INFORMATION TO USERS

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

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

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

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

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

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

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

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106

78-4641

BAILY, Andrew Marc, 1949-
ON THE DENSITY OF DISCRIMINANTS OF
QUARTIC FIELDS.

The University of Michigan,
Ph.D., 1977
Mathematics

University Microfilms International, Ann Arbor, Michigan 48106

ON THE DENSITY OF DISCRIMINANTS OF QUARTIC FIELDS

by
Andrew Marc Baily

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1977

Doctoral Committee

Professor Donald J. Lewis, Chairman
Associate Professor Carl J. Alexius
Associate Professor Melvin Hochster
Assistant Professor K.-Y. Shih
Peter J. Weinberger, Research Scientist, Bell Laboratories

ACKNOWLEDGEMENTS

I would like to express my appreciation to my thesis advisor, Professor Donald J. Lewis, for the tremendous amount of time he spent helping me put this dissertation together and for teaching me how to write mathematics.

I would especially like to thank Dr. Peter J. Weinberger for introducing me to the subject of algebraic number theory and, in particular, to the problem on which this dissertation is based. He has been invaluable as a source of knowledge and encouragement throughout the writing of this dissertation.

I would also like to thank Mr. Pat Morton for acting as a sounding board for many of the ideas in this work, and Ms. Peggy Lubahn who explained to me the fine points of technical typing.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ii

CHAPTER

ONE: INTRODUCTION 1

TWO: PRELIMINARIES 10

THREE: QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS SYMMETRIC GALOIS GROUP 26

FOUR: QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS ALTERNATING GALOIS GROUP 45

FIVE: QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS DIHEDRAL GALOIS GROUP 60

SIX: NORMAL QUARTIC FIELDS WITH KLEIN FOUR GALOIS GROUP 73

SEVEN: NORMAL QUARTIC FIELDS WITH CYCLIC GALOIS GROUP 93

EIGHT: CONCLUSIONS AND CONJECTURES 99

NOTATION 102

BIBLIOGRAPHY 104

CHAPTER ONE

INTRODUCTION

HISTORY OF THE PROBLEM. The general problem is that of counting the number of algebraic number fields of a given degree as a function of their discriminants. If we let $N_n(X)$ denote the number of fields of degree n whose discriminants do not exceed X is absolute value, then there is a conjecture [21, p. 467], that $\lim_{X\to\infty} \frac{N_n(X)}{X}$ exists. More precisely, we are interested in evaluating the size of $N_n(X,G)$, the number of fields of degree n whose discriminants do not exceed X in absolute value and whose normal closure over Q has Galois group G, and even more precisely, we consider the cases of positive and negative discriminants separately, letting a + or - sign indicate this distinction.

The problem is particularly simple for quadratic fields in that they are uniquely characterized by their discriminants in the following way. If $K_2 = Q(\sqrt{d})$ is a quadratic field, with d a squarefree integer, and we let $D = \text{disc}(K_2)$, then

$$D = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \end{cases}$$

Conversely, is D is a quadratic discriminant, i.e. a squarefree integer $d \equiv 1 \pmod 4$ or $4d$ where $d \equiv 2$ or $3 \pmod 4$ with d squarefree, then $K_2 = Q(\sqrt{D}) = Q(\sqrt{d})$ is the unique quadratic field

of discriminant D. It can be easily shown from these considerations that

$$\lim_{X\to\infty} \frac{N_2^+(X)}{X} = \lim_{X\to\infty} \frac{N_2^-(X)}{X} = \frac{3}{\pi^2} .$$

The situation becomes more complicated for fields of higher degree in two respects. First, in general there are no necessary and sufficient conditions for an integer to be the discriminant of a field of given degree. Although special cases are known, e.g. pure cubic fields or cyclic fields of prime degree, the only general cases that seem workable are for Abelian fields and even these cases can become very complicated (see Chapters Six and Seven). Second, there may be a large number of fields of a given degree having the same discriminant, a problem depending on the very difficult question of determining the distribution of class numbers of fields of a given degree.

The first step in solving this problem for cyclic cubic fields was taken by H. Hasse [10], who showed that the discriminant of a cyclic cubic field is necessarily of the form f^2, where f is of the form $p_0p_1 \cdots p_n$ or $9p_1 \cdots p_n$, with p_i distinct primes $\equiv 1 \pmod 6$, and if f is of the above form, then there are 2^n cyclic cubic fields of discriminant f^2, necessarily subfields of the cyclotomic field of f^{th} roots of unity. The final step was taken in 1953 by H. Cohn [4], who showed, on the basis of the above considerations and via the use of generating functions, that

$$\lim_{X\to\infty} \frac{N_3(X,C_3)}{X^{\frac{1}{2}}} \text{ exists (see Lemma 20).}$$

The problem is more difficult for non-cyclic cubic fields in that

they are not subfields of any cyclotomic field and therefore rational class field theory will not apply. If K_3 is a non-cyclic cubic field with normal closure K_6 and K_2 is one of the conjugate quadratic subfields of K_6 then Hasse [11] described the relations between the discriminants and relative discriminants of these fields. Specifically, he gave necessary and sufficient conditions for $\mathrm{disc}(K_2)$ to be equal to $\mathrm{disc}(K_3)$. Davenport and Heilbronn [5] used these considerations to determine lower bounds for $N_3^+(X,S_3)$ and $N_3^-(X,S_3)$ based on the analogous results for quadratic fields. The problem of an upper bound is complicated by the fact that a given quadratic field may be a subfield of a large number of distinct sextic fields of bounded discriminant, and this in turn depends on the rank of the 3 - class group of a quadratic field, about which very little is known. Davenport and Heilbronn [5] were able to circumvent this problem via Davenport's work on cubic forms. They set up a correspondence between cubic fields of discriminant d and classes of strictly inequivalent, irreducible, primitive, integral, binary cubic forms of discriminant d, and were able to determine an upper bound for $N_3^+(X,S_3)$ and $N_3^-(X,S_3)$ of the same order of magnitude as their lower bound. They commented at this point that the work needed to improve the constants, "would not be negligible and would not narrow the gap considerably". In a later paper [6] they refined their upper bound technique to produce a discriminant preserving correspondence between cubic fields and a certain subset of classes of forms and were able to determine the precise asymptotic density of such fields (see Lemma 7).

A different approach to the problem of counting fields was taken by Van der Waerden [26] and P. X. Gallagher [7]. Let $F_n(X)$ denote the set of polynomials of the form $F(t) = t^n + a_1 t^{n-1} + \ldots + a_n$ such that $\text{height}(F) = \max_i(|a_i|) \leq X$ and the Galois group of $F(t)$ is a proper subgroup of S_n, and let $E_n(X) = \text{Card } F_n(X)$. Then Van der Waerden showed that $E_n(X) << X^{n-c}$, with $c = \frac{1}{18n(n!)^3}$, and Gallagher improved this by sieve methods to show that $E_n(X) << X^{n-\frac{1}{2}}\log^{(1-\gamma)}X$, with $\gamma \sim (2\pi n)^{-\frac{1}{2}}$. These results show that almost all polynomials of a fixed degree are irreducible and have Galois group S_n.

STATEMENT OF RESULTS AND METHODS. In this dissertation, we consider the problem of evaluating $N_n(X,G)$ for fields of degree four, i.e. $n = 4$. Here, we have five separate cases, depending on whether the normal closure of the quartic field over Q has Galois group: S_4, A_4, D_4, C_4, or KL_4. These are the only possibilities as these are the only transitive subgroups of S_4.

We obtain lower bounds for $N_4(X,S_4)$ and $N_4(X,A_4)$ by essentially following the argument of Davenport and Heilbronn [5] in their earlier lower bound estimate for $N_3(X,S_3)$. If K_3 is a non-cyclic cubic field, then we give a necessary and sufficient condition for a field K_{24} of degree 24, to contain K_3 and have $\text{Gal}(K_{24}/Q) = S_4$. The field K_{24} is then the normal closure of any of its quartic subfields, say K_4. For fields K_3 and K_4, related in this way, Heilbronn [13] proved a relation between $\text{disc}(K_3)$ and $\text{disc}(K_4)$ analogous to the result of Hasse [11] for cubic and quadratic fields mentioned earlier (see Lemma 1 and equation (17)). These results, together

with Davenport and Heilbronn's asymptotic result for cubic fields enable us to prove

$$\underline{\text{THEOREM 1.}} \quad \varliminf_{X\to\infty} \frac{N_4^+(X,S_4)}{X} \geq [4608\zeta(3)]^{-1}$$

$$\varliminf_{X\to\infty} \frac{N_4^-(X,S_4)}{X} \geq [1536\zeta(3)]^{-1}.$$

In the case of the alternating group A_4, the same method is used except that we start with a cyclic cubic field K_3, and we embed it in a field K_{12} of degree 12, such that $\mathrm{Gal}(K_{12}/Q) = A_4$. Again, Heilbronn's relation holds for K_3 and any of the quartic subfields of K_{12} (see Lemma and equation (24)). These results, together with the result of H. Cohn, mentioned earlier, enable us to prove

$$\underline{\text{THEOREM 3.}} \quad \varliminf_{X\to\infty} \frac{N_4(X,A_4)}{X^{\frac{1}{2}}} \geq K_1, \quad \text{where } K_1 \text{ is a constant.}$$

For the upper bound in the case of the symmetric group S_4, we start with a non-cyclic cubic field K_3 and we need an upper bound on the number of fields K_{24} of degree 24 over Q such that $\mathrm{Gal}(K_{24}/Q) = S_4$, and such that the discriminant of any of the quartic subfields of K_{24} is not too much larger than $\mathrm{disc}(K_3)$. Vie Heilbronn's relations and other considerations (see Lemmas 3, 4, and 5), the problem is reduced to that of finding an upper bound for the number of quadratic extensions K_6, of K_3, subject to certain

conditions on the ideal $f = \mathrm{disc}(K_6/K_3)$. Since $\mathrm{Gal}(K_6/K_3)$ is Abelian, K_6 can be viewed, via class field theory, as a subfield of the ray class field (mod f) over K_3, and, therefore, corresponds to a primitive quadratic ray class character (mod f). By means of a structure theorem for such characters (see Proposition 14), we find an upper bound for the number of such characters, involving the 2-rank of the ideal class group of K_3. From these results we obtain

THEOREM 2. $N_4(X,S_4) << X^{3/2}\log^4 X$.

In the case of A_4, the same method is used. We start with a cyclic cubic field K_3 and reduce the problem of counting the number of fields K_{12}, containing K_3, with $\mathrm{Gal}(K_{12}/Q) = A_4$, and such that the discriminant of any of the quartic subfields of K_{12} is not too much larger than $\mathrm{disc}(K_3)$, to the problem of counting the number of quadratic extensions K_6, of K_3, subject to certain conditions on the ideal $\mathrm{disc}(K_6/K_3)$. We prove

THEOREM 4. $N_4(X,A_4) << X\log^4 X$.

For the upper when the Galois group is the dihedral group of order 8, D_4, we view such quartic fields K_4 as quadratic extensions of their unique quadratic subfield K_2. First, we determine the form of the ideal $\mathrm{disc}(K_4/K_2)$ (see Lemma 24), and , as in the A_4

and S_4 cases, determine an upper bound for the number of such extensions. This result, together with the fact that we know all the quadratic fields, enables us to prove

THEOREM 5. $\overline{\lim_{X\to\infty}} \frac{N_4(X,D_4)}{X} \leq K_2$, where K_2 is a constant.

For the lower bound in the D_4 case, we follow the same procedure as for the upper bound except that we must insure that for a particular choice of the ideal $\mathrm{disc}(K_4/K_2)$, there actually is a quadratic extension K_4 with this ideal as relative discriminant (see Lemmas 27 and 28). This enables us to prove

THEOREM 6. $\underline{\lim_{X\to\infty}} \frac{N_4(X,D_4)}{X} \geq K_3$, where K_3 is a constant.

The two remaining Abelian cases can be handled by rational class field theory. An Abelian field of conductor f can be embedded in the field of f^{th} roots of unity Q_f. It therefore corresponds to a subgroup of the character group of $\mathrm{Gal}(Q_f/Q) = (Z/fZ)^{\times}$.

For the case of the cyclic group of order four, C_4, we therefore have to count the number of primitive quartic characters of conductor f. Hasse [10] described which f can be the conductor of a cyclic quartic field, the value of the discriminant of such a field, and the number of cyclic quartic fields with a given discriminant (see Lemmas 34, 36, and 37). From these results, we construct a generating function for the number of cyclic quartic fields which have a

given discriminant and from this prove

THEOREM 10. $N_4(X,C_4) \sim K_4$, where K_4 is a constant.

When the Galois group is the Klein four group KL_4, it is easier to go directly to the structure of the subfields of the quartic field. Since KL_4 has three elements of order 2, such a quartic field has three quadratic subfields. Each of these is uniquely characterized as $Q(\sqrt{d})$ for some d, and the group structure of KL_4 gives relations between the d's for the three subfields (see the proof of Lemma 31). After several combinatorial lemmas to count the number of ways a fixed set of rational primes can be distributed between the discriminants of the quadratic subfields without affecting the discriminant of the quartic field, we prove

THEOREM 9. Let $J(n) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) = n\}$

a) If n is an integer not of the form m^2, 2^4m^2, 2^6m^2, or 2^8m^2 where m is a squarefree odd integer, then $J(n) = 0$.

b) Let m be a squarefree odd integer. Then

1) $J(m^2) = \frac{1}{2}(3^{\omega(m)-1} - 1)$

2) $J(2^4m^2) = \frac{1}{2}(3^{\omega(m)} - 1)$

3) $J(2^6m^2) = \frac{1}{2}(3^{\omega(m)} - 1)$

4) $J(2^8m^2) = 3^{\omega(m)}$

where $\omega(m)$ is the number of distinct prime divisors of m.

From this theorem, we construct a generating function for the number of Klein four quartic fields with a given discriminant, and this enables us to prove

THEOREM 7. $N_4(X,KL_4) \sim K_5 X^{\frac{1}{2}} \log^2 X$, where K_5 is a constant.

In the results for the symmetric and alternating groups, there is a discrepancy of $X^{\frac{1}{2}}\log^4 X$ between the lower and upper bounds, which at this time seems unavoidable. The reason is that very little is known about the class structure of cubic fields. In the final chapter, we discuss what the problems are and what we conjecture to be true.

CHAPTER TWO

PRELIMINARIES

This chapter contains all the general background results from algebraic and analytic number theory that we shall need. Standard results are stated without proof, although references are provided. Proofs are included where the result is not standard.

Throughout this chapter K, L, M will be a tower of algebraic number fields: $K \subseteq L \subseteq M$.

PROPOSITION 1. $\mathrm{Disc}(K) > 0$ if and only if $r_2(K)$ is even, where $r_2(K)$ denotes the number of pairs of complex conjugates of K.

Proof. See Janusz [16, p. 53].

PROPOSITION 2. $\mathrm{Disc}(M/K) = \mathrm{Disc}(L/K)^{[M:L]} N_{L/K}(\mathrm{Disc}(M/L))$.

Proof. See Narkiewitz [21, p. 148 Prop. 4.8].

PROPOSITION 3. Assume that L/K is normal with $\mathrm{Gal}(L/K)$ cyclic of prime degree p and let $\delta = \mathrm{disc}(L/K)$. Then,

a) If $\mathfrak{P}$ is a prime ideal in K, prime to 2, and ramifying in L, then $\mathfrak{P}^{p-1} \| \delta$.

b) If $\mathfrak{p}$ is a prime ideal in K, dividing 2, and ramifying in L, then $\mathfrak{p}^{(p-1)(\nu+1)} \| \delta$, where ν denotes the number of distinct ramification groups in the Hilbert series for $\mathfrak{p}$

in L/K, and $1 \leq \nu \leq \frac{pe_{K/Q}(\mathfrak{p})}{p-1}$.

Proof. See H. Hasse [9, pp. 74-75].

PROPOSITION 4. Let a be an element of $K \setminus K^2$.

a) If $\mathfrak{P}$ is an odd prime ideal in K then $\mathfrak{P}$ ramifies in $K(a^{\frac{1}{2}})$ if and only if $\mathfrak{P}$ divides the ideal (a) precisely to an odd power.

b) If $\mathfrak{p}$ is an even prime ideal in K. say $\mathfrak{p}^h \| 2$ and $\mathfrak{p}^n \| (a)$, then $\mathfrak{p}$ does not ramify in $K(a^{\frac{1}{2}})$ if and only if there exists an element α in K such that $a \equiv \alpha^2 \pmod{\mathfrak{p}^{2h+n}}$.

Proof. See Hilbert [14, §4 Theorem 4].

By following through the argument in Hilbert's proof of b) above, Godwin [8] was able to prove the following extension of b).

PROPOSITION 5. In the notation of Proposition 4 b), let m be the largest rational integer such that $a \equiv \alpha^2 \pmod{\mathfrak{p}^m}$ has a solution in K and let k be the largest rational integer satisfying $2h + n \leq 2k$ and $m \leq 2k$. Then $\mathfrak{p}^{2h+n-2k} \| \operatorname{disc}(K(a^{\frac{1}{2}})/K)$.

COROLLARY 6. Let a be an element of $O_K \setminus O_K^2$ and let $\delta = \operatorname{disc}(K(a^{\frac{1}{2}})/K)$. Then $(a) = \delta \mathfrak{a}^2$ where $\mathfrak{a}$ is a fractional ideal in K and the only prime ideals that divide $\mathfrak{a}$ to a negative exponent are prime ideals dividing 2.

Proof. Let $(a) = \prod' \mathfrak{P}_i^{2a_i} \prod'' \mathfrak{D}_i^{2b_i} \prod''' \mathfrak{p}_i^{n_i}$

where $\prod'$ runs over all odd prime ideals $\mathfrak{P}_i$ dividing (a) to an even power, $\prod''$ runs over all odd prime ideals $\mathfrak{D}_i$ dividing (a) to an odd power, and $\prod'''$ runs over all even prime ideals $\mathfrak{p}_i$ dividing (a). a_i, b_i, and n_i are positive integers.

It follows from Propositions 3, 4, and 5, using the notation of Proposition 5, that

$$\mathfrak{d} = \prod'' \mathfrak{D}_i \prod''' \mathfrak{p}_i^{2h_i+n_i-2k_i} \prod'''' \mathfrak{B}_i^{2h_i-2k_i}$$

where $\prod''''$ runs over all even prime ideals dividing $\mathfrak{d}$ but not dividing (a). Therefore, if we let

$$\mathfrak{a} = \prod' \mathfrak{P}_i^{a_i} \prod'' \mathfrak{D}_i^{b_i} \prod''' \mathfrak{p}_i^{k_i-h_i} \prod'''' \mathfrak{B}_i^{k_i-h_i}$$

then $(a) = \mathfrak{d}\mathfrak{a}^2$.

The second statement of the corollary follows from the fact that $a_i \geq 0$ and $b_i \geq 0$ but it may be that $h_i > k_i$ for some i.

Let $\mathfrak{a}$ be an ideal in K and let $G(\mathfrak{a}) = (O_K/\mathfrak{a})^\times$ denote the multiplicative group of residue classes (mod $\mathfrak{a}$) which are prime to $\mathfrak{a}$. A character on $G(\mathfrak{a})$ is called <u>primitive</u> if it is not a character on $G(\mathfrak{b})$ for any proper divisor $\mathfrak{b}$ of $\mathfrak{a}$. A character χ on $G(\mathfrak{a})$ is called <u>quadratic</u> if χ^2 is principal.

<u>PROPOSITION 7</u>. Let $\mathfrak{a}$ be an ideal in K. Then, $G(\mathfrak{a})$ has a real, hence quadratic, primitive character if and only if $\mathfrak{a}$ has the following form:

$$\mathfrak{A} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t} \mathfrak{P}_1 \cdots \mathfrak{P}_r$$

where $\mathfrak{P}_i$ are distinct odd prime ideals in K, and $\mathfrak{p}_i$ are distinct even prime ideals and a_i are integers satisfying $0 \leq a_i \leq 1 + 2e_{K/Q}(\mathfrak{p})$.

Proof. See Narkiewitz [21, p. 250 Prop. 6.6].

PROPOSITION 8. Let $\mathfrak{A}$ be an ideal in K. Then, $G(\mathfrak{A})$ is cyclic if and only if one of the following cases holds:

a) $\mathfrak{A} = \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal,

b) $\mathfrak{A} = \mathfrak{p}^2$ where $\mathfrak{p}$ is a prime ideal with $f_{K/Q}(\mathfrak{p}) = 1$,

c) $\mathfrak{A} = \mathfrak{P}^n$ for arbitrary n, where $\mathfrak{P}$ is an ideal, prime to 2, with $f_{K/Q}(\mathfrak{P}) = e_{K/Q}(\mathfrak{P}) = 1$,

d) $\mathfrak{A} = \mathfrak{p}^3$ where $\mathfrak{p}$ is a prime ideal, dividing 2, with $f_{K/Q}(\mathfrak{p}) = 1$ and $e_{K/Q}(\mathfrak{p}) \neq 1$.

e) $\mathfrak{A} = \mathfrak{P}^n\mathfrak{p}$ where $\mathfrak{P} \neq \mathfrak{p}$ are prime ideals with $\mathfrak{p}$ dividing 2, dividing $p \neq 2$ and if we let $f_1 = f_{K/Q}(\mathfrak{P})$ and $f_2 = f_{K/Q}(\mathfrak{p})$ we have one of the following holding:

1) $n = 1$ and $(2^{f_2} - 1, p^{f_1} - 1) = 1$,

2) $n = 2$, $f_1 = 1$ and $(2^{f_2} - 1, p(p - 1)) = 1$,

3) $n \geq 3$, $f_1 = 1$, $e_{K/Q}(\mathfrak{P}) = 1$ and $(2^{f_2} - 1, p(p - 1)) = 1$.

Proof. See Narkiewitz [21, p. 249 Theorem 6.2].

PROPOSITION 9. Let $\mathfrak{A}$ be an ideal in K and let $\phi(\mathfrak{A})$ denote the order of $G(\mathfrak{A})$. Then, if $\mathfrak{A} = \prod \mathfrak{p}_i^{a_i}$, where $\mathfrak{p}_i$ are distinct prime ideals in K, we have $\phi(\mathfrak{A}) = \prod N_{K/Q}(\mathfrak{p}_i)^{a_i - 1}(N_{K/Q}(\mathfrak{p}_i) - 1)$.

Proof. See Lang [19, p. 126].

PROPOSITION 10. Let $B \subseteq A$ be finite Abelian groups and let $C = A/B$. Then, any character on A can be expressed as a product of a character on C and a character on B.

Proof. First, any character on B can be extended to a character on A (see Serre [23, p. 61]). Let χ be a character on A. Then χ_B is a character on B which can be extended to a character χ_B on A such that $\chi_B|_B = \chi|_B$. Then the character χ_C on A defined by $\chi_C(a) = \frac{\chi(a)}{\chi_B(a)}$ is trivial on B, hence a character on C, i.e. $\chi_C(\bar{a}) = \chi_C(a)$, where $\bar{a} = a + B$, and $\chi = \chi_B\chi_C$.

Background on Class Field Theory

The results in this section can be found in Takagi [24], Lang [19, Chapter VII §1], Janusz [16, Chapter IV 1], Hasse [9, p. 61], and Iyanaga [15, pp. 494-496].

A modulus, or integral divisor f in K is a formal product of primes in K, including the infinite primes, of the form

$$f = \prod \mathfrak{p}_i^{a_i}$$

where a_i are nonnegative integers with $a_i > 0$ for only a finite number of $\mathfrak{p}_i$. Furthermore, $a_i = 0$ or 1 if $\mathfrak{p}_i$ is a real infinite prime and $a_i = 0$ if $\mathfrak{p}_i$ is a complex infinite prime.

We can write f as $f = f_o f_\infty$ where

$$f_o = \prod_{\substack{\text{finite} \\ \mathfrak{p}_i | f}} \mathfrak{p}_i^{a_i} \qquad f_\infty = \prod_{\substack{\text{infinite} \\ \mathfrak{p}_{i,\infty} | f}} \mathfrak{p}_{i,\infty}$$

We also use H. Hasse's notion of multiplicative congruence defined as follows. Let $\alpha \in K^\times$. $\alpha \equiv 1 \pmod^\times f$ if the fractional ideal $\frac{(\alpha-1)}{f_o}$ written as a quotient of mutually prime ideals, does not admit any primes dividing f_o in the denominator, and the conjugate α_i of α associated with the Archimedian valuation associated with $\mathfrak{p}_{i,\infty}$ is positive for all $\mathfrak{p}_{i,\infty}$ dividing f. We set $\alpha \equiv \beta \pmod^\times f$ if $\alpha/\beta \equiv 1 \pmod^\times f$.

Let C_K = The ideal class group of K.

I_K = The group of fractional ideals

$I(f)$ = The group of fractional ideals prime to f_o.

$P(f)$ = The group of principal fractional ideals prime to f_o.

P_f = The group of principal fractional ideals (a) satisfying $a \equiv 1 \pmod^\times f$, called the ray or strahl (mod f).

$K_f = \{a \in K \mid a \equiv 1 \pmod^\times f\}$

$K(f) = \{a \in K \mid (a)$ is prime to $f_o\}$

U = The group of units in O_K.

U_f = The group of units $u \equiv 1 \pmod^\times f$.

$S(f)$ = The number of real infinite primes dividing f_∞

Let i denote the homomorphism $K(f) \twoheadrightarrow P(f)$ given by $a \to (a)$. We have therefore $P_f = i(K_f)$ and $P(f) = i(K(f))$.

The ray class group (mod f) is defined by $R_f = I(f)/P_f$.

PROPOSITION 11. 1) $C_K \simeq I(f)/P(f)$, since each ideal class contains an ideal prime to any given ideal.

2) If f is of the form specified above, then

$$K(f)/K_f \simeq \prod_{\mathfrak{p}_i | f_0} G(\mathfrak{p}_i^{a_i}) \prod_{\mathfrak{p}_{i,\infty} | f_\infty} \{\pm 1\}.$$

3) $$\text{Card}(R_f) = \frac{h(K)\phi(f_0)2^{S(f)}}{[U:U_f]}$$

Proof. See Lang [19 pp. 125-127].

A subgroup H of I_K is called a congruence subgroup if there exists a modulus f such that $P_f \subset H \subset I(f)$. In this case we say that H is defined (mod f). If H_1 and H_2 are congruence subgroups (not necessarily defined with respect to the same modulus), then we define $H_1 \sim H_2$ if there exists a modulus f such that $H_1 \cap I(f) = H_2 \cap I(f)$. The relation $\sim$ is an equivalence relation. The equivalence classes are called ideal groups and the greatest common divisor of all such f is called the conductor of the ideal group. Also, if $H_{\mathfrak{a}}$ and $H_{\mathfrak{b}}$ are congruence subgroups which are representatives of the same ideal group, with $H_{\mathfrak{a}}$ defined (mod $\mathfrak{a}$) and $H_{\mathfrak{b}}$ defined (mod $\mathfrak{b}$), then $I(\mathfrak{a})/H_{\mathfrak{a}} \simeq I(\mathfrak{b})/H_{\mathfrak{b}}$.

PROPOSITION 12. Let H be an ideal group of conductor f in K with a representative H_f defined (mod f). Then there exists a unique Abelian extension L of K satisfying the following:

a) $\text{Gal}(L/K) \simeq I(f)/H_f$.

b) A prime ideal $\mathfrak{p}$ in K ramifies in L if and only if $\mathfrak{p} | f$.

c) A prime ideal $\mathfrak{p}$ in K, not dividing f, factors into a product of distinct prime ideals in L each with the same relative degree F, where F is the least positive integer such that $\mathfrak{p}^F \in H_f$.

d) The correspondence between ideal groups and Abelian extensions is order reversing.

Proof. See Iyanaga [15, p. 496] and Janusz [16, p. 179].

The field L in Proposition 12 is called the class field associated with the ideal group H and f is also called the conductor of L.

COROLLARY 13. The class field associated with the ideal group of conductor which has P_f as a representative is the maximal Abelian extension of K, ramified precisely at the primes dividing f. This field is called the ray class field (mod f).

PROPOSITION 14. A character on R_f can be expressed as a product of a character on $G(f_o)$, a character on C_K and a character of signature, which is a product of $S(f)$ characters of order 2.

Proof. $C_K \simeq I(f)/i(K(f))$

$$\simeq [I(f)/i(K_f)]/[i(K(f))/i(K_f)].$$

It follows from Proposition 10 that a character on R_f can be written as a product of a character on C_K and a character on $i(K(f))/i(K_f)$. Let ker denote the kernel of the canonical map $K(f)/K_f \twoheadrightarrow i(K(f))/i(K_f)$. Therefore $[K(f)/K_f]/\ker \simeq i(K(f))/i(K_f)$ and a character on $i(K(f))/i(K_f)$ can be viewed as a character on $K(f)/K_f$ which is trivial on ker. It follows from Proposition 11 2), that a character

on $K(f)/K_f$ can be expressed as a product of a character on $G(f_o)$ and a character on $\prod\{\pm 1\}$ which is in turn a product of $S(f)$ groups of order 2. Hence, the result follows.

Let L/K be an Abelian extension of conductor f corresponding to an ideal group H with representative H_f defined (mod f). Let χ be a character on $Gal(L/K) \simeq I(f)/H_f$, hence a character on R_f which is trivial on H_f. Define H_χ to be the maximal congruence subgroup containing H_f satisfying $\chi(H_\chi) = 1$ and we define the conductor f_χ of χ to be the conductor of the ideal group with representative H_χ.

As usual we let $\hat{G}$ denote the group of characters on the group G.

PROPOSITION 15 (Conductor - discriminant formula). Let L/K be an Abelian extension of conductor f. Then

$$f = \text{L.C.M.}_{\chi \in Gal(L/K)} f_\chi$$

and

$$disc(L/K) = \prod_{\chi \in Gal(L/K)} f_\chi .$$

Proof. See H. Hasse [9, p. 38].

Proposition 16. Let L/K be a cyclic extension with $\langle\tau\rangle = Gal(L/K)$. Let M/L be an Abelian extension which corresponds, as in Proposition 12, to an ideal group H. Then

a) M/K is normal if and only if $\tau(H) = H$.

b) M/K is Abelian if and only if the cosets of H are invariant under τ.

Proof. See H. Hasse [11, pp. 572-573].

PROPOSITION 17. Assume L/K is normal. Let χ be a character on $\mathrm{Gal}(L/K)$ and let $L(s, \chi, L/K)$ denote the Artin L - function associated with χ. Then the following properties hold.

a) $L(s, \chi, L/K)$ is regular for $\mathrm{Re}\ s > 1$.

b) If χ_o is the principal character then $L(s,\chi_o, L/K) = \zeta_K(s)$, where ζ_K is the Dedekind zeta function for K.

c) If χ_1, χ_2 are characters on $\mathrm{Gal}(L/K)$, then $L(s, \chi_1 + \chi_2, L/K) = L(s, \chi_1, L/K)L(s, \chi_2, L/K)$.

d) If M/K is also normal and χ is a character on $\mathrm{Gal}(L/K)$, viewed as a character on $\mathrm{Gal}(M/K)$, then $L(s, \chi, L/K) = L(s, \chi, M/K)$.

e) If M/K is normal and χ^* is the character on $\mathrm{Gal}(M/K)$ induced by a character χ on $\mathrm{Gal}(M/L)$, then $L(s, \chi^*, M/K) = L(s, \chi, M/L)$.

Proof. See Lang [19, p. 233] and Artin [2] and [3].

PROPOSITION 18. Let K_i $(1 \le i \le n)$ be algebraic number fields of degree n_i, discriminant d_i, and let $\zeta_i(s) = \zeta_{K_i}(s)$. If, for some set of rational integers $a_1, \ldots, a_n$, we have $\prod_{i=1}^{n} \zeta_i(s)^{a_i} = 1$ for all $s \in \mathbb{C}$, then it follows that $\prod_{i=1}^{n} d_i^{a_i} = 1$.

Proof. The functional equation for $\zeta_i(s)$ is

$$(1)\quad A_i^s \Gamma(s/2)^{r_1(K_i)} \Gamma(s)^{r_2(K_i)} \zeta_i(s) = A_i^{1-s} \Gamma\left(\frac{1-s}{2}\right)^{r_1(K_i)} \Gamma(1-s)^{r_2(K_i)} \zeta_i(1-s),$$

where $r_1(K_i)$ = the number of real conjugates of K_i

$r_2(K_i)$ = the number of pairs of complex conjugates of K_i

$$A_i = 2^{-r_2(K_i)} \pi^{-\frac{1}{2}n_i} |d_i|^{\frac{1}{2}}.$$

Combining (1) on one side of the equation and raising to the a_i^{th} power, we have, for all $s \in \mathbb{C}$

$$A_i^{(2s-1)} \left[\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\right]^{a_i r_1(K_i)} \left[\frac{\Gamma(s)}{\Gamma(1-s)}\right]^{a_i r_2(K_i)} \left[\frac{\zeta_i(s)}{\zeta_i(1-s)}\right]^{a_i} = 1.$$

Multiplying these together for all i we get

$$(2)\quad \prod_{i=1}^{n} [A_i^{a_i}]^{2s-1} \left[\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\right]^{\sum_{i=1}^{n} a_i r_1(K_i)} \left[\frac{\Gamma(s)}{\Gamma(1-s)}\right]^{\sum_{i=1}^{n} a_i r_2(K_i)} \times \frac{\prod_{i=1}^{n} \zeta_i(s)^{a_i}}{\prod_{i=1}^{n} \zeta_i(1-s)^{a_i}} = 1.$$

Since, by the hypothesis of the Proposition, we have

$$\prod_{i=1}^{n} \zeta_i(s)^{a_i} = \prod_{i=1}^{n} \zeta_i(1-s)^{a_i} = 1 \quad \text{for all } s \in \mathbb{C}$$

it follows that (2) becomes

$$(3)\qquad \prod_{i=1}^{n} [A_i^{a_i}]^{2s-1} \left[\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\right]^{\sum_{i=1}^{n} a_i r_1(K_i)} \left[\frac{\Gamma(s)}{\Gamma(1-s)}\right]^{\sum_{i=1}^{n} a_i r_2(K_i)} = 1$$

for all $s \in \mathbb{C}$.

Now $\Gamma(s)$ has poles at the negative integers and is regular and is non-zero at $s = -\frac{1}{2}$, 1, 2, and 3/2 . At $s = -1$, all the terms in (3) are regular and non-zero except $\Gamma(s)$ which has a pole. Therefore,

$$(4)\qquad \sum_{i=1}^{n} a_i r_2(K_i) = 0 ,$$

and (4) becomes

$$(5)\qquad \prod_{i=1}^{n} [A_i^{a_i}]^{2s-1} \left[\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\right]^{\sum_{i=1}^{n} a_i r_1(K_i)} = 1 \qquad \text{for all } s \in \mathbb{C} .$$

At $s = -2$, all the terms in (5) are regular and non-zero except $\Gamma(\frac{s}{2})$ which has a pole, hence

$$(6)\qquad \sum_{i=1}^{n} a_i r_1(K_i) = 0 ,$$

and (5) becomes

$$\prod_{i=1}^{n} [A_i^{a_i}]^{2s-1} = 1 \qquad \text{for all } s \in \mathbb{C} .$$

On taking $s = 1$, we get

$$(7)\qquad \prod_{i=1}^{n} A_i^{a_i} = 1 .$$

It follows from the fact that $n_i = r_1(K_i) + 2r_2(K_i)$ and from (4) and (6) that

$$\sum_{i=1}^{n} a_i n_i = 0 \ . \tag{8}$$

It follows from (8), (4), (6), and (7) that

$$1 = \prod_{i=1}^{n} 2^{-a_i r_2(K_i)} \ \pi^{-\frac{1}{2}n_i a_i} \ |d_i|^{\frac{1}{2}a_i} = \prod_{i=1}^{n} |d_i|^{\frac{1}{2}a_i} \ .$$

After squaring on both sides we obtain

$$\prod\nolimits' |d_i|^{a_i} \prod\nolimits'' |d_i|^{a_i} = 1 \tag{9}$$

where $\prod'$ runs over all i such that $a_i r_2(K_i)$ is even and $\prod''$ runs over all i such that $a_i r_2(K_i)$ is odd.

If a_i is even then $|d_i|^{a_i} = d_i^{a_i}$ and if $r_2(K_i)$ is even it follows from Proposition 1 that $d_i > 0$ hence $|d_i|^{a_i} = d_i^{a_i}$. But if $a_i r_2(K_i)$ is odd then $d_i < 0$ and $|d_i|^{a_i} = (-d_i)^{a_i}$. Therefore, (9) becomes

$$\prod\nolimits' d_i^{a_i} \prod\nolimits'' (-d_i)^{a_i} = 1 \ . \tag{10}$$

We can break up the sum in (10) as follows

$$\sum\nolimits' a_i r_2(K_i) + \sum\nolimits'' a_i r_2(K_i) = 0$$

where $'$ and $''$ are as in (10) .

Since $\sum' a_i r_2(K_i)$ is even, it follows that $\sum'' a_i r_2(K_i)$ is even and since each term in the second sum is odd, it must consist of an even number of terms. It follows that there are an even

number of terms in $\prod'(-d_i)^{a_i}$ in (10), hence (10) becomes

$$\prod_{i=1}^{n} d_i^{a_i} = 1 .$$

Let $h(K)$ denote the class number of K, $R(K)$ the regulator of K, and $W(K)$ the number of roots of unity in K.

PROPOSITION 19. $h(K)R(K) < c|d|^{\frac{1}{2}} \log^{n-1}|d|$

where $d = \mathrm{disc}(K)$

$n = [K:Q]$

and $c = e^{\frac{1}{2}2^{-n}}(\frac{3}{2\pi^2})^{r_1(K)}\pi^{-\frac{1}{2}r_2(K)}(1 + 1/\log|d|)^{n+1}W(K)$.

In particular for $|d| \geq 5$

$$\frac{h(K)R(K)}{W(K)} < |d|\log^{n-1}|d| .$$

Proof. See Lavrik [20].

PROPOSITION 20. If $n = [K:Q] \geq 2$ and $d = \mathrm{disc}(K)$ then,

$$h(K) \leq \frac{1}{2^{n-1}(n-1)!} \log^{n-1}|d| + b|d|\log^{n-2}|d|$$

where b depends only on n.

Proof. See Landau [17, pp. 95 and 91].

PROPOSITION 21. Let $[K:Q] = n$ and $d = \mathrm{disc}(K)$, then $\zeta_K(s)$ is regular for $\mathrm{Re}(s) > 1 - 1/n$ except for a simple pole at $s = 1$ with residue

$$\frac{2^{r_1(K)}(2\pi)^{r_2(K)}R(K)h(K)}{W(K)|d|^{\frac{1}{2}}} .$$

Proof. See Lang [19, p. 161].

As usual, we shall let $s = \sigma + it$.

PROPOSITION 22. Let $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series with $a_i \geq 0$ which is regular for $\sigma > \eta > 0$, except for a simple pole at $s = \eta$ with residue r and assume further that for we have $f(s) \ll t^k$ for some fixed k. Then,

$$\sum_{n \leq X} a_n = \frac{r}{\eta} X + o(X).$$

Proof. See Landau [18, p. 874].

The narrow class group of K is defined to be the quotient of the group of ideals modulo the group of totally positive principal ideals.

PROPOSITION 23. Let K be a quadratic field of discriminant d. Then the 2 - rank of the narrow class group of K is $\omega(d) - 1$, where $\omega(d)$ is the number of distinct prime factors of d.

Proof. See Narkiewitz [21, p. 394].

PROPOSITION 24. Let K be a quadratic field and let $h^+(K)$ denote the narrow class number of K. Then $h^+(K) = h(K)$ unless K has positive discriminant and the fundamental unit of K has

norm 1 . In this case $h^+(K) = 2h(K)$.

Proof. See Narkiewitz [21, p. 107].

CHAPTER THREE

QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS SYMMETRIC GALOIS GROUP

In this chapter we shall prove

THEOREM 1. $$\lim_{X\to\infty} \frac{N_4^+(X,S_4)}{X} \geq [4608\zeta(3)]^{-1}$$
$$\lim_{X\to\infty} \frac{N_4^-(X,S_4)}{X} \geq [1536\zeta(3)]^{-1}$$

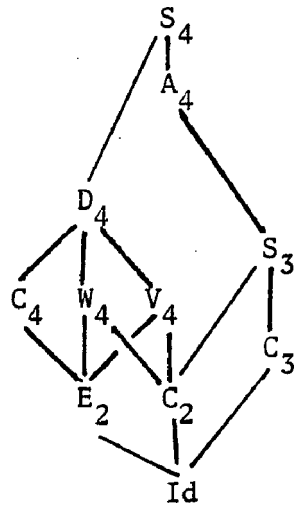
and

THEOREM 2. $$N_4(X,S_4) \ll X^{3/2}\log^4 X.$$

The proofs of these results will require several lemmas and preliminaries.

It follows from elementary group theory that a portion of the lattice of subgroups of S_4 is as follows:

(11)



where $A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

$D_4 = \{1, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}$

$S_3 = \{1, (12), (13), (23), (123), (132)\}$

$C_4 = \{1, (1243), (1342), (14)(23)\}$

$W_4 = \{1, (14), (23), (14)(23)\}$

$V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$

$$E_2 = \{1, (14)(23)\}$$

$$C_2 = \{1, (14)\}.$$

Remark. The complete lattice can be obtained by observing that D_4, C_4, W_4 and E_2 each have three conjugate subgroups; S_3 and C_3 each have four conjugate subgroups; C_2 has six conjugate subgroups; and A_4 and V_4 are normal subgroups.

If we let $K_{24} \varepsilon H(S_4)$, then, via Galois theory, we have the following correspondence between subgroups of S_4 and subfields of K_{24}:

$$\begin{array}{llll} & K_{24} \leftrightarrow \text{Identity} & K_4 \leftrightarrow S_3 \\ (12) & H_6 \leftrightarrow V_4 & K_3 \leftrightarrow D_4 \\ & K_6 \leftrightarrow W_4 & Q \leftrightarrow S_4 \end{array}$$

where the subscript on the field indicates the degree of the field over Q.

It follows from (11) that K_3 is a non-cyclic cubic field with normal closure H_6; and K_4 is a non-normal quartic field with normal closure K_{24}, i.e. $K_4 \varepsilon H(S_4)$.

Let $d_6 = \text{disc}(K_6)$

$d_4 = \text{disc}(K_4)$

$d_3 = \text{disc}(K_3)$.

LEMMA 1. $d_6 = d_3 d_4$.

Proof. Let χ_1, χ_2, χ_3, χ_4, χ_5 be the simple characters of S_4, the number of which is equal to the number of conjugacy classes on S_4, with χ_1 the principal character, and let ψ_3, ψ_4, ψ_6, resp.

be the characters on S_4 induced by the principal characters on D_4, S_3, V_4, resp.

The character table for S_4 is as follows (see Heilbronn [13, pp. 232-239] and Lang [19, p. 236]).

Conjugacy classes	χ_1	χ_2	χ_3	χ_4	χ_5	ψ_3	ψ_6	ψ_4
Identity	1	1	2	3	3	3	6	4
(12)(34)	1	1	2	-1	-1	3	2	0
(123)	1	1	-1	0	0	0	0	1
(12)	1	-1	0	1	-1	1	2	2
(1234)	1	-1	0	-1	1	1	0	0

It follows from the table that

$$\chi_1 + \psi_6 = \psi_3 + \psi_4. \tag{13}$$

By Proposition 17 b) and e), the L - functions associated with χ_1, ψ_6, ψ_3, ψ_4, resp., are the Dedekind zeta functions $\zeta(s)$, $\zeta_{K_6}(s)$, $\zeta_{K_3}(s)$, $\zeta_{K_4}(s)$ for the fields Q, K_6, K_3, K_4 resp. By Proposition 17 b) and (13), it follows that

$$\zeta(s)\zeta_{K_6}(s) = \zeta_{K_3}(s)\zeta_{K_4}(s) \quad \text{for all } s \in \mathbb{C}.$$

Proposition 18 implies that $d_6 = d_3 d_4$.

LEMMA 2. $d_3 d_4 > 0$.

Proof. Let $K_4 = Q(\theta_1)$, and let θ_1, θ_2, θ_3, θ_4 denote the conjugates of θ_1 over Q. Since K_3 is the fixed field of D_4 (see (11) and (12)), it can be generated over Q by the element

$\phi_1 = \theta_1\theta_4 + \theta_2\theta_3$. The conjugates of ϕ_1 are $\phi_2 = \theta_1\theta_2 + \theta_3\theta_4$ and $\phi_3 = \theta_1\theta_3 + \theta_2\theta_4$.

We have three cases depending on the number of real and complex infinite primes there are in K_4.

a) $r_1(K_4) = 4$ and $r_2(K_4) = 0$. Therefore, θ_1, θ_2, θ_3, θ_4 are real, and so ϕ_1 and its conjugates are real; hence $r_1(K_3) = 3$ and $r_2(K_3) = 0$.

b) $r_1(K_4) = 0$ and $r_2(K_4) = 2$. Without loss of generality, we may assume that $\theta_3 = \overline{\theta}_1$ and $\theta_4 = \overline{\theta}_2$, whence $\phi_1 = \theta_1\theta_2 + \overline{\theta}_1\overline{\theta}_2$, $\phi_2 = \theta_1\overline{\theta}_2 + \overline{\theta}_1\theta_2$ and $\phi_3 = \theta_1\overline{\theta}_1 + \theta_2\overline{\theta}_2$ are real; hence $r_1(K_3) = 3$ and $r_2(K_3) = 0$.

c) $r_1(K_4) = 2$ and $r_2(K_4) = 1$. Without loss of generality, we may assume that θ_1, θ_2 are real, and that $\theta_4 = \overline{\theta}_3$. Therefore, $\phi_1 = \theta_1\theta_2 + \theta_3\overline{\theta}_3$ is real, and $\phi_2 = \theta_1\theta_3 + \theta_2\overline{\theta}_3$, $\phi_3 = \theta_1\overline{\theta}_3 + \theta_2\theta_3$ are complex conjugates; hence $r_1(K_3) = 1$ and $r_2(K_3) = 1$.

Therefore, we have the following table for the possible values of $r_1(K_4)$, $r_2(K_4)$, $r_1(K_3)$ and $r_2(K_3)$.

(14)

$r_1(K_4)$	$r_2(K_4)$	$r_1(K_3)$	$r_2(K_3)$
4	0	3	0
2	1	1	1
0	2	3	0

From this table, we see that $r_2(K_4) \equiv r_2(K_3) \pmod 2$ and therefore, by Proposition 1, $d_3d_4 > 0$.

The following three lemmas give a necessary and sufficient condition for a field to lie in $\mathcal{H}(S_4)$.

LEMMA 3. Let $K_{24} \in H(S_4)$, and let K_3, H_6, K_6 be the subfields described in the correspondence preceding Lemma 1. Then, there exists $b \in O_{K_3} \setminus \{Z \cup O_{K_3}^2\}$ such that $K_6 = K_3(b^{\frac{1}{2}})$ and $K_{24} = H_6(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$, where b_1 is a conjugate of b over Q.

Proof. K_6 contains K_3 and $[K_6:K_3] = 2$, hence $K_6 = K_3(b^{\frac{1}{2}})$ for some $b \in K_3 \setminus K_3^2$. Without loss of generality, $b \in O_{K_3}$. If $b \in Z$, then K_6 contains the field $Q(b^{\frac{1}{2}})$ and, since by (11) K_{24} contains a unique quadratic field which must correspond to A_4, this contradicts the fact that $W_4 \not\subseteq A_4$. Hence, $b \notin Z$. Let $K = H_6(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$, where b_1 is a conjugate of b over Q. Since K_{24}/Q is normal, we have $K \subseteq K_{24}$, and since $[K:H_6] = 4 = [K_{24}:H_6]$, we must have $K_{24} = K$.

LEMMA 4. Let K be a non-cyclic cubic field with normal closure H and let $b \in O_K \setminus \{Z \cup O_K^2\}$. Let $L = H(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$, where b_1 is a conjugate of b over Q. If L/Q is normal, then $Gal(L/Q) = S_4$.

Proof. Let b_2 be the third conjugate of b over Q. As $\pm b^{\frac{1}{2}}$, $\pm b_1^{\frac{1}{2}}$, $\pm b_2^{\frac{1}{2}}$ are all the conjugates of the generators of L over Q, the elements of $Gal(L/K)$ must map the set $\{b^{\frac{1}{2}}, b_1^{\frac{1}{2}}, b_2^{\frac{1}{2}}\}$ injectively into the set $\{\pm b^{\frac{1}{2}}, \pm b_1^{\frac{1}{2}}, \pm b_2^{\frac{1}{2}}\}$. We will map elements of S_4 into the set of these maps and, in this way, establish an isomorphism between S_4 and $Gal(L/K)$. Since S_4 is generated by the 2 - cycles, it suffices to define this isomorphism on the 2 - cycles, and extend by multiplicativity. The following table defines this map, indicating

for each 2 - cycle in S_4 where the set $\{b^{\frac{1}{2}}, b_1^{\frac{1}{2}}, b_2^{\frac{1}{2}}\}$ is mapped.

	(12)	(13)	(23)	(14)	(24)	(34)
$b^{\frac{1}{2}}$	$b_1^{\frac{1}{2}}$	$b_2^{\frac{1}{2}}$	$b^{\frac{1}{2}}$	$b^{\frac{1}{2}}$	$-b_2^{\frac{1}{2}}$	$-b_1^{\frac{1}{2}}$
$b_1^{\frac{1}{2}}$	$b^{\frac{1}{2}}$	$b_1^{\frac{1}{2}}$	$b_2^{\frac{1}{2}}$	$-b_2^{\frac{1}{2}}$	$b_1^{\frac{1}{2}}$	$-b^{\frac{1}{2}}$
$b_2^{\frac{1}{2}}$	$b_2^{\frac{1}{2}}$	$b^{\frac{1}{2}}$	$b_1^{\frac{1}{2}}$	$-b_1^{\frac{1}{2}}$	$-b^{\frac{1}{2}}$	$b_2^{\frac{1}{2}}$

This map was constructed as follows. Permutations of the elements $b^{\frac{1}{2}}, b_1^{\frac{1}{2}}, b_2^{\frac{1}{2}}$ in this order, correspond to the obvious elements of S_3 embedded in S_4 as permutations of the symbols 1, 2, 3. Once we fix the image of (14), the other two are determined by the fact that (14)(12)(14) = (24) and (14)(13)(14) = (34).

LEMMA 5. Let K, H, L, b, b_1, and b_2 be as in the previous lemma. Then, L/Q is normal if and only if $N_{K_3/Q}(b)$ is a square in Z.

Proof. Assume that $N_{K_3/Q}(b) = bb_1b_2 = c^2$ with $c \in Z$. Therefore,

$$b_2^{\frac{1}{2}} = \frac{c}{b^{\frac{1}{2}}b_1^{\frac{1}{2}}} . \tag{15}$$

H/Q is normal by assumption, and it follows from (15) that $Q(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})/Q$ is normal. Therefore, $L = H(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})/Q$ is normal, being the compositum of two normal fields.

Conversely, assume that L/Q is normal. By normality, $b_2^{\frac{1}{2}}$ lies in L. Therefore, it follows that $N_{K/Q}(b)^{\frac{1}{2}} = b^{\frac{1}{2}}b_1^{\frac{1}{2}}b_2^{\frac{1}{2}}$ lies in L. If $N_{K/Q}(b)$ is not a square in Z, $N_{K/Q}(b)^{\frac{1}{2}}$ generates a quadratic subfield of L, which must be the fixed field of A_4, since, by Lemma 4, $Gal(L/Q) = S_4$. So, $N_{K/Q}(b)^{\frac{1}{2}}$ must be fixed by precisely by the

elements and no others. But the element $(12) \in S_4 \setminus A_4$ corresponds, via Lemma 4, to the automorphism

$$b^{\frac{1}{2}} \to b_1^{\frac{1}{2}}$$
$$b_1^{\frac{1}{2}} \to b^{\frac{1}{2}}$$
$$b_2^{\frac{1}{2}} \to b_2^{\frac{1}{2}}$$

and this automorphism fixes $N_{K/Q}(b)^{\frac{1}{2}}$. This contradiction implies that $N_{K/Q}(b)$ is a square in Z.

LEMMA 6. Let K_3 be a non-cyclic cubic field of discriminant d_3. Then, there exists a field $K_{24} \in H(S_4)$, such that, if K_4 is any of the quartic subfields of K_{24} and $d_4 = \mathrm{disc}(K_4)$, then $|d_4| \leq 2^9 |d_3|$.

Proof. Let u be a fundamental unit of K_3 and let $K_6 = K_3(u^{\frac{1}{2}})$. It follows from Proposition 4 a), that no odd prime ideal in K_3 can ramify in K_6. Let $\mathfrak{p}$ be an even prime ideal in K_3, and assume that $\mathfrak{p}$ ramifies in K_6. If we let $\mathfrak{d} = \mathrm{disc}(K_6/K_3)$, then it follows from Proposition 3 b), that there exists ν in the range $1 \leq \nu \leq 2e_{K/Q}(\mathfrak{p})$ such that $\mathfrak{p}^{\nu+1} \| \mathfrak{d}$.

We have five cases, depending on the way in which 2 factors in K_3.

a) $2 = \mathfrak{p}$.

Here, $e_{K/Q}(\mathfrak{p}) = 1$, $f_{K/Q}(\mathfrak{p}) = 3$; hence $\nu \leq 2$ and $|N_{K/Q}(\mathfrak{p}^{\nu+1})| \leq 2^9$.

b) $2 = \mathfrak{p}^3$.

Here, $e_{K/Q}(\mathfrak{p}) = 3$, $f_{K/Q}(\mathfrak{p}) = 1$; hence $\nu \leq 6$ and $|N_{K/Q}(\mathfrak{p}^{\nu+1})| \leq 2^7$.

c) $2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Here, $e_{K_3/Q}(\mathfrak{p}_i) = 1$, $f_{K_3/Q}(\mathfrak{p}_i) = 1$; hence $\nu_i \leq 2$, and $|N_{K_3/Q}(\mathfrak{p}_i^{\nu_i+1})| \leq 2^3$.

d) $2 = \mathfrak{p}_1\mathfrak{p}_2$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 1$, $f_{K_3/Q}(\mathfrak{p}_1) = 1$; hence $\nu_1 \leq 2$, and $|N_{K_3/Q}(\mathfrak{p}_1^{\nu_1+1}) \leq 2^3$.

$e_{K_3/Q}(\mathfrak{p}_2) = 1$, $f_{K_3/Q}(\mathfrak{p}_2) = 2$; hence $\nu_2 \leq 2$, and $|N_{K_3/Q}(\mathfrak{p}_2^{\nu_2+1})| \leq 2^6$.

e) $2 = \mathfrak{p}_1\mathfrak{p}_2^2$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 1$, $f_{K_3/Q}(\mathfrak{p}_1) = 1$; hence $\nu_1 \leq 2$, and $|N_{K_3/Q}(\mathfrak{p}_1^{\nu_1+1})| \leq 2^3$.

$e_{K_3/Q}(\mathfrak{p}_2) = 2$, $f_{K_3/Q}(\mathfrak{p}_2) = 1$; hence $\nu_2 \leq 4$, and $|N_{K_3/Q}(\mathfrak{p}_2^{\nu_2+1})| \leq 2^5$.

If $\mathfrak{d}$ contains any even primes, as given by these cases, we see that

$$|N_{K_3/Q}(\mathfrak{d})| \leq 2^9. \tag{16}$$

Now, let $K_{24} = H_6(u^{\frac{1}{2}}, u_1^{\frac{1}{2}})$, where H_6 is the normal closure of K_3, and u_1 is a conjugate of u over Q. If $N_{K_3/Q}(u) = -1$, we may replace u by $-u$ and, therefore, we may assume that $N_{K_3/Q}(u) = 1$, hence a square in Z.

Lemma 5 implies that K_{24}/Q is normal, and Lemma 4 implies that $\mathrm{Gal}(K_{24}/Q) = S_4$, i.e. $K_{24} \in \mathcal{H}(S_4)$.

Let $d_4 = \mathrm{disc}(K_4)$, where K_4 is any of the quartic subfields

of K_{24} (they are all conjugate, hence they have the same discriminant), $d_6 = \mathrm{disc}(K_6)$, and $\mathfrak{d} = \mathrm{disc}(K_6/K_3)$. Lemma 1 implies that $d_6 = d_3 d_4$ and Proposition 2 implies that

$$(d_6) = (d_3)^2 N_{K_3/Q}(\mathfrak{d}).$$

Putting these together, we have

$$(d_4) = (d_3) N_{K_3/Q}(\mathfrak{d}). \tag{17}$$

and from (15) we have

$$d_4 \leq 2^9 |d_3|.$$

LEMMA 7. $N_3^+(X,S_3) = [12\zeta(3)]^{-1} X + o(X)$

$$N_3^-(X,S_3) = [4\zeta(3)]^{-1} X + o(X).$$

Proof. This is the result of Davenport and Heilbronn [6].

Proof of Theorem 1. It follows from Lemmas 6 and 2 that, for each non-cyclic cubic field K_3 of discriminant d_3, satisfying $0 < d_3 \leq 2^{-9} X$, resp. $0 > d_3 \geq -2^{-9} X$, we get a field $K_{24} \in \mathcal{H}(S_4)$, any of whose quartic subfields, K_4, has K_{24} as its normal closure, and discriminant d_4 satisfying $0 < d_4 \leq X$, resp. $0 > d_4 \geq -X$.

It follows from Lemma 7 that the number of non-cyclic cubic fields with $|d_3| \leq 2^{-9} X$ is

$$[2^9 12\zeta(3)]^{-1} X + o(X) \quad \text{if } d_3 > 0$$
$$[2^9 4\zeta(3)]^{-1} X + o(X) \quad \text{if } d_3 < 0.$$

Now, we get the same field K_{24} from each of its three cubic subfields, and each field K_{24} gives four quartic subfields. Therefore, we have

$$N_4^+(X,S_4) \leq [2^9 12\zeta(3)]^{-1} \frac{4}{3}X + o(X)$$

and

$$N_4^-(X,S_4) \leq [2^9 4\zeta(3)]^{-1} \frac{4}{3}X + o(X)$$

and the result of Theorem 1 follows.

We now turn to Theorem 2.

Let $K_4 \in \mathcal{K}_4(S_4)$, $K_{24} = \overline{K}_4$, K_3 a cubic subfield of K_{24}, K_6 the sextic subfield of K_{24} containing K_3 and corresponding, as specified in (11) and (12), to W_4, and let $\delta = \text{disc}(K_6/K_3)$. Also, let $d_3 = \text{disc}(K_3)$ and $d_4 = \text{disc}(K_4)$.

It follows from (17) and Lemma 2, that $d_4 = d_3|N_{K_3/Q}(\delta)|$. Therefore, if we let

(18) $M(K_3,X)$ denote the number of sextic fields of the form $K_6 = K_3(b^{\frac{1}{2}})$, where $b \in O_{K_3} \setminus \{Z \cup O_{K_3}^2\}$, $N_{K_3/Q}(b)$ is a square and $|N_{K_3/Q}(\text{disc}(K_6/K_3))| < X$.

it follows that

(19) $$N_4(X,S_4) \leq \frac{4}{3} \sum_{K_3} M(K_3, X/d_3)$$

where the sum rums over all non-cyclic cubic fields K_3 such that $d_3 = |\text{disc}(K_3)| \leq X$.

This follows because, for each K_6 counted in $M(K_3, X/d_3)$, we get a field K_{24} in $\mathcal{H}(S_4)$, with four quartic subfields, each of which has discriminant less than or equal to X in absolute value, and we get the same field K_{24} from each of its three cubic subfields.

The following two lemmas describe the possible ideals that can occur as $\mathrm{disc}(K_6/K_3)$.

LEMMA 8. Let K_3 be a non-cyclic cubic field, let $b \in O_{K_3} \setminus \{Z \cup O_{K_3}^2\}$ with $N_{K_3/Q}(b)$ a square in Z, and let $K_6 = K_3(b^{\frac{1}{2}})$. Then $N_{K_3/Q}(\mathrm{disc}(K_6/K_3))$ is the square of an ideal in Z.

Proof. It follows from Corollary 6 in Chapter Two, that $(b) = \mathfrak{a}^2 \mathrm{disc}(K_6/K_3)$, where $\mathfrak{a}$ is a fractional ideal in K_3. The conclusion of the lemma follows by taking norms, and by observing that, since (b) is an integral ideal, primes in the denominator of $\mathfrak{a}$ are cancelled by primes dividing $\mathrm{disc}(K_6/K_3)$.

LEMMA 9. Let K_3 and K_6 be as in Lemma 8, and let $\delta = \mathrm{disc}(K_6/K_3)$. Then δ must be of the following form:

$$\delta = \pm \prod' \mathfrak{p}_1 \mathfrak{p}_2 \prod'' \mathfrak{p}_1 \prod''' \mathfrak{p}_1 \mathfrak{p}_2$$

where $\prod'$ runs over all odd primes p dividing $N_{K_3/Q}(\delta)$ with $p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$ and the two primes in the product can be any two of these primes, $\prod''$ runs over all odd primes p dividing $N_{K_3/Q}(\delta)$ with $p = \mathfrak{p}_1 \mathfrak{p}_2$

in K_3 and $f_{K_3/Q}(\mathfrak{P}_1) = 2$, $\prod''$ runs over all odd primes p dividing $N_{K_3/Q}(\mathfrak{d})$ with $p = \mathfrak{P}_1^2\mathfrak{P}_2$ in K_3

and

$$\mathfrak{b} = \begin{cases} \mathfrak{q}_1^i \mathfrak{q}_2^j \mathfrak{q}_3^k & i,j,k = 0, 2, \text{ or } 3 \quad \text{if } 2 = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3 \text{ in } K_3 \\ \mathfrak{q}^i & i = 0, 2, \text{ or } 3 \quad \text{if } 2 = \mathfrak{q} \text{ in } K_3 \\ \mathfrak{q}^i & i = 0, 2, 4, 5, 6, \text{ or } 7 \quad \text{if } 2 = \mathfrak{q}^3 \text{ in } K_3 \\ \mathfrak{q}_1^i \mathfrak{q}_2^j & i = 0, 2, \text{ or } 3,\ j = 0, 2, 4, \text{ or } 5 \quad \text{if } 2 = \mathfrak{q}_1\mathfrak{q}_2^2 \text{ in } K_3 \\ \mathfrak{P}_1^i \mathfrak{P}_2^j & i,j = 0, 2, \text{ or } 3 \quad \text{if } 2 = \mathfrak{P}_1\mathfrak{P}_2 \text{ in } K_3 \end{cases}$$

with $N_{K_3/Q}(\mathfrak{b})$ = a square of an ideal in Z.

Proof. K_6 is a quadratic, hence Abelian, extension of K_3, of conductor $\mathfrak{d}$, hence, by Proposition 15, conductor(K_6/K_3) = disc(K_6/K_3). Therefore, K_6 can be viewed as a subfield of the ray class field (mod $\mathfrak{d}$) of K_3 and, therefore, corresponds, via the isomorphism between a group and its character group, to a quadratic ray class character of conductor $\mathfrak{d}$. By Proposition 12, such a character can be expressed as a product of a quadratic character on the class group of K_3, a character of signature, and a primitive quadratic character on $G(\mathfrak{d})$. Primitivity follows from the fact that a character on $G(\mathfrak{d})$ is primitive modulo its conductor.

It follows from Proposition 7, that $\mathfrak{d}$ must be of the form

$$\mathfrak{d} = \mathfrak{q}_1^{a_1}\mathfrak{q}_2^{a_2}\mathfrak{q}_3^{a_3}\mathfrak{P}_1 \cdots \mathfrak{P}_r \tag{20}$$

where the $\mathfrak{P}_i$'s are distinct odd prime ideals in K_3 and the $\mathfrak{q}_i$'s are distinct even primes in K_3 with the a_i's

integers satisfying $0 \leq a_i \leq 1 + 2e_{K_3/Q}(\mathfrak{p}_i)$.

If $\mathfrak{P}$ is an odd prime, then, by Proposition 8, $G(\mathfrak{P})$ is cyclic and $\phi(\mathfrak{P})$ is even; therefore $G(\mathfrak{P})$ has a unique quadratic character.

We have five cases, depending on how 2 factors in K_3.

a) $2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Here, $e_{K_3/Q}(\mathfrak{p}_i) = 1$; hence $0 \leq a_i \leq 3$. The only case ruled out is $a_i = 1$, since $\phi(\mathfrak{p}_i) = 1$, and so $G(\mathfrak{p}_i)$ has no primitive quadratic characters.

b) $2 = \mathfrak{p}_1$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 1$; hence $0 \leq a_1 \leq 3$. As in a), the only case ruled out is $a_1 = 1$, since $\phi(\mathfrak{p}_1) = 7$.

c) $2 = \mathfrak{p}_1^3$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 3$; hence $0 \leq a_1 \leq 7$. As in a), the case $a_1 = 1$ is ruled out since $\phi(\mathfrak{p}_1) = 1$. By Proposition 8, $G(\mathfrak{p}_1^2)$ and $G(\mathfrak{p}_1^3)$ are cyclic; hence $G(\mathfrak{p}_1^3)$ has a unique non-trivial quadratic character which must come from the unique non-trivial quadratic character on $G(\mathfrak{p}_1^2)$. Therefore, $G(\mathfrak{p}_1^3)$ has no primitive quadratic characters, and we can rule out $a_1 = 3$. In this case, and those following, the cases we cannot rule out are because there exists an Abelian group of the correct order with a primitive quadratic character. Nothing is gained, at this point, by enumerating the large number of cases, in that we will not need to know precisely how many cases actually occur.

d) $2 = \mathfrak{p}_1\mathfrak{p}_2^2$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 1$; hence $0 \leq a_1 \leq 3$ and this is case a),

while $e_{K_3/Q}(\mathfrak{p}_2) = 2$; hence $0 \le a_2 \le 5$, and these are covered in case c).

e) $2 = \mathfrak{p}_1\mathfrak{p}_2$ with $f_{K_3/Q}(\mathfrak{p}_2) = 2$.

Here, $e_{K_3/Q}(\mathfrak{p}_1) = 1$; hence $0 \le a_1 \le 3$, and this is case a), while $e_{K_3/Q}(\mathfrak{p}_2) = 1$; hence $0 \le a_2 \le 3$, and the only case ruled out is $a_2 = 1$ since $\phi(\mathfrak{p}_2) = 3$.

Now, by Lemma 8, $N_{K_3/Q}(\delta)$ is the square of an ideal in Z, and so each prime power component of $N_{K_3/Q}(\delta)$ must be a square. The terms listed in the statement of the lemma are the only possibilities satisfying the above considerations, equation (20) and whose norm is a square.

In order to evaluate $M(K_3,X)$, we must now determine, for a given ideal δ of the form specified in Lemma 9, how many sextic fields K_6 containing K_3 there are with $\mathrm{disc}(K_6/K_3) = \delta$, and $|N_{K_3/Q}(\delta)| < X$. This is provided by the next three lemmas.

LEMMA 10. Let K_3 be a non-cyclic cubic field of discriminant d_3, and let δ be an ideal in K_3 of the form specified in Lemma 9. Then, there exists a constant $D(K_3)$, bounded independent of K_3, such that, if $B(X)$ is the number of primitive quadratic characters on $G(\delta)$, with $|N_{K_3/Q}(\delta)| \le X$, then

$$B(X) \sim \frac{D(K_3)R(K_3)h(K_3)}{|d_3|^{\frac{1}{2}}W(K_3)} X^{\frac{1}{2}}.$$

Proof. Let $h(n)$ be the number of primitive quadratic characters on $G(\mathfrak{d})$, with $|N_{K_3/Q}(\mathfrak{d})| = n$. Then,

$$B(X) = \sum_{n \leq X} h(n).$$

Let $f(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$. We proceed to construct the Euler product for $f(s)$.

Let p be an odd prime dividing $N_{K_3/Q}(\mathfrak{d})$. By Lemma 9, we have three cases, depending on the way p factors in K_3.

a) $p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$. Here, there are three ways of choosing $\mathfrak{p}_1 \mathfrak{p}_2$ to divide $\mathfrak{d}$ and we have $|N_{K_3/Q}(\mathfrak{p}_1 \mathfrak{p}_2)| = p^2$. Hence, the contribution of these primes to the Euler product is $\frac{3}{p^{2s}}$.

b) $p = \mathfrak{p}_1 \mathfrak{p}_2$. Here, there is only one way of choosing $\mathfrak{p}_1$ with $f_{K_3/Q}(\mathfrak{p}_1) = 2$ to divide $\mathfrak{d}$ and we have $|N_{K_3/Q}(\mathfrak{p}_1)| = p^2$. Hence, the contribution to the Euler product is $\frac{1}{p^{2s}}$.

c) $p = \mathfrak{p}_1^2 \mathfrak{p}_2$. Here, there is only one way of choosing $\mathfrak{p}_1 \mathfrak{p}_2$ to divide $\mathfrak{d}$ and we have $|N_{K_3/Q}(\mathfrak{p}_1 \mathfrak{p}_2)| = p^2$. Hence, the contribution to the Euler product is $\frac{1}{p^{2s}}$.

The even primes, being finite in number, each occurring to a bounded power by Lemma 9, and, hence, having a finite number of quadratic characters, contribute a factor $k(s)$ to the Euler product which is regular, non-zero and bound at $s = \frac{1}{2}$, independent of K_3. Therefore, we have

$$f(s) = k(s) \prod\nolimits' \left[1 + \frac{3}{p^{2s}}\right] \prod\nolimits'' \left[1 + \frac{1}{p^{2s}}\right] \prod\nolimits''' \left[1 + \frac{1}{p^{2s}}\right]$$

where $\prod'$ runs over all odd primes p such that $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in K_3, $\prod''$ runs over all odd primes p such that $p = \mathfrak{p}_1\mathfrak{p}_2$ in K_3, $\prod'''$ runs over all odd primes p such that $p = \mathfrak{p}_1^2\mathfrak{p}_2$ in K_3.

In order to evaluate the pole at $s = \frac{1}{2}$, we consider

$$f_1(s) = \frac{\zeta_{K_3}(2s)}{\zeta_{K_3}(4s)} = j(s) \prod' \left[1 + \frac{1}{p^{2s}}\right] \prod'' \left[1 + \frac{1}{p^{2s}}\right]\left[1 + \frac{1}{p^{4s}}\right]$$

$$\prod''' \left[1 + \frac{1}{p^{2s}}\right] \prod'''' \left[1 + \frac{1}{p^{2s}}\right] \prod''''' \left[1 + \frac{1}{p^{6s}}\right]$$

where $\prod''''$ runs over all odd primes p such that $p = \mathfrak{p}^3$ in K_3, and $\prod'''''$ runs over all odd primes p such that $p = \mathfrak{p}$ in K_3 and

$$j(s) = \begin{cases} \left[1 + \frac{1}{2^s}\right]^3 & \text{if } 2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \text{ in } K_3 \\ \left[1 + \frac{1}{2^s}\right]\left[1 + \frac{1}{2^{2s}}\right] & \text{if } 2 = \mathfrak{p}_1\mathfrak{p}_2 \text{ in } K_3 \\ \left[1 + \frac{1}{2^s}\right]^2 & \text{if } 2 = \mathfrak{p}_1^2\mathfrak{p}_2 \text{ in } K_3 \\ \left[1 + \frac{1}{2^s}\right] & \text{if } 2 = \mathfrak{p}^3 \text{ in } K_3 \\ \left[1 + \frac{1}{2^{3s}}\right] & \text{if } 2 = \mathfrak{p} \text{ in } K_3. \end{cases}$$

It follows that

$$g(s) = \frac{f(s)}{f_1(s)} = \frac{k(s)}{j(2s)} \prod' \left[1 + \frac{3p^{2s}+1}{p^{6s}+3p^{4s}}\right]^{-1} \prod'' \left[1 + \frac{1}{p^{4s}}\right]^{-1}$$

$$\times \prod''' \left[1 + \frac{1}{p^{2s}}\right]^{-1} \prod'''' \left[1 + \frac{1}{p^{2s}}\right]^{-1} \prod''''' \left[1 + \frac{1}{p^{6s}}\right]^{-1}$$

and each factor is regular and non-zero at $s = \frac{1}{2}$. By Proposition 21, $\zeta_{K_3}(2s)$ has a simple pole at $s = \frac{1}{2}$, with residue $\frac{1}{2}\rho$, where

$$\rho = \frac{2^{r_1(K_3)}(2\pi)^{r_2(K_3)}R(K_3)h(K_3)}{W(K_3)|d_3|^{\frac{1}{2}}} .$$

Therefore, $f(s)$ has a simple pole at $s = \frac{1}{2}$, with residue $\frac{1}{2}g(\frac{1}{2})[\zeta_{K_3}(2)]^{-1}\rho$. The result of the lemma follows from Proposition 22, with

$$D(K_3) = \frac{k(\frac{1}{2})}{j(1)} \prod\nolimits' \left[1 + \frac{3p+1}{p^3+3p^2}\right]^{-1} \prod\nolimits'' \left[1 + \frac{1}{p^2}\right]^{-1} \prod\nolimits''' \left[1 + \frac{1}{p}\right]^{-1}$$
$$\times \prod\nolimits'''' \left[1 + \frac{1}{p}\right]^{-1} \prod\nolimits''''' \left[1 + \frac{1}{p^3}\right]^{-1} \frac{2^{r_1(K_3)}(2\pi)^{r_2(K_3)}}{\zeta_{K_3}(2)} .$$

Boundedness follows from the fact that

$$j(1) \geq 9/8$$

$$k(\tfrac{1}{2}) \ll 1 \qquad \text{(absolute constant)}$$

$$1 \leq \prod\nolimits' \left[1 + \frac{3p+1}{p^3+3p^2}\right] \leq \prod_p \left[1 + \frac{3p+1}{p^3+3p^2}\right]$$

$$1 \leq \prod\nolimits'' \left[1 + \frac{1}{p^2}\right] \leq \prod_p \left[1 + \frac{1}{p^2}\right]$$

$$1 \leq \prod\nolimits''' \left[1 + \frac{1}{p}\right]$$

$$1 \leq \prod\nolimits'''' \left[1 + \frac{1}{p}\right]$$

$$1 \leq \prod\nolimits''''' \left[1 + \frac{1}{p^3}\right] \leq \prod_p \left[1 + \frac{1}{p^3}\right]$$

$$1 \leq \zeta_{K_3}(2) \leq \prod_p \left[1 - \frac{1}{p^2}\right]^{-3}$$

$$r_1(K_3) \leq 3$$
$$r_2(K_3) \leq 1.$$

LEMMA 11. Let K_3 be a cubic field of discriminant d_3. Then, $2^{h_2(K_3)} << |d_3|^{\frac{1}{2}}$ (absolute constant), where $h_2(K_3)$ is the 2-rank of the class group of K_3.

Proof. It follows from Proposition 20, that for a cubic field K_3, $h(K_3) << d_3^{\frac{1}{2}} \log^2 d_3$ (absolute constant), where $d_3 = \text{disc}(K_3)$. Now, we have $2^{h_2(K_3)} \leq h(K_3)$, with equality occurring only when the class group is a product of groups of order 2, and, therefore, the result of the lemma follows.

LEMMA 12. Let K_3 be a non-cyclic cubic field of discriminant d_3. Then, $M(K_3,X) << X^{\frac{1}{2}}|d_3|^{\frac{1}{2}} \log^4|d_3|$ (absolute constant).

Proof. As stated in the proof of Lemma 9, each sextic field K_6, counted in $M(K_3,X)$, corresponds to a product of a quadratic character on the class group of K_3, a character of signature, and a primitive quadratic character on $G(\mathfrak{f})$, where $\mathfrak{f} = \text{disc}(K_6/K_3)$. The number of quadratic characters on the class group is $2^{h_2(K_3)}$, including the principal character, which, by Lemma 11, is $<< |d_3|^{\frac{1}{2}} \log^2|d_3|$. K_3 has at most three real infinite primes; hence there are at most 2^3 characters of signature. The number of primitive quadratic characters on $G(\mathfrak{f})$, with $|N_{K_3/Q}(\mathfrak{f})| \leq X$ is, by Lemma 10,

$$<< \frac{D(K_3)R(K_3)h(K_3)}{|d_3|^{\frac{1}{2}}W(K_3)}$$

which is $< D(K_3)\log^2|d_3|X^{\frac{1}{2}}$, by Proposition 19 and the fact that $|d_3| \geq 5$. Therefore, the result of the lemma follows.

Proof of Theorem 2. It follows from Lemma 12 and equation (19) that

$$N_4(X,S_4) \leq \sum_{K_3} M(K_3, X/d_3)$$

where the sum runs over all non-cyclic cubic fields of discriminant d_3, with $|d_3| \leq X$.

Therefore, it follows from Lemma 12, that

$$\ll \sum_{K_3} (X/d_3)^{\frac{1}{2}}|d_3|^{\frac{1}{2}}\log^4|d_3|$$

$$= X^{\frac{1}{2}} \int_{1^-}^{X} \log^4 t \, d[N_3(t,S_3)]$$

which, by Lemma 7, is

$$\ll X^{\frac{1}{2}} \int_{1}^{X} \log^4 t \, dt \qquad \text{(absolute constant)}$$

$$\ll X^{3/2}\log^4 X .$$

CHAPTER FOUR

QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS ALTERNATING GALOIS GROUP

In this chapter we shall prove

THEOREM 3. $$\lim_{X\to\infty} \frac{N_4(X,A_4)}{X^{\frac{1}{2}}} \geq \frac{11}{9\cdot 2^{7/2}} C_1 = .03 \ldots$$

where $$C_1 = \frac{3^{\frac{1}{2}}}{2\pi} \prod_{q\equiv 1} \frac{(q+2)(q-1)}{q(q+1)} = .28 \ldots$$

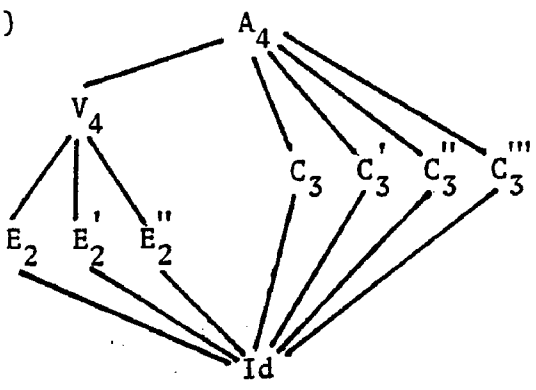
and

THEOREM 4. $N_4(X,A_4) \ll X \log^4 X$.

The proofs of these results will require several lemmas and preliminaries.

It follows from elementary group theory that the lattice of subgroups of A_4 is as follows:

(21)



where $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$

$C_3 = \{1, (123), (132)\}$

$E_2 = \{1, (12)(34)\}$

and C_3', C_3'', C_3''' are the conjugates of C_3

D_2', D_2'' are the conjugates of D_2.

V_4 is normal.

If we let $K_{12} \in \mathcal{H}(A_4)$ then, via Galois theory, we have the following correspondence between subgroups of A_4 and subfields of K_{12}.

$$K_{12} \leftrightarrow \text{Identity} \qquad K_4 \leftrightarrow C_3$$
$$K_6 \leftrightarrow E_2 \qquad K_3 \leftrightarrow V_4$$

where the subscript on the field indicates the degree of the field over Q.

It follows from (21) that K_3 is normal, hence cyclic, cubic field and K_4 is a non-normal quartic field whose normal closure is K_{12}, i.e. $K_4 \in \mathcal{K}_4(A_4)$.

Let $d_6 = \text{disc}(K_6)$

$d_4 = \text{disc}(K_4)$

$d_3 = \text{disc}(K_3)$.

LEMMA 13. $d_6 = d_3 d_4$.

Proof. Let $\chi_1, \chi_2, \chi_3, \chi_4$ be the simple characters on A_4 and let ψ_3, ψ_4, ψ_6 resp. be the characters on A_4 induced by the principal characters on V_4, C_3, E_2 resp.

The character table for A_4 is as follows (see Heilbronn [13, pp. 232 - 239] and Lang[19, p. 236]).

Conjugacy classes	χ_1	χ_2	χ_3	χ_4	ψ_3	ψ_4	ψ_6
Identity	1	1	1	3	3	4	6
(12)(34)	1	1	1	-1	3	0	2

(123)	1	ρ	ρ^2	0	0	1	0
(132)	1	ρ^2	ρ	0	0	1	0

where $\rho^3 = 1$.

It follows from the table that

$$\chi_1 + \psi_6 = \psi_3 + \psi_4.$$

By following the reasoning in the proof of Lemma 1 , we find that

$$\zeta(s)\zeta_{K_6}(s) = \zeta_{K_3}(s)\zeta_{K_4}(s) \quad \text{for all } s \in \mathbb{C},$$

where $\zeta(s)$, $\zeta_{K_6}(s)$, $\zeta_{K_3}(s)$, $\zeta_{K_4}(s)$ are the Dedekind zeta functions for the fields Q, K_6, K_3, K_4 resp., and it therefore follows from Proposition 18 that

$$d_6 = d_3 d_4.$$

LEMMA 14. If $K_4 \in \mathcal{K}_4(A_4)$ then $\mathrm{disc}(K_4) > 0$.

Proof. Let $K_{12} = \overline{K}_4$, K_3 be the cyclic cubic subfield of K_{12} and let $K_4 = Q(\theta_1)$. Let θ_1, θ_2, θ_3, θ_4 denote the conjugates of θ_1 over Q . Since K_3 is the fixed field of V_4 (see (21)), it can be generated over Q by $\phi_1 = \theta_1\theta_4 + \theta_2\theta_3$. As in the proof of Lemma 2, we are led to Table (14) . But K_3/Q is cyclic of odd degree, hence it must necessarily be a real field and, therefore the second line of the table cannot occur. It follows from the other lines of the table that $r_2(K_4)$ is even and so, by Proposition 1, $\mathrm{disc}(K_4) > 0$.

The following four lemmas give a necessary and sufficient condition for a field to lie in $\neg H(A_4)$.

LEMMA 15. Let $K_{12} \in \neg H(A_4)$ and let K_3, K_4, K_6 be the subfields of K_{12} described in the correspondence preceding Lemma 13. Then there exists $b \in O_{K_3} \setminus \{Z \cup O_{K_3}^2\}$ such that $K_6 = K_3(b^{\frac{1}{2}})$ and $K_{12} = K_3(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$, where b_1 is a conjugate of b over Q.

Proof. K_6 contains K_3 and $[K_6:K_3] = 2$, hence $K_6 = K_3(b^{\frac{1}{2}})$ for some $b \in K_3 \setminus K_3^2$. Without loss of generality we can take $b \in O_{K_3}$. Now $b \notin Z$ since K_6 has three conjugate subfields over Q and K_3/Q is normal. Since K_{12}/Q is normal, K_{12} contains the conjugates of b, say b, b_1, and b_2. Therefore, $K = K_3(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$ is a subfield of K_{12}. Since $b_1^{\frac{1}{2}} \notin K_3(b^{\frac{1}{2}})$, it follows that $[K:K_3] = 4 = [K_{12}:K_3]$ and, therefore, $K_{12} = K$.

LEMMA 16. The group A_4 is the only non-Abelian group of order 12 with a unique 2 - Sylow subgroup (necessarily of order 4).

Proof. See Rotman [22, p. 41].

LEMMA 17. Let K be a cyclic cubic field, $b \in O_K \setminus \{Z \cup O_K^2\}$ and let $L = K(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$ where b_1 is a conjugate of b over Q. If L/Q is normal, then $\mathrm{Gal}(L/Q) = A_4$.

Proof. Since K is a normal cubic subfield of L, it follows from Galois theory that $\mathrm{Gal}(L/Q)$ is a group of order 12

with a unique 2 - Sylow subgroup, since they are all conjugate. Therefore the result follows from Lemma 16.

LEMMA 18. Let K, L, b and b_1 be as specified in Lemma 17. Then L/Q is normal if and only if $N_{K/Q}(b)$ is a square in Z.

Proof. Let b_2 be the third conjugate of b over Q and assume that $N_{K/Q}(b) = bb_1b_2 = c^2$ with $c \in Z$. Therefore,

$$b_2^{\frac{1}{2}} = \frac{c}{b^{\frac{1}{2}}b_1^{\frac{1}{2}}} . \tag{22}$$

Since $b \notin Q$, we must have $K = Q(b)$ and so $L = Q(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$. It follows from (22) that $b_2^{\frac{1}{2}} \in L$ and so L/Q is normal.

Conversely, assume that $L = K(b^{\frac{1}{2}}, b_1^{\frac{1}{2}})$ and that L/Q is normal. Normality implies that $b_2^{\frac{1}{2}}$ lies in L, and, therefore, it follows that $[N_{K/Q}(b)]^{\frac{1}{2}} = b^{\frac{1}{2}}b_1^{\frac{1}{2}}b_2^{\frac{1}{2}}$ lies in L. If $N_{K/Q}(b)$ is not a square in Z then $[N_{K/Q}(b)]^{\frac{1}{2}}$ generates a quadratic subfield of L, which, by Galois theory, must correspond to a subgroup of A_4 of order 6. This contradicts the fact that A_4 has no subgroup of order six and the result follows.

LEMMA 19. Let K_3 be a cyclic cubic field of discriminant d_3. Then there exists a field $K_{12} \in \mathcal{H}(A_4)$ such that if K_4 is any of the quartic subfields of K_{12} and $d_4 = \mathrm{disc}(K_4)$, then $d_4 \leq 2^9 d_3$.

Remark. K_3 is real hence $\mathrm{disc}(K_3) > 0$ and $K_4 \in \mathcal{K}_4(A_4)$, hence, by Lemma 14, $\mathrm{disc}(K_4) > 0$.

Proof. Let u be a fundamental unit of K_3 and let $K_6 = K_3(u^{\frac{1}{2}})$. It follows from Proposition 4 a), that no odd prime ideals in K_3 can ramify in K_6. By following the argument for the even prime ideals in the proof of Lemma 6, we find that

$$|N_{K_3/Q}(\mathrm{disc}(K_6/K_3))| \leq 2^9. \tag{23}$$

Now, let $K_{12} = K_3(u^{\frac{1}{2}}, u_1^{\frac{1}{2}})$, where u_1 is a conjugate of u over Q. If $N_{K_3/Q}(u) = -1$, we may replace u by $-u$ and, therefore, we may assume that $N_{K_3/Q}(u) = 1$, hence a square in Q.

Lemma 18 implies that K_{12}/Q is normal and Lemma 17 implies that $\mathrm{Gal}(K_{12}/Q) = A_4$, i.e. $K_{12} \in H(A_4)$.

Let K_4 be any of the quartic subfields of K_{12} and let $d_4 = \mathrm{disc}(K_4)$. Also, let $d_6 = \mathrm{disc}(K_6)$ and $\mathfrak{f} = \mathrm{disc}(K_6/K_3)$. Lemma 13 implies that $d_6 = d_3 d_4$ and Proposition 2 implies that

$$(d_6) = (d_3)^2 N_{K_3/Q}(\mathfrak{f}).$$

Putting these together, we have

$$(d_4) = (d_3) N_{K_3/Q}(\mathfrak{f}) \tag{24}$$

and from (23) we have

$$d_4 \leq 2^9 d_3.$$

LEMMA 20. $N_3(X, S_3) = \frac{11}{18} C_1 X^{\frac{1}{2}} + o(X)$

where $C_1 = \frac{3^{\frac{1}{2}}}{2\pi} \prod_{q \equiv 1 \ (6)} \left[\frac{(q+2)(q-1)}{q(q+1)}\right]$.

Proof. This is the result of Harvey Cohn [4].

Proof of Theorem 3. It follows from Lemma 19 that for each cyclic cubic field K_4 of discriminant d_3 satisfying $d_3 \leq 2^{-9}X$, we get a field $K_{12} \in \mathcal{H}(A_4)$, any of whose quartic subfields K_4 lies in $\mathcal{K}_4(A_4)$, and if $d_4 = \mathrm{disc}(K_4)$, then we have $d_4 \leq X$.

It follows from Lemma 20 that the number of cyclic cubic fields with discriminant less than $2^{-9}X$ is

$$\frac{11}{18}C_1 2^{-9/2} X^{\frac{1}{2}} + o(X).$$

Now, for each field K_{12} we obtain four distinct quartic fields, hence we have

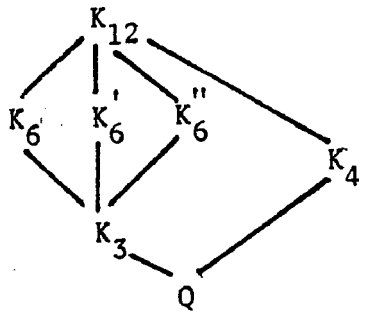
$$N_4(X,A_4) \geq C_1 4 \frac{11}{18} 2^{-9/2} X^{\frac{1}{2}} + o(X^{\frac{1}{2}}).$$

This proves Theorem 3.

We now turn to the proof of Theorem 4.

Let $K_4 \in \mathcal{K}(A_4)$, $K_{12} = \overline{K}_4$, K_3 the cubic subfield of K_{12}, and K_6 the sextic subfield of K_{12} corresponding, via Galois theory and (21), to E_2.

We have the following partial lattice of subfields of K_{12}.



where K_6' and K_6'' are the conjugates of K_6 under $\mathrm{Gal}(K_3/Q)$, K_3 is normal, while K_4 has normal closure K_{12}.

Let $d_3 = \mathrm{disc}(K_3)$

$d_4 = \mathrm{disc}(K_4)$

$\delta = \mathrm{disc}(K_6/K_3)$.

It follows from (23) and Lemma 14 that

$$d_4 = d_3 |N_{K_3/Q}(\delta)|.$$

Therefore, if we start with a cyclic cubic field K_3 of discriminant $d_3 \leq X$, then for each sextic field K_6, as described in Lemma 15, with $|N_{K_3/Q}(\mathrm{disc}(K_6/K_3)| \leq X/d_3$, we get, by Lemma 19, a field $K_{12} \in H(A_4)$ with four quartic subfields each having discriminant $\leq X$. Therefore, we have

$$N_4(X,A_4) \leq 4 \sum_{K_3} M(K_3, X/d_3) \qquad \text{(see (18))} \tag{25}$$

where the sum runs over all cyclic cubic fields of discriminant $d_3 \leq X$.

The following lemma describes the possible ideals that can occur for $\mathrm{disc}(K_6/K_3)$.

LEMMA 21. Let K_3, K_6 be as above. Then $f = \mathrm{disc}(K_6/K_3)$ must be of the following form:

$$f = \mathfrak{k} \prod \mathfrak{P}_1 \mathfrak{P}_2$$

where the product runs over all odd primes dividing $N_{K_3/Q}(f)$ with $p = \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$ in K_3 and the two prime ideals in the product may be any two of the three prime ideals dividing p.

and

$$\mathfrak{k} = \begin{cases} \mathfrak{q}^i & i = 0, 2 \text{ or } 3 \quad \text{if } 2 = \mathfrak{q} \text{ in } K_3 \\ \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3^i & i = 0, 2 \text{ or } 3 \quad \text{if } 2 = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 \text{ in } K_3. \end{cases}$$

Proof. Let f, f_1, f_2 denote the conductors, hence the discriminants, of K_6/K_3, K_6'/K_3, K_6''/K_3 resp., and let $\langle\sigma\rangle = \mathrm{Gal}(K_3/Q)$. Since K_6, K_6' and K_6'' are conjugate under $\mathrm{Gal}(K_3/Q)$ we must have

$$f_1 = f^\sigma \quad \text{and} \quad f_2 = f^{\sigma^2}. \tag{26}$$

Let χ, χ_1, χ_2 denote the ray class characters corresponding to K_6, K_6', K_6'' resp. These characters and the principal character form a group, namely the character group of $\mathrm{Gal}(K_{12}/K_3)$.

Since f is the conductor of χ, χ must be a primitive character and therefore it follows from Proposition 7 that must be of the form

$$f = \mathfrak{q}_1^{a_1} \mathfrak{q}_2^{a_2} \mathfrak{q}_3^{a_3} \mathfrak{P}_1 \cdots \mathfrak{P}_r, \tag{27}$$

where the $\mathfrak{P}_i$'s are distinct odd prime ideals in K_3, and the $\mathfrak{q}_i$'s are distinct even prime ideals in K_3 with $0 \leq 1 + 2e_{K_3/Q}(\mathfrak{q}_i)$.

We now consider separately the cases of odd and even prime

ideals dividing f.

1) Odd primes.

By (27) an odd prime $\mathfrak{P}$ can divide f_1 to at most the first power and $G(\mathfrak{P})$ has a unique primitive quadratic characctic $\chi_{\mathfrak{P}}$. If $\mathfrak{P}$ divides two of the conductors, say f and f_1, then χ will appear in the factorizations of χ and χ_1 into prime power components, and since χ is quadratic, it will not appear in the factorization of $\chi_2 = \chi\chi_1$. Therefore, by primitivity, it follows that $\mathfrak{P} \nmid f_2$. Similarly, if $\mathfrak{P} \mid f$ and $\mathfrak{P} \nmid f_1$, then χ does appear in the factorization of $\chi_2 = \chi\chi_1$ and so $\mathfrak{P} \mid f_2$.

Therefore, any odd prime ideal will divide precisely two of f, f_1, f_2 or none of them. Hence, if $\mathfrak{P}$ is an odd prime which is invariant under σ, it would, by (26), divide all three conductors if it divided any of them. Hence it follows that if $\mathfrak{P}$ divides any of the three conductors, it must restrict to a prime p in Z that splits completely in K_3. Also, each prime ideal dividing p will divide two of the three conductors and, therefore, each conductor will be divisible by precisely two of the prime divisors of p.

2) Even primes.

There are three cases depending on the way 2 factors in K_3.

a) $2 = \mathfrak{P}_1$.

Here, $e_{K_3/Q}(\mathfrak{P}_1) = 1$; hence $0 \leq a_1 \leq 3$. The only case ruled out is $a_1 = 1$, since $\phi(\mathfrak{P}_1) = 7$, implying that $G(\mathfrak{P}_1)$ has no primitive quadratic characters.

b) $2 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$.

Here, $e_{K_3/Q}(\mathfrak{p}_i) = 1$ hence $0 \leq a_i \leq 3$. As in a) the case $a_i = 1$ is ruled out since $\phi(\mathfrak{p}_i) = 1$. Now, if $\mathfrak{p}_1^i$, i = 2 or 3 , divides one of the three conductors, say f , then by (25), $\mathfrak{p}_1^{i\sigma} = \mathfrak{p}_2^i$ divides f_1 and $\mathfrak{p}_1^{i\sigma^2} = \mathfrak{p}_3^i$ divides f_2 . If the corresponding characters are $\chi_{\mathfrak{p}_j^i}$ then $\psi_i = \chi_{\mathfrak{p}_2^i}\chi_{\mathfrak{p}_3^i}$ is a character on K_6 and therefore we must have $\mathfrak{p}_2^i\mathfrak{p}_3^i$ dividing f , hence $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^i$ divides f . The argument is the same regardless of which prime we start with.

c) $2 = \mathfrak{p}_1\mathfrak{p}_2$ and $2 = \mathfrak{p}_1^2\mathfrak{p}_2$ do not occur since K_3/Q is normal.

d) $2 = \mathfrak{p}_1^3$.

The conductor of a cyclic cubic field is necessarily of the form $\prod p_i$ or $9\prod p_i$ with $p_i \equiv 1 \pmod 6$ (See Hasse [8, p. 10]). Therefore, the prime 2 cannot ramify in a cyclic cubic field and this case does not occur.

In order to evaluate $M(K_3,X)$, we must now determine, for a given ideal $\mathfrak{d}$ of the form specified in Lemma 21, how many sextic fields K_6 containing K_3 there are with $\mathrm{disc}(K_6/K_3) = \mathfrak{d}$ and $|N_{K_3/Q}(\mathfrak{d})| \leq X$. This is provided by the following two lemmas.

LEMMA 22. Let K_3 be a cyclic cubic field of discriminant d_3 and let $\mathfrak{d}$ be an ideal in K_3 of the form specified in Lemma 21. Then there exists a constant $E(K_3)$, bounded independent of K_3 , such that if C(X) is the number of primitive quadratic

characters on $G(\mathfrak{d})$ with $|N_{K_3/Q}(\mathfrak{d})| \leq X$, then

$$C(X) \sim \frac{E(K_3)R(K_3)h(K_3)}{|d_3|^{\frac{1}{2}}W(K_3)} X^{\frac{1}{2}}.$$

Proof. Let $h(n)$ be the number of primitive quadratic characters on $G(\mathfrak{d})$ with $|N_{K_3/Q}(\mathfrak{d})| = n$. Then

$$C(X) = \sum_{n \leq X} h(N).$$

Let $f(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$. We proceed to construct the Euler product for $f(s)$

Let p be an odd prime dividing $N_{K_3/Q}(\mathfrak{d})$. By Lemma 21 $p = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ in K_3 and exactly two of the three prime ideals dividing p will divide $\mathfrak{d}$, say $\mathfrak{P}_1$ and $\mathfrak{P}_2$ and we have $|N_{K_3/Q}(\mathfrak{P}_1\mathfrak{P}_2)| = p^2$. There are three ways of choosing the two prime ideals to divide $\mathfrak{d}$ hence the contribution of p to the Euler product is $\frac{3}{p^{2s}}$.

The even primes, being finite in number, each occurring to a bounded power by Lemma 21, and hence having a finite number of quadratic characters, contribute a factor $k(s)$ to the Euler product which is regular, non-zero and bounded at $s = \frac{1}{2}$.

Therefore, we have

$$f(s) = k(s) \prod [1 + \frac{3}{p^{2s}}]$$

where the product runs over all odd primes

p with $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in K_3.

In order to evaluate the pole at $s = \frac{1}{2}$ we consider

$$f_1(s) = \frac{\zeta_{K_3}(2s)}{\zeta_{K_3}(4s)} = j(2s)\prod{}' \left[1 + \frac{3}{p^{2s}}\right] \prod{}'' \left[1 + \frac{1}{p^{6s}}\right] \prod{}''' \left[1 + \frac{1}{p^{2s}}\right]$$

where $\prod'$ runs over all odd primes p such that $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in K_3, $\prod''$ runs over all odd primes p such that $p = \mathfrak{p}$ in K_3 and $\prod'''$ runs over all odd primes p such that $p = \mathfrak{p}^3$ in K_3

and

$$j(s) = \begin{cases} \left[1 + \frac{1}{2^s}\right]^3 & \text{if } 2 \text{ splits completely in } K_3 \\ \left[1 + \frac{1}{2^{3s}}\right] & \text{if } 2 \text{ is inert in } K_3. \end{cases}$$

It follows that

$$g(s) = \frac{f(s)}{f_1(s)} = \frac{k(s)}{j(2s)} \prod{}' \left[1 + \frac{3p^{2s}+1}{p^{6s}+3p^{4s}}\right]^{-1} \prod{}'' \left[1 + \frac{1}{p^{6s}}\right]^{-1} \prod{}''' \left[1 + \frac{1}{p^{2s}}\right]^{-1}$$

and each factor is regular and non-zero at $s = \frac{1}{2}$. By Proposition 21 $\zeta_{K_3}(2s)$ has a simple pole at $s = \frac{1}{2}$ with residue $\frac{1}{2}\rho$, where

$$\rho = \frac{2^{r_1(K_3)}(2\pi)^{r_2(K_3)}R(K_3)h(K_3)}{W(K_3)\, d_3^{\frac{1}{2}}}$$

$$= \frac{8R(K_3)h(K_3)}{W(K_3)\,|d_3|^{\frac{1}{2}}} \qquad \text{since } K_3 \text{ is real.}$$

Therefore, $f(s)$ has a simple pole at $s = \frac{1}{2}$ with residue $\frac{1}{2}\rho g(\frac{1}{2})[\zeta_{K_3}(2)]^{-1}$. The result of the lemma follows from Proposition 22 with

$$E(K_3) = \frac{8k(\frac{1}{2})}{\zeta_{K_3}(2)j(1)} \prod{}' [1 + \frac{3p+1}{p^3+3p^2}]^{-1} \prod{}'' [1 + \frac{1}{p^3}]^{-1} \prod{}''' [1 + \frac{1}{p}]^{-1}$$

Boundedness follows from the fact that

$$j(1) \geq 9/8$$

$$k(\tfrac{1}{2}) << 1 \quad \text{(absolute constant)}$$

$$1 \leq \prod{}' [1 + \frac{3p+1}{p^3+3p^2}] \leq \prod_p [1 + \frac{3p+1}{p^3+3p^2}]$$

$$1 \leq \prod{}'' [1 + \frac{1}{p^3}] \leq \prod_p [1 + \frac{1}{p^3}]$$

$$1 \leq \prod{}''' [1 + \frac{1}{p}] \leq \prod_p [1 + \frac{1}{p}]$$

$$1 \leq \zeta_{K_3}(2) \leq \prod_p [1 - \frac{1}{p^2}].$$

LEMMA 23. Let K_3 be a cyclic cubic field of discriminant d_3. Then $M(K_3,X) << X^{\frac{1}{2}} d_3^{\frac{1}{2}} \log^4 d_3$.

Proof. The proof is identical to that of Lemma 12 except that Lemma 10 is replaced with Lemma 22.

Proof of Theorem 4. It follows from Lemma 23 and equation (24) that

$$N_4(X,A_4) << \sum_{K_3} (X/d_3)^{\frac{1}{2}} d_3^{\frac{1}{2}} \log^4 d_3 \quad \text{(absolute constant)}$$

where the sum runs over all cyclic cubic fields K_3 of

discriminant $d_3 \leq X$. Then,

$$N_4(X,A_4) = \int_{1^-}^{X} (X/t)^{\frac{1}{2}} t^{\frac{1}{2}} \log^4 t \; d[N_3(t,C_3)]$$

which, by Lemma 20, is

$$\ll \int_{1^-}^{X} (X/t)^{\frac{1}{2}} t^{\frac{1}{2}} \log^4 t \; d(t^{\frac{1}{2}}) \quad \text{(absolute constant)}$$

$$= \tfrac{1}{2}X \int_{1}^{X} t^{-\frac{1}{2}} \log^4 t \; dt$$

$$\ll X \log^4 X \quad \text{(absolute constant)}.$$

CHAPTER FIVE

QUARTIC FIELDS WHOSE NORMAL CLOSURE HAS DIHEDRAL GALOIS GROUP

In this chapter we shall prove

THEOREM 5. There exists a constant C_2 such that

$$\overline{\lim_{X\to\infty}} \frac{N_4(X,D_4)}{X} \leq C_2.$$

and

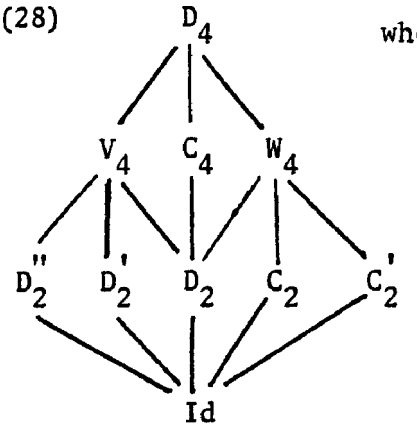
THEOREM 6. There exists a constant C_3 such that

$$\underline{\lim_{X\to\infty}} \frac{N_4(X,D_4)}{X} \geq C_3.$$

The proofs will require a series of lemmas and preliminaries.

It follows from elementary group theory that the lattice of subgroups of D_4 is as follows:

(28)



where $D_4 = \{1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$

$V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$

$C_4 = \{1, (12)(34), (1324), (1423)\}$

$W_4 = \{1, (12), (34), (12)(34)\}$

$D_2 = \{1, (12)(34)\}$

$D_2' = \{1, (13)(24)\}$

$D_2'' = \{1, (14)(23)\}$

$$C_2 = \{1, (12)\}$$
$$C_2' = \{1, (34)\}.$$

Let $K_4 \in \mathcal{K}_4(D_4)$. The field K_4 has a unique quadratic subfield; otherwise it would lie in $\mathcal{K}_4(KL_4)$. Let K_2 be this subfield. Let $d_2 = \mathrm{disc}(K_2)$ and $d_4 = \mathrm{disc}(K_4)$. Proposition 2 implies that

$$(29) \qquad (d_4) = (d_2)^2 N_{K_2/Q}(\mathrm{disc}(K_4/K_2))$$

therefore, if we let $L(K_2,X)$ denote the number of quartic fields containing K_2, whose normal closure has Galois group D_4 and such that $|N_{K_2/Q}(\mathrm{disc}(K_4/K_2))| \leq X$, it follows that

$$(30) \qquad N_4(X,D_4) \leq \sum_{K_2} L(K_2, X/d_2^2)$$

where the sum runs over all quadratic fields K_2 with discriminant d_2 satisfying $|d_2| \leq X$.

LEMMA 24. Let $K_4 \in \mathcal{K}_4(D_4)$, K its quadratic subfield and let $\delta = \mathrm{disc}(K_4/K_2)$. Then δ must be of the following form:

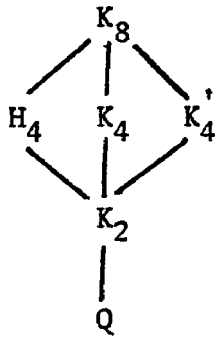
$$\delta = \alpha \prod' \mathfrak{p}_1 \prod' \mathfrak{p}_1 \mathfrak{p}_2 \prod'' \mathfrak{p} \prod''' \mathfrak{p}$$

where $\prod'$ runs over all odd primes p dividing $N_{K_3/Q}(\delta)$ with $p = \mathfrak{p}_1 \mathfrak{p}_2$ in K_2, $\prod''$ runs over all odd primes p dividing $N_{K_3/Q}(\delta)$ with $p = \mathfrak{p}$ in K_2, $\prod'''$ runs over all odd primes p dividing $N_{K_3/Q}(\delta)$ with $p = \mathfrak{p}^2$ in K_2, and the first two products are relatively prime.

and

$$\mathfrak{a} = \begin{cases} \mathfrak{p}_1^i \mathfrak{p}_2^j & i,j = 0, 2 \text{ or } 3 \quad \text{if } 2 = \mathfrak{p}_1 \mathfrak{p}_2 \text{ in } K_2 \\ \mathfrak{q}^i & i = 0, 2 \text{ or } 3 \quad \text{if } 2 = \mathfrak{p} \text{ in } K_2 \\ \mathfrak{p}^i & i = 0, 2, 4 \text{ or } 5 \quad \text{if } 2 = \mathfrak{q}^2 \text{ in } K_2. \end{cases}$$

Proof. Let $K_8 = \overline{K}_4$. It follows from (28) that K_4 and its conjugate field K_4' correspond to either D_2', D_2'' or C_2, C_2' and K_2 must correspond to V_4 or W_4. If, in either case, we let H_4 correspond to D_2, we have the following partial lattice of subfields of K_8



where H_4 is a normal field with Klein four Galois group and $\mathrm{Gal}(K_8/K_2)$ = Klein four group.

K_8 is an Abelian extension of K_2 hence it lies in the ray class field (mod f), where f = conductor(K_8/K_2). Therefore, H_4, K_4, K_4' each correspond to quadratic ray class characters (mod f) χ_{H_4}, χ_{K_4}, $\chi_{K_4'}$ resp. and, together with the principal character, these characters form a group, namely the character group of $\mathrm{Gal}(K_8/K_2)$

Let $\langle\sigma\rangle = \mathrm{Gal}(K_2/Q)$, and let f_1, f_2, f_3 denote the conductors, hence discriminants, of H_4/K_2, K_4/K_2, K_4'/K_2 resp. H_4/Q is normal, hence $f_1^\sigma = f_1$ and, since $K_4^\sigma = K_4'$ it follows that $f_2^\sigma = f_3$. It follows from Proposition 7 that since the quadratic

characters are primitive modulo their conductors that the conductors must be of the form

$$f_i = \mathfrak{q}_1^{a_1} \mathfrak{q}_2^{a_2} \mathfrak{p}_1 \cdots \mathfrak{p}_{r_i}$$

where the $\mathfrak{p}_j$'s are distinct odd prime ideals in K_2 and the $\mathfrak{q}_j$'s are distinct even primes in K_2 with the a_j's integers satisfying $0 \leq a_j \leq 1 + 2e_{K_2/Q}(\mathfrak{q}_j)$. From the group structure, using the same reasoning as in the proof of Lemma 21, odd primes will divide precisely two of the three conductors if they divide any of them.

Let $\mathfrak{p}$ be an odd prime ideal dividing f_1. Therefore, $\mathfrak{p}$ must divide precisely one of f_2 and f_3, say $\mathfrak{p} | f_2$ and $\mathfrak{p} \nmid f_3$. It follows that $\mathfrak{p}^\sigma | f_2^\sigma = f_3$ and $\mathfrak{p}^\sigma \nmid f_2$. So, $\mathfrak{p}^\sigma \neq \mathfrak{p}$ and $\mathfrak{p}^\sigma | f_1$; therefore $p = \mathfrak{p}\mathfrak{p}^\sigma$ divides f_1. Also, f_2 may contain odd factors of the type $p = \mathfrak{p}\mathfrak{p}^\sigma$, p if p is inert in K_2, and $\mathfrak{p}$ if $p = \mathfrak{p}^2$.

For the even primes we have three cases depending on the way the prime 2 factors in K_2.

a) $2 = \mathfrak{q}_1 \mathfrak{q}_2$.

Here, $e_{K_2/Q}(\mathfrak{q}_i) = 1$; hence $0 \leq a_i \leq 3$. The only case ruled out is $a_i = 1$ since $\phi(\mathfrak{q}_i) = 1$ implying that $G(\mathfrak{q}_i)$ has no primitive quadratic characters.

b) $2 = \mathfrak{q}_1^2$.

Here, $e_{K_2/Q}(\mathfrak{q}_1) = 1$; hence $0 \leq a_1 \leq 3$. As in a) the only case ruled out is $a_1 = 1$.

c) $2 = \mathfrak{q}_1^2$.

Here, $e_{K_2/Q}(\mathfrak{q}_1) = 2$; hence $0 \leq a_1 \leq 5$. As in a) the case $a_1 = 1$ is ruled out since $\phi(\mathfrak{q}_1) = 3$. By Proposition 8 $G(\mathfrak{q}_1^2)$ and $G(\mathfrak{q}_1^3)$ are cyclic, hence $G(\mathfrak{q}_1^3)$ has a unique non-trivial quadratic character which must come from the unique non-trivial quadratic character on $G(\mathfrak{q}_1^2)$, therefore is not primitive. The cases $a_1 = 4$ or 5 cannot be ruled out because there are Abelian group of the correct order in these cases that have primitive quadratic characters.

Therefore the cases are those listed in the statement of the lemma with $\mathfrak{f} = \mathfrak{f}_2$.

LEMMA 25. Let K_2 be a quadratic field of discriminant d_3 and let $\mathfrak{f}$ be an ideal in K_2 of the form specified in Lemma 24. Then there exists a constant $F(K_2)$, bounded independant of K_2, such that if $D(X)$ is the number of primitive quadratic characters on $G(\mathfrak{f})$ with $|N_{K_2/Q}(\mathfrak{f})| \leq X$, then

$$D(X) \sim \frac{F(K_2)R(K_2)h(K_2)}{W(K_2)|d_2|^{\frac{1}{2}}} X.$$

Proof. Let $h(n)$ be the number of primitive quadratic characters on $G(\mathfrak{f})$ with $|N_{K_2/Q}(\mathfrak{f})| = n$. Then

$$D(X) = \sum_{n \leq X} \frac{h(n)}{n^s} .$$

Let $f(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$. We proceed to construct the Euler product

for $f(s)$.

Let p be an odd prime. We have three cases depending on the way p factors in K_2.

a) $p = \mathfrak{P}_1 \mathfrak{P}_2$.

Since $|N_{K_2/Q}(\mathfrak{P}_i)| = p$ it follows that each of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ contribute $\frac{1}{p^s}$ to the Euler product since $G(\mathfrak{P}_i)$ has a unique primitive quadratic character. Since $|N_{K_2/Q}(\mathfrak{P}_1 \mathfrak{P}_2)| = p^2$, it follows that $\mathfrak{P}_1 \mathfrak{P}_2$ will contribute $\frac{1}{p^{2s}}$.

b) $p = \mathfrak{P}_1$.

In this case $\mathfrak{P}_1$ contributes $\frac{1}{p^{2s}}$ since $|N_{K_2/Q}(\mathfrak{P}_1)| = p^2$.

c) $p = \mathfrak{P}_1^2$.

In this case $\mathfrak{P}_1$ contributes $\frac{1}{p^s}$ since $|N_{K_2/Q}(\mathfrak{P}_1)| = p$.

The even primes, being finite in number, occurring to a bounded power by Lemma 23, and, hence, having a finite number of quadratic characters, contibute a factor $k(s)$ to the Euler product which is regular, non-zero and bounded at $s = 1$.

Therefore,

$$f(s) = k(s) \prod{}' \left[1 + \frac{2}{p^s} + \frac{1}{p^{2s}}\right] \prod{}'' \left[1 + \frac{1}{p^{2s}}\right] \prod{}''' \left[1 + \frac{1}{p^s}\right]$$

where $\prod'$ runs over all odd primes p such that $p = \mathfrak{P}_1 \mathfrak{P}_2$ in K_2, $\prod''$ runs over all odd primes p such that $p = \mathfrak{P}_1$ in K_2 and $\prod'''$ runs over all odd primes p such that $p = \mathfrak{P}_1^2$ in K_2.

$$= \frac{k(s)}{j(s)} \frac{\zeta_{K_2}(s)}{\zeta_{K_2}(2s)}$$

where

$$j(s) = \begin{cases} [1 + \frac{1}{2^s}]^2 & \text{if } 2 = \mathfrak{q}_1\mathfrak{q}_2 \text{ in } K_2 \\ [1 + \frac{1}{2^{2s}}] & \text{if } 2 = \mathfrak{q}_1 \text{ in } K_2 \\ [1 + \frac{1}{2^s}] & \text{if } 2 = \mathfrak{q}_1^2 \text{ in } K_2. \end{cases}$$

By Proposition 21 $\zeta_{K_2}(s)$ has a simple pole at $s = 1$ with residue

$$\rho = \frac{2^{r_1(K_2)}(2\pi)^{r_2(K_2)}R(K_2)h(K_2)}{W(K_2)|d_2|^{\frac{1}{2}}} .$$

Therefore $f(s)$ has a simple pole at $s = 1$ with residue $k(1)\,\rho\,[j(1)\zeta_{K_2}(2)]^{-1}$ and the result of the lemma follows from Proposition 22 with

$$F(K_2) = \frac{k(1)}{j(1)} \frac{2^{r_1(K_2)}(2\pi)^{r_2(K_2)}}{\zeta_{K_2}(2)} .$$

Boundedness follows from the fact that

$$5/4 \leq j(1) \leq 9/4$$

$$1 << k(1) << 1 \qquad \text{(absolute constants)}$$

$$0 \leq r_1(K_2) \leq 2$$

$$0 \leq r_2(K_2) \leq 1$$

$$1 \leq \zeta_{K_2}(2) \leq \prod_p [1 - \frac{1}{p^2}]^{-2} .$$

LEMMA 26. Let K_2 be a quadratic field. Then

$L(K_2,X) \ll X \log|d_2|^{2^{\omega(d_2)}}$ (absolute constant).

Proof. As in the proof of Lemma 24, a field $K_4 \in \mathcal{K}_4(D_4)$, containing K_2, corresponds to a ray class character of conductor f, where $f = \text{conductor}(K_4/K_2)$ is of the form specified in Lemma 24. By Proposition 12, such a character can be expressed as a product of a primitive character on $G(f)$, a quadratic character on the class group of K_2, and a character of signature. K_2 has at most 2 real infinite primes; hence there are at most 2^2 characters of signiture, and by Propositions 23 and 24, the number of quadratic characters on the class group, including the principal character, is either $2^{\omega(d_2)-1}$ or $2^{\omega(d_2)-2}$. By Lemma 25, the number of primitive quadratic characters on $G(f)$, with $|N_{K_2/Q}(f)| \leq X$ is

$$\ll \frac{R(K_2)h(K_2)}{W(K_2)|d_2|^{\frac{1}{2}}} X$$

which, by Proposition 19, is

$$< \log d_2$$

and the result of the lemma follows.

Proof of Theorem 5. It follows from (29) and Lemma 25 that

$$N_4(X,D_4) \ll \sum_{K_2} (X/d_2) \log|d_2|^{2^{\omega(d_2)}}$$

where the sum runs over all quadratic fields K of discriminant d_2 satisfying $|d_2| \leq X$

and therefore it follows that

$$\overline{\lim_{X\to\infty}} \frac{N_4(X,D_4)}{X} << \sum \frac{\log|d_2|}{d_2^2} 2^{\omega(d_2)}$$

the sum runs over all quadratic fields.

The result of the theorem follows from the fact that

$$\sum \frac{\log|d_2|}{d_2^2} 2^{\omega(d_2)} \leq \sum_{n=1}^{\infty} \frac{\log n}{n^2} 2^{\omega(n)} << 1 .$$

This completes the proof of Theorem 5.

LEMMA 27. Let K_2 be an imaginery quadratic field of discriminant $d_2 < -3$ with even class number and let $\mathfrak{d}$ be an ideal in K_2 of the form

$$\mathfrak{d} = \prod' \mathfrak{p}_1 \prod' \mathfrak{p} \prod'' \mathfrak{p} \prod'''$$

where the notation is that of Lemma 24. Then there exists a quadratic extension K_4 of K_2 such that $\mathrm{disc}(K_4/K_2) = \mathfrak{d}$.

Proof. Let $\mathfrak{p}$ be an odd prime ideal in K_2. By Proposition 11 3), the order of the ray class group (mod $\mathfrak{p}$) is

$$\frac{\phi(\mathfrak{p})h(K_2)}{[U:U_{\mathfrak{p}}]} .$$

Now $[U:U_{\mathfrak{p}}] = 2$ and $h(K_2)$ is even; therefore for such a prime there exists a ray class character $\chi_{\mathfrak{p}}$ of conductor $\mathfrak{p}$ which is

of order 2 . But then $\prod_{\mathfrak{p}|\mathfrak{f}} \chi_{\mathfrak{p}}$ is a ray class character of conductor $\mathfrak{f}$ which is of order 2 . If we let K_4 be the quadratic extension which corresponds to this character, then it follows from Proposition 15 that K_4 has conductor$(K_4/K_2) = \mathfrak{f}$ and $\text{disc}(K_4/K_2) = \mathfrak{f}$.

LEMMA 28. Let K_2, K_4 and $\mathfrak{f}$ be as specified in Lemma 27 and assume that a term of the form $\prod' \mathfrak{p}_1$ occurs as a factor of $\mathfrak{f}$. Then $K_4 \in \tilde{K}_4(D_4)$.

Proof. Let $\langle\sigma\rangle = \text{Gal}(K_2/Q)$. If p is a prime such that $p = \mathfrak{p}_1\mathfrak{p}_2$ in K_2 and we have $\mathfrak{p}_1$ dividing $\mathfrak{f}$ but $\mathfrak{p}_2$ not dividing $\mathfrak{f}$ then $\mathfrak{p}_1^{\sigma} = \mathfrak{p}_2$ and $\mathfrak{f}$ is not invariant under $\text{Gal}(K_2/Q)$. It follows that the ideal group (mod $\mathfrak{f}$) that K_4 corresponds to under the correspondence of class field theory is not invariant under $\text{Gal}(K_2/Q)$ and by Proposition 20 K_4/Q is not normal. Since quartic fields lying in $\tilde{K}_4(S_4)$ and $\tilde{K}_4(A_4)$ have no quadratic subfields, it follows that K_4 must lie in $\tilde{K}_4(D_4)$.

LEMMA 29. Let K_2 and $\mathfrak{f}$ be as in Lemma 28. Then there exists a constant $F(K_2)$, bounded, independent of K_2, such that if $H(X)$ is the number of primitive quadratic characters on $G(\mathfrak{f})$ with $|N_{K_2/Q}(\mathfrak{f})| \leq X$, then

$$H(X) \sim \frac{F(K_2)h(K_2)}{|d_2|^{\frac{1}{2}}} X.$$

Proof. Let $h(n)$ be the number of primitive quadratic characters on $G(\mathfrak{f})$ with $|N_{K_2/Q}(\mathfrak{f})| = n$. Then

$$H(X) = \sum_{n \le X} h(n).$$

Let $f(s) = \sum_{n=1} \frac{h(n)}{n^s}$. We proceed to construct the Euler product for $f(s)$.

In precisely the same way as in the proof of Lemma 24 we find that

$$f(s) = \prod{}' [1 + \frac{2}{p^s} + \frac{1}{p^{2s}}] \prod{}'' [1 + \frac{1}{p^{2s}}] \prod{}''' [1 + \frac{1}{p^s}]$$

$$- \prod{}' [1 + \frac{1}{p^{2s}}] \prod{}'' [1 + \frac{1}{p^{2s}}] \prod{}''' [1 + \frac{1}{p^s}]$$

where the term subtracted is to insure that a term of the form $\prod{}' \mathfrak{g}_1$ occurs as a factor of $\mathfrak{f}$.

As in the proof of Lemma the first term is

$$\frac{1}{j(s)} \frac{\zeta_{K_2}(s)}{\zeta_{K_2}(2s)}$$

and it is easy to see that the second term is

$$- \frac{\zeta(2s)}{\zeta(4s)} \prod_{p \mid d_2} [1 + \frac{p^s - 1}{p^{2s+1}}]$$

which is regular at $s = 1$.

By Proposition 21 $\zeta_{K_2}(s)$ has a simple pole at $s = 1$ with residue

$$\rho = \frac{2\pi h(K_2)}{2|d_2|^{\frac{1}{2}}}$$

since it follows from the fact that K_2 is imaginary that $W(K_2) = 2$ and $R(K_2) = 1$. Therefore the result of the lemma follows with

$$F(K_2) = \frac{\pi}{j(1)\zeta_{K_2}(2)} .$$

Boundedness follows from the fact that

$$5/4 \leq j(1) \leq 9/4$$

$$1 \leq \zeta_{K_2}(2) \leq \prod_p [1 - \frac{1}{p^2}]^{-2} .$$

LEMMA 30. Let K_2 be an imaginary quadratic field of discriminant d_2. Then $L(K_2,X) >> \frac{X}{|d_2|^{\frac{1}{2}}} 2^{\omega(d_2)}$ (absolute constant).

Proof. This follows precisely as in the proof of Lemma 26, from Lemma 29 and the fact that $R(K_2) = 1$, $W(K_2) \leq 6$ and $h(K_2) \geq 1$.

Proof of Theorem 6. It follows from Lemmas 26 and 27 and equation (28) that

$$N_4(X,D_4) \geq \sum_{K_2} L(K_2,X/d_2^2)$$

where the sum runs over all imaginary quadratic fields with even class number and discriminant d_2 satisfying $|d_2| \leq X$.

It follows from Lemma 29 that this is

$$>> \sum_{K_2} (X/|d_2|^{3/2})\ 2^{\omega(d_2)} \qquad \text{(absolute constant)}$$

and therefore it follows that

$$\lim_{X\to\infty} \frac{N_4(X,D_4)}{X} >> \sum_{K_2} |d_2|^{-3/2}\ 2^{\omega(d_2)}$$

$$>> 1 \qquad \text{(absolute constant)}\ .$$

This completes the proof of Theorem 6.

CHAPTER SIX

NORMAL QUARTIC FIELDS WITH KLEIN FOUR GALOIS GROUP

Let $A_1(X) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) \leq X \text{ and } 2 \nmid \text{disc}(K_4)\}$

$A_2(X) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) \leq X \text{ and } 2^4 \| \text{disc}(K_4)\}$

$A_3(X) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) \leq X \text{ and } 2^6 \| \text{disc}(K_4)\}$

$A_4(X) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) \leq X \text{ and } 2^8 \| \text{disc}(K_4)\}$

Remark. We show in Lemma 31 that the above cover all the possible 2 - factors of $\text{disc}(K_4)$.

In this chapter we will prove

THEOREM 7. a) $A_1(X) \sim C_4 X^{\frac{1}{2}} \log^2 X$

b) $A_2(X) \sim \frac{3}{4} C_4 X^{\frac{1}{2}} \log^2 X$

c) $A_3(X) \sim \frac{3}{8} C_4 X^{\frac{1}{2}} \log^2 X$

d) $A_4(X) \sim \frac{3}{8} C_4 X^{\frac{1}{2}} \log^2 X$

where $C_4 = \frac{18}{7\pi^6} \prod_p \left[1 - \frac{3p+1}{p^3+3p^2+3p+1}\right]$

from which it follows

THEOREM 8. $N_4(X, KL_4) \sim \frac{5}{2} C_4 X^{\frac{1}{2}} \log^2 X$ as $X \to \infty$.

In order to prove Theorem 7, we first prove the following:

THEOREM 9. Let $J(n) = \text{Card}\{K_4 \in \mathcal{H}(KL_4) \mid \text{disc}(K_4) = n\}$.

a) If n is an integer, not of the form m^2, 2^4m^2, 2^6m^2 or 2^8m^2 where m is a squarefree odd integer, then $J(n) = 0$.

b) Let m be a squarefree odd integer, then

1) $J(m^2) = \frac{1}{2}(3^{\omega(m)-1} - 1)$

2) $J(2^4m^2) = \frac{1}{2}(3^{\omega(m)} - 1)$

3) $J(2^6m^2) = \frac{1}{2}(3^{\omega(m)} - 1)$

4) $J(2^8m^2) = 3^{\omega(m)}$.

The proof will require a series of lemmas.

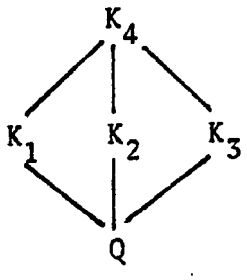
LEMMA 31. Let $K_4 \in \mathcal{H}(KL_4)$. Then

a) $\text{disc}(K_4) > 0$.

b) If p is an odd prime dividing $\text{disc}(K_4)$, then we must have $p^2 \| \text{disc}(K_4)$.

c) Either $\text{disc}(K_4)$ is odd or we have $2^\nu \| \text{disc}(K_4)$ with $\nu = 4$, 6 or 8.

Proof. Since the Klein four group has precisely three elements of order 2, it follows from Galois theory that the lattice of subfields of K_4 must be of the following form:



where $K_4 = Q(\sqrt{d_1}, \sqrt{d_2})$

$K_1 = Q(\sqrt{d_1})$

$K_2 = Q(\sqrt{d_2})$

$K_3 = Q(\sqrt{d_3})$,

where d_1 and d_2 are squarefree integers and d_3 is the squarefree part of d_1d_2.

We now have two cases to consider. Either d_1, d_2, d_3 are positive, hence $r_1(K_4) = 4$ and $r_2(K_4) = 0$; or precisely two of d_1, d_2, d_3 are negative, hence $r_1(K_4) = 0$ and $r_2(K_4) = 2$. In either case $r_2(K_4)$ is even and, therefore, by Proposition 1, $\text{disc}(K_4) > 0$. This proves a).

Any odd prime p dividing d_1 or d_2 will divide precisely two of d_1, d_2, d_3 and, therefore, will divide precisely two of $\text{disc}(K_1)$, $\text{disc}(K_2)$, $\text{disc}(K_3)$. Since K_4/Q is an Abelian extension, K_4 is a subfield of the cyclotomic field $Q(\zeta_f)$, where $\zeta_f = \exp(\frac{2\pi i}{f})$ and f is the conductor of K . The three quadratic subfields K_1, K_2, K_3 correspond to three quadratic characters on $G(f)$, χ_1, χ_2, χ_3 . It follows from Proposition 15 when applied to the quadratic subfields that $\text{conductor}(K_i) = \text{conductor}(\chi_i)$, $i = 1, 2, 3$ and when applied to K_4 that

$$\text{disc}(K_4) = \text{disc}(K_1)\text{disc}(K_2)\text{disc}(K_3). \tag{31}$$

Therefore, $p^2 \| \text{disc}(K_4)$ if $p | \text{disc}(K_4)$.

For the prime 2 we have four cases depending in the residue classes (mod 4) of d_1 and d_2.

a) $d_1 \equiv d_2 \equiv 1 \pmod 4$; hence $d_3 \equiv 1 \pmod 4$. Therefore $\text{disc}(K_1) = d_1$, $\text{disc}(K_2) = d_2$, $\text{disc}(K_3) = d_3$. It follows from (31) that $2 \nmid \text{disc}(K_4)$.

b) $d_1 \equiv 1 \pmod 4$ and $d_2 \equiv 3 \pmod 4$; hence $d_3 \equiv 3 \pmod 4$. Therefore, $\text{disc}(K_1) = d_1$, $\text{disc}(K_2) = 4d_2$ and $\text{disc}(K_3) = 4d_3$. It follows from (31) that $2^4 \| \text{disc}(K_4)$.

c) $d_1 \equiv 1 \pmod 4$ and $d_2 \equiv 2 \pmod 4$; hence $d_3 \equiv 2 \pmod 4$. Therefore, $\text{disc}(K_1) = d_1$, $\text{disc}(K_2) = 4d_2$ and $\text{disc}(K_3) = 4d_3$. It follows from (31) that $2^6 \| \text{disc}(K_4)$.

d) $d_1 \equiv 2 \pmod 4$ and $d_2 \equiv 3 \pmod 4$; hence $d_3 \equiv 2 \pmod 4$. Therefore, $\text{disc}(K_1) = 4d_1$, $\text{disc}(K_2) = 4d_2$ and $\text{disc}(K_3) = 4d_3$. It follows from (31) that $2^8 \| \text{disc}(K_4)$.

Remark. These are all the possible cases because if $d_1 \equiv 2 \pmod 4$ and $d_2 \equiv 2 \pmod 4$, then $d_3 \equiv 1 \pmod 4$, and this is case c); and if $d_1 \equiv 3 \pmod 4$ and $d_2 \equiv 3 \pmod 4$, then $d_3 \equiv 1 \pmod 4$, and this is case b).

Each field $K_4 \in H(KL_4)$ is uniquely characterized by it's three quadratic subfields. Therefore, in order to count the number of such fields K_4 with a given discriminant, it is necessary to count the number of ways a given set of primes may be placed in each of $\text{disc}(K_1)$, $\text{disc}(K_2)$, and $\text{disc}(K_3)$. To facilitate this, we need the following two combinatorial lemmas.

Let N_n denote the number of ways of grouping $2n$ objects, consisting of n objects each occurring twice, into three unordered slots, so that each slot contains no duplicates and no slot is empty. Let O_n denote the number of the above arrangements such that precisely two slots contain an odd number of objects and E_n denote the number of the above arrangements such that all slots contain an even number of objects. By abuse of language, we will also use the terms N_n, O_n, and E_n to refer to the type of the arrangement.

LEMMA 32. $N_n = \frac{1}{2}(3^{n-1} - 1)$.

Proof. The proof is by induction on n.

If $n = 1$, there are no such arrangements, hence $N_1 = 0 = \frac{1}{2}(3^0 - 1)$.

If $n = 2$, there is only one such arrangement, namely A, B, AB, hence $N_2 = 1 = \frac{1}{2}(3^1 - 1)$.

Now, assume that the result holds for $n-1$. For each arrangement of $2(n-1)$ objects of type N_{n-1}, we get three distinct arrangements of $2n$ objects of type N_n, by placing each of the pair of n^{th} objects in two of the three slots, in three ways, namely A_n, A_n, - ; A_n, - , A_n; and - , A_n, A_n. There is one more arrangement of the $2n$ objects of type N_n. This is obtained by putting each of the $2(n-1)$ objects in precisely two slots, each slot containing one each of the $n-1$ distinct objects, leaving one slot vacant. We then add the pair of n^{th} objects, one object in one of the filled slots, and the other in the vacant slot.

Therefore, $N_n = 3N_{n-1} + 1$

$= 3[\frac{1}{2}(3^{n-2} - 1)] + 1$

$= \frac{1}{2}(3^{n-1} - 1)$.

LEMMA 33. $O_n = 1/8[3^n - 2 + (-1)^n]$

$E_n = 1/8[3^{n-1} - 2 + (-1)^{n-1}]$.

Proof. It follows from the fact that $O_n + E_n = N_n = \frac{1}{2}(3^{n-1} - 1)$, that it suffices to consider only the case of O_n. The proof is by induction on n.

If $n = 1$, there are no such arrangements, hence $O_1 = 0 = 1/8(3^1 - 2 - 1)$.

If $n = 2$, there is one arrangement, namely A, B, AB, hence $O_2 = 1/8(3^2 - 2 + 1)$.

Now, assume that the result holds for $n-1$. For each arrangement of type O_{n-1}, say, odd, odd, even, we get two arrangements of type O_n, by placing one of the pair of n^{th} objects in the even slot and the other in either of the odd slots. For each arrangement of type E_{n-1}, namely, even, even, even, we get three arrangements of type O_n, by placing each of the pair of n^{th} objects in two of the three slots, in three ways, as in the proof of Lemma 32. We get one more arrangement by placing each of the $2(n-1)$ objects in precisely two slots, each slot containing one each of the $n-1$ distinct objects, leaving one slot vacant, and placing one of the pair of n^{th} objects in the vacant slot and the other in one of the filled slots.

$$\begin{aligned} \text{Therefore, } O_n &= 2O_{n-1} + 3E_{n-1} + 1 \\ &= 2O_{n-1} + 3(N_{n-1} - O_{n-1}) + 1 \\ &= 3N_{n-1} - O_{n-1} + 1 \\ &= 3/2(3^{n-2} - 1) - 1/8(3^{n-1} - 2 + (-1)^{n-1}) + 1 \\ &= 1/8(3^n - 2 + (-1)^n) \end{aligned}$$

$$\begin{aligned} \text{and } E_n &= N_n - O_n \\ &= \tfrac{1}{2}(3^{n-1} - 1) - 1/8(3^n - 2 + (-1)^n) \\ &= 1/8(3^{n-1} - 2 + (-1)^{n-1}). \end{aligned}$$

Proof of Theorem 9. Let $K_4 \in H(KL_4)$. By the proof of Lemma 31, K_4 is uniquely characterized by the three squarefree numbers

d_1, d_2, and d_3 = the squarefree part of d_1d_2. For a fixed set of primes dividing $\text{disc}(K_4)$ we get different fields for different arrangements of these primes among d_1, d_2, d_3. By Lemma 31, odd primes dividing $\text{disc}(K_4)$ will divide precisely two of d_1, d_2, and d_3, and the prime 2 occurs depending on the residue classes (mod 4) to which these numbers belong. In what follows, we take the numbers d_1, d_2, d_3 to be the "slots" in Lemmas 32 and 33, and the objects will be the primes dividing $\text{disc}(K_4)$ and the integer -1. We will let p_i denote primes $\equiv 1 \pmod 4$ and q_i denote primes $\equiv 3 \pmod 4$. Let r denote the number of primes p_i dividing $\text{disc}(K_4)$ and let t denote the number of primes q_i dividing $\text{disc}(K_4)$. We will let the $t+1^{\text{th}}$ object q_{t+1} be the integer -1, which will count as a divisor of $\text{disc}(K_4)$ which is $\equiv 3 \pmod 4$. By Lemma 31 we have four cases, and in each case we will consider separately whether each slot contains both p_i's and q_i's or not. We consider the number of ways of placing these $2(r+t+1)$ objects in these three slots. Order of an arrangement will not count and each slot must be filled as it represents the discriminant of a quadratic field.

A) $2 \nmid \text{disc}(K_4)$.

It follows from the proof of Lemma 31 that $\text{disc}(K_4)$ will be odd if and only if each of d_1, d_2, d_3 is $\equiv 1 \pmod 4$, i.e. each contains and even number of the primes q_i.

1) Assume $t \geq 1$ and $r \geq 1$.

a) Each slot contains p_i's and q_i's. Then, for each arrangement of $p_1, \ldots, p_r$ of type N_r and each arrangement of $q_1, \ldots, q_t$ of type E_t, or each arrangement of $q_1, \ldots, q_{t+1}$ of type E_{t+1}, we get six arrangements of the p_i's and q_i's,

since , if we fix the p_i's, we can place the same arrangement of the q_i's in six ways, i.e. A B C, A C B, B A C, B C A, C A B, and C B A. This gives $6N_r(E_t + E_t) = 3/2(3^{r-1} - 1)(3^{t-1} - 1)$ arrangements.

b) Three slots contain q_i's and two slots contain p_i's. Then, for each arrangement of the q_i's of type E_t or E_{t+1}, we can put all the p_i's in each of two slots in three ways. This gives $3(E_t + E_{t+1}) = 3/2(3^{t-1} - 1)$ arrangements.

c) Three slots contain p_i's and two slots contain q_i's. Then, for each arrangement of the p_i's of type N_r, can put all the q_i's in each of two slots in three ways, using -1 if and only if t is odd. This gives $3N_r = 3/2(3^{r-1} - 1)$ arrangements.

d) Two slots contain p_i's and two slots contain q_i's. Then, if we put all the p_i's in each of two slots, we can put all the q_i's in each of two slots, using -1 if and only if t is odd, in only one way so that all three slots are filled. This gives 1 arrangement.

Therefore, by a) - d), we have

(32) $$\tfrac{1}{2}(3^{r+t+1} - 1)$$

arrangements.

2) Assume $t \geq 1$ and $r = 0$. Then, we can only use arrangments of the q_i's of type E_t or E_{t+1} and this gives $E_t + E_{t+1} = \tfrac{1}{2}(3^{t-1} - 1)$ arrangements, which agrees with (32).

3) Assume $t = 0$ and $r \geq 1$. Then, we can only use arrangements of the p_i's of type N_r and this gives $\tfrac{1}{2}(3^{r-1} - 1)$ arrangements, which agrees with (32).

4) Assume $r = t = 0$. In this case there are no such arrangements, and this agrees with (32).

B) $2^4 \| \text{disc}(K_4)$.

It follows from the proof of Lemma 31 that $2^4 \| \text{disc}(K_4)$ if and only if precisely two of d_1, d_2, d_3 are $\equiv 3 \pmod 4$ and the third is $\equiv 1 \pmod 4$, i.e. two contain an odd number of q_i's and the third contains an even number.

1) Assume $t \geq 1$ and $r \geq 1$.

a) Each slot contains p_i's and q_i's. Then, for each arrangement of $p_1, \ldots, p_r$ of type N_r and each arrangement of $q_1, \ldots, q_t$ of type O_t, or each arrangement of $q_1, \ldots, q_{t+1}$ of type O_{t+1}, we get six arrangements of the p_i's and q_i's, as in A) 1) a). This gives $6N_r(O_t + O_{t+1}) = 3/2(3^{r-1} - 1)(3^t - 1)$ arrangements.

b) Three slots contain q_i's and two slots contain p_i's. Then, for each arrangement of the q_i's of type O_t or O_{t+1}, we can put all the p_i's in each of two slots in three ways. This gives $3(O_t + O_{t+1}) = 3/2(3^t - 1)$ arrangements.

c) Three slots contain p_i's and two slots contain q_i's. Then, for each arrangement of the p_i's of type N_r, we can put all the q_i's in each of two slots in three ways, using -1 if and only if t is even. This gives $3N_r = 3/2(3^{r-1} - 1)$ arrangements.

d) Two slots contain p_i's and two slots contain q_i's. Then, if we put all the p_i's in each of two slots, we can put all the q_i's in each of two slots, using -1 if and only if t is even, in only one way so that all three slots are filled. This gives

1 arrangement.

Therefore, by a) - d), we have

(33) $$\tfrac{1}{2}(3^{r+t} - 1)$$

arrangements.

2) Assume $t \geq 1$ and $r = 0$. Then, we can only use arrangements of the q_i's of type O_t or O_{t+1} and this gives $O_t + O_{t+1} = \tfrac{1}{2}(3^t - 1)$ arrangements, and this agrees with (33).

3) Assume $t = 0$ and $r \geq 1$. Then, for each arrangement of the p_i's of type N_r, we can put in the pair of -1's in three ways and, if we put all the p_i's in each of two slots, then we can put in the pair of -1's in only one way filling all the slots. This gives $3N_r + 1 = \tfrac{1}{2}(3^r - 1)$ arrangements, which agrees with (33).

4) Assume $r = t = 0$. In this case there are no such arrangements, and this agrees with (33).

C) $2^6 \| \operatorname{disc}(K_4)$.

It follows from the proof of Lemma 31 that $2^6 \| \operatorname{disc}(K_4)$ if and only if one of d_1, d_2, d_3 is $\equiv 1 \pmod 4$ and the other two are $\equiv 2 \pmod 4$, i.e. one contains an even number of q_i's and the other two contain an arbitrary number of q_i's together with the prime 2.

1) Assume $t \geq 1$ and $r \geq 1$.

a) Each slot contains p_i's and q_i's. Then, for each arrangement of $p_1, \ldots, p_r$ of type N_r and each arrangement of $q_1, \ldots, q_t$ of type N_t or each arrangement of $q_1, \ldots, q_{t+1}$ of type N_{t+1}, we get six arrangements of the p_i's and q_i's.

If the arrangement of the q_i's is of type E_t or E_{t+1}, we can put in the pair of 2's in three ways. If the arrangement of the q_i's is of type O_t or O_{t+1}, we can put in the pair of 2's in only one way, i.e. in the slots with an odd number of q_i's. This gives $6N_r[3(E_t + E_{t+1}) + (O_t + O_{t+1})] = 3(3^{r-1} - 1)(3^t - 2)$ arrangements.

b) Three slots contain q_i's and two slots contain p_i's. Then, for each arrangement of the q_i's of type E_t or E_{t+1}, we can put all the p_i's in each of two slots in three ways and we can put in the pair of 2's in three ways. For each arrangement of the q_i's of type O_t or O_{t+1}, we can put all the p_i's in each of two slots in three ways and we can put in the pair of 2's in one way. This gives $3\ 3(E_t + E_{t+1}) + (O_t + O_{t+1}) = 3(3^t - 2)$ arrangements.

c) Three slots contain p_i's and two slots contain q_i's. Then, for each arrangement of the p_i's of type N_r, we can put all the q_i's in each of two slots in three ways. Since we have one arrangement of the q_i's with -1 and one without, one of these arrangements has an even number of q_i's in which we can put the pair of 2's in three ways, and the other arrangement has an odd number of q_i's in which we can put in the pair of 2's in only one way. This gives $3N_r(3 + 1) = 6(3^{r-1} - 1)$ arrangements.

d) Two slots contain p_i's, two slots contain q_i's and all slots are filled. Then, for the one arrangement of all the p_i's in each of two slots, we have, as in c), one arrangement of the q_i's with an even number of q_i's in which we can put the

pair of 2's in three ways, and an arrangement of the q_i's with an odd number of q_i's in which we can put the pair of 2's in only one way. This gives 4 arrangements.

e) Two slots contain p_i's and q_i's and one slot contains only 2. Then, for the one arrangement of all the p_i's and q_i's in each of two slots, using -1 if and only if t is odd, we can put in the pair of 2's in one way, filling the vacant slot. This gives 1 arrangement.

Therefore, by a) - e), we have

$$\tfrac{1}{2}(3^{r+t} - 1) \tag{34}$$

arrangements.

2) Assume $t \geq 1$ and $r = 0$.

a) Each slot contains q_i's. Then, for each arrangement of the q_i's of type E_t or E_{t+1}, we can put in the pair of 2's in three ways, and for each arrangement of the q_i's of type O_t or O_{t+1}, we can put in the pair of 2's in only one way. This gives $3(E_t + E_{t+1}) + (O_t + O_{t+1}) = 3^t - 2$ arrangements.

b) Two slots contain q_i's. Then, for the one arrangement of all the q_i's in each of two slots, we can put in the pair of 2's in one way. This gives 1 arrangement.

Therefore, we have $3^t - 1$ arrangements, which agrees with (34).

3) Assume $t = 0$ and $r \geq 1$.

a) Each slot contains p_i's. Then, for each arrangement of the p_i's of type N_r, we can put in the pair of 2's in three ways. We can also put in the pair of -1's in three ways and then, since two of the slots will be $\equiv 3 \pmod 4$, we can put in the pair

of 2's in only one way. This gives $N_r(3 + 3) = 3(3^{r-1} - 1)$ arrangements.

b) Two slots contain p_i's. Then, for the arrangement of all the p_i's in each of two slots, we can put in the pair of 2's in only one way. We can also put in the pair of -1's, filling the vacant slot, and then put in the pair of 2's in only one way, i.e. in the the slots which are $\equiv 3 \pmod 4$. This gives 2 arrangements.

Therefore, we have $3^r - 1$ arrangements, which agrees with (34).

4) Assume $t = r = 0$. In this case there are no such arrangements, and this agrees with (34).

D) $2^8 \| \operatorname{disc}(K_4)$.

It follows from the proof of Lemma 31 that $2^8 \| \operatorname{disc}(K_4)$ if and only if one of d_1, d_2, d_3 is $\equiv 3 \pmod 4$ and the other two are $\equiv 2 \pmod 4$, i.e. one contains an odd number of q_i's and the other two contain an arbitrary number of q_i's, together with the prime 2.

1) Assume $t \geq 1$ and $r \geq 1$.

a) Each slot contains p_i and q_i's. We note that we can't use arrangements of the q_i's of type E_t or E_{t+1}. Then, for each arrangement of $p_1, \ldots, p_r$ of type N_r and each arrangement of $q_1, \ldots, q_t$ of type O_t, or each arrangement of $q_1, \ldots, q_{t+1}$ of type O_{t+1}, we get six arrangements of the p_i's and q_i's. In each case, two of the slots are $\equiv 3 \pmod 4$, and one is $\equiv 1 \pmod 4$; hence, we may put in the pair of 2's in two ways so that we leave one slot $\equiv 3 \pmod 4$. This gives $6 \times 2N_r(O_t + O_{t+1}) = 3(3^{r-1} - 1) \times (3^t - 1)$ arrangements.

b) Three slots contain q_i's and two slots contain

p_i's. Then, for each arrangement of the q_i's of type 0_t or 0_{t+1}, we can put all the p_i's in each of two slots in three ways and then, as in a), put in the pair of 2's in two ways. This gives $3\times2(0_t + 0_{t+1}) = 3(3^t - 1)$ arrangements.

c) Three slots contain p_i's and two slots contain q_i's. Then, for each arrangement of the p_i's of type N_r, we can put all the q_i's in each of two slots in three ways, using -1 if and only if t is even. This gives $3\times2N_r = 3(3^{r-1} - 1)$ arrangements.

d) Two slots contain p_i's, two slots contain q_i's and all slots are filled. Then, for the one arrangement of the p_i's in each of two slots, we can put in all the q_i's in each of two slots in one way so that all the slots are filled, and then we can put in the pair of 2's in two ways. This gives 2 arrangements.

e) Two slots contain p_i's and q_i's and one slot contains only 2. Then, for the arrangement of all the p_i's and q_i's in each of two slots, leaving one slot vacant and using -1 if and only if t is even, we can put in the pair of 2's in one way, filling the vacant slot. This gives 1 arrangement.

Therefore, by a) - e), we have

$$3^{r+t} \tag{35}$$

arrangements.

2) Assume $t \geq 1$ and $r = 0$.

a) Every slot contains q_i's. Then, for each arrangement of the q_i's of type 0_t or 0_{t+1}, we can put in the

the pair of 2's in two ways. This gives $2(O_t + O_{t+1}) = 3^t - 1$ arrangements.

b) Two slots contain q_i's. Then, for the one arrangement of all the q_i's in each of two slots, using -1 if and only if t is even, we can put in the pair of 2's in only one way, filling the vacant slot. This gives 1 arrangement.

Therefore, we have 3^t arrangements, which agrees with (35).

3) Assume $t = 0$ and $r \geq 1$.

a) Each slot contains p_i's. Then, for each arrangement of the p_i's of type N_r, we can put in the pair of -1's in three ways and then, we can put in the pair of 2's in two ways. This gives $3 \times 2N_r = 3(3^{r-1} - 1)$ arrangements.

b) Two slots contain p_i's. Then, for the one arrangement of all the p_i's in each of two slots, we can put in the pair of -1's in the two filled slots and then, we can put in the pair of 2's in only one way filling the vacant slot. Also, we can put in the pair of -1's filling the vacant slot and then, we can put in the pair of 2's in two ways. This gives 3 arrangements.

Therefore, we have 3^r arrangements, which agrees with (35).

4) Assume $t = r = 0$. Then, for the one arrangement of the pair of -1's in two slots, we can put in the pair of 2's in only one way so that the vacant slot is filled. This gives 1 arrangement.

This completes the proof of Theorem 9.

We need the following technical lemma in order to complete the proof of Theorem 7.

LEMMA 34. $\sum_{\substack{n\le X \\ n \text{ odd}}} \mu^2(n)3^{\omega(n)} \ll CX \log^2 X$

where $C = \frac{2}{7\zeta(2)^3} \prod_p [1 - \frac{3p+1}{p^3+3p^2+3p+1}]$.

Proof. Let $f(s) = \sum_{n=1}^{\infty} \frac{\mu^2(n)3^{\omega(n)}}{n^s} = \prod_p [1 + \frac{3}{p^s}]$.

It follows from Apostol [1, pp. 245-246] that

$$\sum_{n\le X} \mu^2(n)3^{\omega(n)} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{f(s)X^s}{s} ds .$$

Now $3^{\omega(n)} \ll n^{\varepsilon}$ for any $\varepsilon > 0$; hence it follows from Titchmarsh [25, p. 53 Lemma 3.12] that for $T = X^{1/3}$ and $c = 1 + \varepsilon$ we have

$$\sum_{n\le X} \mu^2(n)3^{\omega(n)} = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{f(s)X^s}{s} ds + O(X^{2/3+\varepsilon}).$$

To evaluate the integral in this expression we integrate around the rectangle with vertices $a \pm iT$ and $c \pm iT$, where $a = \frac{1}{2} + \delta$ for any fixed δ satisfying $0 < \delta < \frac{1}{2}$, and use the theory of residues.

A computation shows that

$$\prod_{p\neq 2} [1 + \frac{3}{p^s}] = g(s)\zeta(s)^3$$

where

$$g(s) = \zeta(2s)^{-3}\left[1 + \frac{3}{2^{2s}}\right]^{-1}\prod_{p}\left[1 - \frac{3p^{s}+1}{p^{3s}+3p^{2s}+3p^{s}+1}\right]$$

which is regular for $\sigma \geq \frac{1}{2} + \delta$ where $s = \sigma + it$.

It follows from Titchmarsh 25, p. 82 that

$$|\zeta(\tfrac{1}{2} + \delta + it)| << t^{\frac{1}{4}+\varepsilon} \quad \text{for any} \quad \varepsilon > 0.$$

Therefore, it follows that

$$\frac{1}{2\pi i}\int_{a-iT}^{a+iT}\frac{f(s)X^{s}}{s}ds \;<<\; \int_{a-iT}^{a+iT}\frac{f(s)X^{s}}{s}ds$$

$$<< \int_{-T}^{T}\frac{t^{3/4+}\; X^{\frac{1}{2}+}}{|(\frac{1}{2}+\delta)^{2}+t^{2}|^{\frac{1}{2}}}\,dt$$

$$<< X^{\frac{1}{2}+\delta}\int_{-T}^{T} t^{-3/4+\varepsilon}\,dt$$

$$<< X^{\frac{1}{2}+\delta}T^{3/4+\varepsilon}$$

$$<< X \quad \text{for the choice} \quad T = X^{1/3}.$$

It also follows from Tihmarsh [25, p. 266] that

$$\int_{a+iT}^{c+iT}\frac{f(s)X^{s}}{s}ds \;<<\; \int_{a+iT}^{c+iT}\frac{(s)^{3}X^{s}}{s}ds$$

$$<< X^{c}/T$$

$$<< X.$$

Therefore it follows that

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{f(s)X^s}{s}\,ds = \mathrm{Res}\{\frac{f(s)X^s}{s}\}\Big|_{s=1} + O(X).$$

To evaluate the residue we consider the following

$$f(s) = g(s)\ (s)^3 = \frac{g(1)}{(s-1)^3} + \ \ldots$$

$$X^s = XX^{s-1} = X[1 + (s-1)\log X + \tfrac{1}{2}(s-1)^2\log^2 X + \ \ldots\ ]$$

$$\frac{1}{s} = \frac{1}{1+(s-1)} = 1 - (s-1) + (s-1)^2 - \ \ldots$$

It follows from these expansions that the residue of $\frac{f(s)X^s}{s}$ at $s=1$ is

$$\tfrac{1}{2}g(1)X\log^2 X + O(X)$$

and the result of the lemma follows.

Proof of Theorem 7.

a) It follows from Theorem 9 and Lemma 34 that

$$A_1(X) = \sum_{\substack{m^2 \le X \\ m \text{ odd}}} J(m^2)$$

$$= \sum_{\substack{m \le X^{\frac{1}{2}} \\ m \text{ odd}}} \tfrac{1}{2}(3^{\omega(m)-1} - 1)$$

$$= \frac{1}{6}\sum_{\substack{m \le X^{\frac{1}{2}} \\ m \text{ odd}}} 3^{\omega(m)} + \frac{1}{2}\sum_{\substack{m \le X^{\frac{1}{2}} \\ m \text{ odd}}} 1$$

$$\sim \frac{C}{6} X^{\frac{1}{2}}[\log(X^{\frac{1}{2}})]^2 - \tfrac{1}{4}X^{\frac{1}{2}}$$

$$\sim \frac{C}{24} X^{\frac{1}{2}}\log^2 X$$

and the result follows with

$$C_4 = \frac{C}{24} = \frac{18}{7\pi^6} \prod_p \left[1 - \frac{3p+1}{p^3+3p^2+3p+1}\right].$$

b) As in a)

$$A_2(X) = \sum_{\substack{2^4 m^2 \leq X \\ m \text{ odd}}} J(2^4 m^2)$$

$$= \sum_{\substack{m \leq \frac{X^{\frac{1}{2}}}{4} \\ m \text{ odd}}} \tfrac{1}{2}(3^{\omega(m)} - 1)$$

$$\sim \frac{C}{2} \left(\frac{X^{\frac{1}{2}}}{4}\right)\left[\log\left(\frac{X^{\frac{1}{2}}}{4}\right)\right] - \tfrac{1}{4}\,\frac{X^{\frac{1}{2}}}{4}$$

$$\sim \frac{C}{2^5} X^{\frac{1}{2}} \log^2 X$$

and the result follows since $\frac{C}{2^5} = \frac{3}{4} C_4$.

c) As in b)

$$A_3(X) = \sum_{\substack{2^6 m^2 \leq X \\ m \text{ odd}}} J(2^6 m^2)$$

$$= \sum_{\substack{m \leq \frac{X^{\frac{1}{2}}}{8} \\ m \text{ odd}}} \tfrac{1}{2}(3^{(m)} - 1)$$

$$\sim \frac{C}{2}\left(\frac{X^{\frac{1}{2}}}{8}\right)\left[\log^2\left(\frac{X^{\frac{1}{2}}}{8}\right)\right]^2 - \tfrac{1}{4}\,\frac{X^{\frac{1}{2}}}{8}$$

$$\sim \frac{C}{2^6}\,X^{\frac{1}{2}}\log^2 X$$

and the result follows since $\frac{C}{2^6} = \frac{3}{8}\,C_4$.

d) As in b)

$$A_4(X) = \sum_{\substack{2^8 m^2 \le X \\ m \text{ odd}}} J(2^8 m^2)$$

$$= \sum_{\substack{m \le \frac{X^{\frac{1}{2}}}{16} \\ m \text{ odd}}} 3^{\omega(m)}$$

$$\sim C\left(\frac{X^{\frac{1}{2}}}{16}\right)\left[\log\left(\frac{X^{\frac{1}{2}}}{16}\right)\right]^2$$

$$\sim \frac{C}{2^6}\,X^{\frac{1}{2}}\log^2 X$$

and this completes the proof of Theorem 7.

CHAPTER SEVEN

NORMAL QUARTIC FIELDS WITH CYCLIC GALOIS GROUP

In this chapter we shall prove

THEOREM 10. $N_4(X,C_4) \sim C_5 X^{\frac{1}{2}}$ as $X \to \infty$

$$\text{where } C_5 = \frac{3}{\pi^2}\left(\frac{25}{12}\prod_{p\equiv 1 \ (4)}\left[1+\frac{2}{p^{3/2}+p^{1/2}}\right] - 3\right).$$

The proof will require several lemmas and preliminaries.

Let $K_4 \in \mathcal{H}(C_4)$ and let K_2 be its unique quadratic subfield. Let $f_{K_4} = \text{conductor}(K_4)$ and $f_{K_2} = \text{conductor}(K_2)$. Viewing $\text{Gal}(K_4/Q)$ as embedded in $(Z/f_{K_4}Z)^\times$, let χ generate the character group of $\text{Gal}(K_4/Q)$ and let $f_\chi = \text{conductor}(\chi)$.

It follows that χ is a primitive quartic character on $G(f_\chi)$ and that χ can be uniquely factored as $\chi = \chi_4\chi_2$ where χ_4 is a pure quartic character, i.e. each prime power component χ_p of χ_4 satisfies $\chi_p^4 = 1$ but $\chi_p^2 \neq 1$, and χ_2 is a quadratic character, i.e. $\chi_2^2 = 1$.

Let $f_4 = \text{conductor}(\chi_4)$ and let $f_2 = \text{conductor}(\chi_2)$. Then, $f_\chi = f_4 f_2$ (see Hasse [8, p. 27]).

LEMMA 34.
$$f_4 = \begin{cases} p_o \cdots p_n & \text{if } 2 \nmid f_4 \\ 2^4 p_1 \cdots p_n & \text{if } 2 \mid f_4 \end{cases}$$

where p_i are distinct primes $\equiv 1 \pmod 4$, and

$$\chi_4 = \chi_0\chi_1 \cdots \chi_n,$$

where each χ_i corresponds to a unique prime divisor of f_{K_4}. If p is odd then

$$\chi_i(x) = \chi_p(x) = \left(\frac{x}{\mathfrak{p}}\right)_4 \equiv x^{\frac{1}{4}(p-1)} \pmod{\mathfrak{p}} \quad \text{or} \quad \overline{\chi}_p(x)$$

where $p = \mathfrak{p}\bar{\mathfrak{p}}$ in $Q(\sqrt{p})$ and the conductor of χ_p is p. If p_0 is even then

$$\chi_i(x) = \chi_{2^4}^{(\nu)}(x) = \left(\frac{-1}{x}\right)^{\nu}\left(\frac{1-i}{x}\right)_4 = (-1)^{\nu\frac{x-1}{2}}\, i^{\frac{x^2-1}{8}}$$

where $\nu = 0$ or 1 and the conductor of $\chi_{2^4}^{(\nu)}$ is 2^4.

Proof. See Hasse [10, p. 27].

LEMMA 35.
$$f_2 = \begin{cases} q_0 \cdots q_m & \text{if } 2 \nmid f_2 \\ 2^{\lambda} q_1 \cdots q_m & \text{if } 2 \mid f_2 \end{cases}$$

where $\lambda = 2$ or 3, and q_i are distinct odd primes, prime to f_4, and

$$\psi_2 = \psi_0 \cdots \psi_n$$

where each ψ_i corresponds to a unique prime divisor of f_2. If p is odd then

$$\psi_i(x) = \psi_p(x) = \left(\frac{x}{p}\right) \equiv x^{\frac{1}{2}(p-1)} \pmod p$$

and the conductor of ψ_p is p.

If the divisor is 2^2 then

$$\psi_i(x) = \psi_{2^2}(x) = (-1)^{\frac{1}{4}(x-1)}$$

and the conductor of ψ_{2^2} is 2^2.

If the divisor if 2^3, then

$$\psi_i(x) = \psi_{2^3}(x) = \left(\frac{2}{x}\right) = (-1)^{\frac{x^2-1}{8}} \quad \text{or} \quad \psi_{2^3}(x)\psi_{2^2}(x)$$

and the conductor of ψ_{2^3} is 2^3.

Proof. See Hasse [12, p. 42].

LEMMA 36. Let $n+1$ denote the number of prime divisors of f_4. Then

a) If $2^3 \nmid f_{K_4}$, there are 2^n cyclic quartic fields of conductor f_{K_4}.

b) If $2^3 | f_{K_4}$, there are 2^{n+1} cyclic quartic fields of conductor f_{K_4}.

Proof. See Hasse [10, p. 28].

LEMMA 37. $f_{K_4} = f_\chi = f_4 f_2$

and

$$\operatorname{disc}(K_4) = \begin{cases} f_4^3 f_2^2 & \text{if } 2 \nmid f_{K_2} \\ \frac{1}{2} f_4^3 f_2^2 & \text{if } 2 | f_{K_2} \end{cases}$$

Proof. $\chi = \chi_4 \chi_2$ has conductor $p_0 p_1 \cdots p_n f_2$ or $2^4 p_1 \cdots p_n f_2$,

depending on whether or not $2|f_4$. It follows from the fact that $\chi_2^2 = 1$ that $\chi^2 = \chi_4^2$ and so we have

$$\chi^2 = \begin{cases} \chi_{p_0}^2 \chi_{p_1}^2 \cdots \chi_{p_n}^2 & \text{if } 2\nmid f_4 \\ \chi_{2^4}^2 \chi_{p_1}^2 \cdots \chi_{p_n}^2 & \text{if } 2|f_4 . \end{cases}$$

Now, $\chi_p^2(x) = (\frac{x}{p})$ is of conductor p and $\chi_{2^4}(x) = (\frac{2}{x})$ is of conductor 2^3, therefore it follows that

$$\text{conductor}(\chi^2) = \begin{cases} f_4 & \text{if } 2\nmid f_4 \\ \frac{1}{2}f_4 & \text{if } 2|f_4 . \end{cases}$$

We also have $\chi^3 = \chi_4^3\chi_2$; therefore $\text{conductor}(\chi^3) = f_4 f_2$.

Therefore, the result follows from the conductor - discriminant formula.

Proof of Theorem 10. Let $h(n)$ be the number of fields K_4 in $\mathcal{H}(C_4)$ such that $\text{disc}(K_4) = n$. It follows that

$$N_4(X, C_4) = \sum_{n \le X} h(n) .$$

Let $f(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$ and we proceed to construct the Euler product for $f(s)$.

We have two cases to consider.

a) $2\nmid f_4$. Then, by Lemma 34, f_4 contains only distinct primes $p_i \equiv 1 \pmod 4$ to the first power and, by Lemma 35, f_2 may contain any distinct odd primes dividing f_{K_4} but not dividing f_4, and

possibly 4 or 8 . Let m denote the number of prime divisors of f_4. By Lemma 36, there are 2^{m-1} cyclic quartic fields of discriminant $f_4^3 f_2^2$ unless $2^3 | f_{K_4}$, in which case there are 2^m fields. It follows that the contribution of these primes to the Euler product is

$$\frac{1}{2}\Big(\prod_{p\equiv 1 \ (4)}\Big[1 + \frac{1}{p^{2s}} + \frac{2}{p^{3s}}\Big]\Big)\Big[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}}\Big]\prod_{p\equiv 3 \ (4)}\Big[1 + \frac{1}{p^{2s}}\Big].$$

In order to insure that a quartic conductor occurs in each term we subtract

$$\frac{1}{2}\Big[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}}\Big]\prod_{p \text{ odd}}\Big[1 + \frac{1}{p^{2s}}\Big].$$

b) $2 | f_4$. Then, by Lemma 34, f_4 contains the prime 2 to the fourth power and distinct primes $p_i \equiv 1 \pmod 4$ to the first power and f_2 contains only distinct odd primes, dividing f_{K_4} but not dividing f_4 , to the first power. By Lemma 36, there are 2^m fields of discriminant $\frac{1}{2} f_4^3 f_2^2$. It follows that the contribution on these primes to the Euler product is

$$\frac{2}{16^{3s}}\prod_{p\equiv 1 \ (4)}\Big[1 + \frac{1}{p^{2s}} + \frac{2}{p^{3s}}\Big]\prod_{p\equiv 3 \ (4)}\Big[1 + \frac{1}{p^{2s}}\Big].$$

Putting a) and b) together we find that

$$f(s) = \frac{1}{2}\left[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}} + \frac{4}{16^{3s}}\right] \prod_{p\equiv 1 \ (4)} \left[1 + \frac{1}{p^{2s}} + \frac{2}{p^{3s}}\right] \prod_{p\equiv 3 \ (4)} \left[1 + \frac{1}{p^{2s}}\right]$$

$$- \left[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}}\right] \prod_{p \text{ odd}} \left[1 + \frac{1}{p^{2s}}\right] .$$

In order to evaluate the pole at $s = \frac{1}{2}$ we consider

$$g(s) = \frac{\prod_{p\equiv 1 \ (4)} \left[1 + \frac{1}{p^{2s}} + \frac{2}{p^{3s}}\right] \prod_{p\equiv 3 \ (4)} \left[1 + \frac{1}{p^{2s}}\right]}{\prod_{p}\left[1 + \frac{1}{p^{2s}}\right]}$$

$$= \left[1 + \frac{1}{2^{2s}}\right]^{-1} \prod_{p\equiv 1 \ (4)} \left[1 + \frac{2}{p^{3s}+p^{s}}\right]$$

which is regular and non-zero at $s = \frac{1}{2}$.

It follows from the fact that

$$\prod_{p}\left[1 + \frac{1}{p^{2s}}\right] = \frac{\zeta(2s)}{\zeta(4s)}$$

that

$$f(s) = \left(\frac{1}{2}\left[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}} + \frac{4}{16^{3s}}\right]g(s) - \left[1 + \frac{1}{4^{2s}} + \frac{2}{8^{2s}}\right]\right)\frac{\zeta(2s)}{\zeta(4s)} .$$

It follows that $f(s)$ has a simple pole at $s = \frac{1}{2}$ with residue

$$\left(\frac{1}{2}\left[1 + \frac{1}{4} + \frac{2}{8} + \frac{4}{64}\right]g(\tfrac{1}{2}) - \left[1 + \frac{1}{4} + \frac{2}{8}\right]\frac{1}{2\zeta(2)}\right.$$

$$= \frac{3}{\pi^2}\left[\frac{25}{24} \prod_{p\equiv 1 \ (4)} \left[1 + \frac{2}{p^{3/2}+p^{1/2}}\right] - \frac{3}{2}\right]$$

and the result follows from Proposition 22.

This completes the proof of Theorem 10.

CHAPTER EIGHT

CONCLUSIONS AND CONJECTURES

We have completely solved the problem posed in the two Abelian cases. The reason for this is that the class number of Q is 1 and, therefore, we can calculate the precise order of ray class groups. For the most part, it is this inability to make precise estimates of class numbers of fields of a given degree that limits the accuracy of the results in the other cases.

In the dihedral case, the upper bounds are of the same order of magnitude as the lower bounds. This was due to the classical result that precisely describes the 2-rank of the class group of quadratic fields, and this tells us exactly how many unramified quadratic extensions the field will have. At this point, we cannot derive the precise density of these fields because we do not know, for an arbitrary quadratic field K_2 and an ideal $\mathfrak{f}$ in K_2, whether or not the ray class group (mod $\mathfrak{f}$) is of even order. The problem lies in the units. If u is the fundamental unit of K_2, in the case that K_2 is real, then a precise knowledge of the order of u (mod $\mathfrak{f}$) is necessary for solving the problem. This is the reason that we dealt only with imaginary quadratic fields with only two units when we estimated the lower bounds.

In the cases of the symmetric and alternating groups, the problems are more difficult. Here, we are dealing with cubic fields, and there is very little known about class structure in this case. In the proof of Lemmas 12 and 23, we were forced to use the estimate of Lemma 11

for the 2-rank of the class group of a cubic field. This estimate is made under the rather crude assumption that the class group of a cubic field is a product of groups of order 2, i.e. we were forced to assume the worst possible case, although empirical evidence is that the class number of a cubic field is rarely even and, when it is, the power of 2 dividing the class number is not too large. We should be able to replace the factor of $d_3^{\frac{1}{2}}$ in Lemma 11 by a more reasonable $\log d_3$ or, at best, an absolute constant. This would remove the $X^{\frac{1}{2}}$ term in the upper bounds for the symmetric and alternating cases, and at worst, replace it with further $\log X$ terms. These log terms seem to be a result of the same problem that we encountered in the dihedral case. Given a cubic field K_3, and an ideal $\mathfrak{f}$ in K_3, we do not know if the order of the ray class group (mod $\mathfrak{f}$) is even. In the proof of Lemmas 12 and 23, we have again assumed the worst case, that the order is always even, and we get quadratic characters in all cases. Again, the problem lies with knowing the order (mod $\mathfrak{f}$) of the units. Presumably, as with the class number, we will have large factors of 3 appearing, but few factors of 2, and this would hopefully remove the log factors.

We would then be left with the conjectured asymptotic densities for these cases of CX and $CX^{\frac{1}{2}}$ resp., where the C's are constants. This would also agree with the conjecture stated in the introduction that

$$\lim_{X\to\infty} \frac{N_4(X)}{X} \quad \text{exists.}$$

If this conjecture holds, then we do have one very surprising result. The result of Gallagher, mentioned in the introduction, shows that almost all quartic polynomials will have the symmetric group S_4 as their Galois group; therefore we would have assumed that the same result would hold when counting fields by their discriminants. This is contradicted by the fact that we have proved that there are $>> X$ dihedral quartic fields. This would indicate there is a significant difference between counting polynomials and counting fields, and that there must be a large amount of collapsing, i.e. many more polynomials must correspond to the same field in the symmetric case than in the dihedral case. For whatever reason, this result is far different from the result we would have expected.

Regrettably, the general methods used in the cases of the symmetric and alternating groups will not work for fields of higher degree for the reason that the group S_n, for $n \geq 5$, contains no subgroup, except A_n, of index less than n. Therefore, there is no way of building these fields up from fields of smaller degree.

NOTATION

Z	The ring of rational integers
Q	The field of rational numbers
R	The field of real numbers
$\mathbb{C}$	The field of complex numbers
S_n	The symmetric group on n letters
A_n	The alternating group on n letters
D_n	The dihedral group of order $2n$
C_n	The cyclic group of order n
KL_4	The Klein four group
$\omega(n)$	The number of distinct prime divisors of n

Let K be an algebraic number field.

$\mathrm{disc}(K)$	The absolute discriminant of K
$h(K)$	The class number of K
$h^+(K)$	The narrow class number of K
$h_2(K)$	The 2-rank of the class group of K, i.e. the number of cyclic factors in the 2-Sylow subgroup of the class group of K
O_K	The ring of integers in K
$\overline{K}$	The normal closure of K with respect to Q
$R(K)$	The regulator of K
$W(K)$	The number of roots of unity in K
$r_1(K)$	The number of real conjugates of K
$r_2(K)$	The number of pairs of complex conjugates of K

Let $K \subseteq L$ be algebraic number fields, $\mathfrak{a}$ an ideal in K, and $\mathfrak{y}$, $\mathfrak{z}$ prime ideals in K, L resp., with $\mathfrak{z}^e \| \mathfrak{y}$ $(e \geq 1)$.

$\mathrm{disc}(L/K)$	The discriminant of L/K
$e_{L/K}(\mathfrak{z})$	The ramification index e, of $\mathfrak{z}$ over $\mathfrak{y}$
$f_{L/K}(\mathfrak{z})$	The relative degree $[O_L/\mathfrak{z} : O_K/\mathfrak{y}]$ of $\mathfrak{z}$ over $\mathfrak{y}$
$N_{L/K}$	The norm from L to K
$G(\mathfrak{a})$	The multiplicative group $(O_K/\mathfrak{a})^\times$
$\phi(\mathfrak{a})$	The order of $G(\mathfrak{a})$

Let G be a group.

$\mathcal{H}(G)$	$\{\text{Fields } K \mid \mathrm{Gal}(L/K) = G\}$
$\mathcal{K}_n(G)$	$\{\text{Fields } K \text{ of degree } n \mid \mathrm{Gal}(\overline{K}/Q) = G\}$
$N_n^+(X\ G)$	$\{K \in \mathcal{K}_n(G) \mid 0 < \mathrm{disc}(K) \leq X\}$
$N_n^-(X,G)$	$\{K \in \mathcal{K}_n(G) \mid 0 > \mathrm{disc}(K) \geq -X\}$
$N_n(X,G)$	$\{K \in \mathcal{K}_n(G) \mid \lvert\mathrm{disc}(K)\rvert \leq X\}$

BIBLIOGRAPHY

[1] T. M. Apostol, Introduction To Analytic Number Theory, Springer - Verlag 1976.

[2] E. Artin, "Uber eine neue Art von L-Reihen", Abh. Math. Sem. Univ. Hamburg 3 (1924), 89-108

[3] E. Artin, "Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren", Abh. Math. Sem. Univ. Hamburg 8 (1930), 292-306.

[4] H. Cohn, "The density of Abelian cubic fields", Proc. Amer. Math. Soc. 5 (1954), 476-477.

[5] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields I", Bull. London Math. Soc. 1 (1969), 345-348.

[6] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields II", Proc. Roy. Soc. London A 322 (1971), 405-420.

[7] P. X. Gallagher, "The large sieve and probabilistic number theory", Proc. Sym. Pure Math. AMS Vol. XXIV (1973), 91-101

[8] H. J. Godwin, "On relations between cubic and quartic fields", Quart. J. Math., Oxford Ser. 13 (1962), 206-212.

[9] H. Hasse, Bericht uber neuere Untersuchungen und Probleme aus der Theorie algebraische Zahlkorper, Teil 1, Physica - Verlag 1965.

[10] H. Hasse, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklisch kubische und biquadratische Zahlkorpern", Abh. Deutsch. Akad. Wiss. (1950) nr. 2, 3-95.

[11] H. Hasse, "Arithmetische Theorie der Kubische Zahlkorper auf klassenkorpertheoretischer Grundlage", Math. Z. 31 (1930), 565-582

[12] H. Hasse, Uber die Klassenzahl Abelscher Zahlkorper, Berlin 1952.

[13] H. Heilbronn, "On the 2-classgroup of cubic fields", Studies in Pure Math. Academic Press 1971, 117-119.

[14] D. Hilbert, "Uber die Theorie des relativquadratischen Zahlkorpers", Math. Ann. 51 (1899), 1-127.

[15] S. Iyanaga, The Theory Of Numbers, North - Holland 1975.

[16] G. J. Janusz, Algebraic Number Fields, Academic Press 1973.

[17] E. Landau, "Abschatzungen von charaktersummen, Einheiten und Klassenzahlen", Nachr. Ges. Wiss. Gottingen (1918), 79-97.

[18] E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, B. G. Teubner 1909.

[19] S. Lang, Algebraic Number Theory, Addison - Wesly 1970.

[20] A. F. Lavrik, "The Siegel - Brauer Theorem concerning parameters of algebraic number fields", Translated from Math. Zam. 8 No. 2 (1970), 259-263.

[21] W. Narkiewitz, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers 1973.

[22] J. Rotman, The Theory of Groups, Allyn and Bacon 1965.

[23] J. P. Serre, A Course in Arithmetic, Springer - Verlag 1973.

[24] T. Takagi, "Uber eine Theorie des relativ-Abelschen Zahlkorpers", J. Coll. Sci. Tokyo 41 (1920), 1-133.

[25] E. C. Titchmarsh, The Theory of the Riemann Zeta-Function, Oxford University Press 1951.

[26] B. L. van der Waerden, "Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt", Monatsh Math. 43 (1936), 133-147.