1

PM-1 3½" x 4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

PRECISIONSM RESOLUTION TARGETS

PIONEERS IN METHYLBLEND BLUE TESTING SINCE 1974

METRO

1080 COUNTY ROAD 1, BURNING WOOD, OH 44027 USA
TEL: 914 485 7800 FAX: 914 485 7801 TOLL FREE: 800 451 7800

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your title / Votre référence

Our title / Notre référence

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

Canada

**DIHEDRAL POLYNOMIAL CONGRUENCES
AND BINARY QUADRATIC FORMS:
A CLASS FIELD THEORY APPROACH**

by

Dunxue Liu, B.Sc., M.Sc.

**A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfilment of
the requirements for the degree of
Doctor of Philosophy**

**Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario**

© Copyright

June 1992

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa, Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Your file Votre référence

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-315-79857-2

Canada

The undersigned hereby recommend to
The Faculty of Graduate Studies and Research
acceptance of the thesis,
**DIHEDRAL POLYNOMIAL CONGRUENCES AND BINARY
QUADRATIC FORMS:
A CLASS FIELD THEORY APPROACH**

submitted by
Dunxue Liu, B.Sc., M.Sc.
in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Dr. John D. Dixon, Chair,
Department of Mathematics and Statistics

Dr. Kenneth S. Williams, Thesis Supervisor

Dr. Blair K. Spearman, External Examiner

Carleton University
June, 1992

Abstract

In this thesis the notion of a dihedral polynomial is introduced . It is shown that the splitting of a given dihedral polynomial with integral coefficients modulo a prime p is equivalent to p being represented by the form classes in a certain subgroup of a form class group whose discriminant depends on the given polynomial.

Acknowledgements

I would like to thank my supervisor Dr. Kenneth S. Williams for his invaluable guidance in writing this thesis and for constructive criticism of my manuscript.

I would like to take this opportunity to thank the Faculty of Graduate Studies and Research of Carleton University for a graduate scholarship and my supervisor Dr. Kenneth S. Williams for financial support provided from his NSERC Operating Grant.

Last, I wish to thank my wife Peirong and daughter Jessica for their love, patience and support.

Contents

Abstract	i
Acknowledement	ii
Notation	v
Introduction	vii
1 BASIC DEFINITIONS AND SOME PRELIMINARY RESULTS	1
1.1 Basic Definitions	1
1.2 Some Results from Algebraic Number Theory	5
1.3 Some Results from Class Field Theory	12
2 PROPERTIES OF DIHEDRAL POLYNOMIALS	17
2.1 Some Properties of Dihedral Groups	17
2.2 Some Properties of Dihedral Polynomials	21
2.3 Cyclic Dihedral Polynomials	31
2.4 Cubic Polynomials	40
2.5 Quartic Polynomials	41
2.6 Quintic Polynomials	50
3 NUMBER OF SOLUTIONS OF A DIHEDRAL POLYNOMIAL CON- GRUENCE (mod p)	73
3.1 Proof of Theorem 3.1.3	73
3.2 Discussion of the Integer f in Theorem 3.1.3	82
4 DETERMINATION OF THE CONDUCTOR $f(M/K)$	91
4.1 Proof of Theorem 4.1.3	91

4.2	Determination of the Discriminant of a Dihedral Polynomial $\rho(x)$ whose Degree is an Odd Prime	96
4.3	Proof of Theorem 4.3.5	102
4.4	Proof of Theorem 4.4.11	114
5	SOME APPLICATIONS AND EXAMPLES	123
5.1	Some Corollaries of Theorem 3.1.3	123
5.2	Evaluation of the Legendre Symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$	128
5.3	Some Numerical Examples	131
5.4	Representation of Primes by Principal Forms	134
	Bibliography	159

NOTATION

Z ... domain of rational integers
 Q ... field of rational numbers
 R ... field of real numbers
 C ... field of complex numbers
 Z_m ... cyclic group of order m
 D_m ... cyclic dihedral group of order $2m$ containing Z_m
 $\rho(x)$... dihedral polynomial
 K, L, M ... algebraic number fields
 $f(M/K)$... conductor of extension M/K
 $f_0(M/K)$... the finite part of $f(M/K)$
 $d(L/K)$... relative discriminant ideal of the field extension L/K
 d_L ... discriminant of L over Q
 $H(\Delta)$... form class group of classes of primitive integral binary quadratic forms of discriminant Δ
 (a, b, c) ... the binary quadratic form $ax^2 + bxy + cy^2$
 $[a, b, c]$... the class containing the form $ax^2 + bxy + cy^2$
 1_Δ ... the class containing the principal form of discriminant Δ
 $\left(\frac{M/K}{\cdot}\right)$... Artin symbol of extension M/K
 $\mathcal{O}_K$... ring of algebraic integers of K
 $\mathcal{P}, \mathcal{B}$... prime ideals
 $[L : K]$... degree of L over K
 $\text{Gal}(M/K)$... Galois group of M over K
 $N_{L/K}(\)$... norm of L over K
 $T_{L/K}(\)$... trace of L over K
 $\deg(\varphi)$... degree of the polynomial $\varphi(x)$
 $\text{disc}(\varphi)$... discriminant of the polynomial $\varphi(x)$
 $D(\mathcal{B}/\mathcal{P})$... decomposition group
 $E(\mathcal{B}/\mathcal{P})$... inertia group
 $e(\mathcal{B}/\mathcal{P})$... ramification index

$f(\mathcal{B}/\mathcal{P})$... inertial degree
 $V_m(\mathcal{B}/\mathcal{P})$...ramification group
 L_D ... decomposition field
 L_E ... inertia field
 P_k ... the set of all finite primes of k
 $\mathcal{S}_{L/k}$... the set of finite primes of k each of which splits completely in L
 $|$... divides
 $\parallel$... exactly divides
 $|r|$... absolute value of the real number r
 $|S|$... number of elements in the finite set S
 $o(\alpha)$... order of α
 $\left(\frac{n}{p}\right)$... Legendre-Kronecker symbol
 $\square$... indicates an integer is a perfect square
 $\gcd(a, b)$... the greatest common divisor of a and b
 $\text{lcm}(a, b)$... the least common multiple of a and b
 ϵ_f ... the fundamental unit of the order $\mathcal{O}_f$
 S_n ... symmetric group on n letters
 A_n ... alternating group on n letters
 diff ... different
 $F_f(K)$... the ring class field of conductor f in the quadratic field K
 $F_f^+(K)$... the strict ring class field of conductor f in the quadratic field K
 I_K ...group of all fractional $\mathcal{O}_K$ -ideals
 $I_K(f)$... certain subgroup of I_K (see pp.2-3)
 $P_{K,Z}(f)$...certain subgroup of $I_K(f)$ (see pp.2-3)
 $P_{K,1}(f)$...certain subgroup of $I_K(f)$ (see pp.2-3)
 K_M ... certain set of quadratic fields (see p.vii)
 $v_{\mathcal{P}}$... $\mathcal{P}$ -valuation
 G' ... commutator subgroup of the group G
 p^* ... denotes the number $(-1)^{\frac{p-1}{2}}p$ for an odd prime p

INTRODUCTION

We begin by defining what we will call a dihedral group.

Definition(dihedral group) Let G be a finite group. If G possesses an Abelian subgroup H of index 2 and there is an element $\tau \in G - H$ of order 2 such that

$$\tau\sigma\tau^{-1} = \sigma^{-1} \text{ for any } \sigma \in H, \quad (*)$$

then G is called the **dihedral group** generated by H and τ and we write $G = \langle H, \tau \rangle$.

We remark that the subgroup H and the element τ of $G - H$ in the above definition may not be uniquely determined by G . A particularly important dihedral group $G = \langle H, \tau \rangle$ is one for which H is a cyclic group.

Definition(cyclic dihedral group) If $G = \langle H, \tau \rangle$ is a dihedral group, we call G a **cyclic dihedral group** if H is a cyclic group, and we denote G by D_m , where m is the order of H .

The concept of a dihedral group leads naturally to the notion of a dihedral extension.

Definition(dihedral extension) Let M be a normal extension of the rational field Q . If $\text{Gal}(M/Q)$ is a (cyclic)dihedral group, then M is called a (cyclic)dihedral extension.

If M is a dihedral extension, M is a normal extension and

$$\text{Gal}(M/Q) = \langle H, \tau \rangle,$$

for some Abelian subgroup H of index 2 in $\text{Gal}(M/Q)$ and some element $\tau \in \text{Gal}(M/Q) - H$ satisfying $(*)$ above. By Galois theory M contains a quadratic field K uniquely determined by H , and τ induces a non-trivial automorphism on K . Thus we have

$$\text{Gal}(M/Q) = \langle \text{Gal}(M/K), \tau \rangle.$$

Since H is not in general uniquely determined by M , K is not in general uniquely determined by M . This leads us to define for each dihedral extension M , a set K_M as

follows:

Definition(set K_M) For M a dihedral extension we define the set K_M to be the set

$$K_M = \text{set of quadratic fields } K \subset M \text{ for which} \\ \text{Gal}(M/Q) = \langle \text{Gal}(M/K), \tau \rangle .$$

For example, $M = Q(\sqrt{2}, \sqrt{-2})$ is a dihedral extension and

$$K_M = \{Q(\sqrt{2}), Q(\sqrt{-2}), Q(\sqrt{-1})\}.$$

Now that we have the concept of a dihedral extension we are in a position to define what we mean by a dihedral polynomial.

Definition((cyclic)dihedral polynomial) A monic irreducible polynomial $\rho(x)$ in $Q[x]$ is called a (cyclic)dihedral polynomial if the splitting field M of $\rho(x)$ over Q (M is a normal extension of Q) is a dihedral extension.

The central theme of this thesis is the determination of the number of solutions $x \pmod{p}$ of the congruence

$$\rho(x) \equiv 0 \pmod{p}, \quad (0.1)$$

where $\rho(x)$ is a dihedral polynomial with integral coefficients and p is a prime not dividing the discriminant $\text{disc}(\rho)$ of $\rho(x)$.

Let $\rho(x)$ be a dihedral polynomial of degree d . Let M denote the splitting field of $\rho(x)$ over Q . In Lemma 2.2.3 we show that $[M : Q] = 2d$ or d . Thus dihedral polynomials fall naturally into two types.

Definition(dihedral polynomial of type 1) A dihedral polynomial $\rho(x)$ is said to be a dihedral polynomial of type 1 if $[M : Q] = 2\deg(\rho)$, where M denotes the splitting field of $\rho(x)$ over Q .

Definition(dihedral polynomial of type 2) A dihedral polynomial $\rho(x)$ is said to be a dihedral polynomial of type 2 if $[M : Q] = \deg(\rho)$, where M denotes the splitting field of $\rho(x)$ over Q .

It is shown in Lemma 2.2.5 that if $\rho(x)$ is a dihedral polynomial of type 1 then there is exactly one quadratic field K in K_M . This does not hold for a dihedral polynomial of type 2. For example, for the dihedral polynomial $\rho(x) = x^4 + 16$, the splitting field

of $\rho(x)$ is $M = Q(\sqrt{2}, \sqrt{-2})$, thus we have $[M : Q] = \deg(\rho)$ so that $\rho(x)$ is a dihedral polynomial of type 2. But we have $K_M = \{Q(\sqrt{2}), Q(\sqrt{-2}), Q(\sqrt{-1})\}$.

In Chapter 2 criteria are given to recognize when cubic, quartic and quintic polynomials are dihedral polynomials. An irreducible polynomial $\varphi(x) = x^3 + ax^2 + bx + c \in Q[x]$ is a dihedral polynomial of type 1 (necessarily cyclic) if and only if its discriminant $\text{disc}(\varphi)$ is not a perfect square. In this case the splitting field M of $\varphi(x)$ contains only one quadratic field $K = Q(\sqrt{\text{disc}(\varphi)})$. There are no cubic polynomials which are dihedral polynomials of type 2.

A quartic polynomial $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in Q[x]$ is a dihedral polynomial of type 1 (necessarily cyclic) if and only if its cubic resolvent $r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$ has exactly one root t in Q and both d' and $d'(b^2 - 4d')$ are not in Q^2 , where $b' = a^2 - 2b - 2t$ and $d' = (b+t)^2 - 4(t^2 + ac - 4d)$. If this is the case, then the splitting field M of $\varphi(x)$ contains only one quadratic field $K = Q(\sqrt{(b^2 - 4d')d'})$.

A quartic polynomial $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in Q[x]$ is a dihedral polynomial of type 2 (necessarily cyclic) if and only if its cubic resolvent $r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$ has three roots t_1, t_2 and t_3 in Q . If this is the case, letting M denote the splitting field of $\varphi(x)$, we have

$$K_M = \{K_1, K_2, K_3\},$$

where $K_i = Q(\sqrt{t_i^2 - 4d})$ or $Q(\sqrt{a^2 - 4(b - t_i)})$ for $i = 1, 2, 3$.

Criteria for an irreducible quintic polynomial to be a dihedral polynomial of type 1 can be found in Lemma 2.6.6. There are no quintic dihedral polynomials of type 2.

In Chapter 2 we prove the following results about the congruence (0.1) for a dihedral polynomial $\rho(x)$.

Theorem 2.2.17 *Let $\rho(x) \in Z[x]$ be a dihedral polynomial of type 1. Let $d = \deg(\rho)$. Let M be the splitting field of $\rho(x)$ over Q , and let K be the unique quadratic field in K_M (Lemma 2.2.5). Let $H = \text{Gal}(M/K)$ and let $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Let p be a prime not dividing $\text{disc}(\rho)$.*

(i) *If $\left(\frac{dK}{p}\right) = 1$, the congruence (0.1) has d solutions if and only if the congruence (0.1) has a solution.*

(ii) If $\left(\frac{d_K}{p}\right) = -1$, the congruence (0.1) has either 2^s or 0 solutions, where s denotes the 2-rank of H . More precisely, let $D = \langle h\tau \rangle$ be the decomposition group of p in M , where $h \in H$. Then we have the following:

(1) If h is a square in H , then the congruence (0.1) has exactly 2^s solutions.

(2) If h is not a square in H , then all the irreducible factors of $\rho(x) \pmod{p}$ are of degree 2, in particular, the congruence (0.1) has no solutions.

Theorem 2.2.19 Let $\rho(x) \in Z[x]$ be a dihedral polynomial of type 2. Let M be the splitting field of $\rho(x)$ over Q . Let K be a quadratic subfield of M in K_M . Let p be a prime not dividing $\text{disc}(\rho)$.

(i) If $\left(\frac{d_K}{p}\right) = 1$, then $\rho(x) \pmod{p}$ splits completely if and only if $\rho(x) \pmod{p}$ has a linear factor.

(ii) If $\left(\frac{d_K}{p}\right) = -1$, then $\rho(x) \pmod{p}$ is a product of quadratic irreducible factors.

In Chapter 3 we are concerned with giving a necessary and sufficient condition for the congruence (0.1) to have d solutions when $\left(\frac{d_K}{p}\right) = 1$ (part (i) of Theorems 2.2.17 and 2.2.19). Let $H(\Delta)$ denote the form class group of classes of primitive, integral binary quadratic forms $ax^2 + bxy + cy^2$ of nonsquare discriminant $\Delta = b^2 - 4ac$ (defined in Chapter 1). Let $F_f^+(K)$ denote the strict ring class field of the order of conductor f in the quadratic field K . The first main result of this thesis is the following theorem, which is proved in Chapter 3.

Theorem 3.1.3

(i) Let $\rho(x) \in Z[x]$ be a dihedral polynomial of degree d , and let M be the splitting field of $\rho(x)$ over Q . Let $K \in K_M$ and let f be any positive integer such that $M \subset F_f^+(K)$, the strict ring class field of the order of conductor f in K . Then there is a unique subgroup $J = J(\rho, K, f)$ of $H(d_K f^2)$ such that

$$H(d_K f^2)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$\iff p$ splits completely in M

$\iff p$ is represented by one of the classes in J .

(ii) Conversely, suppose $\rho(x)$ is a monic irreducible polynomial of degree d with integral coefficients. If there exists a subgroup H of the form class group $H(\Delta)$ for some nonsquare integer $\Delta \equiv 0, 1 \pmod{4}$ having the property: for every prime p not dividing $\text{disc}(\rho)$,

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$\iff p$ is represented by one of the classes in H ,

then $\rho(x)$ is a dihedral polynomial.

We remark that Theorem 3.1.3 generalizes results of Spearman and Williams [30], who treated the case when $d = 3$, and of Buell, Leonard and Williams [8], who treated the special case when $\rho(x) = x^4 - 2Tx^2 - 1$ and $T + U\sqrt{m}$ is the fundamental unit of norm -1 of the quadratic field $Q(\sqrt{m})$, where m is a squarefree positive integer.

In order to be able to apply Theorem 3.1.3 one must know a positive integer f divisible by the finite part $f_0(M/K)$ of the conductor $f(M/K)$ of the extension M/K . In this direction we prove two theorems (Theorems 4.1.3 and 4.4.11 below) which enable us to determine such an integer f for use in Theorem 3.1.3 when d is an odd prime (Theorem 4.1.3) and when $d = 4$ (Theorem 4.4.11).

Theorem 4.1.3 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_q = \langle \sigma, \tau \rangle$, for which $\sigma^q = \tau^2 = (\sigma\tau)^2 = 1$, where q is an odd prime. Let K be the quadratic field fixed by σ and let L be the fixed field of τ . Set*

$$S = \{p : p(\text{prime}) \neq q, p \mid d_L, p \equiv \left(\frac{d_K}{p}\right) \pmod{q}\},$$

and let f' denote the product of the primes in S . Then $f_0(M/K) = f_q f'$, where f_q is given as follows:

when $3 \neq q \equiv 3 \pmod{4}$,

$$f_q = \begin{cases} 1, & \text{if } q \text{ is unramified in } M/K, \\ q, & \text{if } q \text{ is totally ramified in } M, \\ q^2, & \text{if } q \text{ is unramified in } K \text{ but is ramified in } M/K, \end{cases}$$

when $q = 3$,

$$f_3 = \begin{cases} 1, & \text{if } 3 \text{ is unramified in } M/K, \\ 3 \text{ or } 3^2, & \text{if } 3 \text{ is totally ramified in } M, \\ 3^2, & \text{if } 3 \text{ is unramified in } K \text{ but is ramified in } M/K, \end{cases}$$

when $q \equiv 1 \pmod{4}$,

$$f_q = \begin{cases} 1, & \text{if } q \text{ is unramified in } M/K, \\ q \text{ or } q^{3/2}, & \text{if } q \text{ is totally ramified in } M, \\ q^2, & \text{if } q \text{ is unramified in } K \text{ but is ramified in } M/K. \end{cases}$$

Theorem 4.4.11 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_4 = \langle \sigma, \tau \rangle$ where $\sigma^4 = \tau^2 = (\sigma\tau)^2 = 1$. Let K be the fixed field of σ . Let F be the fixed field of σ^2 . Let L be a subfield of M of degree 4 over Q different from F . Let k be the unique quadratic subfield of L . Then $f_0(M/K)$ is a positive integer which satisfies*

$$d_L = d_K d_k f_0(M/K)^2.$$

Another result of this thesis is the determination of the finite part of the conductor of a biquadratic field over a quadratic subfield (see Theorem 4.3.5 below). Using this result we determine the genus field of any ring class field (see definition in Chapter 1): reproving and extending results of Hasse [18] and Halter-Koch [17].

Theorem 4.3.5 *Let F be a biquadratic field and let K be a quadratic subfield of F . Then $f_0(F/K)$ is an integer which is given by*

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{\frac{1}{2}},$$

where k and k' are the other two quadratic subfields of F .

Theorem 4.3.12 (Halter-Koch) *Let $K = Q(\sqrt{n})$ be a quadratic field, where n is a squarefree integer. Let f be a positive integer. Suppose that $p_1, p_2, \dots, p_r$ are the distinct odd primes dividing nf . Set $p_i^* = (-1)^{(p_i-1)/2} p_i$. Then the genus field $K^+(f)$ of the*

strict ring class field $F_f^+(K)$ is given as follows: when $n \equiv 1 \pmod{4}$,

$$K^+(f) = \begin{cases} Q(\sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \parallel f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^3 \mid f, \end{cases}$$

when $n \equiv 3 \pmod{4}$,

$$K^+(f) = \begin{cases} Q(\sqrt{-1}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \mid f, \end{cases}$$

when $n \equiv 2 \pmod{8}$,

$$K^+(f) = \begin{cases} Q(\sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \mid f, \end{cases}$$

and when $n \equiv 6 \pmod{8}$,

$$K^+(f) = \begin{cases} Q(\sqrt{-2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \mid f, \end{cases}$$

Theorem 4.3.13 Let $n > 1$ be a squarefree integer. Let $K = Q(\sqrt{n})$. Let f be a positive integer. Suppose that $p_1, p_2, \dots, p_r$ are the distinct odd primes of the form $4k+1$ dividing nf , and suppose that $q_1, q_2, \dots, q_s$ are the distinct odd primes of the form $4k+3$ dividing nf . Then the genus field $K(f)$ of $F_f(K)$ is given as follows:

when $n \equiv 1 \pmod{4}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \parallel f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^3 \mid f, \end{cases}$$

when $n \equiv 3 \pmod{4}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \mid f, \end{cases}$$

when $n \equiv 2 \pmod{8}$,

$$K(f) = \begin{cases} Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2 \mid f, \end{cases}$$

and when $n \equiv 6 \pmod{8}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2 \mid f. \end{cases}$$

In §5.1 we begin by giving a number of corollaries to Theorem 3.1.3 . Then, in §5.2, we use what we have developed in earlier chapters to evaluate the Legendre symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$. In §5.3 we give some numerical examples to illustrate Theorem 3.1.3. Finally, in §5.4 we consider the problem of the representation of primes by certain principal forms.

We conclude by noting that the main new results of this thesis are Theorems 2.2.17, 2.6.6, 2.6.9, 2.6.11, 3.1.3, 4.1.3, 4.2.6, 4.3.13, 4.4.11, 5.2.1.

Chapter 1

BASIC DEFINITIONS AND SOME PRELIMINARY RESULTS

We begin by recalling some basic definitions from algebraic number theory and class field theory. Then we give a collection of known facts from algebraic number theory and from class field theory that will be needed in the proofs of our main theorems. In those cases where the results are not stated explicitly in the literature we give proofs, for the remaining results we supply references.

1.1 Basic Definitions

We use $\deg(f)$ to denote the degree of the polynomial $f(x)$ and write $\text{disc}(f)$ for the discriminant of $f(x)$.

For K an algebraic number field, we use $\mathcal{O}_K$ to denote the ring of algebraic integers of K and we use d_K to denote the discriminant of K over $\mathbb{Q}$. If $K \subset L$ is a finite extension, $[L : K]$ denotes the degree of L over K , $d(L/K)$ denotes the relative discriminant ideal of the field extension L/K , $N_{L/K}(\)$ denotes the norm of L over K and $T_{L/K}(\)$ denotes the trace of L over K . Further if $K \subset L$ is a normal extension, we use $\text{Gal}(L/K)$ to denote the Galois group of L over K , $f(L/K)$ to denote the conductor of the extension L/K , $f_0(L/K)$ to denote the finite part of $f(L/K)$, and $\left(\frac{L/K}{\cdot}\right)$ to denote the Artin symbol of L/K .

For $K \subset L$ a normal extension, let $\mathcal{B}$ be a prime ideal of $\mathcal{O}_L$. Let $\mathcal{P} = \mathcal{B} \cap \mathcal{O}_K$. Then the decomposition group $D(\mathcal{B}/\mathcal{P})$ and the inertial group $I(\mathcal{B}/\mathcal{P})$ of $\mathcal{B}$ over $\mathcal{P}$

are defined by

$$D(\mathcal{B}/\mathcal{P}) = \{\sigma \in \text{Gal}(L/K) : \sigma(\mathcal{B}) = \mathcal{B}\},$$

$$E(\mathcal{B}/\mathcal{P}) = \{\sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{B}} \forall \alpha \in \mathcal{O}_L\}.$$

The ramification groups $V_m(\mathcal{B}/\mathcal{P})$ for $m = 0, 1, 2, \dots$ are defined by:

$$V_m(\mathcal{B}/\mathcal{P}) = \{\sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{B}^{m+1}} \forall \alpha \in \mathcal{O}_L\}.$$

Thus $V_0(\mathcal{B}/\mathcal{P}) = E(\mathcal{B}/\mathcal{P})$ and the $V_m(\mathcal{B}/\mathcal{P})$ ($m = 0, 1, 2, \dots$) form a descending chain of subgroups of $E(\mathcal{B}/\mathcal{P})$.

For $K \subset L$ a finite extension, let $\mathcal{P}$ be a prime of $\mathcal{O}_K$ and let $\mathcal{B}$ be a prime of $\mathcal{O}_L$ containing $\mathcal{P}$. We know that $\mathcal{P} = \mathcal{B} \cap \mathcal{O}_K$, so the inclusion $\mathcal{O}_K \subset \mathcal{O}_L$ induces an embedding $\mathcal{O}_K/\mathcal{P} \rightarrow \mathcal{O}_L/\mathcal{B}$. Hence $\mathcal{O}_L/\mathcal{B}$ is an extension of finite degree over $\mathcal{O}_K/\mathcal{P}$. Let $f(\mathcal{B}/\mathcal{P})$ denote the degree of this extension. $f(\mathcal{B}/\mathcal{P})$ is called the inertial degree of $\mathcal{B}$ over $\mathcal{P}$. We know that $\mathcal{B} \mid \mathcal{P}\mathcal{O}_L$. If $\mathcal{B}^e$ is the exact power of $\mathcal{B}$ dividing $\mathcal{P}\mathcal{O}_L$, then e is called the ramification index of $\mathcal{B}$ over $\mathcal{P}$ and is denoted by $e(\mathcal{B}/\mathcal{P})$.

For K an algebraic number field of finite degree over $\mathbb{Q}$, the prime ideals of $\mathcal{O}_K$ are called the finite primes of $\mathcal{O}_K$. A real infinite prime of K is an embedding $\mu : K \rightarrow \mathbb{R}$. A non-real(complex) infinite prime of K is a pair of complex conjugate embeddings $\mu, \bar{\mu} : K \rightarrow \mathbb{C}$ with $\mu \neq \bar{\mu}$. An infinite prime μ of K ramifies in an extension L of K provided that μ is real but it has an extension to L which is complex. Let $\mathcal{M}_0$ denote an integral ideal of K and let $\mathcal{M}_\infty$ denote a formal squarefree product (possibly empty) of infinite primes. Then $\mathcal{M} = \mathcal{M}_0\mathcal{M}_\infty$ is called a modulus in K . Given a modulus $\mathcal{M} = \mathcal{M}_0\mathcal{M}_\infty$ in K , we define

$$I_K = \text{group of all fractional } \mathcal{O}_K\text{-ideals,}$$

$$I_K(\mathcal{M}) = \text{group of all fractional } \mathcal{O}_K\text{-ideals which are relatively prime to } \mathcal{M}_0,$$

$$P_{K,1}(\mathcal{M}) = \text{subgroup of } I_K(\mathcal{M}) \text{ generated by principal ideals } \alpha\mathcal{O}_K, \text{ where } \alpha \in \mathcal{O}_K \text{ satisfies } \alpha \equiv 1 \pmod{\mathcal{M}_0} \text{ and } \sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma \mid \mathcal{M}_\infty,$$

$$P_{K,z}(\mathcal{M}) = \text{subgroup of } I_K(\mathcal{M}) \text{ generated by principal ideals } \alpha\mathcal{O}_K \text{ with } \alpha \in \mathcal{O}_K \text{ and } \alpha \equiv a \pmod{\mathcal{M}_0} \text{ for some integer } a \text{ coprime with } \mathcal{M}_0,$$

$$P_{K,z}^+(\mathcal{M}) = \text{subgroup of } I_K(\mathcal{M}) \text{ generated by principal ideals } \alpha\mathcal{O}_K \text{ with } \alpha \in \mathcal{O}_K \text{ and } \alpha \equiv a \pmod{\mathcal{M}}, \text{ for some integer } a \text{ coprime with } \mathcal{M}_0 \text{ and } N_{K/\mathbb{Q}}(\alpha) > 0.$$

If $\mathcal{M} = \alpha\mathcal{O}_K$ we write $I_K(\alpha)$ for $I_K(\alpha\mathcal{O}_K)$, $P_{K,Z}(\alpha)$ for $P_{K,Z}(\alpha\mathcal{O}_K)$, and $P_{K,1}(\alpha)$ for $P_{K,1}(\alpha\mathcal{O}_K)$. If $\mathcal{M}$ is divisible by all primes of K which ramify in M and $\mathcal{P}$ is a prime ideal of $\mathcal{O}_K$ not dividing $\mathcal{M}$, the Artin symbol $\left(\frac{M/K}{\mathcal{P}}\right) \in \text{Gal}(M/K)$ is defined, and can be extended by multiplicativity to a homomorphism

$$\phi_{M/K,\mathcal{M}} : I_K(\mathcal{M}) \longrightarrow \text{Gal}(M/K),$$

which is called the Artin map for the extension $K \subset M$ and the ideal $\mathcal{M}$. A subgroup $H \subset I_K(\mathcal{M})$ is called a congruence subgroup for $\mathcal{M}$ if it satisfies

$$P_{K,1}(\mathcal{M})H \subset I_K(\mathcal{M}).$$

Now let K be a quadratic field. Let f be a positive integer. A $\mathbb{Z}$ -module in $\mathcal{O}_K$ of the form

$$\mathcal{O}_f = [1, f\omega_K] = \{a + bf\omega_K : a, b \in \mathbb{Z}\}, \text{ where } \omega_K = \frac{d_K + \sqrt{d_K}}{2},$$

is called an order in K and f is called the conductor of the order. An ideal I of the order $\mathcal{O}_f$ is called a proper ideal provided

$$\mathcal{O}_f = \{\alpha \in K : \alpha I \subset I\}.$$

We can also extend this terminology to fractional ideals. A fractional ideal of $\mathcal{O}_f$ is a subset of K which is a nonzero finitely generated $\mathcal{O}_f$ -module. One can show that every fractional ideal is of the form αI , where $\alpha \in K^*$ and I is an $\mathcal{O}_f$ -ideal. Then a fractional $\mathcal{O}_f$ -ideal J is proper provided that

$$\mathcal{O}_f = \{\alpha \in K : \alpha J \subset J\}.$$

Given an order $\mathcal{O}$ of conductor f in an arbitrary quadratic field K , we let

$$\begin{aligned} I(\mathcal{O}) &= \text{group of proper fractional } \mathcal{O}\text{-ideals,} \\ P(\mathcal{O}) &= \text{group generated by principal } \mathcal{O}\text{-ideals.} \end{aligned}$$

The quotient group

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

is called the ideal class group of the order $\mathcal{O}$. Let

$$P^+(\mathcal{O}) = \text{group generated by principal } \mathcal{O}\text{-ideals } \alpha\mathcal{O} \text{ with } N_{K/Q}(\alpha) > 0,$$

and the quotient group

$$C^+(\mathcal{O}) = I(\mathcal{O})/P^+(\mathcal{O})$$

is called the strict ideal class group of the order $\mathcal{O}$. We say that a nonzero $\mathcal{O}$ -ideal $\mathcal{P}$ is prime to f provided that $\gcd(N(\mathcal{P}), f) = 1$. Let $I(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O})$ generated by all $\mathcal{O}$ -ideals prime to f , let $P(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O}, f)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}$, and let $P^+(\mathcal{O}, f)$ denote the subgroup of $I(\mathcal{O}, f)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}$ and $N_{K/Q}(\alpha) > 0$.

When K is a real quadratic field we denote the fundamental unit (> 1) of K by ϵ_K . Let $\epsilon_K^{u(f)}$ ($u(f) > 0$) denote the least power of ϵ_K which belongs to $\mathcal{O}_f$. Setting $\epsilon_f = \epsilon_K^{u(f)}$, we call ϵ_f the fundamental unit of the order $\mathcal{O}_f$.

We consider binary quadratic forms with integral coefficients in two variables

$$f(x, y) = ax^2 + bxy + cy^2$$

of discriminant $\Delta = b^2 - 4ac \neq 0$. We write the form more simply as $f = (a, b, c)$. Note that $\Delta \equiv 0$ or $1 \pmod{4}$ and that $\Delta \equiv b \pmod{2}$. A quadratic form $f = (a, b, c)$ is called primitive if $\gcd(a, b, c) = 1$. Next, we say that two forms $f(x, y)$ and $g(x, y)$ are equivalent if there are integers p, q, r and s with $ps - qr = 1$ such that

$$f(x, y) = g(px + qy, rx + sy).$$

It is clear that the equivalence of forms is an equivalence relation. We let $H(\Delta)$ denote the form class group of classes of primitive, integral binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant Δ under Gaussian composition. The identity of the group $H(\Delta)$ is the class 1_Δ of the principal form of discriminant Δ , namely,

$$\begin{cases} (1, 0, -\Delta/4), & \text{if } \Delta \equiv 0 \pmod{4} \\ (1, 1, (1 - \Delta)/4), & \text{if } \Delta \equiv 1 \pmod{4} \end{cases}.$$

1_Δ is called the principal class of discriminant Δ .

1.2 Some Results from Algebraic Number Theory

Lemma 1.2.1 *Let K be an algebraic number field of finite degree over Q , say $K = Q(\alpha)$, where $\alpha \in \mathcal{O}_K$. Let g be the minimal monic polynomial of α over Q . Suppose p is a rational prime such that $p \nmid \text{disc}(g)$ and that the decomposition of g as a product of irreducible polynomials $(\text{mod } p)$ is*

$$g = g_1 g_2 \dots g_r \pmod{p},$$

where the g_i are distinct monic irreducible polynomials $(\text{mod } p)$. Then the decomposition of $p\mathcal{O}_K$ into prime ideals is given by

$$p\mathcal{O}_K = \mathcal{B}_1 \mathcal{B}_2 \dots \mathcal{B}_r,$$

where $\mathcal{B}_i = (p, g_i(\alpha))$ is the ideal of $\mathcal{O}_K$ generated by p and $g_i(\alpha)$. Also

$$f(\mathcal{B}_i/p) = \deg(g_i), \quad i = 1, \dots, r.$$

Proof: See [[29], Theorem 27, p.79]. ■

Lemma 1.2.2 *Let K be a number field, and let L and M be two finite extensions of K . Fix a prime $\mathcal{P}$ of K . If $\mathcal{P}$ splits completely in both L and M , then $\mathcal{P}$ splits completely in the composite field LM .*

Proof: See [[29], Theorem 31, p. 107]. ■

Lemma 1.2.3 *Let $\varphi(x)$ be a monic irreducible polynomial with integral coefficients. Let p be a prime not dividing $\text{disc}(\varphi)$. Then $\varphi(x) \pmod{p}$ splits completely if and only if p splits completely in M , the splitting field of $\varphi(x)$ over Q .*

Proof: Suppose that p splits completely in M . Let α be a root of $\varphi(x)$. Then p splits completely in $Q(\alpha)$. Now appealing to Lemma 1.2.1, $\varphi(x)$ splits into linear factors $(\text{mod } p)$.

Conversely, suppose that $\varphi(x)$ splits completely $(\text{mod } p)$. Then, by Lemma 1.2.1, p splits completely in every $Q(\alpha)$, where α is a root of $\varphi(x)$. Note that M is the composite field of these $Q(\alpha)$'s. Hence, by Lemma 1.2.2, p splits completely in M . ■

Lemma 1.2.4 *Let K be a number field and let L be an extension of K with $[L : K] = n$. Let $\mathcal{P}$ be a prime of $\mathcal{O}_K$ and let $\mathcal{B}_1, \dots, \mathcal{B}_r$ be all the primes of $\mathcal{O}_L$ containing $\mathcal{P}$. Then*

$$\sum_{i=1}^r e(\mathcal{B}/\mathcal{P})f(\mathcal{B}/\mathcal{P}) = n.$$

Proof: See [[29], Theorem 21, p.65].

Lemma 1.2.5 *Let K be a number field and let L be a finite normal extension of K . Let $\mathcal{P}$ be a prime of $\mathcal{O}_K$, and let $\mathcal{B}$ be a prime of $\mathcal{O}_L$ containing $\mathcal{P}$. Set $\tilde{G} = \text{Gal}((\mathcal{O}_L/\mathcal{B})/(\mathcal{O}_K/\mathcal{P}))$. Then*

- (i) $D(\mathcal{B}/\mathcal{P})/E(\mathcal{B}/\mathcal{P}) \simeq \tilde{G}$.
- (ii) $|E(\mathcal{B}/\mathcal{P})| = e(\mathcal{B}/\mathcal{P})$.
- (iii) $|D(\mathcal{B}/\mathcal{P})| = e(\mathcal{B}/\mathcal{P})f(\mathcal{B}/\mathcal{P})$.

Proof: See [[11], Proposition 5.10, p.102]. ■

Lemma 1.2.6 *Let K be a number field and let L be a finite extension of K . Let $\mathcal{P}$ be a prime of $\mathcal{O}_K$. If $\mathcal{P}$ remains prime in L , then $\text{Gal}(L/K)$ is cyclic.*

Proof: Suppose that $\mathcal{P}$ remains prime in L . Then $\mathcal{P}\mathcal{O}_L = \mathcal{B}$ is a prime of L and

$$e(\mathcal{B}/\mathcal{P}) = 1, \quad f(\mathcal{B}/\mathcal{P}) = [L : K] = |\text{Gal}(L/K)|.$$

By (ii) and (iii) of Lemma 1.2.5, we have

$$E(\mathcal{B}/\mathcal{P}) = \{1\}, \quad D(\mathcal{B}/\mathcal{P}) = \text{Gal}(L/K).$$

Then by (i) of Lemma 1.2.5 we see that

$$\text{Gal}(L/K) \simeq \text{Gal}(L/K)/\{1\} = D(\mathcal{B}/\mathcal{P})/E(\mathcal{B}/\mathcal{P}) \simeq \tilde{G}.$$

Now note that $\tilde{G}$ is cyclic as $\mathcal{O}_L/\mathcal{B}$ is a finite field, so that $\text{Gal}(L/K)$ is cyclic. ■

Lemma 1.2.7 *Let K be a number field and let L be a finite Abelian extension of K . Let $\mathcal{P}$ be a prime ideal of K . Then $\mathcal{P}$ splits completely in L if and only if the Artin symbol $\left(\frac{L/K}{\mathcal{P}}\right) = 1$.*

Proof: See [[11], Corollary 5.21, p.107]. ■

Lemma 1.2.8 *Let $K \subset L \subset M$ be a tower of three algebraic number fields. Then*

$$d(M/K) = N_{L/K}(d(M/L))d(L/K)^{[M:L]}.$$

Proof: See [[28], Corollary 2.4, p.82]. ■

Theorem 1.2.9 (Conductor-Discriminant Theorem) *Suppose that K is a number field and $K \subset M$ is a finite Abelian extension. Let X be the character group of $G = \text{Gal}(M/K)$. Each $\chi \in X$ determines a extension K_χ of K with $\text{Gal}(K_\chi/K) \simeq \langle \chi \rangle$. As the extension K_χ/K is Abelian, it possesses a conductor $f(K_\chi/K)$. The finite part $f_0(K_\chi/K)$ of the conductor $f(K_\chi/K)$ is denoted by f_χ . Then*

$$\begin{aligned} d(M/K) &= \prod_{\chi \in X} f_\chi, \\ f_0(M/K) &= \text{lcm}_{\chi \in X} f_\chi. \end{aligned}$$

Proof: See [[9], Theorem 17.27, p.219]. ■

Lemma 1.2.10 *Suppose that K is a number field and $K \subset M$ is a finite Abelian extension. Let X be the character group of $G = \text{Gal}(M/K)$. Then there is a bijection between the set of subfields $\cup M$ containing K and the set of subgroups of X .*

Proof: See [[32], (1) and (2), p.23]. ■

Lemma 1.2.11 *Suppose that K is a number field and that $K \subset M$ is a finite cyclic extension with character group $X = \langle \chi \rangle$. Then*

$$d(M/K) = \prod_{r|n} (f_0(M_r/K))^{\varphi(r)},$$

where $n = [M : K]$, M_r is the unique subextension of M with $[M_r : K] = r$, φ denotes Euler's phi-function, and r runs through all the divisors of n .

Proof: Since X is cyclic, for each $r | n$ there is a unique subgroup X_r of order r . Then by Lemma 1.2.10, X_r determines a unique subextension M_r with $\text{Gal}(M_r/K) \simeq$

X_r .

Now it is clear that

$$f_0(X_r/K) = f_{\chi'}, \text{ for any } \chi' \text{ with } X_r = \langle \chi' \rangle.$$

It is well-known that there are $\varphi(r)$ such χ' . Thus Theorem 1.2.9 gives

$$d(M/K) = \prod_{\chi \in X} f_{\chi} = \prod_{r|n} (f_0(M_r/K))^{\varphi(r)}. \quad \blacksquare$$

Lemma 1.2.12 *Suppose that K is a number field and $K \subset M$ is a finite cyclic extension of prime degree p . Then*

$$d(M/K) = f_0(M/K)^{p-1}.$$

Proof: This is an immediate corollary of Lemma 1.2.11 (or see [9], Corollary 17.29). $\blacksquare$

Lemma 1.2.13 *Suppose that K is a number field and $K \subset M$ is a finite normal extension with $\text{Gal}(M/K) = D_2$. Let K_1/K , K_2/K and K_3/K be the three quadratic subextensions of M . Then*

$$d(M/K) = d(K_1/K)d(K_2/K)d(K_3/K).$$

Proof: Since the character group X of the extension M/K is isomorphic to $\text{Gal}(M/K) = D_2$, we have that

$$X = \{1, \chi_1, \chi_2, \chi_3\}, \text{ and } d(K_i/K) = f_{\chi_i} \text{ for } i = 1, 2, 3.$$

Thus by Theorem 1.2.9 we have

$$d(M/K) = \prod_{i=1}^3 f_{\chi_i} = d(K_1/K)d(K_2/K)d(K_3/K). \quad \blacksquare$$

Lemma 1.2.14 *Suppose that K is a number field and $K \subset M$ is a finite normal extension with $\text{Gal}(M/K) = Z_4$. Let F be the unique quadratic subfield of M . Then*

$$d(M/K) = f_0(M/K)^2 f_0(F/K).$$

Proof: Since the character group X of the extension M/K is isomorphic to $\text{Gal}(M/K) = Z_4$, we have that

$$X = \{1, \chi, \chi^2, \chi^3\}.$$

Thus by Theorem 1.2.9 we have

$$d(M/K) = \prod_{i=1}^3 f_{\chi_i} = f_0(M/K)^2 f_0(F/K). \quad \blacksquare$$

Before continuing we introduce some notation. Let K and L be number fields with L a normal extension of K . Let $G = \text{Gal}(L/K)$. Let H be any subgroup of G . We denote the fixed field of H by L_H . Let $\mathcal{P}$ be a prime of K and let $\mathcal{B}$ be a prime of L containing $\mathcal{P}$. We write $\mathcal{B}_H$ for $\mathcal{B} \cap L_H$.

Lemma 1.2.15 *Let K be a number field and let L be a finite extension of K . Let $\mathcal{P}$ be a prime of $\mathcal{O}_K$ and let $\mathcal{B}$ be a prime of $\mathcal{O}_L$ containing $\mathcal{P}$. Set*

$$D = D(\mathcal{B}/\mathcal{P}), \quad E = E(\mathcal{B}/\mathcal{P}).$$

Then we have the following table of ramification indices and inertial degrees:

<u>field degrees</u>			<u>ramification indices</u>	<u>inertial degrees</u>
	L	$\mathcal{B}$		
e	$ $	$ $	e	1
	L_E	$\mathcal{B}_E$		
f	$ $	$ $	1	f
	L_D	$\mathcal{B}_D$		
r	$ $	$ $	1	1
	K	$\mathcal{P}$		

where $e = e(\mathcal{B}/\mathcal{P})$, $f = f(\mathcal{B}/\mathcal{P})$ and $r = [L : K]/(ef)$. In particular, if D is a normal subgroup of G , then $\mathcal{P}$ splits into r distinct primes in L_D (splits completely in L_D). If E is also normal in G , then each of these r distinct primes remains prime in L_E . Further, each one becomes an efh power in L .

Proof: See [[29], Theorem 28, p.100 and Corollary, p.102]. ■

Lemma 1.2.16 *Let M be a dihedral extension of Q , and let K be a quadratic field in K_M . Let p be a prime which is not ramified in M and suppose that*

$$\left(\frac{d_K}{p}\right) = -1.$$

Then $p\mathcal{O}_K$ splits completely in M .

Proof: Suppose that $\mathcal{B}$ is a prime of M containing p . Since $\left(\frac{d_K}{p}\right) = -1$, $p\mathcal{O}_K$ is a prime of K . To prove the lemma we need only show that $D = D(\mathcal{B}/p\mathcal{O}_K) = 1$.

First we note that $K \subset M$ is an Abelian extension. By Lemma 1.2.15, we have

(i) $\mathcal{B}_D$ remains prime in M and (ii) $p\mathcal{O}_K$ splits completely in M_D .

Thus $p\mathcal{O}_K$ splits into $r = [M_D : K]$ primes in M_D . Consequently, pZ splits into r primes in M_D as pZ remains prime in K .

Now consider the extension $Q \subset M_D$. Let L be the decomposition field of $\mathcal{B}_D$ over p . Note that pZ decomposes into r primes in M_D , by Lemma 1.2.15 we have $[L : Q] = r$ and $\mathcal{B}_D \cap L$ remains prime in M_D . Together with (i) we see that $\mathcal{B}_D \cap L$ remains prime in M . Then by Lemma 1.2.6, $\text{Gal}(M/L)$ is a cyclic group containing D as $L \subset M_D$. Note that as $\text{Gal}(M/Q)$ is generated by H and τ , we have

$$\text{Gal}(M/L) = \langle \sigma \rangle \text{ or } \langle \sigma\tau \rangle \text{ for some } \sigma \in H.$$

Now if $\text{Gal}(M/L) = \langle \sigma \rangle$, then $\text{Gal}(M/L) = \langle \sigma \rangle \subset H = \text{Gal}(M/K)$ as $\sigma \in H$. By Galois theory, $K \subset L$, which implies that p splits in K . This a contradiction as $\left(\frac{d_K}{p}\right) = -1$. Thus we must have $\text{Gal}(M/L) = \langle \sigma\tau \rangle$. Further, as $[M_D : L] = 2$ and $(\sigma\tau)^2 = \sigma(\tau\sigma\tau) = \sigma\sigma^{-1} = 1$, we have $D = \langle (\sigma\tau)^2 \rangle = \{1\}$. Finally, by Galois theory we have $M_D = M_{\{1\}} = M$. ■

Lemma 1.2.17 *Let Δ be an integer $\equiv 0, 1 \pmod{4}$ which is not a perfect square. Let $K = Q(\sqrt{\Delta})$. Then*

$$\Delta = d_K g^2, \text{ for some positive integer } g.$$

Proof: Let $\Delta = Dm^2$, where $D(\neq 1)$ is a squarefree integer and m is a positive integer. As $\Delta \equiv 0, 1 \pmod{4}$, we see that

$$m \equiv 0 \pmod{2}, \text{ if } D \equiv 2, 3 \pmod{4}.$$

Note that

$$\begin{aligned} d_K &= d(Q(\sqrt{D})/Q) = \begin{cases} D, & \text{if } D \equiv 1 \pmod{4}, \\ 4D, & \text{if } D \equiv 2, 3 \pmod{4}, \end{cases} \\ &= \begin{cases} \Delta/m^2, & \text{if } D \equiv 1 \pmod{4} \\ \Delta/(\frac{m}{2})^2, & \text{if } D \equiv 2, 3 \pmod{4} \end{cases} = \Delta/g^2, \end{aligned}$$

where

$$g = \begin{cases} m, & \text{if } D \equiv 1 \pmod{4}, \\ m/2, & \text{if } D \equiv 2, 3 \pmod{4}, \end{cases}$$

is a positive integer. ■

Let L be any finite extension of a number field k . For $\mathcal{A} \in I_L$, define

$$\mathcal{A}^{-1} = \{\alpha \in L : \alpha \mathcal{A} \subset \mathcal{O}_L\},$$

$$\mathcal{A}^* = \{\alpha \in L : T_{L/k}(\alpha \mathcal{A}) \subset \mathcal{O}_k\},$$

and define the different of $\mathcal{A}$ as

$$\text{diff}_{L/k}(\mathcal{A}) = (\mathcal{A}^*)^{-1}.$$

Lemma 1.2.18 *Let k be an algebraic number field, and let L be a finite extension of k . Then*

$$d(L/k) = N_{L/k}(\text{diff}_{L/k}(\mathcal{O}_L)).$$

Proof: See [[28], Theorem 2.3, p.81]. ■

Let $k \subset L$ be two number fields, $\mathcal{P}$ a prime of k , and $\mathcal{B}$ a prime of L containing $\mathcal{P}$. Suppose that $\mathcal{B}^t$ is the exact power of $\mathcal{B}$ dividing $\text{diff}_{L/k}(\mathcal{O}_L)$. We denote $t = t(\mathcal{B}/\mathcal{P})$.

Lemma 1.2.19 (Hilbert's formula) *Let k and L be two number fields with $k \subset L$ a normal extension, $\mathcal{P}$ a prime of $\mathcal{O}_k$, and $\mathcal{B}$ a prime of L containing $\mathcal{P}$. Then*

$$t = t(\mathcal{B}/\mathcal{P}) = \sum_{m \geq 0} (|V_m(\mathcal{B}/\mathcal{P})| - 1).$$

Proof: See [[33], Proposition 3-7-25, p.115]. ■

Let $k \subset L$ be two number fields, p a rational prime, $\mathcal{P}$ a prime of k containing p , and $\mathcal{B}$ a prime of L containing $\mathcal{P}$. Suppose that $e(\mathcal{B}/\mathcal{P}) \neq 1$. If $p \nmid e(\mathcal{B}/\mathcal{P})$, we say that $\mathcal{B}/\mathcal{P}$ is **tamely ramified**, otherwise, **strongly ramified**.

Lemma 1.2.20 *Let $k \subset L$ be two number fields, p a rational prime, $\mathcal{P}$ a prime of k containing p , and $\mathcal{B}$ a prime of L containing $\mathcal{P}$.*

- (i) $\mathcal{B}/\mathcal{P}$ is tamely ramified $\iff t(\mathcal{B}/\mathcal{P}) = e(\mathcal{B}/\mathcal{P}) - 1$.
- (ii) $\mathcal{B}/\mathcal{P}$ is strongly ramified $\iff e \leq t(\mathcal{B}/\mathcal{P}) \leq v_{\mathcal{B}}(e) + e - 1$, where $e = e(\mathcal{B}/\mathcal{P})$.

Proof: See [[33], Theorem 3-7-23, p.114]. ■

Lemma 1.2.21 *Let $k \subset L$ be two number fields. Let $\mathcal{P}$ be a prime of k and let $\mathcal{B}_1, \dots, \mathcal{B}_r$ be all the prime of L containing $\mathcal{P}$. Then*

$$v_{\mathcal{P}}(d(L/k)) = \sum_{i=1}^r t(\mathcal{B}_i/\mathcal{P}) f(\mathcal{B}_i/\mathcal{P}).$$

Proof: The lemma follows from Lemmas 1.2.18 and 1.2.19 ■

1.3 Some Results from Class Field Theory

In this section $\mathcal{O}$ denotes an order of conductor f in a quadratic field K . The groups $I(\mathcal{O})$, $P(\mathcal{O})$, $I(\mathcal{O}, f)$, ... are defined in §1.1.

Lemma 1.3.1 *Let $\mathcal{O}$ be an order of conductor f in a quadratic field K . The inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induces an isomorphism*

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O}).$$

Proof: See [[11], Proposition 7.19, p.143]. ■

Lemma 1.3.2 *Let $\mathcal{O}$ be an order of conductor f in a quadratic field K . The inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induces an isomorphism*

$$I(\mathcal{O}, f)/P^+(\mathcal{O}, f) \simeq I(\mathcal{O})/P^+(\mathcal{O}) = C^+(\mathcal{O}).$$

Proof: We know by Lemma 1.3.1 that under the inclusion $I(\mathcal{O}, f) \subset I(\mathcal{O})$,

$$P(\mathcal{O}, f) \longrightarrow P(\mathcal{O}).$$

Note that as $P^+(\mathcal{O}, f) \subset P(\mathcal{O}, f)$, we have

$$P^+(\mathcal{O}, f) \longrightarrow P^+(\mathcal{O}),$$

and

$$I(\mathcal{O}, f)/P^+(\mathcal{O}, f) \simeq I(\mathcal{O})/P^+(\mathcal{O}) = C^+(\mathcal{O}). \quad \blacksquare$$

Lemma 1.3.3 *Let $\mathcal{O}$ be an order of conductor f in a quadratic field K . Then there are natural isomorphisms*

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,Z}(f).$$

Proof: See [[11], Proposition 7.22, p.145]. $\blacksquare$

Lemma 1.3.4 *Let $\mathcal{O}$ be an order of conductor f in a quadratic field K . Then there are natural isomorphisms*

$$C^+(\mathcal{O}) \simeq I(\mathcal{O}, f)/P^+(\mathcal{O}, f) \simeq I_K(f)/P_{K,Z}^+(f).$$

Proof: By Lemma 1.3.3, we know that under the isomorphism $I(\mathcal{O}, f) \longrightarrow I_K(f)$

$$P(\mathcal{O}, f) \longrightarrow P_{K,Z}(f).$$

Note that as $P^+(\mathcal{O}, f) \subset P(\mathcal{O}, f)$, we have

$$P^+(\mathcal{O}, f) \longrightarrow \tilde{P} \subset P_{K,Z}(f).$$

Then using the definition of $P_{K,Z}^+(f)$, we have

$$P^+(\mathcal{O}, f) \longrightarrow \tilde{P} = P_{K,Z}^+(f),$$

so that

$$C^+(\mathcal{O}) \simeq I(\mathcal{O}, f)/P^+(\mathcal{O}, f) \simeq I_K(f)/P_{K,Z}^+(f). \quad \blacksquare$$

Theorem 1.3.5 (Conductor Theorem) *Let $k \subset L$ be an Abelian extension. Then there is a unique modulus $f = f(L/k)$ called the conductor of L over k with the following properties:*

- (i) *A prime of k , finite or infinite, ramifies in L if and only if it divides f .*
- (ii) *Let $\mathcal{M}$ be a modulus divisible by all primes of k which ramify in L . Then $\ker(\phi_{L/k, \mathcal{M}})$ is a congruence subgroup for $\mathcal{M}$ if and only if $f|\mathcal{M}$.*

Proof: See [[11], Theorem 8.5, p.162]. ■

Theorem 1.3.6 (Existence Theorem) *Let $\mathcal{M}$ be a modulus of k , and let H be a congruence subgroup for $\mathcal{M}$, i.e.,*

$$P_{k,1}(\mathcal{M}) \subset H \subset I_k(\mathcal{M}).$$

Then there is a unique Abelian extension L of k , all of whose ramified primes, finite or infinite, divide $\mathcal{M}$, such that if

$$\phi_{M/k, \mathcal{M}} : I_k(\mathcal{M}) \longrightarrow \text{Gal}(L/k)$$

is the Artin map of the extension $k \subset L$, then $H = \ker(\phi_{M/k, \mathcal{M}})$.

Proof: See [[11], Theorem 8.6, p.162]. ■

Lemma 1.3.7 *Let L and M be Abelian extensions of k . Then $L \subset M$ if and only if there is a modulus $\mathcal{M}$, divisible by all the primes of k which are ramified in either L or M , such that*

$$P_{k,1}(\mathcal{M}) \subset \ker(\phi_{M/k, \mathcal{M}}) \subset \ker(\phi_{L/k, \mathcal{M}}).$$

Proof: See [[11], Theorem 8.7, p.163]. ■

Now we define the ring class field and the strict ring class field of an order of conductor f in a quadratic field K . By the Existence Theorem (Theorem 1.3.6),

$$P_{K,1}(f) \subset P_{K,z}(f) \subset I_K(f)$$

determines a unique Abelian extension $F_f(K)$ of the quadratic field K , and the Artin map induces an isomorphism

$$C(\mathcal{O}) \simeq I_K(f)/P_{K,z}(f) \simeq \text{Gal}(F_f(K)/K),$$

so that

$$h(\mathcal{O}) = |C(\mathcal{O})| = |\text{Gal}(F_f(K)/K)| = [F_f(K) : K]$$

We call $F_f(K)$ the **ring class field of the order $\mathcal{O}_f$** . Similarly, by the Existence Theorem (Theorem 1.3.6),

$$P_{K,1}(f\infty) \subset P_{K,z}^+(f\infty) \subset I_K(f\infty)$$

determines a unique Abelian extension $F_f^+(K)$ of K , which is called the **strict ring class field of the order $\mathcal{O}_f$** . Note that in fact

$$I_K(f\infty) = I_K(f), \quad P_{K,z}^+(f\infty) = P_{K,z}^+(f),$$

where ∞ denotes the product of all infinite primes of K , so that we have

$$C^+(\mathcal{O}) \simeq I_K(f)/P_{K,z}^+(f) = I_K(f\infty)/P_{K,z}^+(f\infty) \simeq \text{Gal}(F_f^+(K)/K).$$

Hence

$$h^+(\mathcal{O}) = |C^+(\mathcal{O})| = |\text{Gal}(F_f^+(K)/K)| = [F_f^+(K) : K].$$

It is clear that $F_f^+(K) = F_f(K)$ if K is an imaginary quadratic field.

Next we define the genus field of a (strict)ring class field.

Definition Let K be a quadratic field and let f be a positive integer. The genus field of the ring class field $F_f(K)$ (resp. strict ring class field $F_f^+(K)$) is denoted by $K(f)$ (resp. $K^+(f)$) and is the largest subfield of $F_f(K)$ (resp. $F_f^+(K)$) such that $K(f)$ (resp. $K^+(f)$) is an Abelian extension of Q .

Lemma 1.3.8 *Let K be a quadratic field and let d_K denote the discriminant of K over Q . Let f be a positive integer. If K is real, let $\epsilon_f(> 0)$ denote the fundamental unit of $\mathcal{O}_f$. Then*

$$P_{K,z}(f) = \begin{cases} P_{K,z}^+(f), & \text{if } d_K < 0 \text{ or } d_K > 0 \text{ and } N(\epsilon_f) = -1, \\ P_{K,z}^+(f) \cup \sqrt{d_K} P_{K,z}^+(f), & \text{otherwise.} \end{cases}$$

$$P(\mathcal{O}_f) = \begin{cases} P^+(\mathcal{O}_f), & \text{if } d_K < 0 \text{ or } d_K > 0 \text{ and } N(\epsilon_f) = -1, \\ P^+(\mathcal{O}_f) \cup \sqrt{d_K} P^+(\mathcal{O}_f), & \text{otherwise.} \end{cases}$$

Proof: First we suppose that $d_K < 0$. In this case, since $N(\alpha) > 0$ for any $\alpha \in K^* = K - \{0\}$, the conclusion follows.

Next we suppose that $d_K > 0$ and $N(\epsilon_f) = -1$. In this case, note that as $\alpha\mathcal{O}_K = \alpha\epsilon_f\mathcal{O}_K$ and one of $N(\alpha)$ and $N(\alpha\epsilon_f)$ must be positive, the result follows.

Now suppose that $d_K > 0$ and $N(\epsilon_f) = 1$. In this case, for any $\alpha \in K^*$, as $N_{K/Q}(\alpha)$ and $N_{K/Q}(\alpha\sqrt{d_K})$ have opposite sign so that $\alpha\mathcal{O}_K \neq \alpha\sqrt{d_K}\mathcal{O}_K$ in $I_K(f)/P_{K,Z}^+(f)$, the result follows. ■

Lemma 1.3.9 *Let K be a quadratic field and let d_K denote the discriminant of K over Q . Let f be a positive integer. If K is real, let $\epsilon_f(> 1)$ denote the fundamental unit of $\mathcal{O}_f$. Then*

$$\frac{h^+(\mathcal{O}_f)}{h(\mathcal{O}_f)} = [F_f^+(K) : F_f(K)] = \begin{cases} 1, & \text{if } d_K < 0 \text{ or } d_K > 0 \text{ and } N(\epsilon_f) = -1, \\ 2, & \text{otherwise.} \end{cases}$$

Proof: This is an immediate consequence of Lemmas 1.3.3, 1.3.4 and 1.3.8. ■

Lemma 1.3.10 *Let K be a quadratic field. Let f be a positive integer. Let $I = [\alpha, \beta]$ be a proper $\mathcal{O}_f$ -ideal. Define the quadratic form $g_I(x, y)$ by the formula*

$$g_I(x, y) = \frac{N_{K/Q}(\alpha x - \beta y)}{N_{K/Q}(I)}.$$

Then the discriminant of $g_I(x, y)$ is $d_K f^2$. Further, the map $I \longrightarrow g_I(x, y)$ induces an isomorphism $\lambda : C^+(\mathcal{O}_f) \longrightarrow H(d_K f^2)$.

Conversely, let $g(x, y) = ax^2 + bxy + cy^2$ be a primitive integral binary quadratic form of discriminant $d_K f^2$ with $a > 0$ if $d_K < 0$, define an $\mathcal{O}_f$ -ideal I_g as follows

$$I_g = \begin{cases} [a, \frac{-b + \sqrt{d_K f^2}}{2}], & \text{if either } d_K < 0 \text{ or } d_K > 0 \text{ and } a > 0, \\ \sqrt{d_K} [a, \frac{-b + \sqrt{d_K f^2}}{2}], & \text{if } d_K > 0 \text{ and } a < 0. \end{cases}$$

Further, the map $g \longrightarrow I_g$ induces an isomorphism $\nu : H(d_K f^2) \longrightarrow C^+(\mathcal{O}_f)$, which is the inverse of λ .

Proof: See [[11], Exercises 7.17-7.21, pp.153-154] or see [[19], Lemma (b), p.191 and Theorem 154, p.192].

Chapter 2

PROPERTIES OF DIHEDRAL POLYNOMIALS

In this chapter we give some properties of dihedral polynomials. In §2.1 we begin with some properties of dihedral groups. In §2.2 we discuss the structure of a dihedral extension and give the proofs of Theorems 2.2.18 and 2.2.20 which were stated in the Introduction. In §2.3 we discuss the basic properties of a cyclic dihedral polynomial. In the remaining sections (§§2.4-2.6) we treat cubic, quartic and quintic polynomials.

2.1 Some Properties of Dihedral Groups

Let p be a prime. Suppose that G is a finite group. If the order of every element of G is a power of p , then G is called a p -group. If $G = P_1 \times \dots \times P_r$ with each P_i being a cyclic group of order p , then G is called an elementary p -group.

Lemma 2.1.1 *Let G be a dihedral group generated by H and τ . Then for any $\sigma \in G - H$, σ is of order 2 and G is also generated by H and σ .*

Proof: Since $\sigma \notin H$, we have $\sigma = h\tau$ for some $h \in H$ so that

$$\sigma^2 = (h\tau)^2 = h(\tau h\tau) = hh^{-1} = 1.$$

Further, for any $x \in H$,

$$\sigma x \sigma^{-1} = (h\tau)x(h\tau)^{-1} = h(\tau x \tau^{-1})h^{-1} = hx^{-1}h^{-1} = x^{-1}.$$

Thus G is a dihedral group generated by H and σ . ■

Lemma 2.1.2 *Let G be a dihedral group generated by H and τ . Let G' denote the commutator subgroup of G . Then $H^2 = \{h^2 : h \in H\}$ is a subgroup of G and $G' = G^2 = H^2$. Further, G/G' is an elementary 2-group.*

Proof: First $G^2 = H^2$ is clear from Lemma 2.1.1. Next, since H is Abelian, H^2 is a subgroup of G . Now we show that $G' = H^2$. Note that every element of G/G^2 is of order ≤ 2 , so that G/G^2 is an Abelian group. Thus $G' \subset G^2 = H^2$. On the other hand, suppose $h \in H$, then

$$h^2 = h(\tau h^{-1} \tau^{-1}) = h\tau h^{-1} \tau^{-1} \in G',$$

hence $H^2 \subset G'$, proving $G' = H^2$. Further, as G/G' is Abelian and every element of G/G^2 is of order ≤ 2 , G/G' is an elementary 2-group. ■

Lemma 2.1.3 *Let G be a dihedral group generated by H and τ . Suppose that N is a normal subgroup of G and $N \not\subset H$, then G/N is an elementary 2-group.*

Proof: Since $\{1\} \neq N \not\subset H$, we have $G = NH$, and since

$$G/N = NH/N \simeq H/(N \cap H),$$

we see that G/N is an Abelian group. Hence the commutator subgroup $G' \subset N$. By Lemma 2.1.2 G/G' is an elementary 2-group. Then the assertion of the lemma follows from the isomorphism

$$G/N \simeq (G/G')/(N/G'). \quad \blacksquare$$

Lemma 2.1.4 *Let G be a dihedral group generated by H and τ . Then*

$$G \text{ is Abelian} \iff \langle \tau \rangle \triangleleft G \iff G \text{ is an elementary 2-group.}$$

Proof: It is obvious that if G is Abelian then $\langle \tau \rangle$ is normal in G . Now we suppose that $\langle \tau \rangle$ is normal in G . Since $\tau \notin H$, by Lemma 2.1.3, $H \simeq G/\langle \tau \rangle$ is an elementary 2-group. Further, $G = H \times \langle \tau \rangle$ is an elementary 2-group. Finally, if G is an elementary 2-group, then G is Abelian. ■

Lemma 2.1.5 *Let G be a dihedral group generated by H and τ . If G has a subgroup $H' (\neq H)$ such that G as a dihedral group is generated by H' and τ , then G is an elementary 2-group.*

Proof: Since $H' \neq H$, we can choose $h' \in H'$ but $h' \notin H$. By Lemma 2.1.1, G is also generated by H and h' . Note that as $h' \in H'$, $\langle h' \rangle$ is normal in G , by Lemma 2.1.4, G is an elementary 2-group. ■

Lemma 2.1.6 *Let G be a dihedral group generated by H and τ . Let N be a subgroup of G . Then N is a normal subgroup of G and the quotient G/N is a dihedral group generated by H/N and τH .*

Proof: Let $\sigma \in G$, then $\sigma = h$ or $h\tau$ for some $h \in H$ as G is generated by H and τ . Now let $\gamma \in N$, then

$$\sigma\gamma\sigma^{-1} = \begin{cases} \gamma, & \text{if } \sigma = h \\ \gamma^{-1}, & \text{if } \sigma = h\tau \end{cases} \in N.$$

Thus N is normal in G . It is obvious that G/N is generated by H/N and τN . ■

Lemma 2.1.7 *Let M be a dihedral extension of Q . Let K be a quadratic field in K_M . Then any extension of K contained in M is a dihedral extension of Q .*

Proof: This is an immediate corollary of Lemma 2.1.6. ■

Lemma 2.1.8 *Let G be a finite Abelian group of order $n = p_1^{a_1} \dots p_r^{a_r}$, where the p_i are distinct primes. Then G can be decomposed as the direct product*

- (i) $P_1 \times \dots \times P_r$, where the P_i are the Sylow p_i -subgroups of G ,
- (ii) $C_1 \times \dots \times C_s$, where the C_i are cyclic subgroups of order n_i with $n_1 \mid n_2 \mid \dots \mid n_s$,
- (iii) $CP_1 \times \dots \times CP_r$, where the CP_i are cyclic p_i -subgroups of G , where $p_i \mid n$.

Proof: The assertion (i) is well-known and the assertion (iii) is an obvious corollary of (i) and (ii). For the proof of (ii) see, for example, [[22] Theorem, p.181].

Lemma 2.1.9 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = \langle H, \tau \rangle$ a dihedral group. Let $H = H_1 \times H_2 \times \dots \times H_r$ be a direct product decomposition of H . Let N_i be the product of all the H_j 's except for H_i . Let M_i be the fixed field of N_i . Then*

- (i) M_i is a dihedral extension with $\text{Gal}(M_i/Q) \simeq \langle H_i, \tau \rangle$, and
- (ii) M is the composite field of the M_i 's.

Proof: By Lemma 2.1.6, N_i is a normal subgroup of G so that M_i is a normal extension with $\text{Gal}(M_i/Q) \simeq G/N_i$. Then again by Lemma 2.1.6,

$$G/N_i = \langle H/N_i, \tau N_i \rangle \simeq \langle H_i, \tau \rangle$$

as $H/N_i \simeq H_i$ and $\tau \notin H_i$. This completes the proof of (i).

Next we prove (ii). Note that

$$\bigcap_{1 \leq i \leq r} N_i = \{1\}.$$

Then appealing to Galois theory we have $M = M_1 M_2 \dots M_r$. ■

A group G is said to be transitive on a set S , if for any two elements $x, y \in S$ there is $\sigma \in G$ such that $\sigma(x) = y$. A subgroup H of the symmetric group S_n is called a transitive subgroup of S_n if H is transitive on the set $\{1, 2, \dots, n\}$.

Lemma 2.1.10 *Let k be a number field and let $f(x) \in k[x]$ be without repeated roots. Let $\deg(f) = d$. Let L be the splitting field of $f(x)$ over k .*

(i) $f(x)$ is irreducible in $k[x]$ if and only if $\text{Gal}(L/k)$ is a transitive permutation group on the set of roots of $f(x)$.

(ii) $\text{Gal}(L/k) \subset A_d$ (alternating group on d letters) if and only if $\text{disc}(f) \in k^2$.

Proof: See [[21], Theorem 1 and Corollary, p.91 and Theorem 2, p.93]. ■

Lemma 2.1.11 *Let $\pi = \pi_1 \pi_2 \dots \pi_r$ be a product of disjoint cycles π_i , then*

$$o(\pi) = \text{lcm}(o(\pi_1), o(\pi_2), \dots, o(\pi_r)).$$

Proof: See [[22], p.48] ■

Lemma 2.1.12 *Let G be a transitive permutation group on a finite set S . Suppose that H is a normal subgroup of G . Consider H acting on S . Then H divides S into s orbits each containing the same number of elements.*

Proof: For $x \in S$, a H -orbit of x is the set

$$H_x = \{h(x) : h \in H\}.$$

Now suppose x and y are any two elements of S . Since G is transitive on S , there exists $g \in G$ such that $g(x) = y$. Note that as H is a normal subgroup of G , we have

$$g^{-1}hg \in H \text{ for any } h \in H.$$

We define the map $\pi : H_x \longrightarrow H_y$ by

$$\pi : h(x) \longrightarrow ghg^{-1}(y), \forall h \in H.$$

It is easy to show that π is bijective. ■

2.2 Some Properties of Dihedral Polynomials

Lemma 2.2.1 *Let $\rho(x)$ be a dihedral polynomial. Let p be a prime not dividing $\text{disc}(\rho)$. Then $\rho(x)$ splits completely (mod p) if and only if p splits completely in every M_i , where the M_i 's are defined in Lemma 2.1.9.*

Proof: This is an immediate corollary of Lemmas 1.2.2, 1.2.3 and 2.1.9. ■

Lemma 2.2.2 *Let $\rho(x)$ be a dihedral polynomial of degree d . Let M be the splitting field of $\rho(x)$ over Q . Let $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Let S be the set of all the roots of $\rho(x)$. Suppose that $h \in H$. Then $\alpha(h) \mid d$ and h can be expressed as a disjoint product of $d/\alpha(h)$ cycles of length $\alpha(h)$. In particular, if $h \neq 1$, then h has no fixed points on S .*

Proof: As $\rho(x)$ is irreducible by Lemma 2.1.10(i) $\text{Gal}(M/Q)$ is a transitive group on the S . Since $h \in H$, $\langle h \rangle$ is normal in $\text{Gal}(M/Q)$. Then by Lemma 2.1.12, $\langle h \rangle$ divides S into s orbits each containing the same number of elements. As $\langle h \rangle$ is a cyclic group generated by h , Lemma 2.1.12 shows that h is a product of s disjoint cycles of the same length. Hence by Lemma 2.1.11 we have

$$\alpha(h) = |\langle h \rangle_x| \quad \text{for } x \in S,$$

and

$$d = |S| = s|\langle h \rangle_x| = s\alpha(h). \tag{2.1}$$

Hence h can be expressed as a disjoint product of $d/\alpha(h)$ cycles of length $\alpha(h)$. Now suppose that h fixes $x \in S$. Then $|\langle h \rangle_x| = 1$ and (2.1) gives $s = s\alpha(h)$, so that $h = 1$. ■

Lemma 2.2.3 *Let $\rho(x)$ be a dihedral polynomial of degree d . Let M be the splitting field of $\rho(x)$ over Q . Then $[M : Q] = d$ or $2d$.*

Proof: Let α be a root of $\rho(x)$ and let $L = Q(\alpha)$. We consider two cases according as $L = M$ or $L \neq M$.

(i) Suppose that $L = M$. In this case, $[M : Q] = d$.

(ii) Suppose that L is a proper subfield of M . In this case, $\text{Gal}(M/L)$ is a nontrivial subgroup of $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Now let $\sigma (\neq 1) \in \text{Gal}(M/L)$. By Lemma 2.2.2, as σ fixes α , $\sigma \notin H$. Thus $\sigma = h\tau$ for some $h \in H$. Then by Lemma 2.1.1, σ is of order 2.

Next we show that $\text{Gal}(M/L) = \langle \sigma \rangle$. In fact, if $\sigma' (\neq 1) \in \text{Gal}(M/L)$, then $\sigma' = h'\tau$ for some $h' \in H$. Then

$$\sigma\sigma' = (h\tau)(h'\tau) = h(\tau h'\tau) = hh'^{-1} \in H.$$

Note that as $\sigma\sigma'$ fixes α , by Lemma 2.2.2, we must have $\sigma\sigma' = 1$. Since σ is of order 2, we have $\sigma' = \sigma$.

Finally, $[M : Q] = [M : L][L : Q] = |\text{Gal}(M/L)||Q(\alpha) : Q| = 2d$. ■

Recall that a dihedral polynomial of degree d is called a dihedral polynomial of type 1 if $[M : Q] = 2d$, and a dihedral polynomial of type 2 if $[M : Q] = d$.

Lemma 2.2.4 *Let M be a dihedral extension. Then M is the splitting field of a dihedral polynomial of type 1 if and only if $\text{Gal}(M/Q)$ is not an elementary 2-group.*

Proof: First we suppose that $\text{Gal}(M/Q)$ is not an elementary 2-group. Suppose $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Let L be the fixed field of τ . Now choose $\alpha \in \mathcal{O}_L$ such that $L = Q(\alpha)$. Let $\rho(x)$ be the monic irreducible polynomial of α over Q , then $\deg(\rho(x)) = [L : Q]$. Note that as $\langle \tau \rangle$ is not a normal subgroup (Lemma 2.1.4) of $\text{Gal}(M/Q)$, by Galois theory, L is not a normal extension of Q . Thus the normal closure of L is a proper extension of L , and it must be M . In other words, M is the splitting field of $\rho(x)$. Hence $\rho(x)$ is a dihedral polynomial of type 1.

Conversely, suppose that M is the splitting field of a dihedral polynomial $\rho(x)$ of type 1. Then $[M : Q] = 2 \deg(\rho)$. Let $L = Q(\alpha)$, where α is a root of $\rho(x)$. Then M is the normal closure of L . If $\text{Gal}(M/Q)$ is an elementary 2-group, then $\text{Gal}(M/L)$ is a normal subgroup of $\text{Gal}(M/Q)$. By Galois theory, L is a normal extension of Q , which implies that $M = L$. This is a contradiction. ■

Lemma 2.2.5 *Let $\rho(x)$ be a dihedral polynomial of type 1, and let M be the splitting field of $\rho(x)$. Then there is exactly one quadratic field K in K_M .*

Proof: Let $G = \text{Gal}(M/Q)$. Suppose that K_1 and K_2 are two distinct quadratic fields in K_M . Let $H_1 = \text{Gal}(M/K_1)$, $H_2 = \text{Gal}(M/K_2)$, so that $[G : H_1] = [G : H_2] = 2$. Then

$$|H_1 \cup H_2| = |H_1| + |H_2| - |H_1 \cap H_2| \leq |G| - 1,$$

so that there is a $\tau \in \text{Gal}(M/Q)$ but $\tau \notin H_1 \cup H_2$. By Lemma 2.1.1, τ is order 2 and the dihedral group G is generated by H_i and τ for $i = 1, 2$, that is

$$\text{Gal}(M/Q) = \langle H_1, \tau \rangle = \langle H_2, \tau \rangle.$$

Then, as $H_1 \neq H_2$, we have by Lemma 2.1.5 that $\text{Gal}(M/Q)$ is an elementary 2-group. In particular, $\text{Gal}(M/Q)$ is an Abelian group. By Galois theory, any subfield of M is a normal extension of Q . Now let α be a root of $\rho(x)$, and let $L = Q(\alpha)$. Then L is a normal extension, so that L contains all the conjugates of α . This implies that L is the splitting field of $\rho(x)$ and $L = M$. Then $[M : Q] = [L : Q] = \deg(\rho)$, which is contrary to the assumption that $\rho(x)$ is a dihedral polynomial of type 1. Hence there is exactly one quadratic field K in K_M . ■

Lemma 2.2.6 *Let M be a dihedral extension. Then K_M contains exactly one quadratic field K if and only if M is the splitting field of a dihedral polynomial of type 1.*

Proof: The sufficiency follows immediately from Lemma 2.2.5. Conversely, suppose that K_M contains only one quadratic field K . Let $\tau \in \text{Gal}(M/Q) - \text{Gal}(M/K)$. By Lemma 2.1.1, τ is of order 2 and $\text{Gal}(M/Q)$ is generated by $\text{Gal}(M/K)$ and τ . Since K_M contains only one quadratic field K , $\text{Gal}(M/Q)$ is not an elementary 2-group. Then, appealing to Lemma 2.2.4, M is the splitting field of a dihedral polynomial of type 1. ■

Lemma 2.2.7 *Let $\rho(x)$ be a dihedral polynomial of type 1. Let M be the splitting field of $\rho(x)$ over Q . Let K be the unique quadratic field in K_M . Then $\rho(x)$ is irreducible over K .*

Proof: Let α be a root of $\rho(x)$ and let $L = Q(\alpha)$. Since $Q \subset L$ is not a normal extension, by Galois theory $\text{Gal}(M/L) \not\subset \text{Gal}(M/K)$ so that $K \not\subset L = Q(\alpha)$ and thus the composite field $Q(\alpha)K$ of $Q(\alpha)$ and K is a proper extension of $Q(\alpha)$ and therefore is equal to M as $[M : L] = 2$. On the other hand, as $Q \subset K$ we have

$$M = Q(\alpha)K \subset K(\alpha) \subset M,$$

so that $M = K(\alpha)$. This completes the proof of the lemma. ■

Lemma 2.2.8 *Let $\rho(x)$ be a dihedral polynomial of odd degree d . Let M be the splitting field of $\rho(x)$ over Q . Let K be the unique quadratic field in K_M . Suppose $\tau \in \text{Gal}(M/Q) - \text{Gal}(M/K)$. Then τ fixes exactly one root of $\rho(x)$.*

Proof: As $\tau \in S_d$ and $o(\tau) = 2$, τ can be expressed a product of some disjoint transpositions. Note that d is odd, we see that τ fixes at least one root of $\rho(x)$. Now suppose that α and β are two distinct roots of $\rho(x)$ fixed by τ . By Lemma 2.1.10(i), there is a $\sigma \in \text{Gal}(M/Q)$ such that $\sigma(\alpha) = \beta$. Without loss of generality we may suppose $\sigma \in \text{Gal}(M/K)$. Then from

$$\sigma^2(\alpha) = \tau\sigma^{-1}\tau\sigma(\alpha) = \tau\sigma^{-1}\tau(\beta) = \tau\sigma^{-1}(\beta) = \tau(\alpha) = \alpha,$$

and $\sigma^2 \in \text{Gal}(M/K)$, we have, by Lemma 2.2.2, that $\sigma^2 = 1$. This is contrary to the fact that the order of $\text{Gal}(M/K)$ is of odd d . ■

Recall that a number field F is called a totally real field if for any embedding $\mu : F \longrightarrow C$ we have $\mu(F) \subset R$. A number field M is said to be a CM-field if M is not a totally real field but contains a totally real field F with $[M : F] = 2$.

Lemma 2.2.9 *Let $\rho(x)$ be a dihedral polynomial. Let M be the splitting field of $\rho(x)$ over Q . Let K be a quadratic field in K_M . Let π denote complex conjugation. Then the extension $K \subset M$ has a ramified infinite prime if and only if $\pi|_M \neq 1$ and $\pi|_M \in \text{Gal}(M/K)$.*

Proof: Note that the statement that the extension $K \subset M$ has a ramified infinite prime is equivalent to saying that

- (i) K is a real quadratic field, and,
- (ii) M is not a totally real field.

(i) is equivalent to $\pi|_M \in \text{Gal}(M/K)$ and (ii) is equivalent to $\pi|_M \neq 1$. ■

Lemma 2.2.10 *Let $\rho(x)$ be a dihedral polynomial. Let M be the splitting field of $\rho(x)$ and let $K \in K_M$. Suppose that $\rho(x)$ has at least one real root. Then either M is a totally real field or K is an imaginary quadratic field.*

Proof: Suppose that α is a real root of $\rho(x)$. Then complex conjugation π fixes α . By the last assertion of Lemma 2.2.2, either $\pi|_M = 1$ or $\pi|_M \notin H = \text{Gal}(M/K)$. $\pi|_M = 1$ implies that M is a totally real field. $\pi|_M \notin \text{Gal}(M/K)$ implies that complex conjugation π induces a nontrivial automorphism on K , thus K is an imaginary quadratic field. ■

Lemma 2.2.11 *Let $\rho(x)$ be a dihedral polynomial of odd degree d . Let M be the splitting field of $\rho(x)$ and let $K \in K_M$. Then M/K has no ramified infinite primes. Further, if all the roots of $\rho(x)$ are real, then K is a real quadratic field, otherwise, K is an imaginary quadratic field.*

Proof: This is an immediate corollary of Lemma 2.2.10 as $\rho(x)$ has at least one real root. ■

Lemma 2.2.12 *Let $\rho(x)$ be a dihedral polynomial without real roots. Let M be the splitting field of $\rho(x)$ over $\mathbb{Q}$. Let K be a quadratic field in K_M . If K is a real quadratic field, then M is a CM-field.*

Proof: Let π denote complex conjugation. As K is a real quadratic field and M is not a real field, the extension $K \subset M$ has a ramified infinite prime, and so by Lemma 2.2.9, we have $\pi|_M \neq 1$ and $\pi|_M \in \text{Gal}(M/K)$. Let M_π be the fixed field of π . By Galois theory,

$$K \subset M_\pi \subset M.$$

Thus M_π is the maximal real subfield of M . Further, by Lemma 2.1.7 M_π is a normal extension of Q , M_π is a totally real field and thus M is a CM-field with maximal real subfield M_π . ■

Lemma 2.2.13 *Suppose that $k \subset L \subset M$ are number fields with M normal over k . Let $\mathcal{P}$ be a prime of k which is unramified in M . Fix a prime U of L containing $\mathcal{P}$. Let $D(U/\mathcal{P}) = \langle \phi \rangle$ be the decomposition group of $\mathcal{P}$. Let $H = \text{Gal}(M/L)$. Suppose that the set of right cosets of H in $\text{Gal}(M/k)$ is partitioned into sets*

$$\begin{aligned} &\{H\sigma_1, H\sigma_1\phi, \dots, H\sigma_1\phi^{m_1-1}\}, \\ &\dots\dots\dots, \\ &\{H\sigma_r, H\sigma_r\phi, \dots, H\sigma_r\phi^{m_r-1}\}. \end{aligned}$$

Then the splitting of $\mathcal{P}$ in L is given by

$$\mathcal{P}\mathcal{O}_L = \mathcal{B}_1\mathcal{B}_2\dots\mathcal{B}_r,$$

where $\mathcal{B}_i = \sigma_i(U) \cap \mathcal{O}_L$. Moreover, $f(\mathcal{B}_i/\mathcal{P}) = m_i$.

Proof: See [[29], Theorem 33, p.111]. ■

Lemma 2.2.14 *Suppose that $k \subset L \subset M$ are number fields with M normal over k . Let $\mathcal{P}$ be a prime of k which is unramified in M . Fix a prime U of L containing $\mathcal{P}$. Let $D = D(U/\mathcal{P}) = \langle \phi \rangle$ be the decomposition group of $\mathcal{P}$. Let $H = \text{Gal}(M/L)$. Suppose that*

$$\text{Gal}(M/k) = \cup_{i=1}^r H\sigma_i D$$

is a double coset decomposition of $\text{Gal}(M/k)$. Then the splitting of $\mathcal{P}$ in L is given by

$$\mathcal{P}\mathcal{O}_L = \mathcal{B}_1\mathcal{B}_2\dots\mathcal{B}_r,$$

where $\mathcal{B}_i = \sigma_i(U) \cap \mathcal{O}_L$. Moreover, $f(\mathcal{B}_i/\mathcal{P}) = m_i = |D/(\sigma_i^{-1}H\sigma_i \cap D)|$. In particular, $f(\mathcal{B}_i/\mathcal{P}) \mid |D|$.

Proof: We need only show that $m_i = |D/(\sigma_i^{-1}H\sigma_i \cap D)|$. We see that

$$m_i = |H\sigma_i D|/|H| = |\sigma_i^{-1}H\sigma_i D|/|\sigma_i^{-1}H\sigma_i| = |D/(\sigma_i^{-1}H\sigma_i \cap D)|,$$

as asserted. ■

Lemma 2.2.15 Suppose that $k \subset L \subset M$ are number fields with M normal over k . Let $\mathcal{P}$ be a prime of k which is unramified in M . Let $H = \text{Gal}(M/L)$. Let U be a prime of M containing $\mathcal{P}$. Let $D = D(U/\mathcal{P}) = \langle \phi \rangle$. Let $\sigma \in \text{Gal}(M/k)$. Then the inertial degree $f(\sigma(U) \cap \mathcal{O}_L/\mathcal{P}) = 1$ if and only if $\sigma\phi\sigma^{-1} \in H$. Further, let $n(L)$ denote the number of double cosets of the form $H\sigma D$ with $\sigma\phi\sigma^{-1} \in H$. Then there are exactly $n(L)$ primes of L containing $\mathcal{P}$ with inertial degree 1.

Proof: We have, by Lemma 2.2.14,

$$\begin{aligned} f(\sigma(U) \cap \mathcal{O}_L/\mathcal{P}) = 1 &\iff |D/(\sigma^{-1}H\sigma \cap D)| = 1 \iff D = \sigma^{-1}H\sigma \cap D \iff \\ &D \subset \sigma^{-1}H\sigma \iff \sigma D\sigma^{-1} \subset H \iff \sigma\phi\sigma^{-1} \in H \text{ (as } D \text{ is a cyclic group)}. \end{aligned}$$

The last assertion of the lemma is obvious. ■

Lemma 2.2.16 Suppose that $Q \subset L \subset M$ are number fields with M normal over Q . Suppose that $L = Q(\alpha)$, $\alpha \in \mathcal{O}_L$, and let $\varphi(x)$ be the irreducible polynomial of α over Q . Let p be a prime which does not divide $\text{disc}(\varphi)$. Then $\varphi(x)$ has exactly $n(L)$ linear factors (mod p), where $n(L)$ is defined in Lemma 2.2.15.

Proof: Since $p \nmid \text{disc}(\varphi)$, p is unramified in L . By Lemma 2.2.15, there are exactly $n(L)$ primes of L containing p with inertial degree 1. Then, appealing to Lemma 1.2.1, the conclusion follows. ■

Lemma 2.2.17 Suppose that H is a finite Abelian group. Let $h \in H$. Then either h has no square roots in H or h has 2^s square roots in H , where s is the 2-rank of H .

Proof: Suppose that $H = G_1 \times G_2 \times \dots \times G_t$ is a decomposition of H as a product of cyclic groups G_i , where G_i has order d_i . Suppose that h has a square root $\sigma \in H$. Let

$$\sigma = h_1^{r_1} h_2^{r_2} \dots h_t^{r_t}, \quad 0 \leq r_i < d_i, \quad h_i \in G_i.$$

Now let

$$\sigma' = h_1^{r'_1} h_2^{r'_2} \dots h_t^{r'_t}, \quad 0 \leq r'_i < d_i, \quad h_i \in G_i,$$

be any square root of h in H . Then

$$h_1^{2r_1} h_2^{2r_2} \dots h_t^{2r_t} = h_1^{2r'_1} h_2^{2r'_2} \dots h_t^{2r'_t}.$$

We have, for $i = 1, 2, \dots, t$

$$2r_i \equiv 2r_i' \pmod{d_i}.$$

Thus

$$\begin{cases} r_i \equiv r_i' \pmod{d_i} & \text{for odd } d_i, \\ r_i \equiv r_i' \pmod{d_i/2} & \text{for even } d_i, \end{cases}$$

and

$$\begin{cases} r_i' = r_i & \text{for odd } d_i, \\ r_i' = r_i \text{ or } r_i + (d_i/2) & \text{for even } d_i \text{ and } r_i < d_i/2, \\ r_i' = r_i \text{ or } r_i - (d_i/2) & \text{for even } d_i \text{ and } r_i \geq d_i/2. \end{cases}$$

Thus h has 2^s square roots in H , where s is the 2-rank of H . ■

We are now ready to prove the following Theorem which was stated in the introduction.

Theorem 2.2.18 *Let $\rho(x) \in Z[x]$ be a dihedral polynomial of type 1. Let $d = \deg(\rho)$. Let M be the splitting field of $\rho(x)$ over Q , and let K be the unique quadratic field in K_M (Lemma 2.2.5). Let $H = \text{Gal}(M/K)$ and let $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Let p be a prime not dividing $\text{disc}(\rho)$.*

(i) *If $\left(\frac{d_K}{p}\right) = 1$, the congruence (0.1) has d solutions if and only if the congruence (0.1) has a solution.*

(ii) *If $\left(\frac{d_K}{p}\right) = -1$, the congruence (0.1) has either 2^s or 0 solutions, where s denote the 2-rank of H . More precisely, let $D = \langle h\tau \rangle$ be the decomposition group of p in M , where $h \in H$. Then we have the following:*

(1) *If h is a square in H , then the congruence (0.1) has exactly 2^s solutions.*

(2) *If h is not a square in H , then all the irreducible factors of $\rho(x) \pmod{p}$ are of degree 2, in particular, the congruence (0.1) has no solutions.*

Proof: Let $L = Q(\alpha)$, where α is a root of $\rho(x)$. Without loss of generality we may assume that L is fixed by τ . Let U be a prime of M containing p . Let $D(U/p) = \langle \phi \rangle$.

First we suppose that $\left(\frac{d_K}{p}\right) = 1$. We show that if the congruence (0.1) has a solution then it has d solutions. Since $\left(\frac{d_K}{p}\right) = 1$, $K \subset M_D$, and by Galois theory, $\phi \in H$.

Now since the congruence (0.1) has a solution, by Lemma 2.2.15, there is $\sigma \in G$ such that $\sigma\phi\sigma^{-1} \in \langle \tau \rangle$. We may choose $\sigma = h \in H$. Then, as $\phi \in H$, we have

$$\phi = \sigma\phi\sigma^{-1} \in \langle \tau \rangle,$$

which implies that $\phi = 1$ as $\tau \notin H$. Now from $D = \{1\}$ we know that p splits completely in M , and thus p splits completely in $Q(\alpha)$. Then by Lemma 1.2.1, the congruence (0.1) has d solutions.

Now suppose that $\left(\frac{d_K}{p}\right) = -1$. By Lemma 1.2.16, $p\mathcal{O}_K$ splits completely in M . Consequently, p splits into $d = [M : K]$ primes in M . Then by Lemma 1.2.15, the decomposition field M_D of p is of degree d and therefore the decomposition group D is of order 2. Since p remains prime in K , $K \not\subset M_D$ and thus $D \not\subset H$. Hence

$$D = \langle \phi \rangle, \phi = h\tau \text{ for some } h \in H.$$

First we show that

$$h \in H^2 \iff \text{the congruence (0.1) has a solution.} \quad (2.2)$$

By Lemmas 1.2.1 and 2.2.15, we know that the congruence (0.1) has a solution if and only if there is a $\sigma \in G$ such that $\sigma\phi\sigma^{-1} \in \langle \tau \rangle$. We may assume that $\sigma \in H$. Now we show that

$$\sigma\phi\sigma^{-1} \in \langle \tau \rangle, \sigma \in H \iff h \in H^2. \quad (2.3)$$

Note that as $\phi = h\tau \neq 1$, we have

$$\sigma\phi\sigma^{-1} \in \langle \tau \rangle, \sigma \in H \iff \sigma\phi\sigma^{-1} = \tau \iff h = \sigma^{-1}\tau\sigma\tau = \sigma^{-2},$$

so that (2.3) follows and then (2.2) follows.

In view of Lemma 2.2.15 it is clear that to prove the assertion (1) we need only show that different square roots of h correspond to different double cosets, that is

$$\text{if } h = \sigma^{-2} = \sigma'^{-2} \text{ and } \langle \tau \rangle \sigma \langle h\tau \rangle = \langle \tau \rangle \sigma' \langle h\tau \rangle \text{ then } \sigma = \sigma'. \quad (2.4)$$

Since

$$\langle \tau \rangle \sigma \langle h\tau \rangle = \{\sigma, \tau\sigma\}, \langle \tau \rangle \sigma' \langle h\tau \rangle = \{\sigma', \tau\sigma'\},$$

and since $\tau\sigma \notin H$, (2.4) follows, proving the assertion (1).

Now suppose that h is not a square in H . By (2.2) the congruence (0.1) has no solution. Then by Lemma 1.2.1, each inertial degree $f(\mathcal{B}/p) \neq 1$. By Lemma 2.2.14, $f(\mathcal{B}/p) \mid |D| = 2$, so $f(\mathcal{B}/p) = 2$, proving the assertion (2).

Corollary 2.2.19 *Let $\rho(x)$ be a dihedral polynomial of type 1 with splitting field M . Let $\text{Gal}(M/Q) = \langle H, \tau \rangle$. Let K be the fixed field of H . Let p be a prime not dividing $\text{disc}(\rho)$. Suppose that $\left(\frac{d_K}{p}\right) = -1$, so that $D = \langle h\tau \rangle$ for some $h \in H$. Suppose that h is of odd order. Then $\rho(x) \equiv 0 \pmod{p}$ has exactly 2^s solutions, where s is the 2-rank of H . In particular, if $\rho(x)$ is of odd degree, then $\rho(x) \equiv 0 \pmod{p}$ has exactly one solution.*

Proof: As in Theorem 2.2.18, let $D = \langle h\tau \rangle$ with $h \in H$. If h is of odd order $2n + 1$, then $h = h^{-2n}$, that is h is a square in H . Then appealing to part (ii)(1) of Theorem 2.2.18, the lemma follows. ■

Theorem 2.2.20 *Let $\rho(x) \in Z[x]$ be a dihedral polynomial of type 2. Let M be the splitting field of $\rho(x)$ over Q . Let K be a quadratic subfield of M in K_M . Let p be a prime not dividing $\text{disc}(\rho)$.*

- (i) *If $\left(\frac{d_K}{p}\right) = 1$, then $\rho(x) \pmod{p}$ splits completely if and only if $\rho(x) \pmod{p}$ has a linear factor.*
- (ii) *If $\left(\frac{d_K}{p}\right) = -1$, then $\rho(x) \pmod{p}$ is a product of quadratic irreducible factors.*

Proof: The conclusion of case (i) is an immediate corollary of Lemma 1.2.1. Now we suppose that $\left(\frac{d_K}{p}\right) = -1$. By Lemma 1.2.16, $p\mathcal{O}_K$ splits completely in M . Let U be a prime of M containing p , then $f(U/p) = f(U/p\mathcal{O}_K)f(p\mathcal{O}_K/p) = 2$. Then by Lemma 1.2.1, the lemma is proved.

Theorem 2.2.21 *Let $\rho(x) \in Z[x]$ be a dihedral polynomial. Let M be the splitting field of $\rho(x)$ over Q . Let K be a quadratic subfield of M in K_M . Let p be a prime not dividing $\text{disc}(\rho)$. Then p splits completely in M if and only if $\left(\frac{d_K}{p}\right) = 1$ and the congruence $\rho(x) \equiv 0 \pmod{p}$ has a solution.*

Proof: As $p \nmid \text{disc}(\rho)$, by Lemma 1.2.1, we have that p splits completely in M if and only if the congruence $\rho(x) \equiv 0 \pmod{p}$ has $d(= \deg(\rho))$ solutions. Then the theorem follows from Theorem 2.2.18(i) and Theorem 2.2.20(i). ■

2.3 Cyclic Dihedral Polynomials

Let $\rho(x)$ be a dihedral polynomial. Let M be the splitting field of $\rho(x)$. Recall that $\rho(x)$ is called a cyclic dihedral polynomial if $\text{Gal}(M/Q) = D_m$ for some positive integer m . In this section we study cyclic dihedral polynomials.

Lemma 2.3.1 *Let M be a dihedral extension of Q . Then M is the composite field of its cyclic dihedral subfields M_i , each M_i having $\text{Gal}(M_i/Q) = D_{m_i}$, where each m_i is a prime power.*

Proof: Suppose that $\text{Gal}(M/Q) = \langle H, \tau \rangle$. We have by Lemma 2.1.8(iii)

$$H = CP_1 \times \dots \times CP_s,$$

where the CP_i 's are cyclic p_i -subgroups of G . Let N_i be the product of all the CP_j 's except for CP_i , and let M_i be the fixed field of N_i . Then, by Lemma 2.1.9, the M_i are cyclic dihedral extensions and M is the composite field of the M_i 's. ■

Lemma 2.3.2 *Let $\rho(x)$ be a cyclic dihedral polynomial of degree d with Galois group $D_m = \langle \sigma, \tau \rangle$, where $\sigma^m = \tau^2 = (\sigma\tau)^2 = 1$ and $m > 1$. Then $d = m$ or $2m$. Consequently, σ is a d -cycle if $\rho(x)$ is a dihedral polynomial of type 1, otherwise, σ is a product of two $(d/2)$ -cycles.*

Proof: By Lemma 2.2.3, we have

$$d = \begin{cases} m, & \text{if } \rho(x) \text{ is of type 1,} \\ 2m, & \text{if } \rho(x) \text{ is of type 2.} \end{cases}$$

Then, appealing to Lemma 2.2.2, the lemma is proved.

Lemma 2.3.3 *Let $D_m = \langle \sigma, \tau \rangle$, where $\sigma^m = \tau^2 = (\sigma\tau)^2 = 1$.*

(i) If m is odd, then D_m contains only one subgroup of order m , which is $\langle \sigma \rangle$.

(ii) If m is even, then D_m contains exactly three subgroups of order m , namely

$$\langle \sigma \rangle, \langle \sigma^2, \tau \rangle, \langle \sigma^2, \sigma\tau \rangle.$$

Proof: Suppose that H is a subgroup of D_m of order m . Then H is normal in D_m as $[D_m : H] = 2$. Thus D_m/H has order 2, and it follows that $\sigma^2 \in H$.

(i) If m is odd, then $\langle \sigma^2 \rangle = \langle \sigma \rangle = H$.

(ii) If m is even, then $\langle \sigma^2 \rangle$ is a subgroup of index 2 in H .

We consider three possibilities:

(1) If $\tau \in H$, then $H = \langle \sigma^2, \tau \rangle$ as $\tau \notin \langle \sigma \rangle$.

(2) If $\sigma\tau \in H$, then $H = \langle \sigma^2, \sigma\tau \rangle$ as $\sigma\tau \notin \langle \sigma \rangle$.

(3) If $\tau \notin H$ and $\sigma\tau \notin H$, then we have $H\tau = H\sigma\tau$ as $[D_m : H] = 2$. Hence $\sigma \in H$ and thus $H = \langle \sigma \rangle$. ■

Lemma 2.3.4 *Suppose that M is a cyclic dihedral extension with $\text{Gal}(M/Q) = D_m$.*

(i) If m is odd, then M contains only one quadratic subfield K .

(ii) If m is even, then M contains exactly three quadratic subfields.

Proof: This is an immediate corollary of Lemma 2.3.3.

Lemma 2.3.5 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of degree d . Let M be the splitting field of $\rho(x)$. Then $\text{Gal}(M/Q) = D_d$ is generated by*

$$\sigma = (1, 2, \dots, d), \quad \tau = \prod_{1 \leq i \leq \frac{d}{2}} (i, d-i).$$

Proof: Let α be a root of $\rho(x)$ and let $\text{Gal}(M/Q(\alpha))$ be generated by $\tau \in \text{Gal}(M/Q)$. Then τ fixes α and is of order 2. Let $\sigma \in \text{Gal}(M/Q)$ be of order d (such σ exists by Lemma 2.3.2 as $\rho(x)$ is a cyclic dihedral polynomial of type 1). Let

$$\alpha_i = \sigma^i(\alpha), \quad i = 1, 2, \dots, d.$$

Then

$$\sigma(\alpha_i) = \alpha_{i+1}, \quad i = 1, 2, \dots, d-1, \quad \sigma(\alpha_d) = \alpha_1,$$

$$\tau(\alpha_i) = \tau(\sigma^i(\alpha)) = (\tau\sigma^i)(\alpha) = (\sigma^{-i}\tau)(\alpha) = \sigma^{-i}(\alpha) = \alpha_{d-i}, \quad i = 1, 2, \dots, d-1,$$

so that

$$\sigma = (1, 2, \dots, d), \text{ and } \tau = \prod_{1 \leq i \leq \frac{d}{2}} (i, d-i). \quad \blacksquare$$

Lemma 2.3.6 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of even degree d . Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the roots of $\rho(x)$. Let M be the splitting field of $\rho(x)$ over Q . Suppose that $\text{Gal}(M/Q) = D_d = \langle \sigma, \tau \rangle$, $\sigma = (1, 2, \dots, d)$, $\tau = (1, d-1)(2, d-2) \dots (\frac{d}{2}-1, \frac{d}{2}+1)$. Then $Q(\sqrt{\text{disc}(\rho)})$ is a quadratic field fixed by*

$$\begin{cases} \langle \sigma^2, \tau \rangle, & \text{if } d \equiv 2 \pmod{4}, \\ \langle \sigma^2, \sigma\tau \rangle, & \text{if } d \equiv 0 \pmod{4}. \end{cases}$$

Proof: Let $\delta = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)$ so that $\text{disc}(\rho) = \delta^2$. As $\sigma(\delta) = -\delta$, $\tau(\delta) = (-1)^{d/2-1}\delta$, we see that $\delta^2 \in Z$ and $\pm\sqrt{\text{disc}(\rho)} = \delta \notin Z$, so $Q(\sqrt{\text{disc}(\rho)}) = Q(\delta)$ is a quadratic field. Further, $\sigma^2(\delta) = \delta$ and

$$\tau(\delta) = \delta, \quad \text{if } d \equiv 2 \pmod{4},$$

$$\sigma\tau(\delta) = \delta, \quad \text{if } d \equiv 0 \pmod{4}.$$

Then by Galois theory, the lemma is proved. $\blacksquare$

Lemma 2.3.7 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of even degree d . Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the roots of $\rho(x)$. Let M be the splitting field of $\rho(x)$ over Q . Suppose that $\text{Gal}(M/Q) = D_d = \langle \sigma, \tau \rangle$, $\sigma = (1, 2, \dots, d)$, $\tau = (1, d-1)(2, d-2) \dots (\frac{d}{2}-1, \frac{d}{2}+1)$. Let $\gamma = (\alpha_1 - \alpha_{1+\frac{d}{2}})(\alpha_2 - \alpha_{2+\frac{d}{2}}) \dots (\alpha_{\frac{d}{2}} - \alpha_d)$. Then $Q(\gamma)$ is a quadratic field fixed by*

$$\begin{cases} \langle \sigma^2, \tau \rangle, & \text{if } d \equiv 2 \pmod{4}, \\ \langle \sigma^2, \sigma\tau \rangle, & \text{if } d \equiv 0 \pmod{4}. \end{cases}$$

Proof: Since $\sigma(\gamma) = -\gamma$, $\tau(\gamma) = (-1)^{d/2-1}\gamma$, we have $\sigma(\gamma^2) = \gamma^2$, $\tau(\gamma^2) = \gamma^2$, so that $\gamma^2 \in Z$ and $\gamma \notin Z$, proving $Q(\gamma)$ is a quadratic field. Further, $\sigma^2(\gamma) = \gamma$ and

$$\tau(\gamma) = \gamma, \quad \text{if } d \equiv 2 \pmod{4},$$

$$\sigma\tau(\gamma) = \gamma, \quad \text{if } d \equiv 0 \pmod{4}.$$

Then by Galois theory, the lemma is proved. $\blacksquare$

Lemma 2.3.8 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of even degree d . Let M be the splitting field of $\rho(x)$, and let K be the unique quadratic field in K_M (Lemma 2.3.4). Let $D = \text{disc}(\rho(x))$. The following conditions guarantee that K is an imaginary quadratic field.*

(i) *If $D < 0$ and $d \equiv 0 \pmod{4}$, then K is an imaginary quadratic field.*

(ii) *If $D > 0$, $d \equiv 2 \pmod{4}$, and $\rho(x)$ has at least one complex root, then K is an imaginary quadratic field.*

Proof: Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be all the roots of $\rho(x)$. By Lemma 2.3.5, $\text{Gal}(M/Q)$ is generated by

$$\sigma = (1, 2, \dots, d) \text{ and } \tau = \prod_{1 \leq i \leq \frac{d}{2}} (i, d-i).$$

Since $\sqrt{D} = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)$, and σ is an odd permutation, we have $\sigma(\sqrt{D}) = -\sqrt{D}$, and

$$\sigma^{d/2}(\sqrt{D}) = (-1)^{d/2} \sqrt{D} = \begin{cases} \sqrt{D}, & \text{if } d \equiv 0 \pmod{4}, \\ -\sqrt{D}, & \text{if } d \equiv 2 \pmod{4}. \end{cases} \quad (2.5)$$

First we treat case (i). We let π denote complex conjugation. Since $D < 0$, $\rho(x)$ has at least one pair of complex roots, so that $\pi \in \text{Gal}(M/Q)$. If K is not imaginary, then $\pi \in \text{Gal}(M/K)$. Thus $\pi = \sigma^{d/2}$ and (2.5) gives $\pi(\sqrt{D}) = \sqrt{D}$. This is contrary to the assumption $D < 0$.

Next, we treat case (ii). If $\rho(x)$ has at least one pair of complex roots and K is not imaginary, then exactly as in (i), we have that $\pi = \sigma^{d/2}$ and (2.5) gives $\pi(\sqrt{D}) = -\sqrt{D}$. This is contrary to the assumption $D > 0$. ■

Lemma 2.3.9 *Let $\rho(x) \in Z[x]$ be a cyclic dihedral polynomial of odd degree d , so that $\rho(x)$ is of type 1. Then*

$$\text{disc}(\rho(x)) \begin{cases} = \square, & \text{if } d \equiv 1 \pmod{4}, \\ \neq \square, & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Proof: By Lemma 2.3.5 we have $\text{Gal}(M/Q) = D_d = \langle \sigma, \tau \rangle$, where

$$\sigma = (1, 2, \dots, d), \text{ and } \tau = (1, d-1)(2, d-2) \dots \left(\frac{d-1}{2}, \frac{d+1}{2} \right).$$

Note that $\sigma = (1, 2, \dots, d) = (d-1, d)(d-2, d-1)\dots(1, 2)$ is a product of $(d-1)$ transpositions, so that $\sigma \in A_d$, and τ is a product of $\frac{d-1}{2}$ transpositions, so that

$$\begin{cases} \tau \in A_d, & \text{if } d \equiv 1 \pmod{4}, \\ \tau \notin A_d, & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Thus

$$\begin{cases} \text{Gal}(M/Q) \subset A_d, & \text{if } d \equiv 1 \pmod{4}, \\ \text{Gal}(M/Q) \not\subset A_d, & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Now by Lemma 2.1.10, we have

$$\text{disc}(\rho(x)) \begin{cases} = \square, & \text{if } d \equiv 1 \pmod{4}, \\ \neq \square, & \text{if } d \equiv 3 \pmod{4}. \quad \blacksquare \end{cases}$$

In fact a stronger result than Lemma 2.3.9 is true. We have

Lemma 2.3.10 *Let $\rho(x)$ be a cyclic dihedral polynomial of odd degree d . Let M be the splitting field of $\rho(x)$ over Q and let K be the unique quadratic field in K_M . Then*

$$\text{disc}(\rho) = g^2 d_K^{(d-1)/2},$$

for some positive integer g .

Proof: Without loss of generality we may suppose that $\text{Gal}(M/Q) = D_d = \langle \sigma, \tau \rangle$, where

$$\sigma = (1, 2, \dots, d), \text{ and } \tau = (1, d-1)(2, d-2)\dots\left(\frac{d-1}{2}, \frac{d+1}{2}\right).$$

Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be all the roots of $\rho(x)$. Let

$$\beta_i = \prod_{j=0}^{d-1} \sigma^j(\alpha_1 - \alpha_{i+1}), \quad i = 1, \dots, (d-1)/2.$$

As

$$\sigma(\beta_i) = \beta_i, \quad \tau(\beta_i) = -\beta_i,$$

we have

$$\sigma(\beta_i^2) = \beta_i^2, \quad \tau(\beta_i^2) = \beta_i^2,$$

which implies that for all i

$$\beta_i^2 \in \mathbb{Z}, \quad K = \mathbb{Q}(\beta_i).$$

Next we observe that

$$(\alpha_1 - \alpha_i)^2 = (\alpha_1 + \alpha_i)^2 - 4\alpha_1\alpha_i \equiv (\alpha_1 + \alpha_i)^2 \pmod{4\mathcal{O}_M},$$

$$\sigma^j(\alpha_1 - \alpha_i)^2 \equiv \sigma^j(\alpha_1 + \alpha_i)^2 \pmod{4\mathcal{O}_M},$$

so that

$$\prod_{j=0}^{d-1} \sigma^j(\alpha_1 - \alpha_i)^2 \equiv \prod_{j=0}^{d-1} \sigma^j(\alpha_1 + \alpha_i)^2 \pmod{4\mathcal{O}_M}. \quad (2.6)$$

Since $\prod_{j=0}^{d-1} \sigma^j(\alpha_1 + \alpha_i)$ is fixed by both σ and τ , $\prod_{j=0}^{d-1} \sigma^j(\alpha_1 + \alpha_i) \in \mathbb{Z}$. Then (2.6) becomes

$$\prod_{j=0}^{d-1} \sigma^j(\alpha_1 - \alpha_i)^2 \equiv \prod_{j=0}^{d-1} \sigma^j(\alpha_1 + \alpha_i)^2 \equiv 0, 1 \pmod{4}.$$

By Lemma 1.2.17, for some positive integer g_i , we have

$$\beta_i^2 = \prod_{j=0}^{d-1} \sigma^j(\alpha_1 - \alpha_i)^2 = g_i^2 d_K.$$

Finally, as $\text{disc}(\rho) = \beta_1^2 \dots \beta_{(d-1)/2}^2$, we have

$$\text{disc}(\rho) = \prod_{i=1}^{(d-1)/2} \beta_i^2 = g^2 d_K^{(d-1)/2},$$

where $g = g_1 g_2 \dots g_{(d-1)/2}$. ■

Lemma 2.3.11 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of degree $d \equiv 3 \pmod{4}$. Let M be the splitting field of $\rho(x)$ over $\mathbb{Q}$ and let K be the quadratic subfield of M . Then*

$$K = \mathbb{Q}(\sqrt{\text{disc}(\rho)}).$$

Proof: By Lemma 2.3.10, for some positive integer g , we have

$$\text{disc}(\rho) = g^2 d_K^{(d-1)/2},$$

and the lemma follows as $(d-1)/2$ is odd. ■

Lemma 2.3.12 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 1 of degree d . Then either all the roots of $\rho(x)$ are real or $\rho(x)$ has exactly one real root. Further, for case $d \equiv 3 \pmod{4}$, if $\text{disc}(\rho) > 0$, then all the roots of $\rho(x)$ are real and if $\text{disc}(\rho) < 0$, then $\rho(x)$ has only one real root.*

Proof: Since d is odd, $\rho(x)$ has at least one real root α . Let M be the splitting field of $\rho(x)$. If α' is another real root of $\rho(x)$, then we have, by Lemma 2.2.8, that $M = Q(\alpha, \alpha')$. Hence M is a totally real field and all the roots of $\rho(x)$ are real. Now suppose $d \equiv 3 \pmod{4}$. Let $K \in K_M$. Lemma 2.2.7 shows that $M = K(\alpha)$. It is clear that M is a totally real field if and only if K is a real quadratic field. Then the assertion of the lemma follows from Lemma 2.3.11. ■

Lemma 2.3.13 *Let $\rho(x) \in Z[x]$ be a cyclic dihedral polynomial of odd degree d . Let M denote the splitting field of $\rho(x)$. Then $d_M \mid (\text{disc}(\rho(x)))^3$.*

Proof: Let $\text{Gal}(M/Q) = D_d = \langle \sigma, \tau \rangle$, where $\sigma^d = \tau^2 = (\sigma\tau)^2 = 1$. Let L be the field fixed by τ . Without loss of generality we may suppose that

$$\tau = (1, d-1)(2, d-2) \dots \left(\frac{d-1}{2}, \frac{d+1}{2}\right), \quad \sigma = (1, 2, \dots, d).$$

Let $\theta_1, \theta_2, \dots, \theta_d$ be an integral basis of L over Q . Let $\alpha_1, \alpha_2, \dots, \alpha_d$ be the d roots of $\rho(x)$. Let A denote the matrix $A = (\sigma^{i-1}(\theta_j))_{d \times d}$. Let $\alpha = \text{diag}(\alpha_1, \alpha_2, \dots, \alpha_d)$.

Then

$$\text{disc}_{M/Q}(\theta_1, \theta_2, \dots, \theta_d, \alpha_1\theta_1, \alpha_1\theta_2, \dots, \alpha_1\theta_d) = \det \begin{pmatrix} A & \alpha A \\ \tau(A) & \tau(\alpha A) \end{pmatrix}^2.$$

We note that

$$\tau(A) = JA, \quad \tau(\alpha) = J_1\alpha.$$

where

$$J = \begin{pmatrix} 1 & & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \\ & & & & & \ddots \\ & & & & & & 1 \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix}, \quad J_1 = \begin{pmatrix} & & & & 1 \\ & & & & & \ddots \\ & & & & & & \ddots \\ & & & & & & & \ddots \\ & & & & & & & & 1 \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 1 \end{pmatrix},$$

and

$$\begin{pmatrix} I & 0 \\ -J & I \end{pmatrix} \begin{pmatrix} A & \alpha A \\ \tau(A) & \tau(\alpha A) \end{pmatrix} = \begin{pmatrix} I & 0 \\ -J & I \end{pmatrix} \begin{pmatrix} A & \alpha A \\ JA & J_1 \alpha JA \end{pmatrix} = \begin{pmatrix} A & \alpha A \\ 0 & J_1 \alpha JA - J \alpha A \end{pmatrix}.$$

Thus

$$\begin{aligned} \det \begin{pmatrix} A & \alpha A \\ \tau(A) & \tau(\alpha A) \end{pmatrix}^2 &= \det \begin{pmatrix} A & \alpha A \\ 0 & J_1 \alpha JA - J \alpha A \end{pmatrix}^2 \\ &= \det(A^2) \det(J_1 \alpha JA - J \alpha A)^2 \\ &= (\det(A^2))^2 \det(J_1 \alpha J - J \alpha)^2 \\ &= d_L^2 \det(J J_1 \alpha J - \alpha)^2, \end{aligned}$$

as $\det(A^2) = d_L$ and $J^2 = 1$. By direct computation, we obtain

$$J J_1 \alpha J = \text{diag}(\alpha_{d-1}, \alpha_d, \alpha_1, \dots, \alpha_{d-2}).$$

Thus

$$\det(J J_1 \alpha J - \alpha)^2 = (\alpha_{d-1} - \alpha_1)^2 (\alpha_d - \alpha_2)^2 \prod_{i=3}^d (\alpha_i - \alpha_{i-2})^2 \mid \text{disc}(\rho(x)).$$

Since

$$d_M \mid \text{disc}_{M/Q}(\theta_1, \theta_2, \dots, \theta_d, \alpha_1 \theta_1, \alpha_1 \theta_2, \dots, \alpha_1 \theta_d),$$

we have

$$d_M \mid d_L^2 \text{disc}(\rho(x)).$$

Furthermore, as $d_L \mid \text{disc}(\rho(x))$, we deduce

$$d_M \mid \text{disc}(\rho(x))^3. \quad \blacksquare$$

Lemma 2.3.14 *Let $\rho(x)$ be a cyclic dihedral polynomial of type 2 of degree d . Let M be the splitting field of $\rho(x)$. Then $\text{Gal}(M/Q) = D_{d/2}$ is generated by*

$$\sigma = (1, 2, \dots, \frac{d}{2})(\frac{d}{2} + 1, \dots, d), \quad \tau = (1, d-1)(2, d-2) \dots (\frac{d}{2} - 1, \frac{d}{2} + 1)(\frac{d}{2}, d).$$

Proof: Let α be a root of $\rho(x)$, then $\beta = \tau(\alpha) \neq \alpha$ (otherwise $Q(\alpha)$ is a proper subfield of M). For $i = 1, 2, \dots, \frac{d}{2}$, set

$$\alpha_i = \sigma^i(\alpha), \quad \alpha_{\frac{d}{2}+i} = \sigma^i(\beta).$$

Then

$$\tau(\alpha_i) = \tau\sigma^i(\alpha) = \sigma^{\frac{d}{2}-i}\tau(\alpha) = \sigma^{\frac{d}{2}-i}(\beta) = \alpha_{d-i} \text{ for } 1 \leq i \leq \frac{d}{2} - 1.$$

This completes the proof of the lemma. ■

Lemma 2.3.15 *Let $\rho(x) \in Z[x]$ be a cyclic dihedral polynomial of type 2 of degree d . Let M be the splitting field of $\rho(x)$. Then*

$$\begin{cases} \text{disc}(\rho(x)) = \square, & \text{if } d \equiv 0 \pmod{4}, \\ \text{disc}(\rho(x)) \neq \square, & \text{if } d \equiv 2 \pmod{4}. \end{cases}$$

Proof: By Lemma 2.3.14 we may assume that

$$\sigma = (1, 2, \dots, \frac{d}{2})(\frac{d}{2} + 1, \dots, d), \quad \tau = (1, d-1)(2, d-2) \dots (\frac{d}{2} - 1, \frac{d}{2} + 1)(\frac{d}{2}, d).$$

Thus

$$\begin{cases} \tau \in A_{d/2}, & \text{if } d \equiv 0 \pmod{4}, \\ \tau \notin A_{d/2}, & \text{if } d \equiv 2 \pmod{4}, \end{cases}$$

and

$$\sigma \in A_{d/2}.$$

Hence we have

$$\begin{cases} \text{Gal}(M/Q) \subset A_{d/2}, & \text{if } d \equiv 0 \pmod{4}, \\ \text{Gal}(M/Q) \not\subset A_{d/2}, & \text{if } d \equiv 2 \pmod{4}. \end{cases}$$

Now appealing to Lemma 2.1.10 the lemma follows. ■

Lemma 2.3.16 *Let $\rho(x) \in Z[x]$ be a cyclic dihedral polynomial of type 2 of degree $d \equiv 2 \pmod{4}$. Let M be the splitting field of $\rho(x)$, and let K be the unique quadratic subfield of M . Then*

$$K = Q(\sqrt{\text{disc}(\rho)}).$$

Proof: By Lemma 2.3.15, we have $\text{disc}(\rho) \neq \square$ as $d \equiv 2 \pmod{4}$. Thus $Q(\sqrt{\text{disc}(\rho)})$ is a quadratic field contained in M . As $\frac{d}{2} \equiv 1 \pmod{2}$ Lemma 2.3.4 shows that M contains only one quadratic field K , so that $K = Q(\sqrt{\text{disc}(\rho)})$. ■

2.4 Cubic Polynomials

In this section we give a necessary and sufficient condition for an irreducible cubic polynomial over Z to be dihedral.

Recall that a group G is said to be solvable if there is a finite series of subgroups of G

$$\{1\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G$$

such that

- (i) $G_i \triangleleft G_{i-1}$ for $1 \leq i \leq n$, and
- (ii) G_{i-1}/G_i is cyclic, for $1 \leq i \leq n$.

Recall also that a group G acting on a set S is said to be transitive on S , if for any two elements $x, y \in S$ there is $\sigma \in G$ such that $\sigma(x) = y$. A subgroup H of the symmetric group S_n is called a transitive subgroup of S_n if H is transitive on the set $\{1, 2, \dots, n\}$.

Lemma 2.4.1 *Suppose that G is a transitive subgroup of the symmetric group S_p , where p is an odd prime. Then G is a solvable group if and only if there exists a subgroup H of the cyclic group Z_p^* such that G is isomorphic to the group of transformations $\{\tau_{(a,b)} : a \in Z_p, b \in H\}$ of Z_p , where $\tau_{(a,b)}(k) = ak + b$.*

Proof: See [[15], Theorem 20.3, p. 160]. ■

Lemma 2.4.2 *Let p be an odd prime and let N denote the number of divisors of $p-1$. Then up to isomorphism there are N solvable transitive subgroups of S_p .*

Proof: Since Z_p^* is a cyclic group, Z_p^* has exactly N subgroups. Then appealing to Lemma 2.4.1, the lemma is proved. ■

Lemma 2.4.3 *Let $\varphi(x)$ be an irreducible cubic polynomial over k , where k is a field of characteristic 0. Let M be the splitting field of $\varphi(x)$ over k . Then*

$$\text{Gal}(M/k) = \begin{cases} A_3, & \text{if } \text{disc}(\varphi) \in k^2, \\ S_3, & \text{if } \text{disc}(\varphi) \notin k^2. \end{cases}$$

Thus, if $\varphi(x)$ is a monic irreducible cubic polynomial in $Z[x]$, then

$$\varphi(x) \text{ is a dihedral polynomial} \iff \text{disc}(\varphi) \neq \square.$$

Proof: Since $\varphi(x)$ is irreducible, $\text{Gal}(M/k)$ is a transitive group on the set of roots of $\varphi(x)$. By Lemma 2.4.2, $\text{Gal}(M/k) = A_3$ or S_3 . Then by Lemma 2.1.10,

$$\text{Gal}(M/k) = \begin{cases} A_3, & \text{if } \text{disc}(\varphi) \in k^2, \\ S_3, & \text{if } \text{disc}(\varphi) \notin k^2. \end{cases} \quad \blacksquare$$

2.5 Quartic Polynomials

Let $\varphi(x)$ be an irreducible quartic polynomial in $Q[x]$. Let M be the splitting field of $\varphi(x)$, so that

$$\text{Gal}(M/Q) = S_4, A_4, D_4, Z_4, \text{ or } D_2.$$

Kappe and Warren [24] have given a necessary and sufficient condition for each of the above five possibilities. Applying their result to a quartic dihedral polynomial $\rho(x)$ gives information about the subfield structure of the splitting field M of $\rho(x)$ over Q (see Lemmas 2.5.3, 2.5.4, 2.5.5 and 2.5.6). Further, Lemma 2.5.9 gives a new way of determining the Galois group of a quartic polynomial.

Let $\varphi(x)$ be a monic irreducible quartic polynomial over Q . Let $\alpha_1, \alpha_2, \alpha_3$ and α_4 be the roots of $\varphi(x)$. Set

$$t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad t_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad t_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

The cubic resolvent of $\varphi(x)$ is defined by

$$r(x) = (x - t_1)(x - t_2)(x - t_3)$$

and an easy calculation gives

$$r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2).$$

Lemma 2.5.1 *Suppose that $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d$ is an irreducible quartic polynomial in $Q[x]$, $r(x)$ its cubic resolvent with splitting field E , and M the splitting field of $\varphi(x)$ over Q . Then*

- (i) $\text{Gal}(M/Q) = S_4$ if and only if $r(x)$ is irreducible over Q and $\text{disc}(\varphi) \notin Q^2$;
- (ii) $\text{Gal}(M/Q) = A_4$ if and only if $r(x)$ is irreducible over Q and $\text{disc}(\varphi) \in Q^2$;

(iii) $\text{Gal}(M/Q) = D_4$ if and only if $r(x)$ has exactly one root $t \in Q$ and $g(x) = (x^2 - tx + d)(x^2 + ax + (b - t))$ does not split over E ;

(iv) $\text{Gal}(M/Q) = Z_4$ if and only if $r(x)$ has exactly one root in Q and $g(x)$ splits over E ;

(v) $\text{Gal}(M/Q) = D_2$ if and only if $r(x)$ splits into linear factors over Q .

Proof: The earliest complete determination of the Galois group of a quartic polynomial is asserted to be due to F. Hack in 1895 (see [24], Theorem 1). ■

Lemma 2.5.2 Suppose $\varphi(x) = x^4 + bx^2 + d \in Q[x]$ is irreducible. Let M denote the splitting field of $\varphi(x)$. Then

(i) $\text{Gal}(M/Q) = D_4 \iff d \text{ and } d(b^2 - 4d) \notin Q^2$;

(ii) $\text{Gal}(M/Q) = Z_4 \iff d(b^2 - 4d) \in Q^2$;

(iii) $\text{Gal}(M/Q) = D_2 \iff d \in Q^2$.

Proof: See [[24], Theorem 3]. ■

Lemma 2.5.3 Let $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in Q[x]$ be irreducible. Let M be the splitting field of $\varphi(x)$ and suppose that

$$\text{Gal}(M/Q) = D_4 = \langle \sigma, \tau \rangle, \text{ where } \sigma^4 = \tau^2 = (\sigma\tau)^2 = 1.$$

Without loss of generality we assume that $\sigma = (1234)$, $\tau = (13)$ (Lemma 2.3.5). Let k denote the fixed field of $\langle \sigma^2, \sigma\tau \rangle$, let k' denote the fixed field of $\langle \sigma^2, \tau \rangle$, and let K denote the fixed field of $\langle \sigma \rangle$. Then

(i) $k = Q(\sqrt{D})$,

(ii) $k' = Q(\sqrt{t^2 - 4d})$ or $Q(\sqrt{a^2 - 4(b - t)})$,

(iii) $K = Q(\sqrt{(t^2 - 4d)D})$ or $Q(\sqrt{(a^2 - 4(b - t))D})$,

where t is the unique rational root of $r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$ and $D = \text{disc}(\varphi(x))$.

Proof: Since $K = kk'$, in order to prove the lemma we need only prove (i) and (ii). Let $\alpha_1, \alpha_2, \alpha_3, \alpha$ denote the roots of $\varphi(x)$ so that

$$\sqrt{D} = \pm \prod_{1 \leq i < j \leq 4} (\alpha_i - \alpha_j).$$

Since σ and τ are odd permutations,

$$\sigma(\sqrt{D}) = -\sqrt{D}, \quad \tau(\sqrt{D}) = -\sqrt{D}. \quad (2.7)$$

Further,

$$\sigma^2(\sqrt{D}) = \sqrt{D}, \quad \sigma\tau(\sqrt{D}) = \sqrt{D}.$$

Since $D \neq 0$, (2.7) shows that $Q(\sqrt{D})$ is a quadratic field so that we have (i). Next, by Lemma 2.5.1, exactly one of the quantities

$$\alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \alpha_1\alpha_4 + \alpha_2\alpha_3$$

is in Q . Note that

$$\begin{aligned} \sigma(\alpha_1\alpha_3 + \alpha_2\alpha_4) &= \alpha_1\alpha_3 + \alpha_2\alpha_4, \\ \tau(\alpha_1\alpha_3 + \alpha_2\alpha_4) &= \alpha_1\alpha_3 + \alpha_2\alpha_4, \end{aligned}$$

so that $t = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in Q$. Next, since

$$(\alpha_1\alpha_3 - \alpha_2\alpha_4)^2 = (\alpha_1\alpha_3 + \alpha_2\alpha_4)^2 - 4(\alpha_1\alpha_3)(\alpha_2\alpha_4) = t^2 - 4d,$$

we have

$$\sqrt{t^2 - 4d} = \pm(\alpha_1\alpha_3 - \alpha_2\alpha_4).$$

Also since

$$\begin{aligned} [(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)]^2 &= [(\alpha_1 + \alpha_3) + (\alpha_2 + \alpha_4)]^2 - 4(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ &= a^2 - 4(b - t), \end{aligned}$$

we have

$$\sqrt{a^2 - 4(b - t)} = \pm[(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)].$$

In addition, since

$$\begin{aligned} \sigma(\alpha_1\alpha_3 - \alpha_2\alpha_4) &= -(\alpha_1\alpha_3 - \alpha_2\alpha_4), \\ \sigma[(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)] &= -[(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)], \\ \tau(\alpha_1\alpha_3 - \alpha_2\alpha_4) &= (\alpha_1\alpha_3 - \alpha_2\alpha_4), \\ \tau[(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)] &= [(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)], \end{aligned}$$

we have

$$\sigma(\sqrt{t^2 - 4d}) = -\sqrt{t^2 - 4d}, \quad \sigma(\sqrt{a^2 - 4(b-t)}) = -\sqrt{a^2 - 4(b-t)}, \quad (2.8)$$

$$\tau(\sqrt{t^2 - 4d}) = \sqrt{t^2 - 4d}, \quad \tau(\sqrt{a^2 - 4(b-t)}) = \sqrt{a^2 - 4(b-t)}. \quad (2.9)$$

Hence both $\sqrt{t^2 - 4d}$ and $\sqrt{a^2 - 4(b-t)}$ are in k' . We show that at least one of them is not in Q . If both $\sqrt{t^2 - 4d}$ and $\sqrt{a^2 - 4(b-t)}$ are in Q , then (2.8) implies that

$$t^2 - 4d = 0 \quad \text{and} \quad a^2 - 4(b-t) = 0,$$

that is

$$\alpha_1\alpha_3 = \alpha_2\alpha_4 \quad \text{and} \quad \alpha_1 + \alpha_3 = \alpha_2 + \alpha_4.$$

Then

$$\begin{aligned} \varphi(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \\ &= (x - \alpha_1)(x - \alpha_3)(x - \alpha_2)(x - \alpha_4) \\ &= (x^2 - (\alpha_1 + \alpha_3)x + \alpha_1\alpha_3)(x^2 - (\alpha_2 + \alpha_4)x + \alpha_2\alpha_4) \\ &= (x^2 - (\alpha_1 + \alpha_3)x + \alpha_1\alpha_3)^2, \end{aligned}$$

which is a contradiction as $\varphi(x)$ is a separable polynomial. This proves (ii). ■

Lemma 2.5.4 *Let $\varphi(x) = x^4 + bx^2 + d \in Q[x]$ be irreducible. Let M be the splitting field of $\varphi(x)$ and suppose that*

$$\text{Gal}(M/Q) = D_4 = \langle \sigma, \tau \rangle, \quad \text{where } \sigma^4 = \tau^2 = (\sigma\tau)^2 = 1.$$

Without loss of generality we assume that $\sigma = (1234)$, $\tau = (13)$ (Lemma 2.3.5). Let k denote the fixed field of $\langle \sigma^2, \sigma\tau \rangle$, and let k' denote the fixed field of $\langle \sigma^2, \tau \rangle$, and let K denote the fixed field of $\langle \sigma \rangle$. Then

- (i) $k = Q(\sqrt{d})$,
- (ii) $k' = Q(\sqrt{b^2 - 4d})$,
- (iii) $K = Q(\sqrt{(b^2 - 4d)d})$.

Proof: First since $D = 4^2(b^2 - 4d)^2d$, (i) of Lemma 2.5.3 gives $k = Q(\sqrt{d})$. Next, since $r(x) = x^3 - bx^2 - 4dx + 4bd = (x - b)(x^2 - 4d)$, by Lemma 2.5.1, we have $t = b$. In this case, $a^2 - 4(b - t) = 0$, and the lemma follows from Lemma 2.5.3. ■

Lemma 2.5.5 *Let $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in Q[x]$ be irreducible. Let M be the splitting field of $\varphi(x)$ and suppose that*

$$\text{Gal}(M/Q) = D_2 = \langle \sigma, \tau \rangle, \text{ where } \sigma^2 = \tau^2 = (\sigma\tau)^2 = 1.$$

Without loss of generality we assume that $\sigma = (13)(24)$, $\tau = (12)(34)$ (Lemma 2.3.14). Let k_1 denote the fixed field of τ , let k_2 denote the fixed field of $\sigma\tau$, and let k_3 denote the fixed field of σ . Then

$$(i) \ k_1 = Q(\sqrt{t_1^2 - 4d}) \text{ or } Q(\sqrt{a^2 - 4(b - t_1)}),$$

$$(ii) \ k_2 = Q(\sqrt{t_2^2 - 4d}) \text{ or } Q(\sqrt{a^2 - 4(b - t_2)}),$$

$$(iii) \ k_3 = Q(\sqrt{t_3^2 - 4d}) \text{ or } Q(\sqrt{a^2 - 4(b - t_3)}),$$

where $t_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $t_2 = \alpha_1\alpha_4 + \alpha_2\alpha_3$, $t_3 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ are the rational roots of $r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$.

Proof: Since the proofs are similar, we prove only (i). Since

$$\sqrt{t_1^2 - 4d} = \pm(\alpha_1\alpha_2 - \alpha_3\alpha_4), \quad \sqrt{a^2 - 4(b - t_1)} = \pm[(\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4)],$$

we see that

$$\tau(\sqrt{t_1^2 - 4d}) = \sqrt{t_1^2 - 4d}, \quad \tau(\sqrt{a^2 - 4(b - t_1)}) = \sqrt{a^2 - 4(b - t_1)}, \quad (2.10)$$

and

$$\sigma(\sqrt{t_1^2 - 4d}) = -\sqrt{t_1^2 - 4d}, \quad \sigma(\sqrt{a^2 - 4(b - t_1)}) = -\sqrt{a^2 - 4(b - t_1)}. \quad (2.11)$$

If (i) is false, (2.10) and (2.11) imply that

$$t_1^2 - 4d = 0, \quad a^2 - 4(b - t_1) = 0, \quad (2.12)$$

which implies

$$\alpha_1\alpha_2 = \alpha_3\alpha_4 \text{ and } \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4.$$

Then

$$\begin{aligned} \varphi(x) &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \\ &= (x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2)(x^2 - (\alpha_3 + \alpha_4)x + \alpha_3\alpha_4) \\ &= (x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2)^2, \end{aligned}$$

which is a contradiction as $\varphi(x)$ is a separable polynomial. This completes the proof of (i). ■

Lemma 2.5.6 *Let $\varphi(x) = x^4 + bx^2 + d \in Q[x]$ be irreducible. Let M be the splitting field of $\varphi(x)$ and suppose that $\text{Gal}(M/Q) = D_2$. Then the three quadratic subfields of M are*

$$Q(\sqrt{b^2 - 4d}), Q(\sqrt{-b + 2\sqrt{d}}), Q(\sqrt{-b - 2\sqrt{d}}).$$

Proof: Since $\text{Gal}(M/Q) = D_2$, by Lemma 2.5.2, $d \in Q^2$. Then

$$r(x) = x^3 - bx^2 - 4dx + 4bd = (x - b)(x + 2\sqrt{d})(x - 2\sqrt{d}),$$

and we have

$$t_1 = b, t_2 = -2\sqrt{d}, t_3 = 2\sqrt{d}.$$

Note that

$$a^2 - 4(b - t_1) = 0, t_2^2 - 4d = t_3^2 - 4d = 0$$

and appealing to Lemma 2.5.5, the proof of the lemma follows. ■

Lemma 2.5.7 *Let $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d \in Q[x]$. Let $\alpha_1, \alpha_2, \alpha_3$ and α_4 be the four roots of $\varphi(x)$. Let $t = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha = \alpha_1 - \alpha_3$ and $\beta = \alpha_2 - \alpha_4$. Then*

$$\alpha^2 + \beta^2 = a^2 - 2(t + b), \alpha^2\beta^2 = (b + t)^2 - 4(t^2 + ac - 4d).$$

Proof: By direct computation we have

$$\begin{aligned} \alpha^2 + \beta^2 &= (\alpha_1 - \alpha_3)^2 + (\alpha_2 - \alpha_4)^2 \\ &= \alpha_1^2 + \alpha_3^2 + \alpha_2^2 + \alpha_4^2 - 2(\alpha_1\alpha_3 + \alpha_2\alpha_4) \\ &= a^2 - 2b - 2t = a^2 - 2(t + b). \end{aligned}$$

To prove the second equality we set $s = (\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)$. Combining with the equality $-a = (\alpha_1 + \alpha_3) + (\alpha_2 + \alpha_4)$, we have

$$2(\alpha_1 + \alpha_3) = s - a, -2(\alpha_2 + \alpha_4) = s + a,$$

and

$$s^2 - a^2 = -4(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -4(b - t).$$

Then

$$\begin{aligned}
 16\alpha^2\beta^2 &= 4(\alpha_1 - \alpha_3)^2 \cdot 4(\alpha_2 - \alpha_4)^2 \\
 &= 4[(\alpha_1 + \alpha_3)^2 - 4\alpha_1\alpha_3] \cdot 4[(\alpha_2 + \alpha_4)^2 - 4\alpha_2\alpha_4] \\
 &= [(s - a)^2 - 16\alpha_1\alpha_3][(s + a)^2 - 16\alpha_2\alpha_4] \\
 &= (s^2 - a^2)^2 + 16^2d - 16[\alpha_1\alpha_3(s + a)^2 + \alpha_2\alpha_4(s - a)^2] \\
 &= (s^2 - a^2)^2 + 16^2d - 16[t(s^2 + a^2) + 2as(\alpha_1\alpha_3 - \alpha_2\alpha_4)],
 \end{aligned}$$

and

$$\begin{aligned}
 s(\alpha_1\alpha_3 - \alpha_2\alpha_4) &= [(\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4)](\alpha_1\alpha_3 - \alpha_2\alpha_4) \\
 &= [(\alpha_1 + \alpha_3)\alpha_1\alpha_3 + (\alpha_2 + \alpha_4)\alpha_2\alpha_4] - [(\alpha_1 + \alpha_3)\alpha_2\alpha_4 + (\alpha_2 + \alpha_4)\alpha_1\alpha_3] \\
 &= [(\alpha_1 + \alpha_3)(t - \alpha_2\alpha_4 + (\alpha_2 + \alpha_4)(t - \alpha_1\alpha_3))] - [(\alpha_1 + \alpha_3)\alpha_2\alpha_4 + (\alpha_2 + \alpha_4)\alpha_1\alpha_3] \\
 &= -at - 2[(\alpha_1 + \alpha_3)\alpha_2\alpha_4 + (\alpha_2 + \alpha_4)\alpha_1\alpha_3] = -at + 2c.
 \end{aligned}$$

Thus

$$\begin{aligned}
 16\alpha^2\beta^2 &= (s^2 - a^2)^2 + 16^2d - 16[t(s^2 + a^2) + 2as(\alpha_1\alpha_3 - \alpha_2\alpha_4)] \\
 &= (s^2 - a^2)^2 + 16^2d - 16[t(s^2 + a^2) + 2a(-at + 2c)] \\
 &= (s^2 - a^2)^2 + 16^2d - 16[t(s^2 - a^2) + 4ac] \\
 &= 16(b - t)^2 + 16^2d - 16[-4(b - t)t + 4ac] \\
 &= 16[(b + t)^2 - 16 \cdot 4(t^2 + ac - 4d)]. \blacksquare
 \end{aligned}$$

Lemma 2.5.8 *Let $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d$ be irreducible over Q with splitting field M . Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of $\varphi(x)$. Suppose $\text{Gal}(M/Q) = D_4$ or Z_4 . Without loss of generality we suppose that*

$$D_4 = \langle (1234), (13) \rangle, \quad Z_4 = \langle (1234) \rangle.$$

Let $\alpha = \alpha_1 - \alpha_3$, $\beta = \sigma(\alpha) = \alpha_2 - \alpha_4$. Let $f(x) = x^4 - (\alpha^2 + \beta^2)x^2 + (\alpha\beta)^2$. Then

(i) $f(x) = x^4 - (a^2 - 2(t + b))x^2 + (b + t)^4 - 4(t^2 + ac - 4d) \in Q[x]$ and $f(x)$ is irreducible over Q .

(ii) $f(x)$ and $\varphi(x)$ have the same splitting field.

Proof: Let $\sigma = (1234)$, $\tau = (13)$. Since $\text{Gal}(M/Q) = D_4$ or Z_4 , by Lemma 2.5.1, exactly one of the quantities

$$\alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \alpha_1\alpha_4 + \alpha_2\alpha_3$$

is in Q . Note that

$$\begin{aligned}\sigma(\alpha_1\alpha_3 + \alpha_2\alpha_4) &= \alpha_1\alpha_3 + \alpha_2\alpha_4, \\ \tau(\alpha_1\alpha_3 + \alpha_2\alpha_4) &= \alpha_1\alpha_3 + \alpha_2\alpha_4,\end{aligned}$$

so that $t = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in Q$. Now appealing to Lemma 2.5.7,

$$f(x) = x^4 - (a^2 - 2(t+b))x^2 + (b+t)^4 - 4(t^2 + ac - 4d) \in Q[x].$$

Next as (1234) acts transitively on the set $\{\pm\alpha, \pm\beta\}$, by Lemma 2.1.10, $f(x)$ is irreducible over Q .

Let M' denote the splitting field of $f(x)$. As $M' \subset M$, to prove (ii) we need only show that $\text{Gal}(M'/Q) = \text{Gal}(M/Q)$.

First we suppose $\text{Gal}(M/Q) = D_4$. As $f(x)$ is irreducible over Q , by Lemma 2.5.2 we need only show that

$$(\alpha\beta)^2, (\alpha\beta)^2(\alpha^2 - \beta^2)^2 \notin Q^2,$$

or equivalently,

$$\alpha\beta, \alpha\beta(\alpha^2 - \beta^2) \notin Q.$$

Since $\tau(\alpha\beta) = -\alpha\beta$, we have $\alpha\beta \notin Q$. Suppose $\alpha\beta(\alpha^2 - \beta^2) \in Q$. Then, in view of

$$\tau(\alpha\beta(\alpha^2 - \beta^2)) = -\alpha\beta(\alpha^2 - \beta^2),$$

we must have $\alpha\beta(\alpha^2 - \beta^2) = 0$, which implies that $\alpha^2 = \beta^2$ so that $\alpha = \pm\beta$. This is contrary to the fact that $f(x)$ has no repeated roots. Hence $\text{Gal}(M'/Q) = D_4$.

Secondly, we suppose $\text{Gal}(M/Q) = Z_4$. As $f(x)$ is irreducible over Q , by Lemma 2.5.2 we need only show that

$$(\alpha\beta)^2(\alpha^2 - \beta^2)^2 \in Q^2,$$

or equivalently,

$$\alpha\beta(\alpha^2 - \beta^2) \in Q. \quad (2.13)$$

As $\sigma(\alpha) = \beta$, $\sigma(\beta) = -\alpha$, (2.13) follows. Hence $\text{Gal}(M'/Q) = Z_4$. ■

Remark: In view of Lemma 2.5.8, if a quartic polynomial $\varphi(x)$ has Galois group D_4 or Z_4 , then we can find another quartic polynomial $f(x)$ with the same Galois group which has the form $f(x) = x^4 + bx^2 + d$. Let $L = Q(\sqrt{(-b + \sqrt{b^2 - 4d})/2})$. The explicit evaluation of d_L has been carried out by J.A. Huard, B.K. Spearman and K.S. Williams [20]. Theorem 4.4.11 (resp. Lemma 1.2.14) then enable us to determine the conductor of the extension M/K (resp. L/Q , if L/Q is a cyclic extension), where M is a dihedral extension with $\text{Gal}(M/Q) = D_4$, and K is the unique quadratic subfield of M with $\text{Gal}(M/K)$ cyclic.

Lemma 2.5.9 Suppose $\varphi(x) = x^4 + ax^3 + bx^2 + cx + d$ is irreducible over Q and that the cubic resolvent $r(x)$ of $\varphi(x)$ has a rational root t . Let M denote the splitting field of $\varphi(x)$ over Q . Set

$$b' = -(a^2 - 2b - 2t), \quad d' = (b + t)^2 - 4(t^2 + ac - 4d).$$

Then

- (iii)' $\text{Gal}(M/Q) = D_4 \iff d' \text{ and } d'(b'^2 - 4d') \notin Q^2,$
- (iv)' $\text{Gal}(M/Q) = Z_4 \iff d'(b'^2 - 4d') \in Q^2,$
- (v)' $\text{Gal}(M/Q) = D_2 \iff d' \in Q^2.$

Proof: (iii)' and (iv)' follow from Lemma 2.5.8. Now we show (v)'. First we suppose that $d' \in Q^2$. Then (iii)' shows that $\text{Gal}(M/Q) \neq D_4$. If $\text{Gal}(M/Q) = Z_4$, then by (iv)' we have $d'(b'^2 - 4d') \in Q^2$ so that $(b'^2 - 4d') \in Q^2$, which implies that $f(x) = x^4 - b'x^2 + d'$ is reducible over Q . This is a contradiction by Lemma 2.5.8(i). Hence we must have $\text{Gal}(M/Q) = D_2$. Conversely, suppose $\text{Gal}(M/Q) = D_2$. Let $\alpha_1, \dots, \alpha_4$ be the roots of $\varphi(x)$. Without loss of generality we may assume that $t = \alpha_1\alpha_3 + \alpha_2\alpha_4$, then by Lemma 2.5.7 we have

$$d' = \alpha^2\beta^2,$$

where $\alpha = \alpha_1 - \alpha_3$, $\beta = \alpha_2 - \alpha_4$. Since $\text{Gal}(M/Q) = D_2 = \langle (12)(34), (13)(24) \rangle$, and $\alpha\beta$ is fixed by (12)(34) and (13)(24) so that $\alpha\beta \in Q$, and $d' \in Q^2$. This completes the proof of the lemma. ■

Example 2.5.1 $\varphi(x) = x^4 - 4x^3 + 7x^2 - 6x + 1$. Here $r(x) = (x-3)(x^2 - 4x + 8)$ so that

$$t = 3, \quad b' = 4, \quad d' = -16, \quad (b'^2 - 4d')d' = -5 \cdot 16^2.$$

Hence the Galois group of $\varphi(x)$ is D_4 .

Example 2.5.2 $\varphi(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Here $r(x) = x(x-2)(x-4)$ so that the Galois group of $\varphi(x)$ is D_2 . For $t = 0, 2$ and 4 the corresponding $d' = 4, 16$ and 4 .

Example 2.5.3 $\varphi(x) = x^4 + x^3 + x^2 + x + 1$. The corresponding $r(x) = (x-2)(x^2+x-1)$, thus we have $t = 2, b' = d' = 5$ and $(b'^2 - 4d')d' = 5^2 \in Z^2$. Hence the Galois group of $\varphi(x)$ is Z_4 .

2.6 Quintic Polynomials

The determination of the Galois group of an irreducible polynomial in $Q[x]$ in terms of its coefficients is of considerable interest. For cubic polynomials, this was done in Lemma 2.4.3. For quartic polynomials, this has been done by Kappe and Warren [24]. Here we treat the same problem for a quintic polynomial, see Theorems 2.6.6-2.6.12 and 2.6.16.

Lemma 2.6.1 (Newton's Identities) Let $\varphi(x) = x^n - a_1x^{n-1} + \dots + (-1)^na_n$ be a polynomial, and let $\alpha_1, \dots, \alpha_n$ be roots of $\varphi(x)$. Let $S_i = \sum_{k=1}^n \alpha_k^i$, for $i = 1, 2, \dots$. Then

$$S_i - S_{i-1}a_1 + \dots + (-1)^{i-1}S_1a_{i-1} + (-1)^ia_i = 0 \quad (i = 1, 2, \dots),$$

where $a_i = 0$ for $i > n$.

Proof: see [[13], §12, p.12]

Lemma 2.6.2 The symmetric group S_n is a nonsolvable group for $n \geq 5$.

Proof: See [[15], Corollary p.134]. ■

Lemma 2.6.3 *Let q be an odd prime. Let M/Q be a cyclic extension of degree q . Let p be a prime which is ramified in M . Then the p -part of $f_0(M/Q)$ is given by*

$$\begin{cases} p, & \text{if } p \neq q, \\ p^2, & \text{if } p = q, \end{cases}$$

and the p -part of d_M is given by

$$\begin{cases} p^{q-1}, & \text{if } p \neq q, \\ p^{2(q-1)}, & \text{if } p = q. \end{cases}$$

Proof: By Lemma 1.2.12 we have

$$d_M = f_0(M/Q)^{q-1}, \quad v_p(d_M) = (q-1)v_p(f_0(M/Q)). \quad (2.14)$$

Let $\mathcal{P}$ be a prime of M containing p . As q is a prime we have $p\mathcal{O}_M = \mathcal{P}^q$.

First we suppose that $p \neq q$. In this case as p is tamely ramified in M , by Lemma 1.2.20 we have that $t(\mathcal{P}/p) = q-1$. Then appealing to Lemma 1.2.21 we have $v_p(d_M) = q-1$. Then (2.14) gives $v_p(f_0(M/Q)) = 1$.

Now we suppose that $p = q$. In this case as p is strongly ramified in M , by Lemma 1.2.20 we have that $q \leq t(\mathcal{P}/p) = 2q-1$. By Lemma 1.2.21 we have $v_p(d_M) = t(\mathcal{P}/p)$. Then (2.14) gives

$$v_p(d_M) = 2(p-1), \quad v_p(f_0(M/Q)) = 2. \quad \blacksquare$$

Lemma 2.6.4 *A transitive subgroup of S_5 is isomorphic to exactly one of the following groups:*

$$\begin{array}{ll} Z_5, D_5, F_{20}, & \text{solvable,} \\ A_5, S_5, & \text{nonsolvable,} \end{array}$$

where $Z_5 = \langle (12345) \rangle$, $D_5 = \langle (12345), (14)(23) \rangle$, $F_{20} = \langle (12345), (1243) \rangle$.

Proof: The solvable cases follow from Lemma 2.4.2 and the nonsolvable cases follow from Lemma 2.6.2. ■

Lemma 2.6.5 *Let k be a field of characteristic 0. Let $\varphi(x)$ be an irreducible quintic polynomial in $k[x]$. Let M be the splitting field of $\varphi(x)$. Then*

- (i) $\text{Gal}(M/k) \subset D_5$ if and only if $\text{disc}(\varphi) \in k^2$ and $\varphi(x)$ is solvable by radicals over k .
- (ii) $\text{Gal}(M/k) = A_5$ if and only if $\text{disc}(\varphi) \in k^2$ and $\varphi(x)$ is not solvable by radicals over k .
- (iii) $\text{Gal}(M/k) = F_{20}$ if and only if $\text{disc}(\varphi) \notin k^2$ and $\varphi(x)$ is solvable by radicals over k .
- (iv) $\text{Gal}(M/k) = S_5$ if and only if $\text{disc}(\varphi) \notin k^2$ and $\varphi(x)$ is not solvable by radicals over k .

Proof: The assertion of the lemma follows from Lemmas 2.1.10 and 2.6.4. ■

Example 2.6.1 Let $\varphi(x) = x^5 - 5ax^3 + 5a^2x - b \in \mathbb{Q}[x]$ be irreducible. Here $\text{disc}(\varphi) = 5^5(4a^5 - b^2)^2$. Now we show that $\varphi(x)$ is solvable by radicals. In the equation

$$x^5 - 5ax^3 + 5a^2x - b = 0$$

set $x = u + v$ and $a = uv$, we can obtain the system of equations

$$\begin{cases} u^5 + v^5 = b \\ uv = a. \end{cases} \quad (2.15)$$

Clearly (2.15) is solvable by radicals so that $x^5 - 5ax^3 + 5a^2x - b$ is solvable by radicals. Hence $\text{Gal}(M/\mathbb{Q}) = F_{20}$.

Theorem 2.6.6 *Let k be a field of characteristic 0. Let $\tilde{\varphi}(x) = x^5 - t_1x^4 + t_2x^3 - t_3x^2 + t_4x - t_5$ be a general quintic polynomial with roots x_1, x_2, x_3, x_4, x_5 . Let $F = k(x_1, x_2, x_3, x_4, x_5)$ so that $\text{Gal}(F/k(t_1, \dots, t_5)) = S_5$. Let $\hat{D} = \text{disc}(\tilde{\varphi}(x))$ and set $K = k(t_1, \dots, t_5, \sqrt{\hat{D}})$ so that $\text{Gal}(F/K) = A_5$. Let $\hat{M}$ be the fixed field of D_5 . Then for any $\theta \in \hat{M} - K$, we have $\hat{M} = K(\theta)$. Let $\tilde{r}(x)$ be the monic irreducible polynomial of θ over K so that $\deg(\tilde{r}) = 6$.*

Now let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Then the map $x_i \longrightarrow \alpha_i, i = 1, 2, \dots, 5$ induces a homomorphism

$$h : F = k(x_1, x_2, x_3, x_4, x_5) \longrightarrow k(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

Under the homomorphism we have

$$\begin{aligned} \tilde{\varphi}(x) &\longrightarrow \varphi(x), & t_i &\longrightarrow a_i, & \hat{D} &\longrightarrow D = \text{disc}(\varphi), \\ \theta &\longrightarrow \gamma \text{ (say)}, & \tilde{r}(x) &\longrightarrow r(x) \text{ (say)}. \end{aligned}$$

Then $\varphi(x)$ is solvable by radicals over k if and only if $r(x)$ has a root in $k(\sqrt{D})$. More precisely, Let M be the splitting field of $\varphi(x)$ over k . Then

- (i) $\text{Gal}(M/k) \subset D_5$ if and only if $D \in k^2$ and $r(x)$ has a root in k .
- (ii) $\text{Gal}(M/k) = A_5$ if and only if $D \in k^2$ and $r(x)$ has no roots in k .
- (iii) $\text{Gal}(M/k) = F_{20}$ if and only if $D \notin k^2$ and $r(x)$ has a root in $k(\sqrt{D})$.
- (iv) $\text{Gal}(M/k) = S_5$ if and only if $D \notin k^2$ and $r(x)$ has no roots in $k(\sqrt{D})$.

Proof: Since $\text{Gal}(F/\hat{M}) = D_5$ is a solvable group, by Galois theory, $\tilde{\varphi}(x)$ is solvable by radicals over $\hat{M} = k(t_1, \dots, t_5, \sqrt{\hat{D}}, \theta)$ and thus $\varphi(x)$ is solvable by radicals over $M = k(\sqrt{D}, \gamma)$.

Now suppose that $r(x)$ has a root in $k(\sqrt{D})$. Without loss of generality we may assume that $\gamma \in k(\sqrt{D})$. Thus $\varphi(x)$ is solvable by radicals over $k(\sqrt{D}, \gamma) = k(\sqrt{D})$, consequently, $\varphi(x)$ is solvable by radicals over k .

Conversely, suppose that $\varphi(x)$ is solvable by radicals over k . Then $\text{Gal}(M/k)$ is a solvable transitive subgroup of S_5 . By Lemma 2.6.4, $\text{Gal}(M/k) = Z_5, D_5, F_{20}$. We consider two cases according as $\text{Gal}(M/k) \subset A_5$ or $\text{Gal}(M/k) \not\subset A_5$. (i) Suppose that $\text{Gal}(M/k) \subset A_5$. Then $\text{Gal}(M/k) = Z_5$ or D_5 . Since the general element θ is fixed by D_5 , γ is fixed by $\text{Gal}(M/k)$ as $\text{Gal}(M/k) \subset D_5$. Thus $\gamma \in k$.

(ii) Suppose that $\text{Gal}(M/k) \not\subset A_5$. Then $\text{Gal}(M/k) = F_{20}$. Note that as D_5 is the unique subgroup of index 2 in F_{20} and $[k(\sqrt{D}) : k] = 2$, we have $\text{Gal}(M/k(\sqrt{D})) = D_5$. Since the general element θ is fixed by D_5 , γ is fixed by $D_5 = \text{Gal}(M/k(\sqrt{D}))$, thus $\gamma \in k(\sqrt{D})$. Finally, appealing to Lemma 2.6.5, the assertions (i)-(iv) follow. ■

We see that

$$\theta = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_1x_4 + x_2x_5)$$

is fixed by $D_5 = \langle (12345), (14)(23) \rangle$ but not fixed by A_5 . Let $\hat{r}(x)$ be the monic irreducible polynomial of θ over K . By Theorem 2.6.6 we have

$$\hat{r}(x) = x^6 - B_1x^5 + B_2x^4 - B_3x^3 + B_4x^2 - B_5x + B_6 \in K[x]. \quad (2.16)$$

In the following Lemmas 2.6.7 and 2.6.8, we will express the coefficients B_i 's in terms of t_i 's. In order to do this, we set

$$\tau_1 = 1, \tau_2 = (234), \tau_3 = (432), \tau_4 = (345), \tau_5 = (543), \tau_6 = (24)(35).$$

It is easy to check that $C = \{\tau_i : 1 \leq i \leq 6\}$ is a set of coset representations of D_5 in A_5 , F_{20} in S_5 , namely,

$$A_5 = \bigcup_{i=1}^6 \tau_i D_5, \quad S_5 = \bigcup_{i=1}^6 \tau_i F_{20}.$$

The six conjugates of θ in $K = k(t_1, \dots, t_5, \sqrt{D})$ are following:

$$\begin{aligned} \theta_1 &= \theta = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_1x_4 + x_2x_5) \\ \theta_2 &= \tau_2(\theta) = (x_1x_3 + x_3x_4 + x_2x_4 + x_2x_5 + x_1x_5) - (x_1x_4 + x_2x_3 + x_4x_5 + x_1x_2 + x_3x_5) \\ \theta_3 &= \tau_3(\theta) = (x_1x_4 + x_2x_4 + x_2x_3 + x_3x_5 + x_1x_5) - (x_1x_2 + x_3x_4 + x_2x_5 + x_1x_3 + x_4x_5) \\ \theta_4 &= \tau_4(\theta) = (x_1x_2 + x_2x_4 + x_4x_5 + x_3x_5 + x_1x_3) - (x_1x_4 + x_2x_5 + x_3x_4 + x_1x_5 + x_2x_3) \\ \theta_5 &= \tau_5(\theta) = (x_1x_2 + x_2x_5 + x_3x_5 + x_3x_4 + x_1x_4) - (x_1x_5 + x_2x_3 + x_4x_5 + x_1x_3 + x_2x_4) \\ \theta_6 &= \tau_6(\theta) = (x_1x_4 + x_4x_5 + x_2x_5 + x_2x_3 + x_1x_3) - (x_1x_5 + x_2x_4 + x_3x_5 + x_1x_2 + x_3x_4) \end{aligned}$$

Set

$$S_i = x_1^i + x_2^i + x_3^i + x_4^i + x_5^i, \quad T_i = \theta_1^i + \theta_2^i + \theta_3^i + \theta_4^i + \theta_5^i + \theta_6^i.$$

Lemma 2.6.7

$$B_1 = B_3 = 0, \quad B_5^2 = 2^{10} \tilde{D},$$

where $\tilde{D} = \text{disc}(\tilde{r})$.

Proof: As

$$\begin{aligned} (12)\theta_1 &= (x_1x_2 + x_1x_3 + x_3x_4 + x_4x_5 + x_2x_5) - (x_2x_3 + x_1x_4 + x_3x_5 + x_2x_4 + x_1x_5) = -\theta_3 \\ (12)\theta_2 &= (x_2x_3 + x_3x_4 + x_1x_4 + x_1x_5 + x_2x_5) - (x_2x_4 + x_1x_3 + x_4x_5 + x_1x_2 + x_3x_5) = -\theta_4 \\ (12)\theta_5 &= (x_1x_2 + x_1x_5 + x_3x_5 + x_3x_4 + x_2x_4) - (x_2x_5 + x_1x_3 + x_4x_5 + x_2x_3 + x_1x_4) = -\theta_6 \\ (12)\theta_3 &= -\theta_1, \quad (12)\theta_4 = -\theta_2, \quad (12)\theta_6 = -\theta_5, \end{aligned}$$

for odd i we have

$$(12)T_i = (12)\sum_{j=1}^5 \theta_j = \sum_{j=1}^5 (12)\theta_j = -T_i. \quad (2.17)$$

Since $T_i \in K = k(t_1, \dots, t_5, \sqrt{\tilde{D}})$, we have

$$T_i = y + z\sqrt{\tilde{D}}, \text{ where } y, z \in k(t_1, \dots, t_5).$$

Then by (2.17) we have that

$$-y - z\sqrt{\tilde{D}} = -T_i = (12)T_i = (12)(y + z\sqrt{\tilde{D}}) = y - z\sqrt{\tilde{D}},$$

so that $y = 0$ and $T_i = z\sqrt{\tilde{D}}$. Note that as T_1 , T_3 and $\sqrt{\tilde{D}}$ are polynomials in $k[x_1, \dots, x_5]$ and

$$\deg(T_1) = 2, \quad \deg(T_3) = 6, \quad \deg(\sqrt{\tilde{D}}) = 10,$$

we have $z = 0$ so that $T_1 = T_3 = 0$. For $i = 5$, as $\deg(T_5) = \deg(\sqrt{\tilde{D}}) = 10$, we have $z \in k$. Taking $(x_1, x_2, x_3, x_4, x_5) = (1, -1, 2, -2, 0)$ we have

$$z^2 = T_5^2 / \tilde{D} = 2^{10} 5^2.$$

Finally, by Lemma 2.6.1 we have

$$B_1 = T_1 = 0, \quad B_3 = (T_3 - T_2B_1 + T_1B_2)/3 = 0,$$

$$B_5 = (T_5 - T_4B_1 + T_3B_2 - T_2B_3 + T_1B_4)/5 = T_5/5. \quad \blacksquare$$

Let $\delta = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$, $\delta' = x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2$ so that $\theta = \delta - \delta'$ and $t_2 = \delta + \delta'$. We have the following identities:

$$\begin{aligned} (\delta - \delta')^2 &= 2(\delta^2 + \delta'^2) - 2t_2, \\ (\delta - \delta')^4 &= 4(\delta^2 + \delta'^2)^2 - 4t_2^2(\delta^2 + \delta'^2) + t_2^4, \\ (\delta - \delta')^6 &= 8(\delta^2 + \delta'^2)^3 - 12t_2^2(\delta^2 + \delta'^2)^2 + 6t_2^4(\delta^2 + \delta'^2) - t_2^6, \\ (\delta^2 + \delta'^2)^2 &= 2(\delta^4 + \delta'^4) - 2t_2^2(\delta^2 + \delta'^2) + t_2^4, \\ (\delta^2 + \delta'^2)^3 &= 4(\delta^6 + \delta'^6) - 6t_2^2(\delta^2 + \delta'^2)^2 + 3t_2^4(\delta^2 + \delta'^2). \end{aligned} \quad (2.18)$$

By the above identities, in order to compute the coefficients B_2 , B_4 and B_6 , we need only compute the following

$$\Delta_i = \sum_{j=1}^6 \tau_j(\delta^i + \delta'^i), \quad i = 2, 4, 6.$$

Note that as

$$\delta = \sum_{\sigma \in Z_5} \sigma(x_1x_2), \quad \delta' = \sum_{\sigma \in Z_5} \sigma(x_1x_3),$$

where $Z_5 = \langle (12345) \rangle$, we have

$$\delta^i + \delta'^i = \sum_{t=0}^i \binom{i}{t} \sum_{\sigma \in Z_5} \sigma(w(i, t)),$$

thus, we need to compute the sum:

$$S(i, t) = \sum_{j=1}^6 \tau_j \left(\sum_{\sigma \in Z_5} \sigma(w(i, t)) \right), \quad (2.19)$$

As

$$\begin{aligned} \tau_1 Z_5 &= Z_5 \\ \tau_2 Z_5 &= (234)Z_5 = \{(234), (13245), (14)(35), (12543), (152)\}, \\ \tau_3 Z_5 &= (432)Z_5 = \{(432), (145), (12354), (13)(25), (15342)\}, \\ \tau_4 Z_5 &= (345)Z_5 = \{(345), (12435), (14)(25), (15423), (132)\}, \\ \tau_5 Z_5 &= (543)Z_5 = \{(543), (125), (15234), (13)(24), (14532)\}, \\ \tau_6 Z_5 &= (24)(35)Z_5 = \{(24)(35), (14325), (154), (123), (13542)\}, \end{aligned}$$

and

$$Z_5\tau_1 = Z_5$$

$$Z_5\tau_2 = Z_5(234) = \{(234), (12435), (13)(25), (14532), (154)\},$$

$$Z_5\tau_3 = Z_5(432) = \{(432), (125)(13452), (14)(35), (15432)\},$$

$$Z_5\tau_4 = Z_5(345) = \{(345), (12354), (13)(24), (14325), (152)\},$$

$$Z_5\tau_5 = Z_5(543) = \{(543), (123), (13245), (14)(25), (15342)\},$$

$$Z_5\tau_6 = Z_5(24)(35) = \{(24)(35), (12543), (132), (145), (15234)\},$$

we see that we can interchange the order of the sums in (2.19), that is,

$$S(i, t) = \sum_{\sigma \in Z_5} \sigma \left(\sum_{j=1}^6 \tau_j(w(i, t)) \right). \quad (2.20)$$

The following formulae will be used in computation of B_2 , B_4 and B_6 . Set $R_n = x_2^n + x_3^n + x_4^n + x_5^n$ and $S(n, n') = S_n S_{n'} - S_{n+n'}$. We have

$$\sum_{1 \leq i < j \leq 5} x_i^n x_j^n = \frac{1}{2} S(n, n) \quad (2.21)$$

$$\sum_{2 \leq i < j \leq 5} x_i^n x_j^n = \frac{1}{2} S(n, n) - S_n x_1^n + 2x_1^{2n} \quad (2.22)$$

$$R_n R_m - R_{n+m} = S(n, m) - S_n x_1^m - S_m x_1^n + 2x_1^{n+m} \quad (2.23)$$

$$\begin{aligned} \sum_{i=2}^5 x_i^m (x_3^n x_4^n + x_3^n x_5^n + x_4^n x_5^n) &= \frac{1}{2} (S(n, n) S_m - S(n, n+m)) \\ &- S(n, m) x_1^n - \frac{1}{2} S(n, n) x_1^m + S_m x_1^{2n} + 2S_n x_1^{n+m} - 3x_1^{2n+m} \end{aligned} \quad (2.24)$$

$$\begin{aligned} \sum_{i=2}^5 x_i^k (x_3^n x_4^m + x_3^n x_5^m + x_4^n x_5^m + x_3^m x_4^n + x_3^m x_5^n + x_4^m x_5^n) \\ = S(n, m) S_k - S(n, k+m) - S(m, k+n) + 2S_k x_1^{n+m} + 2S_m x_1^{k+n} \\ + 2S_n x_1^{k+m} - 6x_1^{k+n+m} - S(k, n) x_1^m - S(k, m) x_1^n - S(n, m) x_k \end{aligned} \quad (2.25)$$

Let's now compute Δ_2 to illustrate our idea. Since

$$\begin{aligned} \delta^2 + \delta'^2 &= \sum_{\sigma \in Z_5} \sigma(x_1^2 x_2^2 + 2(x_1 x_2^2 x_3 + x_1 x_2 x_3 x_4)) \\ &\quad + \sum_{\sigma \in Z_5} \sigma(x_1^2 x_3^2 + 2(x_1^2 x_3 x_4 + x_1 x_2 x_3 x_4)) \\ &= \sum_{\sigma \in Z_5} \sigma(x_1^2 x_2^2 + x_1^2 x_3^2 + 4x_1 x_2 x_3 x_4) + 2 \sum_{\sigma \in Z_5} \sigma(x_1^2 (x_2 x_5 + x_3 x_4)) \\ &= \sum_{\sigma \in Z_5} \sigma(w_1) + 2 \sum_{\sigma \in Z_5} \sigma(w_2), \end{aligned}$$

where

$$w_1 = x_1^2 x_2^2 + x_1^2 x_3^2 + 4x_1 x_2 x_3 x_4, \quad w_2 = x_1^2 (x_2 x_5 + x_3 x_4).$$

For w_1 , apply directly (2.19), we have

$$\begin{aligned}
& \sum_{i=1}^6 \tau_i(\sum_{\sigma \in Z_6} \sigma(w_1)) \\
&= \sum_{i=1}^6 \tau_i(\sum_{\sigma \in Z_6} \sigma(x_1^2 x_2^2 + x_1^2 x_3^2)) + 4 \sum_{i=1}^6 \tau_i(\sum_{\sigma \in Z_6} \sigma(x_1 x_2 x_3 x_4)) \\
&= \sum_{i=1}^6 \tau_i(\frac{1}{2}(S_2^2 - S_4)) + 4 \sum_{i=1}^6 \tau_i(t_4) \\
&= 3(S_2^2 - S_4) + 24t_4.
\end{aligned}$$

For w_2 , apply (2.20), we have

$$\begin{aligned}
\sum_{j=1}^6 \tau_j(\sum_{\sigma \in Z_6} \sigma(w_2)) &= \sum_{\sigma \in Z_6} \sigma(\sum_{j=1}^6 \tau_j(x_1^2(x_2 x_5 + x_3 x_4))) \\
&= \sum_{\sigma \in Z_6} \sigma(2x_1^2(t_2 - t_1 x_1 + x_1^2)) \\
&= 2(t_2 S_2 - t_1 S_3 + S_4) = 2(t_1 t_3 - 4t_4).
\end{aligned}$$

Thus

$$\Delta_2 = 3(S_2^2 - S_4) + 24t_4 + 4(t_1 t_3 - 4t_4) = 3(S_2^2 - S_4) + 4(t_1 t_3 + 2t_4).$$

Lemma 2.6.8 *We have*

$$\begin{aligned}
\Delta_2 &= 3(S_2^2 - S_4) + 4(t_1 t_3 + 2t_4), \\
\Delta_4 &= 3(S_4^2 - S_8) + 8(t_4(S_2^2 - S_4) - 2t_5(S_1 S_2 - S_3) + (S_1 S_3 - S_4) \\
&\quad - (S_3 S_5 - S_8) - (S_1 S_7 - S_8) \\
&\quad + 6((S_2^2 - S_4)S_4 - 2(S_2 S_6 - S_8) + 12(t_4^2 - 2t_3 t_5)) \\
&\quad + 12((S_1 S_2 - S_3)S_2 - (S_1 S_4 - S_5) - (S_2 S_3 - S_5))S_3 + 4(S_2 S_6 - S_8) + 2(S_1 S_7 - S_8) \\
&\quad - (S_2^2 - S_4)S_4 - 2(S_1 S_2 - S_3)S_5 \\
&\quad + (S_2^2 - S_4)t_4 + (S_1^2 - S_2)S_1 t_5 + 2(S_1 S_2 - S_3)t_5 \\
&\quad + 144t_3 t_5, \\
\Delta_6 &= 3(S_6^2 - S_{12}) + 12(S_4^2 - S_8)t_4 - 2t_5(S_3 S_4 - S_7) + (S_1 S_5 - S_6)S_6 - (S_5 S_7 - S_{12}) \\
&\quad - (S_1 S_{11} - S_{12})) + 30(S_2^2 - S_4)(t_4^2 - 2t_3 t_5) - 8S_2 t_5^2 + (S_2 S_4 - S_6)S_6 \\
&\quad - (S_4 S_8 - S_{12}) - (S_2 S_{10} - S_{12}) + 20((S_3^2 - S_6)S_6 - 2(S_3 S_9 - S_{12})) \\
&\quad - 10(3S_6(S_3^2 - S_6) - 6(S_3 S_9 - S_{12}) + 2S_3(S_3 S_6 - S_9) - 3S_3^2(S_3^2 - S_6)) \\
&\quad + 30((S_1 S_2 - S_3)S_4 - (S_1 S_6 - S_7) - (S_2 S_5 - S_7))S_5 + 2(S_4 S_8 - S_{12}) \\
&\quad + 2(S_2 S_{10} - S_{12}) + 2(S_1 S_{11} - S_{12})
\end{aligned}$$

$$\begin{aligned}
 & -(S_2S_4 - S_6)S_8 - (S_1S_4 - S_5)S_7 - (S_1S_2 - S_3)S_9 \\
 & + (S_4^2 - S_8)t_4 + (S_3^2 - S_6)S_1t_5 + 2(S_3S_4 - S_7)t_5 \\
 & + 60(((S_1S_2 - S_3)(S_4 + t_4) - (S_1S_6 - S_7) - (S_2S_5 - S_7) \\
 & - (S_1^2 + 3S_2)t_5 + 3(t_3t_4 - 3t_2t_5)) \times 2t_5) \\
 & + ((S_2^2 - S_4)S_4 - 2(S_2S_6 - S_8))t_4 + (2(S_3S_4 - S_7) \\
 & + 4(S_2S_5 - S_7) - 2(S_2S_4 - S_6)S_1 - (S_2^2 - S_4)S_3)t_5 \\
 & + 2(t_1t_3 - 4t_4)(t_4^2 - 2t_3t_5) - 2(t_1t_2 - 3t_3)t_4t_5 + 8t_1^2t_5^2 \\
 & - 18t_2t_5^2 + ((S_1S_2 - S_3)S_4 - (S_1S_6 - S_7) - (S_2S_5 - S_7)S_5 \\
 & + 2(S_4S_8 - S_{12}) + 2(S_2S_{10} - S_{12}) - 2(S_1S_{11} - S_{12}) \\
 & - (S_2S_4 - S_6)S_8 - (S_1S_4 - S_5)S_7 - (S_1S_2 - S_3)S_9) \\
 & + 240(6t_2t_5 - 4t_1^2t_5 + (t_1t_2 - 3t_3)t_4 + (S_3^2 - S_6)S_1 - 2(S_3S_4 - S_7)t_5 \\
 & + 90((S_2^2 - S_4)(t_4^2 - 2t_3t_5) + 4S_2t_5^2) \\
 & + 180((6t_2t_5 - 4t_1^2t_5 + (t_1t_2 - 3t_3)t_4 + 3(t_3t_4 - 3t_2t_5) \times 2t_5 \\
 & + (S_2^2 - S_4)S_3 - 2(S_2S_5 - S_7) + 6t_2t_5^2) \\
 & + 360 \times 6t_2t_5^2.
 \end{aligned}$$

Theorem 2.6.9 *Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Let*

$$y = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1.$$

$$y' = \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_5 + \alpha_1\alpha_4 + \alpha_2\alpha_5,$$

$$\gamma = y - y'.$$

Let $r(x)$ be the monic irreducible polynomial of γ over k . Let M be the splitting field of $\varphi(x)$ over k . Let $D = \text{disc}(\varphi)$. Then

- (i) $\text{Gal}(M/k) \subset D_5$ if and only if $D \in k^2$ and $r(x)$ has a root in k .
- (ii) $\text{Gal}(M/k) = A_5$ if and only if $D \in k^2$ and $r(x)$ has no roots in k .
- (iii) $\text{Gal}(M/k) = F_{20}$ if and only if $D \notin k^2$ and $r(x)$ has a root in $k(\sqrt{D})$.
- (iv) $\text{Gal}(M/k) = S_5$ if and only if $D \notin k^2$ and $r(x)$ has no roots in $k(\sqrt{D})$.

Further,

$$s_1 = \alpha_1^1 + \alpha_2^1 + \alpha_3^1 + \alpha_4^1 + \alpha_5^1.$$

We have

$$r(x) = x^6 + b_2x^4 + b_4x^2 + 2^5 \cdot \sqrt{D} x + b_6,$$

where b_2 , b_4 and b_6 can be obtained by in Lemma 2.6.8 and the identities (2.18) just replacing S_i by s_i , t_i by a_i , Δ_i by $\sum_{j=1}^6 \tau_j(y^i + y^{\bar{i}})$, δ by y and δ' by y' .

For the particular case when $\varphi(x) = x^5 + ax + b$, we have

$$r(x) = x^6 - 20ax^4 + 240a^2x^2 + 2^5\sqrt{(4^4a^5 + 5^5b^4)} + 320a^3.$$

Note that in this case $\varphi(x)$ has at least one pair of complex roots so that $\text{Gal}(M/Q) \neq Z_5$. Thus we have the following:

Corollary 2.6.10 *Let $\varphi(x) = x^5 + ax + b \in k[x]$ be an irreducible quintic polynomial. Let M be the splitting field of $\varphi(x)$. Let*

$$r(x) = x^6 - 20ax^4 + 240a^2x^2 + 2^5\sqrt{4^4a^5 + 5^5b^4}x + 320a^3.$$

Then $\text{Gal}(M/k) = D_5$ if and only if $4^4a^5 + 5^5b^4 \in k^2$ and $r(x)$ has a root k .

Example 2.6.2 $\varphi(x) = x^5 - 5x + 12$, whose discriminant is $2^{12}5^6$. The corresponding resolvent $r(x)$ is

$$r(x) = x^6 + 100x^4 + 6000x^2 + 256000x - 40000,$$

which has $x = -10$ as a root. It follows that the Galois group of $\varphi(x)$ is the dihedral group D_5 .

Example 2.6.3 Let $\rho_q(x)$ be the following quintics

q	quintic $\rho_q(x)$	$\text{disc}(\rho_q)$
119	$x^5 - x^4 - x^2 + 3x - 1$	119^2
143	$x^5 - x^4 - x^3 + 3x - 1$	143^2
159	$x^5 + x^3 - 3x^2 + x - 3$	$3^2 \cdot 159^2$

303	$x^5 + 3x^3 + x^2 + 3x - 3$	$3^2 \cdot 303^2$
319	$x^5 + x^4 - x^3 + 3x^2 + 6x - 1$	$3^2 \cdot 319^2$
611	$x^5 - 3x^3 - x^2 + 7x - 5$	611^2
635	$x^5 - x^4 + 2x^3 - 3x^2 - 3x - 5$	$3^2 \cdot 635^2$

The corresponding $r_q(x)$ (as in Theorem 2.6.9) and the integral root r_q of $r_q(x)$ are given in the following table:

q	quintic $r_q(x)$	r_q
119	$x^6 - 52x^4 + 1376x^2 + 2^5 \cdot 119x + 2432$	-4
143	$x^6 - 63x^4 + 1787x^2 + 2^5 \cdot 143x + 2019$	-3
159	$x^6 - 23x^4 - 3221x^2 + 2^5 \cdot 477x + 17739$	-9
303	$x^6 - 87x^4 + 3435x^2 + 2^5 \cdot 909x + 126539$	-7
319	$x^6 - 99x^4 + 7939x^2 + 2^5 \cdot 957x + 27711$	-3
611	$x^6 - 167x^4 + 9451x^2 + 2^5 \cdot 611x - 316645$	7
635	$x^6 + 72x^4 - 464x^2 + 2^5 \cdot 1905x + 242496$	-6

By Theorem 2.6.9, the Galois group of each $\rho_q(x)$ is D_5 .

Similarly, if θ is a general element in $k(x_1, x_2, \dots, x_5)$ fixed by F_{20} but not fixed by S_5 , using the same kind of argument in Theorem 2.6.6, we can obtain the following results(Theorems 2.6.11 and 2.6.12 below).

Theorem 2.6.11 *Let k be a field of characteristic 0. Let $\tilde{\varphi}(x) = x^5 - t_1x^4 + t_2x^3 - t_3x^2 + t_4x - t_5$ be a general quintic polynomial with roots x_1, x_2, x_3, x_4, x_5 . Let $F = k(x_1, x_2, x_3, x_4, x_5)$ and $K = k(t_1, \dots, t_5)$ so that $\text{Gal}(F/k(t_1, \dots, t_5)) = S_5$. Let $\tilde{M}$ be the fixed field of F_{20} . Then for any $\theta \in \tilde{M} - K$, we have $\tilde{M} = K(\theta)$. Let $\tilde{r}(x)$ be the monic irreducible polynomial of θ over K so that $\deg(\tilde{r}) = 6$.*

Now let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Then the map $x_i \longrightarrow \alpha_i, i = 1, 2, \dots, 5$ induces a homomorphism

$$h : F = k(x_1, x_2, x_3, x_4, x_5) \longrightarrow k(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

Under the homomorphism we have

$$\begin{aligned}\tilde{\varphi}(x) &\longrightarrow \varphi(x), & t_i &\longrightarrow a_i, & \text{disc}(\tilde{\varphi}(x)) &\longrightarrow D = \text{disc}(\varphi), \\ \theta &\longrightarrow \gamma \text{ (say)}, & \tilde{r}(x) &\longrightarrow r(x) \text{ (say)}.\end{aligned}$$

Then $\varphi(x)$ is solvable by radicals over k if and only if $r(x)$ has a root in k . More precisely, Let M be the splitting field of $\varphi(x)$ over k . Then

- (i) $\text{Gal}(M/k) \subset D_5$ if and only if $D \in k^2$ and $r(x)$ has a root in k .
- (ii) $\text{Gal}(M/k) = A_5$ if and only if $D \in k^2$ and $r(x)$ has no roots in k .
- (iii) $\text{Gal}(M/k) = F_{20}$ if and only if $D \notin k^2$ and $r(x)$ has a root in k .
- (iv) $\text{Gal}(M/k) = S_5$ if and only if $D \notin k^2$ and $r(x)$ has no roots in k .

Proof: Since $\text{Gal}(F/\tilde{M}) = F_{20}$ is a solvable group, by Galois theory, $\tilde{\varphi}(x)$ is solvable by radicals over $\tilde{M} = K(\theta)$ and thus $\varphi(x)$ is solvable by radicals over $k(\gamma)$.

Now suppose that $r(x)$ has a root in k . Without loss of generality we may assume that $\gamma \in k$. Thus $\varphi(x)$ is solvable by radicals over $k(\gamma) = k$.

Conversely, suppose that $\varphi(x)$ is solvable by radicals over k . Then $\text{Gal}(M/k)$ is a solvable transitive subgroup of S_5 . By Lemma 2.6.4, $\text{Gal}(M/k) = Z_5, D_5, F_{20}$. Since the general element θ is fixed by F_{20} , γ is fixed by $\text{Gal}(M/k)$ as $\text{Gal}(M/k) \subset F_{20}$. Thus $\gamma \in k$. This completes the proof. ■

We see that

$$\theta = ((x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2))^2$$

is fixed by $F_{20} = \langle (12345), (1243) \rangle$ but not fixed by S_5 , so that we have the following:

Theorem 2.6.12 Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Let

$$\gamma = ((\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_5 + \alpha_5\alpha_1) - (\alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_5 + \alpha_4\alpha_1 + \alpha_5\alpha_2))^2,$$

and let $r(x)$ be the monic irreducible polynomial of γ over k . Then

$$r(x) = (x^3 + b_2x^2 + b_4x + b_6)^2 - 2^{10}Dx,$$

where b_2, b_4, b_6 are given in Theorem 2.6.9. Let $D = \text{disc}(\varphi(x))$. Let M be the splitting field of $\varphi(x)$ over k . Then

- (i) $\text{Gal}(M/k) \subset D_5$ if and only if $D \in k^2$ and $r(x)$ has a root in k .
- (ii) $\text{Gal}(M/k) = A_5$ if and only if $D \in k^2$ and $r(x)$ has no roots in k .
- (iii) $\text{Gal}(M/k) = F_{20}$ if and only if $D \notin k^2$ and $r(x)$ has a root in k .
- (iv) $\text{Gal}(M/k) = S_5$ if and only if $D \in k^2$ and $r(x)$ has no roots in k .

For the particular case when $\varphi(x) = x^5 + ax + b$, we have

$$r(x) = (x^3 - 20ax^2 + 240a^2x + 320a^3)^2 - 2^{10}(4^4a^5 + 5^5b^4)x.$$

Note that in this case $\varphi(x)$ has at least one pair of complex roots so that $\text{Gal}(M/Q) \neq Z_5$. Thus we have the following:

Corollary 2.6.13 *Let $\varphi(x) = x^5 + ax + b \in Q[x]$ be an irreducible quintic polynomial. Let M be the splitting field of $\varphi(x)$. Let*

$$r(x) = (x^3 - 20ax^2 + 240a^2x + 320a^3)^2 - 2^{10}(4^4a^5 + 5^5b^4).$$

Then $\text{Gal}(M/Q) = D_5$ if and only if $4^4a^5 + 5^5b^4 \in k^2$ and $r(x)$ has a root in k .

Example 2.6.4 $\varphi(x) = x^5 + 11x + 44$. The corresponding resolvent $r(x)$ is

$$r(x) = (x^3 - 220x^2 + 29040x + 425910)^2 - 12036130000000,$$

which has $x = 484$ as a root. It follows that the Galois group of $\varphi(x)$ is the dihedral group D_5 .

We now give some further examples of quintic polynomials with Galois group D_5 . These are the polynomials $\rho(x)$ given in the following table.

Example 2.6.5 Let $\varphi_q(x)$ be one the following quintic polynomials.

q	quintic $\rho_q(x)$	$\text{disc}(\rho_q)$
<hr/>		

47	$x^5 - x^3 - 2x^2 - 2x - 1$	47^2
79	$x^5 + 2x^4 - 3x^2 - 2x - 1$	79^2
103	$x^5 - x^4 - 3x^3 - 3x^2 - 2x - 1$	103^2
127	$x^5 - 3x^4 - x^3 + 2x^2 + x - 1$	127^2
131	$x^5 + x^4 + 2x^3 + x^2 + x - 2$	$2^2 \cdot 131^2$
179	$x^5 + x^4 - 3x^2 - x - 2$	$2^2 \cdot 179^2$
227	$x^5 - x^3 + 2x^2 + 3x - 4$	$2^4 \cdot 227^2$
347	$x^5 + 2x^4 + 3x^3 - 4x^2 - x - 2$	$2^4 \cdot 347^2$
443	$x^5 - x^4 - x^3 + 5x^2 + 3x - 5$	$2^4 \cdot 443^2$
523	$x^5 + x^4 + 3x^3 - 5x^2 - x - 3$	$2^4 \cdot 523^2$
571	$x^5 + x^4 - 2x^3 - 7x^2 - 3x - 2$	$2^2 \cdot 571^2$
619	$x^5 + x^4 + 4x^3 + 5x^2 + 3x - 2$	$2^2 \cdot 619^2$
691	$x^5 - 2x^4 + 3x^3 - 8x^2 - x - 6$	$2^4 \cdot 691^2$
739	$x^5 - 5x^4 + 6x^3 + 3x^2 + x - 2$	$2^2 \cdot 739^2$
787	$x^5 - 3x^3 - 3x^2 - 2x - 9$	$2^6 \cdot 787^2$

The corresponding $r_q(x)$ (as in Theorem 2.6.12) and the integral root x_q of $r_q(x)$ are given in the following table:

q	quintic $r_q(x)$	x_q
47	$(x^3 + 37x^2 + 115x - 247)^2 - 2^{10} \cdot 47^2$	9
79	$(x^3 - 8x^2 - 496x - 3264)^2 - 2^{10} \cdot 79^2$	36
103	$(x^3 + 37x^2 - 589x - 7545)^2 - 2^{10} \cdot 103^2$	25
127	$(x^3 - 71x^2 - 227x - 6597)^2 - 2^{10} \cdot 103^2$	81
131	$(x^3 - 24x^2 + 128x + 30144)^2 - 2^{12} \cdot 131^2$	36
179	$(x^3 - 4x^2 - 2224x - 11776)^2 - 2^{12} \cdot 179^2$	64
227	$(x^3 - 63x^2 + 5275x - 21469)^2 - 2^{14} \cdot 227^2$	49

347	$(x^3 - 71x^2 - 2645x - 104421)^2 - 2^{14} \cdot 347^2$	9
443	$(x^3 - 103x^2 + 12331x + 23995)^2 - 2^{14} \cdot 443^2$	25
523	$(x^3 - 47x^2 - 5701x - 61197)^2 - 2^{14} \cdot 523^2$	1
571	$(x^3 - 8x^2 - 4800x - 74560)^2 - 2^{12} \cdot 571^2$	100
619	$(x^3 - 68x^2 + 3984x + 108032)^2 - 2^{12} \cdot 619^2$	16
691	$(x^3 + 121x^2 - 6613x + 516315)^2 - 2^{14} \cdot 691^2$	25
739	$(x^3 - 248x^2 + 21824x - 227136)^2 - 2^{12} \cdot 739^2$	36
787	$(x^3 + 13x^2 - 9885x - 908401)^2 - 2^{16} \cdot 787^2$	169

By Theorem 2.6.12 we have $\text{Gal}(M/Q) = Z_5$ or D_5 . By Lemma 2.6.3, if $\text{Gal}(M/Q) = Z_5$ then $d_M \in Z^4$. This is impossible as in this case we have $D_M \mid \text{disc}(\rho_q)$. Hence $\text{Gal}(M/Q) = D_5$.

In [12], D.S. Dummit chose

$$\begin{aligned} \theta = & x_1^2 x_2 x_5 + x_1^2 x_3 x_4 + x_2^2 x_1 x_3 + x_2^2 x_4 x_5 + x_3^2 x_1 x_5 \\ & + x_3^2 x_2 x_4 + x_4^2 x_1 x_2 + x_4^2 x_3 x_5 + x_5^2 x_1 x_4 + x_5^2 x_2 x_3 \end{aligned}$$

which is fixed by F_{20} , and obtained the following result:

Theorem 2.6.14 *The irreducible quintic $f(x) = x^5 + px^3 + qx^2 + rx + s \in Q[x]$ is solvable by radicals if and only if the polynomial $f_{20}(x)$ below has a rational root. If this is the case, the sextic $f_{20}(x)$ factors into the product of a linear polynomial and an irreducible quintic over Q .*

$$\begin{aligned} f_{20}(x) = & x^6 + 8rx^5 + (2pq^2 - 6p^2r + 40r^2 - 50qrs)x^4 \\ & + (-2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 150p^2qs - 400qrs + 125ps^2)x^3 \\ & + (p^2q^4 - 6p^3q^2r - 8q^4r + 9p^4r^2 + 76pq^2r^2 - 136p^2r^3 + 400r^4 \\ & - 50pq^3s + 90p^2qrs - 1400qr^2s + 625q^2s^2 + 500prs^2)x^2 \\ & + (-2pq^6 + 19p^2q^4r - 51p^3q^2r^2 + 3q^4r^2 + 32p^4r^3 + 76pq^2r^3 \\ & - 250p^2r^4 + 512r^2 - 31p^3q^3s - 58q^5s + 117p^4qrs + 105pq^3rs \\ & 260p^2qr^2s - 2400qr^3s - 108p^5s^2 - 325p^2q^2s^2 + 525p^3rs^2 \\ & + 2750q^2rs^2 - 500pr^2s^2 + 625pqs^3 - 3125s^4)x \end{aligned}$$

$$\begin{aligned}
& +(q^8 - 13pq^6r + p^5q^2r^2 + 65p^2q^4r^2 - 4p^6r^3 - 128p^3q^2r^3 + 17q^4r^3 \\
& + 48p^4r^4 - 16pq^2r^4 - 192p^2r^5 + 256r^6 - 4p^5q^3s - 12p^2q^5s + 18p^6qrs \\
& + 12p^3q^3rs - 124q^5rs + 196p^4qr^2s + 590pq^3r^2s - 160p^2qr^3s - 1600qr^4s \\
& - 27p^7s^2 - 150p^4q^2s^2 - 125pq^4s^2 - 99p^5rs^2 - 725p^2q^2rs^2 + 1200p^3r^2s^2 \\
& + 3250q^2r^2s^2 - 2000pr^3s^2 - 1250prs^3 + 3125p^2s^4 - 9375rs^4).
\end{aligned}$$

For the particular case when $f(x) = x^5 + ax + b$, the polynomial $f_{20}(x)$ is simply

$$\begin{aligned}
f_{20}(x) = & x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 \\
& + (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4).
\end{aligned}$$

Lemma 2.6.15 *Let k be a field of characteristic 0. Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 be the five roots of $\varphi(x)$. Let $r(x)$ be the polynomial of degree 10 given by*

$$r(x) = \prod_{1 \leq i < j \leq 5} (x - (\alpha_i + \alpha_j)).$$

Then $r(x)$ and $\varphi(x)$ have the same splitting field over k . Further, if $\varphi(x)$ is irreducible, then the ten elements $\alpha_i + \alpha_j$ ($1 \leq i < j \leq 5$) are distinct.

Proof: Since $\alpha_1 = a_1 - (\alpha_2 + \alpha_3) - (\alpha_4 + \alpha_5)$ and since similar equations are satisfied by $\alpha_2, \alpha_3, \alpha_4, \alpha_5$, it follows that $r(x)$ and $\varphi(x)$ have the same splitting field over k .

Now suppose $\varphi(x)$ is irreducible. Then $\varphi(x)$ is a separable polynomial. Let M be the splitting field of $\varphi(x)$. Since $\varphi(x)$ is irreducible, by Lemma 2.1.10, $\text{Gal}(M/k)$ is a transitive subgroup of S_5 . In particular, $\text{Gal}(M/k)$ contains a 5-cycle, say, $\sigma = (12345)$. Suppose the assertion of Lemma is not true. Then at least one of the following three equalities holds

$$(i) \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \quad (ii) \alpha_1 + \alpha_3 = \alpha_2 + \alpha_4 \quad (iii) \alpha_1 + \alpha_2 = \alpha_3 + \alpha_5.$$

(i) Suppose $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. Applying σ^2 to both sides of the equality, we have $\alpha_3 + \alpha_4 = \alpha_5 + \alpha_1$ and thus $\alpha_2 = \alpha_5$. This is a contradiction as $\varphi(x)$ is a separable polynomial.

(ii) Suppose $\alpha_1 + \alpha_3 = \alpha_2 + \alpha_4$. Applying σ to both sides of the equality, we have $\alpha_2 + \alpha_4 = \alpha_3 + \alpha_5$ and thus $\alpha_1 = \alpha_5$. This is a contradiction as $\varphi(x)$ is a separable polynomial.

(iii) Suppose $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_5$. Consider the system of 5 linear equations in $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$:

$$\begin{cases} \sigma^i(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_5) = 0, & 0 \leq i \leq 3 \\ \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = a_1. \end{cases}$$

The determinant of this system of equations is not zero, this implies that α_i ($1 \leq i \leq 5$) are in k . This is a contradiction as $\varphi(x)$ is irreducible over k .

Theorem 2.6.16 *Let k be a field of characteristic 0. Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 be the five roots of $\varphi(x)$. Set*

$$r(x) = \prod_{1 \leq i < j \leq 5} (x - (\alpha_i + \alpha_j)).$$

Let M be the splitting field of $\varphi(x)$. Then

$$\text{Gal}(M/k) \subset D_5 \iff r(x) \text{ is reducible.}$$

If this is the case, the $r(x)$ factors into the product of two irreducible quintics over k .

Proof: Suppose $\text{Gal}(M/k) \subset D_5$. Without loss of generality we may suppose that $D_5 = \langle (12345), (14)(23) \rangle$, and let $\sigma = (12345)$. Let $S = \{\alpha_i + \alpha_j : 1 \leq i < j \leq 5\}$. Under the action of D_5 , S is divided into two orbits, namely,

$$\begin{aligned} &\{\alpha_1 + \alpha_2, \sigma(\alpha_1 + \alpha_2), \sigma^2(\alpha_1 + \alpha_2), \sigma^3(\alpha_1 + \alpha_2), \sigma^4(\alpha_1 + \alpha_2)\} \\ &\{\alpha_1 + \alpha_3, \sigma(\alpha_1 + \alpha_3), \sigma^2(\alpha_1 + \alpha_3), \sigma^3(\alpha_1 + \alpha_3), \sigma^4(\alpha_1 + \alpha_3)\} \end{aligned}$$

Let

$$r_1(x) = \prod_{0 \leq i \leq 4} (x - \sigma^i(\alpha_1 + \alpha_2)), \quad r_2(x) = \prod_{0 \leq i \leq 4} (x - \sigma^i(\alpha_1 + \alpha_3)).$$

By Galois theory, $r_1(x), r_2(x) \in k[x]$. By Lemma 2.6.15, both $r_1(x)$ and $r_2(x)$ have no repeated roots. Then appealing to Lemma 2.1.10, $r(x)$ is irreducible over k .

Conversely, suppose $\text{Gal}(M/k) \not\subset D_5$. Then, by Lemma 2.6.4, $\text{Gal}(M/k) = F_{20}, A_5$ or S_5 . Note that as each of F_{20} , A_5 and S_5 acts transitively on the set S , by Lemma 2.1.10, $r(x)$ is irreducible.

Corollary 2.6.17 *Let k be a field of characteristic 0. Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in k[x]$ be irreducible. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 be the five roots of $\varphi(x)$. Set*

$$r(x) = \prod_{1 \leq i < j \leq 5} (x - (\alpha_i + \alpha_j)).$$

Suppose that $\text{disc}(\varphi)$ is a nonsquare in k . Let $K = k(\sqrt{\text{disc}(\varphi)})$. Let M be the splitting field of $\varphi(x)$. Then

$$\text{Gal}(M/k) = F_{20} \iff r(x) \text{ is reducible over } K.$$

If this is the case, the $r(x)$ factors into the product of two irreducible quintics over K .

Proof: Since $\text{disc}(\varphi)$ is a nonsquare in k , $\text{Gal}(M/Q) = F_{20}$ or S_5 and $\text{Gal}(M/K) = D_5$ or A_5 . Then appealing to the lemma, the assertion of the corollary follows.

Lemma 2.6.18 *Let $\varphi(x) = x^5 - a_1x^4 + a_2x^3 - a_3x^2 + a_4x - a_5 \in Q[x]$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and α_5 be the five roots of $\varphi(x)$. Set*

$$r(x) = \prod_{1 \leq k < l \leq 5} (x - (\alpha_k + \alpha_l)).$$

Let

$$S_i = \sum_{k=1}^5 \alpha_k^i, \quad T_i = \sum_{1 \leq k < l \leq 5} (\alpha_k + \alpha_l)^i.$$

Then

$$r(x) = x^{10} - B_1x^9 + B_2x^8 - B_3x^7 + B_4x^6 - B_5x^5 + B_6x^4 - B_7x^3 + B_8x^2 - B_9x + B_{10},$$

where for $i = 1, 2, \dots, 10$

$$S_i = \sum_{k=1}^i (-1)^{k-1} a_k S_{i-k}, \quad (2.26)$$

$$T_i = \begin{cases} 4S_i + \sum_{1 \leq k \leq i/2} \binom{i}{k} (S_k S_{i-k} - S_i), & \text{if } i \text{ is odd,} \\ 4S_i + \frac{1}{2} \binom{i}{i/2} + \sum_{1 \leq k \leq (i-2)/2} \binom{i}{k} (S_k S_{i-k} - S_i), & \text{if } i \text{ is even.} \end{cases} \quad (2.27)$$

$$B_i = \frac{1}{i} \sum_{k=0}^i (-1)^{i-k} T_{i-k} B_k. \quad (2.28)$$

Proof: First, by Lemma 2.6.18, we can express the S_i 's in terms of $a_1, a_2, \dots, a_5$, as in (2.26). Then using the Binomial Theorem, we can express the T_i 's in terms of the S_i 's as in (2.27). Finally, again appealing to Lemma 2.6.18, we can express the B_i 's in terms of the T_i 's as in (2.28).

Example 2.6.6 $\varphi(x) = x^5 - 5x + 12$. By Lemma 2.6.16, we have

$$r(x) = x^{10} + 15x^6 - 132x^5 - 100x^2 - 240x - 144,$$

and it can be shown that

$$r(x) = (x^5 + 5x^3 + 10x^2 + 10x + 4)(x^5 - 5x^3 - 10x^2 + 30x - 36).$$

Hence, by Lemma 2.6.16, the Galois group G of $\varphi(x)$ is a subgroup of D_5 . Further, as $\varphi(x)$ has only one real root, we have $G = D_5$. Similarly, $\varphi(x) = x^5 + 11x + 44$ has Galois group D_5 . Here the corresponding $r(x)$ is

$$\begin{aligned} r(x) &= x^{10} - 33x^6 - 484x^5 - 484x^2 + 1936x - 1936 \\ &= (x^5 + 11x^3 + 22x^2 + 22x + 44)(x^5 - 11x^3 - 22x^2 + 66x - 44). \end{aligned}$$

Example 2.6.7 Let $\varphi_q(x)$ be the quintics listed in Example 2.6.5.

The corresponding $r_q(x)$ (as in Theorem 2.6.16) are as follows

$$\begin{aligned} r_{47}(x) &= x^{10} - 3x^8 - 2x^7 + 9x^6 + 15x^5 - 9x^4 - 22x^3 + 17x + 5 \\ r_{79}(x) &= x^{10} - 4x^9 - 3x^8 + 20x^7 + 19x^6 - 41x^5 - 87x^4 + 16x^3 + 124x^2 + 81x + 9 \\ r_{103}(x) &= x^{10} - 12x^9 + 51x^8 - 79x^7 - 24x^6 + 175x^5 - 132x^4 + 65x^3 - 61x^2 - 2x - 3 \\ r_{127}(x) &= x^{10} + 8x^9 + 24x^8 + 29x^7 - 2x^6 - 29x^5 + 3x^4 + 40x^3 + 37x^2 + 27x + 9 \\ r_{131}(x) &= x^{10} + 4x^9 + 12x^8 + 23x^7 + 32x^6 + 56x^5 + 71x^4 + 64x^3 + 36x^2 + 9x - 4 \\ r_{179}(x) &= x^{10} + 4x^9 + 6x^8 + x^7 - 8x^6 + 12x^5 + 31x^4 + 20x^3 + 46x^2 + 55x + 8 \\ r_{227}(x) &= x^{10} - 3x^8 + 2x^7 - 6x^6 + 40x^5 + x^4 - 38x^3 - 85x^2 - 52x - 20 \\ r_{347}(x) &= x^{10} + 8x^9 + 33x^8 + 82x^7 + 122x^6 + 108x^5 + 13x^4 - 38x^3 + 51x^2 + 320x + 100 \\ r_{443}(x) &= x^{10} - 4x^9 + 3x^8 + 10x^7 - 34x^6 + 82x^5 - 113x^4 - 14x^3 - 101x^2 - 42x - 44 \\ r_{523}(x) &= x^{10} + 4x^9 + 15x^8 + 26x^7 + 38x^6 + 46x^5 + 3x^4 - 14x^3 + 27x^2 + 332x + 108 \end{aligned}$$

$$r_{571}(x) = x^{10} + 4x^9 - 21x^7 - 24x^6 + 48x^5 + 63x^4 - 48x^3 + 56x^2 + 269x + 84$$

$$r_{619}(x) = x^{10} + 4x^9 + 18x^8 + 45x^7 + 96x^6 + 180x^5 + 231x^4 + 228x^3 + 74x^2 - 13x - 48$$

$$r_{691}(x) = x^{10} - 8x^9 + 33x^8 - 94x^7 + 218x^6 - 332x^5 + 237x^4 - 86x^3 + 195x^2 + 136x - 12$$

$$r_{739}(x) = x^{10} - 20x^9 + 168x^8 - 767x^7 + 2020x^6 - 2872x^5$$

$$+ 1335x^4 + 1664x^3 - 2264x^2 + 927x - 504$$

$$r_{787}(x) = x^{10} - 9x^8 - 3x^7 + 33x^6 + 117x^5 - 48x^4 - 159x^3 + 182x^2 + 180x - 144$$

The corresponding factorization as follows

$$r_{47}(x) = (x^5 - 3x^3 + x^2 + 7x + 5)(x^5 - 3x^2 + 2x + 1)$$

$$r_{79}(x) = (x^5 + 4x^4 + 7x^3 + 5x^2 + 3x + 1)(x^5 + 4x^4 + x^3 - 8x^2 + 9)$$

$$r_{103}(x) = (x^5 - 2x^4 - x^3 - x^2 + 7x + 1)(x^5 - 2x^4 - 6x^3 + 7x^2 + 18x + 9)$$

$$r_{127}(x) = (x^5 - 6x^4 + 12x^3 - 9x^2 + 4x - 3)(x^5 - 6x^4 + 3x^3 + 20x^2 + 2x + 1)$$

$$r_{131}(x) = (x^5 + 2x^4 + 7x^3 + 3x^2 + 4x - 1)(x^5 + 2x^4 + x^3 + 4x^2 + 7x + 4)$$

$$r_{179}(x) = (x^5 + 2x^4 + 5x^3 + x^2 + 6x + 1)(x^5 + 2x^4 - 3x^3 - 4x^2 + 7x + 8)$$

$$r_{227}(x) = (x^5 + 2x^3 - 5x^2 + 4x - 4)(x^5 - 5x^3 + 7x^2 + 8x - 5)$$

$$r_{347}(x) = (x^5 + 4x^4 + 10x^3 + 15x^2 + 16x + 4)(x^5 + 4x^4 + 7x^3 - x^2 - 20x + 25)$$

$$r_{443}(x) = (x^5 - 2x^4 + 2x^3 - 7x^2 - 6x - 4)(x^5 - 2x^4 - 3x^3 + 15x^2 - 6x + 11)$$

$$r_{523}(x) = (x^5 + 2x^4 + 6x^3 + 9x^2 + 14x + 4)(x^5 + 2x^4 + 5x^3 - 5x^2 - 14x + 27)$$

$$r_{571}(x) = (x^5 + 2x^4 + 3x^3 - x^2 + 8x + 3)(x^5 + 2x^4 - 7x^3 - 12x^2 + 15x + 28)$$

$$r_{619}(x) = (x^5 + 2x^4 + 9x^3 + 5x^2 + 2x - 3)(x^5 + 2x^4 + 5x^3 + 2x^2 + 15x + 16)$$

$$r_{691}(x) = (x^5 - 4x^4 + 11x^3 - 29x^2 + 40x - 3)(x^5 - 4x^4 + 6x^3 + 3x^2 + 8x + 4)$$

$$r_{739}(x) = (x^5 - 10x^4 + 37x^3 - 52x^2 - 9x + 72)(x^5 - 10x^4 + 31x^3 - 35x^2 + 12x - 7)$$

$$r_{787}(x) = (x^5 + 2x^3 - 7x^2 + 10x - 4)(x^5 - 11x^3 + 4x^2 + 45x + 36)$$

Further, as $\rho_q(x)$ has only one real root for each q , the Galois group of each $\rho_q(x)$ is the dihedral group D_5 .

Next we give an example of a quintic polynomial with Galois group Z_5 .

Example 2.6.8 Let $\varphi(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$. Here $\text{disc}(\varphi) = 11^4$. The corresponding $r(x)$ is

$$x^{10} + 4x^9 - 6x^8 - 35x^7 - 8x^6 + 67x^5 + 37x^4 - 28x^3 - 13x^2 + 3x + 1,$$

which factors as

$$(x^5 + 2x^4 - 5x^3 - 13x^2 - 7x - 1)(x^5 + 2x^4 - 5x^3 - 2x^2 + 4x - 1).$$

Let M denote the splitting field of $\varphi(x)$. By Theorem 2.6.16 we have that $\text{Gal}(M/Q) = Z_5$ or D_5 . Suppose that $\text{Gal}(M/Q) = D_5$. Let $K \in K_M$. By Lemma 2.3.10 we have $K = Q(\sqrt{-1})$ or $Q(\sqrt{-11})$ so that $\left(\frac{d_K}{7}\right) = -1$. Then by Corollary 2.2.19 the congruence

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 \equiv 0 \pmod{7}$$

has one solution. But it is easy to check the above congruence has no solutions. Hence we must have $\text{Gal}(M/Q) = Z_5$.

Next we give an example of a quintic polynomial with Galois group A_5 .

Example 2.6.9 $\varphi(x) = x^5 + 20x + 16$. Here $\text{disc}(\varphi) = 2^{16} \cdot 5^6$. Let M denote the splitting field of $\varphi(x)$. Suppose that $\text{Gal}(M/Q) \neq A_5$. As $\varphi(x)$ has only one real root, $\text{Gal}(M/Q) \neq Z_5$ so that $\text{Gal}(M/Q) = D_5$. Let $K \in K_M$. By Lemma 2.3.10 we have

$$K = Q(\sqrt{-4}) \text{ or } Q(\sqrt{-8}) \text{ or } Q(\sqrt{-20}) \text{ or } Q(\sqrt{-40}).$$

Since the congruence

$$x^5 + 20x + 16 \equiv 0 \pmod{7}$$

has exactly two solutions, namely, $x = 3, 4$, Theorem 2.2.18(i) shows that $K \neq Q(\sqrt{-20})$ and $K \neq Q(\sqrt{-40})$ as $\left(\frac{-20}{7}\right) = \left(\frac{-40}{7}\right) = 1$, and Corollary 2.2.19 shows that $K \neq Q(\sqrt{-4})$ and $K \neq Q(\sqrt{-8})$ as $\left(\frac{-4}{7}\right) = \left(\frac{-8}{7}\right) = -1$, hence we must have $\text{Gal}(M/Q) = A_5$.

Finally, we give an example of a quintic polynomial with Galois group F_{20} .

Example 2.6.10 Let $\varphi(x) = x^5 - a$, where a is not a perfect 5th power. Since $\text{disc}(\varphi) = 5^5 \cdot a^4$ and

$$r(x) = x^{10} + 11ax^5 - a^2 = \left(x^5 + \frac{11 + 5\sqrt{5}}{2} \cdot a\right)\left(x^5 + \frac{11 - 5\sqrt{5}}{2} \cdot a\right),$$

by Corollary 2.6.17, the Galois group of $\varphi(x)$ is F_{20} .

Chapter 3

NUMBER OF SOLUTIONS OF A DIHEDRAL POLYNOMIAL CONGRUENCE (mod p)

In this chapter we prove our first main theorem which for a dihedral polynomial $\rho(x)$ relates the number of solutions of the congruence $\rho(x) \equiv 0 \pmod{p}$ to the representability of the prime p by forms in a certain subgroup of a form class group whose discriminant depends only on the splitting field M of $\rho(x)$.

3.1 Proof of Theorem 3.1.3

First we require a lemma.

Lemma 3.1.1 *Let M be a dihedral extension of Q and let $K \in K_M$ (K_M is defined on p.viii). Let f be a positive integer such that $M \subset F_f^+(K)$. Then there exists a unique subgroup $S = S(M, K, f)$ of $I_K(f)$ with $I_K(f)/S \simeq \text{Gal}(M/K)$. Further, we have for all prime ideals $\mathcal{P}$ in K*

$$\left(\frac{M/K}{\mathcal{P}} \right) = 1 \iff \mathcal{P} \in S.$$

Proof: As $K \subset M \subset F_f^+(K)$, we have that $\text{Gal}(F_f^+(K)/M) \subset \text{Gal}(F_f^+(K)/K)$. Under the isomorphism $\text{Gal}(F_f^+(K)/K) \simeq I_K(f)/P_{K,Z}^+(f)$, there is a unique subgroup S of $I_K(f)$ with

$$\text{Gal}(F_f^+(K)/M) \simeq S/P_{K,Z}^+(f),$$

so that

$$P_{K,Z}^+(f) \subset S \subset I_K(f),$$

and

$$I_K(f)/S \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map $\phi_{M/K,f}$. Thus we have

$$\left(\frac{M/K}{\mathcal{P}}\right) = 1 \iff \mathcal{P} \in S. \blacksquare$$

Theorem 3.1.2 *Let M be a dihedral extension of Q . Let $K \in K_M$ and let f be any positive integer such that $M \subset F_f^+(K)$, the strict ring class field of the order of conductor f in K . Then there is a unique subgroup $J = J(M, K, f)$ of $H(d_K f^2)$ such that*

$$H(d_K f^2)/J \simeq \text{Gal}(M/K).$$

Further, J has the property: if p is a prime which is unramified in M then

$$p \text{ splits completely in } M \iff p \text{ is represented by one of the classes in } J.$$

Proof: Let $\mu : I_K(f) \rightarrow C^+(\mathcal{O}_f)$ be the natural homomorphism passing from ideals to strict ideal classes given by

$$I_K(f) \rightarrow I(\mathcal{O}_f, f) \rightarrow I(\mathcal{O}_f, f)/P^+(\mathcal{O}_f, f) \simeq I(\mathcal{O}_f)/P^+(\mathcal{O}_f) = C^+(\mathcal{O}_f).$$

Let $\lambda : C^+(\mathcal{O}_f) \rightarrow H(d_K f^2)$ be the isomorphism between strict ideal classes and form classes defined in Lemma 1.3.10. Let $S = S(M, K, f)$ be as in Lemma 3.1.1 and set

$$J = \lambda(\mu(S)).$$

Clearly J is in $H(d_K f^2)$ and

$$H(d_K f^2)/J \simeq I_K(f)/S \simeq \text{Gal}(M/K).$$

Then we have

p splits completely in M

$$\iff p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}' \text{ and } \left(\frac{M/K}{\mathcal{P}}\right) = 1 \text{ (Lemma 1.2.7)}$$

$$\iff p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}' \text{ and } \mathcal{P} \in S \text{ (Lemma 3.1.1)}$$

$$\iff p \text{ is represented by a form in } J. \blacksquare$$

We are now ready to prove part (i) of Theorem 3.1.3, part (ii) will be proved after Lemma 3.1.11 below.

Theorem 3.1.3 (i) Let $\rho(x) \in \mathbb{Z}[x]$ be a dihedral polynomial of degree d , and let M be the splitting field of $\rho(x)$ over $\mathbb{Q}$. Let $K \in K_M$ and let f be any positive integer such that $M \subset F_f^+(K)$, the strict ring class field of the order of conductor f in K . Then there is a unique subgroup $J = J(M, K, f)$ of $H(d_K f^2)$ such that

$$H(d_K f^2)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$$\iff p \text{ splits completely in } M$$

$$\iff p \text{ is represented by one of the classes in } J.$$

(ii) Conversely, suppose $\rho(x)$ is a monic irreducible polynomial of degree d with integral coefficients. If there exists a subgroup H of the form class group $H(\Delta)$ for some nonsquare integer $\Delta \equiv 0, 1 \pmod{4}$ having the property: for every prime p not dividing $\text{disc}(\rho)$,

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$$\iff p \text{ is represented by one of the classes in } H,$$

then $\rho(x)$ is a dihedral polynomial.

Proof of Theorem 3.1.3 (i): Let p be a prime not dividing $\text{disc}(\rho)$, by Lemma 1.2.3, we have

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$$\iff p \text{ splits completely in } M$$

Then the theorem follows from Theorem 3.1.2. ■

Lemma 3.1.4 Let k be a number field and L be an Abelian extension of k . Let $\sigma : L \rightarrow \sigma(L)$ be an isomorphism (not necessarily fixing k). Then

$$\left(\frac{\sigma(L)/\sigma(k)}{\sigma(\mathcal{P})} \right) = \sigma \left(\frac{L/k}{\mathcal{P}} \right) \sigma^{-1}.$$

Proof: See [[25], A, p.198].

Lemma 3.1.5 *Let K be a quadratic field, and let f be a positive integer. Then $F_f^+(K)$ is a dihedral extension of Q .*

Proof: Let $\text{Gal}(K/Q) = \langle \tau \rangle$. First we show that $F_f^+(K)/Q$ is a normal extension. We do this by showing that for any imbedding $\sigma : F_f^+(K) \rightarrow C$ we have

$$\sigma(F_f^+(K)) = F_f^+(K). \quad (3.1)$$

We consider two possibilities according as σ fixes K or not. (i). If σ fixes K , then in fact $\sigma \in \text{Gal}(F_f^+(K)/K)$, so we have (3.1).

(ii). If σ induces a non-trivial automorphism of K , then σ is an extension of τ to $F_f^+(K)$, in other words, $\sigma|_K = \tau$. We have by Lemma 3.1.4, as $\sigma(K) = K$,

$$\sigma \left(\frac{F_f^+(K)/K}{\mathcal{P}} \right) \sigma^{-1} = \left(\frac{\sigma(F_f^+(K))/K}{\sigma(\mathcal{P})} \right), \quad (3.2)$$

where $\mathcal{P}$ is any prime of K such that the Artin symbol is defined. From (3.2) we have

$$\left(\frac{F_f^+(K)/K}{\mathcal{P}} \right) = 1 \iff \left(\frac{\sigma(F_f^+(K))/K}{\sigma(\mathcal{P})} \right) = 1,$$

so that

$$\mathcal{P} \in \ker \phi_{F_f^+(K)/K, f\infty} \iff \sigma(\mathcal{P}) \in \ker \phi_{\sigma(F_f^+(K))/K, f\infty},$$

which implies that

$$\sigma(\ker \phi_{F_f^+(K)/K, f\infty}) = \ker \phi_{\sigma(F_f^+(K))/K, f\infty}. \quad (3.3)$$

Now since $F_f^+(K)$ is the strict ring class field of the order $\mathcal{O}_f$, $\ker \phi_{F_f^+(K)/K, f\infty} = P_{K,Z}^+(f)$, thus we have

$$\ker \phi_{\sigma(F_f^+(K))/K, f\infty} = \sigma(\ker \phi_{F_f^+(K)/K, f\infty}) = \sigma(P_{K,Z}^+(f)) = P_{K,Z}^+(f) = \ker \phi_{F_f^+(K)/K, f\infty}. \quad (3.4)$$

Then (3.1) follows from Lemma 1.3.7.

Next we show that $\text{Gal}(F_f^+(K)/K)$ is a dihedral group. If $\mathcal{P} \in I_K(f)$ is a prime ideal, then $\mathcal{P}\tau(\mathcal{P}) = N_{K/Q}(\mathcal{P})\mathcal{O}_K$ lies in $P_{K,Z}^+(f)$. In other words, $\tau(\mathcal{P})$ gives the inverse of $\mathcal{P}$ in the quotient $I_K(f)/P_{K,Z}^+(f)$. Thus (3.2) gives

$$\tau \left(\frac{F_f^+(K)/K}{\mathcal{P}} \right) \tau^{-1} = \left(\frac{F_f^+(K)/K}{\tau(\mathcal{P})} \right) = \left(\frac{F_f^+(K)/K}{\mathcal{P}} \right)^{-1}. \quad (3.5)$$

Since $\text{Gal}(F_f^+(K)/K)$ is generated by all elements of the form $\left(\frac{F_f^+(K)/K}{p}\right)$, (3.5) implies that

$$\tau\sigma\tau^{-1} = \sigma^{-1} \text{ for any } \sigma \in \text{Gal}(F_f^+(K)/K).$$

This completes the proof. ■

Lemma 3.1.6 *Let M be a dihedral extension of Q and let $K \in K_M$. Suppose that f is a positive integer and let $F_f^+(K)$ be the strict ring class field of the order of conductor f in K . Then $M \subset F_f^+(K)$ if and only if $f_0(M/K)$ divides f , where $f_0(M/K)$ denotes the finite part of the conductor $f(M/K)$.*

Proof: Suppose that $f_0(M/K) \mid f$. We will prove that

$$M \subset F_f^+(K). \quad (3.6)$$

Since $f(M/K) \mid f_\infty$, by Theorem 1.3.5, $H = \ker(\phi_{M/K, f_\infty})$ is a congruence subgroup, that is

$$P_{K,1}^+(f_\infty) \subset H \subset I_K(f_\infty), \quad I_K(f_\infty)/H \simeq \text{Gal}(M/K).$$

We recall that $P_{K,1}^+(f_\infty)$ is the subgroup of $I_K(f_\infty)$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies

$$\alpha \equiv 1 \pmod{f\mathcal{O}_K} \text{ and } \tau(\alpha) > 0 \text{ for every real infinite prime } \tau.$$

To prove (3.6), it suffices to show that

$$P_{K,Z}^+(f_\infty) \subset H. \quad (3.7)$$

First we show that if $\alpha\mathcal{O}_K, \beta\mathcal{O}_K \in P_{K,Z}^+(f_\infty)$ then

$$\alpha \equiv \beta \pmod{f_\infty} \implies (\alpha\mathcal{O}_K \in H \iff \beta\mathcal{O}_K \in H), \quad (3.8)$$

where $\alpha \equiv \beta \pmod{f_\infty}$ means that $\alpha\beta^{-1} \in P_{K,1}^+(f_\infty)$. We choose

$$\gamma \in \mathcal{O}_K \text{ such that } \alpha\gamma \equiv 1 \pmod{f\mathcal{O}_K}.$$

If K is imaginary, let $\gamma' = \gamma$. If K is real, to simplify the proof we assume that $\alpha > 0$. Let n be a positive integer such that $\gamma' = nf + \gamma$ satisfies $\gamma' > 0$ and $\tau(\gamma') > 0$. Then

$$\alpha\gamma'\mathcal{O}_K, \beta\gamma'\mathcal{O}_K \in P_{K,1}^+(f_\infty) \subset H.$$

Now it is clear that

$$\alpha\mathcal{O}_K \in H \iff \gamma'\mathcal{O}_K \in H \iff \beta\mathcal{O}_K \in H,$$

proving (3.8).

Next we prove that for any ideal $\mathcal{R} \in I_K(f)$, we have

$$N_{K/Q}(\mathcal{R})\mathcal{O}_K \in H. \quad (3.9)$$

As $F_f^+(K)$ is a dihedral extension of Q (Lemma 3.1.5), for $\mathcal{R} \in I_K(f)$ we have that $\tau(\mathcal{R})H = (\mathcal{R}H)^{-1}$, so that $\mathcal{R}\tau(\mathcal{R}) \in H$. Since $\mathcal{R}\tau(\mathcal{R}) = N_{K/Q}(\mathcal{R})\mathcal{O}_K$, we obtain (3.9).

Now we prove that

$$r\mathcal{O}_K \in H, \text{ if } r \text{ is a prime not dividing } f. \quad (3.10)$$

Let r be a prime which does not divide f . First we treat the case when r splits or ramifies in K . In this case $r = N_{K/Q}(\mathcal{R})$ for some prime ideal $\mathcal{R}$ of $\mathcal{O}_K$. Then, by (3.9), we have

$$r\mathcal{O}_K = N_{K/Q}(\mathcal{R})\mathcal{O}_K \in H.$$

Secondly we treat the case when r remains prime in K . In this case we have $\left(\frac{d_K}{r}\right) = -1$. Note that $r \nmid f$, so $r \nmid f_0(M/K)$ and $r\mathcal{O}_K$ is unramified in M . Then, by Lemma 1.2.16, $r\mathcal{O}_K$ splits completely in M , and by Lemma 1.2.7 we have $\left(\frac{M/K}{r\mathcal{O}_K}\right) = 1$, so that $r\mathcal{O}_K \in H$. This completes the proof of (3.10).

We see immediately from (3.10) by multiplicativity that:

$$c\mathcal{O}_K \in H, \text{ if } c \text{ is an integer coprime with } f. \quad (3.11)$$

We are now ready to prove (3.7). Suppose that $\alpha\mathcal{O}_K \in P_{K,Z}^+(f\infty)$. By the definition of $P_{K,Z}^+(f\infty)$, we have $N_{K/Q}(\alpha) > 0$ and $\alpha \equiv c \pmod{f\mathcal{O}_K}$ for some integer c . If K is imaginary, by (3.8) and (3.11), $\alpha\mathcal{O}_K \in H$. If K is real, without loss of generality, we may suppose that $\alpha > 0$ and $c > 0$ (if $c < 0$, $c' = nf + c > 0$ for a suitably large n and $\alpha \equiv c' \pmod{f\mathcal{O}_K}$). Thus we have $\alpha \equiv c \pmod{f\infty}$ and by (3.8) and (3.11), $\alpha\mathcal{O}_K \in H$. This completes the proof of (3.7), and thus of (3.6).

Conversely, suppose that $M \subset F_f^+(K)$. Let $X(F_f^+(K))$ denote the character group of $\text{Gal}(F_f^+(K)/K)$, and let $X(M)$ denote the character group of $\text{Gal}(M/K)$. By Lemma

1.2.10, $X(M) \subset X(F_f^+(K))$. By Theorem 1.2.9, $f_0(M/K) \mid f_0(F_f^+(K)/K)$, and by the definition of a strict ring class field, we have $f_0(F_f^+(K)) \mid f$, so $f_0(M/K) \mid f$. ■

Lemma 3.1.7 *Let M be a real dihedral extension of Q and let $K \in K_M$. Suppose that f is a positive integer and let $F_f(K)$ be the ring class field of the order of conductor f in K . Then $M \subset F_f(K)$ if and only if $f_0(M/K)$ divides f , where $f_0(M/K)$ denotes the finite part of the conductor $f(M/K)$.*

Proof: In the proof of Lemma 3.1.6, replacing $F_f^+(K)$ by $F_f(K)$, $P_{K,1}^+(f\infty)$ by $P_{K,1}(f)$, $P_{K,2}^+(f\infty)$ by $P_{K,2}(f)$, the lemma follows. ■

Definition Let L be a finite extension of a number field k . Let P_k denote the set of all finite primes of k . We set

$$S_{L/k} = \{\mathcal{P} \in P_k : \mathcal{P} \text{ splits completely in } L\}.$$

Given two sets S and T , we write $S \subset' T$ if $S \subset T \cup \Sigma$ for some finite set Σ .

Lemma 3.1.8 *Let L and M be finite extensions of a number field k . If L is Galois over k , then*

$$M \subset L \iff S_{L/k} \subset' S_{M/k}.$$

Proof: See [[11], Proposition 8.20, p.171]. ■

Lemma 3.1.9 *Let M' be a finite extension of Q . Let K be a quadratic field over Q . Suppose that f is a positive integer having the following property: if a prime p is represented by the principal class 1_Δ , where $\Delta = d_K f^2$, then p splits completely in M' . Then $M' \subset F_f^+(K)$.*

Proof: By Lemma 3.1.5, $F_f^+(K)$ is a normal extension of Q , and thus by Lemma 3.1.8, we need only show that

$$S_{F_f^+(K)/Q} \subset' S_{M'/Q}.$$

Now let $p \in S_{F_f^+(K)/Q}$. Then p splits completely in $F_f^+(K)$. In Theorem 3.1.2, choosing $M = F_f^+(K)$, as $H(K, f^2) \simeq \text{Gal}(F_f^+(K)/K)$, we have $J = J(K, f) = \{1_\Delta\}$, so that p is represented by the principal form class 1_Δ of discriminant $\Delta = d_K f^2$. Then by the assumption of the lemma, p splits completely in M' , that is, $p \in S_{M'/Q}$, as asserted. ■

21 of/de 2

PM-1 3 1/4" x 4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

Lemma 3.1.10 *Let $\varphi(x) \in Q[x]$ be irreducible. Let M be the splitting field of $\varphi(x)$ over Q . Then $\varphi(x)$ is a dihedral polynomial if and only if M is contained in a strict ring class field over a quadratic field K .*

Proof: Suppose that $\varphi(x)$ is a dihedral polynomial, and let M be the splitting field of $\varphi(x)$ over Q . Then by the definition of a dihedral extension of Q , there is a quadratic subfield K of M such that $\text{Gal}(M/Q)$ is generated by $\text{Gal}(M/K)$ and $\text{Gal}(K/Q)$. Suppose that f is a positive integer such that $f_0(M/K) \mid f$. Then Lemma 3.1.6 shows that M is contained in the strict ring class field $F_f^+(K)$ over K .

Conversely suppose that $M \subset F_g^+(K)$ for some positive integer g . Let $G = \text{Gal}(F_g^+(K)/Q)$, $N = \text{Gal}(F_g^+(K)/M)$ and $H = \text{Gal}(F_g^+(K)/K)$. By Lemma 3.1.5, $F_g^+(K)$ is a dihedral extension of Q . We consider two cases (i) $N \subset H$ and (ii) $N \not\subset H$.

Case (i): Suppose that $N \subset H$. By Galois theory, $K \subset M \subset F_g^+(K)$ and by Lemma 2.1.6, $\text{Gal}(M/Q) \simeq G/N$ is a dihedral group. Thus $\varphi(x)$ is a dihedral polynomial.

Case (ii): Suppose that $N \not\subset H$. By Lemma 2.1.3, $\text{Gal}(M/Q) \simeq G/N$ is an elementary 2-group. Hence $\varphi(x)$ is a dihedral polynomial. ■

Lemma 3.1.11 *Let $\varphi(x) \in Z[x]$ be monic and irreducible. Then $\varphi(x)$ is a dihedral polynomial if and only if there exists a nonsquare integer $\Delta \equiv 0, 1 \pmod{4}$ having the following property: if p is a prime not dividing $\text{disc}(\varphi)$*

$$p \text{ is represented by } 1_\Delta \implies \varphi(x) \text{ splits completely } (\text{mod } p). \quad (3.12)$$

Proof: Suppose that $\varphi(x)$ is a dihedral polynomial. Then Theorem 3.1.3 (i) shows that the statement (3.12) holds.

Conversely, suppose that the property (3.12) holds. Then by Lemma 1.2.17, $\Delta = d_K g^2$ for some positive integer g , where $K = Q(\sqrt{\Delta})$. Now let M be the splitting field of $\varphi(x)$ over Q . Then by Lemma 3.1.9, $M \subset F_g^+(K)$. By Lemma 3.1.10, $\varphi(x)$ is a dihedral polynomial. ■

Proof of Theorem 3.1.3(ii): Suppose that $\rho(x)$ is a monic irreducible polynomial of degree d with integral coefficients, and suppose that H is a subgroup of a form class group $H(\Delta)$ with the property: if p is a prime not dividing $\text{disc}(\rho)$, then

$$\rho(x) \equiv 0 \pmod{p} \text{ has } d \text{ solutions}$$

$\iff p$ is represented by one of the classes in H .

Then, as $1_\Delta \in H$, we have

p is represented by $1_\Delta \implies \rho(x)$ splits completely (mod p).

Now appealing to Lemma 3.1.11, $\rho(x)$ is a dihedral polynomial. This completes the proof of Theorem 3.1.3. ■

In Theorem 3.1.3 we characterized those polynomials $\rho(x) \in Z[x]$ whose splitting modulo a prime p is determined by the representability of p by some form class in a subgroup of a form class group. Theorem 3.1.13 below shows that the representability of a prime p by some form in a given subgroup of a form class group can be characterized in terms of the splitting of certain integral polynomials modulo p .

Lemma 3.1.12 *Let $\Delta \equiv 0, 1 \pmod{4}$ be an integer which is not a perfect square. Set $K = Q(\sqrt{\Delta})$. Let N be a subgroup of $H(\Delta)$. Then there exists a unique dihedral extension M of Q such that if p is unramified in M then p is represented by a form in N if and only if p splits completely in M . In particular, p is represented by the principal form 1_Δ if and only if p splits completely in $F_f^+(K)$, where $f = \sqrt{\Delta/d_K}$.*

Proof: By Lemma 1.2.17, there is a positive integer f such that $\Delta = d_K f^2$. We have the isomorphisms

$$H(\Delta) \simeq C^+(\mathcal{O}_f) \simeq I_K(f)/P_{K,Z}^+(f).$$

Under the above isomorphisms, as $N \subset H(\Delta)$, there exists a unique subgroup H with

$$P_{K,Z}^+(f) \subset H \subset I_K(f) \tag{3.13}$$

such that $N \simeq H/P_{K,Z}^+(f)$. By Theorem 1.3.6, (3.13) determines a unique Abelian extension M of K such that

$$I_K(f)/H \simeq \text{Gal}(M/K).$$

Further, we have that

$$\text{Gal}(M/K) \simeq I_K(f)/H \simeq (I_K(f)/P_{K,Z}^+(f))/(H/P_{K,Z}^+(f)) \simeq H(\Delta)/N.$$

Now appealing to Theorem 3.1.2, the assertion of the lemma follows.

In particular, suppose $N = \{1_\Delta\}$. Then we have $M = F_f^+(K)$ so that the last assertion of the lemma follows. ■

Theorem 3.1.13 *Let $\Delta \equiv 0, 1 \pmod{4}$ be an integer which is not a perfect square. Set $K = Q(\sqrt{\Delta})$. Let N be a subgroup of $H(\Delta)$. Then there exists a set of cyclic dihedral polynomials $\rho_i(x)$ of degree $p_i^{n_i}$ for some prime p_i such that except for a finite number of exceptions*

$$p \text{ is represented by a form in } N \iff \begin{cases} \left(\frac{d_K}{p}\right) = 1, \rho_i(x) \equiv 0 \pmod{p} \forall i \\ \text{has a solution.} \end{cases}$$

Proof: Let M be the dihedral extension specified in Lemma 3.1.12. By Lemmas 2.1.8 and 2.1.9 M is a composite field of cyclic dihedral extensions M_i , where $\text{Gal}(M_i/Q) = D_{p_i^{n_i}}$ for some prime p_i . If $\text{Gal}(M_i/Q)$ is not an elementary 2-group, Lemma 2.2.4 shows that M_i is a splitting field of a cyclic dihedral polynomial $\rho_i(x)$ of degree $p_i^{n_i}$. If $\text{Gal}(M_i/Q)$ is an elementary 2-group, then $\text{Gal}(M_i/Q) = D_2$ and $M_i = K(\sqrt{m_i})$ for some squarefree integer m_i . In this case, we set $\rho_i(x) = x^2 - m_i$. Now appealing to Theorem 2.2.18 (i) and Lemma 2.2.20 a prime p not dividing $\text{disc}(\rho_i)$ splits completely in M_i if and only if

$$\left(\frac{d_K}{p}\right) = 1, \text{ and } \rho_i(x) \equiv 0 \pmod{p} \text{ has an integer solution.}$$

Since M is the composite field of M_i 's, we have by Lemma 2.2.1 except for a finite number of exceptions

$$\begin{aligned} p \text{ splits completely in } M &\iff p \text{ splits completely in every } M_i \\ &\iff \left(\frac{d_K}{p}\right) = 1 \text{ and } \rho_i(x) \equiv 0 \pmod{p} \text{ has an integer solution for all } i. \end{aligned}$$

Finally, appealing to Theorem 3.1.12, the assertion of the theorem follows. ■

3.2 Discussion of the Integer f in Theorem 3.1.3

Theorem 3.1.3(i) shows that the splitting modulo a prime p of a given dihedral polynomial with integral coefficients is equivalent to p being represented by form classes in

a certain subgroup of $H(d_K f^2)$ provided f is divisible by $f_0(M/K)$, where M is the splitting field of the polynomial and $K \in K_M$. It is easy to see that number of elements of $H(d_K f^2)$ increases with f . Thus the best choice of f is the least positive integer f_0 divisible by $f_0(M/K)$. But to determine f_0 is not an easy task. In most situations to find a relatively large f is not too difficult. In this section we prove some results which enable us obtain a 'smaller f ' from a given 'larger f '.

Lemma 3.2.1 *Let K be a quadratic field. Let f and g be two positive integers. Then*

- (i) $F_g(K) \subset F_f(K) \implies h(\mathcal{O}_g) \mid h(\mathcal{O}_f)$.
- (ii) $F_g^+(K) \subset F_f^+(K) \implies h^+(\mathcal{O}_g) \mid h^+(\mathcal{O}_f)$.

Proof: From the following isomorphisms

$$\begin{aligned} C(\mathcal{O}_f) &\simeq I_K(f)/P_{K,Z}(f) \simeq \text{Gal}(F_f(K)/K), \\ C(\mathcal{O}_g) &\simeq I_K(g)/P_{K,Z}(g) \simeq \text{Gal}(F_g(K)/K), \\ \text{Gal}(F_g(K)/K) &\simeq \text{Gal}(F_f(K)/K)/\text{Gal}(F_f(K)/F_g(K)), \end{aligned}$$

we have

$$\begin{aligned} h(\mathcal{O}_f)/h(\mathcal{O}_g) &= |C(\mathcal{O}_f)|/|C(\mathcal{O}_g)| = |\text{Gal}(F_f(K)/K)|/|\text{Gal}(F_g(K)/K)| \\ &= |\text{Gal}(F_f(K)/F_g(K))| \in \mathbb{Z}^+. \end{aligned}$$

Similarly, we can prove (ii). ■

Lemma 3.2.2 (Gauss' formula) *Let K be a quadratic field and let f be an integer > 1 . Then*

$$\begin{cases} h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K) \varphi(f)}{u_f} \\ \varphi(f) = f \prod_{r|f} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), \end{cases}$$

where r runs through all the primes dividing f , and u_f is the "unit index", i.e., when $d_K > 0$, $u_f = (\log \epsilon_f)/(\log \epsilon_K)$, whereas, when $d_K < 0$, $u_f = 1$, except for $d_K = -4$, $u_f = 2$; and for $d_K = -3$, $u_f = 3$.

Proof: See [[10], Theorem 2, p.217 or [9], Cor. 15.40, p.180]. ■

Lemma 3.2.3 *Let K be a quadratic field and let f be a positive integer. Then*

$$h^+(\mathcal{O}_f) = \begin{cases} h(\mathcal{O}_f), & \text{if } d_K < 0 \text{ or } d_K > 0 \text{ and } N(\epsilon_f) = -1, \\ 2h(\mathcal{O}_f), & \text{otherwise.} \end{cases}$$

Proof: As $P_{K,Z}^+(f) \subset P_{K,Z}(f)$, we have

$$I_K(f)/P_{K,Z}(f) \simeq (I_K(f)/P_{K,Z}^+(f))/(P_{K,Z}(f)/(P_{K,Z}^+(f))),$$

so that

$$h^+(\mathcal{O}_f) = h(\mathcal{O}_f)[P_{K,Z}(f) : P_{K,Z}^+(f)].$$

Then appealing to Lemma 1.3.8, the assertion of the lemma follows. ■

Lemma 3.2.4 *Let K be a quadratic field. Let f and g be two integers > 1 with $g \mid f$. Then we have*

$$\frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \begin{cases} \frac{f}{g} \prod_{r \mid f, r \nmid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), & \text{if } d_K < 0, \\ \frac{f}{g^v} \prod_{r \mid f, r \nmid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), & \text{if } d_K > 0, \end{cases}$$

where $v = \log \epsilon_f / \log \epsilon_g$ is a positive integer when $d_K > 0$. Further,

$$\frac{h^+(\mathcal{O}_f)}{h^+(\mathcal{O}_g)} = \begin{cases} \frac{2h(\mathcal{O}_f)}{h(\mathcal{O}_g)}, & \text{if } d_K > 0 \text{ and } N(\epsilon_f) = 1, N(\epsilon_g) = -1, \\ \frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)}, & \text{otherwise.} \end{cases}$$

Proof: For convenience we treat the cases $d_K < 0$ and $d_K > 0$ separately.

Case (i): $d_K < 0$. By Gauss' formula for the class number of an order in an imaginary quadratic field (Lemma 3.2.2), we have

$$h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K)f}{u} \prod_{r \mid f} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right),$$

where r runs through all the primes dividing f and

$$h(\mathcal{O}_g) = \frac{h(\mathcal{O}_K)g}{u} \prod_{r \mid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right),$$

where r runs through all the primes dividing g , and

$$u = \begin{cases} 3, & \text{if } d_K = -3, \\ 2, & \text{if } d_K = -4, \\ 1, & \text{otherwise.} \end{cases}$$

Then we have

$$\frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \frac{f}{g} \prod_{r|f, r \nmid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right)$$

as asserted.

Case(ii): $d_K > 0$. By Gauss' formula for the class number of an order in a real quadratic field (Lemma 3.2.2), we have

$$h(\mathcal{O}_f) = \frac{h(\mathcal{O}_K) f \log \epsilon_1}{\log \epsilon_f} \prod_{r|f} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right),$$

where r runs through all the primes dividing f and

$$h(\mathcal{O}_g) = \frac{h(\mathcal{O}_K) g \log \epsilon_1}{\log \epsilon_g} \prod_{r|g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right),$$

where r runs through all the primes dividing g . Then

$$\begin{aligned} \frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} &= \frac{f}{g} \cdot \frac{\log \epsilon_g}{\log \epsilon_f} \prod_{r|f, r \nmid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right) \\ &= \frac{f}{g^v} \prod_{r|f, r \nmid g} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), \end{aligned}$$

where $v = \log \epsilon_f / \log \epsilon_g$. Next we show that v is a positive integer. As $g \mid f$, we have $\mathcal{O}_f \subset \mathcal{O}_g$ and thus $\epsilon_f \in \mathcal{O}_g$ so that $\epsilon_f = \epsilon_g^v$ for some positive integer v . Hence $\log \epsilon_f / \log \epsilon_g = v$ is a positive integer.

The last assertion of the lemma follows from Lemma 3.2.3. ■

Lemma 3.2.5 *Let G be an Abelian group, and let H be a subgroup of G . Suppose that m is a positive integer such that $\gcd(|H|, m) = 1$. Then G and G/H have the same m -part.*

Proof: Note that as G is an Abelian group, G can be expressed in the form

$$G = N \times N',$$

where N is the direct product of all q -Sylow subgroups of G with $q \mid m$.

Since $\gcd(|H|, m) = 1$, we must have $H \subset N'$ and thus

$$G/H = (N \times N')/H \simeq N \times (N'/H),$$

which means G and G/H have the same m -part N . ■

Lemma 3.2.6 *Let M be a dihedral extension of Q and let K be a quadratic field in K_M . Suppose that f and g are positive integers such that $M \subset F_f^+(K)$ and $F_g^+(K) \subset F_f^+(K)$. Then*

$$\gcd(|\text{Gal}(M/K)|, |\text{Gal}(F_f^+(K)/F_g^+(K))|) = 1 \implies M \subset F_g^+(K).$$

Proof: Let $m = [M : K]$. As $\text{Gal}(F_f^+(K)/K)/\text{Gal}(F_f^+(K)/F_g^+(K)) \simeq \text{Gal}(F_g^+(K)/K)$, Lemma 3.2.5 shows that $\text{Gal}(F_f^+(K)/K)$ and $\text{Gal}(F_g^+(K)/K)$ have the same m -part. Then, by Galois theory, $F_f^+(K)$ and $F_g^+(K)$ contain the same number of subfields of degree m over K . Note that as $F_g^+(K) \subset F_f^+(K)$ and $K \subset M \subset F_f^+(K)$, it follows that $M \subset F_g^+(K)$. ■

Lemma 3.2.7 *Let M be a dihedral extension of Q and let K be a quadratic field in K_M . Let f be a positive integer such that $M \subset F_f^+(K)$. Let A be the set of primes dividing $m = [M : K]$. Write*

$$f = f_1 f_2,$$

where f_1 contains only primes which are in A , and f_2 contains only primes which are not in A , so that $\gcd(f_1, f_2) = 1$. Set

$$B = \{q : q \text{ prime, } q|f_2 \text{ and } q \equiv \left(\frac{d_K}{q}\right) \pmod{p} \text{ for some } p \in A\}.$$

Let

$$g = f_1 \prod_{q \in B} q = f_1 f_2'.$$

Then

$$M \subset F_g^+(K).$$

Proof: Since $g|f$, we have $F_g^+(K) \subset F_f^+(K)$. Then, in view of Lemma 3.2.6, in order to show that $M \subset F_g^+(K)$, we need only show that

$$\gcd(|\text{Gal}(M/K)|, h^+(\mathcal{O}_f)/h^+(\mathcal{O}_g)) = 1, \quad (3.14)$$

as $h^+(\mathcal{O}_f)/h^+(\mathcal{O}_g) = |\text{Gal}(F_f^+(K)/F_g^+(K))|$ (see proof of Lemma 3.2.1). To do this, we set $h = f_2 \prod_{r|f_2, r \nmid f_2'} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right)$, and show that

$$h^+(\mathcal{O}_f)/h^+(\mathcal{O}_g) \mid h, \quad (3.15)$$

and

$$\gcd(|G(M/K)|, h) = 1. \quad (3.16)$$

We consider two cases according as d_K is negative or positive.

(i) If $d_K < 0$, by Lemmas 3.2.4 and 3.2.2, we have

$$\frac{h^+(\mathcal{O}_f)}{h^+(\mathcal{O}_g)} = \frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \begin{cases} \frac{h}{f_2'} \prod_{r|f_2, r \nmid f_2'} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), & \text{if } g \neq 1, \\ \frac{h}{u_f} \prod_{r|f_2} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right), & \text{if } g = 1, \end{cases}$$

so that (3.15) holds.

(ii). If $d_K > 0$, by Lemma 3.2.2 we have

$$\frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \frac{f_2}{v f_2'} \prod_{r|f_2, r \nmid f_2'} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right) = \frac{h}{v f_2'},$$

where v is such that $\epsilon_f = \epsilon_g^v$ (see proof of Lemma 3.2.4). By Lemma 3.2.4, we have

$$\frac{h^+(\mathcal{O}_f)}{h^+(\mathcal{O}_g)} = \begin{cases} \frac{2h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \frac{2h}{v f_2'}, & \text{if } N_{K/Q}(\epsilon_f) = 1, N_{K/Q}(\epsilon_g) = -1, \\ \frac{h(\mathcal{O}_f)}{h(\mathcal{O}_g)} = \frac{h}{v f_2'}, & \text{otherwise.} \end{cases}$$

For the case $N_{K/Q}(\epsilon_f) = 1$, $N_{K/Q}(\epsilon_g) = -1$, as $\epsilon_f = \epsilon_g^v$, we must have v is even so that (3.15) holds.

Now we show (3.16). Suppose that

$$\gcd(|\text{Gal}(M/K)|, h) \neq 1.$$

Then there is a prime p in A such that

$$p \mid f_2 \prod_{r|f_2, r \nmid f_2'} \left(1 - \left(\frac{d_K}{r}\right) \frac{1}{r}\right).$$

Hence there is a prime r_0 with $r_0 | f_2$ and $r_0 \nmid f_2'$ such that

$$p | r_0 \left(1 - \left(\frac{d_K}{r_0}\right) \frac{1}{r_0}\right),$$

so that $r_0 \in B$. Further, since $f_2' = \prod_{q \in B} q$, we have $r_0 \mid f_2'$. This is a contradiction.

■

Lemma 3.2.8 *Let $\mathcal{O}_f$ be an order in a quadratic field K of.*

(i) *If $\mathcal{A}$ is an $\mathcal{O}_K$ -ideal prime to f , then $\mathcal{A} \cap \mathcal{O}_f$ is an $\mathcal{O}_f$ -ideal prime to f of the same norm.*

(ii) *If $\mathcal{A}$ is an $\mathcal{O}_f$ -ideal prime to f , then $\mathcal{A}\mathcal{O}_K$ is an $\mathcal{O}_K$ -ideal prime to f of the same norm.*

(iii) *The map $\mathcal{A} \longrightarrow \mathcal{A} \cap \mathcal{O}_f$ induces an isomorphism $I_K(f) \longrightarrow I(\mathcal{O}_f, f)$, and the inverse of this map is given by $\mathcal{A} \longrightarrow \mathcal{A}\mathcal{O}_K$.*

Proof: See [[11], Proposition 7.20, p.144]. ■

Lemma 3.2.9 *Let K be a quadratic field, and let $\mathcal{O}_f$ and $\mathcal{O}_{ft}$ be two orders in K . Let $\beta \in \mathcal{O}_f$ and $a \in \mathbb{Z}$, so that $[a, \beta]$ is an $\mathcal{O}_f$ -ideal and $[a, \beta t]$ is a $\mathcal{O}_{ft}$ -ideal. Then*

$$[a, \beta t]\mathcal{O}_f = [a, \beta].$$

Proof: Since $a, \beta t \in [a, \beta]$, we have $[a, \beta t]\mathcal{O}_f \subset [a, \beta]$. Let $\beta = c + df\omega_K$, $c, d \in \mathbb{Z}$, so that

$$(a, \beta) = (1, f\omega_K) \begin{pmatrix} a & c \\ 0 & d \end{pmatrix},$$

and thus $[a, \beta]$ has norm equal to $|\det \begin{pmatrix} a & c \\ 0 & d \end{pmatrix}| = |ad|$ as an $\mathcal{O}_f$ -ideal. Since

$$(a, \beta t) = (1, ft\omega_K) \begin{pmatrix} a & ct \\ 0 & d \end{pmatrix},$$

$[a, \beta t]$ has norm equal to $|\det \begin{pmatrix} a & ct \\ 0 & d \end{pmatrix}| = |ad|$, as an $\mathcal{O}_{ft}$ -ideal. By Lemma 3.2.8, $[a, \beta t]\mathcal{O}_f$ has norm $|ad|$. Now note that as the two $\mathcal{O}_f$ -ideals $[a, \beta t]\mathcal{O}_f$ and $[a, \beta]$ have the same norm and $[a, \beta t]\mathcal{O}_f \subset [a, \beta]$, it follows that $[a, \beta t]\mathcal{O}_f = [a, \beta]$. ■

Lemma 3.2.10 *Let K be a quadratic field, and let M be a normal extension of K . Let f and g be two positive integers with $g|f$ and suppose $M \subset F_f^+(K)$. Let μ denote the natural surjective homomorphism $\mu : \text{Gal}(F_f^+(K)/K) \longrightarrow \text{Gal}(F_g^+(K)/K)$, then*

$$([\text{Gal}(F_g^+(K)/K) : \mu(\text{Gal}(F_f^+(K)/M))] = [M : K]) \implies M \subset F_g^+(K).$$

Proof: Since μ is surjective, elementary group theory shows that

$$\text{Gal}(F_f^+(K)/K)/\text{Gal}(F_f^+(K)/M) \ker \mu \simeq \text{Gal}(F_g^+(K)/K)/\mu(\text{Gal}(F_f^+(K)/M)).$$

Then we have

$$\begin{aligned} [\text{Gal}(F_f^+(K)/K) : \text{Gal}(F_f^+(K)/M) \ker \mu] &= [\text{Gal}(F_g^+(K)/K) : \mu(\text{Gal}(F_f^+(K)/M))] \\ &= [M : K] = |\text{Gal}(M/K)| = [\text{Gal}(F_f^+(K)/K) : \text{Gal}(F_f^+(K)/M)], \end{aligned}$$

and thus

$$\text{Gal}(F_f^+(K)/M) \ker \mu = \text{Gal}(F_f^+(K)/M),$$

which implies that

$$\ker \mu \subset \text{Gal}(F_f^+(K)/M).$$

As

$$\ker \mu = \text{Gal}(F_f^+(K)/F_g^+(K)),$$

we have

$$\text{Gal}(F_f^+(K)/F_g^+(K)) \subset \text{Gal}(F_f^+(K)/M).$$

Then by Galois theory we deduce $M \subset F_g^+(K)$. $\blacksquare$

Lemma 3.2.11 *Let K be a quadratic field. Let f and g be positive integers with $g \mid f$. Consider the diagram*

$$\begin{array}{ccccc} H(d_K f^2) & \xrightarrow{\nu} & C^+(\mathcal{O}_f) & \xrightarrow{\phi} & \text{Gal}(F_f^+(K)/K) \\ \downarrow \kappa & & & & \downarrow \mu \\ H(d_K g^2) & \xrightarrow{\nu} & C^+(\mathcal{O}_g) & \xrightarrow{\phi} & \text{Gal}(F_g^+(K))/K \end{array}$$

where ν denotes the isomorphism between the form class group and the ideal class group given in Lemma 1.9.10, ϕ denotes the isomorphism induced by the Artin map, μ is as in Lemma 3.2.10 and κ denotes the Gauss surjective homomorphism

$$H(d_K f^2) \longrightarrow H(d_K g^2),$$

which is given by

$$\kappa([a, bf, cf^2]) = [a, bg, cg^2],$$

where $[a, b, c]$ denotes the class of the form (a, b, c) . Then the diagram commutes.

Proof: Let G be a form class of discriminant $d_K f^2$. Without loss of generality we may assume that $G = [a, bf, cf^2]$. Set

$$I = \begin{cases} [a, \frac{-bf + \sqrt{d_K f^2}}{2}] & \text{if either } d_K < 0 \text{ or } d_K > 0 \text{ and } a > 0, \\ \sqrt{d_K} [a, \frac{-bf + \sqrt{d_K f^2}}{2}] & \text{if } d_K > 0 \text{ and } a < 0, \end{cases}$$

and

$$J = \begin{cases} [a, \frac{-bg + \sqrt{d_K g^2}}{2}] & \text{if either } d_K < 0 \text{ or } d_K > 0 \text{ and } a > 0, \\ \sqrt{d_K} [a, \frac{-bg + \sqrt{d_K g^2}}{2}] & \text{if } d_K > 0 \text{ and } a < 0, \end{cases}$$

so that $I\mathcal{O}_g = J$. Then we have

$$\begin{aligned} \mu\phi\nu(G) &= \mu\phi\nu([a, bf, cf^2]) = \mu\phi([I]) = \mu\left(\left(\frac{F_f^+(K)/K}{I}\right)\right) = \left(\frac{F_g^+(K)/K}{J}\right) \\ \phi &= (J) = \phi\nu([a, bg, cg^2]) = \phi\nu\kappa([a, bf, cf^2]) = \phi\nu\kappa(G), \end{aligned}$$

proving the commutativity of the diagram. ■

Lemma 3.2.12 *Let M be a dihedral extension, and let K be a quadratic field in K_M . Let f and g be two positive integers with $g \mid f$ and suppose that $M \subset F_f^+(K)$. Let H be the subgroup of $H(d_K f^2)$ such that $\text{Gal}(F_f^+(K)/M) \simeq H$ under the isomorphism $\text{Gal}(F_f^+(K)/K) \simeq H(d_K f^2)$. Let κ denote the Gauss surjective homomorphism $H(d_K f^2) \longrightarrow H(d_K g^2)$ defined in Lemma 3.2.11, then*

$$([H(d_K g^2) : \kappa(H)] = [M : K]) \implies M \subset F_g^+(K).$$

Proof: This is an immediate corollary of Lemma 3.2.11 and Lemma 3.2.10. ■

Remark: Let f be a positive integer such that $f_0(M/K) \mid f$. Then Lemma 3.2.6, Lemma 3.2.10 and Lemma 3.2.12 tell us how to find a ‘smaller f ’ from the given ‘larger f ’.

Chapter 4

DETERMINATION OF THE CONDUCTOR $f(M/K)$

In this chapter, we first prove Theorem 4.1.3 which gives the finite part of the conductor of the extension M/K , where M is a dihedral extension of Q with $\text{Gal}(M/Q) = D_q$, for some odd prime q , and K is the unique quadratic subfield of M . Then we prove Theorem 4.3.5 which, on the one hand, is a necessary preliminary result needed in the proof of Theorem 4.4.11, and, on the other hand, enables us to determine the genus field of both the strict ring class field $F_f^+(K)$ and the ordinary ring class field $F_f(K)$ (defined in Chapter 1), see Theorems 4.3.12 and 4.3.13.

4.1 Proof of Theorem 4.1.3

Lemma 4.1.1 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_q$, where q is a prime. Let K be the unique quadratic field in M . Suppose $\mathcal{B}$ is a prime ideal of K dividing $f_0(M/K)$ with $\mathcal{B} \cap Z = pZ$. Then $p = q$ or $p \equiv \left(\frac{d_K}{p}\right) \pmod{q}$. In particular, $p (\neq q)$ is not totally ramified in M .*

Proof: By Lemma 3.1.6, we have $M \subset F_f^+(K)$ for any positive integer f with $f_0(M/K) \mid f$. Then, by Lemma 3.2.7, we have $M \subset F_g^+(K) = F_{f_1 f_2}^+(K)$, where f_1 and f_2' are defined in Lemma 3.2.7.

Next as $\mathcal{B}$ ramifies in M , we have $\mathcal{B}$ ramifies in $F_{f_1 f_2}^+(K)$ so that $\mathcal{B} \mid f_1 f_2'$ by the Conductor theorem of class field theory. Now, since $f_1 f_2'$ is in Z and $\mathcal{B} \cap Z = pZ$, we have

$p \mid f_1 f_2'$, so that $p \mid f_1$ or $p \mid f_2'$.

(i) If $p|f_1$, then $p = q$ as $A = \{q\}$.

(ii) If $p|f'_2$, then $p \equiv \left(\frac{d_K}{p}\right) \pmod{q}$ as $A = \{q\}$. ■

Lemma 4.1.2 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_q = \langle \sigma, \tau \rangle$, for which $\sigma^q = \tau^2 = (\sigma\tau)^2 = 1$, where q is a prime. Let K be the quadratic field fixed by σ and let L be the fixed field of τ . Suppose $p \neq q$ is a prime and $\mathcal{B}$ is a prime of $\mathcal{O}_K$ containing p . Suppose that p is unramified in K . Then*

$$v_{\mathcal{B}}(f_0(M/K)) \neq 0 \iff v_p(d_L) \neq 0. \quad (4.1)$$

If this is the case, we have

$$p \equiv \left(\frac{d_K}{p}\right) \pmod{q}.$$

Proof: Suppose that p is unramified in K . Then p is unramified in M/L . By Lemma 1.2.8 we have

$$d_M = d_L^2 N_{L/Q}(d(M/L)) = d_K^q N_{K/Q}(d(M/K)),$$

so that

$$2v_p(d_L) = v_p(N_{K/Q}(d(M/K))).$$

Further, by Lemma 1.2.12, we have $d(M/K) = f_0(M/K)^{q-1}$, thus

$$2v_p(d_L) = (q-1)v_p(N_{K/Q}(f_0(M/K))) = (q-1)v_{\mathcal{B}}(f_0(M/K)),$$

proving (4.1).

Now suppose that $v_{\mathcal{B}}(f_0(M/K)) \neq 0$. Then, by Lemma 4.1.1, as $p \neq q$, we have

$$p \equiv \left(\frac{d_K}{p}\right) \pmod{q}. \quad \blacksquare$$

Theorem 4.1.3 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_q = \langle \sigma, \tau \rangle$, for which $\sigma^q = \tau^2 = (\sigma\tau)^2 = 1$, where q is an odd prime. Let K be the quadratic field fixed by σ and let L be the fixed field of τ . Set*

$$\mathcal{S} = \{p : p(\text{prime}) \neq q, p \nmid d_L, p \equiv \left(\frac{d_K}{p}\right) \pmod{q}\},$$

and let f' denote the product of the primes in S . Then $f_0(M/K) = f_q f'$, where f_q is given as follows:

when $q \equiv 3 \pmod{4}$, $q > 3$,

$$f_q = \begin{cases} 1, & \text{if } q \text{ is unramified in } M/K, \\ q, & \text{if } q \text{ is totally ramified in } M, \\ q^2, & \text{if } q \text{ is unramified in } K \text{ but is ramified in } M/K, \end{cases}$$

when $q = 3$,

$$f_3 = \begin{cases} 1, & \text{if } 3 \text{ is unramified in } M/K, \\ 3 \text{ or } 3^2, & \text{if } 3 \text{ is totally ramified in } M, \\ 3^2, & \text{if } 3 \text{ is unramified in } K \text{ but is ramified in } M/K, \end{cases}$$

when $q \equiv 1 \pmod{4}$,

$$f_q = \begin{cases} 1, & \text{if } q \text{ is unramified in } M/K, \\ q \text{ or } q^{3/2}, & \text{if } q \text{ is totally ramified in } M, \\ q^2, & \text{if } q \text{ is unramified in } K \text{ but is ramified in } M/K. \end{cases}$$

Proof: Suppose that $\mathcal{P}$ is a prime of $\mathcal{O}_K$ dividing $f_0(M/K)$ and containing a prime p . Since M/K is an Abelian extension and $[M : K] = q$ is a prime, we must have that $\mathcal{P}$ is totally ramified in M , say $\mathcal{P}\mathcal{O}_M = \mathcal{B}^q$. By Lemma 1.2.12, we have $d(M/K) = f_0(M/K)^{q-1}$. Recall that $t(\mathcal{B}/\mathcal{P}) = v_{\mathcal{B}}(\text{diff}_{M/K}(\mathcal{O}_M))$. Then

$$\begin{aligned} (q-1)v_{\mathcal{P}}(f_0(M/K)) &= v_{\mathcal{P}}(d(M/K)) \\ &= v_{\mathcal{P}}(N_{M/K}(\text{diff}_{M/K}(\mathcal{O}_M))) \quad (\text{Lemma 1.2.18}) \\ &= v_{\mathcal{B}}(\text{diff}_{M/K}(\mathcal{O}_M)) \cdot f(\mathcal{B}/\mathcal{P}) = t(\mathcal{B}/\mathcal{P}), \end{aligned}$$

as

$$N_{M/K}(\mathcal{B}) = \mathcal{P}^{f(\mathcal{B}/\mathcal{P})} = \mathcal{P}.$$

For convenience we treat the cases (i) $p \neq q$ and (ii) $p = q$ separately.

Case (i): $p \neq q$. In this case $\mathcal{P}$ is tamely ramified. Hence, by Lemma 1.2.20, we have

$$t(\mathcal{B}/\mathcal{P}) = e(\mathcal{B}/\mathcal{P}) - 1 = q - 1.$$

Thus from above we have

$$(q-1)v_{\mathcal{P}}(f_0(M/K)) = q-1,$$

and so

$$v_{\mathcal{P}}(f_0(M/K)) = 1.$$

Next, by Lemma 4.1.1, $p \equiv \left(\frac{d_K}{p}\right) \pmod{q}$, and thus p is unramified in K . Hence p either remains prime in K or p splits in K . If p remains prime in K , then $p\mathcal{O}_K = \mathcal{P}$, and we have

$$v_p(f_0(M/K)) = 1.$$

If p splits in K , then

$$p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}',$$

and thus

$$\mathcal{P}'\mathcal{O}_M = \mathcal{B}'^q, \mathcal{B}' \neq \mathcal{B},$$

so that $\mathcal{P}'$ totally ramifies in M . Replacing $\mathcal{P}$ by $\mathcal{P}'$ in the previous proof, we obtain

$$v_{\mathcal{P}'}(f_0(M/K)) = 1.$$

Thus

$$\mathcal{P} \parallel f_0(M/K), \quad \mathcal{P}' \parallel f_0(M/K),$$

so that

$$p \parallel f_0(M/K), \text{ as } p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}',$$

that is

$$v_p(f_0(M/K)) = 1.$$

By Lemma 4.1.2, f' is the non- q part of $f_0(M/K)$.

Case (ii): $p = q$. First we suppose that q is unramified in K , then

$$v_{\mathcal{B}}(e(\mathcal{B}/\mathcal{P})) = v_{\mathcal{B}}(q) = q.$$

We have, by Lemma 1.2.20,

$$q \leq t(\mathcal{B}/\mathcal{P}) \leq v_{\mathcal{B}}(e(\mathcal{B}/\mathcal{P})) + e(\mathcal{B}/\mathcal{P}) - 1 = 2q - 1.$$

so that

$$q \leq (q-1)v_{\mathcal{P}}(f_0(M/K)) \leq 2q-1,$$

from which it follows that

$$v_{\mathcal{P}}(f_0(M/K)) = 2.$$

Since q is unramified in K , exactly as in the proof of case (i), we have

$$v_q(f_0(M/K)) = 2.$$

Secondly, we suppose that q ramifies in K . In this case q is totally ramified in M , and we have

$$v_{\mathcal{B}}(e(\mathcal{B}/\mathcal{P})) = v_{\mathcal{B}}(q) = 2q.$$

By Lemma 1.2.20 we have

$$q \leq t(\mathcal{B}/\mathcal{P}) \leq v_{\mathcal{B}}(e(\mathcal{B}/\mathcal{P})) + e(\mathcal{B}/\mathcal{P}) - 1 = 3q - 1,$$

so that

$$q \leq (q-1)v_{\mathcal{P}}(f_0(M/K)) \leq 3q-1,$$

from which it follows that

$$v_{\mathcal{P}}(f_0(M/K)) = \begin{cases} 2 \text{ or } 3, & \text{if } q > 3, \\ 2, 3 \text{ or } 4, & \text{if } q = 3. \end{cases}$$

If $v_{\mathcal{P}}(f_0(M/K)) \neq 3$, then

$$v_q(f_0(M/K)) = \begin{cases} 1, & \text{if } q > 3, \\ 1 \text{ or } 2, & \text{if } q = 3, \end{cases} \quad (4.2)$$

as $q\mathcal{O}_K = \mathcal{P}^2$.

Next we prove that if $q \equiv 3 \pmod{4}$ then $v_{\mathcal{P}}(f_0(M/K)) \neq 3$. In fact, from the formula (Lemma 1.2.8)

$$N_{L/Q}(d(M/L))d(L/Q)^2 = d_M = N_{K/Q}(d(M/K))d(K/Q)^q,$$

where L is the field fixed by τ , we have

$$v_q(N_{L/Q}(d(M/L))) + 2v_q(d_L) = v_q(N_{K/Q}(d(M/K))) + qv_q(d_K).$$

Noting that q is tamely ramified in both M/K and K/Q , we have

$$v_q(N_{L/Q}(d(M/L))) = 1 \text{ and } v_q(d_K) = 1,$$

and

$$v_q(N_{K/Q}(d(M/K))) = (q-1)v_q(N_{K/Q}(f_0(M/K))) = (q-1)v_{\mathcal{P}}(f_0(M/K)),$$

as $N_{K/Q}(\mathcal{P}) = qZ$. Thus we have

$$v_q(d_L) = \frac{q-1}{2}(1 + v_{\mathcal{P}}(f_0(M/K))). \quad (4.3)$$

Next, by Lemma 2.3.11, we have $K = Q(\sqrt{d_L})$. Since q ramifies in K , we must have that $v_q(d_L)$ is odd, so that by (4.3) $v_{\mathcal{P}}(f_0(M/K))$ is even as $\frac{q-1}{2}$ is odd. Hence if $q \equiv 3 \pmod{4}$ we have (4.2). This completes the proof of the theorem. ■

4.2 Determination of the Discriminant of a Dihedral Polynomial $\rho(x)$ whose Degree is an Odd Prime

In this section we always suppose that M is a cyclic dihedral extension with $\text{Gal}(M/Q) = D_q = \langle \sigma, \tau \rangle$, where q is an odd prime and $\sigma^q = \tau^2 = (\sigma\tau)^2 = 1$. Let K be the quadratic field fixed by σ , and let L be the field fixed by τ . Further, we always assume that p is a prime dividing d_L , and $\mathcal{P}$ is prime of K containing p .

Lemma 4.2.1 *Suppose that p ramifies in K , then*

$$\mathcal{P} \text{ is unramified in } M \implies \mathcal{P} \text{ splits completely in } M.$$

Proof: Since $[M : K] = q$ is a prime, $\mathcal{P}$ either splits completely in M or remains prime in M . If $\mathcal{P}$ remains prime in M , then $\mathcal{P}\mathcal{O}_M = \mathcal{B}$ is a prime of $\mathcal{O}_M$ and $e(\mathcal{B}/p) = 2$. Since $\mathcal{B}$ is the unique prime of M containing p , $\mathcal{B} \cap L$ is the unique prime of L containing p . Thus, by Lemma 1.2.4, we have

$$e(\mathcal{B} \cap L/p)f(\mathcal{B} \cap L/p) = [L : Q] = q,$$

which implies that $e(\mathcal{B} \cap L/p) = 1$ or q . As $e(\mathcal{B}/p) = 2 < q$ we must have

$$e(\mathcal{B} \cap L/p) = 1.$$

Thus p is unramified in L . This is impossible as $p|d_L$. ■

Lemma 4.2.2 *Suppose that p ramifies in K but does not ramify in the extension M/K . Then the prime decomposition of $p\mathcal{O}_L$ is given by*

$$p\mathcal{O}_L = U_1^2 \dots U_t^2 V_1 \dots V_s, \quad (4.4)$$

where t and s are integers such that $t \geq 1$ and $2t + s = q$, the V_j ramify in M , and $f(U_i/p) = f(V_j/p) = 1$ for $i = 1, \dots, t, j = 1, \dots, s$.

Proof: Let $\mathcal{P}$ be the prime ideal of K containing p . Then by Lemma 4.2.1 $\mathcal{P}$ splits completely in M , and thus

$$f(\mathcal{B}/\mathcal{P}) = e(\mathcal{B}/\mathcal{P}) = 1 \text{ for any prime } \mathcal{B} \text{ of } M \text{ containing } \mathcal{P}.$$

Since p ramifies in K , we have

$$f(\mathcal{P}/p) = 1 \text{ and } e(\mathcal{P}/p) = 2,$$

so that

$$f(\mathcal{B}/p) = f(\mathcal{B}/\mathcal{P})f(\mathcal{P}/p) = 1, \quad e(\mathcal{B}/p) = e(\mathcal{B}/\mathcal{P})e(\mathcal{P}/p) = 2.$$

Now let $\mathcal{W}$ be a prime ideal of $\mathcal{O}_L$ containing p . Then from

$$f(\mathcal{B}/p) = f(\mathcal{B}/\mathcal{W})f(\mathcal{W}/p) = 1, \quad e(\mathcal{B}/p) = e(\mathcal{B}/\mathcal{W})e(\mathcal{W}/p) = 2,$$

we have

$$f(\mathcal{W}/p) = 1 \text{ and } e(\mathcal{W}/p) = \begin{cases} 1, & \text{if } e(\mathcal{B}/\mathcal{W}) = 2, \\ 2, & \text{if } e(\mathcal{B}/\mathcal{W}) = 1. \end{cases}$$

as asserted. ■

Lemma 4.2.3 *Suppose that p ramifies in K but does not ramify in the extension M/K . Then for $p \neq 2$ we have*

$$v_p(d_L) = (q - s)/2 \text{ for some positive integer } s \equiv 1 \pmod{4}, \quad s \neq q,$$

for $p = 2$ we have

$$v_2(d_L) = \begin{cases} 3(q-s)/2 \text{ for some } q \not\equiv s \equiv 1 \pmod{4}, & \text{if } v_2(d_K) = 3, \\ q-s \text{ for some } s \equiv 1 \pmod{2}, & \text{if } v_2(d_K) = 2. \end{cases}$$

Proof: First we consider the case when $p \neq 2$. In this case the U_i of Lemma 4.2.2 are tamely ramified over Q . Thus

$$t(U_i/p) = e(U_i/p) - 1 = 2 - 1 = 1 \text{ for } 1 \leq i \leq t,$$

so that

$$v_p(d_L) = \sum_{i=1}^t f(U_i/p)t(U_i/p) = t = (q-s)/2 \geq 1.$$

Lemma 2.3.9 tells us that

$$(q-s)/2 \equiv 0 \text{ or } 1 \pmod{2} \text{ according as } q \equiv 1 \text{ or } 3 \pmod{4},$$

which implies that $s \equiv 1 \pmod{4}$.

Secondly, we treat the case when $p = 2$. In this case the U_i of Lemma 4.2.2 are strongly ramified over Q and the V_j of Lemma 4.2.2 are strongly ramified in M . By Lemma 1.2.20, we have

$$2 \leq t(U_i/p) \leq 3 \text{ and } 2 \leq t(\mathcal{B}/V_j) \leq 3,$$

where $V_j \mathcal{O}_M = \mathcal{B}_j^2$. Without loss of generality, we let

$$t(U_i/p) = 2 \text{ for } 1 \leq i \leq t_1, t(U_i/p) = 3 \text{ for } t_1 + 1 \leq i \leq t,$$

$$t(\mathcal{B}_j/V_j) = 2 \text{ for } 1 \leq j \leq s_1, t(\mathcal{B}_j/V_j) = 3 \text{ for } s_1 + 1 \leq j \leq s.$$

Then the formulae

$$N_{L/Q}(d(M/L))d_L^2 = d_M = N_{K/Q}(d(M/K))d_K^2$$

gives

$$v_2(N_{L/Q}(d(M/L))) + 2v_2(d_L) = v_2(N_{K/Q}(d(M/K))) + 2v_2(d_K).$$

Note that as

$$v_2(d_L) = 2t_1 + 3(t - t_1) = 3t - t_1,$$

$$v_2(N_{L/Q}(d(M/L))) = 2s_1 + 3(s - s_1) = 3s - s_1,$$

and 2 does not ramify in M/K , we have

$$(3s - s_1) + 2(3t - t_1) = qv_2(d_K).$$

Hence (recalling that $s + 2t = q$) we have

$$2t_1 + s_1 = q(3 - v_2(d_K)) = \begin{cases} q, & \text{if } v_2(d_K) = 2, \\ 0, & \text{if } v_2(d_K) = 3, \end{cases}$$

which implies that

$$t_1 = t \text{ and } s_1 = s \text{ if } v_2(d_K) = 2 \text{ and } s_1 = t_1 = 0 \text{ if } v_2(d_K) = 3,$$

and thus

$$v_2(d_L) = 3t - t_1 = \begin{cases} 2t = q - s, & \text{if } v_2(d_K) = 2, \\ 3t = 3(q - s)/2, & \text{if } v_2(d_K) = 3. \end{cases}$$

As $t \geq 1$ clearly we have $s \neq q$. Using the same argument as in the case when $p \neq 2$ we can prove when $v_2(d_K) = 3$ that $q \neq s \equiv 1 \pmod{4}$. ■

Lemma 4.2.4 *Suppose that p is totally ramified in M (so that $p = q$). Then for $q \neq 3$,*

$$v_q(d_L) = \begin{cases} \frac{3}{2}(q - 1), & \text{if } q \equiv 3 \pmod{4}, \\ \frac{3}{2}(q - 1) \text{ or } 2(q - 1), & \text{if } q \equiv 1 \pmod{4}, \end{cases}$$

and for $q = 3$,

$$v_3 = 3 \text{ or } 5.$$

Proof: Since q is totally ramified in M , exactly as in the proof of Theorem 4.1.3 we have (4.3), that is,

$$v_q(d_L) = \frac{q-1}{2}(1 + v_p(f_0(M/K))).$$

Since q is ramified in K we have $v_p(f_0(M/K)) = 2v_q(f_0(M/K))$, so that

$$v_q(d_L) = \frac{q-1}{2}(1 + 2v_q(f_0(M/K))).$$

Then appealing to Theorem 4.1.3, the lemma follows. ■

Lemma 4.2.5 Suppose p ramifies in M/K but does not ramify in K . Then

$$v_p(d_L) = \begin{cases} q-1, & \text{if } p \neq q, \\ 2(q-1), & \text{if } p = q. \end{cases}$$

Proof: By Theorem 4.1.3, in this case we have

$$v_p(f_0(M/K)) = \begin{cases} 1, & \text{if } p \neq q, \\ 2, & \text{if } p = q. \end{cases}$$

Since p does not ramify in K , we have that p does not ramify in M/L . By the formulae

$$N_{L/Q}(d(M/L))d_L^2 = d_M = N_{K/Q}(d(M/K))d_K^q,$$

$$d(M/K) = f_0(M/K)^{q-1},$$

we have

$$2v_p(d_L) = (q-1)v_p(N_{K/Q}(f_0(M/K))) = 2(q-1)v_p(f_0(M/K)).$$

Thus

$$v_p(d_L) = (q-1)v_p(f_0(M/K)) = \begin{cases} q-1, & \text{if } p \neq q, \\ 2(q-1), & \text{if } p = q. \end{cases} \quad \blacksquare$$

Putting together what we have proved, we have the following:

Theorem 4.2.6 Let p denote a prime dividing d_L . Then the values of $v_p(d_L)$ (≥ 1) are given as follows

(i) $p = q$, $q = 3$

$$v_3(d_L) = \begin{cases} 3 \text{ or } 5, & \text{if } 3 \text{ is totally ramified in } M, \\ 4, & \text{if } 3 \text{ does not ramify in } K \text{ but ramifies in } M/K, \\ 1, & \text{if } 3 \text{ ramifies in } K \text{ but does not ramify in } M/K. \end{cases}$$

(ii) $p = q \neq 3$, $q \equiv 3 \pmod{4}$

$$v_q(d_L) = \begin{cases} \frac{3}{2}(q-1), & \text{if } q \text{ is totally ramified in } M \text{ but ramifies in } M/K, \\ 2(q-1), & \text{if } q \text{ does not ramify in } K, \\ \frac{1}{2}(q-3), & \text{if } q \text{ ramifies in } K \text{ but does not ramify in } M/K, \end{cases}$$

where s is a positive integer satisfying $s \equiv 1 \pmod{4}$ and $s < q$.

(iii) $p = q$, $q \equiv 1 \pmod{4}$

$$v_q(d_L) = \begin{cases} \frac{3}{2}(q-1) \text{ or } 2(q-1), & \text{if } q \text{ is totally ramified in } M, \\ 2(q-1), & \text{if } q \text{ does not ramify in } K \text{ but ramifies in } M/K, \\ \frac{1}{2}(q-s), & \text{if } q \text{ ramifies in } K \text{ but does not ramify in } M/K, \end{cases}$$

where s is a positive integer satisfying $s \equiv 1 \pmod{4}$ and $s < q$.

(iv) $p \neq q$, $p \neq 2$

$$v_p(d_L) = \begin{cases} q-1, & \text{if } p \equiv \left(\frac{d_K}{p}\right) \pmod{q}, \\ \frac{1}{2}(q-s), & \text{if } p \not\equiv \left(\frac{d_K}{p}\right) \pmod{q}, \end{cases}$$

where s is a positive integer satisfying $s \equiv 1 \pmod{4}$ and $s < q$.

(v) $p = 2$

$$v_2(d_L) = \begin{cases} 3(q-s)/2 \text{ for some positive integer } s \equiv 1 \pmod{4}, & \text{if } v_2(d_K) = 3, \\ q-s > 0 \text{ for some positive integer } s \equiv 1 \pmod{2}, & \text{if } v_2(d_K) = 2. \end{cases}$$

Theorem 4.2.7 *Let M be a dihedral extension with $\text{Gal}(M/Q) = D_3$. Suppose $L \subset M$ and $[L:Q] = 3$, and let K be the unique quadratic field $\subset M$. Then*

$$d_L = d_K f_0(M/K)^2.$$

Proof: We show that for any prime p ,

$$v_p(d_L) = v_p(d_K) + 2v_p(f_0(M/K)). \quad (4.5)$$

We consider cases (i) p is unramified in M , (ii) p is totally ramified in M , (iii) p is ramified in K but not in M/K and (iv) p is unramified in K but does ramify in M/K .

Case (i). In this case p is unramified in L , K and M/K so that (4.5) holds.

Case (ii). In this case we must have $p = 3$ and $v_3(d_K) = 1$. By Theorem 4.1.3 we have

$$v_3(f_0(M/K)) = 1 \text{ or } 2,$$

and by Theorem 4.2.6 we have

$$v_3(d_L) = 3 \text{ or } 5,$$

so that (4.5) holds.

Case (iii). In this case we have $v_p(f_0(M/K)) = 0$. There are two possibilities: $p \neq 2$ or $p = 2$. First suppose $p \neq 2$. Then $v_p(d_K) = 1$ and Theorem 4.2.6(i) and (iv) give $v_p(d_L) = 1$ so that (4.5) holds. Now suppose $p = 2$. By Theorem 4.2.6(v) we have $v_2(d_L) = v_2(d_K)$ so that (4.5) holds.

Case (iv). In this case we have $v_p(d_K) = 0$. There are two possibilities: $p \neq 3$ or $p = 3$. First suppose $p \neq 3$. By Theorem 4.1.3, we have $v_p(f_0(M/K)) = 1$ and by Theorem 4.2.6(iv) we have $v_p(d_L) = 2$ so that (4.5) holds. Now suppose $p = 3$. By Theorem 4.1.3 we have $v_3(f_0(M/K)) = 2$ and by Theorem 4.2.6(i) we have $v_3(d_L) = 4$ so that (4.5) holds. This completes the proof of the theorem. ■

4.3 Proof of Theorem 4.3.5

Recall that a biquadratic field F is a composite field of two quadratic fields over Q . In this section we first prove Theorem 4.3.5 which gives the conductor of a biquadratic field F over one of its quadratic subfields. This theorem is then used to give the structure of the genus field of a ring class field (see Theorems 4.3.12 and 4.3.13).

Lemma 4.3.1 *Let F be a biquadratic field and let K be a quadratic subfield of F . Then $N_{K/Q}(f_0(F/K)) = g^2$, where g is a positive integer.*

Proof: By Lemma 1.2.8, we have

$$d_F = d_K^2 N_{K/Q}(d(F/K)) = d_K^2 N_{K/Q}(f_0(F/K)),$$

so that

$$N_{K/Q}(f_0(F/K)) = d_F/d_K^2.$$

As $\text{Gal}(F/Q) = D_2 \subset A_4$ we have $d_F \in \mathbb{Z}^2$, and the lemma follows. ■

Lemma 4.3.2 *Let K be a quadratic field and let M be a finite Abelian extension of K . Let p be a prime and let $\mathcal{P}$ be a prime of K containing p .*

(i) If $p\mathcal{O}_K = \mathcal{P}$, then the p -part of $f_0(M/K)$ is a positive integer and $v_p(f_0(M/K)) = v_{\mathcal{P}}(f_0(M/K))$.

(ii) If $p\mathcal{O}_K = \mathcal{P}^2$ and $N_{K/Q}(f_0(M/K)) \in \mathbb{Z}^2$, then the p -part of $f_0(M/K)$ is a positive integer and $v_p(f_0(M/K)) = v_{\mathcal{P}}(f_0(M/K))/2$.

Proof: Case (i) is obvious. Now we consider case (ii). Suppose that $\mathcal{P}^t \parallel f_0(M/K)$. Then $\mathcal{P}^t \parallel N_{K/Q}(f_0(M/K))$. Since $N_{K/Q}(f_0(M/K)) \in \mathbb{Z}^2$, we see that t is even. Then from $\mathcal{P}^t \parallel f_0(M/K)$ we have $\mathcal{P}^{t/2} \parallel f_0(M/K)$. This complete the proof of the lemma. ■

Lemma 4.3.3 *Let F be a biquadratic field and let K be a quadratic subfield of F . Let p be a prime which splits in K and ramifies in F/K . Then the p -part of $f_0(F/K)$ is a positive integer and given by*

$$\begin{cases} 2^2, 2^3, & \text{if } p = 2, \\ p, & \text{if } p \neq 2. \end{cases}$$

Proof: Let $\mathcal{P}$ be a prime of K dividing $f_0(F/K)$ and containing the prime p . We show that

$$p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}' \implies v_{\mathcal{P}}(f_0(F/K)) = v_{\mathcal{P}'}(f_0(F/K)). \quad (4.6)$$

First we suppose that p is odd. Then $\mathcal{P}$ is tamely ramified in F , and by Lemma 1.2.20, we have

$$v_{\mathcal{P}}(f_0(F/K)) = v_{\mathcal{P}}(d(F/K)) = 1.$$

Next, since $Q \subset F$ is a normal extension, $\mathcal{P} \mid f_0(F/K)$ implies that $\mathcal{P}' \mid f_0(F/K)$. Replacing $\mathcal{P}$ by $\mathcal{P}'$ in the above formula, we obtain

$$v_{\mathcal{P}'}(f_0(F/K)) = v_{\mathcal{P}'}(d(F/K)) = 1.$$

This proves that (4.6) holds and $v_p(f_0(F/K)) = 1$.

Now we suppose that $p = 2$. Let $t = v_{\mathcal{P}}(f_0(F/K))$ and $t' = v_{\mathcal{P}'}(f_0(F/K))$. Then $2^{t+t'} \parallel N_{K/Q}(f_0(F/K))$. By Lemma 4.3.1, we have $N_{K/Q}(f_0(F/K)) \in \mathbb{Z}^2$ so that

$$t + t' \equiv 0 \pmod{2}. \quad (4.7)$$

On the other hand, by Lemma 1.2.20, we have

$$2 \leq t \leq 3, \quad 2 \leq t' \leq 3. \quad (4.8)$$

Putting (4.7) and (4.8) together, we see that $t = t' = 2$ or 3 . This proves that (4.6) holds and $v_p(f_0(F/K)) = 2$ or 3 . This completes the proof of the lemma. ■

Lemma 4.3.4 *Let F be a biquadratic field and let K be a quadratic subfield of F . Then $f_0(F/K)$ is a positive integer. Moreover the 2-part of $f_0(F/K)$ is given by*

$$\begin{cases} 1, & \text{if 2 is unramified in } F/K, \\ 2, 2^2, & \text{if 2 is totally ramified in } F/Q, \\ 2^2, 2^3, & \text{if 2 ramifies in } F/K \text{ but does not ramify in } K/Q. \end{cases}$$

and for a prime $p \neq 2$, the p -part of $f_0(F/K)$ is given by

$$\begin{cases} 1, & \text{if } p \text{ is unramified in } F/K, \\ p, & \text{otherwise.} \end{cases}$$

Proof: Let $\mathcal{P}$ be a prime of K containing p . Without loss of generality we can suppose that $\mathcal{P}$ ramifies in F so that $\mathcal{P}\mathcal{O}_F = \mathcal{B}^2$. By Lemma 1.2.18 we have

$$\begin{aligned} v_{\mathcal{P}}(f_0(F/K)) &= v_{\mathcal{P}}(d(F/K)) = v_{\mathcal{P}}(N_{F/K}(\text{diff}_{F/K}(\mathcal{O}_F))) \\ &= v_{\mathcal{B}}(\text{diff}_{F/K}(\mathcal{O}_F)) = t(\mathcal{B}/\mathcal{P}). \end{aligned} \tag{4.9}$$

First we suppose $p = 2$. We treat cases (i) 2 remains prime in K , (ii) 2 ramifies in K and (iii) 2 splits completely in K separately.

Case (i). Since $\mathcal{B}/\mathcal{P}$ is strongly ramified, by Lemma 1.2.20 we have $2 \leq t(\mathcal{B}/\mathcal{P}) \leq 3$. Then by Lemma 4.3.2(i) and (4.9) we obtain

$$v_2(f_0(F/K)) = v_{\mathcal{P}}(f_0(F/K)) = 2 \text{ or } 3.$$

Case (ii). In this case 2 is totally ramified in F so that $2\mathcal{O}_F = \mathcal{B}^4$. By Lemma 1.2.20 we have $2 \leq t(\mathcal{B}/\mathcal{P}) \leq 5$. Then by Lemma 4.3.2(ii) and (4.9) we obtain

$$v_2(f_0(F/K)) = v_{\mathcal{P}}(f_0(F/K))/2 = 1 \text{ or } 2.$$

Case (iii). The assertion follows from Lemma 4.3.3.

Now we suppose that $p \neq 2$. We treat cases (i) p remains prime in K , (ii) p ramifies in K and (iii) p splits completely in K separately.

Case (i). Since $\mathcal{B}/\mathcal{P}$ is tamely ramified, by Lemma 1.2.20 we have $t(\mathcal{B}/\mathcal{P}) = 1$. Then by Lemma 4.3.2(i) and (4.9) we obtain

$$v_p(f_0(F/K)) = v_{\mathcal{P}}(f_0(F/K)) = 1.$$

Case (ii). It is impossible.

Case (iii). The assertion follows from Lemma 4.3.3. ■

Theorem 4.3.5 *Let F be a biquadratic field and let K be a quadratic subfield of F . Then the $f_0(F/K)$ is given by*

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{\frac{1}{2}},$$

where k and k' are the other two quadratic subfields of F .

Proof: As

$$d_F = d_K^2 N_{K/Q}(d(F/K)) \text{ (Lemma 1.2.8),}$$

$$d(F/K) = f_0(F/K), \quad d_F = d_K d_k d_{k'}, \text{ (Lemmas 1.2.12 and 1.2.13),}$$

we have

$$N_{K/Q}(f_0(F/K)) = d_k d_{k'} / d_K.$$

Further, as $f_0(F/K)$ is a positive integer, the above formula gives

$$f_0(F/K)^2 = d_k d_{k'} / d_K,$$

so that

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2}. \quad \blacksquare$$

Theorem 4.3.6 *Let n and m be two distinct squarefree integers. Set $K = Q(\sqrt{n})$, $k = Q(\sqrt{m})$ and $F = Q(\sqrt{n}, \sqrt{m})$. Let $g = \gcd(n, m)$. Then*

$$\begin{aligned} \text{(i)} \quad f_0(F/K) &= |m/g| \quad \text{if} \quad \begin{cases} m \equiv 1 \pmod{4} \text{ or} \\ n \equiv m \equiv 3 \pmod{4} \text{ or} \\ n \equiv m \equiv \pm 2 \pmod{8}, \end{cases} \\ \text{(ii)} \quad f_0(F/K) &= 2|m/g| \quad \text{if} \quad \begin{cases} n \equiv 3 \pmod{4} \text{ and } m \equiv 2 \pmod{4} \text{ or} \\ n \equiv 2 \pmod{4} \text{ and } m \equiv 3 \pmod{4} \text{ or} \\ n \equiv -m \equiv \pm 2 \pmod{8}, \end{cases} \\ \text{(iii)} \quad f_0(F/K) &= 4|m/g| \quad \text{if} \quad n \equiv 1 \pmod{4} \text{ and } m \equiv 2, 3 \pmod{4}. \end{aligned}$$

Proof: Since $g = \gcd(n, m)$, $n' = nm/g^2$ is squarefree and $k' = Q(\sqrt{n'})$ is the third quadratic subfield of F .

First we treat case (i). If $m \equiv 1 \pmod{4}$, then g is an odd integer, and we have

$$n' \equiv n'g^2 \equiv nm \equiv n \pmod{4}. \quad (4.10)$$

Thus

$$d_K = cn, d_{k'} = cn', \text{ where } c = 1 \text{ or } 4.$$

By Theorem 4.3.5, we have

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{m \cdot cn' / cn} = |m/g|.$$

If $n \equiv m \equiv 3 \pmod{4}$, then we have

$$n' \equiv n'g^2 \equiv nm \equiv 1 \pmod{4}.$$

Thus we have

$$d_{K'} = 4n, d_k = 4m, d_{k'} = n'. \quad (4.11)$$

Then, by Theorem 4.3.5, we have

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{4m \cdot n' / 4n} = |m/g|.$$

Similarly, if $n \equiv m \equiv \pm 2 \pmod{8}$, we have $n' \equiv 1 \pmod{4}$. Thus, by Theorem 4.3.5,

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{4m \cdot n' / 4n} = |m/g|.$$

Now we treat case (ii). First we suppose that either $n \equiv 3 \pmod{4}$ and $m \equiv 2 \pmod{4}$ or $n \equiv 2 \pmod{4}$ and $m \equiv 3 \pmod{4}$. We have

$$n' \equiv n'g^2 \equiv nm \equiv 2 \pmod{4}.$$

Thus we have

$$d_{K'} = 4n, d_k = 4m, d_{k'} = 4n'. \quad (4.12)$$

Then, by Theorem 4.3.5, we have

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{4m \cdot 4n' / 4n} = 2|m/g|.$$

Similarly, if $n \equiv -m \equiv \pm 2 \pmod{8}$, we have

$$d_{K'} = 4n, d_k = 4m, d_{k'} = 4n'.$$

Then, by Theorem 4.3.5, we have

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{4m \cdot 4n'/4n} = 2|m/g|.$$

Finally, we consider case (iii). Here $n \equiv 1 \pmod{4}$, and $m \equiv 2, 3 \pmod{4}$, so that

$$n' \equiv n'g^2 \equiv nm \equiv m \pmod{4},$$

and

$$d_K = n, d_k = 4m, d_{k'} = 4n'. \quad (4.13)$$

Then, by Theorem 4.3.5, we have

$$f_0(F/K) = \left(\frac{d_k d_{k'}}{d_K} \right)^{1/2} = \sqrt{4m \cdot 4n'/n} = 4|m/g|. \quad \blacksquare$$

Lemma 4.3.7 *Let n and m be two distinct squarefree integers. Set $K = Q(\sqrt{n})$ and $k = Q(\sqrt{m})$. Let f be a positive integer, and let $F_f^+(K)$ denote the strict ring class field of the order in K of conductor f . Then*

$$k \subset F_f^+(K) \implies m \mid nf.$$

Proof: Let $g = \gcd(n, m)$. Since $K \neq k$, $F = Q(\sqrt{n}, \sqrt{m})$ is a biquadratic field. By Theorem 4.3.6, we have

$$f_0(F/K) = cm/g, \quad c = 1, 2 \text{ or } 4. \quad (4.14)$$

Now suppose that $k \subset F_f^+(K)$, then $F \subset F_f^+(K)$. Appealing to Theorem 1.2.9, we see that $f_0(F/K) \mid f$. Then, by (4.14), we have $m/g \mid f$, which is equivalent to $m \mid nf$. $\blacksquare$

Lemma 4.3.8 *Let n and m be two distinct squarefree positive integers. Set $K = Q(\sqrt{n})$ and $k = Q(\sqrt{m})$. Let f be a positive integer, and let $F_f(K)$ denote the ring class field of the order in K of conductor f . Then*

$$k \subset F_f(K) \implies m \mid nf.$$

Proof: Let $g = \gcd(n, m)$. Since $K \neq k$, $F = Q(\sqrt{n}, \sqrt{m})$ is a biquadratic field. By Theorem 4.3.6, we have

$$f_0(F/K) = c|m/g|, \quad c = 1, 2 \text{ or } 4. \quad (4.15)$$

Now suppose that $k \subset F_f(K)$, then $F \subset F_f(K)$. Appealing to Theorem 1.2.9, we see that $f_0(F/K) \mid f$. Then, by (4.15), we have $m/g \mid f$, which is equivalent to $m \mid nf$. ■

Lemma 4.3.9 *Let n be a squarefree integer. Let $K = Q(\sqrt{n})$. Let f be a positive integer. Suppose that m is a squarefree integer dividing nf .*

(i) *If either $m \equiv 1 \pmod{4}$ or $n \equiv m \equiv 3 \pmod{4}$ or $n \equiv m \equiv \pm 2 \pmod{8}$, then*

$$k = Q(\sqrt{m}) \subset F_f^+(K).$$

(ii) *If either $n \equiv 2 \pmod{4}$ and $m \equiv 3 \pmod{4}$ or $n \equiv -m \equiv \pm 2 \pmod{8}$, then*

$$k = Q(\sqrt{m}) \subset F_f^+(K) \iff 2 \mid f.$$

(iii) *If either $n \equiv 3 \pmod{4}$ and $m \equiv 2 \pmod{4}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 3 \pmod{4}$, then*

$$k = Q(\sqrt{m}) \subset F_f^+(K) \iff 2^2 \mid f.$$

(iv) *If $n \equiv 1 \pmod{4}$ and $m \equiv 2 \pmod{4}$, then*

$$k = Q(\sqrt{m}) \subset F_f^+(K) \iff 2^3 \mid f.$$

Proof: Let $g = \gcd(n, m)$. It is obvious that

$$m \mid nf \iff m/g \mid f.$$

By Lemma 3.1.6, we have

$$F \subset F_f^+(K) \iff f_0(F/K) \mid f.$$

By Theorem 4.3.6, we have

$$f_0(F/K) = c|m/g|,$$

where $c = 1, 2$ or 4 in cases (i), (ii) or (iii) respectively. Thus we have

$$F \subset F_f^+(K) \iff f_0(F/K) \mid f \iff cm/g \mid f \iff c \mid f/(m/g). \quad (4.16)$$

From (4.16) we see immediately that (i) follows. For the cases when either $n \equiv 2 \pmod{4}$ and $m \equiv 3 \pmod{4}$ or $n \equiv -m \equiv \pm 2 \pmod{8}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 3 \pmod{4}$, as m/g is an odd integer, thus

$$F \subset F_f^+(K) \iff c \mid f.$$

For the remaining cases, that is, either $n \equiv 3 \pmod{4}$ and $m \equiv 2 \pmod{4}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 2 \pmod{4}$, since $2 \parallel m/g$, we have

$$F \subset F_f^+(K) \iff 2c \mid f. \quad \blacksquare$$

Lemma 4.3.10 *Let n be a squarefree positive integer. Let $K = Q(\sqrt{n})$. Let f be a positive integer. Suppose that m is a positive squarefree integer dividing nf .*

(i) *If either $m \equiv 1 \pmod{4}$ or $n \equiv m \equiv 3 \pmod{4}$ or $n \equiv m \equiv \pm 2 \pmod{8}$, then*

$$k = Q(\sqrt{m}) \subset F_f(K).$$

(ii) *If either $n \equiv 2 \pmod{4}$ and $m \equiv 3 \pmod{4}$ or $n \equiv -m \equiv \pm 2 \pmod{8}$, then*

$$k = Q(\sqrt{m}) \subset F_f(K) \iff 2 \mid f.$$

(iii) *If either $n \equiv 3 \pmod{4}$ and $m \equiv 2 \pmod{4}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 3 \pmod{4}$, then*

$$k = Q(\sqrt{m}) \subset F_f(K) \iff 2^2 \mid f.$$

(iv) *If $n \equiv 1 \pmod{4}$ and $m \equiv 2 \pmod{4}$, then*

$$k = Q(\sqrt{m}) \subset F_f(K) \iff 2^3 \mid f.$$

Proof: Let $g = \gcd(n, m)$. It is obvious that

$$m \mid nf \iff m/g \mid f.$$

By Lemma 3.1.7, we have

$$F \subset F_f(K) \iff f_0(F/K) \mid f.$$

By Theorem 4.3.6, we have

$$f_0(F/K) = cm/g,$$

where $c = 1, 2$ or 4 in cases (i), (ii) or (iii) respectively. Thus we have

$$F \subset F_f(K) \iff f_0(F/K) \mid f \iff cm/g \mid f \iff c \mid f/(m/g). \quad (4.17)$$

From (4.17) we see immediately that (i) follows. For the cases when either $n \equiv 2 \pmod{4}$ and $m \equiv 3 \pmod{4}$ or $n \equiv -m \equiv \pm 2 \pmod{8}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 3 \pmod{4}$, m/g is an odd integer, thus

$$F \subset F_f(K) \iff c \mid f.$$

For the remaining cases, that is, either $n \equiv 3 \pmod{4}$ and $m \equiv 2 \pmod{4}$ or $n \equiv 1 \pmod{4}$ and $m \equiv 2 \pmod{4}$, since $2 \parallel m/g$, we have

$$F \subset F_f(K) \iff 2c \mid f. \quad \blacksquare$$

Lemma 4.3.11 *Let M be a dihedral extension with $G = \text{Gal}(M/Q) = \langle H, \tau \rangle$. Let K be the fixed field of H . Let $\tilde{M}$ be the field fixed by the commutative subgroup G' of G . Then $\tilde{M}$ is the maximal extension of K contained in M which is Abelian over Q . Moreover, $\tilde{M}$ is the composite field of all the quadratic fields contained in M and $[\tilde{M} : K] = 2^s$, where s is 2-rank of H .*

Proof: Let L be an Abelian extension of K contained in M , so that $\text{Gal}(L/Q)$ is an Abelian group. Hence $G/\text{Gal}(M/L) \simeq \text{Gal}(L/Q)$ is an Abelian group. Thus $G' \subset \text{Gal}(M/L)$, that is $\text{Gal}(M/\tilde{M}) \subset \text{Gal}(M/L)$. Then, by Galois theory, $L \subset \tilde{M}$. This proves that $\tilde{M}$ is the maximal extension of K contained in M which is Abelian over Q .

Now, by Lemma 2.1.2, $\text{Gal}(\tilde{M}/Q) \simeq G/G'$ is an elementary 2-group. Then, by Galois theory, $\tilde{M}$ is the composite field of a finite number of quadratic fields. It is clear that these quadratic fields are contained in M . Next, we show that if k is a quadratic

field $\subset M$, then $k \subset \tilde{M}$. Since the composite field kK of k and K is an Abelian extension of Q contained in M , we have $k \subset Kk \subset \tilde{M}$.

The last assertion of the lemma follows from that $\text{Gal}(\tilde{M}/K) \simeq H/H^2$. ■

Theorem 4.3.12 *Let $K = Q(\sqrt{n})$ be a quadratic field, where n is a squarefree integer. Let f be a positive integer. Suppose that $p_1, p_2, \dots, p_r$ are the distinct odd primes dividing nf . Set $p_i^* = (-1)^{(p_i-1)/2} p_i$. Then the genus field $K^+(f)$ of the strict ring class field $F_f^+(K)$ is given by*
when $n \equiv 1 \pmod{4}$,

$$K^+(f) = \begin{cases} Q(\sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \parallel f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^3 \mid f, \end{cases}$$

when $n \equiv 3 \pmod{4}$,

$$K^+(f) = \begin{cases} Q(\sqrt{-1}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2^2 \mid f, \end{cases}$$

when $n \equiv 2 \pmod{8}$,

$$K^+(f) = \begin{cases} Q(\sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \mid f, \end{cases}$$

and when $n \equiv 6 \pmod{8}$,

$$K^+(f) = \begin{cases} Q(\sqrt{-2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \nmid f, \\ Q(\sqrt{-1}, \sqrt{2}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}), & \text{if } 2 \mid f, \end{cases}$$

Proof: Since the proofs are similar, we only treat the case $n \equiv 3 \pmod{4}$. By Lemma 4.3.11, $K^+(f)$ is the composite field of all the quadratic subfields of $F_f^+(K)$. First we show that for any odd prime $p \mid nf$,

$$Q(\sqrt{p^*}) \subset F_f^+(K). \quad (4.18)$$

If $p^* = n$, we have $Q(\sqrt{p^*}) = K \subset F_f^+(K)$ so that (4.18) holds. If $p^* \neq n$, then $F = Q(\sqrt{n}, \sqrt{p^*})$ is a biquadratic field. Since $p^* \equiv 1 \pmod{4}$, by Theorem 4.3.6, we have

$$f_0(F/K) = f_0(Q(\sqrt{n}, \sqrt{p^*})/K) = p/g,$$

where $g = \gcd(n, p)$. Since $p \mid nf$, we have $p/g \mid n/g \cdot f$, and as $\gcd(p/g, n/g) = 1$, we see that $p/g \mid f$, that is $f_0(F/K) = f_0(Q(\sqrt{n}, \sqrt{p^*})/K) \mid f$. Now appealing to Lemma 3.1.6 we see that $Q(\sqrt{n}, \sqrt{p^*}) \subset F_f^+(K)$, so that we have (4.18). Hence we have shown that

$$Q(\sqrt{p_1^*}, \dots, \sqrt{p_r^*}) \subset K^+(f).$$

Now suppose $Q(\sqrt{a}) \subset F_f^+(K)$ and $Q(\sqrt{a}) \not\subset Q(\sqrt{p_1^*}, \dots, \sqrt{p_r^*})$. By Lemma 4.3.7, we have $a \mid nf$. If a contains an odd prime divisor p , then $a' = a/p^*$ is such that $Q(\sqrt{a'}) \subset F_f^+(K)$, as $Q(\sqrt{p^*}) \subset F_f^+(K)$. Thus we may assume that $a = -1, 2$, or -2 . Then appealing to Lemma 4.3.7, we obtain the required results. ■

Theorem 4.3.13 *Let $n > 1$ be a squarefree integer. Let $K = Q(\sqrt{n})$. Let f be a positive integer. Suppose that $p_1, p_2, \dots, p_r$ are the distinct odd primes of the form $4k+1$ dividing nf , and suppose that $q_1, q_2, \dots, q_s$ are the distinct odd primes of the form $4k+3$ dividing nf . Then the genus field $K(f)$ of $F_f(K)$ is given by*

when $n \equiv 1 \pmod{4}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \parallel f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^3 \mid f, \end{cases}$$

when $n \equiv 3 \pmod{4}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2^2 \mid f, \end{cases}$$

when $n \equiv 2 \pmod{8}$,

$$K(f) = \begin{cases} Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2 \mid f, \end{cases}$$

and when $n \equiv 6 \pmod{8}$,

$$K(f) = \begin{cases} Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}), & \text{if } 2 \nmid f, \\ Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}), & \text{if } 2 \mid f. \end{cases}$$

Proof: Since the proofs are similar, we only treat the case when $n \equiv 1 \pmod{4}$. First we suppose that $4 \nmid f$. By Lemma 4.3.10, in this case, a real quadratic field $Q(\sqrt{m}) \subset F_f(K)$ if and only if $m \mid nf$ and $m \equiv 1 \pmod{4}$. Thus

$$Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}) \subset K(f).$$

Now suppose $Q(\sqrt{a}) \subset F_f(K)$. Then $a \mid nf$ and $a \equiv 1 \pmod{4}$. Thus a contains an even number of divisors q_i . Note that as

$$\sqrt{q_i q_j} \in Q(\sqrt{q_1 q_i}, \sqrt{q_1 q_j}) \subset Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}),$$

we can conclude that

$$Q(\sqrt{a}) \subset Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}).$$

Since a is arbitrary, we have

$$K(f) = Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1 q_2}, \dots, \sqrt{q_1 q_s}).$$

Next we suppose that $2^2 \parallel f$. By Lemma 4.3.10, we have

$$Q(\sqrt{p_i}), Q(\sqrt{q_j}) \subset F_f(K),$$

so that

$$Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}) \subset K(f). \quad (4.19)$$

Now suppose $Q(\sqrt{a}) \subset F_f(K)$. Since $a \mid nf$, in view of (4.19), we may suppose that a contains neither p_i nor q_j , thus $a = 2$. But Lemma 4.3.9 shows that $Q(\sqrt{2}) \not\subset F_f(K)$. This a contradiction. Thus we must have

$$K(f) = Q(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}).$$

Now suppose that $2^3 \mid f$. Using a similar argument to the one above, we have

$$K(f) = Q(\sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{q_1}, \dots, \sqrt{q_s}). \quad \blacksquare$$

4.4 Proof of Theorem 4.4.11

Throughout this section we always assume that M is a dihedral extension of Q with $\text{Gal}(M/Q) = D_4 = \langle \sigma, \tau \rangle$, where $\sigma^4 = \tau^2 = (\sigma\tau)^2 = 1$. We suppose that

K is the fixed field of σ , k is the fixed field of $\langle \sigma^2, \tau \rangle$,
 k' is the fixed field of $\langle \sigma^2, \sigma\tau \rangle$, F is the fixed field of σ^2 ,
 L is the fixed field of τ , L' is the fixed field of $\sigma^2\tau$.

Lemma 4.4.1 $d_L = d_k g^2$, where g is a positive integer.

Proof: In order to prove the lemma it suffices by Lemma 1.2.17 to show that

$$k' = Q(\sqrt{d_L}).$$

Suppose $L = Q(\alpha)$ and Let $\varphi(x)$ be the minimal polynomial of α over Q . Then M is the splitting field of $\varphi(x)$. By Lemma 2.5.3, we have $k' = Q(\sqrt{\text{disc}(\varphi)})$ and thus $k' = Q(\sqrt{d_L})$. ■

Lemma 4.4.2 $d_K d_k = c^2 d_{k'}$, where c is a positive integer.

Proof: By Theorem 4.3.5, $c = f_0(F/k') = \sqrt{d_k d_K / d_{k'}}$ is a positive integer. ■

Lemma 4.4.3 $d_L = d_K d_k g_1^2$, where g_1 is a positive integer.

Proof: It is clear that the lemma is equivalent to saying that for any prime p

$v_p(d_L) - v_p(d_K) - v_p(d_k)$ is a non-negative even integer,

or equivalently,

$$\begin{cases} \text{(i)} & v_p(d_L) - v_p(d_K) - v_p(d_k) \equiv 0 \pmod{2} \\ \text{(ii)} & v_p(d_L) - v_p(d_K) - v_p(d_k) \geq 0 \end{cases} \quad (4.20)$$

First we prove (4.20-i). By Lemmas 4.4.1 and 4.4.2, we have

$$c^2 d_L = c^2 d_{k'} g^2 = d_K d_k g^2,$$

so that

$$v_p(d_L) - v_p(d_K) - v_p(d_k) \equiv 0 \pmod{2}.$$

Next we prove (4.20-ii). We consider the following two cases.

(i). Suppose $v_p(d_k) \geq v_p(d_K)$. Then

$$\begin{aligned} v_p(d_L) - v_p(d_K) - v_p(d_k) &\geq v_p(d_L) - 2v_p(d_k) \\ &= v_p(d_L/d_k^2) = v_p(N_{k/Q}(d(L/k))) \geq 0. \end{aligned}$$

(ii). Suppose $v_p(d_K) > v_p(d_k)$. We show that either

$$v_p(d_K) = v_p(d_{k'}), \quad v_p(d_k) = 0 \text{ (allowing } p = 2), \quad (4.21)$$

or

$$v_2(d_K) = v_2(d_{k'}) = 3, \quad v_2(d_k) = 2. \quad (4.22)$$

In fact, if $p \neq 2$, then p is tamely ramified in K . In this case we have $v_p(d_K) = v_p(d_{k'}) = v_p(d_k) + 1 = 1$, proving that (4.21) holds.

If $p = 2$, we have either

$$v_2(d_K) = v_2(d_{k'}) = 2, \quad 3 \text{ and } v_2(d_k) = 0$$

or

$$v_2(d_K) = v_2(d_{k'}) = 3, \quad v_2(d_k) = 2.$$

Thus either (4.21) or (4.22) holds. If (4.21) holds, then

$$v_p(d_L) - v_p(d_K) - v_p(d_k) = v_p(d_L) - v_p(d_{k'}) = v_p(g^2) \geq 0.$$

If (4.22) holds, from the formulae

$$d_k^2 N_{k/Q}(d(L/k)) = d_L = d_{k'} g^2,$$

we have $v_2(g) \geq 1$. Thus

$$\begin{aligned} v_2(d_L) - v_2(d_K) - v_2(d_k) &= v_2(d_{k'}) + 2v_2(g) - v_2(d_K) - v_2(d_k) \\ &= 3 + 2v_2(g) - 3 - 2 = 2(v_2(g) - 1) \geq 0. \end{aligned}$$

Lemma 4.4.4 $\sigma(L) = L'$.

Proof: We have

$$(\sigma^2 \tau)(\sigma(L)) = \sigma^2(\tau \sigma(L)) = \sigma^2(\sigma^{-1} \tau(L)) = \sigma(L)$$

and as L' is the fixed field of $\sigma^2 \tau$, the conclusion follows from Galois theory. ■

Lemma 4.4.5

$$\text{Gal}(L/k) = \{1_L, \sigma^2|_L\} \text{ and } \text{Gal}(L'/k) = \{1_{L'}, \sigma^2|_{L'}\}.$$

Proof: Note that $\sigma^2 \in \text{Gal}(M/k)$, and both $\sigma^2|_L$ and $\sigma^2|_{L'}$ are nontrivial. ■

Lemma 4.4.6 Let $\mathcal{P}$ be a prime of k which is ramified in L , say $\mathcal{P}\mathcal{O}_L = \mathcal{B}^2$. Then

$$\sigma(V_m(\mathcal{B}/\mathcal{P})) = V_m(\sigma\mathcal{B}/\mathcal{P}), \text{ for } m \geq 0.$$

Proof: By Lemma 4.4.4, $\sigma\mathcal{B}$ is a prime of L' and $\mathcal{P}\mathcal{O}_{L'} = (\sigma\mathcal{B})^2 = \mathcal{B}'^2$. Now suppose $\pi \in V_m(\mathcal{B}/\mathcal{P})$, then

$$\pi(\alpha) \equiv \alpha \pmod{\mathcal{B}^{m+1}} \text{ for } \alpha \in \mathcal{O}_L. \quad (4.23)$$

From this we obtain the congruence

$$\sigma\pi(\alpha) \equiv \sigma(\alpha) \pmod{\sigma\mathcal{B}^{m+1}}.$$

Since $\pi = 1_L$ or $\sigma^2|_L$, we have $\sigma\pi = \pi\sigma$. Thus

$$\pi(\sigma(\alpha)) \equiv \sigma(\alpha) \pmod{\sigma\mathcal{B}^{m+1}},$$

that is

$$\pi(\alpha') \equiv \alpha' \pmod{\mathcal{B}'^{m+1}} \text{ for } \alpha' \in \mathcal{O}_{L'}, \quad (4.24)$$

so that $\pi \in V_m(\mathcal{B}'/\mathcal{P})$. Conversely, by the same argument, (4.24) $\implies$ (4.23). ■

Lemma 4.4.7

$$d(L/k) = d(L'/k).$$

Proof: This is an immediate corollary of Lemmas 1.2.19 and Lemma 4.4.6. ■

Lemma 4.4.8

$$N_{L/k}(d(M/L)) = d(F/k) \text{ and } N_{L/Q}(d(M/L)) = d(F/k)^2.$$

Proof: Since $\text{Gal}(M/k)$ is a Klein 4-group and L, L', F are the three quadratic subfields of M , by Lemma 1.2.13, we have

$$d(M/k) = d(L/k)d(L'/k)d(F/k).$$

Appealing to Lemma 4.4.7, we obtain

$$d(M/k) = d(L/k)^2 d(F/k).$$

On the other hand, by Lemma 1.2.8 we know that

$$d(M/k) = d(L/k)^2 N_{L/k}(d(M/L)).$$

Thus we have

$$d(M/k) = d(L/k)^2 N_{L/k}(d(M/L)) = d(L/k)^2 d(F/k),$$

so

$$N_{L/k}(d(M/L)) = d(F/k).$$

Further, since $d(F/k)$ is an integer (by Theorem 4.3.5), we have

$$N_{L/Q}(d(M/L)) = N_{k/Q}(N_{L/k}(d(M/L))) = N_{k/Q}(d(F/k)) = d(F/k)^2. \quad \blacksquare$$

Lemma 4.4.9

$$N_{K/Q}(f_0(M/K)) = g_1^2,$$

where g_1 is the positive integer given in Lemma 4.4.3.

Proof: Since $d(M/K) = f_0^2(M/K)f_0(F/K)$ we have

$$\begin{aligned} d_M &= N_{K/Q}(d(M/K))d_K^4 \quad (\text{Lemma 1.2.8}) \\ &= (N_{K/Q}(f_0(M/K)))^2 N_{K/Q}(f_0(F/K))d_K^4 \\ &= (N_{K/Q}(f_0(M/K)))^2 (f_0(F/K))^2 d_K^4, \end{aligned}$$

and

$$\begin{aligned} d_M &= N_{L/Q}(d(M/L))d_L^2 \quad (\text{Lemma 1.2.8}) \\ &= d(F/k)^2 d_L^2 \quad (\text{Lemma 4.4.8}) \\ &= d(F/k)^2 (d_K d_k g_1^2)^2 \quad (\text{Lemma 4.4.3}), \end{aligned}$$

we have

$$(N_{K/Q}(f_0(M/K)))^2 (f_0(F/K))^2 d_K^4 = d_K^2 d_k^2 d(F/k)^2 g_1^4.$$

Noting that, by Lemma 1.2.8 and Theorem 4.3.5 we have

$$d_F = d_k^2 d(F/k)^2 = d_K^2 d(F/K)^2 = d(F/Q),$$

we deduce

$$N_{K/Q}(f_0(M/K)) = g_1^2.$$

This completes the proof of the lemma. $\blacksquare$

Lemma 4.4.10 $f_0(M/K)$ is a positive integer.

Proof: Let $\mathcal{P}$ be a prime of K dividing $f_0(M/K)$ and containing the prime p . By Lemmas 4.3.1 and 4.3.2, we need only show that

$$p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}' \implies p\text{-part of } f_0(M/K) \text{ is a positive integer.} \quad (4.25)$$

It is obvious that (4.25) is equivalent to the following

$$p\mathcal{O}_K = \mathcal{P}\mathcal{P}', \mathcal{P} \neq \mathcal{P}' \implies v_{\mathcal{P}}(f_0(M/K)) = v_{\mathcal{P}'}(f_0(M/K)). \quad (4.26)$$

By Lemma 1.2.11 we have

$$d(M/K) = f_0(M/K)^2 f_0(F/K), \quad (4.27)$$

First we suppose that p is odd. Let $\mathcal{B}$ be a prime of M containing $\mathcal{P}$. We consider the two cases (i) $e(\mathcal{B}/\mathcal{P}) = 4$ and (ii) $e(\mathcal{B}/\mathcal{P}) = 2$ separately.

Case (i): Since $\mathcal{P}$ is tamely ramified in M , we have by Lemma 1.2.20, $\mathcal{B}^3 \parallel \text{diff}_{M/K}(\mathcal{O}_M)$. Then we have by Lemma 1.2.18, $\mathcal{P}^3 \parallel d(M/K)$. Applying this to (4.27) we have

$$3 = v_{\mathcal{P}}(d(M/K)) = 2v_{\mathcal{P}}(f_0(M/K)) + v_{\mathcal{P}}(f_0(F/K)). \quad (4.28)$$

By Lemma 4.3.4, we have $v_{\mathcal{P}}(f_0(F/K)) = 1$ so that (4.28) gives

$$v_{\mathcal{P}}(f_0(M/K)) = 1. \quad (4.29)$$

Next, since $Q \subset M$ is a normal extension, $\mathcal{P} \mid f_0(M/K)$ implies that $\mathcal{P}' \mid f_0(M/K)$. Replacing $\mathcal{P}$ by $\mathcal{P}'$ in the formula (4.29), we obtain

$$v_{\mathcal{P}'}(f_0(M/K)) = 1.$$

This proves that (4.26) holds and $v_{\mathcal{P}}(f_0(M/K)) = 1$.

Case (ii): In this case, we have by Lemma 1.2.15, $D(\mathcal{B}/\mathcal{P}) = \langle \sigma^2 \rangle$ which implies that

$$\mathcal{P}\mathcal{O}_M = \mathcal{B}^2\mathcal{B}'^2, \quad \mathcal{B} \neq \mathcal{B}', \quad (4.30)$$

and

$$v_{\mathcal{P}}(f_0(F/K)) = 0. \quad (4.31)$$

In addition, we have by Lemma 1.2.20

$$v_{\mathcal{B}}(\text{diff}_{M/K}(\mathcal{O}_M)) = v_{\mathcal{B}'}(\text{diff}_{M/K}(\mathcal{O}_M)) = 1. \quad (4.32)$$

From (4.32) and Lemma 1.2.18, we have

$$v_{\mathcal{P}}(d(M/K)) = 2. \quad (4.33)$$

Now appealing to (4.27) and (4.33), we have

$$v_{\mathcal{P}}(f_0(M/K)) = 1. \quad (4.34)$$

Replacing $\mathcal{P}$ by $\mathcal{P}'$ in (4.34), we have

$$v_{\mathcal{P}'}(f_0(M/K)) = 1,$$

so that

$$v_{\mathcal{P}}(f_0(M/K)) = v_{\mathcal{P}'}(f_0(M/K)) = 1.$$

This proves that (4.26) holds and $v_{\mathcal{P}}(f_0(M/K)) = 1$.

Now we suppose that $p = 2$. Let $t = v_{\mathcal{P}}(f_0(M/K))$ and $t' = v_{\mathcal{P}'}(f_0(M/K))$. Then $2^{t+t'} \parallel N_{K/Q}(f_0(M/K))$. Further, by Lemma 4.4.9, we have $N_{K/Q}(f_0(M/K)) = g_1^2$, so that $t + t'$ is even. Without loss of generality we may suppose that

$$t - t' = 2s, \text{ where } s \text{ is a non-negative integer.} \quad (4.35)$$

From the formulae

$$d(M/K) = d(F/K)^2 N_{F/K}(d(M/F)) = f_0(M/K)^2 f_0(F/K), \quad d(F/K) = f_0(F/K),$$

we have

$$v_{\mathcal{P}}(f_0(F/K)) + v_{\mathcal{P}}(N_{F/K}(d(M/F))) = 2v_{\mathcal{P}}(f_0(M/K)). \quad (4.36)$$

We consider two cases (i) $e(\mathcal{B}/\mathcal{P}) = 4$ and (ii) $e(\mathcal{B}/\mathcal{P}) = 2$ separately.

Case (i): In this case, as $\mathcal{B}$ is the unique prime of M containing $\mathcal{P}$, (4.36) gives

$$v_{\mathcal{P}}(f_0(F/K)) + v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) = 2v_{\mathcal{P}}(f_0(M/K)). \quad (4.37)$$

Replacing $\mathcal{P}$ by $\mathcal{P}'$ in (4.37), we have

$$v_{\mathcal{P}'}(f_0(F/K)) + v_{\mathcal{B}'}(\text{diff}_{M/F}(\mathcal{O}_M)) = 2v_{\mathcal{P}'}(f_0(M/K)). \quad (4.38)$$

Note as $v_{\mathcal{P}}(f_0(F/K)) = v_{\mathcal{P}'}(f_0(F/K)) = 1$ (Lemma 4.3.4), we have by (4.37) and (4.38)

$$v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) - v_{\mathcal{B}'}(\text{diff}_{M/F}(\mathcal{O}_M)) = 2v_{\mathcal{P}}(f_0(M/K)) - 2v_{\mathcal{P}'}(f_0(M/K)). \quad (4.39)$$

On the other hand, by Lemma 1.2.20 we have

$$2 \leq v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) \leq 5, \quad 2 \leq v_{\mathcal{B}'}(\text{diff}_{M/F}(\mathcal{O}_M)) \leq 5. \quad (4.40)$$

Now appealing to (4.35) and (4.40) we obtain

$$4s = 2v_{\mathcal{P}}(f_0(M/K)) - 2v_{\mathcal{P}'}(f_0(M/K)) = v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) - v_{\mathcal{B}'}(\text{diff}_{M/F}(\mathcal{O}_M)) \leq 5 - 2 = 3,$$

which gives $s = 0$ and

$$v_{\mathcal{P}}(f_0(M/K)) = v_{\mathcal{P}'}(f_0(M/K)).$$

This proves that (4.26) holds and using (4.37) we have

$$v_2(f_0(M/K)) = v_{\mathcal{P}}(f_0(M/K)) = \begin{cases} 2, & \text{if } v_2(f_0(F/K)) = v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) = 2, \\ 3, & \text{if } v_2(f_0(F/K)) = 3 \text{ and } v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) = 4, \\ 3, & \text{if } v_2(f_0(F/K)) = v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) = 3, \\ 4, & \text{if } v_2(f_0(F/K)) = 3 \text{ and } v_{\mathcal{B}}(\text{diff}_{M/F}(\mathcal{O}_M)) = 2. \end{cases}$$

Case (ii): In this case, we have by Lemma 1.2.15, $D(\mathcal{B}/\mathcal{P}) = \langle \sigma^2 \rangle$ which implies that

$$\mathcal{P}\mathcal{O}_M = \mathcal{B}^2\mathcal{B}', \quad \mathcal{B} \neq \mathcal{B}', \quad (4.41)$$

and

$$v_{\mathcal{P}}(f_0(F/K)) = 0. \quad (4.42)$$

In addition, we have by Lemma 1.2.20

$$2 \leq v_{\mathcal{B}}(\text{diff}_{M/K}(\mathcal{O}_M)) \leq 3, \quad 2 \leq v_{\mathcal{B}'}(\text{diff}_{M/K}(\mathcal{O}_M)) \leq 3. \quad (4.43)$$

By Lemma 1.2.18, we have

$$v_{\mathcal{P}}(d(M/K)) = v_{\mathcal{B}}(\text{diff}_{M/K}(\mathcal{O}_M)) + v_{\mathcal{B}'}(\text{diff}_{M/K}(\mathcal{O}_M)). \quad (4.44)$$

On the other hand, by (4.27), we have

$$v_{\mathcal{P}}(d(M/K)) = 2v_{\mathcal{P}}(f_0(M/K)). \quad (4.45)$$

Putting (4.43), (4.44) and (4.45) together we obtain

$$t = v_{\mathcal{P}}(f_0(M/K)) = 2 \text{ or } 3. \quad (4.46)$$

Replacing $\mathcal{P}$ by $\mathcal{P}'$ in (4.46), we have

$$t' = v_{\mathcal{P}'}(f_0(M/K)) = 2 \text{ or } 3. \quad (4.47)$$

Finally, as $t - t'$ is even by (4.35), we see that from (4.46) and (4.47) that

$$t = t' = v_{\mathcal{P}}(f_0(M/K)) = v_{\mathcal{P}'}(f_0(M/K)) = 2 \text{ or } 3.$$

This proves that (4.26) holds and $v_{\mathcal{P}}(f_0(M/K)) = 2$ or 3 . This completes the proof of the lemma. ■

Theorem 4.4.11 *Let M be a dihedral extension of Q with $\text{Gal}(M/Q) = D_4 = \langle \sigma, \tau \rangle$ where $\sigma^4 = \tau^2 = (\sigma\tau)^2 = 1$. Let K be the fixed field of σ . Let F be the fixed field of σ^2 . Let L be a subfield of M of degree 4 over Q different from F . Let k be the unique quadratic subfield of L . Then $f_0(M/K)$ is a positive integer which satisfies*

$$d_L = d_K d_k f_0(M/K)^2.$$

Proof: We have by Lemma 4.4.9 and 4.4.10

$$f_0(M/K)^2 = g_1^2,$$

so that $f_0(M/K) = g_1$. Then Theorem 4.4.11 follows by appealing to Lemma 4.4.3.

Chapter 5

SOME APPLICATIONS AND EXAMPLES

In this chapter we begin by giving some corollaries of Theorem 3.1.3(i) in §5.1. In §5.2 we consider the problem of evaluating the Legendre symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$. This evaluation will be used in §5.4 to characterize the representation of primes by certain principal forms. In §5.3 we give some numerical examples to illustrate Theorem 3.1.3.

5.1 Some Corollaries of Theorem 3.1.3

In this section we always assume that $\rho(x) \in Z[x]$ is a dihedral polynomial of degree d , M is the splitting field of $\rho(x)$, and $K \in K_M$.

Corollary 5.1.1 *Let f be a positive integer such that $f_0(M/K) \mid f$. Then there is a unique subgroup $J = J(\rho, K, f)$ of $H(d_K f^2)$ such that*

$$H(d_K f^2)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has d solutions

$\iff$ *p splits completely in M*

$\iff$ *p is represented by one of the classes in J .*

Proof: Since $f_0(M/K) \mid f$, we have $M \subset F_f^+(K)$ by Lemma 3.1.6 and the corollary follows from Theorem 3.1.3(i). ■

The next lemma will be used in the proof of our next corollary to Theorem 3.1.3(i), namely Corollary 5.1.3.

Lemma 5.1.2 *Let $q \equiv 3 \pmod{4}$ be a prime. Let $\rho(x)$ be a dihedral polynomial of degree q . Let α be a root of $\rho(x)$ and set $L = Q(\alpha)$. Let M be the normal closure of L . Let K be the unique quadratic subfield of M . Then*

$$d_L = d_K f_0(M/K)^2 \cdot g_1^2,$$

where g_1 is a positive integer.

Proof: For case $q = 3$ the lemma follows from Theorem 4.2.7. Thus we assume $q \geq 7$. By Lemma 1.2.17, as $d_L \equiv 0, 1 \pmod{4}$, we have

$$d_L = d_K g^2, \text{ where } g \text{ is a positive integer.}$$

To prove the lemma it suffices to show that $f_0(M/K) \mid g$ (note that $f_0(M/K)$ is an integer by Theorem 4.1.3), or equivalently, to show that for any prime p ,

$$v_p(f_0(M/K)) \leq v_p(g) = \frac{1}{2}(v_p(d_L) - v_p(d_K)).$$

Without loss of generality we may assume $v_p(f_0(M/K)) > 0$ so that there are two possibilities: (i) p is totally ramified in M and (ii) p is unramified in K .

Case (i). In this case we must have $p = q$ and $v_q(d_K) = 1$. By Theorem 4.1.3 we have $v_q(f_0(M/K)) = 1$, and by Theorem 4.2.6 we have $v_q(d_L) = 3(q-1)/2$ so that

$$\frac{1}{2}(v_p(d_L) - v_p(d_K)) = \frac{1}{2}(3(q-1)/2 - 1) \geq 1 = v_p(f_0(M/K)).$$

Case (ii). In this case we have $v_p(d_K) = 0$ and $p \neq 2$ as p satisfies $p \equiv \left(\frac{d_K}{p}\right) \pmod{q}$ by Theorem 4.1.3. By Theorem 4.1.3 we have $v_p(f_0(M/K)) = 2$, and by Theorem 4.2.6(ii) and (iv) we have

$$v_p(d_L) = 2(q-1), \quad q-1,$$

so that

$$\frac{1}{2}(v_p(d_L) - v_p(d_K)) \geq \frac{1}{2}(q-1) \geq \frac{1}{2}(7-1) > 2 = v_p(f_0(M/K)).$$

This completes the proof of the lemma. ■

Corollary 5.1.3 *Let $q \equiv 3 \pmod{4}$ be a prime. Let $\rho(x) \in \mathbb{Z}[x]$ be a dihedral polynomial of degree q . Let α be a root of $\rho(x)$ and set $L = \mathbb{Q}(\alpha)$. Let M be the normal closure of L . Let K be the unique quadratic subfield of M . Then there is a unique subgroup $J = J(\rho)$ of $H(d_L)$ such that*

$$H(d_L)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has q solutions

$$\iff p \text{ splits completely in } M$$

$$\iff p \text{ is represented by one of the classes in } J.$$

Proof: We choose $f = f_0(M/K)g_1$, where g_1 is given in Lemma 5.1.2, and the corollary follows from Corollary 5.1.1. ■

Corollary 5.1.4 *Let $q \equiv 3 \pmod{4}$ be a prime. Let $\rho(x) \in \mathbb{Z}[x]$ be a dihedral polynomial of degree q . Let $D = \text{disc}(\rho(x))$. Then there is a unique subgroup $J = J(\rho)$ of $H(D)$ such that*

$$H(D)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has q solutions

$$\iff p \text{ splits completely in } M$$

$$\iff p \text{ is represented by one of the classes in } J.$$

Proof: Let L be the field in Corollary 5.1.3. Then

$$D = \text{disc}(1, \alpha, \dots, \alpha^{p-1}) = a^2 d_L, \text{ for some } a \in \mathbb{Z}^+.$$

We choose $f = f_0(M/K)g_1 a$, so that f is a positive integer satisfying Corollary 5.1.1. ■

Corollary 5.1.5 (Spearman and Williams [30]) Let $\rho(x) = x^3 + Ax^2 + Bx + C \in \mathbb{Z}[x]$ be irreducible over $\mathbb{Q}$ with $D = \text{disc}(\rho(x)) \neq \square$. Then there is a unique subgroup $J = J(A, B, C)$ of index 3 in $H(D)$ with the property:

If p is any prime (> 3) such that $\left(\frac{D}{p}\right) = +1$ then $\rho(x) \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by one of the forms in $J(A, B, C)$.

Proof: As $\text{disc}(\rho) \neq \square$, by Lemma 2.4.3, $\rho(x)$ is a dihedral polynomial. In addition, $\left(\frac{D}{p}\right) = +1$ implies that $p \nmid D$. Thus all the conditions of Corollary 5.1.4 are satisfied. ■

Corollary 5.1.6 Let $\rho(x) \in \mathbb{Z}[x]$ be a dihedral polynomial with $\text{Gal}(M/\mathbb{Q}) = D_4$. Let K be the unique quadratic field in K_M . Let $E = d_K f_0(M/K)^2$. Then there is a unique subgroup $J = J(\rho)$ of $H(E)$ such that

$$H(E)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

$\rho(x) \pmod{p}$ splits completely

$\iff p$ splits completely in M

$\iff p$ is represented by one of the classes in J .

Proof: By Theorem 4.4.11, $f_0(M/K)$ is a positive integer. The corollary then follows from Corollary 5.1.1. ■

Corollary 5.1.7 Let $\rho(x)$ be a dihedral polynomial of type 1 of degree 4. Let K be the unique quadratic field in K_M and let k be as in Theorem 4.4.11. Let $E = \text{disc}(\rho(x))/d_k$. Then there is a unique subgroup $J = J(\rho)$ of $H(E)$ such that

$$H(E)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

$\rho(x) \pmod{p}$ splits completely

$\iff p$ splits completely in M

$\iff p$ is represented by one of the classes in J .

Proof: Let L be as in Theorem 4.4.11. Then $\text{disc}(\rho(x)) = d_L a^2$ for some positive integer a . Choose $f = a f_0(M/K)$, then appealing to Theorem 4.4.11, we have

$$d_K f^2 = d_K f_0(M/K)^2 a^2 = d_L a^2 / d_k = E. \quad \blacksquare$$

Corollary 5.1.8 *Let $\rho(x) \in Z[x]$ be a dihedral polynomial of type 2 with $\text{Gal}(M/Q) = D_2$. Let k, k' be any two of the three quadratic subfields of M . Set $E = d_k d_{k'}$. Then there is a unique subgroup $J = J(\rho)$ of $H(E)$ such that*

$$H(E)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: if p is an odd prime not dividing $\text{disc}(\rho)$ then

the congruence $\rho(x) \equiv 0 \pmod{p}$ has 4 solutions

$$\iff p \text{ splits completely in } M$$

$$\iff p \text{ is represented by one of the classes in } J.$$

Proof: Let $K = kk'$ be the fixed field of $\sigma \in \text{Gal}(M/Q)$ (say). By Theorem 4.3.5, $f_0(M/K)$ is a positive integer and

$$d_K f_0(M/K)^2 = d_k d_{k'}. \quad \blacksquare$$

Corollary 5.1.9 *Let $\rho(x)$ be a dihedral polynomial of type 2 with $\text{Gal}(M/Q) = D_2$. Let K, k and k' be the three quadratic subfields of M . Let $J(K, k)$, $J(k, k')$ and $J(k', K)$ be as in Corollary 5.1.8. Then with at most finitely many exceptions a prime p is represented by one of the forms in $J(K, k) \iff q$ is represented by one of the forms in $J(k, k') \iff p$ is represented by one of the forms in $J(k', K)$.*

Proof: Suppose that M is the splitting field of $\rho(x)$. Note that there are only finitely many primes dividing $\text{disc}(\rho(x))$. The result then follows by appealing to Corollary 5.1.8. $\blacksquare$

Example 5.1.1 Let $F = Q(\sqrt{-4}, \sqrt{-8})$. Here $K = Q(\sqrt{-4})$, $k = Q(\sqrt{-8})$, $k' = Q(\sqrt{8})$ and

$$H(d_K d_k) = H(32) = \{(1, 0, -8), (-1, 4, 4)\},$$

$$H(d_K d_{k'}) = H(-32) = \{(1, 0, 8), (3, 2, 3)\},$$

$$H(d_k d_{k'}) = H(-64) = \{(1, 0, 16), (4, 4, 5)\}.$$

By the corollary we have for an odd prime p that

$$p = x_1^2 - 8y_1^2 \iff p = x_2^2 + 8y_2^2 \iff p = x_3^2 + 16y_3^2.$$

5.2 Evaluation of the Legendre Symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$

Let $d(\neq 1)$ be a squarefree integer. Let $A, B \in Z$ and let p be an odd prime. Suppose that

$$\left(\frac{d}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = 1.$$

As $\left(\frac{d}{p}\right) = 1$ there exists an integer s such that $s^2 \equiv d \pmod{p}$. We have

$$\left(\frac{A + Bs}{p}\right) \left(\frac{A - Bs}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = 1,$$

so that $\left(\frac{A+Bs}{p}\right) = \left(\frac{A-Bs}{p}\right)$. Hence the Legendre symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$ is well-defined. In this section we consider the problem of determining the value of the Legendre symbol $\left(\frac{A+B\sqrt{d}}{p}\right)$, see Theorems 5.2.1 and 5.2.2. The Lemmas at the end of the section will be used in §5.4. We note that $\sqrt{A + B\sqrt{d}}$ is a root of the irreducible polynomial $\rho(x) = x^4 - 2Ax^2 + A^2 - B^2d$. Let M be the splitting field of $\rho(x)$ over Q . Then by Lemma 2.5.2 we have

$$\text{Gal}(M/Q) = \begin{cases} D_4, & \text{if } A^2 - B^2d \neq \square \text{ and } (A^2 - B^2d)d \neq \square, \\ Z_4, & \text{if } (A^2 - B^2d)d = \square, \\ D_2, & \text{if } A^2 - B^2d = \square. \end{cases} \quad (5.1)$$

In order to apply our results on dihedral polynomials we suppose that $(A^2 - B^2d)d \neq \square$ so that

$$\text{Gal}(M/Q) = \begin{cases} D_4, & \text{if } A^2 - B^2d \neq \square, \\ D_2, & \text{if } A^2 - B^2d = \square. \end{cases}$$

The case when $A^2 - B^2d = C^2d$ has been treated by K.S.Williams, K. Hardy and C. Friesen [34] and R.J. Evans [14].

Theorem 5.2.1 *Let $\rho(x) = x^4 - 2Ax^2 + A^2 - B^2d$, where $A^2 - B^2d \neq \square$ and $(A^2 - B^2d)d \neq \square$. Let M be the splitting field of $\rho(x)$, and let K be the unique quadratic field in K_M . Let p be an odd prime not dividing B with $\left(\frac{d}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = 1$. Let f be any positive integer divisible by $f_0(M/K)$. Then there is a unique subgroup $J = J(\rho, f)$ of $H(d_K f^2)$ such that*

$$H(d_K f^2)/J \simeq \text{Gal}(M/K),$$

where the isomorphism is induced by the Artin map. Further, J has the property: $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$ if and only if p is represented by one of the forms in J .

Proof: Let $L = Q(\sqrt{A + B\sqrt{d}})$, $k = Q(\sqrt{d})$ and $k' = Q(\sqrt{A^2 - B^2d})$. By Lemma 2.5.4, we have $K = Q(\sqrt{(A^2 - B^2d)d})$. By Corollary 5.1.1, we only need show that

$$\left(\frac{d}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = \left(\frac{A+B\sqrt{d}}{p}\right) = 1 \iff p \text{ splits completely in } M.$$

First we suppose that p splits completely in M . Then p splits completely in every subfield of M so that

$$\left(\frac{d}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = \left(\frac{A + B\sqrt{d}}{p}\right) = 1. \quad (5.2)$$

Conversely, suppose that (5.2) holds. $p \nmid dB(A^2 - B^2d)$, we have $p \nmid \text{disc}(\rho(x))$. $\left(\frac{d}{p}\right) = 1$ implies that p splits in k , and $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$ implies that p splits completely in L/k (by Lemma 1.2.1) so that p splits completely in L . In addition, $\left(\frac{d}{p}\right) = \left(\frac{A^2 - B^2d}{p}\right) = 1$ implies that p splits completely in K so that p splits completely in M as M is the composite field of L and K .

By the assumptions of the lemma $\rho(x) = x^4 - 2Ax^2 + (A^2 - B^2d)$ is a dihedral polynomial of type 1. Since $p \nmid dB(A^2 - B^2d)$, we have $p \nmid \text{disc}(\rho(x))$. Hence we only have to show that $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$ if and only if p splits completely in M .

Suppose $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$. Then p splits completely in $L = Q(\sqrt{A + B\sqrt{d}})$. On the other hand, since $\left(\frac{A^2 - B^2d}{p}\right) = 1$, p splits completely in $k = Q(\sqrt{A^2 - B^2d})$. Note that M is the composite field of L and k . Hence, by Lemma 1.2.2, p splits completely in

M .

Conversely, suppose that p splits completely in M , then p splits completely in L . Thus $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$. ■

Theorem 5.2.2 Let $\rho(x) = x^4 - 2Ax^2 + A^2 - B^2d$, where $A^2 - B^2d = C^2$ for some integer C . Let M be the splitting field of $\rho(x)$. Let p be an odd prime not dividing $d(A^2 - B^2d)$ with $\left(\frac{d}{p}\right) = 1$. Then the following are equivalent. (i). $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$, (ii). p splits completely in M , (iii). $\left(\frac{2(A \pm C)}{p}\right) = 1$.

Proof: By (5.1), we have that $\text{Gal}(M/Q) = D_2$. By Lemma 2.5.6, the three quadratic fields of M are $k_1 = Q(\sqrt{d})$, $k_2 = Q(\sqrt{2(A+C)})$ and $k_3 = Q(\sqrt{2(A-C)})$.
(i) $\implies$ (ii).

Suppose $\left(\frac{A+B\sqrt{d}}{p}\right) = 1$. Then p splits completely in M/k_1 . Since $\left(\frac{d}{p}\right) = 1$, p splits completely in k_1 . Thus p splits completely in M .

(ii) $\implies$ (iii).

Suppose p splits completely in M . Then p splits completely in both k_2 and k_3 , thus $\left(\frac{2(A \pm C)}{p}\right) = 1$.

(iii) $\implies$ (i).

Note that $A + B\sqrt{d} = (\sqrt{2(A+C)} + \sqrt{2(A-C)})^2/4$, then the conclusion follows. ■

Lemma 5.2.3 Let $\varphi(x) = x^2 - bx + c \in Z[x]$ and let α and β be the two roots of $\varphi(x)$. Let $v_n (n = 0, 1, 2, \dots)$ be given by the recurrence relation

$$v_{n+2} = bv_{n+1} - cv_n, \quad v_0 = 2, \quad v_1 = b,$$

so that $v_n = \alpha^n + \beta^n$. Let p be an odd prime such that

$$\left(\frac{c}{p}\right) = \left(\frac{b^2 - 4c}{p}\right) = 1.$$

Then we have

$$v_{(p-1)/2} \equiv 2 \left(\frac{\alpha}{p}\right) \pmod{p},$$

so that

$$\left(\frac{\alpha}{p}\right) = 1 \iff v_{\frac{p-1}{2}} \equiv 2 \pmod{p}.$$

Proof: As $c = \alpha\beta$ and $\left(\frac{c}{p}\right) = 1$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{\beta}{p}\right).$$

Note that as

$$\alpha^{(p-1)/2} \equiv \left(\frac{\alpha}{p}\right) \pmod{p}, \quad \beta^{(p-1)/2} \equiv \left(\frac{\beta}{p}\right) \pmod{p},$$

we have

$$\alpha^{(p-1)/2} + \beta^{(p-1)/2} \equiv 2 \left(\frac{\alpha}{p}\right) \pmod{p}.$$

This completes the proof of the lemma. ■

Lemma 5.2.4 *Let b and d be integers, and let p be an odd prime such that $\left(\frac{d}{p}\right) = \left(\frac{b^2-4d}{p}\right) = 1$. Then we have $\left(\frac{-b+\sqrt{b^2-4d}}{2}\right) = \left(\frac{-b+2\sqrt{d}}{p}\right)$.*

Proof: It is clear as

$$\left(\frac{-b+\sqrt{b^2-4d}}{2}\right)(-b+2\sqrt{d}) = \left(\frac{b-\sqrt{b^2-4d}-2\sqrt{d}}{2}\right)^2.$$

5.3 Some Numerical Examples

Example 5.3.1 $\rho(x) = x^3 + 3x^2 + 7x + 13$. Here $\text{disc}(\rho(x)) = -1984 = -2^6 \cdot 31$. By Lemma 2.3.11, $K = Q(\sqrt{-31})$, and, by Theorem 4.1.3, $f_0(M/K) = 1$. Since $h(-31) = 3$, for an odd prime p the congruence $\rho(x) = x^3 + 3x^2 + 7x + 13 \equiv 0 \pmod{p}$ has three solutions if and only if p is represented by the principal form $(1, 1, 8)$ of discriminant -31 .

Example 5.3.2 $\rho(x) = x^4 - 4x^3 + 7x^2 - 6x + 1$. Let M denote the splitting field of $\rho(x)$. By Example 2.5.1, $\rho(x)$ and $f(x) = x^4 + 4x^2 - 16$ have the same splitting field M and $\text{Gal}(M/Q) = D_4$. It is clear that $f_1(x) = x^4 + x^2 - 1$ also has splitting field M (if α is a root of $f(x)$ then $\alpha/2$ is a root of $f_1(x)$). Now appealing to Lemma 2.5.4 for $f_1(x)$, we find that the three quadratic subfields of M are

$$k' = Q(\sqrt{5}), \quad k = Q(\sqrt{-4}), \quad K = Q(\sqrt{-20}) \in K_M.$$

We note that $D = \text{disc}(f_1(x)) = -4^2 5^2$. Thus $D/d_k = -80$. Then by Corollary 5.1.7, for an odd prime p the congruence

$$x^4 - 4x^3 + 7x^2 - 6x + 1 \equiv 0 \pmod{p}$$

has four solutions if and only if p is represented by $(1, 0, 20)$ as $h(-80) = 4$.

Example 5.3.3 $\rho(x) = x^4 - 4x^3 + 4x^2 + 6$. $\rho(x)$ is irreducible by Eisenstein's criterion. With the notation of Lemma 2.5.1 we have $r(x) = x(x^2 - 4x - 24)$ and $E = Q(\sqrt{7})$. Now $g(x) = (x-2)^2(x^2+6)$ obviously does not split over E , so $\text{Gal}(M/Q) = D_4$. Since $\rho(x)$ and $r(x)$ have the same discriminant, we obtain $D = 2^{10} \cdot 3^2 \cdot 7$, $t^2 - 4d = -4d = -24$. Appealing to Lemma 2.5.3, we see that the fixed field of $\langle \sigma^2, \tau \rangle$ is $k = Q(\sqrt{-24})$ and $D/d_k = -2688$. Then by Corollary 5.1.7, there is a unique subgroup H of $H(-2688)$ with the properties:

- (i). $H(-2688)/H \simeq \text{Gal}(M/K) \simeq Z_4$.
- (ii). If $p (\neq 2, 3, 7)$ is a prime, then the congruence $x^4 - 4x^3 + 4x^2 + 6 \equiv 0 \pmod{p}$ has four solutions if and only if p is represented by one of the forms in H . We now determine the subgroup H . By direct computation we find

$$\begin{aligned} H(-2688) = & \{(1, 0, 672), (3, 0, 224), (4, 4, 169), (7, 0, 96), (12, 12, 59) \\ & (13, \pm 4, 52), (16, \pm 8, 43), (17, \pm 10, 41), \\ & (21, 0, 32), (23, \pm 16, 32), (28, 28, 31), (29, 26, 29)\}, \end{aligned}$$

so that $h(-2688) = 16$. It is clear that $H(-2688)$ has 2^3 elements of order ≤ 2 , thus the 2-rank of $H(-2688)$ is 3, and thus $H(-2688) \simeq Z_2 \times Z_2 \times Z_4$. Hence as $H(-2688)/H \simeq Z_4$ we must have $H \simeq Z_2 \times Z_2$. By direct computation, we have

$$\begin{aligned} 193 &= 4 \cdot 3^2 + 4 \cdot 3 \cdot (-1) + 169 \cdot 1^2, & 59 &= 12 \cdot 1^2 + 12 \cdot 1 \cdot (-1) + 59 \cdot (-1)^2, \\ 31 &= 28 \cdot 1^2 + 28 \cdot 1 \cdot (-1) + 31 \cdot (-1)^2, & 413 &= 29 \cdot (-3)^2 + 26 \cdot (-3) \cdot 4 + 29 \cdot 4^2, \end{aligned}$$

and $\rho(x) = x^4 - 4x^3 + 4x^2 + 6 \equiv 0 \pmod{p}$ has no solutions for $p = 193, 59, 31$ and 413. Hence we have

$$H = \{(1, 0, 672), (3, 0, 224), (7, 0, 96), (21, 0, 32)\}.$$

Example 5.3.4 $\rho(x) = x^5 - 5x + 12$. Here $D = \text{disc}(\rho(x)) = 2^{12}5^6$. Let M be the splitting field of $\rho(x)$. By Example 2.6.2, we know that $\text{Gal}(M/Q) = D_5$. Let $K \in K_M$. Let $L = Q(\alpha)$, where α is a root of $\rho(x)$. It is easy to show that $\rho(x)$ has only one real root. Thus, by Lemma 2.2.11, K is an imaginary quadratic field. We begin by showing that $K = Q(\sqrt{-40})$. By Lemma 2.3.10 we have

$$K = Q(\sqrt{-4}) \text{ or } Q(\sqrt{-8}) \text{ or } Q(\sqrt{-20}) \text{ or } Q(\sqrt{-40}).$$

Since the congruence

$$x^5 - 5x + 12 \equiv 0 \pmod{7}$$

has no solutions, Corollary 2.2.19 shows that $K \neq Q(\sqrt{-4})$ and $K \neq Q(\sqrt{-8})$ as $\left(\frac{-4}{7}\right) = \left(\frac{-8}{7}\right) = -1$. Since the congruence

$$x^5 - 5x + 12 \equiv 0 \pmod{3}$$

has only one solution, namely, $x = 0$, Theorem 2.2.18(i) shows that $K \neq Q(\sqrt{-20})$ as $\left(\frac{-20}{3}\right) = 1$. Hence we must have $K = Q(\sqrt{-40})$.

Next, we show that $f_0(M/K) = 5$. It is clear that the possible divisors of $f_0(M/K)$ are 2 and 5. As 2 is ramified in K , by Lemma 4.1.1, 2 is unramified in M/K . By Theorem 4.1.3, we have

$$f_0(M/K) = 1, 5 \text{ or } 5^{3/2}.$$

Suppose $f_0(M/K) = 1$. Then by Lemma 3.1.6, we obtain

$$M \subset F_1^+(K) = K,$$

it is clearly impossible. Suppose $f_0(M/K) = 5^{3/2}$. Then by Theorem 4.2.6(iii), we have $v_5(d_L) = 8$. This is impossible as $d_L \mid \text{disc}(\rho(x)) = 2^{12} \cdot 5^6$. Hence we must have $f_0(M/K) = 5$.

Finally, in Corollary 5.1.1, choose $f = f_0(M/K) = 5$, so that $d_K f^2 = -1000$. We have

$$\begin{aligned} H(-1000) = \{ & (1, 0, 250), (2, 0, 125), (7, \pm 6, 37), \\ & (11, \pm 10, 25), (13, \pm 12, 22), (14, \pm 8, 19) \} \end{aligned}$$

and $H = \{ (1, 0, 250), (2, 0, 125) \}$ is its unique subgroup of order 2. Thus for an odd prime $\neq 5$,

$$x^5 - 5x + 12 \equiv 0 \pmod{p}$$

has five solutions if and only if p is represented by one of the forms $(1, 0, 250)$ and $(2, 0, 125)$.

Finally we remark that $d_L = 2^6 \cdot 5^6$.

5.4 Representation of Primes by Principal Forms

As an application of our main theorems, we consider in this section the problem of the representation of primes by certain principal forms. Most of the results we obtain here unify existing results in the literature(see for example [1],[2], [3],[4],[5],[26], [27], and [35]).

Proposition 5.4.1 *Let K be a quadratic field and let f be a positive integer. Let $\Delta = d_K f^2$. As $F_f^+(K)$ is a dihedral extension, by Lemmas 2.1.8 and 2.1.9 we know that $F_f^+(K)$ is a composite field of cyclic dihedral extensions M_i 's where M_i 's satisfy $M_i \cap M_j = K$ if $i \neq j$. Let $\rho_i(x) \in \mathbb{Z}[x]$ be a dihedral polynomial with splitting field M_i . Let p be a prime not dividing $\text{disc}(\rho_i)$ for all i . Then*

$$p \text{ is represented by } 1_\Delta \iff \begin{cases} \left(\frac{d_K}{p}\right) = 1, \rho_i(x) \equiv 0 \pmod{p} \\ \text{has a solution for all } i. \end{cases}$$

Proof: By Lemma 3.1.12, p is represented by the principal form 1_Δ if and only if p splits completely in $F_f^+(K)$. As $F_f^+(K)$ is the composite field of M_i 's, by Lemma 1.2.2, we see that p is represented by the principal form 1_Δ if and only if p splits completely in every M_i . Now appealing to Theorem 3.1.2 the proposition follows. ■

Proposition 5.4.2 (Williams and Hudson [35]) *Let $K = \mathbb{Q}(\sqrt{-q})$, where $q = 11, 19, 43, 67, 163$. There exists a cubic dihedral polynomial $\rho_q(x)$ such that if p is a prime not dividing $\text{disc}(\rho_q)$ then*

$$p = x^2 + qy^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution,} \end{cases}$$

and we can choose $\rho_q(x)$ as follows:

q	$\rho_q(x)$	$\text{disc}(\rho_q)$
11	$x^3 + x^2 - x - 1$	$-2^2 \cdot 11$
19	$x^3 - 2x + 2$	$-2^2 \cdot 19$
43	$x^3 - x^2 - x + 3$	$-2^2 \cdot 43$
67	$x^3 + 2x^2 - 2x + 2$	$-2^2 \cdot 67$
163	$x^3 + 3x^2 - 5x + 3$	$-2^2 \cdot 163$

Proof: Since $d_K = -q \equiv 5 \pmod{8}$ and $h(\mathcal{O}_K) = 1$ we have

$$h(\mathcal{O}_2) = 2h(\mathcal{O}_K) \left(1 - \left(\frac{d_K}{2} \right) \frac{1}{2} \right) = 3,$$

so that the ring class field $F_2(K)$ is of degree 3 over K . By Lemma 2.2.4, $F_2(K)$ is the splitting field of a cubic dihedral polynomial $\rho_q(x)$. Then, the assertion of the lemma follows from Proposition 5.4.1. Next we show that the splitting field M of the polynomial $\rho_q(x)$ specified in the statement of the proposition is the ring class field $F_2(K)$. Since $\text{disc}(\rho_q) = -2^2 q$, Lemma 2.3.11 shows that $K \subset M$. We have by Theorem 4.1.3, $f_0(M/K) = 1$ or 2. Then, by Lemma 3.1.6, we have $M \subset F_2(K)$ so that $M = F_2(K)$. ■

Proposition 5.4.3 *Let $K = Q(\sqrt{q})$, where $q \equiv 5 \pmod{8}$ is a prime. Suppose that $h(\mathcal{O}_K) = 1$.*

(i) *Suppose that the fundamental unit of K has the form $\epsilon_K = T + U\sqrt{q}$, where $T, U \in \mathbb{Z}$. Then there exists a cubic dihedral polynomial $\rho_q(x)$ such that if p is a prime not dividing $\text{disc}(\rho_q)$ then*

$$p = x^2 - qy^2 \iff \begin{cases} \left(\frac{q}{p} \right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

(ii) *Suppose that the fundamental unit of K has the form $\epsilon_K = \frac{T+U\sqrt{q}}{2}$, where $T, U \in \mathbb{Z}$ with $T \equiv U \equiv 1 \pmod{2}$. Then for a prime $p \neq q$ we have*

$$p = x^2 - qy^2 \iff \left(\frac{q}{p} \right) = 1.$$

Proof: By Lemma 3.2.2, as $d_K = q \equiv 5 \pmod{8}$, we have

$$h(\mathcal{O}_2) = \frac{2h(\mathcal{O}_K)}{v} \left(1 - \left(\frac{d_K}{2} \right) \frac{1}{2} \right) = 3/v,$$

where $v = \log \epsilon_2 / \log \epsilon_K$. For the case (i) we have

$$\epsilon_K = T + U\sqrt{q} = \begin{cases} T + 2 \cdot \frac{U}{2} \sqrt{q}, & \text{if } U \text{ is even} \\ (T-1) + 2 \cdot \frac{1+U}{2} \sqrt{q}, & \text{if } U \text{ is odd} \end{cases} \in \mathcal{O}_2,$$

so that $\epsilon_2 = \epsilon_K$ and $v = 1$. Hence the ring class field $F_2(K)$ is of degree 3 over K . By Lemma 2.2.4, $F_2(K)$ is the splitting field of a cubic dihedral polynomial $\rho_q(x)$. Then the assertion of the proposition follows from Proposition 5.4.1.

For the case (ii), as $\epsilon_K \notin \mathcal{O}_2$, we must have $v = 3$, that is $\epsilon_2 = \epsilon_K^3$. Hence we have $N(\epsilon_2) = N(\epsilon_K)^3 = (-1)^3 = -1$, as $q \equiv 1 \pmod{4}$ is a prime. Then the assertion of the proposition follows from Proposition 5.4.1. This result can also be deduced directly from Gauss' theory of genera. ■

Example 5.4.1 $q = 37, 101, 197$

q	$\epsilon_{Q(\sqrt{q})}$	$\rho_q(x)$	$\text{disc}(\rho_q)$
37	$6 + \sqrt{37}$	$x^3 - 4x + 2$	$2^2 \cdot 37$
101	$10 + \sqrt{101}$	$x^3 - 4x^2 + 2$	$2^2 \cdot 101$
197	$14 + \sqrt{197}$	$x^3 - 4x^2 - 2x + 2$	$2^2 \cdot 197$

Using the same argument as in the proof of Proposition 5.4.2, we can show that $F_2(Q(\sqrt{q}))$ is the splitting field of $\rho_q(x)$. By Proposition 5.4.3 we have for $p \neq 2, q$

$$p = x^2 - qy^2 \iff \begin{cases} \left(\frac{q}{p} \right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Corollary 5.4.4 *Let m be an odd integer such that $q = m^2 + 4$ is a prime. Set $K = Q(\sqrt{q})$. Suppose that $h(\mathcal{O}_K) = 1$. Then for a prime $p \neq q$*

$$p = x^2 - qy^2 \iff \left(\frac{q}{p} \right) = 1.$$

Proof: This is an immediate corollary of Proposition 5.4.3(ii) as here we have $e_K = \frac{m+\sqrt{q}}{2}$. ■

Example 5.4.2 $q = 5, 13, 29, 53$.

Proposition 5.4.5 (Williams and Hudson [35]) Let $K = \mathbb{Q}(\sqrt{-q})$, where $q \equiv 3 \pmod{4}$ is a prime. Suppose that $h(\mathcal{O}_K) = 3$. Then there exists a cubic dihedral polynomial $\rho_q(x)$ such that if p is a prime not dividing $\text{disc}(\rho_q)$ we have

$$p = x^2 + xy + \left(\frac{1+q}{4}\right)y^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Further, if $q \equiv 7 \pmod{8}$ then

$$p = x^2 + qy^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Proof: The first assertion of the Proposition follows by appealing to Proposition 5.4.1. If $q \equiv 7 \pmod{8}$ then

$$h(\mathcal{O}_2) = 2h(\mathcal{O}_K) \left(1 - \left(\frac{d_K}{2}\right) \frac{1}{2}\right) = 3,$$

so that $F_2(K) = F_1(K)$. Then the second assertion of the lemma follows by appealing to Proposition 5.4.1. ■

Example 5.4.3 $q = 23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907$ (so that $h(-q) = 3$).

q	$\rho_q(x)$	q	$\rho_q(x)$
23	$x^3 - x + 1$	31	$x^3 + x + 1$
59	$x^3 + 2x + 1$	83	$x^3 + x^2 + x + 2$
107	$x^3 + x^2 + 3x + 2$	139	$x^3 - x^2 + x + 2$
211	$x^3 - 2x + 3$	283	$x^3 + 4x + 1$
307	$x^3 - x^2 + 3x + 2$	331	$x^3 - 2x^2 + 4x + 1$
379	$x^3 + x^2 + x + 4$	499	$x^3 + 4x + 3$
547	$x^3 + x^2 - 3x + 4$	643	$x^3 - 2x + 5$
883	$x^3 + 5x^2 - 5x + 2$	907	$x^3 - 5x^2 + x - 2$

$$\text{disc}(\rho_q) = -q.$$

Proposition 5.4.6 *Let $K = Q(\sqrt{q})$, where $q \equiv 1 \pmod{4}$ is a prime. Suppose that $h(\mathcal{O}_K) = 3$. Then there exists a cubic dihedral polynomial $\rho_q(x)$ such that if p is a prime not dividing $\text{disc}(\rho_q)$ then*

$$p = x^2 + xy + \left(\frac{1+q}{4}\right)y^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Further, if $q \equiv 1 \pmod{8}$ then

$$p = x^2 + qy^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Proof: Since $q \equiv 1 \pmod{4}$ is a prime, we have $N(\epsilon_K) = -1$. Then the first assertion of the lemma follows by appealing to Proposition 5.4.1. Next, we suppose that $q \equiv 1 \pmod{8}$. We have by Lemma 3.2.2

$$h(\mathcal{O}_2) = (2/v)h(\mathcal{O}_K) \left(1 - \left(\frac{-q}{2}\right)\frac{1}{2}\right) = 1/v.$$

Hence $v = 1$ and $F_2(K) = F_1(K)$ and the second assertion of the lemma follows. ■

Example 5.4.4 $q = 229, 257, 733, 761, 1373, 1489, 1901$.

q	$\rho_q(x)$	q	$\rho_q(x)$
229	$x^3 - 4x + 1$	257	$x^3 - 5x + 3$
733	$x^3 - 5x^2 + x + 2$	761	$x^3 - 4x^2 + x + 3$
1373	$x^3 - 3x^2 - 5x + 2$	1489	$x^3 - 4x^2 - 5x + 1$
1901	$x^3 - 4x^2 - 4x + 3$		

$$\text{disc}_q(\rho) = q.$$

Lemma 5.4.7 *Let q be an odd prime and let $K = Q(\sqrt{-2q})$. Then*

$$h(\mathcal{O}_K) \equiv \begin{cases} 2 \pmod{4}, & \text{if } \left(\frac{2}{q}\right) = -1, \\ 0 \pmod{4}, & \text{if } \left(\frac{2}{q}\right) = 1. \end{cases}$$

Further, suppose that $\left(\frac{2}{q}\right) = 1$, that is, $q \equiv \pm 1 \pmod{8}$. Then q can be expressed in the form

$$q = \begin{cases} -a^2 + 2b^2, & \text{if } q \equiv -1 \pmod{8}, \\ a^2 + 2b^2, & \text{if } q \equiv 1 \pmod{8}, \end{cases}$$

where the integers a and b satisfy

$$a \equiv \begin{cases} 1 \pmod{4}, & \text{if } b \equiv 0 \pmod{4}, \\ -1 \pmod{4}, & \text{if } b \equiv 2 \pmod{4}. \end{cases} \quad (5.3)$$

Set

$$\rho_q(x) = \begin{cases} (x^2 - a)^2 - 2b^2 = x^4 - 2ax^2 - q, & \text{if } q \equiv -1 \pmod{8}, \\ (x^2 - a)^2 + 2b^2 = x^4 - 2ax^2 + q, & \text{if } q \equiv 1 \pmod{8}. \end{cases} \quad (5.4)$$

Then the splitting field M of $\rho_q(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h(\mathcal{O}_K) = 4$ then $M = F_1(K)$.

Proof: We have by Theorem 4.3.12 that the Hilbert class field $F_1(K)$ contains the genus field

$$K(1) = \begin{cases} Q(\sqrt{2}, \sqrt{-q}), & \text{if } q \equiv 3 \pmod{4}, \\ Q(\sqrt{-2}, \sqrt{q}), & \text{if } q \equiv 1 \pmod{4}, \end{cases}$$

so that $[K(1) : K] = 2$. This implies that the 2-rank of $\text{Gal}(F_1(K)/K)$ is 1, so that $h(\mathcal{O}_K) \equiv 0 \pmod{2}$. We now show that

$$h(\mathcal{O}_K) \equiv 0 \pmod{4} \text{ if and only if } q \equiv \pm 1 \pmod{8}.$$

Suppose first that $h(\mathcal{O}_K) \equiv 0 \pmod{4}$. Set

$$\text{Gal}(F_1(K)/K) = G_2 \times G_{2'},$$

where G_2 is the 2-Sylow subgroup of $\text{Gal}(F_1(K)/K)$ and $G_{2'}$ is the direct product of all odd p -Sylow subgroups of $\text{Gal}(F_1(K)/K)$. G_2 is a cyclic group as the 2-rank of $\text{Gal}(F_1(K)/K)$ is 1. Let M be the fixed field of the subgroup $G_2^4 \times G_{2'}$. By Lemma

2.1.6, M is a dihedral extension with $\text{Gal}(M/K) \simeq G_2/G_2^4 \simeq Z_4$. It is obvious that $K(1) \subset M$. Set

$$k = \begin{cases} Q(\sqrt{2}), & \text{if } q \equiv 3 \pmod{4}, \\ Q(\sqrt{-2}), & \text{if } q \equiv 1 \pmod{4}. \end{cases}$$

Let $L = Q(\sqrt{\alpha})$ be a quadratic extension of k contained in M . Then there are integers a and b such that

$$\alpha = \begin{cases} a + b\sqrt{2}, & \text{if } q \equiv 3 \pmod{4}, \\ a + b\sqrt{-2}, & \text{if } q \equiv 1 \pmod{4}, \end{cases}$$

and $\gcd(a, b)$ is squarefree. It is obvious that

$$\rho_q(x) = \begin{cases} (x^2 - a)^2 - 2b^2 = x^4 - 2ax^2 + (a^2 - 2b^2), & \text{if } q \equiv 3 \pmod{4}, \\ (x^2 - a)^2 + 2b^2 = x^4 - 2ax^2 + (a^2 + 2b^2), & \text{if } q \equiv 1 \pmod{4} \end{cases}$$

is the minimal polynomial of $\sqrt{\alpha}$ over Q and M is the splitting field of $\rho(x)$ over Q . We now suppose $q \equiv 3 \pmod{4}$, and show that $q \equiv 7 \pmod{8}$. The case $q \equiv 1 \pmod{4}$ can be treated similarly. By Lemma 2.5.4, we have

$$K = Q(\sqrt{2(a^2 - 2b^2)}).$$

Let $g = \gcd(a, b)$ and set $a = ga_1$, $b = gb_1$. Then $K = Q(\sqrt{2(a_1^2 - 2b_1^2)})$, and as $K = Q(\sqrt{-2q})$, we see that $q \mid a_1^2 - 2b_1^2$ so that $q \equiv 7 \pmod{8}$.

Conversely, suppose that $q \equiv 7 \pmod{8}$. Set $k = Q(\sqrt{2})$. Since $\left(\frac{-q}{2}\right) = 1$, $h(\mathcal{O}_k) = 1$ and $N_{k/Q}(\epsilon_k) = N_{k/Q}(1 + \sqrt{2}) = -1$, there exists integers a and b such that

$$-q = a^2 - 2b^2.$$

Further, since $q \equiv 7 \pmod{8}$, we see that a is odd and b is even. Replacing a by $-a$ if necessary we obtain (5.3). Set $\alpha = \sqrt{a + b\sqrt{2}}$ and $L = Q(\alpha)$. Let $\rho(x) = x^4 - 2ax^2 - q$ be as in (5.4) and let M be the splitting field of $\rho(x)$ so that $\text{Gal}(M/Q) = D_4$. Next we prove that $M \subset F_1(K)$. First by Theorem 4.4.11

$$d_L = d_K d_k f_0(M/K)^2 = -2^6 q f_0(M/K)^2.$$

On the other hand, as a and b satisfy (5.3), from TABLE 1 of Theorem 2 of [20]

$$d_L = -2^6 q,$$

so that $f_0(M/K) = 1$. Thus, the extension $K \subset M$ is unramified, so that $M \subset F_1(K)$, which implies $h(\mathcal{O}_K) \equiv 0 \pmod{4}$.

In particular, if $h(\mathcal{O}_K) = 4$, then $M = F_1(K)$. Finally we remark that the first part of the lemma can also be proved by Gauss' theory of genera, see for example Brown [3]. ■

Proposition 5.4.8 *Let q be a prime which is congruent to ± 1 modulo 8 and let $K = Q(\sqrt{-2q})$. Let $\rho_q(x)$ be as in Lemma 5.4.7. Suppose that $h(\mathcal{O}_K) = 4$. Let p be a prime not dividing $\text{disc}(\rho_q) = 2^{14}b^4q^*$, then*

$$\begin{aligned} p = x^2 + 2qy^2 &\iff \begin{cases} \left(\frac{-2q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution} \end{cases} \\ &\iff \left(\frac{-2q}{p}\right) = \left(\frac{a + b\sqrt{\pm 2}}{p}\right) = 1 \\ &\iff \left(\frac{-2q}{p}\right) = \left(\frac{(a + \sqrt{\mp q})/2}{p}\right) = 1. \end{aligned}$$

Further we have

$$\begin{aligned} p = x^2 + 8qy^2 &\iff \begin{cases} p \equiv 1 \pmod{8}, \left(\frac{q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases} \\ &\iff p \equiv 1 \pmod{8}, \left(\frac{q}{p}\right) = \left(\frac{a + b\sqrt{\pm 2}}{p}\right) = 1 \\ &\iff p \equiv 1 \pmod{8}, \left(\frac{q}{p}\right) = \left(\frac{(a + \sqrt{\mp q})/2}{p}\right) = 1. \end{aligned}$$

Proof: By the assumptions of the lemma, Lemma 2.2.4 shows that the Hilbert class field of K is the splitting field of $\rho_q(x)$ over Q . The first assertion of the lemma follows by appealing to Proposition 5.4.1. Then the second assertion of the lemma follows from the fact that $F_2(K)$ is the composite field of $F_1(K)$ and $Q(\sqrt{-1})$. The latter equivalences follow from Theorem 5.2.1 and Lemma 5.2.4. ■

Example 5.4.5 $q = 7, 23, 41$ and 71 .

Proposition 5.4.9 *Let q be a prime which is congruent to ± 3 modulo 8, and set $K = Q(\sqrt{-2q})$. Suppose that $h(\mathcal{O}_K) = 2$. Let $p (\neq q)$ be an odd prime. Then*

$$p = x^2 + 2qy^2 \iff \left(\frac{\pm 2}{p}\right) = \left(\frac{\mp q}{p}\right) = 1.$$

Proof: Since $F_1(K)$ contains the genus field $K(1)$ and $h(\mathcal{O}_K) = 2$, we have $F_1(K) = K(1)$. Then appealing to Theorem 3.1.3(i), the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4]. ■

Example 5.4.6 $q = 11, 29$.

Lemma 5.4.10 *Let q be a prime which is congruent to 1 modulo 4. Let $K = Q(\sqrt{2q})$. Then*

$$h^+(\mathcal{O}_K) \equiv \begin{cases} 2 \pmod{4}, & \text{if } q \equiv 5 \pmod{8}, \\ 0 \pmod{4}, & \text{if } q \equiv 1 \pmod{8}. \end{cases}$$

Further, suppose that $q \equiv 1 \pmod{8}$. Then q can be expressed

$$q = a^2 - 2b^2,$$

where a and b are integers satisfying

$$a \equiv \begin{cases} 1 \pmod{4}, & \text{if } b \equiv 0 \pmod{4}, \\ -1 \pmod{4}, & \text{if } b \equiv 2 \pmod{4}. \end{cases}$$

Set

$$\rho_q(x) = (x^2 - a)^2 - 2b^2 = x^4 - 2ax^2 + q.$$

Then the splitting field M of $\rho_q(x)$ over Q satisfies

$$K \subset M \subset F_1^+(K).$$

In particular, if $h^+(\mathcal{O}_K) = 4$ then $M = F_1^+(K)$.

Proof: The proof is similar to that of Lemma 5.4.7. ■

Proposition 5.4.11 *Let q be a prime which is congruent to 1 modulo 8. Let $K = Q(\sqrt{2q})$. Suppose that $N(\epsilon_K) = -1$ and that $h(\mathcal{O}_K) = 4$. Let $\rho_q(x)$ be as in Lemma 5.4.10. Let p be a prime not dividing $\text{disc}(\rho_q) = 2^{14}b^4q$. Then we have*

$$\begin{aligned} p = x^2 - 2qy^2 &\iff \begin{cases} \left(\frac{2q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases} \\ &\iff \left(\frac{2q}{p}\right) = \left(\frac{a+b\sqrt{2}}{p}\right) = 1 \\ &\iff \left(\frac{2q}{p}\right) = \left(\frac{(a+\sqrt{-q})/2}{p}\right) = 1. \end{aligned}$$

Proof: Since $F_1(K)$ contains the genus field $K(1)$ and $h(\mathcal{O}_K) = 4$, we have by Lemma 5.4.10, $F_1(K) = K(1)$. Then appealing to Proposition 5.4.1, the assertion of the lemma follows. The latter equivalences follows from Theorem 5.2.1 and Lemma 5.2.4. ■

Example 5.4.7 $q = 41, 137, 313, 377, \dots$

Proposition 5.4.12 *Let q be a prime which is congruent to 5 modulo 8. Let $K = Q(\sqrt{2q})$, and suppose that $h(\mathcal{O}_K) = 2$. Let $p (\neq q)$ be an odd prime. Then*

$$p = x^2 - 2qy^2 \iff \left(\frac{2}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Proof: As $q \equiv 5 \pmod{8}$ we have $N(\epsilon_K) = -1$. Since $F_1(K)$ contains the genus field $K(1)$ and $h(\mathcal{O}_K) = 2$, we have by Lemma 5.4.7 $F_1(K) = K(1)$. Then appealing to Proposition 5.4.1, the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4]. ■

Example 5.4.8 $q = 5, 13, 29, 37, 53, 61, 101, \dots$

Proposition 5.4.13 *Let q be a prime which is congruent to 3 modulo 4. Let $K = Q(\sqrt{2q})$. Suppose that $h^+(\mathcal{O}_K) = 2$. Let $p (\neq q)$ be an odd prime. Then*

$$p = x^2 - 2qy^2 \iff \left(\frac{-2}{p}\right) = \left(\frac{-q}{p}\right) = 1.$$

Proof: Since $F_1^+(K)$ contains the genus field $K^+(1)$ and $h^+(\mathcal{O}_K) = 2$, we have $F_1^+(K) = K^+(1)$. Then appealing to Proposition 5.4.1, the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4]. ■

Example 5.4.9 $q = 3, 7, 11, 23, \dots$

Lemma 5.4.14 *Let q_1 and q_2 be two distinct odd primes at least one of which is congruent to 1 (mod 4). Set $q_1^* = (-1)^{\frac{q_1-1}{2}} q_1$, $q_2^* = (-1)^{\frac{q_2-1}{2}} q_2$, so that $q_1^* \equiv q_2^* \equiv 1 \pmod{4}$. Let $K = Q(\sqrt{q_1^* q_2^*})$. Then $h^+(\mathcal{O}_K) \equiv 0 \pmod{4}$ if and only if there are integers a , b and c such that*

$$c^2 q_2^* = a^2 + b^2 q_1^*,$$

where a and b satisfy either

$$a \equiv 1 \pmod{2}, b \equiv 0 \pmod{2}, a + b \equiv 1 \pmod{4}$$

or

$$q_1^* \equiv 5 \pmod{8}, a \equiv 6 \pmod{8}, a - b - q_1^* \equiv 3, 5 \pmod{16},$$

or

$$q_1^* \equiv 1 \pmod{8}, a \equiv 2 \pmod{8}, r \text{ even}, \frac{a^2 - q_1^* b^2}{2^r} \equiv 1 \pmod{4},$$

where $2^r \parallel a^2 - b^2 q_1^*$. Further, if $h^+(\mathcal{O}_K) \equiv 0 \pmod{4}$, set

$$\rho_q(x) = (x^2 - a)^2 - q_1^* b^2,$$

where a and b are given as above. Then the splitting field M of $\rho_q(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h^+(\mathcal{O}_K) = 4$ then $M = F_1(K)$.

Proof: By Theorem 4.3.12, the strict ring class field $F_1^+(K)$ of K contains the genus field

$$K^+(1) = Q(\sqrt{q_1^*}, \sqrt{q_2^*}).$$

This implies that the 2-part of $\text{Gal}(F_1^+(K)/K)$ is a cyclic group of order 2^r , $r \geq 1$. Now suppose that $h^+(\mathcal{O}_K) \equiv 0 \pmod{4}$. By Galois theory there is an extension $K \subset K^+(1) \subset M \subset F_1(K)$ with $\text{Gal}(M/K) = Z_4$. Let $k = Q(\sqrt{q_1^*})$ and let $L = k(\sqrt{a + b\sqrt{q_1^*}}) \subset M$, where a and b are integers with $\gcd(a, b)$ squarefree. It is obvious that $\sqrt{a + b\sqrt{q_1^*}}$ is a root of the irreducible polynomial

$$\rho_q(x) = (x^2 - a)^2 - q_1^* b^2,$$

and M is the splitting field of $\rho_q(x)$. Now by Lemma 2.5.4,

$$K = Q(\sqrt{4q_1^* b^2 (a^2 - q_1^* b^2)}) = Q(\sqrt{q_1^* (a^2 - q_1^* b^2)}) = Q(\sqrt{q_1^* q_2^*}).$$

Thus there is a positive integer c such that

$$q_2^* c^2 = a^2 - q_1^* b^2.$$

As $f_0(M/K) = 1$, we have by Theorem 4.4.11

$$d_L = d_K d_k = q_1^2 q_2^*. \quad (5.5)$$

Since $L = k(\sqrt{a + b\sqrt{q_1^*}})$, we have by TABLES 3 and 4 of Theorem 2 of [20] that (5.5) holds if and only if the conditions involving a and b of the lemma are satisfied.

Conversely, suppose that the conditions involving a and b of the lemma are satisfied. Set $\rho_q(x) = (x^2 - a)^2 - q_1^* b^2$, and $k = Q(\sqrt{q_1^*})$, $L = Q(\sqrt{a + b\sqrt{q_1^*}})$. Let M be the splitting field of $\rho_q(x)$. By Lemma 2.5.2 we have that $\text{Gal}(M/Q) = D_4$. By TABLES 3 and 4 of Theorem 2 of [20] that (5.5) holds, and then, by Theorem 4.4.11 we have $f_0(M/K) = 1$ so that $M \subset F_1^+(K)$, which implies that $h^+(\mathcal{O}_K) \equiv 0 \pmod{4}$. ■

Proposition 5.4.15 *Let q_1 and q_2 be two distinct odd primes at least one of which is congruent to 1 (mod 4). Let $K = Q(\sqrt{q_1^* q_2^*})$. Let $\rho(x)$ be as in Lemma 5.4.14. Further, if $q_1 \equiv q_2 \equiv 1 \pmod{4}$, we impose the additional condition $N(\epsilon_K) = -1$. Suppose that $h^+(\mathcal{O}_K) = 4$. Let p be a prime not dividing $\text{disc}(\rho)$. Then*

$$p = x^2 + xy + \left(\frac{1 - q_1^* q_2^*}{4}\right) y^2 \iff \left(\frac{q_1^*}{p}\right) = \left(\frac{q_2^*}{p}\right) = \left(\frac{a + b\sqrt{q_1^*}}{p}\right) = 1,$$

where the integers a and b are defined in Lemma 5.4.14. Further, if $q_1^* q_2^* = -q_1 q_2 \equiv 1 \pmod{8}$ then

$$p = x^2 + q_1 q_2 y^2 \iff \left(\frac{q_1^*}{p}\right) = \left(\frac{q_2^*}{p}\right) = \left(\frac{a + b\sqrt{q_1^*}}{p}\right) = 1,$$

if $q_1^* q_2^* = q_1 q_2 \equiv 1 \pmod{8}$ then

$$p = x^2 - q_1 q_2 y^2 \iff \left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = \left(\frac{a + b\sqrt{q_1}}{p}\right) = 1.$$

Proof: Since $F_1^+(K)$ contains the splitting field M of $\rho(x)$ and $h^+(\mathcal{O}_K) = 4$, we have by Lemma 5.4.14, $F_1^+(K) = M$. Further, if $q_1^* q_2^* = -q_1 q_2 \equiv 1 \pmod{8}$ then $F_2^+(K) = F_1^+(K)$. Finally, appealing to Proposition 5.4.1, the assertion of the lemma follows. ■

Example 5.4.10 Case $d_K < 0$. $q_1 q_2 = 39, 55, 155, 203, 259, 291, 323, 355, 667, 723, 763, \dots$

For $q_1q_2 = 39$, we have $13 = (-1)^2 + 2^2 \cdot 3$, and by Proposition 5.4.15

$$p = x^2 + 39y^2 \iff \left(\frac{-3}{p}\right) = \left(\frac{13}{p}\right) = \left(\frac{-1 + 2\sqrt{-3}}{p}\right) = 1.$$

For $q_1q_2 = 55$, we have $5 \cdot 3^2 = (-1)^2 + 2^2 \cdot 11$, and by Proposition 5.4.15

$$p = x^2 + 55y^2 \iff \left(\frac{-11}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{-1 + 2\sqrt{-11}}{p}\right) = 1.$$

For $q_1q_2 = 291$, we have $97 = (-7)^2 + 4^2 \cdot 3$, and by Proposition 5.4.15

$$p = x^2 + xy + 73y^2 \iff \left(\frac{-3}{p}\right) = \left(\frac{97}{p}\right) = \left(\frac{-7 + 4\sqrt{-3}}{p}\right) = 1.$$

Case $d_K > 0$. $q_1q_2 = 145, 445, \dots$

Proposition 5.4.16 *Let q_1 and q_2 be two distinct odd primes at least one of which is congruent to 1 (mod 4). Let $K = Q(\sqrt{q_1^*q_2^*})$. Suppose that $h^+(\mathcal{O}_K) = 2$. Further if $q_1 \equiv q_2 \equiv 1 \pmod{4}$, we impose the additional condition $N_{K/Q}(\epsilon_K) = -1$. Let p ($\neq q_1, q_2$) be a prime. Then*

$$p = x^2 + xy + \left(\frac{1 - q_1^*q_2^*}{4}\right)y^2 \iff \left(\frac{q_1^*}{p}\right) = \left(\frac{q_2^*}{p}\right) = 1.$$

Further, if $q_1^*q_2^* = -q_1q_2 \equiv 1 \pmod{8}$ then

$$p = x^2 + q_1q_2y^2 \iff \left(\frac{q_1^*}{p}\right) = \left(\frac{q_2^*}{p}\right) = 1,$$

and, if $q_1^*q_2^* = q_1q_2 \equiv 1 \pmod{8}$, then

$$p = x^2 - q_1q_2y^2 \iff \left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = 1.$$

Proof: Since $F_1(K)$ contains $K(1)$ and since $h(\mathcal{O}_K) = 2$, we have $F_1(K) = K(1)$. Then appealing to Theorem 3.1.3(i), the assertion of the proposition follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4]. ■

Example 5.4.11 Case $d_K < 0$. $q_1q_2 = 15, 35, 51, 91, 115, 123, 187, 235, 267, \dots$

Case $d_K > 0$. $q_1q_2 = 65, 85, 185, 365, 481, 485, 493, 533, 629, \dots$

Proposition 5.4.17 *Let q_1 and q_2 be two distinct primes both congruent to 3 (mod 4). Let $K = \mathbb{Q}(\sqrt{q_1 q_2})$. Suppose that $h^+(\mathcal{O}_K) = 2$. Let p ($\neq q_1, q_2$) be a prime. Then*

$$p = x^2 + xy + \left(\frac{1 - q_1 q_2}{4}\right) y^2 \iff \left(\frac{-q_1}{p}\right) = \left(\frac{-q_2}{p}\right) = 1.$$

Further, if $q_1 q_2 \equiv 1 \pmod{8}$ then

$$p = x^2 - q_1 q_2 y^2 \iff \left(\frac{-q_1}{p}\right) = \left(\frac{-q_2}{p}\right) = 1.$$

Proof: Since $F_1(K)$ contains $K(1)$ and since $h^+(\mathcal{O}_K) = 2$, we have $F_1(K) = K(1)$. Then appealing to Theorem 3.1.3(i), the assertion of the proposition follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4]. ■

Example 5.4.12 $q_1 q_2 = 21, 33, 57, 69, 77, 93, 129, 133, 141, 161, \dots$

Proposition 5.4.18 *Let q be a prime which is congruent to ± 1 modulo 8. Set $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{\frac{q-1}{2}} q$. Suppose that $h^+(\mathcal{O}_K) = 1$. Let p ($\neq q$) be a prime. Then*

$$p = x^2 + xy + \frac{1 - q^*}{4} y^2 \iff \left(\frac{q^*}{p}\right) = 1$$

and

$$p = x^2 - q^* y^2 \iff \left(\frac{q^*}{p}\right) = 1.$$

Further, for $q \equiv 7 \pmod{8}$, so that $q = 7$ by the Baker-Stark theorem, we have

$$p = x^2 + 28y^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{-7}{p}\right) = 1 \iff p \equiv 1, 9, 25 \pmod{28},$$

$$p = x^2 + 112y^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-7}{p}\right) = 1 \iff p \equiv 1, 9, 25 \pmod{56}.$$

For $q \equiv 1 \pmod{8}$ we have $\epsilon_4 = \epsilon_2$ and

$$h^+(\mathcal{O}_2) = 1, h^+(\mathcal{O}_4) = 2,$$

so that

$$p = x^2 - 4qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{q}{p}\right) = 1,$$

and

$$p = x^2 - 16qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Proof: For $K = Q(\sqrt{-7})$, we have by Lemma 3.2.2

$$h(\mathcal{O}_2) = h(\mathcal{O}_K) = 1, \quad h(\mathcal{O}_4) = 2, \quad h(\mathcal{O}_8) = 4$$

and by Theorem 4.3.12

$$F_4(K) = Q(\sqrt{-1}, \sqrt{-7}), \quad F_8(K) = Q(\sqrt{-1}, \sqrt{2}, \sqrt{-7}).$$

Then the assertion of the lemma follows from Proposition 5.4.1.

Now we suppose that $q \equiv 1 \pmod{8}$. In this case $d_K > 0$, and we have by Lemma 3.2.2

$$h(\mathcal{O}_2) = 1/v_2, \quad h(\mathcal{O}_4) = 2/v_4, \quad h(\mathcal{O}_8) = 4/v_8,$$

where v_i denotes the least positive integer n such that $\epsilon^n \in \mathcal{O}_i$. Clearly $v_2 = 1$. Next, we prove that

$$v_4 = 2, \quad v_8 = 2.$$

Suppose that $v_4 = 1$. Then $h(\mathcal{O}_4) = 2$ and $F_4(K)$ is a quadratic extension of K , that is, $\text{Gal}(F_4(K)/Q) = D_2$ is an Abelian group. On the other hand, by Theorem 4.3.12, we know that the maximal subfield of $F_4(K)$ which is Abelian over Q is the genus field $K(4) = Q(\sqrt{q}) = K$. This is a contradiction. Hence we must have $v_4 = 2$ and $h(\mathcal{O}_4) = 1$. Since $\epsilon_4 = \epsilon_K^2$, we have $N(\epsilon_4) = 1$, so that $h^+(\mathcal{O}_4) = 2h(\mathcal{O}_4) = 2$. By Theorem 4.3.12, $F_4^+(K)$ contains $K^+(4) = Q(\sqrt{-1}, \sqrt{q})$, so that $F_4^+(K) = Q(\sqrt{-1}, \sqrt{q})$. Using the same argument as above, we can show that $v_8 = 2$ and $F_8^+(K) = Q(\sqrt{-1}, \sqrt{2}, \sqrt{q})$. Finally, appealing to Proposition 5.4.1 the assertion of the proposition follows. ■

Example 5.4.13 $q = 17$

$$p = x^2 - 17y^2 \iff \left(\frac{17}{p}\right) = 1,$$

$$p = x^2 - 68y^2 \iff p \equiv 1 \pmod{4} \text{ and } \left(\frac{17}{p}\right) = 1,$$

$$p = x^2 - 272y^2 \iff p \equiv 1 \pmod{8} \text{ and } \left(\frac{17}{p}\right) = 1.$$

Lemma 5.4.19 Let q be a prime which is congruent to 1 modulo 4. Set $K = Q(\sqrt{-q})$.

Then

$$h(\mathcal{O}_K) \equiv 0 \pmod{4} \text{ if and only if } q \equiv 1 \pmod{8}. \quad (5.6)$$

Further, if $q \equiv 1 \pmod{8}$, then q can be expressed uniquely up to sign of b in the form

$$q = a^2 + b^2,$$

where $a \equiv 1 \pmod{4}$ and $b \equiv 0 \pmod{4}$. Set

$$\rho_q(x) = x^4 - 2ax^2 + q.$$

Then the splitting field M of $\rho_q(x)$ over Q satisfies

$$K \subset M \subset F_1(K).$$

In particular, if $h(\mathcal{O}_K) = 4$ then $M = F_1(K)$.

Proof: By Theorem 4.3.12, the Hilbert class field $F_1(K)$ of K contains

$$K(1) = Q(\sqrt{-1}, \sqrt{q}).$$

This, by Lemma 4.3.11, implies that the 2-rank of $\text{Gal}(F_1(K)/K)$ is 1, so that $h(\mathcal{O}_K) \equiv 0 \pmod{2}$. Further, suppose that $h(\mathcal{O}_K) \equiv 0 \pmod{4}$. Set

$$\text{Gal}(F_1(K)/K) = G_2 \times G_{2'},$$

where G_2 is the 2-Sylow subgroup of $\text{Gal}(F_1(K)/K)$ and $G_{2'}$ is the direct product of all odd p -Sylow subgroups of $\text{Gal}(F_1(K)/K)$. G_2 is a cyclic group as the 2-rank of $\text{Gal}(F_1(K)/K)$ is 1. Let M be the fixed field of the subgroup $G_2^4 \times G_{2'}$. By Lemma 2.2.4, M is a dihedral extension with $\text{Gal}(M/K) \simeq G_2/G_2^4 \simeq Z_4$. It is obvious that $K(1) \subset M$. Set $k = Q(\sqrt{-1})$. Let $L = Q(\sqrt{\alpha})$ be a quadratic extension of k contained in M . Then there are integers a and b such that $\alpha = a + b\sqrt{-1}$ and $\gcd(a, b)$ is squarefree. It is obvious that $\rho_q(x) = (x^2 - a)^2 + b^2 = x^4 - 2ax^2 + (a^2 + b^2)$ is the minimal polynomial of $\sqrt{\alpha}$ over Q and M is the splitting field of $\rho(x)$ over Q . By Lemma 2.5.4, we have

$$K = Q(\sqrt{-(a^2 + b^2)}) = Q(\sqrt{-q}),$$

so that there is a c such that $c^2q = a^2 + b^2$. By TABLE 2 of Theorem 2 of [20], as $L = Q(\sqrt{a + b\sqrt{-1}})$, we have

$$d_L = q \cdot 2^e, \text{ for some integer } e = 2, 4, 6 \text{ or } 8.$$

On the other hand, as $f_0(M/K) = 1$, we have by Theorem 4.3.5

$$d_L = d_K d_k = (-4q)(-4) = 2^4 q,$$

showing that $e = 4$. This holds, by TABLE 2 of Theorem 2 of [20], we must have $a \equiv 1 \pmod{2}$ and $b \equiv 0 \pmod{4}$. This condition implies that $q \equiv 1 \pmod{8}$. Conversely, suppose that $q \equiv 1 \pmod{8}$. Then there are integers a and b such that $q = a^2 + b^2$ with a odd and $b \equiv 0 \pmod{4}$. We may choose a such that $a \equiv 1 \pmod{4}$. By Lemma 2.5.2, $\rho_q(x) = x^4 - 2ax^2 + q$ is a dihedral polynomial of type 1. Let M be the splitting field, and let $k = Q(\sqrt{-1})$, $L = Q(\sqrt{a + b\sqrt{-1}})$. Then by TABLE 2 of Theorem 2 of [20] we have

$$d_L = 2^4 q,$$

and by Theorem 4.4.11 we have

$$d_L = d_K d_k f_0(M/K)^2 = (-4)(-4q) f_0(M/K)^2 = 2^4 q f_0(M/K)^2,$$

so that $f_0(M/K) = 1$. This implies $M \subset F_1(K)$ so that $h(\mathcal{O}_K) \equiv 0 \pmod{4}$. Finally, if $h(\mathcal{O}_K) = 4$, we have $M = F_1(K)$. ■

Proposition 5.4.20 (Brandler [6]) *Let q be a prime which is congruent to 1 modulo 8. Set $K = Q(\sqrt{-q})$. Let $\rho(x)$ as be in Lemma 5.4.19. Suppose that $h(\mathcal{O}_K) = 4$. Let p be a prime not dividing bq . Then*

$$\begin{aligned} p = x^2 + qy^2 &\iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases} \\ &\iff \left(\frac{-q}{p}\right) = \left(\frac{a+b\sqrt{-1}}{p}\right) = 1 \\ &\iff \left(\frac{-q}{p}\right) = \left(\frac{(a+\sqrt{q})/2}{p}\right) = 1. \end{aligned}$$

Proof: As $h(\mathcal{O}_K) = 4$, by Lemma 5.4.19, we have $F_1(K)$ is the splitting field of $\rho(x) = x^4 - 2ax^2 + q$. Then appealing to Proposition 5.4.1, the first assertion of the lemma follows. The latter assertions follow from Theorem 5.2.1 and Lemma 5.2.4. ■

Example 5.4.14 $q = 17, 73, 97, 193$.

Proposition 5.4.21 *Let q be a prime which is congruent to 1 modulo 4. Set $K = Q(\sqrt{-q})$. Suppose that $h(\mathcal{O}_K) = 2$. Let $p (\neq q)$ be a prime. Then*

$$p = x^2 + qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{q}{p}\right) = 1. \quad (5.7)$$

Let p be a prime not dividing bq . Then

$$p = x^2 + 4qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{a + b\sqrt{-1}}{p}\right) = 1, \quad (5.8)$$

and

$$p = x^2 + 16qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{a + b\sqrt{-1}}{p}\right) = 1, \quad (5.9)$$

where $q = a^2 + b^2$ and $a \equiv 1 \pmod{2}$ and $b \equiv 2 \pmod{4}$.

Proof: Since $F_1(K) = Q(\sqrt{-1}, \sqrt{-q})$, (5.7) follows from Theorem 3.1.3(i). By Lemma 3.2.2, we have

$$h(\mathcal{O}_2) = 4, \quad h(\mathcal{O}_4) = 8.$$

Next we show that (5.8). Let $k = Q(\sqrt{-1})$, $L = Q(\sqrt{a + b\sqrt{-1}})$. Let $\rho(x) = x^4 - 2ax^2 + q$ and let M be the splitting field of $\rho(x)$. By Lemma 2.5.2 we have $\text{Gal}(M/Q) = D_4$. Then By Theorem 4.4.11 we have

$$d_L = d_K d_k f_0(M/K)^2 = 2^4 q f_0(M/K)^2,$$

by TABLE 2 of Theorem 2 of [20] we have

$$d_L = 2^6 q,$$

so that $f_0(M/K) = 2$. By Lemma 3.1.6, we have $M \subset F_2(K)$ so that $M = F_2(K)$ as $h(\mathcal{O}_2) = 4$. Then (5.8) follows from Proposition 5.4.1 and Theorem 5.2.1.

Note that as $F_4(K)$ is the composite field of $F_2(K)$ and $Q(\sqrt{2})$, (5.9) follows from Proposition 5.4.1 and Theorem 5.2.1. ■

Example 5.4.15 $q = 5, 13, 37$.

Proposition 5.4.22 *Let q be a prime which is congruent to 3 modulo 4. Set $K = Q(\sqrt{q})$. Suppose that $h^+(\mathcal{O}_K) = 2$. Then*

$$p = x^2 - qy^2 \iff \left(\frac{-1}{p}\right) = \left(\frac{-q}{p}\right) = 1.$$

Proof: Since $F_1^+(K)$ contains $K^+(1)$ and $h^+(\mathcal{O}_K) = 2$, we have by Theorem 4.3.12

$$F_1^+(K) = K^+(1) = Q(\sqrt{-1}, \sqrt{-q}).$$

Then appealing to Theorem 3.1.3(i), the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4].

■

Example 5.4.16 $q = 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 83, 103, 107, \dots$

Proposition 5.4.23 *Let q_1 and q_2 be two distinct odd primes. Set $K = Q(\sqrt{-2q_1q_2})$. Suppose that $h(\mathcal{O}_K) = 4$. Let p ($\neq 2, q_1, q_2$) be a prime. Then*

$$p = x^2 + 2q_1q_2y^2 \iff \left(\frac{\pm 2}{p}\right) = \left(\frac{q_1^*}{p}\right) = \left(\frac{q_2^*}{p}\right) = 1,$$

where the $\pm$ sign is determined by $q_1q_2 \equiv \pm 3 \pmod{4}$.

Proof: Since $F_1(K)$ contains $K(1)$ and $h(\mathcal{O}_K) = 4$, we have by Theorem 4.3.12

$$F_1(K) = K(1) = Q(\sqrt{\pm 2}, \sqrt{q_1^*}, \sqrt{q_2^*}).$$

Then, appealing to Theorem 3.1.3(i), the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4].

■

Example 5.4.17 $q_1q_2 = 15, 35, 39, 51, 65, 95, \dots$

Proposition 5.4.24 *Let q_1 and q_2 be two distinct odd primes which are congruent to 1 modulo 4. Set $K = Q(\sqrt{2q_1q_2})$. Suppose that $h(\mathcal{O}_K) = 4$. Let p ($\neq 2, q_1, q_2$) be an odd prime. Then*

$$p = x^2 - 2q_1q_2y^2 \iff \left(\frac{2}{p}\right) = \left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = 1.$$

Proof: Since $F_1(K)$ contains $K(1)$ and $h(\mathcal{O}_K) = 4$, we have by Theorem 4.3.12

$$F_1(K) = K(1) = Q(\sqrt{2}, \sqrt{q_1}, \sqrt{q_2}).$$

Then, appealing to Theorem 3.1.3(i), the assertion of the lemma follows. This result can also be deduced directly from Gauss' theory of genera, see for example Brown [4].

■

Example 5.4.18 $q_1 q_2 = 65, 85, 145, 185, 265, 305, \dots$.

Proposition 5.4.25 Set $K = Q(\sqrt{-1})$. Then we have

$$F_2(K) = K, F_4(K) = K(\sqrt{2}), F_8(K) = K(\sqrt[4]{2}).$$

Let p be an odd prime. Then

$$p = x^2 + 4y^2 \iff p \equiv 1 \pmod{4}, \quad (5.10)$$

$$p = x^2 + 16y^2 \iff p \equiv 1 \pmod{8}, \quad (5.11)$$

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1 \pmod{8} \text{ and } x^4 \equiv 2 \pmod{p} \\ \text{has a solution.} \end{cases} \quad (5.12)$$

Proof: Since $h(K) = 1$, we have by Gauss' formula (Lemma 3.2.2)

$$h(\mathcal{O}_2) = 1, h(\mathcal{O}_4) = 2, h(\mathcal{O}_8) = 4,$$

so that $F_2(K) = K$, $[F_4(K) : K] = 2$ and $[F_8(K) : K] = 4$. On the other hand, we have by Theorem 4.3.12, the genus field of $F_4(K)$ is $K(4) = Q(\sqrt{-1}, \sqrt{2})$, so

$$F_4(K) = K(4) = Q(\sqrt{-1}, \sqrt{2}) = K(\sqrt{2}).$$

Next, let M be the splitting field of the dihedral polynomial $x^4 - 2$, that is $M = Q(\sqrt{-1}, \sqrt[4]{2}) = K(\sqrt[4]{2})$, and set

$$k = Q(\sqrt{2}), \quad L = Q(\sqrt[4]{2}).$$

By TABLE 1 of Theorem 2 of [20], we have $d_L = -2^{11}$. Further, by Theorem 4.4.11, we obtain

$$f_0(M/K) = \sqrt{\frac{d_L}{d_K d_k}} = \sqrt{\frac{-2^{11}}{-4 \cdot 8}} = 8.$$

Now appealing to Lemma 3.1.6, we have $M \subset F_8(K)$ and consequently,

$$F_8(K) = M = K(\sqrt[4]{2}).$$

The results (5.10)-(5.12) are well-known. The first two can be deduced directly from Gauss' theory of genera, see for example Brown [4]. We prove the last statement. Since $F_8(K) = Q(\sqrt{-1}, \sqrt[4]{2})$ is the splitting field of the dihedral polynomial $x^4 - 2$, by Theorem 3.1.3(i),

$$p = x^2 + 64y^2 \iff x^4 \equiv 2 \pmod{p} \text{ has four integer solutions.}$$

Then (5.12) follows from Proposition 5.4.1. The result (5.12) is due to Gauss [16].

■

Proposition 5.4.26 *Set $K = Q(\sqrt{-2})$. Then we have*

$$F_2(K) = K(\sqrt{-1}), F_4(K) = K(\sqrt{1 + \sqrt{-1}}) = K(\sqrt{1 + \sqrt{2}}).$$

Let p be an odd prime. Then

$$p = x^2 + 2y^2 \iff \left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \pmod{8}, \quad (5.13)$$

$$p = x^2 + 8y^2 \iff \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{8}, \quad (5.14)$$

$$\begin{aligned} p = x^2 + 32y^2 &\iff p \equiv 1 \pmod{8}, \left(\frac{1 + \sqrt{-1}}{p}\right) = 1 \\ &\iff p \equiv 1 \pmod{8}, \left(\frac{1 + \sqrt{2}}{p}\right) = 1. \end{aligned} \quad (5.15)$$

Proof: Since $h(K) = 1$, we have by Gauss' formula (Lemma 3.2.2) $h(\mathcal{O}_2) = 2$, $h(\mathcal{O}_4) = 4$, so that $[F_2(K) : K] = 2$ and $[F_4(K) : K] = 4$. On the other hand, we have by Theorem 4.3.12, the genus field of $F_2(K)$ is $K(2) = Q(\sqrt{-1}, \sqrt{-2})$, so

$$F_2(K) = K(2) = Q(\sqrt{-1}, \sqrt{-2}).$$

Next, let M be the splitting field of the dihedral polynomial $x^4 - 2x^2 + 2$ so that $M = K(\sqrt{1 + \sqrt{-1}})$ and let $k = Q(\sqrt{-1})$ and $L = Q(\sqrt{1 + \sqrt{-1}})$. By TABLE 2 of Theorem 2 of [20], we have $d_L = 2^9$. Further, by Theorem 4.4.11, we obtain

$$f_0(M/K) = \sqrt{\frac{d_L}{d_K d_k}} = \sqrt{\frac{2^9}{(-8)(-4)}} = 4.$$

Now appealing to Lemma 3.1.6, we have $M \subset F_4(K)$ and consequently,

$$F_4(K) = M = K(\sqrt{1 + \sqrt{-1}}).$$

Similarly, using $x^4 - 2x^2 - 1$ in place of $x^4 - 2x^2 + 2$, we obtain

$$F_4(K) = K(\sqrt{1 + \sqrt{2}}).$$

The results (5.13)-(5.14) are well-known. They can be deduced directly from Gauss' theory of genera, see for example Brown [4]. We prove (5.15). Since $F_4(K) = Q(\sqrt{-1}, \sqrt{1 + \sqrt{-1}})$ is the splitting field of the dihedral polynomial $(x^2 - 1)^2 + 1$, by Theorem 3.1.3(i),

$$p = x^2 + 32y^2 \iff (x^2 - 1)^2 + 1 \equiv 0 \pmod{p} \text{ has four integer solutions.}$$

Then the assertion of the proposition follows by appealing to Proposition 5.4.1 and Theorem 5.2.1. The result (5.15) is due to Barrucand and Cohn [1]. ■

Proposition 5.4.27 *Set $K = Q(\sqrt{2})$. Then we have*

$$F_2^+(K) = Q(\sqrt{-1}).$$

Let p be an odd prime. Then

$$p = x^2 - 2y^2 \iff \left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}, \quad (5.16)$$

and for any positive integer n

$$p = x^2 - 2 \cdot 2^{2n}y^2 \iff \left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{8}. \quad (5.17)$$

Proof: As $h(K) = 1$, the assertion (5.16) follows from Proposition 5.4.1.

It is easy to show that $\epsilon_{2^n} = \epsilon_K^{2^n}$. By Lemmas 3.2.2 and 1.3.9 we have $h^+(\mathcal{O}_{2^n}) = 2$, so that $[F_{2^n}^+(K) : K] = 2$. On the other hand, we have by Theorem 4.3.12, the genus field of $F_{2^n}^+(K)$ is $K^+(2^n) = Q(\sqrt{2}, \sqrt{-1})$, so

$$F_{2^n}^+(K) = K^+(2^n) = Q(\sqrt{2}, \sqrt{-1}).$$

the assertion (5.17) of the proposition follows by appealing to Proposition 5.4.1. ■

Proposition 5.4.28 Set $K = Q(\sqrt{-3})$. Then we have

$$F_2(K) = K, F_4(K) = K(\sqrt{-1}), F_8(K) = K(\sqrt{-1}, \sqrt{2}), F_6(K) = K(\sqrt[3]{2}).$$

Let p be a prime $\neq 2, 3$. Then

$$p = x^2 + 3y^2 \iff \left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod{3}, \quad (5.18)$$

$$p = x^2 + 12y^2 \iff \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{12}, \quad (5.19)$$

$$p = x^2 + 48y^2 \iff \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1 \iff p \equiv 1 \pmod{24}, \quad (5.20)$$

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod{3} \text{ and } x^3 \equiv 2 \pmod{p} \\ \text{has a solution.} \end{cases} \quad (5.21)$$

Proof: Since $h(K) = 1$, we have by Gauss' formula (Lemma 3.2.2)

$$h(\mathcal{O}_2) = 1, h(\mathcal{O}_4) = 2, h(\mathcal{O}_8) = 4, h(\mathcal{O}_6) = 3,$$

so that

$$F_2(K) = K, [F_4(K) : K] = 2, [F_8(K) : K] = 4, [F_6(K) : K] = 3.$$

On the other hand, by Theorem 4.3.12 we have

$$K(4) = Q(\sqrt{-3}, \sqrt{-1}), \quad K(8) = Q(\sqrt{-3}, \sqrt{-1}, \sqrt{2}),$$

so that

$$F_4(K) = Q(\sqrt{-3}, \sqrt{-1}), \quad F_8(K) = Q(\sqrt{-3}, \sqrt{-1}, \sqrt{2}).$$

Next, let M be the splitting field of the dihedral polynomial $x^3 - 2$, and let $L = Q(\sqrt[3]{2})$. Since $\text{disc}(x^3 - 2) = -2^2 \cdot 3^3$, the possible prime divisors of d_L are 2 or 3. Now by Theorem 4.1.3, we have that $f_0(M/K) \mid 6$. Then, appealing to Lemma 3.1.6, we have $M \subset F_6(K)$ and consequently,

$$F_6(K) = M = Q(\sqrt{-3}, \sqrt[3]{2}).$$

The results (5.18)-(5.21) are well-known. The first three can be deduced directly from Gauss' theory of genera, see for example Brown [4]. We prove the last statement. As $F_6(K) = Q(\sqrt{-3}, \sqrt[3]{2})$ is the splitting field of the dihedral polynomial $x^3 - 2$, (5.21) follows from Proposition 5.4.1. ■

Proposition 5.4.29 *Let $\rho_q(x)$ be any one of the quintics listed below:*

q	$\rho_q(x)$	$\text{disc}(\rho_q)$
47	$x^5 - x^3 - 2x^2 - 2x - 1$	47^2
79	$x^5 + 2x^4 - 3x^2 - 2x - 1$	79^2
103	$x^5 - x^4 - 3x^3 - 3x^2 - 2x - 1$	103^2
127	$x^5 - 3x^4 - x^3 + 2x^2 + x - 1$	127^2
131	$x^5 + x^4 + 2x^3 + x^2 + x - 2$	$2^2 \cdot 131^2$
179	$x^5 + x^4 - 3x^2 - x - 2$	$2^2 \cdot 179^2$
227	$x^5 - x^3 + 2x^2 + 3x - 4$	$2^4 \cdot 227^2$
347	$x^5 + 2x^4 + 3x^3 - 4x^2 - x - 2$	$2^4 \cdot 347^2$
443	$x^5 - x^4 - x^3 + 5x^2 + 3x - 5$	$2^4 \cdot 443^2$
523	$x^5 + x^4 + 3x^3 - 5x^2 - x - 3$	$2^4 \cdot 523^2$
571	$x^5 + x^4 - 2x^3 - 7x^2 - 3x - 2$	$2^2 \cdot 571^2$
619	$x^5 + x^4 + 4x^3 + 5x^2 + 3x - 2$	$2^2 \cdot 619^2$
691	$x^5 - 2x^4 + 3x^3 - 8x^2 - x - 6$	$2^4 \cdot 691^2$
739	$x^5 - 5x^4 + 6x^3 + 3x^2 + x - 2$	$2^2 \cdot 739^2$
787	$x^5 - 3x^3 - 3x^2 - 2x - 9$	$2^6 \cdot 787^2$

Let p denote a prime not dividing $\text{disc}(\rho_q)$. Then

$$p = x^2 + xy + \frac{1+q}{4}y^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Further if $q \equiv 7 \pmod{8}$, then

$$p = x^2 + qy^2 \iff \begin{cases} \left(\frac{-q}{p}\right) = 1 \text{ and } \rho_q(x) \equiv 0 \pmod{p} \\ \text{has a solution.} \end{cases}$$

Proof: Let M be the splitting field of $\rho_q(x)$ over Q and K be the unique quadratic subfield of M . We know that $\text{Gal}(M/Q) = D_5$ (see Example 2.6.5). Since $\rho_q(x)$ has only one real root, by Lemma 2.2.11, K is an imaginary quadratic field. Thus we have

$$K = Q(\sqrt{-q}) \text{ or } Q(\sqrt{-8q}).$$

Using Theorem 4.2.6 it is easy to see that $K = Q(\sqrt{-q})$ for $q \neq 787$. For $q = 787$, suppose $K = Q(\sqrt{-8 \cdot 787})$. Note that $\left(\frac{-8 \cdot 787}{3}\right) = 1$ and the congruence

$$\rho_{787}(x) = x^5 - 3x^3 - 3x^2 - 2x - 9 \equiv x(x^4 - 2) \equiv 0 \pmod{3}$$

has only one solution $x \equiv 0 \pmod{3}$, which is contrary to Theorem 2.2.18(i). Hence for $q = 787$, we also have $K = Q(\sqrt{-q})$. Next, Theorem 4.1.3 shows that $f_0(M/K) = 1$, so that M is contained in the Hilbert class field $F_1(K)$ of K . Since $h(\mathcal{O}_K) = 5$, we have $M = F_1(K)$. Then the assertion of the lemma follows by appealing to Proposition 5.4.1. ■

Bibliography

- [1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. **238**(1969), 67-70.
- [2] E. Brown, *The power of 2 dividing the class number of a binary quadratic discriminant*, J. Number Theory **5**(1973), 413-419.
- [3] E. Brown, *Class numbers of complex quadratic fields*, J. Number Theory **6**(1974), 185-191.
- [4] E. Brown, *Class numbers of quadratic fields*, Istituto Nazionale di Alta Matematica, Symposia Mathematica , XV (1975), 403-411.
- [5] E. Brown, *The class number and fundamental unit of $Q(\sqrt{2p})$, for $p \equiv 1 \pmod{16}$ a prime*, J. Number Theory **16**(1983), 95-99.
- [6] J. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory **5**(1973), 271-287.
- [7] D.A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer-Verlag New York Inc., 1989.
- [8] D.A. Buell, P.A. Leonard and K.S. Williams, *Note on the quadratic character of a quadratic unit*, Pacific J. Math. **92**(1981), 35-38.
- [9] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag New York Inc., 1978.
- [10] H. Cohn, *Advanced Number Theory*, Dover Publications, Inc., 1980.

- [11] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class field theory and Complex Multiplication*, John Wiley & Sons, New York, 1989.
- [12] D.S. Dummit, *Solving solvable quintics*, Math. Comp. **50**(1991), 387-401.
- [13] H.M. Edwards, *Galois Theory*, Springer-Verlag New York Inc., 1984.
- [14] R.J. Evans, *Residuacity of primes*, Preprint, University of California (La Jolla), January 1987.
- [15] D.J.H. Garling, *Galois Theory*, Cambridge University Press, 1986.
- [16] C.F. Gauss, *Theoria Residuorum Biquadraticorum, Commentatio Prima*, in Werke Vol. 2, published 1876, 65-92.
- [17] F. Halter-Koch, *Geschlechtertheorie der Ringklassenkörper*, J. Reine Angew. Math. **250**(1971), 107-108.
- [18] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3**(1951), 45-51.
- [19] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag New York Inc., 1981.
- [20] J.G. Huard, B.K. Spearman and K.S. Williams, *Integral bases for quartic fields with quadratic subfields*, Carleton-Ottawa Mathematical Lecture Note Series Number 4, June 1991.
- [21] N. Jacobson, *Lectures in Abstract Algebra Volume III, Theory of Fields and Galois Theory*, D. Van Nostrand Company, Inc., 1964.
- [22] N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, 1974.
- [23] P. Kaplan, K.S. Williams and Y. Yamamoto, *An application of dihedral fields to representations of primes by binary quadratic forms*, Acta Arith. **44**(1984), 407-413.
- [24] L-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, Amer. Math. Monthly **96**(1989), 133-137.

- [25] S. Lang, *Algebraic Number Theory*, Springer-Verlag New York Inc., 1986.
- [26] E. Lehmer, *On the quadratic character of the Fibonacci root*, *Fibonacci Quart.* **5**(1967), 135-138.
- [27] E. Lehmer, *On some special quartic reciprocity laws*, *Acta Arith.* **21**(1972), 367-377.
- [28] R.L. Long, *Algebraic Number Theory*, Marcel Dekker, Inc., 1977.
- [29] D.A. Marcus, *Number Fields*, Springer-Verlag New York Inc., 1977.
- [30] B.K. Spearman and K.S. Williams, *The cubic congruence $x^3 + Ax^2 + Bx + C \equiv 0 \pmod{p}$ and binary quadratic forms*, *J. London Math. Soc.* (to appear).
- [31] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, *Verhandlungen des ersten internationalen Mathematiker Kongresses in Zürich*, 1897, Leipzig, 1898, 182-193.
- [32] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag New York Inc., 1982.
- [33] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Book Company, Inc., 1963.
- [34] K.S. Williams, K. Hardy and C. Friesen, *On the evaluation of the Legendre symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$* , *Acta Arith.* **45** (1985), 255-272.
- [35] K.S. Williams and R.H. Hudson, *Representation of primes by the principal form of discriminant $-D$ when the class number $h(-D)$ is 3*, *Acta Arith.* **57** (1991), 131-153.

END

2|5 0|5 93

FIN