t-1} \cdot \frac{[\overline{E} : \overline{K}]}{[E : L]} = 2^d. \]

Let $m$ be any natural number not less than $2g - 1$. Then
by the Riemann-Roch Theorem, the dimension of a class of degree \( m \) is \( m - g + 1 \). The total number of integral divisors in all the classes of degree \( m \) is

\[
2^d(q^{m-g+1} - 1)(q - 1)^{-1}.
\]

Also, by the Riemann Hypothesis, the constant extension of degree \( m \) has, at least,

\[
q^{m/2}(q^{m/2} - 2g)
\]

primes of degree one. Considering that a prime of \( E \) of degree dividing \( m \) can give, at most, \( m \) primes of degree one in the constant extension, we see that \( E \) has, at least,

\[
m^{-1}q^{m/2}(q^{m/2} - 2g)
\]

integral divisors of degree \( m \). Therefore, the exponent of \( C_{OE} \) is larger than 2, if

\[
(q - 1)q^{m/2}(q^{m/2} - 2g) > m \cdot 2^d \cdot (q^{m-g+1} - 1).
\]

We consider the two cases when the characteristic is even and when it is odd.

**Case 1. Characteristic = 2**

In this case, (69) and (74) give
The genus formula gives

\begin{equation}
2g + 2 = D,
\end{equation}

\(D\) denoting the degree of the different. We observe that the ramification being wild, a ramified prime of degree \(s\) makes a contribution of, at least, \(2s\) to \(D\).

Consider the case when \(q = 2\) and no prime of degree one ramifies. For \(g = 9\), \((77)\) gives \(D = 20\). This implies \(t \leq 3\). Therefore, \((76)\) gives \(2^d \leq 2^3\). Substituting \(m = 2g - 1\), \(d = 3\) in \((75)\), we verify that the inequality is satisfied. We omit the formal argument showing that \((75)\) is satisfied for all \(g \geq 9\). It is not satisfied for \(g = 8\).

When \(q = 4\), \(g \geq 2\), and no prime of degree one ramifies, one sees, similarly, that \((75)\) is always satisfied.

If \(q = 4\) or \(2\) and a prime of degree one ramifies, Madden has shown that \(g \leq 2\), \(g \leq 8\) respectively. These bounds are better than those derived from \((75)\).

\textbf{Case 2. Characteristic Different from 2}

Consider the case when no prime of degree one ramifies. By \((73)\) and [1]
Therefore,

\[ h_X = 2h_E = \begin{cases} 
2^t & \text{if } \delta(E/K(X)) = 2, \\
2^{t-1} & \text{if } \delta(E/K(X)) = 1.
\end{cases} \]

In this case, the ramification is tame. A ramified prime of degree \( s \) makes a contribution of, at least, \( s \) to \( D \). Taking \( m = 2g - 1 \), one can show that (75) is satisfied for \( q = 3 \) and 5 if \( g \geq 5, \ g \geq 2 \), respectively. For example, if \( q = 3, \ g = 5 \) then \( D = 12 \). This implies \( t \leq 5 \). Therefore, from (78), \( d \leq \frac{1}{4} \), in each case. Substitution in (75) shows that it is satisfied.

If a prime of degree one ramifies, Madden's estimates are better. Combining our results with those of Madden, we have

**Theorem 9.** Let \( E/K(X) \) be an imaginary quadratic extension such that the integral closure of \( K[X] \) in \( E \) has class group of exponent 2. Then, the null class group of \( E \) has, also, exponent 2. The various possibilities are
\[ q = 7, 9, \quad g = 1; \]
\[ q = 4, 5, \quad g \leq 2; \]
\[ q = 3, \quad g \leq 4; \]
\[ q = 2, \quad g \leq 8. \]

If no prime of degree one ramifies, \( g = 2 \) is not possible for \( q = 4 \) and 5.


