1986

Dyadic Ramification in Quartic Algebraic Number Fields.

Stella Roberson Ashford

Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation
https://digitalcommons.lsu.edu/gradschool_disstheses/4279

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
INFORMATION TO USERS

While the most advanced technology has been used to photograph and reproduce this manuscript, the quality of the reproduction is heavily dependent upon the quality of the material submitted. For example:

- Manuscript pages may have indistinct print. In such cases, the best available copy has been filmed.

- Manuscripts may not always be complete. In such cases, a note will indicate that it is not possible to obtain missing pages.

- Copyrighted material may have been removed from the manuscript. In such cases, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, and charts) are photographed by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is also filmed as one exposure and is available, for an additional charge, as a standard 35mm slide or as a 17”x 23” black and white photographic print.

Most photographs reproduce acceptably on positive microfilm or microfiche but lack the clarity on xerographic copies made from the microfilm. For an additional charge, 35mm slides of 6”x 9” black and white photographic prints are available for any photographs or illustrations that cannot be reproduced satisfactorily by xerography.
Ashford, Stella Roberson

DYADIC RAMIFICATION IN QUARTIC ALGEBRAIC NUMBER FIELDS

The Louisiana State University and Agricultural and Mechanical Col. 

University Microfilms International 300 N. Zeeb Road, Ann Arbor, MI 48106
PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark.

1. Glossy photographs or pages ______
2. Colored illustrations, paper or print ______
3. Photographs with dark background ______
4. Illustrations are poor copy ______
5. Pages with black marks, not original copy ______
6. Print shows through as there is text on both sides of page ______
7. Indistinct, broken or small print on several pages ______
8. Print exceeds margin requirements ______
9. Tightly bound copy with print lost in spine ______
10. Computer printout pages with indistinct print ______
11. Page(s) _______ lacking when material received, and not available from school or author.
12. Page(s) _______ seem to be missing in numbering only as text follows.
13. Two pages numbered ______. Text follows.
14. Curling and wrinkled pages ______
15. Dissertation contains pages with print at a slant, filmed as received ______
16. Other ____________________________________________

University Microfilms International
DYADIC RAMIFICATION
IN
QUARTIC ALGEBRAIC NUMBER FIELDS

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in
Mathematics

by
Stella Roberson Ashford
B.S., Southern University, 1963
M.A., Louisiana State University, 1967
December 17, 1986
ACKNOWLEDGEMENTS

I am especially grateful to my Major Professor, Dr. Robert V. Perlis who worked with dedication and diligence. I thank him for his kindness, his patience and the confidence that he had in me. Without his direction and the questions that he asked, this dissertation would not be possible.

Chapter II depends on the results of [C-Y] relating invariants $\gamma_p$ to root numbers. I am grateful to Dr. P.E. Conner for explaining these concepts to me and for asking the questions that led to the results of Chapters II and III.

I thank Southern University for its support under the Faculty Development Program.

Finally, I am most grateful to my husband Marvin, and our children Marvin, Jr., Katrina and Marcus for their patience and understanding during the past few years and especially during the preparation of this dissertation; and also, I am extremely grateful to my parents Cleve M. and Lillie W. Roberson for their love and nurturing.
# TABLE OF CONTENTS

ACKNOWLEDGEMENTS .......................................................................................................... ii

LIST OF TABLES ................................................................................................................ iv

LIST OF FIGURES ................................................................................................................ v

ABSTRACT ............................................................................................................................ vi

INTRODUCTION .................................................................................................................. vii

CHAPTER I. DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx + d)$ ....................... 1

  I.1 Introduction .................................................................................................................. 1

  I.2 Newton's Polygon ........................................................................................................ 2

  I.3 The Newton Polygon for $x^4 + cx + d$ in $\mathbb{Z}[x]$ .............................................. 3

  I.4 The Discriminant of $x^4 + cx + d$ ......................................................................... 5

  I.5 Dyadic Ramification in $\mathbb{Q}[x]/(x^4 + cx + d)$ ..................................................... 6

CHAPTER II. DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx^2 + d)$ ..................... 12

  II.1 Introduction .............................................................................................................. 12

  II.2 Synopsis of Witt Theory ............................................................................................ 14

  II.2.1 Van der Blij's Invariant ..................................................................................... 14

  II.2.2 Local Root Numbers ............................................................................................ 15

  II.2.3 The Additive Character $\gamma_p$ .......................................................................... 17

  II.3 Six Lemmas ............................................................................................................... 18

  II.4 Dyadic Ramification in $\mathbb{Q}[x]/(x^4 + cx^2 + d)$ .................................................. 25

CHAPTER III. AN APPLICATION OF THEOREM 2 TO FUNDAMENTAL UNITS OF NORM 1 ................................................................. 31

  III.1 Introduction ............................................................................................................. 31

  III.2 The Quartic Field $\mathbb{Q}(\sqrt{\epsilon})$ .................................................................. 34

  III.3 Standard Facts About the Norm of $\epsilon$ ............................................................ 35

  III.4 Dyadic Ramification in $E = F(\sqrt{\epsilon})/\mathbb{Q}$ ................................................... 37

CHAPTER IV. WEIL RECIPROCITY AND FUNDAMENTAL UNITS OF NORM -1 ...... 41

BIBLIOGRAPHY .................................................................................................................. 46

VITA .................................................................................................................................... 47
LIST OF TABLES

II.2.2 LOCAL ROOT NUMBERS ........................................ 15
  Table 1 ......................................................... 17

II.2.3 THE ADDITIVE CHARACTER γ_p ................................ 17
  Table 2 ......................................................... 18
LIST OF FIGURES

I.3 THE NEWTON'S POLYGON FOR $x^4 + cx + d$ IN $\mathbb{Z}[x]$ ............. 3

Figure 1 ................................................ 4

Figure 2 ................................................ 4

I.5 DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx + d)$ ..................... 6

Figure 3 ................................................ 8
ABSTRACT

This dissertation is concerned with dyadic ramification in quartic number fields \( E \). If \( f(x) \) is a defining polynomial for \( E \), then

\[
E = \mathbb{Q}[x]/(f(x)).
\]

The problem is to decide whether or not 2 ramifies in \( E \), in terms of the coefficients of \( f(x) \). In this dissertation, this problem is studied when \( f(x) \) is an irreducible quartic trinomial. That is, \( f \) has one of the two forms

1. \( f(x) = x^4 + cx + d \)
2. \( f(x) = x^4 + cx^2 + d \quad c,d \text{ in } \mathbb{Z} \)

(any irreducible trinomial can be reduced to one of these two forms).

When \( f(x) \) has the first form

\[
f(x) = x^4 + cx + d
\]

I have shown that 2 is always ramified in \( E \) except possibly when the polynomial discriminant \( D_f = 5 \cdot t^2 \) in the 2-adic integers \( \mathbb{Z}_2 \).

When \( f(x) \) has the form

\[
f(x) = x^4 + cx^2 + d
\]

I use Weil's additive characters \( \gamma_p \) of the rational Witt ring \( W(\mathbb{Q}) \) to devise a test of whether or not 2 ramifies in \( E \). The result appears as Theorem 2. Applications of Theorem 2 to fundamental units in real quadratic fields are discussed.
INTRODUCTION

One problem in the arithmetic of an algebraic number field $K$ is that of how a prime $p$ in the field $\mathbb{Q}$ of rational numbers decomposes in the extension field $K$. The prime $p$ in $\mathbb{Q}$ need not remain prime in $K$. It may decompose in $K$ as a product of powers of distinct prime ideals

$$(p) = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r} \quad \text{with} \quad e_i > 1 \text{ for some } i$$

($p$ ramifies) or $p$ may be the product of powers of distinct prime ideals

$$(p) = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r} \quad \text{with} \quad e_i = 1 \text{ for all } i.$$

It is known that the rational prime $p$ ramifies in the extension field if and only if $p$ divides the discriminant $\text{Dis}(K/\mathbb{Q})$ of the extension. This rule is simple indeed. But in order to compute $\text{Dis}(K/\mathbb{Q})$ one usually needs to know the integers in $K$, and the computation of the ring of integers in an arbitrary number field can be complicated. What is needed then is an efficient device that will decide whether or not a rational prime $p$ ramifies in the extension field.

A number field $K$ is of the form

$$K = \mathbb{Q}(\theta)$$

for some algebraic integer $\theta$ in $K$. If $f(x)$ in $\mathbb{Z}[x]$ is the minimal polynomial of $\theta$ then $K$ may be expressed as

$$K = \mathbb{Q}[x]/(f(x)).$$
There is a fairly efficient procedure for computing the polynomial dis-
criminant $D_f$ of $f(x)$ in terms of its coefficients. In general the
polynomial discriminant is related to the discriminant $\text{Dis}(K/Q)$ of the
extension by

$$D_f = \text{Dis}(K/Q) \cdot x^2$$

for some $x > 1$ in $\mathbb{Z}$, the ring of rational integers. So if a rational
prime $p$ divides $D_f$ to an odd power, then $p$ divides $\text{Dis}(K/Q)$ and
$p$ ramifies in $K$. But in general because of the potential non-trivial
square factor $x^2$ in $D_f$ it is possible for a rational prime $p$ to
divide $D_f$ and not divide $\text{Dis}(K/Q)$. The worst case occurs when $D_f$ is
itself a square.

When $K$ is a quadratic field there is a simple well-known algo-
rithm to actually compute $\text{Dis}(K/Q)$ in terms of the coefficients of a
defining polynomial. This solves the problem of ramification for qua-
dratic number fields.

For a cubic number field $K$, choose a defining polynomial $f$, so
$K = \mathbb{Q}[x]/(f(x))$, and write the polynomial discriminant $D_f$ as

$$D_f = (\text{square}) \cdot t \quad \text{in} \quad \mathbb{Q}_2$$

for some 2-adic integer $t$. It is easily seen that:

The rational prime 2 is at most tamely ramified in $K$ if and
only if $t \equiv 1 \pmod{4}$.

So for cubic fields, knowledge of the polynomial discriminant $D_f$ alone
gives some significant information about dyadic ramification. While one
can reasonably ask what invariants are needed in addition to the
discriminant $D_f$ in order to guarantee that $2$ is unramified, we will
accept for now that $D_f$ alone basically controls ramification in cubic
fields, and turn our attention to fourth-degree fields where $D_f$ alone
can no longer be expected to give much information.

In this dissertation we will study the ramification of the prime $2$
in degree four number fields, i.e. in quartic number fields. We do not
consider all quartic number fields but only those that are defined by
(irreducible) quartic trinomials. For these fields we will provide
reasonable criteria for the dyadic prime $2$ to ramify in terms of the
coefficients of a minimal polynomial.

If $E$ is a quartic algebraic number field defined by an irreduc-
ible monic trinomial with integral coefficients, then $E$ may be written
as $E = \mathbb{Q}[x]/(f(x))$ where $f(x)$ is a trinomial having one of the
following three forms:

1. $f_1(x) = x^4 + cx + d$
2. $f_2(x) = x^4 + cx^2 + d$
3. $f_3(x) = x^4 + cx^3 + d$

The field $E$ generated by a root $\theta$ of $f_3(x)$ is also generated
by a quartic trinomial of the form $f_1(x)$ since $K = \mathbb{Q}[\theta] = \mathbb{Q}[\frac{1}{\theta}]$ and
$\frac{1}{\theta}$ satisfies a polynomial of the form $f_1(x)$ if $\theta$ satisfies a poly-
nomial of the form $f_3(x)$. Therefore just two types of fields will be
investigated.
Chapter I studies quartic algebraic number fields defined by the family of irreducible trinomials $x^4 + cx + d$ in $\mathbb{Z}[x]$, and chapter II studies the quartic algebraic number fields defined by the family of irreducible trinomials $x^4 + cx^2 + d$ in $\mathbb{Z}[x]$.

Here is a summary of chapter I. Let $D_f$ be the discriminant of the irreducible quartic

$$f(x) = x^4 + cx + d$$

with $c, d$ in $\mathbb{Z}$. Over the 2-adic field $\mathbb{Q}_2$ write

$$D_f = 2^s \cdot u \cdot t^2$$

with $s = 0$ or 1, $t$ a 2-adic integer and $u = 1, 3, 5$ or 7. As above $E = \mathbb{Q}[x]/(f(x))$.

**Theorem 1.** (a) If $s = 1$ then 2 ramifies in $E$.

(b) If $s = 0$ and $u = 1, 3$ or 7 then 2 ramifies in $E$.

So 2 ramifies in every case except possibly where $D_f = 5 \cdot x^2$ in $\mathbb{Z}_2$. We have been unable to settle this exceptional case.

In chapter II we consider the extension field

$$E = \mathbb{Q}[x]/(x^4 + cx^2 + d).$$

Associated with the irreducible quartic $x^4 + cx^2 + d$ is the irreducible quadratic $T^2 + cT + d$.

Let $\sigma$ be a root of $T^2 + cT + d$. Then $\sqrt{\sigma}$ is a root of $x^4 + cx^2 + d$, so we have a tower of quadratic extensions
\[
E = \mathbb{Q}(\sqrt{\sigma}) \\
F = \mathbb{Q}(\sigma) \\
Q \\
\]

We can write the quadratic field \( F = \mathbb{Q}(\sigma) \) in standard form \( \mathbb{Q}(\sqrt{m}) \) by letting

\[
m = \text{square-free part of } c^2 - 4d.
\]

Now 2 is unramified in \( E \) if and only if 2 is unramified in \( F \) and each dyadic prime of \( F \) is unramified in \( E \). Thus, if 2 is unramified in \( E \) then certainly

\[
m \equiv 1 \pmod{4}
\]

and also for every dyadic prime \( P \) of \( F \) we have \( \text{ord}_P(\sigma) \equiv 0 \pmod{2} \).

But there is an additional condition coming from Witt theory. Namely, the field \( E \) becomes an innerproduct space over \( \mathbb{Q} \) with respect to the trace form

\[
b(v, w) = \text{trace}_{E/\mathbb{Q}}(vw)
\]

for \( v, w \) in \( E \). The resulting Witt class of \( (E, b) \) in the Witt ring \( W(\mathbb{Q}) \) is denoted by \( \langle E \rangle \).

There is an additive homomorphism

\[
\gamma_2 : W(\mathbb{Q}) \longrightarrow \mathbb{C}^*
\]

defined in ([M-H] p. 131), whose values are complex eighth roots of unity contained in the group \( \mathbb{C}^* \) of complex numbers. Recently Conner and Yui ([C-Y], (5.3) p. 31) have shown that \( \gamma_2 \langle E \rangle \) can be computed by
\[ \gamma_2 \langle E \rangle = (-2,d)_2 c_2 \langle E \rangle r_2(d) \]

where \((-2,d)_2\) in \(\mathbb{Z}^*\) is the dyadic Hilbert symbol, \(c_2 \langle E \rangle\) in \(\mathbb{Z}^*\) is the stable dyadic Hasse-Witt symbol of \(\langle E \rangle\) and \(r_2(d)\), a fourth root of unity, is the dyadic local root number associated with the constant \(d\) appearing in \(x^4 + cx^2 + d\) (see Section II.2). Despite appearances, the computation of \(\gamma_2 \langle E \rangle\) can be read off easily enough from the original coefficients \(c\) and \(d\). The main theorem of Chapter II is

**THEOREM 2.** Let \(x^4 + cx^2 + d\) be an irreducible trinomial with root \(\sqrt{d}\) and let \(m\) be the square-free part of \(c^2 - 4d\). Then the prime 2 is unramified in \(E = \mathbb{Q}(\sqrt{d})\) if and only if

1. \(m \equiv 1 \pmod{4}\).
2. \(\text{ord}_p(o) \equiv 0 \pmod{2}\) for every dyadic prime ideal \(P\) of \(F = \mathbb{Q}(o)\).
3. \(\gamma_2 \langle E \rangle = -1\).

Chapters III and IV contain two applications of the theorem established in chapter II. Starting with a positive square-free integer

\[ m \equiv 1 \pmod{4} \]

we form the real quadratic field \(\mathbb{Q}(\sqrt{m})\). This has a fundamental unit \(\epsilon\), which has norm

\[ N(\epsilon) = 1 \text{ or } -1 \]

in \(\mathbb{Z}\). Let us suppose \(N(\epsilon) = 1\). Replacing \(\epsilon\) by \(-\epsilon\) if necessary, we may take \(\epsilon\) to be totally positive. Put
\[ E = F(\sqrt{e}). \]

Writing
\[ e = k_1 + k_2 \left( \frac{1 + \sqrt{e}}{2} \right) \]
shows that \( \sqrt{e} \) satisfies the irreducible trinomial
\[ x^4 - (2k_1 + k_2)x^2 + 1 \]
in \( \mathbb{Z}[x] \), so \( E/Q \) is an extension of the form discussed in chapter II, with \( c = -(2k_1 + k_2) \) and \( d = 1 \).

Now we chose \( m \equiv 1 \pmod{4} \) and we automatically have \( \text{ord}_p(e) \equiv 0 \pmod{2} \) for every dyadic prime \( P \) of \( F \), so Theorem 2 reduces to the statement

2 is unramified in \( E \) if and only if \( \gamma_2^{E^2} = -1 \).

This condition is analyzed in Chapter III, where it is shown that 2 ramifies in exactly one of

\[ E = \mathbb{Q}(\sqrt{e}) \quad E_c = \mathbb{Q}(\sqrt{-e}). \]

In the special case that every prime divisor \( p \) of \( m \) is congruent to 1 modulo 4, we show that the dyadic primes of \( F \) are ramified in \( E \). Since \( e \) is a totally positive unit, no other primes of \( F \), including the infinite prime, can ramify in \( E \). So \( E/F \) is a quadratic unramified extension, showing us how to construct a quadratic piece of the Hilbert class field of \( K \). Various numerical examples are discussed.

Finally chapter IV discusses the case when the fundamental unit has norm \(-1\).
CHAPTER I: DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx + d)$

1.1. INTRODUCTION

Let $f(x) = x^4 + cx + d$ be an irreducible polynomial with coefficients in $\mathbb{Z}$. Then $f(x)$ has discriminant

$$D_f = 4^4d^3 - 3^3c^4$$

(see Section 1.4).

Put $E = \mathbb{Q}[x]/(f(x))$. Then

$$D_f = \text{Dis}(E/Q) \cdot t^2$$

for some $t$ in $\mathbb{Z}$. We are concerned with the question when does 2 ramify in $E$?

If $\text{ord}_2(D_f)$ is odd, then also $\text{ord}_2(\text{Dis}(E/Q))$ is odd, so 2 ramifies. However if $\text{ord}_2(D_f)$ is even then also $\text{ord}_2(\text{Dis}(E/Q))$ is even, which allows the possibility that 2 does not divide $\text{Dis}(E/Q)$.

Saying that $\text{ord}_2(D_f)$ is even means that

$$D_f = u \cdot \text{(square)}$$

in the ring $\mathbb{Z}_2$ of 2-adic integers, where $u$ is one of the 2-adic units 1, 3, 5 and 7. We treat the case $u = 1, 3$ and 7 in this dissertation.

In [C-P], Conner and Perlis studied the case $u = 1$ and showed that in that case 2 always ramifies in $E$. Their arguments made sophisticated use of the trace form of $E/Q$. In this chapter we replace their arguments by simpler ones using only the classical notion of
Newton's polygon. We also treat the easier cases \( u = 3 \) and 7. The main result of this chapter is the following theorem, proved in Section 1.5:

**Theorem 1.** Let \( f(x) = x^4 + cx + d \) be an irreducible polynomial in \( \mathbb{Z}[x] \). Write

\[
D_f = 2^s \cdot u \cdot t^2
\]

in \( \mathbb{Z}_2 \), with \( s = 0,1 \) and \( u = 1,3,5, \) or 7. Let \( E = \mathbb{Q}[x]/(f(x)) \).

a) If \( s = 1 \), then 2 ramifies in \( E \).

b) If \( s = 0 \) and \( u = 1,3, \) or 7, then 2 ramifies in \( E \).

We have been unable to settle the case \( s = 0 \) and \( u = 5 \).

### 1.2. NEWTON'S POLYGON

Consider the polynomial

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0
\]

in \( \mathbb{Q}_2[x] \) and assume \( a_n a_0 \neq 0 \). Associate a polygon with \( f(x) \) by assigning a point to each term of \( f(x) \) by the following rules:

i. If \( a_i x^i \neq 0 \), the term \( a_i x^i \) of \( f(x) \) is assigned to the point \( (i, \text{ord}_2(a_i)) \).

ii. If \( a_i x^i = 0 \), the (missing) term \( a_i x^i \) of \( f(x) \) is assigned to the (missing) point \( (i, \infty) = (i, \text{ord}_2(0)) \).

The lower convex envelope of the points so obtained is called the Newton polygon of \( f(x) \).

We note:

(P-1) The condition \( a_n a_0 \neq 0 \) means that the Newton polygon starts from a finite point on the Y-axis and ends in a finite point.
As we go from left to right in a Newton polygon the slopes of the segments of the Newton polygon increase.

Newton's polygon gives information about the 2-order of the roots \( \theta \) of \( f(x) \). The following proposition is from Weiss (see [W], p. 74).

(1.2.1) **PROPOSITION.** Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \) \( a_n a_0 \neq 0 \) be a polynomial over \( \mathbb{Q}_2 \). Suppose that \( (r, \text{ord}_2(a_r)) \) and \( (s, \text{ord}_2(a_s)) \) are endpoints of a segment in the Newton polygon of \( f(x) \), with \( s > r \) and with slope \(-w\). Then \( f(x) \) has exactly \( s - r \) roots \( \theta \) with \( \text{ord}_2(\theta) = w \).

(1.2.2) **COROLLARY.** Let \( \theta \) be a root of an irreducible polynomial \( f(x) \) in \( \mathbb{Q}_2[x] \). If the Newton polygon of \( f(x) \) has a segment of slope \( \frac{m}{2^a} \) in lowest terms, with \( a > 1 \), then the extension \( \mathbb{Q}_2(\theta)/\mathbb{Q}_2 \) is ramified.

**PROOF:** Let \( N|\mathbb{Q}_2 \) be the normal closure of \( \mathbb{Q}_2(\theta) \). By Proposition, (1.2.1) \( f(x) \) has a root \( \alpha \) in \( N \) with \( \text{ord}_2(\alpha) = \frac{m}{2^a} \). To account for the denominator, \( N/\mathbb{Q}_2 \) must be ramified. So \( \mathbb{Q}_2(\theta)/\mathbb{Q}_2 \) is ramified.

**1.3. THE NEWTON POLYGON FOR** \( x^4 + cx + d \) **IN** \( \mathbb{Z}[x] \).

We associate a polygon to the irreducible trinomial \( x^4 + cx + d \) in \( \mathbb{Z}[x] \subseteq \mathbb{Q}_2[x] \) by the correspondence

\[

d |\rightarrow (0, \text{ord}_2(d)) \text{ with } \text{ord}_2(d) > 0.
\]

\[

cx |\rightarrow (1, \text{ord}_2(c)) \text{ with } \text{ord}_2(c) > 0.
\]

\[

1 \cdot x^4 |\rightarrow (4, \text{ord}_2(1)) = (4,0).
\]

The missing terms are assigned to \( (0, \infty) \).
The Newton polygon for \( x^4 + cx + d \) starts at \((0, \text{ord}_2(d))\) and ends at \((4,0)\). If \( \text{ord}_2(d) = 0 \), then the Newton polygon for \( x^4 + cx + d \) is the horizontal segment from \((0,0)\) to \((4,0)\). Suppose \( \text{ord}_2(d) > 0 \).

The line connecting \((0,\text{ord}_2(d))\) to \((4,0)\) has equation

\[
g(x) = -\frac{\text{ord}_2(d)}{4} x + \text{ord}_2(d).
\]

If \( \text{ord}_2(c) > g(1) = \frac{3}{4} \text{ord}_2(d) \), the Newton polygon for \( x^4 + cx + d \) in \( \mathbb{Z}[x] \) consists of one segment as in (Fig. 1). Otherwise the Newton polygon consists of two distinct segments as in (Fig. 2). Note if \( \text{ord}_2(c) = 0 \), one of the segments has endpoints \((1,0)\) and \((4,0)\).
I.4. THE DISCRIMINANT OF $x^4 + cx + d$

(I.4.1) LEMMA. Let $f(x) = x^4 + cx + d$ in $\mathbb{Q}[x]$ be irreducible. Then the discriminant of $f(x)$ is

$$D_f = 4^4d^3 - 3^3c^4.$$  

**PROOF:** $f(x) = x^4 + cx + d$ and $f'(x) = 4x^3 + c$. Let $\theta$ be a root of $f(x)$. Put $K = \mathbb{Q}(\theta)$. Then

$$D_f = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}} f'(\theta)$$  

where $n = [K : \mathbb{Q}] = 4$.

Thus $D_f = N_{K/\mathbb{Q}}(f'(\theta)) = N_{K/\mathbb{Q}}(4\theta^3 + c)$. If $c = 0$ we find $D_f = 4^4d^3$ since $N_{K/\mathbb{Q}}(\theta) = d$. If $c \neq 0$ then

$$\theta \cdot f'(\theta) = 4\theta^4 + c\theta = -4c\theta - 4d + c\theta = -3c\theta - 4d$$

so $\theta \cdot f'(\theta) = -3c(\theta + \frac{4d}{3c})$. Taking norms, we see

$$N_{K/\mathbb{Q}}(\theta \cdot f'(\theta)) = dN_{K/\mathbb{Q}}(f'(\theta)) = (-3c)^4 N_{K/\mathbb{Q}}(\theta + \frac{4d}{3c}).$$

Now the norm of $\theta$ is $f(0)$ and the norm of $(\theta + \frac{4d}{3c})$ is $g(0)$ where

$$g(x) = f(x - \frac{4d}{3c}) = (x - \frac{4d}{3c})^4 + c(x - \frac{4d}{3c}) + d.$$  

So

$$g(0) = ((\frac{4d}{3c})^4 - \frac{d}{3}) = N_{K/\mathbb{Q}}(\theta + \frac{4d}{3c})$$

Thus

$$dN_{K/\mathbb{Q}}(f'(\theta)) = (-3c)^4((\frac{4d}{3c})^4 - \frac{d}{3})$$

so

$$N_{K/\mathbb{Q}}(f'(\theta)) = \frac{1}{d} (3c)^4((\frac{4d}{3c})^4 - \frac{d}{3}).$$

Therefore

$$D_f = 4^4d^3 - 3^3c^4.$$
I.5. DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx + d)$.

Now we are ready to prove

THEOREM 1. Let $f(x) = x^4 + cx + d$ be an irreducible polynomial in $\mathbb{Z}[x]$. Write

$$D_f = 2^s \cdot u \cdot t^2$$

in $\mathbb{Z}_2$ with $s = 0$ or 1 and $u = 1, 3, 5$ or 7. Let $E = \mathbb{Q}[x]/(f(x))$.

(a) If $s = 1$, then 2 ramifies in $E$.

(b) If $s = 0$ and $u = 1, 3, 5$ or 7, then 2 ramifies in $E$.

PROOF: We have

$$D_f = \text{Dis}(E/\mathbb{Q}) \cdot w^2$$

for some $w$ in $\mathbb{Z}$. If $s = 1$, then $\text{ord}_2(D_f)$ is odd. Thus $\text{ord}_2(\text{Dis}(E/\mathbb{Q}))$ is odd, so 2 divides $\text{Dis}(E/\mathbb{Q})$ at least once. So 2 ramifies in $E$. This proves (a).

Now suppose $s = 0$. Then $D_f = u \cdot t^2$ in $\mathbb{Z}_2$. Let $N$ be the normal closure of $E/\mathbb{Q}$, $q$ a dyadic prime ideal of $N$, and $N_q$ be the completion of $N$ at $q$. We will first show $N_q$ contains $\mathbb{Q}_2(\sqrt{u})$.

Let $\theta$ be a primitive element for $E/\mathbb{Q}$. $N$ contains the conjugates $\{\theta_i\}$ of $\theta$ and therefore $N$ contains $\prod_{i<j} (\theta_i - \theta_j) = \sqrt{D_f}$. Since $N \subseteq N_q$ it follows that $N_q$ contains $\sqrt{D_f} = \sqrt{u} \cdot t^2 = t\sqrt{u}$, so $N_q$ contains $\sqrt{u}$. So $\mathbb{Q}_2(\sqrt{u}) \subset N_q$. But 2 is ramified in $\mathbb{Q}_2(\sqrt{u})$ for $u = 3$ or 7. So 2 is ramified in $N_q$ and hence in $N$ and therefore in $E/\mathbb{Q}$ for $u = 3$ or 7. Now suppose $s = 0$ and $u = 1$. Then $D_f$ is a square in $\mathbb{Z}_2$. The following lemmas will tell us about the Newton polygon of $f(x)$. 
LEMMA. Let \( f(x) = x^4 + cx + d \) be an irreducible trinomial over \( \mathbb{Z} \). If \( D_f \) is a square in \( \mathbb{Z}_2 \), then

\[
\text{ord}_2(\frac{2^5 d^3}{c^4}) < 0.
\]

Moreover

\[
\text{ord}_2(c) > \max\left\{\frac{3}{4} \cdot \text{ord}_2(d) + \frac{5}{4}, \ 2\right\}
\]

PROOF: By (1.4.1), \( D_f = 4^4d^3 - 3^3c^4 \). Suppose

\[
\text{ord}_2(\frac{2^5 d^3}{c^4}) > 0.
\]

Then

\[
\left(\frac{2^5 d^3}{c^4}\right)
\]

is in \( \mathbb{Z}_2 \). Now \( D_f = 2^8d^3 - 3^3c^4 \). So

\[
\frac{D_f}{c^4} = 2^3\left(\frac{2^5 d^3}{c^4}\right) - 3^3
\]

is in \( \mathbb{Z}_2 \) and therefore is a square in \( \mathbb{Z}_2 \), since \( D_f \) is a square in \( \mathbb{Z}_2 \).

But

\[
\frac{D_f}{c^4} = 8\left(\frac{2^5 d^3}{c^4}\right) - 3^3 \equiv -3 \equiv 5 \pmod{8}
\]

and hence is not a square in \( \mathbb{Z}_2 \), a contradiction. Therefore

\[
\text{ord}_2(\frac{2^5 d^3}{c^4}) < 0.
\]

Hence

\[
\text{ord}_2(c^4) > \text{ord}_2(d^3) + \text{ord}_2(2^5)
\]

Equivalently
\[
\text{ord}_2(c) > \frac{3 \cdot \text{ord}_2(d)}{4} + \frac{5}{4} > 1 + \frac{1}{4}.
\]

Since \( \text{ord}_2(c) > \frac{1}{4} \) and since \( \text{ord}_2(c) \) is a whole number we have \( \text{ord}_2(c) > 2 \). Also, \( \text{ord}_2(c) > \frac{3}{4} \cdot \text{ord}_2(d) \). \( \square \)

(1.5.3) **COROLLARY.** If \( f(x) = x^4 + cx + d \) in \( \mathbb{Z}_2[x] \) is irreducible and has square discriminant in \( \mathbb{Z}_2 \) then the Newton polygon consists of one segment with slope \( -\frac{\text{ord}_2(d)}{4} \).

**PROOF:**

The line passing through the points \((0, \text{ord}_2(d))\) and \((4,0)\) has equation \( y = -\frac{\text{ord}_2(d)}{4} x + \text{ord}_2(d) \). The point \((1, \text{ord}_2(c))\) definitely lies above this line since the point \((1, \frac{3}{4} \text{ord}_2(d))\) is on the line and \( \text{ord}_2(c) > \frac{3}{4} \text{ord}_2(d) \) by (1.5.2). Therefore, by (1.3), the Newton polygon for \( f(x) \) consists of one segment with slope \( -\frac{\text{ord}_2(d)}{4} \). \( \square \)

Each root of \( f(x) \) has value \( \frac{\text{ord}_2(d)}{4} \) by (1.2.1).

Fix a root \( \theta \) of \( f(x) \). We will consider the following 2 cases:

Case I: 4 does not divide \( \text{ord}_2(d) \).

Case II: 4 divides \( \text{ord}_2(d) \).
We will show that \( f(x) \) has a root \( \alpha \) with \( \text{ord}_2(\alpha) = \frac{n_1}{2^s} \) in lowest terms, where \( s \) and \( n_1 \) are natural numbers.

Case I: 4 does not divide \( \text{ord}_2(d) \).

If 4 does not divide \( \text{ord}_2(d) \), then there exists an odd natural number \( n_1 \) such that either

\[
\text{ord}_2(d) = \frac{n_1}{4} = \frac{1}{4}
\]

or

\[
\text{ord}_2(d) = \frac{2n_1}{4} = \frac{n_1}{2}.
\]

By (1.2.2) \( Q_2(\Theta) = E \) is ramified.

Case II: 4 divides \( \text{ord}_2(d) \).

If 4 divides \( \text{ord}_2(d) \), then \( \text{ord}_2(d) = i \) for some \( i > 0 \) in \( \mathbb{Z} \).

So \( \text{ord}_2(d) = \frac{i}{4} = i \) implies \( \text{ord}_2(d) = 4i \).

OBSERVATIONS:

1. Since \( \text{ord}_2(\Theta) = i \), \( \Theta = 2^i u_0 \) for some appropriate unit \( u_0 \) in \( \mathbb{Z}_2 \). Furthermore \( \Theta^4 = 2^{4i} u_0^4 \).
2. From (1) \( Q_2(\Theta) = Q_2(u_0) \).
3. Since \( \text{ord}_2(d) = 4i \), we have \( d = 2^{4i} d_1 \) for some unit \( d_1 \) in \( \mathbb{Z}_2 \).
4. We have from (1.5.2) that \( \text{ord}_2(c) > \frac{3}{4} \text{ord}_2(d) + \frac{5}{4} > 3i + \frac{5}{4} \).

Since \( \text{ord}_2(c) \) is a whole number we see \( \text{ord}_2(c) > 3i + 2 \). Thus there exists \( c_1 \) in \( \mathbb{Z}_2 \) with \( \text{ord}_2(c_1) > 2 \) such that \( c = 2^{3i} c_1 \).
Applying (1) and (4) to \( c_0 \), we get
\[
c_0 = (2^3d_1)(2^4u_0) = 2^{41}c_1u_0.
\]

Now \( \theta \) is a root of \( f(x) \). Thus
\[
f(\theta) = \theta^4 + c_0 + d = 2^{41}u_0^4 + 2^{41}c_1u_0 + 2^{41}d_1 = 0.
\]
Hence
\[
u_0^4 + c_1u_0 + d_1 = 0.
\]
So \( u_0 \) satisfies the irreducible equation
\[
m(x) = x^4 + c_1x + d_1 = 0
\]
over \( \mathbb{Z}_2 \).

The discriminant \( D_m = 4^4d_1^3 - 3^3c_1^4 \) of \( m(x) \) is a square in \( \mathbb{Z}_2 \). This is true since \( E = \mathbb{Q}_2(\theta) = \mathbb{Q}_2(u_0) \) so
\[
D_m = \text{Disc}(E/\mathbb{Q}_2) = 1 \text{ in } \mathbb{Q}_2^*/\mathbb{Q}_2^{***}.
\]
So \( D_m \in \mathbb{Z}_2 \) is a square in \( \mathbb{Q}_2 \) and therefore is a square in \( \mathbb{Z}_2 \).

Lemma (1.5.2) applied to \( m(x) \) yields \( \text{ord}_2(c_1) > 2 \).

Now let \( g(x) = m(x + 1) = (x + 1)^4 + c_1(x + 1) + d_1 \). Then
\[
g(x) = x^4 + 4x^3 + 6x^2 + (4 + c_1)x + (1 + c_1 + d_1).
\]
Furthermore

(1) Since \( \text{ord}_2(4) = 2 \) and \( \text{ord}_2(c_1) > 2 \) we must have
\[
\text{ord}_2(4 + c_1) > 2.
\]

(2) Also \( 1 + d_1 \equiv 0 \pmod{2} \) and \( c_1 \equiv 0 \pmod{2} \). Therefore
\[
\text{ord}_2(1 + c_1 + d_1) > 1.
\]
The Newton polygon for
\[
g(x) = x^4 + 4x^3 + 6x^2 + (4 + c_1)x + (1 + c_1 + d_1)
\]
is determined from the points
\[
(0, \text{ord}_2(1 + c_1 + d_1)), (1, \text{ord}_2(4 + c_1)), (2,1), (3,2) \text{ and } (4,0).
\]
We will show that the Newton polygon of \( g(x) \) contains a segment with slope \( w = -\frac{1}{2} \) or \( w = -\frac{1}{4} \).

Consider the following segments:

a) From \((4,0)\) to \((3,2)\) with slope \( w = -2 \).

b) From \((4,0)\) to \((2,1)\) with slope \( w = -\frac{1}{2} \).

c) From \((4,0)\) to \((1, \text{ord}_2(4 + a_1))\) with slope \( w = -\frac{\text{ord}_2(4 + c_1)}{3} \). 

d) From \((4,0)\) to \((0, \text{ord}_2(1 + c_1 + d_1))\) with slope \( w = -\frac{\text{ord}_2(1 + c_1 + d_1)}{4} \).

The right endpoint is a vertex in the Newton polygon for \( g(x) \). Starting with \((4,0)\) and going left, the slopes of the segments of the Newton polygon decrease. So the first segment (counting from the right) has largest slope. This means that the Newton polygon for \( g(x) \) contains a segment with slope either

\[ w = -\frac{1}{2} \] or \[ w = -\frac{\text{ord}_2(1 + c_1 + d_1)}{4} \].

If \( \text{ord}_2(1 + c_1 + d_1) = 1 \), then the Newton polygon contains a segment with slope \( w = -\frac{1}{4} \).

If \( \text{ord}_2(1 + c_1 + d_1) > 2 \) then \( -\frac{\text{ord}_2(1 + c_1 + d_1)}{4} < -\frac{2}{4} \). In that case the Newton polygon contains a segment with slope \( w = -\frac{1}{2} \).

We have shown that the Newton polygon for \( g(x) \) contains a segment with slope \( w = -\frac{1}{2} \) or \( w = -\frac{1}{4} \). By Corollary (1.2.2), 2 ramifies in \( \mathbb{Q}_2(\theta) = E \). This completes the proof of Theorem 1. \( \square \)
CHAPTER II: DYADIC RAMIFICATION IN \( \mathbb{Q}[x]/(x^4 + cx^2 + d) \)

II.1 INTRODUCTION

Let \( f(x) = x^4 + cx^2 + d \) be an irreducible trinomial over \( \mathbb{Z} \). Put

\[
E = \mathbb{Q}[x]/(x^4 + cx^2 + d)
\]

Associated with \( x^4 + cx^2 + d \) is the quadratic trinomial \( T^2 + cT + d \).

Put

\[
F = \mathbb{Q}[T]/(T^2 + cT + d).
\]

Let \( \sigma \) be a root of \( T^2 + cT + d \). Then \( \sqrt{\sigma} \) is a root of \( x^4 + cx^2 + d \).

Furthermore \( F = \mathbb{Q}(\sigma) \) and \( E = F(\sqrt{\sigma}) \). So we have a tower of quadratic fields

\[
\begin{align*}
E &= F(\sqrt{\sigma}) \\
F &= \mathbb{Q}(\sigma) \\
Q &.
\end{align*}
\]

We will study the ramification of the rational prime 2 in \( E \). We will find necessary and sufficient conditions for 2 to be unramified in \( E/\mathbb{Q} \).

Write the quadratic field \( F = \mathbb{Q}(\sigma) \) in standard form \( F = \mathbb{Q}(\sqrt{m}) \), where \( m \) is the square-free part of \( c^2 - 4d \). So if 2 is to be unramified in \( E \) we must have 2 unramified in \( F/\mathbb{Q} \), so necessarily
m \equiv 1 \pmod{4}. The quadratic field $F$ contains one or two dyadic prime ideals. If $\text{ord}_P(\sigma)$ is odd for some dyadic prime ideal $P \subset O_F$, then clearly $P$ ramifies in $E/F$, so if $E/Q$ is unramified at 2 we must have $\text{ord}_P(\sigma) \equiv 0 \pmod{2}$ at every dyadic prime ideal $P \subset O_F$. The two conditions

(1) $m \equiv 1 \pmod{4}$,

(2) $\text{ord}_P(\sigma) \equiv 0 \pmod{2}$ at every dyadic prime ideal $P \subset O_F$

are thus necessary for $E/Q$ to be unramified at 2. However, by themselves these two conditions are not sufficient. There is a third condition coming from Witt theory (see Section II.2), namely

$$\gamma_2^E = -1.$$ 

One case from Section II.3 of this chapter is of special interest.

(II.3.5) **Lemma.** Let $m \equiv 1 \pmod{8}$ be a square-free integer. Put $F = \mathbb{Q}(\sqrt{m})$. Let $P_1$ and $P_2$ be dyadic primes of $F$. Let $\sigma \in F$ have $\text{ord}_{P_1}(\sigma) \equiv \text{ord}_{P_2}(\sigma) \equiv 0 \pmod{2}$ and let $E = \mathbb{Q}(\sqrt{\sigma})$. Then

(1) One of $P_1$, $P_2$ ramifies in $E$, the other is unramified if and only if $\gamma_2^E = 1$.

(2) Both $P_1$ and $P_2$ ramify in $E$ if and only if $\gamma_2^E = 1$.

(3) Both $P_1$ and $P_2$ are unramified in $E$ if and only if $\gamma_2^E = -1$.

We also study the companion of $E$. Define $E_c = E(\sqrt{-\sigma})$. Under very general hypothesis (see Section II.4), we prove that 2 is unramified in exactly one of $E/Q$, $E_c/Q$. An application involving fundamental units will be given in Chapters III and IV.
II.2. SYNOPSIS OF WITT THEORY

In this section we recall briefly some basic facts from Witt theory.

II.2.1. VAN der BLIJ'S INARIANT

Let \((V, b)\) be an inner product space over \(\mathbb{Z}_2\); that is, \((V, b)\) is an innerproduct space over \(\mathbb{Q}_2\) with \(\text{ord}_2(\text{dis} V) \equiv 0 \pmod{2}\). Then there is a basis for \(V\) in which the matrix of \(b\) has entries in \(\mathbb{Z}_2\) and determinant equal to a unit in \(\mathbb{Z}_2\). Thus the reduction \(V/2V\) of \((V, b)\) modulo 2 is an innerproduct space over the finite field \(\mathbb{F}_2\).

The map \(V/2V \to \mathbb{F}_2\) given by

\[ x \mid \mapsto b(x, x) \pmod{2} \]

is \(\mathbb{F}_2\)-linear. But as an \(\mathbb{F}_2\)-space

\[ \text{adjoint} : V/2V = \text{Hom}(V/2V, \mathbb{F}_2) \]

so there is an element \(u \in V\) for which

\[ b(u, x) \equiv b(x, x) \pmod{2} \]

for every \(x \in V\).

Van der Blij's invariant for \((V, b)\) is defined to be

\[ \beta(V, b) \equiv b(u, u) \pmod{8}. \]

Van der Blij proved that this is an invariant of \((V, b)\) in the sense that, modulo 8, \(b(u, u)\) does not depend on the choice of \(u \in V\), and he showed that

\[ W(\mathbb{Z}_2) \to \mathbb{Z}/8 + 0 \]
is a surjective ring homomorphism (see [M-H], p. 25). The kernel of $\beta$ consists of the so-called Type II spaces. If $L/\mathbb{Q}_2$ is an unramified extension of degree $f$ then

$$\beta(L) = f \text{ in } \mathbb{Z}/\mathbb{Z}$$

(See [C-P] (III.8.3) p. 158).

II.2.2 LOCAL ROOT NUMBERS

Let $p$ be a rational prime and $\mathbb{Q}_p$ be the $p$-adic completion of $\mathbb{Q}$. For each square class $d \in \mathbb{Q}^*/\mathbb{Q}^{**}$ the Hilbert symbol defines a real quadratic character

$$\chi_d : \mathbb{Q}_p^* \rightarrow \mathbb{Z}^* = \{1,-1\}$$
given by

$$\chi_d(x) = (x,d)_2.$$  

Following ([T], p. 94) there is associated to $\chi_d$ a fourth root of unity $r_p(d)$ in $\mathbb{C}^*$, called the $p$-adic local root number. Tate has proved

$$r_p(a)r_p(b) = r_p(ab) \cdot (a,b)_p$$

for any two square classes $a,b$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{**}$. Putting $a = b = d$ yields

$$[r_p(d)]^2 = (-1,d)_p^2.$$  

We briefly recall the formal definition of local root number.

There is a canonical additive map

$$\psi : \mathbb{Q}_2^+ \rightarrow \mathbb{C}^*$$
on the additive group $\mathbb{Q}_p^+$ with values in $\mathbb{C}^*$ and where $\psi$ is a composition of the canonical maps.
where $S^1$ denotes the unit circle in $\mathbb{C}$.

Let $I \subseteq \mathbb{Z}_p$ be an ideal. Put

$$U_I = \ker\{ \mathbb{Z}_p^* \to (\mathbb{Z}_p/I)^* \} = \{ t \in \mathbb{Z}_p^* | t \equiv 1 \pmod{I} \}$$

The conductor $f$ of $x$ is the largest ideal $I$ with

$$U_I \subseteq \ker(x)$$

Now $f = p^j$ for some $j$ in $\mathbb{N}$. Further let $L$ be a set of representatives of cosets of $\mathbb{Z}_p^*$ modulo $U_f$. Then the $p$-adic local root number associated with the real additive character $\chi_d$ defined by the square class $d$ is

$$r_p(d) = \frac{1}{\sqrt{N}} \sum_{\chi_d} \chi_d(x) \psi(x) \psi(x)$$

Here, $N$ is the absolute norm of $f$, and the sum is taken over $L$.

The following proposition is from Conner and Yui (see [C-Y] (4.2) p. 22 and (4.3) p. 23).

(II.2.2) PROPOSITION. Let $d$ be a square-free rational integer and $q \equiv 1 \pmod{4}$ be a rational prime. Then

1. If $q$ divides $d$ then $r_q(d) = \left( \frac{-d}{q} \right) q$.
2. $r_p(q) = r_q(p) = 1$ for all primes $p$ in $\mathbb{Q}$.

We now turn our attention to $\mathbb{Q}_2$. There are 8 square classes $d$ in $\mathbb{Q}_2^*/\mathbb{Q}_2^{**}$, namely the classes of $1, 3, 5, -1, 2, 6, -6, -2$. By Tate's formula $r_2(d)$ can be computed for any $d$ once $r_2(1), r_2(-1), r_2(2), r_2(3)$ and $r_2(5)$ are known. Clearly $r_2(1) = 1$. The remaining 4 values were determined in ([C-Y], (4.3), (4.4) p. 23) as follows: $r_2(-1) = r_2(3) = 1$.
and \( r_2(2) = r_2(5) = 1 \). Then for \( d \in \mathbb{Q}_2^*/\mathbb{Q}_2^{**} \) we have the result

<table>
<thead>
<tr>
<th>( d )</th>
<th>( r_2(d) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>-1</td>
<td>i</td>
</tr>
<tr>
<td>2</td>
<td>i</td>
</tr>
<tr>
<td>-2</td>
<td>i</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>-i</td>
</tr>
<tr>
<td>-6</td>
<td>-1</td>
</tr>
</tbody>
</table>

Table 1.

II.2.3. THE ADDITIVE CHARACTER \( \gamma_p \)

Briefly we say that for any finite rational prime \( p \), \( \gamma_p \) is an additive character of the Witt ring \( W(Q_p) \) with values in \( \mathbb{C}^* \).

Recently Conner and Yui ([C-Y]) p. 31) have derived a formula which allows us to compute the value \( \gamma_p(X) \). In particular

\[
\gamma_p : W(Q_p) \rightarrow \mathbb{C}^*
\]

is given by

\[
\gamma_p(X) = \begin{cases} 
(-2,d)_p \cdot c_p(X) \cdot r_p(d), & \text{if } X \text{ has even rank} \\
(-2,d)_p \cdot c_p(X) \cdot r_p(d) \cdot \eta, & \text{if } X \text{ has odd rank} 
\end{cases}
\]

where \( \eta = e^{\frac{2\pi i}{8}} \), \( d = \text{Dis}(X) \), and \( c_p(X) \) is the stable Hasse-Witt symbol. In particular if \( X \in W(Q) \), then \( \gamma_p(X) \) is defined for all finite primes. Then by Weil Reciprocity

\[
\prod_{p \text{ finite}} \gamma_p(x) = \exp(\pi i \cdot \text{sgn}(x)/4).
\]
Our computations with additive characters for the most part will involve having to compute $\gamma_2(X)$. Moreover when $\text{ord}_2(\text{Dis } X) \equiv 0 \pmod{2}$ then Van der Blij's invariant is defined for $X$, and then

$$\gamma_2(X) = \eta^{\beta(X)} \quad (***)$$

(see [C-Y], (7.1) p. 39).

To compute $\gamma_2(X)$ efficiently from formula (**) we need the local root numbers which we have from Table 1, the values $c_2(X)$ which depend on $X$, and the Hilbert symbols $(-2,d)_2$ computed as follows

$$(2,1)_2 = (2,-1)_2 = 1$$
$$(2,3)_2 = (2,5)_2 = -1$$
$$(2,2)_2 = (2,-2)_2 = 1$$
$$(2,6)_2 = (2,-6)_2 = -1$$

Table 2.

II.3. SIX LEMMAS

In this section we state and prove the technical results we will need.

(II.3.1) LEMMA. Let $m \equiv 1 \pmod{4}$ be a rational integer. Then $(-1,m)_2 = 1$.

PROOF: Write $m = \varepsilon \cdot p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} q_1 q_2 \cdots q_s$, where

$\varepsilon = \text{sign}(m)$, $p_i \equiv 1 \pmod{4}$ and $q_j \equiv 3 \pmod{4}$. By reciprocity

$$1 = \prod_{p} (-1,m)_2^{e_1} \prod_{j=1}^{t} (-1,m)_{q_j}^{e_j} \prod_{j=1}^{s} (-1,m)_{q_j}^{e_j}.$$
Suppose $\epsilon = +1$. Since $m \equiv 1 \pmod{4}$ then $s = \prod_{i=1}^{s} q_i \equiv 1 \pmod{4}$ so $s$ is even. Moreover $m > 0$ so $(-1,m)_m = +1$. Each $p_j \equiv 1 \pmod{4}$ so each $(-1,m)_{p_j} = +1$. Each $q_i \equiv 3 \pmod{4}$ so each $(-1,m)_{q_i} = -1$. But $s$ is even, so $\prod_{i=1}^{s} (-1,m)_{q_i} = +1$. All together we find: $1 = (-1,m)_2$.

Suppose $\epsilon = -1$. Then $m < 0$ and $-m \equiv 3 \pmod{4}$ so $s$ is odd. Also, $(-1,m)_m = -1$. As before we have $(-1,m)_{p_j} = 1$ and $(-1,m)_{q_i} = -1$. Since $s$ is odd $\prod_{i=1}^{s} (-1,m)_{q_i} = -1$. Thus the result $1 = (-1,m)_2$. This proves Lemma (II.3.1).

**Lemma (II.3.2).** Let $x^4 + cx^2 + d$ be an irreducible trinomial in $\mathbb{Z}[x]$. Put $E = Q[x]/(x^4 + cx^2 + d)$. Let $m$ be the square-free part of $c^2 - 4d$ and let $\sigma$ be a root of $T^2 + cT + d$. Then

1. $\langle E \rangle = \langle 1, m, -2c, -2cdm \rangle$ in $W(Q)$
2. $c_2\langle E \rangle = (-1,-m)_2 \cdot (-2c,-md)_2$
3. $\text{Dis} E = d = \text{Dis}(E/Q)$ in $Q^*/Q^{**}$.

**Proof:** Put $F = Q(\sigma) = Q(\sqrt{m})$. Since $\sigma$ satisfies $T^2 + cT + d$, we see that $N_{F/Q}(\sigma) = d$ and $\text{trace}_{F/Q}(\sigma) = -c$. Then following ([C-P], (1.4.2) p. 26 and p. 51-52) we compute

$$\langle E \rangle = \langle F(\sqrt{\sigma}) \rangle = 2\langle F \rangle + \langle F_\sigma \rangle$$

where $\langle F_\sigma \rangle$ is the Witt class of the scaled trace form $\text{trace}_{F/Q}(\sigma xy)$. In terms of $c,d$ and $m$, we have

$$\langle F \rangle = \langle 2,2m \rangle$$

and $\langle F_\sigma \rangle = \langle -c,-cdm \rangle$. So

$$\langle E \rangle = \langle F(\sqrt{\sigma}) \rangle = 2(\langle 2,2m,-c,-cdm \rangle)$$.
Thus

\[<E> = <1, m, -2c, -2cmd>\]

and

\[c_2 <E> = (-1, -m)_2(-2c, -md)_2.\]

Put \(\delta = (-1)^{2(4-1)}\). Then \(\text{Dis}<E> = d = \delta \cdot \text{Dis}(E/\mathbb{Q})\) in \(\mathbb{Q}^*/\mathbb{Q}^{**}\). But \(\delta = 1\). So

\[\text{Dis}(E/\mathbb{Q}) = d \text{ in } \mathbb{Q}^*/\mathbb{Q}^{**},\]

proving Lemma II.3.2. []

(II.3.3) LEMMA. Let \(x^4 + cx^2 + d\) be irreducible in \(\mathbb{Z}[x]\) and \(T^2 + cT + d\) be the associated quadratic polynomial. Put \(E = \mathbb{Q}[x]/(x^4 + cx^2 + d)\) and \(F = \mathbb{Q}[T]/(T^2 + cT + d)\).

(1) \(E/\mathbb{Q}\) is a normal degree 4 extension if and only if \(d\) is a square in \(F\).

(2) \(E/\mathbb{Q}\) is a cyclic degree 4 extension if and only if \(d\) is a square in \(F\) and \(d\) is not a square in \(\mathbb{Q}\).

(3) \(E/\mathbb{Q}\) is an abelian extension with Galois group the Klein Vierergruppe if and only if \(d\) is a square in \(\mathbb{Q}\).

PROOF: \(F\) is a quadratic extension of \(\mathbb{Q}\) so \(F = \mathbb{Q}(\sqrt{m})\) for a square-free integer \(m\). In fact, \(m\) is the square-free part of \(c^2 - 4d\), as is easily seen by completing the square of \(T^2 + cT + d\). Let \(\sigma\) be a root of \(T^2 + cT + d\). Then \(\sqrt{\sigma}\) is a root of \(x^4 + cx^2 + d\). The extension \(E/\mathbb{Q}\) is a normal degree 4 extension if and only if every embedding \(\tau : E \to \mathbb{C}\) maps \(E\) to itself. The restriction of \(\tau\) to \(F\)

\[\tau|_{F}\]

is either 1 or \(\alpha\).
where the identity 1 and \( \alpha(\sqrt{m}) = -\sqrt{m} \) are the two automorphisms of \( F \). 

Now 
\[
(\sqrt{\sigma})^2 = \sigma \quad \text{so,} \quad \tau(\sqrt{\sigma})^2 = \tau(\sigma) \quad \text{in} \quad F.
\]

Thus if \( \tau|_F = 1 \) then \( \tau(\sqrt{\sigma}) = \pm \sqrt{\sigma} \) certainly maps \( E \) to \( -E \).

If \( \tau|_F = \alpha \) then \( \tau(\sqrt{\sigma}) = \pm \sqrt{\alpha \sigma} \). So \( E/Q \) is normal if and only if \( \sqrt{\alpha \sigma} \) belongs to \( E \). Along with \( \sigma, \alpha \sigma \) is also a non-square in \( F \). So the condition for normality is \( F(\sqrt{\alpha \sigma}) = F(\sqrt{\sigma}) \), i.e. \( \sqrt{\alpha \sigma} = h\sqrt{\sigma} \) for some \( h \) in \( F \). That is, \( E/Q \) is normal if and only if \( \alpha \sigma = h^2 \sigma \) if and only if \( N(\sigma) = d = \sigma \cdot \alpha \sigma = (h \sigma)^2 \) is a square in \( F \). This proves (1).

Let \( G \) be the Galois group of \( E/Q \). From ([C-P] (1.3.4) p. 24) \( G \) contains a non-trivial cyclic Sylow 2-subgroup if and only if \( \text{Dis}(E/Q) \) is not a square in \( Q \). By Lemma (II.3.2) \( \text{Dis}(E/Q) = d \) in \( Q^*/Q^{**} \).

Therefore \( G \) is a cyclic group of order 4 if and only if \( d \) is not a square in \( Q^* \) and \( d \) is a square in \( F \). Consequently, \( G \) is the Klein Vierergruppe if and only if \( d \) is a square in \( Q \), proving the lemma. []

(II.3.4) LEMMA. Let \( K = Q_2(\sqrt{u}) \) be an extension of \( Q_2 \) with \( u = 1, -1, 3, \) or 5, a unit in \( Q_2^*/Q_2^{**} \). Let \( \eta = e^\frac{2\pi i}{8} \). Then 
\[
\gamma_2^{K} = \begin{cases} 
1 & \text{if } u = 5 \\
1 & \text{if } u = 3 \text{ or } -1 \\
\eta & \text{if } u = 1 
\end{cases}
\]

PROOF: If \( u = 1 \), then \( K = Q_2(\sqrt{1}) = Q_2 \) is a degree 1 extension of \( Q_2 \).

So \( d = \text{Dis } Q_2 = 1, c_2^{Q_2} = 1, \) and \( r_2(d) = 1 \). Thus 
\[
\gamma_2^{Q_2} = (-2,1)_2 \cdot c_2^{Q_2} \cdot r_2(1) \cdot \eta = \eta.
\]
If \( u = -1 \), then \( K = \mathbb{Q}_2(\sqrt{-1}) \) is a ramified quadratic extension of \( \mathbb{Q}_2 \) and \( \langle K \rangle = \langle 2, -2 \rangle \) in \( \mathbb{W}(\mathbb{Q}_2) \). So
\[
\text{Dis}<K> = (-1)^{\frac{2(2-1)}{2}} \text{Dis}(\mathbb{Q}_2(\sqrt{-1})) = (-1)(-4) = 4 = 1 \text{ in } \mathbb{Q}_2^*/\mathbb{Q}_2^{**}
\]
and \( c_2<K> = 1 \). Applying ((**), Section II.2.3, Tables 2 and 3)
\[
\gamma_2<\mathbb{Q}_2(\sqrt{-1})> = (-2, 1)_2 \cdot c_2(\mathbb{Q}_2(\sqrt{-1})) \cdot r_2(1) = 1 \cdot 1 \cdot 1 = 1.
\]
If \( K = \mathbb{Q}_2(\sqrt{3}) \) then \( \langle K \rangle = \langle 2, 6 \rangle \) and \( c_2<K> = -1, \text{Dis}<K> = -3 = 5 \text{ in } \mathbb{Q}_2^*/\mathbb{Q}_2^{**} \) and \( r_2(5) = 1 \). So
\[
\gamma_2<\mathbb{Q}_2(\sqrt{3})> = (-2, 5)_2 \cdot c_2<\mathbb{Q}_2(\sqrt{3})> \cdot r_2(5) = (-1)(-1)(1) = 1.
\]
Finally, suppose \( K = \mathbb{Q}_2(\sqrt{5}) \). Then \( K \) is the unique unramified quadratic extension of \( \mathbb{Q}_2 \). Therefore, since \( \text{ord}_2(5) \equiv 0 \pmod{2} \), Van der Blij's invariant \( \beta \in \mathbb{Z}/8\mathbb{Z} \) is defined on \( \langle K \rangle \) and \( \beta<K> = 2 \). (see (*) section II.2.1). Thus
\[
\gamma_2<\mathbb{Q}_2(\sqrt{5})> = \eta^2 = 1.
\]
So Lemma (II.3.4) is proved. \[\]

(II.3.5) **LEMMA.** Let \( m \equiv 1 \pmod{8} \) be a square-free integer. Put \( F = \mathbb{Q}(\sqrt{m}) \). Let \( P_1 \) and \( P_2 \) be dyadic primes of \( F \). Let \( \sigma \in F \) have \( \text{ord}_{P_1}^{P_2} \equiv \text{ord}_{P_1}^{P_2} \equiv 0 \pmod{2} \) and let \( E = \mathbb{Q}(\sqrt{\sigma}) \). Then

1. One of \( P_1, P_2 \) ramifies in \( E \), the other is unramified if and only if \( \gamma_2<E> = 1 \).
2. Both \( P_1 \) and \( P_2 \) ramify in \( E \) if and only if \( \gamma_2<E> = 1 \).
3. Both \( P_1 \) and \( P_2 \) are unramified in \( E \) if and only if \( \gamma_2<E> = -1 \).
PROOF: Since \( m \equiv 1 \pmod{8} \), the dyadic primes \( P_1 \) and \( P_2 \) of \( F \) are distinct conjugate primes of \( F \). Then \( F = \mathbb{Q}_2 \sim F \). At a dyadic prime \( q \) of \( E \), \( E_q = \mathbb{Q}_2(\sqrt{q}) \). Since \( \text{ord}_{p_j}(\sigma) \) is even at a dyadic prime \( p_j \) of \( F \), we have

\[
\sigma = \pi^2 \cdot u \quad \text{for some unit } u \text{ in } \mathbb{Q}_2
\]

where \( \pi \) is a prime element for \( P \). Thus

\[
E_q = \mathbb{Q}_2(\sqrt{u})
\]

(Note that \( u \) depends on the choice of \( P_1 \) and \( P_2 \) and \( u = 1, -1, 3 \) or 5 in \( \mathbb{Q}_2^*/\mathbb{Q}_2^{**} \). If \( p_j \) is ramified in \( E \) then \( u = -1 \) or \( 3 \); if \( p_j \) is inert \( u = 5 \) and if \( p_j \) splits \( u = 1 \).) By Lemma (II.3.4)

\[
\gamma_2<\mathbb{Q}_2(\sqrt{3})> = \gamma_2<\mathbb{Q}_2(-1)> = 1, \quad \gamma_2<\mathbb{Q}_2(\sqrt{5})> = 1 \quad \text{and} \quad \gamma_2<\mathbb{Q}_2> = \eta.
\]

If \( P_1 \) is ramified in \( E \) and \( P_2 \) is unramified in \( E \) then either \( u = -1 \) or \( 3 \) and \( P_2 \) is inert, whence

\[
\gamma_2<E> = \gamma_2<\mathbb{Q}_2(\sqrt{u})> \cdot \gamma_2<\mathbb{Q}_2(\sqrt{5})> = 1 \cdot i = i;
\]

or \( u = -1 \) or \( 3 \) and \( P_2 \) splits, whence

\[
\gamma_2<E> = \gamma_2<\mathbb{Q}_2(\sqrt{u})> \cdot \gamma_2<\mathbb{Q}_2> \cdot \gamma_2<\mathbb{Q}_2> = 1 \cdot \eta \cdot \eta = i.
\]

If both \( P_1 \) and \( P_2 \) are ramified in \( E \) then

\[
\gamma_2<E> = \gamma_2<\mathbb{Q}_2(\sqrt{u})> \cdot \gamma_2<\mathbb{Q}_2(\sqrt{u'})> = 1 \cdot 1 = 1,
\]

since \( u \) and \( u' \) lie in \( \{-1, 3\} \).

If both \( P_1 \) and \( P_2 \) are unramified in \( E \) then either both \( P_1 \) and \( P_2 \) are inert, whence

\[
\gamma_2<E> = \gamma_2<\mathbb{Q}_2(\sqrt{5})> \cdot \gamma_2<\mathbb{Q}_2(\sqrt{5})> = 1 \cdot i = -1,
\]
or $P_1$ is inert and $P_2$ splits, whence

$$\gamma_2^{<E>} = \gamma_2^{<\mathbb{Q}_2(\sqrt{5})>} \cdot \gamma_2^{<\mathbb{Q}_2>} \cdot \gamma_2^{<\mathbb{Q}_2>} = i \cdot n \cdot n = -1$$

or both $P_1$ and $P_2$ split, whence

$$\gamma_2^{<E>} = \gamma_2^{<\mathbb{Q}_2>} \cdot \gamma_2^{<\mathbb{Q}_2>} \cdot \gamma_2^{<\mathbb{Q}_2>} \cdot \gamma_2^{<\mathbb{Q}_2>} = n \cdot n \cdot n \cdot n = -1$$

This proves Lemma (II.3.5). \[ \square \]

(II.3.6) **Lemma.** Let $F_2 = \mathbb{Q}_2(\sqrt{5})$. Let $u_1 = -1$ and $u_5 = 5 + 2\sqrt{5}$.

Then for each choice $j = 1, 5$ the prime 2 is unramified in exactly one of $F_2(\sqrt{u_j})$ or $F_2(\sqrt{-u_j})$.

**Proof:** Consider $u_1 = -1$. The local field $F_2(\sqrt{-u_1}) = F_2(\sqrt{-1}) = F_2$ is unramified over $F_2$, and $F_2(\sqrt{u_1}) = F_2(\sqrt{-1})$ contains $\mathbb{Q}_2(\sqrt{-1})$, and is ramified over $Q_2$ and thus over $F_2$. Now we consider $u_5 = 5 + 2\sqrt{5}$. Put $L = F_2(\sqrt{5 + 2\sqrt{5}})$ and its companion $L_c = F_2(\sqrt{-(5 + 2\sqrt{5})})$. First we show that $L_c$ is unramified over $F_2$.

Observe that

$$-u_5 = -5 - 2\sqrt{5} = -3 - 4\left(\frac{1 + \sqrt{5}}{2}\right) = -3 + 4 - 4\left(\frac{1 + \sqrt{5}}{2}\right)$$

Hence $-u_5 = 1 - 4(1 + 1\left(\frac{1 + \sqrt{5}}{2}\right))$. Thus $-5 - 2\sqrt{5} \equiv 1 \pmod{4 \cdot O_{F_2}}$.

Since $N_{F_2/Q_2}(-u_5) = 5$, $-u_5$ is itself not a local square in $F_2$, but $-u_5$ is congruent to a square in $4 \cdot O_{F_2}$. Therefore $-u_5$ has quadratic defect $4 \cdot O_{F_2}$ (see [O'M], p. 159-160). Therefore ([O'M], (63:3) p. 161) $L_c = F_2(\sqrt{-5 - 2\sqrt{5}})/F_2$ is unramified.

To show that $L = F_2(\sqrt{u_5})$ is ramified over $Q_2$ we observe that

$$u_5 = 5 + 2\sqrt{5} = 3 + 4\left(\frac{1 + \sqrt{5}}{2}\right).$$
So $u_5 \equiv 3 \pmod{40_{(2)}}$. So $u_5$ is not congruent to a local square modulo $4 \cdot O_{F(2)}$, so $u_5$ does not have quadratic defect $4 \cdot O_{F(2)}$.

Therefore $L = F_{(2)}(\sqrt{3+2/5})$ is ramified over $F_{(2)}$. 

II.4 DYADIC RAMIFICATION IN $\mathbb{Q}[x]/(x^4 + cx^2 + d)$

In this section we prove the main theorem of chapter II.

**THEOREM 2.** Let $x^4 + cx^2 + d$ be an irreducible trinomial in $\mathbb{Z}[x]$ with root $\sqrt{\sigma}$ and let $m$ be the square-free part of $c^2 - 4d$. The rational prime $2$ is unramified in $E = \mathbb{Q}(\sqrt{\sigma})$ if and only if

1. $m \equiv 1 \pmod{4}$
2. $\text{ord}_p(\sigma) \equiv 0 \pmod{2}$ for every dyadic prime ideal $P \subset F = \mathbb{Q}(\sigma) = \mathbb{Q}(\sqrt{m})$.
3. $\gamma_2(E) = -1$.

**PROOF:** ($\Rightarrow$) Suppose $2$ is unramified in $E/\mathbb{Q}$. Then $2$ is unramified in $F$, hence $m \equiv 1 \pmod{4}$. This proves (1).

Each prime ideal $P$ of $F$ lying above $2$ is unramified in $E$. Now $E = F(\sqrt{\sigma})$, so $E = F[x]/(x^2 - \sigma)$ and the discriminant of $x^2 - \sigma$ is $4\sigma$. Also the principal ideal $(4\sigma) = A^2 \cdot (\text{Disc}(E/F))$ as ideals in $O_F$ for some ideal $A$ in $O_F$. If $\text{ord}_p(\sigma)$ were odd then $P$ divides $(4\sigma)$ to an odd power, so $P$ divides $(\text{Disc}(E/F))$, so $P$ ramifies. Since $P$ is unramified, $\text{ord}_p(\sigma)$ is even, proving (2).

Using (2) we see that

$\sigma = 2^{2s} \cdot t$ with $(2,t) = 1$ if $2$ is inert in $F$ and

$\sigma = p_1^{2a} p_2^{2b} \cdot Q$ with $(p_1,Q) = (p_2,Q) = 1$
if \((2) = P_1 \cdot P_2\) in \(F\) with distinct conjugate prime ideals \(P_1, P_2\) in \(F\).

In the first case, \(N(\sigma) = 4^a N(t)\) with \(N(t)\) odd. In the second case, \(N(\sigma) = 2^{2a} 2^{2b} N(Q)\) with \(N(Q)\) odd. In either case,
\[
\text{ord}_2(N(\sigma)) \equiv 0 \pmod{2}.
\]
Thus Van der Blij's invariant \(\beta(\mathcal{E})\) in \(\mathbb{Z}/\mathbb{Q}\) is defined and since \(E/\mathbb{Q}\) is unramified, \(\beta(\mathcal{E}) = \text{deg}_Q(E) \equiv 4 \pmod{8}\) (by \((*)\), (II.2.1)). Then (by \((***)\) Section II.2.3)
\[
\gamma_2^{\mathcal{E}} = \eta^4 = -1
\]
where \(\eta = 2\pi i/8\), proving (3).

\((<=)\) Conversely, suppose (1), (2) and (3) hold. We must show that 2 is unramified in \(E/\mathbb{Q}\).

By (1) \(m \equiv 1 \pmod{4}\) so 2 is unramified in \(F\). We must show that the dyadic primes of \(F\) are unramified in \(E\).

Take a dyadic prime \(q\) of \(E\) and let the restriction of \(q\) to \(F\) be \(P\). Let \(E_q\) be the completion of \(E\) at \(q\) and let \(F_p\) be the completion of \(F\) at \(P\). It is to be shown that \(E_q/F_p\) is unramified.

Arguing by contradiction we will show: If \(q|P\) is ramified and if (1) and (2) hold then \(\gamma_2^{\mathcal{E}} \neq -1\).

We have \(c^2 - 4d = m \cdot t^2\) for some \(t\) in \(\mathbb{Z}\). If \(c = 0\) then \(d = -m\) in \(\mathbb{Q}^*/\mathbb{Q}^{**}\). Now \(-m \equiv -1 \equiv 3 \pmod{4}\) hence \(-m \equiv 3\) or \(-1\) mod 8. Thus \(-m = 3\) or \(-1\) in \(\mathbb{Q}_2^*/\mathbb{Q}_2^{**}\), so \(r_2(d) = 1\) (see Table 1).

Therefore
\[
\gamma_2^{\mathcal{E}} = (\pm 2, -m)_2 \cdot c_2^{\mathcal{E}} \cdot \gamma_2(-m) = \pm i \neq -1.
\]
So we may assume \(c \neq 0\).

We will consider two cases:

\[ m \equiv 1 \pmod{8} \quad \text{and} \quad m \equiv 5 \pmod{8} \]
Case I: \( m \equiv 1 \pmod{8} \)

The prime 2 in \( \mathbb{Q} \) decomposes in \( \mathcal{O}_F \) as a product of two distinct conjugate prime ideals \( P_1 \cdot P_2 \). We are assuming that \( E/\mathbb{Q} \) is ramified. Therefore one of \( P_1 \) and \( P_2 \) must ramify in \( E \); say \( P_1 \) ramifies in \( E \). In \( \mathcal{O}_E \) the other dyadic prime \( P_2 \) may either remain prime, split or ramify. In either case Lemma (II.3.5) shows \( \gamma_2^{E_{\mathbb{Q}}} \neq -1 \), proving Case I.

Case II: \( m \equiv 5 \pmod{8} \)

Since \( m \equiv 5 \pmod{8} \) the prime 2 is inert in \( F \). We are still operating under the assumption that \( c \neq 0 \) and \( \text{ord}_p(c) \equiv 0 \pmod{2} \) at the unique prime ideal \( P \subseteq \mathcal{O}_F \) lying over 2, and \( E/\mathbb{Q} \) is ramified. It is to be shown that \( \gamma_2^{E_{\mathbb{Q}}} \neq -1 \).

Let \( q \) be a dyadic prime of \( E \) and let \( P \) be the restriction of \( q \) to \( F \). Then \( P \) is the unique dyadic prime of \( F \) and

\[
E_q = F_p(\sqrt{q}) = F_p(\sqrt{u})
\]

for some unit \( u \) in \( F_p \), determined up to squares of units in \( F_p \). Now \( F_p \) has degree \( n = 2 \) over \( \mathbb{Q}_2 \) so there are

\[
2^{n+1} = 8
\]

classes of units modulo squares, and \( u \) is one of these 8 possibilities. Hence \( N_{F_p/\mathbb{Q}_2}(u) \) is one of

\[
1, 3, 5, -1
\]

modulo unit squares in \( \mathbb{Q}_2 \). Suppose the norm of \( u \) is 3 or \(-1\). Then \( d = \text{Dis}^{E_q} = N(u) \) is 3 or \(-1 \pmod{2} \) squares in \( \mathbb{Q}_2 \) so
\[ \gamma_2 \mathcal{E} = \pm r_2(d) = \pm 1 \neq -1 \]

by Lemma (II.3.5). It remains to consider \( N(u) = 1 \) or 5.

Consider \( u_1 = -1 \) and \( u_5 = 5 + 2\sqrt{5} \). Then \( \pm u_1 \) each have norm 1 and represent distinct square classes in \( \mathbb{F}_p \). Similarly, \( \pm u_5 \) each have norm 5 and represent distinct square classes in \( \mathbb{F}_p \). Now \( \mathbb{F}_p(\sqrt{-u_1}) \) and \( \mathbb{F}_p(\sqrt{-u_5}) \) give rise to unramified extensions of \( \mathbb{F}_p \) by Lemma (II.3.6), noting that \( \mathbb{F}_p = \mathbb{Q}_2(\sqrt{5}) \). Since we are assuming \( \mathbb{E}_q | \mathbb{Q}_2 \) is ramified, i.e. that \( \mathbb{E}_q | \mathbb{F}_p \) is ramified, we exclude the possibilities \( u = -u_1 \) and \( u = -u_5 \). This leaves \( u = u_1 = -1 \) and \( u = u_5 \) to consider.

Let \( L = \mathbb{F}_p(\sqrt{u_1}) = \mathbb{F}_p(\sqrt{5+2\sqrt{5}}) \). Both \( L \) and \( \mathbb{F}_p(\sqrt{-1}) \) are ramified over \( \mathbb{F}_p \) by Lemma (II.3.6). We'll show

\[ \gamma_2 \langle \mathbb{F}_p(\sqrt{-1}) \rangle = 1 \quad \text{and} \quad \gamma_2 \langle L \rangle = 1. \]

Since \( \sqrt{-1} \) satisfies \( x^4 + 2x^2 + 1 \) in \( \mathbb{Z}[x] \) we have

\[ c_2 \langle \mathbb{F}_p(\sqrt{-1}) \rangle = (-1, -5)_2 \cdot (-2(2), -5)_2 = (-1, -5)_2 (-1, -5)_2 = 1 \]

by (II.3.2). Therefore

\[ \gamma_2 \langle \mathbb{F}_p(\sqrt{-1}) \rangle = (-2, 1)_2 \cdot c_2 \langle \mathbb{F}_p(\sqrt{-1}) \rangle \cdot r_2(1) = 1 \cdot 1 \cdot 1 = 1 \]

by (**), (II.2.3)). Also \( \sqrt{5+2\sqrt{5}} \) satisfies \( x^4 - 10x^2 + 5 \) in \( \mathbb{Z}[x] \), and hence

\[ c_2 \langle L \rangle = (-1, -5)_2 (20, -25)_2 = (-1, -5)_2 (5, -1)_2 = -1. \]

Therefore

\[ \gamma_2 \langle \mathbb{F}_p(\sqrt{5+2\sqrt{5}}) \rangle = (-2, 5)_2 \cdot (-1) \cdot r_2(5) = 1. \]

This proves Theorem 2. \( \square \)
(II.4.1) COROLLARY. Let $m \equiv 1 \pmod{4}$ be a square-free rational integer and let $F = \mathbb{Q}(\sqrt{m})$. Take $\sigma = a + b\sqrt{m}$ in $F$ with $a, b$, in $\mathbb{Q}$ and

1. $ab \neq 0$.
2. $\text{ord}_p (\sigma) \equiv 0 \pmod{2}$ for all dyadic primes $P$ of $F$.
3. $N(\sigma) = 1$ or $5$ in $\mathbb{Q}_2^*/\mathbb{Q}_2^{**}$.

Put $E = F(\sqrt{\sigma})$ and $E_c = F(\sqrt{-\bar{\sigma}})$. Then the rational prime $2$ is unramified in one of $E$ or $E_c$ and ramified in the other.

PROOF: If $\sigma$ is a square in $F$ then $E = F$ and $E_c = F(\sqrt{-1})$ contains $\mathbb{Q}(\sqrt{-1})$, so $2$ is ramified in $E_c/\mathbb{Q}$. The same argument holds if $-\sigma$ is a square. So from now on, we assume that neither $\sigma$ nor $-\sigma$ is a square in $F$. Then $\sqrt{\sigma}$ satisfies the irreducible polynomial

$$f(x) = x^4 - 2ax^2 + (a^2 - mb^2)$$

and $\sqrt{-\sigma}$ satisfies the irreducible polynomial

$$f_c(x) = x^4 + 2ax^2 + (a^2 - mb^2).$$

Applying Lemma (II.3.2) to the coefficients of $f(x)$ and $f_c(x)$ we see that

$$c_2^E = (-1, -m)_2 \cdot (a, -md)_2$$

and

$$c_2^{E_c} = (-1, -m)_2 \cdot (-a, -md)_2 = (-1, -m)_2 \cdot (a, -md)_2 \cdot (-1, -md)_2.$$ 

So

$$c_2^{E_c} = (-1, -md)_2 \cdot c_2^E.$$ 

Since $md \equiv 1 \pmod{4}$, $(-1, md)_2 = 1$ by Lemma (II.3.1). Thus
\[ c_2^{E_c} = (-1,-1)_2 \cdot (-1,md)_2 \cdot c_2^{E} = -c_2^{E}. \]

Since \( d = N(\sigma) = 1 \) or 5, the local root number \( r_2(d) \) is 1, by Table 1, Section (II.2.2). Thus
\[
\gamma_2^{E_c} = -\gamma_2^{E} = \pm 1.
\]

Therefore precisely one of \( \gamma_2^{E} \) and \( \gamma_2^{E_c} = -1 \). Therefore 2 is unramified in precisely one of
\[
E = \mathbb{Q}(\sqrt{\sigma}) \quad \text{and} \quad E_c = \mathbb{Q}(\sqrt{-\sigma}).
\]

This proves Corollary (II.4.1).
CHAPTER III: AN APPLICATION OF THEOREM 2 TO FUNDAMENTAL UNITS OF NORM 1

III.1. INTRODUCTION

Theorem 2 gives necessary and sufficient conditions for the rational prime $2$ to be unramified in the quartic field $E = \mathbb{Q}[x]/(x^4 + cx^2 + d)$. It is interesting to apply Theorem 2 to the particular quartic fields

$$E = \mathbb{Q}(\sqrt{e})$$

where $e$ is a fundamental unit in the real quadratic field $F = \mathbb{Q}(\sqrt{m})$. Depending on $m$ the fundamental unit $e$ may have norm $+1$ or $-1$. In this chapter we chose $m$ so that $N_{F/\mathbb{Q}}(e) = +1$. Chapter IV deals with $N_{F/\mathbb{Q}}(e) = -1$.

To begin, choose a positive rational square-free integer $m$

$$m \equiv 1 \pmod{4}.$$ 

Then $F = \mathbb{Q}(\sqrt{m})$ is a real quadratic field and possesses a fundamental unit $e$. We assume that $m$ is chosen so that

$$N_{F/\mathbb{Q}}(e) = +1.$$ 

(If $m$ has a prime factor $p \equiv 3 \pmod{4}$ then $N_{F/\mathbb{Q}}(e) = +1$ is guaranteed.) Replace $e$ by $-e$ if necessary so that $e$ is totally positive.
Since \( m \equiv 1 \pmod{4} \) an integral basis of \( \mathcal{O}_F \) is \( 1, \frac{1 + \sqrt{m}}{2} \).

Writing \( \varepsilon \) in the form

\[
\varepsilon = k_1 + k_2 \left( \frac{1 + \sqrt{m}}{2} \right)
\]

for \( k_1, k_2 \) in \( \mathbb{Z} \), we see that \( \sqrt{\varepsilon} \) satisfies the irreducible trinomial

\[
f(x) = x^4 - (2k_1 + k_2)x^2 + 1
\]

in \( \mathbb{Z}[x] \). Thus \( E = F(\sqrt{\varepsilon}) = \mathbb{Q}(\sqrt{\varepsilon}) \) is a quartic extension of \( \mathbb{Q} \) of the form discussed in Chapter II and \( m \) is the square-free part of \( (2k_1 + k_2)^2 - 4 \). This quartic field \( E \) comes with its companion

\[
E_c = \mathbb{Q}(\sqrt{-\varepsilon})
\]

where \( \sqrt{-\varepsilon} \) satisfies

\[
f_c(x) = x^4 + (2k_1 + k_2)x^2 + 1
\]

obtained from \( f(x) \) by changing the sign of the coefficient of \( x^2 \).

Can 2 ramify in both \( E \) and its companion \( E_c \)? As an immediate corollary of (II.4.1) we have

([III.1.1] PROPOSITION. Choose a rational integer \( m > 1, m \equiv 1 \pmod{4} \) so that the norm of a totally positive fundamental unit \( \varepsilon \) in \( F = \mathbb{Q}(\sqrt{m}) \) is \( +1 \). Put \( E = F(\sqrt{\varepsilon}) \). Then the rational prime 2 is unramified in one of

\[
E = \mathbb{Q}(\sqrt{\varepsilon}) \quad E_c = \mathbb{Q}(\sqrt{-\varepsilon})
\]

and is ramified in the other.

So in which of \( E \) or its companion \( E_c \) does 2 ramify?

In Section III.4 of this chapter we show
(III.4.1) **PROPOSITION.** Let \( m > 1, m \equiv 1 \pmod{4} \) be a rational integer and suppose \( \varepsilon \) is a totally positive fundamental unit in \( \mathbb{Q}(\sqrt{m}) \) with \( N_{\mathbb{F}/\mathbb{Q}}(\varepsilon) = +1 \). Then the rational prime 2 is unramified in \( E = \mathbb{Q}(\sqrt{\varepsilon}) \) if and only if the following dyadic Hilbert symbol equals 1:

\[
(2 \cdot \text{trace}_{\mathbb{F}/\mathbb{Q}}(\varepsilon), -m)_2 = 1.
\]

We note that this condition reduces to

\[
(\text{trace}_{\mathbb{F}/\mathbb{Q}}(\varepsilon), -1)_2 = 1 \quad \text{when} \quad m \equiv 1 \pmod{8}
\]

and

\[
(\text{trace}_{\mathbb{F}/\mathbb{Q}}(\varepsilon), 3)_2 = -1 \quad \text{when} \quad m \equiv 5 \pmod{8}.
\]

For any given \( m \), Proposition (III.4.1) decides which of \( E \) or \( E_C \) is dyadically unramified. In at least one case it is possible to give general conditions on \( m \) guaranteeing that 2 is unramified in \( E \). Namely:

(III.4.3) **PROPOSITION.** Let \( m, F \) and \( \varepsilon \) be as above. If no prime \( p \equiv 3 \pmod{4} \) divides \( m \) and if \( N_{\mathbb{F}/\mathbb{Q}}(\varepsilon) = 1 \) then \( E/\mathbb{Q} \) is a dyadically unramified extension. Moreover, the quadratic extension \( E/F \) is everywhere unramified; hence \( E/F \) is a quadratic piece of the Hilbert class field over \( F \).

This is proved in (III.4).

When \( m \) has prime divisors \( p \equiv 3 \pmod{4} \) it is harder in general to decide which of \( E \) or \( E_C \) is dyadically unramified. Of course Proposition (III.4.1) applies for any specific \( m \). We obtain a general result in at least one interesting case, namely: when \( m = p_1 \cdot p_2 \) is a product to two distinct primes both of which are congruent to 3 modulo
4, then \( N(\varepsilon) = +1 \) is satisfied automatically (see Lemma (III.3.1)) and we have

\[ (III.4.4) \text{ PROPOSITION.} \quad \text{If } m = p_1 p_2 \text{ with } p_1 \text{ and } p_2 \text{ distinct primes and } p_1 \equiv p_2 \equiv 3 \pmod{4} \text{ then } E = \mathbb{Q}(\sqrt{\varepsilon}) \text{ is a quartic ramified extension.} \]

\[ (III.2.1) \text{ REMARK.} \quad \text{Since } N(\varepsilon) = 1, E/\mathbb{Q} \text{ is a normal non-cyclic extension by Lemma (II.3.3). Hence the Galois group of } E/\mathbb{Q} \text{ is the Klein Vierergruppe. Thus } E \text{ is the composite of two quadratic extensions of } \mathbb{Q}, \text{ so there is a square-free natural number } n \text{ such that} \]

\[ E = \mathbb{Q}(\sqrt{m}, \sqrt{n}). \]

Moreover,

1. \( n\varepsilon \) is a square in \( \mathbb{O}_F \)
2. \( n \) divides \( m \).

Namely: \( E = \mathbb{F}(\sqrt{\varepsilon}) = \mathbb{F}(\sqrt{n}) \) so \( \varepsilon = x^2n \) for some \( x \in \mathbb{F} \). So \( n\varepsilon = (nx)^2 \) is a square in \( \mathbb{F} \) and is in \( \mathbb{O}_F \); i.e. \( n\varepsilon \) is a square in \( \mathbb{O}_F \). To see (2), it suffices to show that any prime \( p \) in \( \mathbb{Q} \) that
divides \( n \) ramifies in \( F = \mathbb{Q}(\sqrt{m}) \). Let \( q \) be a prime ideal in \( \mathcal{O}_F \) lying above \( p \). Then

\[(p) = q^e, \text{ with } e = 1 \text{ or } 2.\]

It is to be shown that \( e = 2 \). But the restriction of the function \( \text{ord}_q \) to \( \mathbb{Z} \) gives

\[\text{ord}_q(a) = e \cdot \text{ord}_p(a)\]

for any \( a \in \mathbb{Z} \). For \( a = n \) we have

\[\text{ord}_p(n) = 1\]

since \( p \) divides \( n \) and \( n \) is square-free. Moreover

\[\text{ord}_q(n) = \text{ord}_q(\frac{m}{n}) \text{ is even}\]

since \( \epsilon \) is a unit and since \( \frac{m}{n} \) is a square in \( \mathcal{O}_F \). Hence \( e = 2 \), so \( p \) ramifies in \( F \). That is, \( p \) divides \( m \), showing that \( n \) divides \( m \).

By (2), \( \frac{m}{n} \) is an integer unequal to \( n \) (since \( m \) is square-free).

Replacing \( n \) by the smaller of \( \{n, \frac{m}{n}\} \) we can also say

\[(3) \quad 1 < n < \frac{m}{n}.\]

III.3 STANDARD FACTS ABOUT THE NORM OF \( \epsilon \).

Having chosen \( m \), we would like to know when \( N(\epsilon) = +1 \). Of course this is a famous unsolved problem in general. In this section we distinguish two cases which we call \text{NICE CASE} and \text{PATHOLOGICAL CASE}. 
A. NICE CASE

If there is at least one rational prime congruent to 3 modulo 4 dividing \( m \), then the norm of the fundamental unit is \(+1\). For completeness, we include the short proof of this classical fact.

(III.3.1) Lemma. Let \( m > 0 \) be a square-free integer and \( q \equiv 3 \pmod{4} \) a positive prime dividing \( m \). Then

\[ N(e) = 1 \]

where \( e \) is a fundamental unit of \( F = \mathbb{Q}(\sqrt{m}) \).

Proof. Write

\[ e = \frac{x}{r} + \frac{y}{r} \sqrt{m} \]

with \( r = 1 \) or \( 2 \), \( x, y \) in \( \mathbb{Z} \). Multiplying by \( r \) and taking norms

\[ r^2 N(e) = x^2 - y^2 m. \]

Suppose \( N_{F/Q}(e) = -1 \). Then

\[ -r^2 \equiv x^2 \pmod{q}. \]

Since \( r^2 = 1 \) or \( 4 \) is not \( 0 \pmod{q} \), this means \(-1\) is a square modulo \( q \). This a contradiction since \( q \equiv 3 \pmod{4} \). So we must have

\[ N_{F/Q}(e) = +1. \]

B. PATHOLOGICAL CASE

If no prime congruent to 3 modulo 4 divides \( m \) it can still happen that the norm of the fundamental unit is \(+1\). Short of seeing the fundamental unit in a table, these cases can be difficult to recognize. At least when \( m = p_1 \equiv 1 \pmod{4} \) then \( N_{F/Q}(e) = -1 \). This follows from
class-number considerations: The narrow class number $h^+_F$ is odd (Corollary to Theorem 8, Chapter 3, section 8, p. 247, [B-S]) so $h^+_F = h_F$ (in general $h^+_F = h_F$ or $h^+_F = 2 \cdot h_F$ for quadratic fields) and this forces $N(\epsilon) = +1$.

Conjecturally, there are infinitely-many $m$ leading to pathological cases.

III.4 DYADIC RAMIFICATION IN $E = F(\sqrt{\epsilon})/Q$.

Since $\epsilon$ is a totally positive unit only the dyadic primes in $F$ can possibly ramify in $E = F(\sqrt{\epsilon})$. Such ramification occurs if and only if the rational prime 2 ramifies in $E/Q$. The first two conditions of Theorem 2 are automatically satisfied by $m$ and $\epsilon : m \equiv 1 \pmod{4}$ and $\text{ord}_q(\epsilon) \equiv 0 \pmod{2}$ for all dyadic $q$ of $F$. So the rational prime 2 is unramified in $E/Q$ if and only if $\mathcal{V}_2^{E/Q} = -1$. It turns out that this condition on $\mathcal{V}_2$ simplifies to a condition on a Hilbert symbol.

(III.4.1) PROPOSITION. Let $m > 1$, $m \equiv 1 \pmod{4}$ be a rational integer and let $\epsilon$ be a totally positive fundamental unit in $F = Q(\sqrt{m})$. We assume $m$ is chosen so that $N_{F/Q}(\epsilon) = +1$. Then the rational prime 2 is unramified in $E = Q(\sqrt{\epsilon})$ if and only if the dyadic Hilbert symbol

$$(2 \cdot \text{trace}_{F/Q}(\epsilon), -m)_2 = 1.$$ 

PROOF. Since $m \equiv 1 \pmod{4}$ and $\text{ord}_q(\epsilon) \equiv 0 \pmod{2}$ for all dyadic prime ideals $q$ of $F$, conditions (1) and (2) of Theorem 2 are clearly satisfied by $m$ and $\epsilon$. Write

$$\epsilon = k_1 + k_2\left(\frac{1+\sqrt{m}}{2}\right)$$

for some positive integers $k_1$ and $k_2$. Then $\sqrt{\epsilon}$ satisfies
\[ x^4 - (2k_1 + k_2)x^2 + 1. \]

So the rational prime 2 is unramified in \( E \) if and only if

\[ \gamma_2^{<E>} = -1. \]

From (***) Section (II.2.3) we have

\[ \gamma_2^{<E>} = (-2,1)_2(-1,-m)_2(2(2k_1 + k_2), -m)_2r_2(1). \]

But \((-2,1)_2 = 1\) and \((-1,-1)_2 = -1\). A simple manipulation with the Hilbert symbol together with Lemma (II.2.3) yields \((-1,-1)_2(-1,m)_2 = -1\).

Then from Table 1, Section (II.2.2) we have \( r_2(1) = 1 \). Also \( 2k_1 + k_2 = \text{trace}_{F/Q}(\epsilon) \). So

\[ \gamma_2^{<E>} = -(2 \cdot \text{trace}_{F/Q}(\epsilon), -m)_2. \]

Thus we can say that 2 is unramified in \( E/Q \) if and only if

\[ (2 \cdot \text{trace}_{F/Q}(\epsilon), -m)_2 = 1. \]

Observation: Since

\[ (2, -m) = \begin{cases} 1 & \text{when } m \equiv 1 \pmod{8} \\ -1 & \text{when } m \equiv 5 \pmod{8} \end{cases} \]

Proposition (III.4.1) can be stated:

\[ 2 \text{ is unramified in } E \text{ when } \begin{cases} (\text{trace}_{F/Q}(\epsilon), -1)_2 = 1 \text{ if } m \equiv 1 \pmod{8} \\ (\text{trace}_{F/Q}(\epsilon), 3)_2 = -1 \text{ if } m \equiv 5 \pmod{8}. \end{cases} \]

By (II.4.1) the dyadic primes of \( F \) are unramified in either \( F(\sqrt{2})/F \) or in \( F(\sqrt{-2})/F \); but are never unramified in both. So in which of \( F(\sqrt{2})/F \) or \( F(\sqrt{-2})/F \) are the dyadic primes of \( F \) unramified?
(III.4.2) PROPOSITION. Let \( m > 1, m \equiv 1 \pmod{4} \) be a rational integer and let \( \epsilon \) be a totally positive fundamental unit in \( F = \mathbb{Q}(\sqrt{m}) \). Also let \( n \) be such that \( E = \mathbb{Q}(\sqrt{m}, \sqrt{n}) \) with \( 1 < n < \frac{m}{n} \) (see Remark III.2.1). Then

1. the quadratic extension \( E = \mathbb{F}(\sqrt{\epsilon})/F \) is everywhere unramified if and only if \( n \equiv 1 \pmod{4} \).

2. The dyadic primes of \( F = \mathbb{Q}(\sqrt{m}) \) are unramified in the companion field \( E_c = \mathbb{F}(\sqrt{-\epsilon})/F \) if and only if \( n \equiv 3 \pmod{4} \).

PROOF: Since \( m \equiv 1 \pmod{4} \), \( E = \mathbb{Q}(\sqrt{m}, \sqrt{n}) \) is dyadically unramified if and only if \( n \equiv 1 \pmod{4} \). Thus the quadratic extension

\[ E = \mathbb{F}(\sqrt{\epsilon})/F = \mathbb{F}(\sqrt{n})/F \]

is everywhere unramified if and only if \( n \equiv 1 \pmod{4} \), proving (1). The dyadic primes of \( F = \mathbb{Q}(\sqrt{m}) \) are unramified in the companion field \( E_c = \mathbb{F}(\sqrt{-\epsilon}) \) if and only if they are ramified in \( E = \mathbb{F}(\sqrt{\epsilon}) = \mathbb{Q}(\sqrt{m}, \sqrt{n}) \) if and only if \( n \equiv 3 \pmod{4} \). []

REMARK: It is an interesting question to ask whether there is a reasonable way to directly identify the integer \( n \) with \( E = \mathbb{Q}(\sqrt{m}, \sqrt{\epsilon}) = \mathbb{Q}(\sqrt{m}, \sqrt{n}) \). We leave this as an open problem.

We now consider the Pathological Case: \( m \) is a product of distinct primes \( p_i \equiv 1 \pmod{4} \). Then surely no integer divisor \( n \) of \( m \) can be congruent to 3 modulo 4. Thus in the Pathological Case \( E = \mathbb{F}(\sqrt{\epsilon})/F \) is always an everywhere unramified quadratic extension. This proves

(III.4.3) PROPOSITION. If no prime \( p \equiv 3 \pmod{4} \) divides \( m \) and if \( N_{F/Q}(\epsilon) = 1 \) then \( E/Q \) is a dyadic unramified extension. Moreover, the quadratic extension \( E/F \) is everywhere unramified; hence \( E/F \) is a
quadratic piece of the Hilbert class field over $F$. []

For general $m > 0$, $m \equiv 1 \pmod{4}$, it is harder to decide which of $E$, $E_{\sigma}$ is dyadically unramified. We obtain a result in the Nice Case when $m = p_1 \cdot p_2$ is a product of two distinct primes both of which are congruent to 3 modulo 4. By Lemma (III.3.1), $N(\sigma) = +1$ is automatic.

(III.4.4) Proposition. Let $m = p_1 \cdot p_2$ where $p_1 \equiv p_2 \equiv 3 \pmod{4}$ are distinct rational primes. Then $E/\mathbb{Q}$ is dyadically ramified.

Proof. Since $m = p_1 \cdot p_2$ with $p_1 \equiv p_2 \equiv 3 \pmod{4}$ distinct rational primes, $F$ has odd class number (see [C-H] (21.1) p. 155) and cannot admit an unramified quadratic extension. So $E|F$ ramifies somewhere. But $E = F(\sqrt{\sigma})$ and $\sigma$ is totally positive, so $E|F$ is unramified at infinity and at every finite odd prime. Thus $E|F$ is dyadically ramified. []
CHAPTER IV. WEIL RECIPROCITY AND FUNDAMENTAL UNITS OF NORM -1

In the previous chapter we investigated whether 2 ramifies in

\[ E = \mathbb{Q}(\sqrt{m}, \sqrt{\epsilon}) \]

where \( \epsilon \) is a totally positive fundamental unit in the real quadratic field \( \mathbb{Q}(\sqrt{m}) \) with \( m \) chosen so that \( \epsilon \) has norm +1. In this chapter we investigate the same question when \( \epsilon \) has norm -1.

To be precise, let \( m > 1 \) be a square-free integer congruent to 1 modulo 4 and assume

\[ F = \mathbb{Q}(\sqrt{m}) \]

has a fundamental unit \( \epsilon \) with

\[ N_{F/\mathbb{Q}}(\epsilon) = -1. \]

(Then by Lemma (III.3.1) every prime dividing \( m \) is congruent to 1 modulo 4.) Now \( F \) is a real quadratic field so \( \epsilon \) and its conjugate are real, one positive and the other negative. Let \( \epsilon \) be positive. Then

\[ \sigma = \epsilon\sqrt{m} \]

is totally positive. And

\[ N_{F/\mathbb{Q}}(\sigma) = N_{F/\mathbb{Q}}(\epsilon) N_{F/\mathbb{Q}}(\sqrt{m}) = m \]

which is a square in \( F \) but not in \( \mathbb{Q} \).
It follows from Lemma (II.3.3) that

\[ E = (\sqrt{m}, \sqrt{\sigma}) = \mathbb{Q}(\sqrt{\sigma}) \]

is a cyclic extension of \( \mathbb{Q} \) of degree 4. Furthermore, since

\[ N_{E/\mathbb{Q}}(\sqrt{\sigma}) = m, \] the companion of \( E \)

\[ E_c = \mathbb{Q}(\sqrt{-\sigma}) \]

is also a cyclic extension of degree 4.

Now \( E \) is totally real while its companion \( E_c \) is totally complex, so the infinite prime of \( \mathbb{Q} \) is unramified in \( E \) and is ramified in \( E_c \). Clearly, the only finite rational primes \( p \) that can ramify in \( E \) are 2 (possibly) and the divisors of \( m \).

Since \( m \) is odd it is clear that

\[ \text{ord}_p(\pm \sqrt{m}) \equiv 0 \pmod{2} \]

for all dyadic prime ideals \( P \) in \( F \). So Corollary (II.4.1) applies and we can say

**(IV.1) THEOREM.** The rational prime 2 is unramified in exactly one of

\[ E = \mathbb{Q}(\sqrt{m}, \sqrt{\varepsilon \sqrt{m}}) \quad E_c = \mathbb{Q}(\sqrt{m}, \sqrt{-\varepsilon \sqrt{m}}). \]

The question is to decide which of the two extensions \( E/\mathbb{Q}, E_c/\mathbb{Q} \) is dyadically unramified. In his study of relative quadratic fields, Hilbert showed that \( E \) and \( E_c \) are contained in one of the cyclotomic fields

\[ \mathbb{Q}(\zeta_m) \text{ or } \mathbb{Q}(\zeta_{4m}). \]
It is clear that the rational prime 2 is ramified in the choice of $E, E_c$ that is contained in $\mathbb{Q}(\zeta_m)$; that is, the one of $E, E_c$ of conductor $m$. But this still doesn't tell us which field it is. Of course, we want to compute $\gamma_2^E$ and apply Theorem 2. However, rather than compute $\gamma_2^E$ directly, we compute $\gamma_q^E$ for $q$ odd and obtain $\gamma_2^E$ by Weil reciprocity (see Section (II.2.3)).

Write

$$\sigma = a + b\sqrt{m}$$

with $a, b$ in $\mathbb{Q}$ and $a \neq 0$. Then $\sqrt{\sigma}$ satisfies

$$x^4 - 2ax^2 + m$$

and by Lemma (II.3.2)

$$\langle E \rangle = \langle 1, m, a, am^2 \rangle = \langle 1, m, a, a \rangle.$$ 

Then

$$\gamma_q^E = (-2, m)_q \cdot c_q^E \cdot r_q(m)$$

where $c_q^E = (-1, -m)_q(a, -m^2)_q = 1$ since $m \equiv 1 \pmod{4}$, so $-1$ is a local square at $q$.

Therefore

$$\gamma_q^E = (-2, m)_q \cdot \gamma_2(m) = (2, m)_2 \cdot r_q(m).$$

Equivalently

$$\gamma_q^E = (2, q)_q \cdot r_q(m).$$

From Proposition (II.2.2), the root number

$$r_q(m) = (q, \frac{-m}{q})_q = (q, \frac{m}{q})_q.$$ 

Hence

$$\gamma_q^E = (2, q)_q \cdot (\frac{m}{q})_q = (\frac{2m}{q}, q)_q.$$
for all primes $q$ dividing $m$.

By Weil Reciprocity (see section II.2.3) we have

$$\gamma_2^{<E>} \cdot \prod_{q \text{ odd}} \gamma_q^{<E>} = \exp(\pi i \cdot \text{sgn}<E>/4).$$

Now $\gamma_q^{<E>} = 1$ when $q$ is odd and $q$ does not divide $m$, (see [C-Y] Lemma (4.3) p. 23). Moreover since $E/\mathbb{Q}$ is totally positive of degree 4, the signature of $<E>$ is 4. So

$$\gamma_2^{<E>} \cdot \prod_{q | m} \gamma_q^{<E>} = -1.$$

Now $\gamma_2^{<E>} = 1$ or $-1$ by Theorem 2 and Table 1 since $m \equiv 1$ or 5 mod 8. So 2 ramifies in $E$ if and only if $\gamma_2^{<E>} = 1$ by Theorem 2. So we conclude:

**Theorem 2.** The rational prime 2 ramifies in $E$ if and only if there are an odd number of primes $q$ dividing $m$ with

$$\left(\frac{2m}{q}, q\right) = -1.$$

This allows us to compute examples.

Suppose $q_1 \equiv q_2 \equiv 1 \pmod{4}$ are two distinct rational primes, with

$$\left(\frac{q_1}{q_2}\right) = \left(\frac{q_2}{q_1}\right) = -1.$$

Put $m = q_1 \cdot q_2$. Then necessarily a fundamental unit $\varepsilon$ in

$$F = \mathbb{Q}(\sqrt{q_1q_2})$$

has norm $-1$ (see [C-H] (19.9) Proposition, p. 147). Then in

$$E = \mathbb{Q}(\sqrt{q_1q_2}, \sqrt{\varepsilon/q_1q_2})$$
the rational prime 2 is ramified if and only if there are an odd number of prime divisors $q$ of $m = q_1 \cdot q_2$ with

$$\left(\frac{2m}{q}, q_1\right)_q = -1.$$ 

Taking $q = q_1$, we're looking at

$$\left(\frac{2q_2}{q_1}\right)_{q_1} = \left(\frac{2}{q_1}\right)_{q_1} \left(q_2, q_1\right)_{q_1} = -(2, q_1)_{q_1}$$

and this equals $-1$ if and only if

$$q_1 \equiv 1 \pmod{8}$$

since we already know $q_1 \equiv 1$ or $5 \pmod{8}$. This means that 2 ramifies in $E$ if exactly one of $q_1, q_2$ is congruent to $1 \pmod{8}$. This proves

(IV.3) THEOREM. Let $q_1$ and $q_2$ be distinct rational primes congruent to 1 modulo 4 and

$$\left(\frac{q_1}{q_2}\right) = \left(\frac{q_2}{q_1}\right) = -1$$

(a) If $q_1 \equiv q_2 \equiv 1 \pmod{8}$ or $q_1 \equiv q_2 \equiv 5 \pmod{8}$ then 2 is unramified in $E/Q$ and $E \subseteq Q(\zeta_m)$ with $m = q_1 q_2$.

(b) If $q_1 \equiv 1 \pmod{8}$ and $q_2 \equiv 5 \pmod{8}$ then 2 is ramified in $E/Q$ and is unramified in the companion $E_c/Q$. []

We note that in case (a) above, $E$ is actually contained in the maximal real subfield of $Q(\zeta_m)$. In case (b), the companion $E_c$ is contained in $Q(\zeta_m)$ but, being complex, $E_c$ is not contained in the maximal real subfield.
BIBLIOGRAPHY


VITA

Stella Roberson Ashford was born to Cleve M. and Lillie W. Roberson on February 22, 1942 in Richland Parish. She graduated from Rhymes High School in 1959. In 1963 she received the Bachelor of Science Degree from Southern University and in 1967 she received the Master of Arts Degree in Mathematics from Louisiana State University. At present, she is a candidate for the degree of Doctor of Philosophy in the Department of Mathematics of Louisiana State University.
DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Stella Roberson Ashford

Major Field: Mathematics/Algebraic Number Theory

Title of Dissertation: Dyadic Ramification in Quartic Number Fields

Approved:

Robert V. Perlis
Major Professor and Chairman

Dean of the Graduate School

EXAMINING COMMITTEE:

J. R. Davie

Raymond C. Miller

John A. Todd

Jurgen Hurrelbrink

L. Diane Miller

Date of Examination:

December 4, 1986