ON THE GENUS FIELD AND ITS APPLICATIONS TO FOUR PROBLEMS IN ALGEBRAIC NUMBER THEORY

Thesis for the Degree of Ph. D.
MICHIGAN STATE UNIVERSITY
THOMAS RANDLE BUTTS
1973

This is to certify that the

thesis entitled

On the Genus Field and its Applications
to Four Problems in Algebraic Number Theory

presented by

Thomas Randle Butts

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

Major professor

Date July 23, 1973

O-7639

ABSTRACT

ON THE GENUS FIELD AND ITS
APPLICATIONS TO FOUR PROBLEMS
IN ALGEBRAIC NUMBER THEORY

BY

Thomas Randle Butts

The genus field of an algebraic number field K, denoted by $GSF(K)$, is the maximal unramified extension of K of the form AK where A/Q is abelian.

In this dissertation I first construct the genus field of most algebraic number fields. This construction and the theory underlying it are then applied to two recent problems:

(1) (MacCluer) For which normal extensions K/Q does the multiplicative group $\|I\|_K$ generated by the absolute norms of all fractional ideals of K coincide with the group $\|H\|_K$ of absolute norms of all principal fractional ideals of K?

(2) (Burgess) If f is a polynomial with rational integral coefficients, let V_f be the multiplicative group generated by the non-zero values of f for integral values of the variable. Does V_f consist

of all rational numbers not excluded by obvious algebraic conditions?

and to two classical problems:

(3) Which abelian groups occur as ideal class groups of algebraic number fields?

(4) Construct the Hilbert class field of an algebraic number field.

A sampling of the results obtained involving these problems is:

(1) $\|I\|_K = \|H\|_K \Longleftrightarrow K = GSF(K) = ZCF(K)$ where $ZCF(K)$ is the central class field of K.

(2) $GSF(K) \neq K \Longrightarrow V_f \neq \|I_K\|$, meaning the answer to (2) is usually "no".

(3) Every abelian group occurs as a subgroup of the ideal class group of infinitely many a) abelian b) non-abelian and c) non-normal algebraic number fields.

(4) If the exponent of the ideal class group of a quadratic number field K divides 12, the Hilbert class field of K is constructed.

Many examples are given to illustrate the constructions and theorems.

ON THE GENUS FIELD AND ITS APPLICATIONS TO FOUR PROBLEMS IN ALGEBRAIC NUMBER THEORY

BY

Thomas Randle Butts

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1973

69-3042

TABLE OF CONTENTS

INTRODUCTION

The value group V_f of a polynomial $f(x)$ in $\mathbb{Z}[x]$ is defined by $V_f = \langle f(n) \mid n \in \mathbb{Z} \rangle$. At the 1969 AMS Number Theory Conference, two problems concerning the value group of a polynomial were posed:

<u>Problem 1</u>. (Stolarsky) Let $f(x) = x^4+x^3+x^2+x+1$. If $p \equiv 1 \bmod 10$, does $p \in V_f$?

<u>Problem 1a</u>. (Burgess) If $f(x) \in \mathbb{Z}[x]$, does V_f contain all rational numbers not excluded by obvious algebraic conditions?

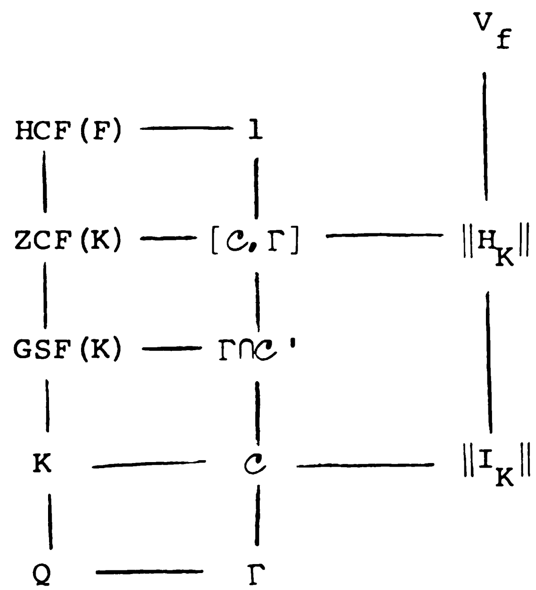
If $\|I_K\|$ denotes the group generated by the absolute norms of all fractional ideals of an algebraic number field K and $\|H_K\|$ denotes the group generated by the absolute norms of all principal fractional ideals of K, then $V_f \subset \|H_K\| \subset \|I_K\|$ where K is the splitting field of f. This observation gives rise to a stronger version of Problem 1, namely,

<u>Problem 1'</u>. If $f(x) \in \mathbb{Z}[x]$ is irreducible with splitting field K, when does $V_f = \|I_K\|$?

We are also led to consider the simpler

<u>Problem 2</u>. (MacCluer) For which normal extensions $K/\mathbb{Q}$ does $\|I_K\| = \|H_K\|$?

Attempts to solve these problems led to consideration of the Hilbert class field (HCF), the central class field (ZCF) and the genus field (GSF) of K as evidenced in the Artin diagram: ($\mathcal{C}$ is the ideal class group of K)



This diagram also brings to mind two classical problems:

<u>Problem 3</u>: Which abelian groups occur as ideal class groups?

<u>Problem 4</u>. Construct the Hilbert class field of an algebraic number field.

In this dissertation I focus on the genus field and its application to these four problems. Because the genus field, unlike the central class field or the Hilbert class field, can generally be computed, it can be considered a meaningful unifying concept.

Chapter I is devoted to the derivation of the group-field structure of the Artin diagram. This complements the work of Frohlich [4], [6], [7], Furuta [9], and others.

The construction of the genus field is carried out in Chapter II. Several references on genus fields are given.

Necessary and/or sufficient conditions involving Problem 2 are discussed in Chapter III with the general result being that the equality $\|I_K\| = \|H_K\|$, or equivalently ZCF(K) = GSF(K) = K, occurs infrequently. No generally necessary and sufficient condition seems possible so some special cases are considered.

The results of Chapter III imply the answer to Problem la is generally negative. Discussion of this problem consitituesChapter IV.

In Chapter V the results of Madan [20], [21] and Ishida [15] are generalized to show that every abelian group occurs as a subgroup of the class group of infinitely many a) abelian b) non-abelian c) non-normal algebraic number fields.

A compilation of many known results concerning the construction of Hilbert class fields is given in Chapter VI. The contribution of the genus field is emphasized. Class number tables are from Borevich and Shafarevich [2]. The results of §5 and §6 are due to Herz [13], however the proofs are original.

CHAPTER I

PRELIMINARIES

1. SOME HILBERT THEORY

Throughout this section let K be a finite galois extension of the number field k with galois group G of order n. Let R and S denote the rings of algebraic integers in k and K respectively. Suppose $\mathfrak{P}$ is a prime of K. (For most applications in the dissertation, only the case $k = Q$, $R = Z$ is necessary.)

Definition A: The subset $Z(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ of G is called the decomposition group of $\mathfrak{P}$ over k. The subfield Ξ of K corresponding to $Z(\mathfrak{P})$ is called the decomposition field of $\mathfrak{P}$ over k.

Definition B: The subset $T(\mathfrak{P}) = \{\sigma \in G \mid (x) \equiv x \bmod \mathfrak{P}$ for all x in $S\}$ of G is the inertia group of $\mathfrak{P}$ over k. The subfield $\mathfrak{J}$ of K corresponding to $T(\mathfrak{P})$ is called the inertia field of $\mathfrak{P}$ over k.

It is easy to verify that $Z(\mathfrak{P})$ is a subgroup of G and that $T(\mathfrak{P})$ is a normal subgroup of $Z(\mathfrak{P})$. Suppose $\mathfrak{p} = \mathfrak{P} \cap k$ and $\mathfrak{p} = (\mathfrak{P}_1 \ldots \mathfrak{P}_g)^e$ in K where $\mathfrak{P}_1 = \mathfrak{P}$. Then since G acts transitively on the primes $\mathfrak{P}_1, \ldots \mathfrak{P}_g$, it follows that the index $[G:Z] = g$ so $Z(\mathfrak{P})$ has order n/g.

<u>Definition C</u>: The sequence of groups

$$G \supset Z \supset T \supset 1$$

is called the <u>short Hilbert sequence</u> of $\mathfrak{P}$ over k.

One important property of the Hilbert sequence is expressed in the following:

<u>Result I</u>: For each prime $\mathfrak{P}$ of K,

$$Z(\mathfrak{P}) \;/\; T(\mathfrak{P})$$

is naturally isomorphic to

$$G(S/\mathfrak{P} \mid R/\mathfrak{p}) \;,$$

the galois group of the finite field extension $S/\mathfrak{P}$ over $R/\mathfrak{p}$.

<u>Result II</u>: $\mathfrak{P}$ is of degree 1 and ramification index e over its inertia field $\mathcal{J}(\mathfrak{P})$. The prime $\mathfrak{P}_T$ of $\mathcal{J}(\mathfrak{P})$ below $\mathfrak{P}$ is of degree f and ramification index 1 over the

decomposition field $\Xi(\mathfrak{P})$. Moreover

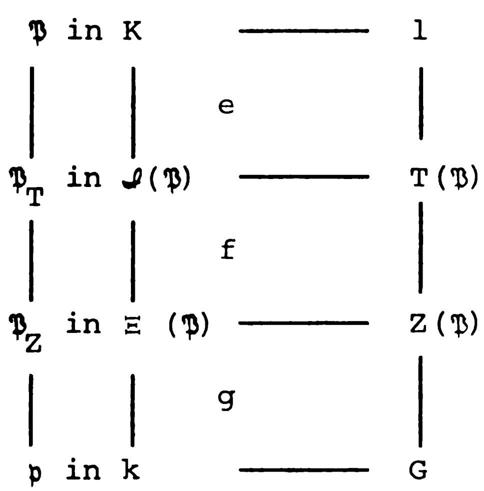
$$[K:\mathcal{J}(\mathfrak{P})] = [T(\mathfrak{P}):1] = e$$

$$[\mathcal{J}(\mathfrak{P}):\Xi(\mathfrak{P})] = [Z(\mathfrak{P}):T(\mathfrak{P})] = f$$

and

$$[\Xi(\mathfrak{P}):k] = [G:Z(\mathfrak{P})] = g \quad .$$

An Artin diagram illustrating Result II is



Now suppose $\mathfrak{P}$ is unramified over k , so $T(\mathfrak{P}) = 1$ and

$$Z(\mathfrak{P}) \cong G(S/\mathfrak{P} \ / \ R/\mathfrak{p}) \quad .$$

But $R/\mathfrak{p} = GF(\|\mathfrak{p}\|_k)$ and $S/\mathfrak{P} = GF(\|\mathfrak{p}\|_k^f)$ where $\|\mathfrak{p}\|_k$ is the absolute norm of $\mathfrak{p}$. Thus $G(S/\mathfrak{P} \ / \ R/\mathfrak{p})$

is cyclic and generated by the map

$$x \longrightarrow x^{\|\mathfrak{p}\|_k} .$$

Hence we can choose a generator σ of $Z(\mathfrak{P})$ so that

$$\sigma(x) \equiv x^{\|\mathfrak{p}\|_k} \bmod \mathfrak{P}$$

for all $x \in S$. This unique element of $Z(\mathfrak{P})$ is called the <u>Frobenius Automorphism</u> of $\mathfrak{P}$ over k. The symbol $\left[\frac{K/k}{\mathfrak{P}}\right] = \sigma$ is called the <u>Frobenius symbol</u> of $\mathfrak{P}$ over k.

<u>Remark</u>: The Frobenius automorphisms of the prime factors of $\mathfrak{p}$ are conjugate under G.

<u>PROOF</u>: Note that for $\tau \in G$, $x \in S$,

$$\sigma(\tau^{-1}x) \equiv (\tau^{-1}x)^{\|\mathfrak{p}\|_k} \equiv \tau^{-1}(x^{\|\mathfrak{p}\|_k}) \bmod \mathfrak{P}$$

so that

$$\tau\sigma\tau^{-1}(x) \equiv x^{\|\mathfrak{p}\|_k} \bmod (\tau\mathfrak{P}) .$$

Hence

$$\left[\frac{K/k}{\tau\mathfrak{P}}\right] = \tau\left[\frac{K/k}{\mathfrak{P}}\right]\tau^{-1} .$$

The conjugacy class formed by the Frobenius symbols of the factor of $\mathfrak{p}$, of a prime unramified in K, is called the <u>Artin symbol</u> of $\mathfrak{p}$ and is denoted by $\left(\frac{K/k}{\mathfrak{p}}\right)$. As is the common practice for abelian extensions, the Artin symbol will be thought of as element valued.

2. HILBERT CLASS FIELDS

Let K be an algebraic number field and let I denote the group of fractional ideals of K. I is free on the prime ideals of K. Let H denote the subgroup of I consisting of all principal fractional ideals of K. Then

$$I/H = \mathcal{C}$$

is called the <u>ideal class group</u> of K and

$$h = [I:H] = |I/H|$$

is called the <u>class number</u> of K.

The fact that relations existed between the ideal class group of a number field K and its abelian extension fields was first observed toward the end of the nineteenth century. Hilbert defined the class field of K as that extension field of K where exactly the prime ideals in the unit class split completely.

He conjectured that the galois group of the class field of K with respect to K was isomorphic to the ideal class group of K . Furtwangler (1907) was the first to verify his conjecture. During the next twenty years, Artin (and Takagi) constructed general class field theory and gave another proof of Hilbert's conjecture based on the Artin symbol defined in §1. He noted that the Artin symbol associates to each prime ideal $\mathfrak{P}$ of K an element in the galois group of every abelian extension of K in which $\mathfrak{P}$ is unramified. Artin's formulation of Hilbert's class field is

<u>Definition D</u>: The <u>Hilbert</u> <u>class</u> <u>field</u> of an algebraic number field of K , denoted by HCF(K) , is the maximal abelian unramified extension of K .

Most of the properties of the Hilbert class field of K are summarized in the

<u>Artin Reciprocity Theorem</u>: The homomorphism defined by linearly extending the map

$$\mathfrak{P} \longrightarrow \left(\frac{HCF(K)/K}{\mathfrak{P}} \right)$$

to all of I is surjective with kernel H .

Thus the galois group of HCF(K)/K is canonically isomorphic to the class group $\mathcal{C}$ of K , that is

$$1 \longrightarrow H \longrightarrow I \longrightarrow G \xrightarrow[\text{symbol}]{\text{Artin}} 1$$

is short exact where G is the galois group of HCF(K)/K .

That the Artin map from I into G is surjective even on the primes of K is seen via the Cebotarev density theorem. The deep insight afforded by the Reciprocity Theorem is that the kernel is H , that is

$$\left(\frac{HCF(K)/K}{\mathfrak{P}} \right) = 1 \Leftrightarrow \mathfrak{P} \equiv 1 \bmod H \quad .$$

When $K/\mathbb{Q}$ is a normal extension, $HCF(K)/\mathbb{Q}$ is also normal since it is unique. Thus if Γ denotes the galois group of $HCF(K)/\mathbb{Q}$, we have the following Artin diagram denoting the galois correspondence:

$$\begin{array}{ccc} HCF(K) & \text{———} & 1 \\ | & & | \\ K & \text{———} & \mathcal{C} \\ | & & | \\ \mathbb{Q} & \text{———} & \Gamma \end{array}$$

3. BETWEEN K AND HCF(K)

Of the fields between K and HCF(K) for K an algebraic number field, two are of interest in this dissertation:

<u>Definition E</u>: The <u>genus</u> <u>field</u> (Geschlecterkörper) of an algebraic number field K, denoted by $GSF(K)$, is the maximal unramified extension of K of the form AK where $A/\mathbb{Q}$ is a finite abelian extension.

In fact $A/\mathbb{Q}$ is the maximal abelian extension of $\mathbb{Q}$ contained in $HCF(K)/\mathbb{Q}$. Notice that the genus field is defined even for non-normal extensions of $\mathbb{Q}$.

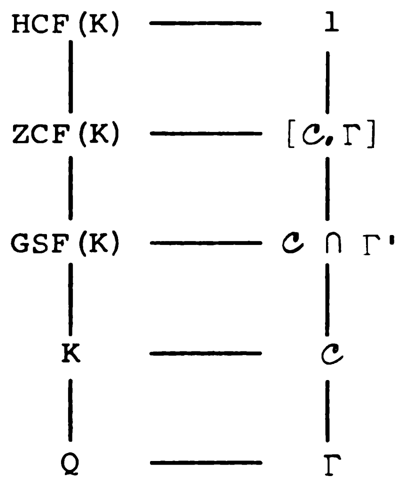
<u>Definition F</u>: For a normal algebraic number field $K/\mathbb{Q}$, the <u>central</u> <u>class</u> <u>field</u> (Zentralen Klassenkörper) of K, denoted by $ZCF(K)$, is the maximal abelian unramified extension of K normal over $\mathbb{Q}$ such that the galois group of $ZCF(K)/K$ is contained in the center of the galois group of $ZCF(K)/\mathbb{Q}$.

If Γ denotes the galois group of $HCF(K)/\mathbb{Q}$, then it is clear that the genus field $GSF(K)$ corresponds to $\mathcal{C} \cap \Gamma'$ under the Galois correspondence.

If N is the normal subgroup of Γ corresponding to $ZCF(K)$ under the Galois correspondence, $\mathcal{C}/N$ is contained in the center of Γ/N. But for any normal subgroup B of Γ contained in $\mathcal{C}$,

$$\mathcal{C}/B \subset Z(\Gamma/B) \Leftrightarrow B \supset [\mathcal{C},\Gamma]$$

where $[\mathcal{C},\Gamma]$ is the group generated by all commutators $c^{-1}\gamma^{-1}c\gamma$ where $c \in \mathcal{C}$ and $\gamma \in \Gamma$. Thus $N = [\mathcal{C},\Gamma]$ and $[\mathcal{C},\Gamma] \subset \mathcal{C} \cap \Gamma'$. An Artin diagram illustrating these relationships when $K/\mathbb{Q}$ is normal is,

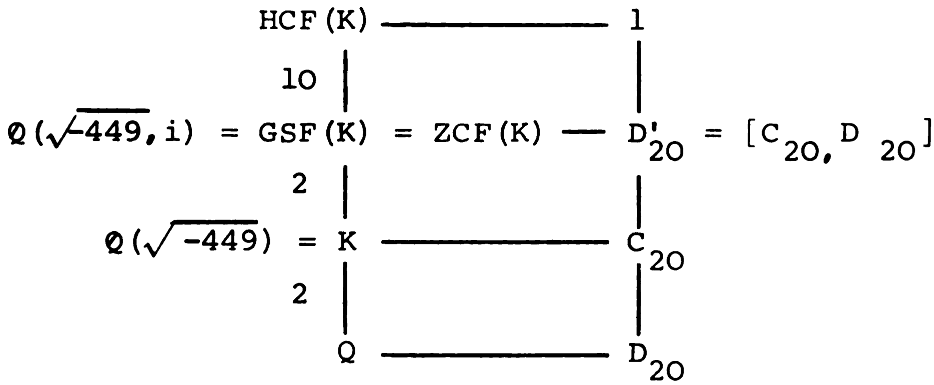


4. AN EXAMPLE: $K = \mathbb{Q}(\sqrt{-449})$

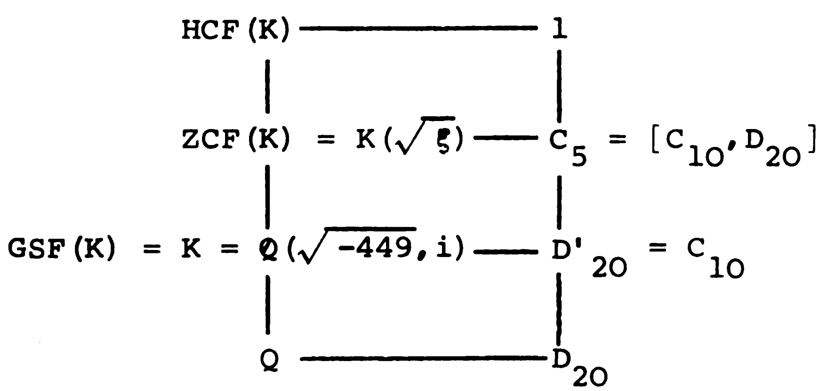
In this example $h(K) = 20$, $\mathcal{C}$ is cyclic, and so $|\Gamma| = 40$. The Sylow 5-subgroup C_5 is normal in Γ , so Γ/C_5 is either abelian (A) , dihedral (D_4) , or quaternion $(\mathcal{Q})$. Let L denote the subfield of HCF(K) with galois group Γ/C_5 . If $\Gamma/C_5 = A$ or $\mathcal{Q}$, then every subgroup of Γ/C_5 is normal. Thus the inertia fields over $\mathbb{Q}$ of all prime divisors in L of 2 or 449, the only primes ramifying in K, coincide. Since L/K is unramified, the ramification indices of 2 and 449 are 2 in $L/\mathbb{Q}$. Then the intersection of the inertia fields $\mathcal{J}(2) \cap \mathcal{J}(449)$ is an unramified extension of degree at least 2 over $\mathbb{Q}$ which contradicts the Dedekind-Minkowski Theorem that there are no unramified extensions of $\mathbb{Q}$. Hence $\Gamma/C_5 = D_4$.

Since $C_5 \triangleleft \Gamma$ and $(5,8) = 1$, Γ is a semi-direct product of C_5 and D_4. These groups are determined by the homomorphisms θ of D_4 into $\text{Aut } C_5 = C_4$. Now $|\ker \theta| \neq 2$ since the only normal subgroup of order 2 in D_4 is contained in the cyclic subgroup of order 4. $D_4 = \langle a^2 = b^4 = 1, aba^{-1} = b^{-1}\rangle$ and there are three alternatives: (1) $\ker \theta = D_4$, (2) $\ker \theta = \langle b\rangle$, (3) $\ker \theta = \langle a, b^2\rangle$. Alternative (3) is impossible since this group contains no cyclic subgroup of order 20 so two possibilities remain: (1) $\Gamma = C_5 \otimes D_4$ and (2) $\Gamma = D_{20}$. In (1), $D_4 \triangleleft \Gamma$, so there exists an abelian subfield $M/\mathbb{Q}$ of $HCF(K)/\mathbb{Q}$ of degree 5. But $M/\mathbb{Q}$ must contain a prime of ramification index 5 over $\mathbb{Q}$ contradicting the fact that $HCF(K)/K$ is unramified. Thus we finally obtain that $\Gamma = D_{20} = \langle x^2 = y^{20} = 1, xyx^{-1} = y^{-1}\rangle$.

Now $|\Gamma'| = 10$ since $xyx^{-1}y^{-1} = y^{-2}$ has order 10 so that $GSF(K)/\mathbb{Q}$ has degree 4 . The only normal subgroup of Γ properly contained in Γ' is C_5 , but $|Z(\Gamma/C_5)| = 2$, so $ZCF(K) = GSF(K) = \mathbb{Q}(\sqrt{-449}, i)$ as can be shown. We have the lattice of fields



Now take $K = \mathbb{Q}(\sqrt{-449}, i)$. In this case $h(K) = 10$ and the group-field structure is the same as before. We note $GSF(K) = K$ and since $|Z(D_4)| = 2$, $ZCF(K)/K$ has degree 2 . It can be shown that $ZCF(K) = K(\sqrt{\xi})$ where ξ is a fundamental unit of $\mathbb{Q}(\sqrt{449})$, giving the lattice of fields:



CHAPTER II

GENUS FIELDS

Let K be an algebraic number field and $GSF(K)$ be its genus field. In this chapter I give a construction of $GSF(K)$ when $K/\mathbb{Q}$ is normal and determine a formula for the genus number of K,

$$g(K) = [GSF(K):K].$$

In addition, the genus field of a non-normal extension is discussed briefly.

In order to understand this construction, it is necessary to extend our knowledge of the way a rational prime ramifies in a normal extension $K/\mathbb{Q}$, so we develop

§1 More Hilbert Theory

Throughout this section $K/\mathbb{Q}$ is a normal extension with galois group G and ring of integers S. If $\mathfrak{P}$ is a prime ideal of K, then e denotes the ramification index of $\mathfrak{P}$ over $\mathbb{Q}$, f denotes the degree of $\mathfrak{P}$ over $\mathbb{Q}$, $Z(\mathfrak{P})$ denotes the decomposition group of $\mathfrak{P}$ over $\mathbb{Q}$ and $T(\mathfrak{P})$ denotes the inertia group of $\mathfrak{P}$ over $\mathbb{Q}$.

<u>Definition A</u>: The subgroup $V_n(\mathfrak{P})$ of $T(\mathfrak{P})$ defined by $V_n(\mathfrak{P}) = \{\sigma \in G \mid \sigma(x) \equiv x \bmod \mathfrak{P}^{n+1}$ for all x in $S\}$ is called the <u>n^{th} ramification group</u> of $\mathfrak{P}$ over $\mathcal{Q}$.

As is well known, the higher ramification groups of $\mathfrak{P}$ over $\mathcal{Q}$ form a finite strictly decreasing normal series,

$$Z(\mathfrak{P}) \supset T(\mathfrak{P}) \supset V_1(\mathfrak{P}) \supset \cdots \supset 1.$$

<u>Definition B</u>: The sequence of groups

$$G \supset Z \supset T \supset V_1 \supset \cdots \supset 1$$

is called the <u>long Hilbert sequence</u> of $\mathfrak{P}$ over $\mathcal{Q}$.

As is well known,

<u>Result I</u>: $T(\mathfrak{P})/V_1(\mathfrak{P})$ is cyclic with order dividing p^f-1. $V_i(\mathfrak{P})/V_{i+1}(\mathfrak{P})$ are elementary abelian p-groups where $(p) = \mathfrak{P} \cap \mathcal{Q}$.

Note that $e = \sum_0^\infty (V_i : V_{i+1})$.

For abelian extensions, there is the not so well known delicate result of Speiser [22],

<u>Result II</u>: If $Z(\mathfrak{P})$ is abelian, then $[T(\mathfrak{P}):V_1(\mathfrak{P})] \mid p-1$.

If $(p,e) = 1$, $\mathfrak{P}$ is said to be <u>tamely ramified</u> and it is clear that

$$V_1(\mathfrak{P}) = V_2(\mathfrak{P}) = \cdots = 1.$$

Thus in this case Results I and II become

<u>Result III</u>: If $\mathfrak{P}$ is tamely ramified over $\mathbb{Q}$, $T(\mathfrak{P})$ is cyclic and $|T(\mathfrak{P})| \mid p^f-1$. Furthermore if $Z(\mathfrak{P})$ is abelian, then $|T(\mathfrak{P})| \mid p-1$.

If we localize at a prime $\mathfrak{P}$ of K, then $\Xi(\mathfrak{P})_{\mathfrak{P}} = K_{\mathfrak{P}}$ becomes the decomposition field of $\mathfrak{P}$ and the galois group of $K_{\mathfrak{P}}/\mathbb{Q}_p = \Xi(\mathfrak{P})_{\mathfrak{P}/\mathbb{Q}_p}$ is $Z(\mathfrak{P})$. The long Hilbert sequence for $K_{\mathfrak{P}}/\mathbb{Q}_p$ is

$$Z \supset T \supset V_1 \supset \cdots = 1$$

and all global results are also local results.

§2 <u>Construction of the Genus Field</u>

Recall that the genus field $GSF(K)$ of an algebraic number field K is the maximal unramified extension of K

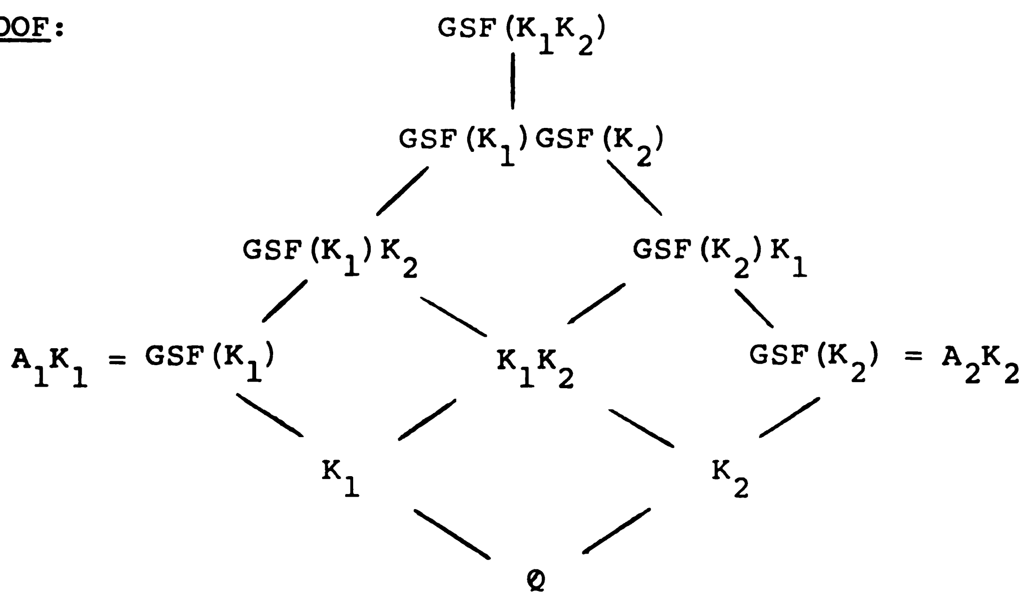
of the form AK where $A/\mathbb{Q}$ is a finite abelian extension and the genus number of K, $g(K) = [GSF(K):K]$.

The genus field and consequently the genus number of K will be determined in steps when (A) $K/\mathbb{Q}$ is abelian, (B) $K/\mathbb{Q}$ is non-abelian, and then when (C) $K/\mathbb{Q}$ is non-normal.

(A) If $K/\mathbb{Q}$ is abelian, GSF(K) becomes the maximal unramified extension of K which is abelian over $\mathbb{Q}$. As it turns out, it suffices to consider abelian extensions of degree p^{α} because of the following

<u>Lemma A</u>: If $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are finite and normal, then $GSF(K_1K_2) \supseteq GSF(K_1) \cdot GSF(K_2)$.

<u>**PROOF**</u>:



By tracing through this Artin diagram applying the results

(1) M/N unramified $\Rightarrow MK/NK$ is unramified

(2) M/k, N/k abelian (unramified) $\Rightarrow MN/k$ is abelian (unramified),

we see that $A_1A_2K_1K_2 = GSF(K_1)\cdot GSF(K_2)$ is unramified over K_1K_2 and therefore is contained in the maximal unramified extension of K_1K_2 of the form AK_1K_2 where $A/\mathbb{Q}$ is abelian.

Consequently let $K/\mathbb{Q}$ be abelian of degree p^{α}. We show that $GSF(K)$ is a certain subfield of the minimal cyclotomic field containing K guaranteed by the famous

<u>Kronecker-Weber Theorem:</u> Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Specifically I prove,

<u>Proposition</u>: Let $K/\mathbb{Q}$ be abelian of degree p^{α} with finite ramified primes $\{p_j\}_{j=1}^{s}$, $p = p_s$, having ramification indices $\{e_j\}_{j=1}^{s}$ over $\mathbb{Q}$. Then $GSF(K)$ is the inertia field of p_∞ in $\prod_{j=1}^{s} L_j$ over K where p_∞ is any one of the infinite primes of K and where L_j is the subfield of $\mathbb{Q}(\zeta_{p_j})$ of degree e_j over $\mathbb{Q}$, $1 \leq j \leq s-1$, and L_s is the subfield of $\mathbb{Q}(\zeta_{p^{\gamma+1}})$ of degree p^{γ} over $\mathbb{Q}$ where $e_s = p^{\gamma}$ if p is odd; or either $\mathbb{Q}(\zeta_{2^{\gamma+1}})$ or the maximal real subfield of $\mathbb{Q}(\zeta_{2^{\gamma+2}})$ where $e_s = 2^{\gamma}$, if $p = 2$.

Moreover

$$g(K) = \frac{\prod_{j=1}^{s} e_s}{p^{\alpha}\,\delta_\infty}$$

where

$$\delta_\infty = \begin{cases} 2 & \text{if } p_\infty \text{ ramifies in } \prod_{j=1}^{s} L_j/K \\ 1 & \text{otherwise} \end{cases}$$

We observe that the Proposition implies that $p^{\alpha} \mid \prod_{j=1}^{s} e_j$. As well as being a step in the proof, this fact is of independent interest, so we state it as

<u>Lemma B</u>: If $K/\mathbb{Q}$ is abelian of degree n with finite ramified primes $\{p_j\}_1^s$ having ramification indices $\{e_j\}_1^s$, then

$$\prod_{j=1}^{s} e_j \equiv 0 \bmod n.$$

Lemma B can then be used to show equality holds in Lemma A. By putting everything together we will obtain the main

<u>Theorem 1</u>: Let $K/\mathbb{Q}$ be abelian of degree $n = \prod_{i=1}^{m} q_i^{\alpha_i}$ with finite ramified primes $\{p_j\}_{j=1}^{s}$

having ramification indices $\{e_j\}_{j=1}^{s}$ over $\mathbb{Q}$. Then

$$GSF(K) = \prod_{i=1}^{m} GSF(K_i)$$

where $K = \prod_{i=1}^{m} K_i$ and $[K_i:Q] = q_i^{\alpha_i}$.

Moreover

$$g(K) = \frac{\prod_{j=1}^{s} e_j}{n\delta_\infty}$$

where $\delta_\infty = \begin{cases} 2 \text{ if } \delta_\infty = 2 \text{ for } K_i/\mathbb{Q},\ [K_i : \mathbb{Q}] = 2^{\alpha_i} \\ 1 \text{ otherwise} \end{cases}$

Now for the proofs.

<u>PROOF (Lemma B)</u>: The inertia fields of the prime divisors in K of any ramified prime in $\mathbb{Q}$ are conjugate. Thus if $K/\mathbb{Q}$ is abelian, the inertia fields of these divisors are equal, so we speak of the inertia field of p.

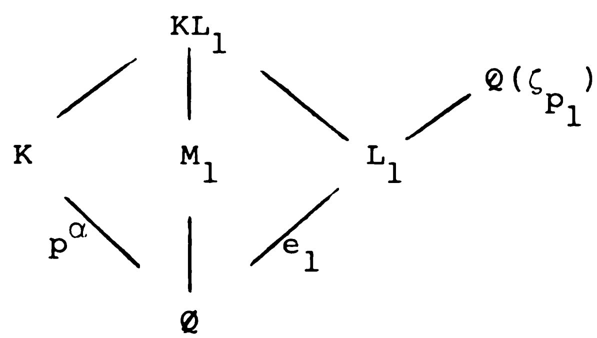
K
| e_1
$\mathcal{J}_1$
| e_2'
$\mathcal{J}_2$
⋮
|
$\mathbb{Q}$

Let $\mathcal{J}_1$ denote the inertia field of p_1 so that $[K:\mathcal{J}_1] = e_1$. Let $\mathcal{J}_2$ be the inertia field of p_2 in $\mathcal{J}_1$ and define recursively $\mathcal{J}_j$ as the inertia field of p_j in $\mathcal{J}_{j-1}$, setting $e_j' = [\mathcal{J}_j:\mathcal{J}_{j-1}]$. Since there are no unramified extensions of $\mathbb{Q}$ by the Dedekind-Minkowski Theorem, $\mathcal{J}_s = \mathbb{Q}$ so that $\prod_{j=1}^{s} e_j' \equiv 0 \bmod n$. But $e_j' | e_j$ for all j, so

$\prod_{j=1}^{s} e_j \equiv 0 \bmod n$ completing the proof.

<u>PROOF</u>: (Proposition) The portions of this proof which are identical with the steps in Speiser's [22] proof of the Kronecker-Weber Theorem will only be sketched. For an elementary proof of the Kronecker-Weber Theorem see Zassenhaus [26].

By Result III (Speiser), $e_1 | p_1 - 1$. Now $\mathbb{Q}(\zeta_{p_1})$ contains a unique subfield of degree e_1 which we will denote by L_1. Let M_1 be the inertia field of p_1 in the abelian extension $KL_1/\mathbb{Q}$, an extension of p^{th} power degree.



Because p_1 is tamely ramified in KL_1, its inertia group is a cyclic subgroup of $G(KL_1/\mathbb{Q})$ and of order divisible by e_1. But by Galois theory, $G(KL_1/\mathbb{Q})$ is isomorphic to a subgroup of the external direct product

$$G(K/\mathbb{Q}) \otimes G(L_1/\mathbb{Q}),$$

an abelian p-group together with a cyclic p-group of order e_1. Consequently

$$e_1 = KL_1/M_1$$

that is <u>the index of ramification of</u> p_1 <u>in</u> KL_1/Q <u>is still</u> e_1! Moreover since p_1 is totally ramified in L_1 yet unramified in M_1,

$$M_1 \cap L_1 = Q$$

and so

$$[M_1L_1:Q] = [M_1:Q][L_1:Q] = [M_1:Q]e_1 = [KL_1:Q]$$

that is

$$KL_1 = M_1L_1$$

and so a fortiori

$$K \subset M_1L_1.$$

Thus M_1/Q is abelian of degree p^β with finite ramified primes $p_2, p_3, \ldots, p_s$ where $e_j = e_j(M_1/Q)$ for $j = 2,3,\ldots,s$. Because p_j is unramified in L_1/Q, it is also unramified in L_1M_1/M_1 and KL_1/K. This construction, then, effectively isolates the ramification of p_1 in the field L_1, while not disturbing the ramification of the other primes.

Applying this argument s-2 more times, we obtain a sequence of fields $L_1, L_2, \ldots, L_{s-1}$ where L_j is the subfield of the p_j^{th} roots of unity $Q(\zeta_{p_j})$ of degree e_j over Q. Then $K \subseteq M_{s-1}L_1 \cdots L_{s-1}$ where $M = M_{s-1}$ is abelian of degree p^γ over Q where only p and possibly the infinite prime ramify.

As usual the cases p odd and $p = 2$ must be considered separately with $p = 2$ being the more difficult.

(1) When p is odd, M turns out to be the subfield of $\mathbb{Q}(\zeta_{p^{\gamma+1}})$ of degree p^{γ} over $\mathbb{Q}$. Setting $M = L_s$, we see that $L = \prod_{j=1}^{s} L_j$ is an abelian extension of $\mathbb{Q}$ of degree $\prod_{j=1}^{s} e_j$ since $L_i \cap L_j = \mathbb{Q}$ for all i,j as different primes ramify totally in each L_i. Furthermore L/K is unramified since $\{p_j\}_1^s$ are the only finite primes ramifying in $L/\mathbb{Q}$ and $e_j(L/\mathbb{Q}) = e_j(K/\mathbb{Q})$ for all j. As p is odd, the infinite prime is also unramified since normal extensions of odd degree are real. Thus $L \subset GSF(K)$ implying $\prod_{j=1}^{s} e_j \mid [GSF(K):\mathbb{Q}]$. But by Lemma B, $[GSF(K):\mathbb{Q}] \mid \prod_{j=1}^{s} e_j$ so $GSF(K) = L$ and the description of $GSF(K)$ is valid. Since $[GSF(K):K] = \frac{[GSF(K):\mathbb{Q}]}{[K:\mathbb{Q}]}$, the formula for $g(K)$ is also clear thus completing the proof of the Proposition when p is odd.

(2) When $p = 2$, $M = L_s$ is either $\mathbb{Q}(\zeta_{2^{\gamma+1}})$ on the maximal real subfield of $\mathbb{Q}(\zeta_{2^{\gamma+2}})$ if $\gamma \geq 2$. If $\gamma = 2$, then L_s is $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}(\sqrt{-2})$. Arguing as in (1), we see that $L = \prod_{j=1}^{s} L_j$ is abelian over $\mathbb{Q}$, $[L:\mathbb{Q}] = \prod_{j=1}^{s} e_j$, and L/K is unramified at all finite primes. If the infinite prime (in $\mathbb{Q}$) ramifies in K, then L/K is unramified and $L = GSF(K)$ as in (1). If however the infinite primes of K ramify in L, then $GSF(K)$ is their inertia field in L. The description of $GSF(K)$ and the validity of the formula

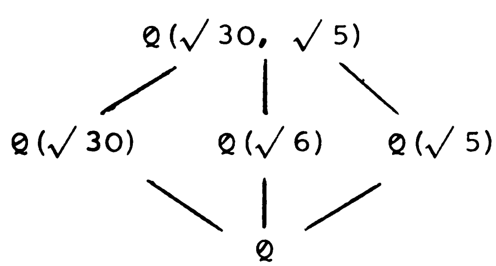
for $g(K)$ are now clear in this case, so the proof of the Proposition is complete.

The proof of Theorem 1 now follows trivially from the Proposition and the two lemmas.

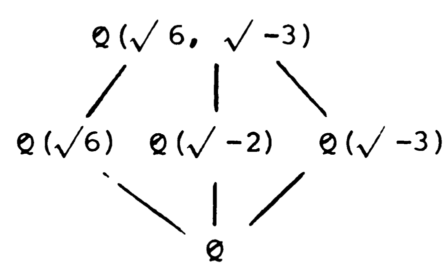
Example 1. $K = Q(\zeta_m) \Longrightarrow GSF(K) = K$. Since $Q(\zeta_m) = \prod_{p|m} Q(\zeta_{p^\alpha})$ where $m = \prod_{p|m} p^\alpha$ and p is the only ramified prime in $Q(\zeta_{p^\alpha})$ and p ramifies totally. Thus $GSF(Q(\zeta_{p^\alpha})) = Q(\zeta_{p^\alpha})$ and the conclusion follows from Theorem 1.

Example 2. $K = Q(\sqrt{30})$, 2,3,5 are finite ramified primes, p_∞ is unramified in K.

Step (1). $L_1 = Q(\sqrt{5})$ since $5 \equiv 1 \bmod 4$ so $M_1 = Q(\sqrt{6})$.



(1)



(2)

Step (2). $L_2 = Q(\sqrt{-3})$ since $3 \equiv 3 \bmod 4$ so $M_2 = Q(\sqrt{-2})$. Thus $L = Q(\sqrt{30}, \sqrt{6}, \sqrt{-3})$. p_∞

ramifies in L/K, so $GSF(K) = \mathbb{Q}(\sqrt{30}, \sqrt{6}) = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ which is $HCF(K)$ since $h(K) = 2$.

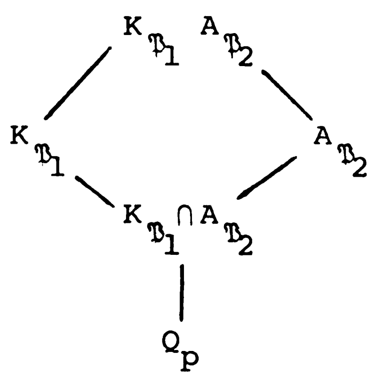
Example 3. $K = \mathbb{Q}(\sqrt{66})$. 2,3,11 are the finite ramified primes, p_∞ is unramified in K. Analogous reasoning to Example 2 shows $L = \mathbb{Q}(\sqrt{66}, \sqrt{-3}, \sqrt{-11})$ so $GSF(K) = \mathbb{Q}(\sqrt{66}, \sqrt{33}) = \mathbb{Q}(\sqrt{2}, \sqrt{33})$.

Example 4. $K = \mathbb{Q}(\sqrt{231})$. 2,3,7,11 are the finite ramified primes. p_∞ is unramified in K. Analogous reasoning shows $L = \mathbb{Q}(\sqrt{231}, \sqrt{-3}, \sqrt{-7}, \sqrt{-11})$ so $GSF(K) = \mathbb{Q}(\sqrt{231}, \sqrt{21}, \sqrt{33}) = \mathbb{Q}(\sqrt{21}, \sqrt{33}, \sqrt{11}) = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{11})$.

(B) To recapitulate, the genus field of an abelian extension K/Q with finite ramified primes $\{p_j\}_1^s$ with ramification indices $\{e_j\}_1^s$ is determined by constructing an abelian extension $\prod_{j=1}^{s} L_j/Q$ having the same ramification as K/Q at all finite primes and then making allowance for the infinite primes. In fact L_j is the compositum of the subfield of $Q(\zeta_{p_j})$ of degree e_j' over Q and the subfield of $Q(\zeta_{p_j^{\alpha_j+1}})$ of degree $p_j^{\alpha_j}$ over Q (with suitable modifications for $p = 2$) where $e_j = e_j' p_j^{\alpha_j}$, $(e_j', p_j) = 1$.

To determine the genus field of K where K/Q is not necessarily abelian, we seek to construct a maximal abelian extension A/Q such that AK/K is unramified. This extension should have the same "abelian ramification" as K/Q, an idea I will now make precise.

Let p_j denote any finite ramified prime of the non-abelian extension K/Q and let $\mathfrak{P}_1$ resp. $\mathfrak{P}_2$ denote any prime divisor of p_j in K resp. A. Then e_j is the ramification index of p_j in the local field $K_{\mathfrak{P}_1}$. Let e_j' denote the ramification index of p_j in $A_{\mathfrak{P}_2}$.

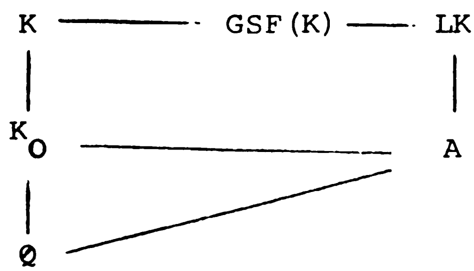


Then the "abelian ramification" e'_j of p_j in K is the ramification index of p_j in $K_{\mathfrak{P}_1} \cap A_{\mathfrak{P}_2}/\mathbb{Q}_p$, that is the ramification index of p_j in the maximal abelian subfield of $K_{\mathfrak{P}_1}/\mathbb{Q}_p$. Now if $e'_j = e''_j p_j^{\alpha_j}$, $(e''_j, p_j) = 1$, then $e''_j | p_j - 1$ applying the local version of Result II. Let then L_j denote the compositum of the subfield of $\mathbb{Q}(\zeta_{p_j})$ of degree e''_j over $\mathbb{Q}$ and the subfield of $\mathbb{Q}(\zeta_{p_j^{\alpha_j+1}})$ of degree $p_j^{\alpha_j}$ over $\mathbb{Q}$ (or if $p_j = 2$, either $\mathbb{Q}(\zeta_{2^{\alpha+1}})$ or the maximal real subfield of $\mathbb{Q}(\zeta_{2^{\alpha+2}})$ as the case may be). If $L = \prod_{j=1}^{s} L_j$, LK/K is unramified at all finite primes and it is again a question of the ramification of the infinite primes of K in LK/K. Thus $GSF(K)$ is the inertia field of the infinite primes of K in LK/K so $GSF(K)$ has the form AK where $A = L$ if K is imaginary and A is the inertia field of the infinite rational prime in L if K is real.

We observe that A contains K_0 and $GSF(K_0)$ where $K_0/\mathbb{Q}$ is the maximal abelian subfield of $K/\mathbb{Q}$ and that $A \cap K = K_0$. Thus

$$g(K) = [GSF(K):K] = \frac{[A:K_0]}{\delta_\infty} = \frac{[A:\mathbb{Q}]}{[K_0:\mathbb{Q}]\delta_\infty} = \frac{\prod_{j=1}^{s} e'_j}{[K_0:\mathbb{Q}]\delta_\infty}$$

since $L_j \cap L_i = \mathbb{Q}$ for all i,j since different primes ramify totally in each extension.



Thus we have constructed the genus field of any normal extension $K/\mathbb{Q}$. We summarize this construction in the following theorem which, of course, contains Theorem 1 as a special case.

<u>Theorem 2</u>: Let $K/\mathbb{Q}$ be a normal extension with finite ramified primes $\{p_j\}_{j=1}^{s}$. Let e_j' denote the ramification index of p_j in the maximal abelian subfield of the local field $K_{\mathfrak{P}_j}/\mathbb{Q}_p$ and let $e_j' = e_j'' p_j^{\alpha_j}$ where $(e_j'', p_j) = 1$. Then GSF(K) is the inertia field of the infinite primes of K in LK/K where $L = \prod_{j=1}^{s} L_j$ with L_j being the compositum of the subfield of $\mathbb{Q}(\zeta_{p_j})/\mathbb{Q}$ of degree e_j'' and the subfield of $\mathbb{Q}(\zeta_{p_j^{\alpha_j+1}})/\mathbb{Q}$ of degree $p_j^{\alpha_j}$ (or if $p_j = 2$ either $\mathbb{Q}(\zeta_{2^{\alpha+1}})$ or the maximal real subfield of $\mathbb{Q}(\zeta_{2^{\alpha+2}})$).

Moreover

$$g(K) = \frac{\prod_{j=1}^{s} e_j'}{[K_0:\mathbb{Q}]\,\delta_\infty}$$

where K_0/Q is maximal abelian subfield of K/Q

and $\delta_\infty = \begin{cases} 2 & \text{if the infinite primes of K ramify } LK/K \\ 1 & \text{otherwise} \end{cases}$

<u>Example 5</u>: Let K be the Kummer extension $K = Q(\sqrt[n]{a}, \zeta_n)$, $n > 2$, $a \neq \pm 1$ is square-free and odd.

The primes divisors of $\operatorname{lcm}(a,n)$ are the finite ramified primes of K. Suppose $p_1, p_2, \ldots, p_m$ divide n and $p_{m+1}, \ldots, p_s$ divide $\frac{a}{(a,n)}$. Then $L_j \subset Q(\zeta_n)$ for $j = 1,2,\ldots,m$. For $p_{m+1}, \ldots, p_s$, L_j is the subfield of $Q(\zeta_{p_j})/Q$ of degree $(n, p_j - 1)$, since the maximal abelian subfield of the local field $Q_p(\sqrt[n]{a}, \zeta_n)$ over Q_p is $Q_p(\sqrt[t]{a})$ where $t = (n, p_j - 1)$ and p_j is totally ramified in $Q_p(\sqrt[t]{a})$. Then $L = \prod_{j=m+1}^{s} L_j$ so $GSF(K) = K(\theta_{m+1}, \ldots, \theta_s)$ where θ_j is a primitive element for L_j/Q, $j = m+1, \ldots, s$. Since $K_0 = Q(\zeta_n)$,

$$g(K) = \frac{\prod_{j=1}^{s} e_j'}{\varphi(n)} = \frac{\prod_{j=1}^{m} e_j' \cdot \prod_{j=m+1}^{s} e_j'}{\varphi(n)} = 1 \cdot \prod_{j=m+1}^{s} (n, p_j - 1) = \prod_{p \mid \frac{a}{(a,n)}} (n, p-1).$$

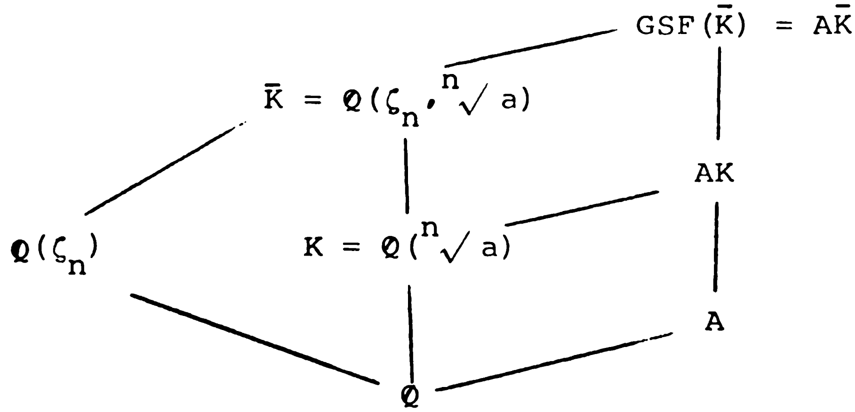
(C) The genus field, unlike the central class field, is defined for non-normal extensions. In this case we obtain

<u>Theorem 3</u>: If K/Q is a non-normal algebraic number field and $\bar{K}/Q$ is its normal closure, then $GSF(K)$ is the maximal unramified extension of K contained in AK where $GSF(\bar{K}) = A\bar{K}$.

PROOF: A prime unramified in K is unramified in $\bar{K}$, so the same primes ramify in both K and $\bar{K}$. Thus $GSF(K) \subseteq AK$ and the conclusion is immediate.

I have not investigated conditions for equality of $GSF(K)$ and AK except for the following

Example 6: $K = \mathbb{Q}(\sqrt[n]{a})$, $(a,n) = 1$, $a \neq \pm 1$ is square-free and odd



The prime divisors $\{p_j\}_1^s$, of an are the finite ramified primes of K. Let $\{p_j\}_1^t$ denote divisors of a and $\{p_j\}_{t+1}^s$ denote divisors of n.

From Example 5, $GSF(\bar{K}) = A\bar{K} = (\prod_{j=1}^{t} L_j)\bar{K}$ where $L_j/\mathbb{Q}$ is the subfield of $\mathbb{Q}(\zeta_{p_j})/\mathbb{Q}$ of degree $(n, p_j - 1)$. Now $p_j, j = 1,2,\ldots,t$, is unramified in $\bar{K}/K$. Since $A\bar{K}/\bar{K}$ is also unramified, prime divisors of p_j in K are unramified AK/K. For $p_k, k=t+1,\ldots,s$, p_k is unramified in A and hence unramified in AK/K. Therefore AK/K is unramified and by Theorem 3 $GSF(K) = AK = K(\theta_1, \ldots, \theta_t)$ where θ_j is a primitive element for L_j.

To my knowledge the connection between the genus field and the Kronecker-Weber Theorem has not been noted in literature. Furuta [8] has computed a formula for a general genus number g(K/k), where k is any algebraic number field, using class field theory and idele class groups. Special cases of the genus number formula have been proved in similar fashion by Yokoi [24] and Iyanga-Tamagawa [16]. Hasse [12] and Leopoldt [19] have discussed genus fields using character theory. Fröhlich [4] has computed the genus number using rational congruence groups. It appears that he is responsible for the definition of genus field used here. For cyclic extensions of prime degree, Herz [13] has constructed the genus field using a different technique. Historically the primary interest has been in genus fields of quadratic fields looked at in terms of quadratic forms.

CHAPTER III

NORM GROUPS

1. Recall that for K/k a finite separable extension, k a number field, the (relative) norm $N_{K/k}(\mathfrak{P})$ of a prime ideal $\mathfrak{P}$ in K is defined to be the ideal $\mathfrak{p}^f$ in k where $\mathfrak{p} = \mathfrak{P} \cap k$ is the prime ideal of k lying below $\mathfrak{P}$ and f is the degree of $\mathfrak{P}$ over k. This map is extended to I_K, the group of fractional ideals of K, by multiplicavity. $N_{K/Q}(\mathfrak{P})$ then is a principal ideal in $\mathbb{Z}$ generated by its least positive integral element, p^f, where p is the rational prime lying below $\mathfrak{P}$ in $\mathbb{Q}$. The integer p^f is called the absolute norm of the prime ideal $\mathfrak{P}$ and, in deference to the analysts, will be denoted by $\|\mathfrak{P}\|_K$, or simply $\|\mathfrak{P}\|$ where only one field is being discussed. An alternative characterization of $\|\mathfrak{P}\|_K$ is the order of the residue class ring $S/\mathfrak{P}$ where S is the ring of integers of K.

Since the absolute norm inherits the multiplicative property, $\mathfrak{A} \to \|\mathfrak{A}\|_K$ is a group homomorphism from I_K into the multiplicative group of positive rationals.

The image group $\|I_K\|$ is therefore generated by the absolute norms of (integral) prime ideals of K . Similarly if H_K denotes the subgroup of principal fractional ideals, then the homomorphic image $\|H_K\|$ is generated by the absolute norms of the principal integral ideals of K .

In this chapter, I will investigate necessary and sufficient conditions for $\|I_K\| = \|H_K\|$ where $K/\mathbb{Q}$ is normal.

2. Let K be a finite galois extension of $\mathbb{Q}$ with galois group G of order n and ideal class group $\mathcal{C}$ of order h . We first check that $\|I_K\|$ and $\|H_K\|$ uniquely determine K by proving the

<u>Proposition</u>: Assume $K/\mathbb{Q}$ and $L/\mathbb{Q}$ are normal. Then

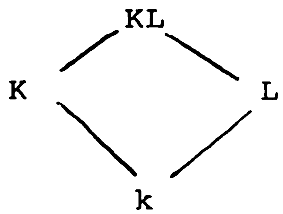
(1) if $\|I_K\| = \|I_L\|$, then $K = L$ and

(2) if $\|H_K\| = \|H_L\|$, then $K = L$.

This Proposition is a consequence of:

<u>Bauer's Theorem</u> (1916) [1]: Let K/k be normal and L/k be finite. Let S_K denote the set of all prime ideals of k which split completely in K . Then $S_K \subset S_L$, if and only if $L \subset K$.

Proof: Since a prime splitting completely in L also splits completely in $\bar{L}$, the galois closure of L, we may assume that L/k is also normal.



Since a prime ideal splitting completely in two extensions of a field k also splits completely in their compositum

$$S_{KL} = S_K \cap S_L \quad \text{so that} \quad S_{KL} = S_K \; .$$

For a normal extension M/k, the Dirichlet density of S_M is $\frac{1}{[M:k]}$, thus $\frac{1}{[K:k]} = \frac{1}{[KL:k]}$ or $KL = K$ implying $L \subset K$.

Note that Bauer's Theorem is true under the weaker hypothesis that the Dirichlet density of $S_K - S_L$ is zero.

Proof of Proposition: (1) $\|I_K\|$ is generated by all p^f where f is the degree of each prime divisor of p in K. Therefore $p \in \|I_K\|$ if and only if p splits completely in K. Thus if $\|I_K\| = \|I_L\|$ then $S_K = S_L$, so $K = L$ follows by letting $k = \mathbb{Q}$ in Bauer's Theorem. (2) If $K \not\supset L$, then by Bauer's Theorem there exists rational prime p such that $p \in S_K$ and $p \notin S_L$. For $\mathfrak{P}$, a prime divisor of p in K, there exists an integral ideal $\mathfrak{A}$ in K with $(\mathfrak{P},\mathfrak{A}) = 1$ such that

$\mathfrak{P}\cdot\mathfrak{A} \equiv 1 \bmod H_K$. Thus $\|\mathfrak{P}\cdot\mathfrak{A}\|_K = p\|\mathfrak{A}\|_K \in \|H_K\|$. But p^f , $f > 1$, is the minimal power of p which could occur as a factor of an integer in $\|H_L\|$ since $L/\mathbb{Q}$ is normal. Thus $K \supset L$. Exchanging the roles of K and L yields the proposition.

To prove $\|I\| = \|H\|$ then, it suffices to prove $p^f \in \|H\|$ for every rational prime p . This observation leads trivially to one class of fields for which $\|I\| = \|H\|$, namely

> Theorem I: If $(h,n) = 1$, then $\|I\| = \|H\|$ whether or not $K/\mathbb{Q}$ is normal. (h denotes the class number of K .)

Proof: Let p denote an arbitrary positive rational prime and $\mathfrak{P}$ a prime divisor of p in K of degree f . Since $(h,n) = 1$, there exist positive integers x and y such that $hx - ny = 1$. Then $\dfrac{\mathfrak{P}^{hx}}{(p)^{fy}} \in H$ and $\left\|\dfrac{\mathfrak{P}^{hx}}{(p)^{fy}}\right\| = \dfrac{p^{fhx}}{p^{nfy}} = p^f$ completing the proof.

This proof, however, sheds no light on the general problem. $\|I\| = \|H\|$ means that for every rational prime p ; there exists in K a prime divisor $\mathfrak{P}$ of p , a principal ideal (β) , and an ideal $\mathfrak{U}$, such that

$\mathfrak{P} = (\beta)\mathfrak{U}$ where $\|\mathfrak{U}\|_K = 1$ and hence $\|\mathfrak{P}\|_K = \|(\beta)\|_K = p^f$. Such ideals $\mathfrak{U}$ will be called unitary ideals, that is

> <u>Definition</u>: An ideal $\mathfrak{U}$ in a finite extension $K/\mathbb{Q}$ for which $\|\mathfrak{U}\|_K = 1$ is called a <u>unitary ideal</u> .

Since the absolute norm is multiplicative, the unitary ideals form a subgroup of the group of fractional ideals I_K which will be denoted by U_K . The subgroup U_K/H_K of the class group $\mathcal{C}_K$ will be denoted by $\mathcal{U}_K$. Subscripts will be omitted when the meaning is clear.

The problem then can be reformulated as:

(1) For which finite galois extensions $K/\mathbb{Q}$ does $I_K = H_K U_K$? or

(2) For which finite galois extensions $K/\mathbb{Q}$ does $\mathcal{C}_K = \mathcal{U}_K$?

I will consider formulation (2) since it is a problem involving finite, rather than infinite, groups.

Now U is an infinite abelian group generated by unitary ideals of the form $\mathfrak{P}^{-1}\sigma(\mathfrak{P})$ where $\mathfrak{P}$ is a prime divisor of p in K . Thus, since prime ideals are equidistributed among all ideal classes, $\mathcal{U}$ is a finite abelian group generated by unitary ideal classes of the the form $c^{-1}\sigma(c)$ where c ranges over $\mathcal{C}$ and σ ranges over G .

The converse of Theorem 1 is true for quadratic fields K , for primes splitting completely in K factor as $(p) = \mathfrak{P}_1\mathfrak{P}_2$ so that $\mathfrak{P}_1^{-1}\mathfrak{P}_2 \equiv (\mathfrak{P}_1^{-1})^2 \bmod H$. Thus for every $c \in \mathcal{C}$, $c^{-1}\sigma(c) = (c^{-1})^2$ implying $\mathfrak{U}$ is generated by the squares of elements of $\mathcal{C}$. But $A^2 = A$ only in abelian groups A of odd order, hence $\mathfrak{U} = \mathcal{C}$ only when h is odd.

Sadly, however, the converse is false as evidenced in the following interesting

<u>Example 1</u>. $K = \mathbb{Q}(\sqrt[3]{11}, \omega)$, ω a primitive cube root of unity.

If $k/\mathbb{Q}$ is a non-normal cubic extension and $\bar{k}$ is the normal closure of k , then $h(\bar{k})$ is either $h^2(k)$ or $h^2(k)/3$ (cf. [14]). Since $h(\mathbb{Q}(\sqrt[3]{11})) = 2$, we have $h(K) = 4$. Let σ denote an automorphism in $G(K/\mathbb{Q}) = S_3$ of order 3 . Then as $\mathcal{C}$ is C_4 (cyclic group of order 4) or V_4 (Klein four group), σ either fixes every element in $\mathcal{C}$ or permutes the three non-identity elements. The latter alternative insures that $\mathfrak{U} = \mathcal{C}$ as the map $c \to c^{-1}\sigma(c)$ is an isomorphism. The impossibility of the former is guaranteed by

Lemma B: Let K/k be galois of degree m, $(p,m) = 1$. Then the p-class group of k coincides with the p-class group of K iff $G(K/k)$ fixes the p-class group of K elementwise.

For a proof of Lemma B, cf. [25]. In this example let $K = \mathbb{Q}(\sqrt[3]{11}, \omega)$, $k = \mathbb{Q}(\omega)$, $p = 2$ and hence $|G(K/k)| = 3$. Since $h(\mathbb{Q}(\omega)) = 1$, the 2-class group of k cannot coincide with that of K.

To reiterate we have an example of a galois field K where $(h,n) = 2$, yet $\|I\| = \|H\|$.

Remark: It is worth noting that if $K/\mathbb{Q}$ is a normal extension of degree n and $(h_K, n) = 1$, then at least one prime divisor of n must divide $|\mathrm{Aut}\ \mathcal{C}|$.

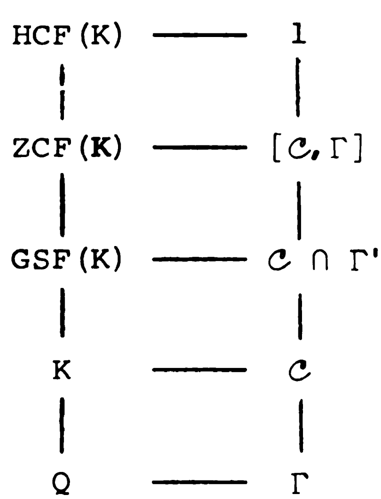
Proof: If not, then every $\sigma \in G(K/\mathbb{Q})$ must fix all elements in $\mathcal{C}$ so that $\mu = 1$ contradicting Theorem 1.

This means, for example, that there are no normal extensions $K/\mathbb{Q}$ of degree p with $h_K = q$ if $p \nmid (q-1)$.

Examination of class number tables shows that normal extensions where $(h,n) = 1$ occur far less frequently than those where $(h,n) \neq 1$. This seems attributable to the limited number of ways $G(K/\mathbb{Q})$ can be embedded in Aut $\mathcal{C}$ for $(h,n) = 1$ to be true.

3. The notation remains in effect for the remainder of this chapter: $K/\mathbb{Q}$ is a finite normal extension of degree n with galois group G, ideal class group $\mathcal{C}$, class number h, unitary ideal group $\mathfrak{U}$, genus field GSF(K), Hilbert class field HCF(K), and central class field ZCF(K).

We first show how our problem of when $\|I_K\| = \|H_K\|$ fits into the general setting of Chapter 1. Recall the Artin diagram



<u>Lemma C</u>: $\mathfrak{U} = [\mathcal{C}, \Gamma]$. Thus in the galois correspondence, <u>the unitary group and the central class field correspond</u>!

PROOF: By the Artin Reciprocity Theorem, $\mathcal{C}$ is canonically isomorphic to $G(HCF(K)/K)$ under the map $c \longmapsto \left(\frac{HCF(K)/K}{\mathfrak{P}}\right)$ where $\mathfrak{P}$ is any prime ideal in c since

$$\left(\frac{HCF(K)/K}{\mathfrak{A}}\right) = \left(\frac{HCF(K)/K}{\mathfrak{B}}\right) \Longleftrightarrow \mathfrak{A} \equiv \mathfrak{B} \bmod H$$

for any integral ideals $\mathfrak{A}$ and $\mathfrak{B}$. Since $\Gamma/\mathcal{C} \simeq G$, for any $\sigma \in G$ we have $\sigma = \gamma c$ for some $\gamma \in \Gamma$, γ cut back to K is σ. But

$$\left(\frac{HCF(K)/K}{\gamma\mathfrak{P}}\right) = \gamma\left(\frac{HCF(K)/K}{\mathfrak{P}}\right)\gamma^{-1} \quad \text{for}$$

any prime ideal $\mathfrak{P}$ in K so that

$$c^{-1}\sigma(c) = c^{-1}(\gamma c) \longmapsto c^{-1}\left(\frac{HCF(K)/K}{\gamma\mathfrak{P}}\right)$$

$$= c^{-1}\gamma\left(\frac{HCF(K)/K}{\mathfrak{P}}\right)\gamma^{-1} = c^{-1}\gamma c\gamma^{-1}$$

completing the proof.

Thus the following statements are equivalent:

(1) $\|I\| = \|H\|$

(2) $UH = I$

(3) $\mathfrak{U} = \mathcal{C}$

(4) $\mathcal{C} = \mathcal{C} \cap \Gamma' = [\mathcal{C}, \Gamma]$

(5) $K = GSF(K) = ZCF(K)$.

4. Sufficient Conditions

In this section I give some sufficient conditions for $\mathfrak{U} = \mathcal{C}$. By Theorem I, $(h,n) = 1$ is always a sufficient condition.

When Γ is a semi-direct product of G and $\mathcal{C}$, we show $\Gamma' \cap \mathcal{C} = \mathfrak{U}$ and hence, in this situation, the condition $GSF(K) = K$ is also sufficient.

<u>Lemma D</u>: If Γ is a semi-direct product of G and $\mathcal{C}$, then $\Gamma' \cap \mathcal{C} = \mathfrak{U}$.

<u>PROOF</u>: It suffices to show $\Gamma' \cap \mathcal{C} \subseteq \mathfrak{U}$. If (σ, c) denotes an arbitrary element in Γ, a semi-direct product of G and $\mathcal{C}$, then multiplication is defined by $(\sigma,c)(\tau,d) = (\sigma\tau, \tau(c)d)$ where τ represents both an element of G and its image in Aut $\mathcal{C}$. Any element in $\Gamma' \cap \mathcal{C}$ then has the form $x = (\sigma,c)(\tau,d)(\sigma^{-1},\sigma^{-1}(c^{-1}))(\tau^{-1},\tau^{-1}(d^{-1}))$ where σ and τ commute. Thus

$$
\begin{aligned}
x &= (\sigma\tau,\tau(c)d)(\sigma^{-1},\sigma^{-1}(c^{-1}))(\tau^{-1},\tau^{-1}(d^{-1})) \\
&= (\tau,\sigma^{-1}(\tau(c)d)\sigma^{-1}(c^{-1}))(\tau^{-1},\tau^{-1}(d^{-1})) \\
&= (\tau,\sigma^{-1}(c^{-1}\tau(c))\sigma^{-1}(d))(\tau^{-1},\tau^{-1}(d^{-1})) \\
&= (1,(\sigma\tau)^{-1}(c^{-1}\tau(c))\cdot\tau^{-1}(d^{-1}\sigma^{-1}(d))
\end{aligned}
$$

which belongs to $\mathfrak{U}$ thus completing the proof.

From the lemma easily follows

<u>Theorem II</u>: If Γ is a semi-direct product of G and $\mathcal{C}$, and $GSF(K) = K$, then $\mathfrak{U} = \mathcal{C}$.

<u>Example 2</u>: $K = \mathbb{Q}(\sqrt[3]{11}, \omega)$.
Here $G = S_3$, $\mathcal{C} = V_4$. Since Aut $V_4 = S_3$, Γ is a semi-direct product. $GSF(K) = K$ since 11 remains prime in $\mathbb{Q}(\omega)$, so $\mathfrak{U} = \mathcal{C}$ for this field.

Generalizing from Example 2, we make the sometimes useful

<u>Remark</u>: If Aut $\mathcal{C}$ is non-trivial and is isomorphic to a direct factor of G, then Γ is a semi-direct product of G and $\mathcal{C}$.

No other general sufficient conditions seems possible, so we explore some special cases.

When $K/\mathbb{Q}$ is cyclic the necessary condition $GSF(K) = K$ is also sufficient as shown by

<u>Theorem III</u>: If $K/\mathbb{Q}$ is cyclic, then $ZCF(K) = GSF(K)$.

<u>PROOF</u>: We show that if $\Gamma/\mathcal{C}$ is cyclic, then $\Gamma/[\mathcal{C},\Gamma]$ is abelian; whence $[\mathcal{C},\Gamma] = \Gamma'$ and the conclusion is clear. So suppose $\Gamma/\mathcal{C}$ is cyclic. Then for every γ_1, γ_2 in Γ,

$\gamma_2 c = \gamma_1^k c$ so that $\gamma_2 = c_2\gamma_1^k c_1$. Now $\Gamma/[\mathcal{C},\Gamma]$ is abelian iff $\gamma_2^{-1}\gamma_1^{-1}\gamma_2\gamma_1$ belongs to $[\mathcal{C},\Gamma]$ for all γ_1, γ_2 in Γ. But $\gamma_2^{-1}\gamma_1^{-1}\gamma_2\gamma_1 = c_1^{-1}\gamma_1^{-k}c_2^{-1}\gamma_1^{-1}c_2\gamma_1^k c_1\gamma_1 = c_1^{-1}\gamma_1^{-k}c_2^{-1}\gamma_1^k\gamma_1^{-1}\gamma_1^{-k}c_2\gamma_1^k c_1\gamma_1$

$= c^{-1}\gamma_1^{-1}c\gamma_1$ where $c = \gamma_1^{-k}c_2\gamma_1^k c_1$. Now $c \in \mathcal{C}$ since $\mathcal{C} \triangleleft \Gamma$ and the proof is complete.

5. Necessary conditions

The most obvious necessary condition for $\mathcal{U} = \mathcal{C}$ is GSF(K) = K. In view of the construction of genus fields in Chapter 2 and the Kronecker-Weber Theorem, we have

Theorem IV: If $K/\mathbb{Q}$ is abelian, then

$$GSF(K) = K \iff K = \prod K_j$$

where either

(1) $K_j = \mathbb{Q}(\zeta_{p_j^{\alpha_j}})$ for any prime power $p_j^{\alpha_j}$

or

(2) K_j is a real field of degree 2^α over $\mathbb{Q}$ which has exactly two ramified primes q_1, q_2 such that the subfield of the cyclotomic field of degree $e(q_2)$ over $\mathbb{Q}$ where only q_2 ramifies is imaginary

and $K_i \cap K_j = \mathbb{Q}$ for all i, j.

PROOF: Contemplation

Examples of fields of type (2) are $Q(\sqrt{pq})$, $p = 2$ or $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ and $Q(\sqrt{p}, \sqrt{q})$, $p = 2$ or $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$, where $p > 0$, $q > 0$ in both cases.

<u>Example 3</u>. $\mathbb{Q}(\zeta_m) = \prod_{p|m} \mathbb{Q}(\zeta_{p^\alpha})$ where $m = \prod_{p|m} p^\alpha$.

<u>Example 4</u>. Quadratic fields $K/\mathbb{Q}$ for which $GSF(K) = K$ are

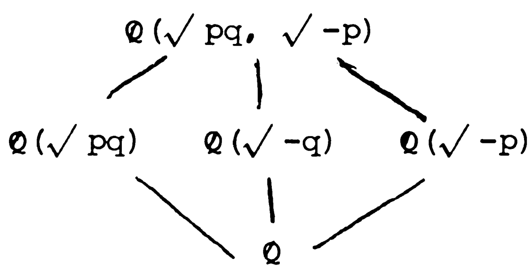
(1) $K = \mathbb{Q}(\sqrt{p})$, $p \equiv 1 \bmod 4$

(2) $K = \mathbb{Q}(\sqrt{pq})$, $p \equiv q \equiv 3 \bmod 4$, $p > 0$, $q > 0$

(3) $K = \mathbb{Q}(\sqrt{2p})$, $p \equiv 3 \bmod 4$, $p > 0$.

The construction in (2), for instance, is

$L_1 = \mathbb{Q}(\sqrt{-p})$ since $p \equiv 3 \bmod 4$, so $M_1 = \mathbb{Q}(\sqrt{-q})$



Thus $L = \mathbb{Q}(\sqrt{pq}, \sqrt{-p})$ but the infinite primes of K ramify in L/K, and their inertia field is $\mathbb{Q}(\sqrt{pq})$.

Since $\mathfrak{U} = \mathcal{C} \Longrightarrow (h,n) = 1$ for quadratic fields, we remark that the fields of (1), (2), and (3) are precisely the quadratic fields with odd class number.

It is clear, then, how to construct abelian fields $K/\mathbb{Q}$ for which $GSF(K) = K$. However given an arbitrary abelian field $L/\mathbb{Q}$, much computation may be required to determine whether or not $GSF(L) = L$.

The non-abelian case seems even more intractible. One obvious criterion which follows from the construction of genus fields for non-abelian fields (Theorem 2, Chapter 2) is

<u>Theorem V</u>: Suppose $K/\mathbb{Q}$ is non-abelian and $K_0/\mathbb{Q}$ is the maximal abelian subfield of $K/\mathbb{Q}$. Then $GSF(K) = K \iff GSF(K_0) = K_0$ and $e_j' = e_j(K_0/\mathbb{Q})$ for all ramified primes $\{p_j\}_{j=1}^{s}$ of K where e_j' is the ramification index of p_j in the maximal abelian subfield of $K_{\mathfrak{P}_j}/\mathbb{Q}_{p_j}$.

The application of this criterion can, again, lead to extensive computation.

<u>Example 5</u>: $K_1 = \mathbb{Q}(\sqrt[9]{5}, \zeta_9)$, $K_2 = \mathbb{Q}(\sqrt[9]{7}, \zeta_9)$. $[K_1:\mathbb{Q}] = [K_2:\mathbb{Q}] = 54$. Now $K_0 = \mathbb{Q}(\zeta_9)$ in both cases and $GSF(K_0) = K_0$. By the formula for $g(K)$ of Example 5, Chapter 2, we see $g(K_1) = (9,4) = 1$ and $g(K_2) = (9,6) = 3$. Thus $GSF(K_1) = K_1$ while $GSF(K_2) = K_2(\zeta_7 + \frac{1}{\zeta_7})$ since $e_7' = 3$ and $\mathbb{Q}(\zeta_7 + \frac{1}{\zeta_7})$ is the subfield of $\mathbb{Q}(\zeta_7)$ of degree 3 over $\mathbb{Q}$.

Salvaging what we can, we state the sometimes useful

<u>Corollary</u>: Suppose $K/\mathbb{Q}$ is non-abelian and K_0/Q is its maximal abelian subfield. Then
$GSF(K) = K \iff GSF(K_0) = K_0$ and every prime ramifying in K either ramifies totally or remains prime in K_0.

PROOF: In both cases, for any ramified prime p,

$$K_{\mathfrak{P}}/\mathbb{Q}_p = K/\mathbb{Q} \quad \text{so} \quad e'_p = e_p(K_0/\mathbb{Q}).$$

<u>Example 6</u>. $K = \mathbb{Q}(\sqrt[p]{a}, \zeta_p)$, p odd prime, a square-free <u>and</u> odd, with $(a,p) = 1$.
$GSF(K) = K \iff$ every prime factor of a is a primitive root modulo p.
The case $a = 11$, $p = 3$ is Example 2.

It appears difficult to determine when $GSF(K) = ZCF(K)$ for an arbitrary normal extension $K/\mathbb{Q}$. But we do note that $[ZCF(K):GSF(K)]$ is divisible by only primes dividing n, for

<u>Lemma E</u>: Let c be any ideal class in $\mathcal{C}$. If $(|c|, n) = 1$, then $c \in \mathfrak{U}$.

PROOF: Let $\mathfrak{P}$ be any prime divisor of p of degree 1 over $\mathbb{Q}$ in c. Since $(|c|, n) = 1$, there exist positive integers x and y such that $|c|x - ny = -1$. Then $\mathfrak{P} \equiv \dfrac{\mathfrak{P}^{|c|x}\mathfrak{P}}{(p)^y}$ mod H and

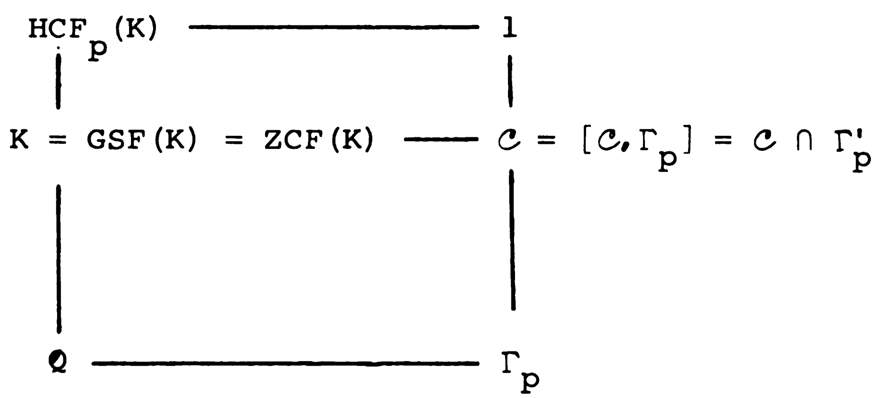
$\left\|\frac{\mathfrak{P}^{|c|x_{\mathfrak{P}}}}{(p)^y}\right\| = p^{|c|x+1-ny} = 1.$ So $c \in \mathfrak{U}$ completing the proof.

We now turn to p-extensions and show that $(h,p) = 1$ is a necessary as well as sufficient condition.

<u>Theorem VI</u>: If $K/\mathbb{Q}$ has degree p^α, then

$$\mathfrak{U} = \mathcal{C} \iff (h,p) = 1$$

<u>PROOF</u>: Only $(\Longrightarrow)$ need be proved. Suppose $p|h$. Let $HCF_p(K)$ denote the p-class field of K, that is the field corresponding to the Sylow p-subgroup of $\mathcal{C}$. $HCF_p(K)/\mathbb{Q}$ is then normal and we let $\Gamma_p = G(HCF_p(K)/\mathbb{Q})$. Thus we have the Artin diagram



But if $\mathcal{C} = [\mathcal{C},\Gamma]$, the descending central series of Γ_p must break off at $\mathcal{C}$ contradicting the nilpotence of Γ_p. Thus $p \nmid h$ and the theorem is proved.

Frohlich [7] has determined those abelian extensions $K/\mathbb{Q}$ of degree p^α which have $(h,p) = 1$. Though Frohlich's theorem is expressed in a way I cannot completely interpret, the gist of the theorem seems to be:

If $K/\mathbb{Q}$ is abelian of degree p^{α}, p odd, then $(h,p) = 1$ if and only if

(1) K has exactly one ramified prime.

(2) $K = K_1 K_2$ where each K_i has exactly one ramified prime one of which remains prime in the other extension.

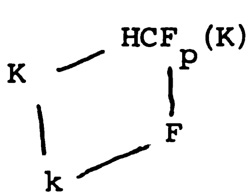
(3) $K = K_1 K_2 K_3$ where each K_i has exactly one ramified prime and (?) .

Every extension $K/\mathbb{Q}$ with four or more ramified primes has $(h,p) > 1$.

Conditions (1) and (2) follow from

<u>Lemma F</u>: Suppose K/k is normal with exactly one ramified prime. If $p|h(K)$, then $p|h(k)$.

<u>PROOF</u>:



Let $\mathfrak{P}$ be a prime divisor of the ramified prime of k in $HCF_p(K)$ and let $T(\mathfrak{P})$ be its inertia group. Then since $G(HCF_p(K)/k)$ is a p-group, $T(\mathfrak{P})$ is contained in a maximal normal subgroup N of $G(HCF_p(K)/k)$ of index p. It is easy to see that the inertia groups of the other prime divisors of the ramified prime are also contained in N. Let F be the intermediate field of $HCF_p(K)/k$ corresponding to N. Then F is an abelian, unramified extension of degree p over k, and the theorem follows.

In (1), if $p|h(K)$, then $p|h(Q) = 1$, a contradiction.

In (2), suppose q_1 ramifies in K, and remains prime in K_2. Then K_1/K_2 has exactly one ramified prime, so if $p|h(K_1)$, then $p|h(K_2)$ contradicting (1).

For (3) I have been unable to construct an example. I suspect the condition is vacuous since if $K = K_1K_2K_3$ then K contains a subfield L such that more than one prime ramifies in L and K/L is not cyclic. Thus $g \neq 1$ for all primes in L contradicting the necessary condition that $g = 1$ for the ramified primes in order for the method of (1) and (2) to apply.

Since the direct product of nilpotent groups is nilpotent, one attempts to extend Theorem VI to the compositum of p-extensions. However if $K = \prod K_i$ and $[K_i : Q] = p_i^{\alpha_i}$, then $HCF(K) \supset \prod HCF(K_i)$ where equality seldom obtains. Thus a general necessary and sufficient condition for an arbitrary extension K/Q seems hopeless. Summarizing those fields for which a necessary and sufficient condition does exist, we note for p-extensions: $\mathcal{U} = \mathcal{C} \Longleftrightarrow (h, p) = 1$

cyclic extensions: $\mathcal{U} = \mathcal{C} \Longleftrightarrow \mathrm{GSF}(K) = K$

extensions where Γ is semi-direct product of G and $\mathcal{C}$: $\mathcal{U} = \mathcal{C} \Longleftrightarrow \mathrm{GSF}(K) = K.$

CHAPTER IV

THE BURGESS PROBLEM

In this chapter we examine the problem, now almost forgotten, which prompted the investigation of the genus field and the central class field.

Suppose $r(x)$ is a polynomial with rational integral coefficients. The <u>value group</u> of $r(x)$, V_r, is the multiplicative group generated by the non-zero values of $r(x)$ as x ranges over the integers. There are many unsolved problems concerning value groups of polynomials. Two of these which were posed at the 1969 AMS Number Theory Institute at Stony Brook, New York are:

> <u>Problem 1</u>: (Kenneth Stolarsky) If $r(x) = x^4+x^3+x^2+x+1$ does $p \in V_r$ if $p \equiv 1 \mod 10$?
>
> <u>Problem 2</u>: (D. A. Burgess) For any polynomial $r(x)$ with rational integral coefficients, does V_r consist of all rational numbers not excluded by obvious algebraic conditions?

We show that the answer to Problem 2, is a mild-to-emphatic "no" depending on one's definition of "obvious". We then indicate a more reasonable problem of which Problem 1 is a special case.

For simplicity, let $r(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial over $\mathbb{Q}$ and let K denote the splitting field of $r(x)$. Then $K = Q(\theta)$ where θ is a primitive element for K and $r(x) = \prod_{i=1}^{n} (x-\sigma_i(\theta))$ where $\sigma_1 = 1, \sigma_2, \ldots, \sigma_n$ are the elements of the galois group $G(K/\mathbb{Q})$. For any rational integer a, $r(a) = \prod_{i=1}^{n} (a-\sigma_i(\theta))$ is within a sign the absolute norm of the principal ideal $(a-\theta)$. Thus V_r is a subgroup of $\|H_K\|$ and $\|I_K\|$. Since $\|I_K\|$ is generated by the rational integers $\pm p^f$ where f is the degree of any prime divisor of p in K over $\mathbb{Q}$, it is clear that $V_r \not\supseteq \mathbb{Q}$ because not every prime splits completely in K. Suppose we ask the more plausible question: Does $p \in V_r$ if p splits completely in K? We see that this, too, is clearly impossible unless $\|I_K\| = \|H_K\|$ or $\mathcal{C}_K = \mathcal{U}_K$, which as we saw in Chapter 3 occurs very infrequently.

Hence we modify Problem 2 and pose the more reasonable

<u>Problem 3</u>: Suppose $r(x)$ is a monic irreducible polynomial with rational integral coefficients and splitting field K. If $GSF(K) = ZCF(K) = K$, does V_r contain all primes p splitting completely in K or, stronger, does $V_r = \|I_K\|$?

Since $\mathbb{Q}(\zeta_5)$ is the splitting field for $r(x) = x^4 + x^3 + x^2 + x + 1$ and primes p splitting completely in $Q(\zeta_5)$ are precisely those $p \equiv 1 \mod 10$, we see that Problem 1 is indeed a special case of Problem 3.

As a first case we consider quadratic polynomials $r(x) = x^2 - m$ so that $K = \mathbb{Q}(\sqrt{m})$. V_r can contain all primes splitting completely in K only if $h(K)$ is odd. For some of those fields, the following ad hoc technique can be used; though it cannot be generalized to fields with degree greater than 2.

<u>Example</u>: $r(x) = x^2 - 21$ so $K = \mathbb{Q}(\sqrt{21})$

$h(K) = 1$ so $GSF(K) = ZCF(K) = K$. Only 3 and 7 ramify in K and $-3 = \dfrac{3^2 - 21}{5^2 - 21}$ and $7 = \dfrac{7^2 - 21}{5^2 - 21}$.

5 and 17 split completely in K and $-5 = 4^2 - 21$, $-17 = 2^2 - 21$. 2, 11, 13, and 19 remain prime in K. Thus for every prime p, $|p| < 21$ splitting completely in K, either $\pm p$ belongs to V_r. Let $p_1, p_2, \ldots, p_n, \ldots$ denote the primes which split completely (or ramify) in K. Then $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 17$, etc. Suppose $p_1, \ldots, p_{n-1}$ belong the V_r for $n \geq 5$. Then since p_n splits completely, the congruence $x^2 \equiv 21 \mod p_n$ has a solution x_0 with $|x_0| \leq \frac{p_n - 1}{2}$. Thus

$$\left(\frac{p_n - 1}{2}\right)^2 - 21 \geq ap_n \quad \text{for some positive integer } a$$

or

$$\frac{p_n^2 - 2p_n - 1}{4p_n} - \frac{21}{p_n} \geq a$$

or

$$\frac{p_n}{4} \geq a.$$

But every prime divisor of a splits completely or ramifies in K and, by the induction hypothesis, belongs to V_r. Thus $p_n = \frac{x_o^2 - 21}{a}$ also belongs to V_r completing the proof.

A similar technique is valid for polynomials of the form $r(x) = x^2 + ax + b$. We remark that V_r contains all primes splitting completely in the splitting fields of $r(x) = x^2 + 1$ and $r(x) = x^2 + x + 1$ which indicates the origin of Problem 1.

Numerical evidence supports the conjecture that all primes splitting completely in a quadratic field K of odd class number belong to V_r where $r(x)$ is any quadratic polynomial whose splitting field is K. In fact I conjecture that for $r(x) = x^2 - m$, each prime p splitting completely in K satisfies $\pm p = \frac{x^2 - m}{y^2 - m}$ for some integers x and y.

CHAPTER V

IDEAL CLASS GROUPS

A classical problem of algebraic number theory is the determination of all abelian groups which occur as ideal class groups of algebraic number fields. While not attempting to solve this general problem, I can show that every abelian group occurs as a subgroup of infinitely many abelian, non-abelian, and non-normal algebraic number fields, by showing every abelian group $\mathcal{A}$ is isomorphic to $G(GSF(K)/K)$ for infinitely many number fields K. This result contains recent ones of Madan [20], [21] and Ishida [15].

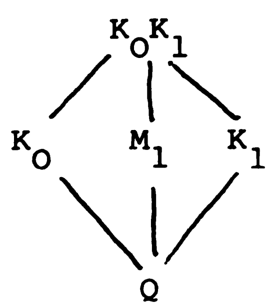
I begin by proving

> <u>Lemma</u>: For every finite abelian p-group $\mathcal{P}$ of exponent p^e, p prime, there exist infinitely many abelian number fields $L/\mathbb{Q}$ of degree p^e whose ideal class group contains a subgroup isomorphic to $\mathcal{P}$.

<u>PROOF</u>: Let $\mathcal{P} = \prod_{i=1}^{n} P_i$ be the decomposition of $\mathcal{P}$ into a product of cyclic subgroups with $|P_i| = p^{e_i}$, $e_i \leq e$. By

Dirichlet's Theorem on the infinitude of primes in an arithmetic progression, there exist infinitely many primes q_i, $q_i \neq q_j$ satisfying $q_i \equiv 1 \bmod p^{e_i}$, $e_0 = e$, $i = 0,1,2,\ldots,n$. Let $K_i/\mathbb{Q}$ denote the unique cyclic subfield of $Q(\zeta_{q_i})$ of degree p^{e_i}, $i=0,1,\ldots,n$. Then $K = \prod_{i=0}^{n} K_i$ is a field for which $GSF(K) = K$. We show how to determine a subfield $L/\mathbb{Q}$ of degree p^e in which all the q_i, $i=0,1,\ldots,n$ ramify with $e(q_i) = p^{e_i}$. Then $GSF(L) = K$ and $G(GSF(L)/L) \cong \mathcal{P}$.

Let now $G(K_i/Q) = \langle\sigma_i\rangle$, $i=0,1$. Let M_i denote the cyclic subfield of $K_0 K_1/\mathbb{Q}$ with $G(M_1/Q) = \langle\sigma_0\sigma_1^{-1}\rangle$. Then it follows easily that



$$\deg\ M_1/\mathbb{Q} = p^e \quad \text{and}$$

$$K_0K_1 = M_1K_0 = M_1K_1 \ .$$

Now q_0 is unramified in K_1/Q and hence in $K_1M_1/\mathbb{Q}M_1 = K_0K_1/M_1$. Similarly q_1 is unramified in $M_1K_0/M_1 = K_0K_1/M_1$, thus K_0K_1/M_1 is unramified. Applying this construction to M_1 and K_2, we obtain a field $M_2/\mathbb{Q}$ of degree p^e where $K_0K_1K_2/M_2$ is unramified. Continuing in this manner, we obtain a sequence of fields $M_3, M_4, \ldots, M_n$ such that deg $M_j/\mathbb{Q} = p^e$ and $K_0K_1\ldots K_j/M_j$ is unramified for $j=3,\ldots,n$.

Then $L = M_n$ is the desired field for which $\deg L/\mathbb{Q} = p^e$ $GSF(L) = \prod_{i=1}^{n} K_i = K$ and hence $G(GSF(L)/L) \cong \mathcal{P}$ completing the proof.

From the Lemma we now obtain

> <u>Theorem 1</u>: For every finite abelian group $\mathcal{A}$ of order a and exponent m, there exist infinitely many abelian number fields of degree m whose ideal class group contains a subgroup isomorphic to $\mathcal{A}$.

<u>**PROOF**</u>: Let $m = \prod_{i=1}^{n} p_i^{e_i}$ and $\mathcal{A} = \prod_{i=1}^{n} \mathcal{P}_i$ be the decomposition of $\mathcal{A}$ into direct product of its Sylow p-subgroups. For each $\mathcal{P}_i$, we obtain, by the Lemma, infinitely many abelian fields $L_i/\mathbb{Q}$ of degree $p_i^{e_i}$ whose ideal class group has $\mathcal{P}_i$ as a subgroup. Then, as $(\deg L_i/\mathbb{Q}, \deg L_j/\mathbb{Q}) = 1$ for all i,j, it follows that for any set of fields $L_1, L_2, \ldots, L_n$ so obtained, $L = \prod_{i=1}^{n} L_i$ is an abelian field of degree m over $\mathbb{Q}$ whose ideal class group contains a subgroup isomorphic to $\mathcal{A}$, thereby completing the proof.

The non-abelian and non-normal cases can be proved by simply reconsidering two examples from Chapter 2. Specifically, we have, Theorem 2: For every finite abelian group $\mathfrak{a}$ of order a and exponent m, there exist infinitely many non-abelian number fields of degree $m\,\varphi(m)$ and non-normal number fields of degree m whose ideal class group contains a subgroup isomorphic to $\mathfrak{a}$.

PROOF: Let $\{p_r^{e_s}\}$ denote the invariants of $\mathfrak{a}$. Dirichlet's Theorem again insures that there are infinitely many primes q_{rs} satisfying $(q_{rs},m) = 1$ and $q_{rs} \equiv 1 \bmod p_r^{e_s}$, $q_{rs} \not\equiv 1 \bmod p_r^{e_s+1}$ for every $p_r^{e_s}$. For each set $\{q_{rs}\}$ so determined, let $K = \mathbb{Q}(\sqrt[m]{\prod_{r,s} q_{rs}})$ and then $\bar{K} = K(\zeta_m)$ Clearly $K/\mathbb{Q}$ is non-normal and $\bar{K}/\mathbb{Q}$ is non-abelian of degrees m and $m\,\varphi(m)$ respectively. Then as $(m, q_{rs}-1) = p_r^{e_s}$, it follows from Examples 5 and 6 of Chapter 2 that

$$G(GSF(K)/K) \cong G(GSF(\bar{K})/\bar{K}) \cong \mathfrak{a}$$

completing the proof.

CHAPTER VI

CONSTRUCTION OF HILBERT CLASS FIELDS

In one of his typical understatements Serge Lang [18] remarks, "It becomes a problem to exhibit the Hilbert class field explicitly". I will examine the tip of this iceberg in this chapter.

The algebraic number fields K for which HCF(K) is most easily determined are those where HCF(K) = GSF(K). After considering several classes of such fields, I conclude by examining the simplest class of fields for which GSF(K) $\neq$ HCF(K). Specifically I give a method to construct an unramified extension of a quadratic number field of degree 3 or 4. Thus if the exponent of the ideal class group of a quadratic number field divides 12, its Hilbert class field can be constructed.

§1 Quadratic Fields: $Q(\sqrt{m})$

From the examples of genus fields of quadratic number fields computed earlier, the general method is apparent. Thus the known cases of quadratic fields K for which GSF(K) = HCF(K) are merely listed in tabular form.

Table - Hilbert Class Fields for Certain Quadratic Fields $Q(\sqrt{m})$

m	Conditions	h	HCF$(Q\sqrt{m}$=GSF$(Q(\sqrt{m}))$	Frequency $\|m\| < 500$
$-p$	$p\equiv 1 \bmod 4$	2	$Q(\sqrt{+p}, i)$	3
$-2p$	$p\equiv 1 \bmod 4$	2	$Q(\sqrt{p}, \sqrt{-2})$	2
$-2p$	$p\equiv 3 \bmod 4$	2	$Q(\sqrt{-p}, \sqrt{2})$	2
$-pq$	$p\equiv 3 \bmod 4$, $q\equiv 1 \bmod 4$	2	$Q(\sqrt{-p}, \sqrt{q})$	11
pq	$p\equiv 1 \bmod 4$	2	$Q(\sqrt{p}, \sqrt{q})$	73
pqr	$p\equiv 1 \bmod 4$, $r,q\not\equiv 1 \bmod 4$	2	$Q(\sqrt{p}, \sqrt{qr})$	30
$2pq$	$p\equiv q\equiv 3 \bmod 4$	2	$Q(\sqrt{pq}, \sqrt{2})$	15
$-pq$	$p\equiv q\equiv 3 \bmod 4$	4	$Q(\sqrt{-p}, \sqrt{-q}, i)$	7
$-pq$	$p\equiv q\equiv 1 \bmod 4$	4	$Q(\sqrt{p}, \sqrt{q}, i)$	1
$-2pq$	$p,q\neq 2$	4	$Q(\sqrt{-2pq}, \sqrt{p^*}, \sqrt{q^*})$	7
$-pqr$	$pqr\equiv 3 \bmod 4$	4	$Q(\sqrt{-pqr}, \sqrt{p^*}, \sqrt{q^*})$	3
pqr	$p,q,r\neq 2$	4	$Q(\sqrt{p}, \sqrt{q}, \sqrt{r})$	11
$2pqr$	$p\equiv 1 \bmod 4$, $q\equiv r\equiv 3 \bmod 4$	4	$Q(\sqrt{p}, \sqrt{qr}, \sqrt{2})$	3
$2pqr$	$p\equiv q\equiv 1 \bmod 4$, $r\equiv 3 \bmod 4$	4	$Q(\sqrt{p}, \sqrt{q}, \sqrt{2r})$	1
$pqrs$	$p\equiv q\equiv 1 \bmod 4$, $r\equiv s\equiv 3 \bmod 4$	4	$Q(\sqrt{r,s}, \sqrt{p}, \sqrt{q})$	0
$-pqr$	$p\equiv 1 \bmod 4$, $q\equiv r\equiv 3 \bmod 4$	8	$Q(\sqrt{p}, \sqrt{pq}, \sqrt{r}, i)$	6
$-2pqr$	$p,q,r\neq 2$	8	$Q(\sqrt{-pqr}, \sqrt{p^*}, \sqrt{q^*}, \sqrt{r^*})$	3
$-pqrs$	$p\equiv 1 \bmod 4$, $q\equiv r\equiv s\equiv 3 \bmod 4$	8	$Q(\sqrt{p}, \sqrt{-q}, \sqrt{-r}, \sqrt{-s})$	0(3)
$-pqrs$	$p\equiv q\equiv r\equiv 1 \bmod 4$, $s\equiv 3 \bmod 4$	8	$Q(\sqrt{p}, \sqrt{q}, \sqrt{r}, \sqrt{-s})$	0(1)
$-pqrs$	$p\equiv q\equiv 1 \bmod 4$, $r\equiv s\equiv 3 \bmod 4$	8	$Q(\sqrt{p}, \sqrt{q}, \sqrt{-r}, \sqrt{-s})$	0(1)

p,q,r,s represent distinct primes; 2 is possible unless indicated otherwise.

$$p^* = \begin{cases} p & \text{if } p \equiv 1 \bmod 4 \\ -p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

The numbers in parentheses in the last column indicate the number of known quadratic fields with $|m| < 500$ satisfying the given conditions.

I do not know whether there exist any real quadratic fields K with $h(K) = 2^t$, $t \geq 3$, and $GSF(K) = HCF(K)$. The problem is unsolved for arbitrary t.

Chowla [3] proved in 1934 that there are only a finite number of imaginary quadratic fields K where $HCF(K) = GSF(K)$. An old conjecture is that there are 65 such fields which are, in addition to those indicated in Table 1:

$K = \mathbb{Q}(\sqrt{-m})$, $h(K) = 4$: $m = 555, 595, 715, 795, 1435$

$K = \mathbb{Q}(\sqrt{-m})$, $h(K) = 8$: $m = 1155, 1365, 1995, 3003, 3315$.

Selfridge showed that these are the only such fields for $m < 2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot44{,}838$. For a complete account of this problem see Grosswald [11].

§2 Compositums of Quadratic Fields

Let $K_1, K_2, \ldots, K_m$ be quadratic extensions of $\mathbb{Q}$. Suppose these fields are <u>independent</u>, that is the degree of $K = \prod_{i=1}^{m} K_i$ is 2^m over $\mathbb{Q}$. Then the galois group of $K/\mathbb{Q}$ is an elementary abelian 2-group and there are $t = 2^m - 1$ different quadratic subfields of K denoted by $K_1, K_2, \ldots, K_t$. Let h_i and ε_i denote the class number and unit group of K. Then it is known (cf.[17]) that:

$$H = \frac{1}{2^v}[E: \prod_{i=1}^{t}\varepsilon_i] \prod_{i=1}^{t} h_i$$

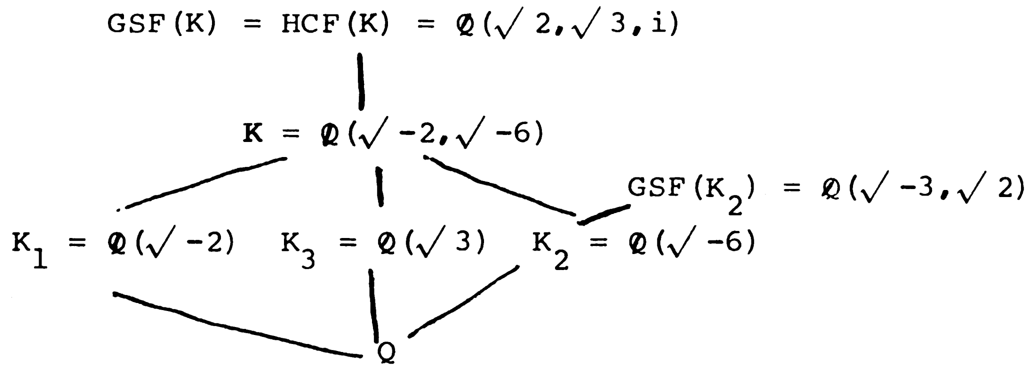
$$\text{where} \quad v = \begin{cases} m(2^{m-1}-1) & \text{if } K \text{ is real} \\ (m-1)(2^{m-2}-1) + 2^{m-1}-1 & \text{if } K \text{ is imaginary} \end{cases}$$

If $GSF(K_i) = HCF(K_i)$ for all i and $GSF(K) = HCF(K)$ then of course, the Hilbert class field of K is determined. When K is imaginary, this occurs only a few times. For example if K is imaginary biquadratic, a necessary condition that $GSF(K) = HCF(K)$ is that exactly two primes ramify in K as I shall now show. $K = Q(\sqrt{-m_1}, \sqrt{-m_2})$ has three quadratic subfields $K_1 = Q(\sqrt{-m_1})$, $K_2 = Q(\sqrt{-m_2})$, and $K_3 = Q(\sqrt{m_1 m_2})$. The ramified primes of K are the prime divisors of $m_1 m_2$, say $p_1, p_2, \ldots, p_k$, and each p_i ramifies in two of the three quadratic subfields. If $GSF(K_i) = HCF(K_i)$, then $h_j = \frac{2^{r_j-1}}{\delta_\infty}$ where r_j is the number of primes ramifying in K_i and δ_∞ is as defined in the genus-number formula. It can be shown that $[E: \prod_{i=1}^{3} \epsilon_i] = \prod_{i=1}^{3} \delta_\infty$ so that

$$H \geq \frac{(\prod_{i=1}^{3} \delta_\infty) 2^{r_1-1} 2^{r_2-1} 2^{r_3-1}}{2(\prod_{i=1}^{3} \delta_\infty)} = 2^{r_1+r_2+r_3-4} = 2^{2k-4}.$$

However $g(K) = 2^{k-2}$, so if $GSF(K) = HCF(K)$, then $2^{2k-4} = 2^{k-2}$ implying $k = 2$.

Example 1: $K = \mathbb{Q}(\sqrt{-2}, \sqrt{-6})$. Here $K_1 = \mathbb{Q}(\sqrt{-2})$, $K_2 = \mathbb{Q}(\sqrt{-6})$, $K_3 = \mathbb{Q}(\sqrt{3})$ and $h_1 = h_3 = 1$, $h_2 = 2$, $H = 2$.

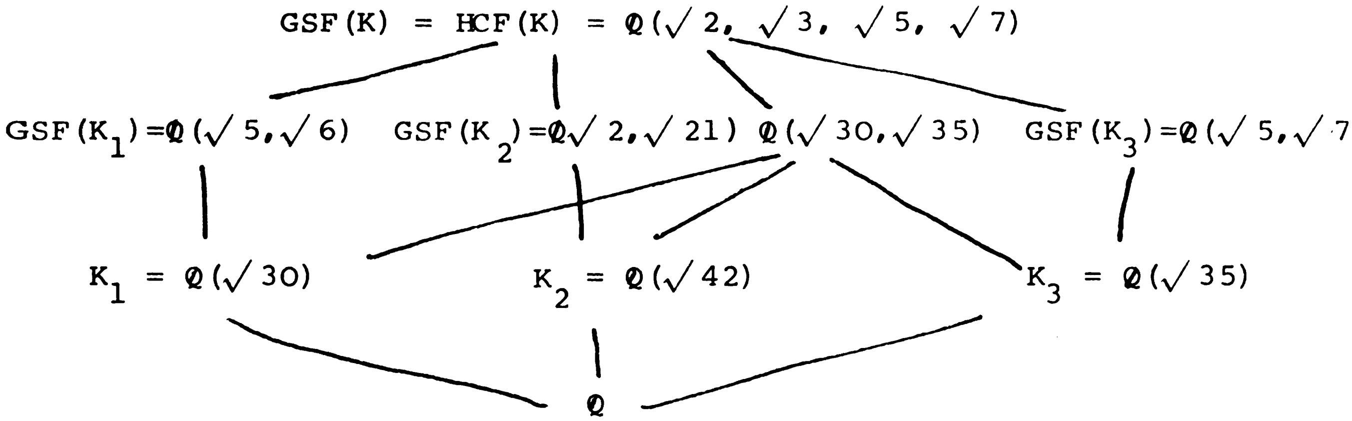


Since there are only 9 imaginary quadratic fields with $h = 1$ and either 47 or 48 with $h = 2$, the number of compositums K of imaginary quadratic fields with $GSF(K) = HCF(K)$ can be completely determined.

More examples of compositums K of real quadratic fields for which $GSF(K) = HCF(K)$ exist. I have not attempted to completely solve this problem, though I suspect only the cases $H = 2$ and $H = 4$ are possible. Two examples will illustrate the situation.

Example 2: $K = \mathbb{Q}(\sqrt{30}, \sqrt{35})$.

Here $K_1 = \mathbb{Q}(\sqrt{30})$, $K_2 = \mathbb{Q}(\sqrt{35})$, $K_3 = \mathbb{Q}(\sqrt{42})$ and $h_i = h_2 = h_3 = 2$, $H = 4$.



Example 3: $K = \mathbb{Q}(\sqrt{2}, \sqrt{15}, \sqrt{21})$.

The seven quadratic subfields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{21})$, $\mathbb{Q}(\sqrt{30})$, $\mathbb{Q}(\sqrt{35})$, $\mathbb{Q}(\sqrt{42})$, $\mathbb{Q}(\sqrt{70})$. $H = 4$ and a diagram like that of Example 2 shows

$HCF(K) = GSF(K) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$.

§3 $n = h = p$

If $K/\mathbb{Q}$ is a cyclic extension of degree p with $h(K) = p$, then $HCF(K)/\mathbb{Q}$ is abelian since all groups of order p^2 are abelian. Thus $HCF(K) = GSF(K)$ and the Hilbert class field of K is determined.

There are only eight cyclic cubic fields of class number 3 with discriminant $\Delta < 20{,}000$, two each with $\Delta = 63^2, 91^2, 117^2, 133^2$.

Example 4: $K = \mathbb{Q}(\theta)$, $\theta^3 - 21\theta - 35 = 0$.

$\Delta(K) = 63^2$ and $HCF(K) = GSF(K) = K(\zeta_7 + \frac{1}{\zeta_7})$ where ζ_7 is a primitive 7^{th} root of unity.

§4 Pure Cubic Fields: $K = \mathbb{Q}(\sqrt[3]{a})$.

In Example 6 of Chapter 2, the genus field of the pure field $K = \mathbb{Q}(\sqrt[n]{a})$ $(n,a) = 1$, $a \neq \pm 1$ is square-free and odd was determined. In that case $g(K) = \prod_{p|a} (n,p-1)$ so for $n = 3$, $HCF(K) = GSF(K)$ if $h(K) = 3^t$ where t is the number of primes $p \equiv 1 \bmod 3$ dividing a. Known examples (with small discriminants) are:

Example 5: $K = \mathbb{Q}(\sqrt[3]{a})$, $h(K) = 3$, $a = 7$, 13, 19, 21, 35, 37. $HCF(K) = GSF(K) = K(\theta)$ where θ is a primitive element for the subfield of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ of degree 3 where $p|a$ and $p \equiv 1 \bmod 3$.

Example 6: $K = \mathbb{Q}(\sqrt[3]{91})$, $h(K) = 9$, $GSF(K) = HCF(K) = K(\theta_1, \theta_2)$ (θ_i determined as in Example 5).

§5 Quadratic fields $K = \mathbb{Q}(\sqrt{m})$ where $3|h$.

The genus field is the "easy part" of the Hilbert class field of an algebraic number field K. To complete the construction of $HCF(K)$ it is necessary to construct abelian unramified extensions of K. In general, this is very difficult so I will focus on two cases: constructing unramified extensions of degree 3 and 4 of quadratic fields.

Let $K = \mathbb{Q}(\sqrt{m})$ with $3 | h(K)$. There exists, then, a field L such that L/K is unramified of degree 3. Suppose, in addition, that $L/\mathbb{Q}$ is normal (which occurs if $3 \| h$ for example). Since the galois group of $L/\mathbb{Q}$ is S_3, L is the splitting field for a cubic polynomial $f(x) = x^3 - ax - b$ whose discriminant $\Delta = mk^2$. We seek to determine a and b so that $K(\theta)/K$ is unramified where $\theta^3 - a\theta - b = 0$. Now

$$(*) \qquad \Delta = 4a^3 - 27b^2 = mk^2$$

$$\text{Set} \quad a = 3t,\ b = st,\ k = \begin{cases} 9tl & \text{if } 3 \nmid m \\ 3tl & \text{if } 3 | m \end{cases}$$

Then (*) becomes

$$(**) \qquad 4t - s^2 = \begin{cases} 3ml^2 \\ \frac{m}{3}\, l^2 \end{cases}$$

Suppose first that $m < 0$, set $m = -m$. Then t is a norm from $Q(\sqrt{3m})$ (or $Q\sqrt{\frac{m}{3}}$), so taking $t = \pm 1$, we can determine s and t by finding the fundamental unit ϵ of $\mathbb{Q}(\sqrt{3m})$ (or $\mathbb{Q}(\sqrt{\frac{m}{3}})$, that is $\epsilon = \frac{s - \sqrt{3m}\, l}{2}$ (or $\frac{s - \sqrt{\frac{m}{3}}\, l}{2}$). Now $K(\theta)/K$ can ramify only at primes dividing 3 in K.

<u>Case 1</u>: $t = 1$, $3 \nmid m$, (the most frequent case).

Since $3 \nmid m$, $K(\theta)/K$ is unramified $\Longleftrightarrow$ 3 is unramified in $\mathbb{Q}(\theta)/Q$. But in this case

$f(x) = x^3 - 3x - s$ and $\Delta = 27(4-s^2)$

so 3 is unramified in $\mathbb{Q}(\theta)$, $\theta^3 - 3\theta - s = 0 \Longleftrightarrow$

$s \equiv \pm 2 \bmod 27$.

<u>Example 7</u>: $K = \mathbb{Q}(\sqrt{-23})$, $h = 3$.

GSF(K) = K and $\epsilon = \dfrac{25 - 3\sqrt{69}}{2}$

So HCF(K) = $\mathbb{Q}(\sqrt{-23}, \theta)$ where $\theta^3 - 3\theta - 25 = 0$.

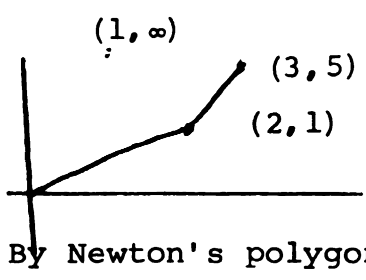
<u>Example 8</u>: $K = \mathbb{Q}(\sqrt{-38})$, $h = 6$.

GSF(K) = $\mathbb{Q}(\sqrt{19}, \sqrt{-2})$ and $\epsilon = \dfrac{2050 - 192\sqrt{114}}{2}$

So HCF(K) = $\mathbb{Q}(\sqrt{19}, \sqrt{-2}, \theta)$ where $\theta^3 - 3\theta - 2050 = 0$.

<u>Case 2</u>: $t = \pm 1$, $3 | m$.

$K(\theta)/K$ will be unramified $\Longleftrightarrow$ $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals in $Q(\theta)$ of degree 1 over $\mathbb{Q}$. In this case $f(x) = x^3 \pm 3x \pm s$. To check the ramification of 3 in $Q(\theta)$, $\theta^3 \pm 3\theta \pm s = 0$, we apply Newton's polygon (see Weiss [23]).



Newton's polygon for $x^3 \pm 3x \pm s$.

By Newton's polygon $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ in $Q(\theta)$ if $s \equiv 0 \bmod 9$.

Example 9: $k = \mathbb{Q}(\sqrt{-231})$, $h = 12$.

GSF(K) $= \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{-11})$ and $\varepsilon = \frac{9+\sqrt{77}}{2}$

so HCF(K) $= Q(\sqrt{-3}, \sqrt{-7}, \sqrt{-11}, \theta)$ where $\theta^3 - 3\theta - 9 = 0$.

Case 3: $t = -1$. Then $3 \mid m$ for in any quadratic field $Q(\sqrt{d})$ if d is divisible by a prime $p \equiv 3 \bmod 4$, then $N(\varepsilon) = +1$. Again $K(\theta)/K$ is unramified $\Longleftrightarrow$ $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ in $Q(\theta)$. Now $f(x) = x^3 + 3x + s$ so applying Newton's polygon directly for $s \not\equiv 0 \bmod 9$ is futile. However

$$f(x+1) = x^3 + 3x^2 + 6x + (s+4)$$

and $f(x+2) = x^3 + 6x^2 + 15x + (s+14)$

so if $s+4 \equiv 0 \bmod 9$ or $s + 14 \equiv s + 5 \equiv 0 \bmod 9$, $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ in $Q(\theta)$, $\theta^3 + 3\theta + s = 0$ so that $K(\theta)/K$ is unramified.

Example 10: $K = \mathbb{Q}(\sqrt{-87})$, $h = 6$

GSF(K) $= Q(\sqrt{29}, \sqrt{-3})$ and $\varepsilon = \frac{5+\sqrt{29}}{2}$

so HCF(K) $= Q(\sqrt{29}, \sqrt{-3}, \theta)$ where $\theta^3 + 3\theta + 5 = 0$

Summarizing these cases is

Proposition: Let $K = Q(\sqrt{-m})$ be an imaginary quadratic field with class number h. For $K_1 = \mathbb{Q}(\sqrt{3m})$, let ε denote the fundamental unit of K_1, t the norm of ε, and s the trace of ε.

Then $3 \mid h$ if

(1) $t = 1$ $s \equiv \pm 2 \bmod 27$

(2) $t = \pm 1$ $s \equiv 0 \bmod 9$

(3) $t = -1$ $s \equiv \pm 4 \bmod 9$.

$K(\theta)/K$ is unramified of degree 3 where

$\theta^3 - 3t\theta - st = 0$.

Unfortunately all cases are not covered by the Proposition.

<u>Example 11</u>: $K = \mathbb{Q}(\sqrt{687})$, $h = 6$

$GSF(K) = \mathbb{Q}(\sqrt{-3}, \sqrt{229})$ and $\epsilon = \frac{15 + \sqrt{229}}{3}$

Unhappily $x^3 + 3x + 15$ is Eisenstein, so 3 ramifies totally in $Q(\theta)/Q$ where $\theta^3 + 3\theta + 15 = 0$. If, however, we can find s, t so that $s \equiv 0 \bmod 9$, $t \not\equiv 0 \bmod 3$, Newton's polygon can then be applied to $x^3 - 3tx - st$ as in Example 7. Since 27 is the first odd multiple of 9 greater than 15, we consider $6 + \epsilon$. Now $\|6 + \epsilon\| = \frac{27^2 - 229}{5} = 125$. So $(3) = \mathfrak{p}_1^2\mathfrak{p}_2$ in $\mathbb{Q}(\theta)/\mathbb{Q}$ where $\theta^3 - 3\cdot 125\theta - 27\cdot 125 = 0$ so that

$HCF(K) = \mathbb{Q}(\sqrt{-3}, \sqrt{229}, \theta)$.

A similar analysis can be applied to any imaginary quadratic field not satisfying the conditions of the Proposition.

For real quadratic fields, an analogous strategy can be employed.

<u>Example 12</u>. $K = \mathbb{Q}(\sqrt{79})$, $h = 3$.

For real quadratic fields, (**) becomes

$t = \frac{s^2+3ml^2}{4}$ or $\frac{s^2+\frac{m}{3}l^2}{4}$ as $3\nmid m$ or $3|m$.

Since $3\nmid 79$, we mimic Case (1) of the Proposition by seeking integers s and t such that

$t = \frac{s^2+237\ l^2}{4}$ and $s^2 \equiv 4t \bmod 27$.

One solution is $s = 2$, $t = 2134$ so that $HCF(K) = \mathbb{Q}(\sqrt{79}, \theta)$ where $\theta^3 - 3\cdot 2134\theta - 2\cdot 2134 = 0$.

This method appears capable of generalization to the construction of an unramified extension of degree p over some quadratic fields by considering $f(x) = x^p - ax - b$ with discriminant $\Delta = (-1)^{\binom{p}{2}}[(p-1)^{p-1}a^p - p^p b^{p-1}]$. This idea will not be pursued here.

§6 Quadratic fields $K = \mathbb{Q}(\sqrt{m})$ where $4|h$.

Let $K = \mathbb{Q}(\sqrt{m})$ with $4|h(K)$ and $GSF(K) \neq HCF(K)$. There exists then a field L such that L/K is unramified of degree 4. Suppose, in addition, that $L/\mathbb{Q}$ is normal (which occurs if $4\|h$ for example). Since the galois group G of $L/\mathbb{Q}$ is non-abelian of order 8, $|G'| = 2$. So $g(K) \geq 2$ and by the discussion in Chapter 2 there exists a subfield of $GSF(K)/\mathbb{Q}$ of the form $M = Q(\sqrt{a}, \sqrt{b})$ where $a = -1$ or $a \equiv 1 \bmod 4$ and $b = 2$ or is a positive prime $p \equiv 1 \bmod 4$. Thus $h(\mathbb{Q}(\sqrt{b}))$ is odd and hence $\|I\|_{\mathbb{Q}(\sqrt{b})} = \|H\|_{\mathbb{Q}(\sqrt{b})}$ by

Theorem 1 of Chapter 3. By examining the various cases it can be shown that a belongs to $\|I\|_{\mathbb{Q}(\sqrt{b})}$ and thus the equation $a = x^2 - by^2$ has a solution where x and y are rational. Consequently $M(\sqrt{\alpha})/M$ where $\alpha = x + \sqrt{b}y$ is unramified since it is clearly unramified at all prime divisors of p in M and since $a = -1$ or $a \equiv 1 \bmod 4$, it is also unramified at prime divisors of 2. Hence $L = K(\sqrt{b}, \sqrt{\alpha})$ is an unramified extension of $K = \mathbb{Q}(\sqrt{m})$ of degree 4.

<u>Example 13</u>: $K = Q(\sqrt{-142})$ $h = 4$.

$a = -71$, $b = 2$, $\alpha = 1 + 6\sqrt{2}$

So $HCF(K) = Q(\sqrt{-71}, \sqrt{2}, \sqrt{1+6\sqrt{2}})$

<u>Example 14</u>: $K = \mathbb{Q}(\sqrt{145})$, $h = 4$.

$a = 5$, $b = 29$, $\alpha = 11+2\sqrt{29}$

or $a = 29$, $b = 5$, $\alpha = 7+2\sqrt{5}$.

So $HCF(K) = Q(\sqrt{5}, \sqrt{29}, \sqrt{11+2\sqrt{29}}) = Q(\sqrt{5}, \sqrt{29}, \sqrt{7+2\sqrt{5}})$

<u>Example 15</u>: $\mathbb{Q}(\sqrt{-65})$, $h = 8$.

Here $\mathbb{Q}(\sqrt{5}, i)$ is a subfield of $GSF(K) = Q(\sqrt{5}, \sqrt{13}, i)$

Thus $a = -1$, $b = 5$, $\alpha = \sqrt{5}$, so

$HCF(K) = Q(\sqrt{5}, \sqrt{13}, i, \sqrt{2+\sqrt{5}})$.

<u>Example 16</u>: $K = \mathbb{Q}(\sqrt{-89})$, $h = 12$.

$GSF(K) = Q(\sqrt{89}, i)$ so extensions of degree 3 and 4 must be determined. For 4, $a = -1$ $b = 89$ so α

is the fundamental unit of $\mathbb{Q}(\sqrt{89})$,

$$\alpha = \frac{1000 + 106\sqrt{89}}{2} = 500 + 53\sqrt{89}$$

Now $3 \nmid 89$, so $1 = \dfrac{s^2 - 267\, 1^2}{4}$. So s is determined

by the fundamental unit of $\mathbb{Q}(\sqrt{267})$.

Thus $HCF(K) = Q(\sqrt{89}, i, \sqrt{500+53\sqrt{89}}, \theta)$ where

$\theta^3 - 3\theta - s = 0$

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Bauer, M., "Zur Theorie der Algebraischen Zählkorper", Math. Ann. 77, 1916, pp. 353-356.

2. Borevich, Z.I. and Shafarevich, I.R., Number Theory, Academic Press, New York, 1966.

3. Chowla, S., "An Extension of Heilbron's Class-Number Theorem", Quart. Journ. Oxford Ser. 5, 1934, pp. 304-307.

4. Frohlich, A., "The Genus Field and Genus Group in Number Fields I, II", Mathematika 6, 1959, pp. 40-46, 142-146.

5. __________, "On a Method for the Determination of Class Number Factors in Number Fields", Mathematika, 4, 1957, pp. 113-131.

6. __________, "On Fields of Class Two", Proc. London Math. Soc. (3), 4, 1954, pp. 235-256.

7. __________, "On the Absolute Class Group of Abelian Fields I, II, J. London Math. Soc., 29, 1954, pp. 211-217; 30, 1955, pp. 72-80.

8. Furuta, Yoshiomi, "The Genus Field and Genus Number in Algebraic Number Fields", Nagoya Math. J., 29, 1967, pp. 281-285.

9. __________, "Über das Geschlect und die Klassenzahl eines Relativ-Galoisschen Zahlkörpers vom Primzahlpotenzgrade", Nagoya Math J., 37, 1969, pp. 197-200.

10. __________, "Über dies Zentrale Klassenzahl eines Relativ-Galoisschen Zahlkörpers, J. Number Theory, 3, 1971, pp. 318-322.

11. Grosswald, Emil, "Negative Discriminants of Binary Quadratic Forms with One Class in each Genus", Acta Arith., 8, 1963, pp. 295-306.

12. Hasse, Helmut, "Zur Geschlecter theorie in Quadratischen Zahlkorpern", J. Math. Soc. Japan, 3, 1951, pp. 45-51.

13. Herz, C. S., "Construction of Class Fields", Seminar on Complex Multiplication, Springer-Verlag, Berlin, 1966.

14. Honda, Taria, "Pure Cubic Fields whose Class Numbers are Multiples of Three", J. Number Theory, 3, 1971, pp. 7-12.

15. Ishida, Makoto, "Class Numbers of Algebraic Number Fields of Eisenstein Type", J. Number Theory, 2, 1970, pp. 404-413.

16. Iyanga, S. and Tamagawa, T., "Sur la Theorie du Corps de Classes de Nombres Rationelles, J. Math. Soc. Japan, 3, 1951, pp. 220-227.

17. Kuroda, S. N., "Über die Klassenzahlen Algebraischer Zahlkörper", Nagoya Math. J., 1, 1950, pp. 1-10.

18. Lang, Serge, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.

19. Leopoldt, H., "Zur Geschlectertheorie in Abelschen Zahlkörpern", Math. Nachr. 9, 1953, pp. 351-362.

20. Madan, Manohar, "Class Groups of Global Fields", J. Reine Angew Math., 252, 1972, pp. 171-177.

21. __________, "On Class Numbers of Algebraic Number Fields", J. Number Theory, 2, 1970, pp. 116-119.

22. Speiser, A., "Die Zerlegungsgruppe", J. Reine Angew Math., 149, 1919, pp. 174-188.

23. Weiss, Edwin, Algebraic Number Theory, McGraw-Hill, New York, 1963.

24. Yokoi, Hideo, "On the Class Number of a Relatively Cyclic Field", Nagoya Math. J., 29, 1967, pp. 31-44.

25. Yokoyama, Akio, "On Class Numbers of Finite Algebraic Number Fields", Tôhoku Math. J., 17, 1965, pp. 349-357.

26. Zassenhaus, Hans, "On a Theorem of Kronecker", Delta, 1, 1969, pp. 1-14.