DETERMINATION OF THE HILBERT CLASS FIELD FOR CERTAIN ALGEBRAIC NUMBER FIELDS

Thesis for the Degree Of Ph. D.

MICHIGAN STATE UNIVERSITY
COLLEEN THEUSCH

1971

This is to certify that the

thesis entitled

DETERMINATION OF THE HILBERT CLASS FIELD

FOR CERTAIN ALGEBRAIC NUMBER FIELDS

presented by

C. THEUSCH

has been accepted towards fulfillment
of the requirements for

PH.D. degree in MATHEMATICS

Major professor

Date February 5, 1971

O-7639

ABSTRACT

DETERMINATION OF THE HILBERT CLASS FIELD
FOR CERTAIN ALGEBRAIC NUMBER FIELDS

By

Colleen Theusch

To each algebraic number field K is associated the Hilbert Class Field $CF(K)$. This Field $CF(K)$ is characterized as the (unique) maximal abelian unramified extension of K. $CF(K)/K$ is of degree h where h is the order of the ideal class group of K, that is, $h = h(K)$ is the class number of the field K.

In general the determination of the Hilbert Class Field of K is a very difficult problem. In this thesis the properties of the number discriminant of an element are employed to explicitly determine the Hilbert Class Field of some quadratic number fields. Then localization techniques are used to determine the Hilbert Class Field of certain non-normal algebraic number fields. A characterization of the pure fields (fields of the form $Q(\sqrt[n]{a})$) for which these techniques are valid is given through the theorems and corollaries.

DETERMINATION OF THE HILBERT CLASS FIELD FOR CERTAIN ALGEBRAIC NUMBER FIELDS

By

Colleen Theusch

A THESIS

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

DOCTOR OF PHILOSOPHY

Department of Mathematics

1971

ACKNOWLEDGMENTS

The author thanks her adviser, Professor Charles R. MacCluer, for his suggestions in the preparation of this thesis. She acknowledges useful discussions with various members of the department of mathematics, particularly with Professor Robert Spira. She thanks Edith Stern for her aid in proofreading. Finally, she wishes to express her gratitude to Philip Pfaff for his encouragement, understanding, typewriter and other arrangements.

TABLE OF CONTENTS

INTRODUCTION

To each algebraic number field K is associated the Hilbert Class Field $CF(K)$. This field $CF(K)$ is characterized as the (unique) maximal abelian unramified extension of K. $CF(K)/K$ is of degree h where h is the order of the ideal class group of K, that is, $h = h(K)$ is the class number of the field K.

In general the determination of the class field of K is a very difficult problem. The theory of complex multiplication presents an adequate, though rather involved, analytic method for determining the class fields of the imaginary quadratic fields. When K/Q is cyclic of prime degree n, $CF(K)$ may be abelian and hence identical with the genus field of K, the maximal abelian subfield of $CF(K)/Q$. Thus the method used to determine the genus field as found in [2] applies. However, even in these cases the explicit determination of the Hilbert Class Field is difficult since the necessary calculation of the class invariants and automorphisms is frequently extremely tedious.

In the second chapter of this thesis I will employ the properties of the number discriminant of an element to explicitly determine the Hilbert Class Field of some quadratic number fields. Localization techniques which can be used to explicitly determine the Hilbert Class Field of certain non-normal number fields are presented in the third chapter. A characterization of the pure fields (fields of the form $Q(\sqrt[n]{a})$) for which these techniques are valid is given through the theorems and corollaries.

CHAPTER I

BACKGROUND MATERIAL

In this chapter we will consider certain concepts which are basic to the understanding of the material in Chapters II and III.

We will be concerned here with algebraic number fields, that is, finite algebraic extensions of Q, the field of rational numbers. Any such extension K of Q can be obtained by adjoining to Q the root α of an irreducible monic polynomial $f(X)$ in $Q[X]$. The algebraic number α is referred to as a primitive element for the extension while $f(X) = 0$ is called the defining equation of α which is denoted by $f(X) = \text{Irr.}(\alpha,Q)$. These two concepts are defined similarly for an arbitrary algebraic number field $K = Q(\alpha)$ so that we have an extension $L = K(\beta)$ with $f(X) = \text{Irr.}(\beta,K)$ in $K[X]$.

To retain the notion of unique factorization in the algebraic number field K one considers the ideals of K rather than its elements. Following common practice we shall refer to a prime ideal of K simply as a finite prime.

Ramification of the primes of K in extensions of K plays a crucial role in class field theory.

Definition 1. A finite prime P of a field K ramifies in an extension L of K if it has a repeated factor in L, that is, if P extends to $Q_1^{e_1}\cdots Q_n^{e_n}$ with each Q_i prime in L and for which at least one e_i is greater than 1.

We state Kummer's Theorem here since it supplies one method for determining the factorization of all finite primes P of K in $L = K(\beta)$.

Kummer's Theorem. Let R be a Dedekind Domain with quotient field k, K a finite separable extension of k of degree n, and let $S = \text{int}_R K$ be the integers of K. Suppose K has an integral basis $1,\theta,\ldots,\theta^{n-1}$ over R. Let $f(X) = \text{Irr.}(\theta,k)$ and for a prime ideal P of R suppose $f(X) \equiv f_1^{e_1}(X)\cdots f_g^{e_g}(X) \pmod{P}$ where the $f_i(X)$ are all distinct monic R-polynomials which are irreducible modulo P. Then in S, P has the prime ideal factorization $SP = Q_1^{e_1}\cdots Q_g^{e_g}$ where $Q_i = (SP, f_i(\theta))$.

Consideration of some valuation theory will enable us to understand the ramification of the finite and infinite primes of K.

Definition 2. A valuation of the field K is a function ϕ from K into the non-negative reals such that

(i) $\phi(a) = 0$ if and only if $a = 0$

(ii) $\phi(ab) = \phi(a)\phi(b)$

(iii) There exists a real constant C such that $\phi(a) \leq 1$ implies $\phi(1+a) \leq C$.

An equivalent condition to (iii) is

(iiia) $\phi(a+b) \leq \phi(a) + \phi(b)$. [6].

Definition 3. $\|\phi\| = \inf. C$ where C runs over all constants of Definition 2, (iii) above is called the norm of ϕ.

Each valuation on a field determines a Hausdorff topology on that field. Those valuations which yield the same topology are considered equivalent and thus all valuations can be divided into equivalence classes. For convenience we shall refer to a complete equivalence class of valuations as a valuation. The equivalence classes are sometimes

also called prime divisors of the field K and thus each valuation $\phi:K \to R$ is associated with some prime divisor or prime P of K. If $\|\phi\| = 1$ we term ϕ a nonarchimedian valuation and the associated P is then a nonarchimedian or finite prime. On the other hand when $\|\phi\| > 1$, ϕ and P are called archimedian or infinite. We are primarily concerned with the latter here since we already have a method for determining the ramification of the finite primes in a given field.

Archimedian valuations are in a sense an extension of the concept of absolute value in a complex field. For consider any isomorphism $\sigma^{(i)}$ of K into the complex number field C. Galois theory assures us that there are exactly n such isomorphisms where n is the degree of K over Q. The image field of say r of these isomorphisms will be contained in the field of real numbers. The remaining $n-r$ occur in s conjugate pairs and have complex image fields. Clearly $n = r+2s$. We set $\phi^{(i)}(x) = |\sigma^{(i)}(x)|$ and note that this yields $r+s$ distinct valuations. As one would expect, the $\phi^{(i)}$ which correspond to those $\sigma^{(i)}$ which have real images are termed real valuations, the others being called complex valuations. The infinite primes $P_\infty^{(i)}$ are termed real or complex in accord with their

associated real or complex valuation $\phi^{(i)}$.

Now if $\phi^{(i)}$ is a real valuation of K which when extended to L becomes complex, we say that its associated prime $P_\infty^{(i)}$ has ramification index $e_i = 2$. In all other cases, that is, when $\phi^{(i)}$ remains real when extended or when $\phi^{(i)}$ is complex in K, the ramification index of the associated $P_\infty^{(i)}$ is 1. A fact that will be used repeatedly in what follows is that when K/k is unramified, so is KL/kL.

While discussing ramification we referred to class field theory. In the following pages we will be particularly interested in the Absolute or Hilbert Class Field of an algebraic number field $K = Q(\alpha)$.

Definition 4. The Hilbert Class Field of K is the (unique) maximal abelian unramified extension of K and is denoted by the symbol $CF(K)$, where unramified means unramified with respect to both finite and infinite primes. Such an extension $CF(K)$ exists as demonstrated by Furtwangler in 1903. [4].

Let I be the group of all fractional ideals and H the subgroup of principal ideals in K. The

order of I/H, the ideal class group of K, is called the class number of K denoted h(K). One of the standard facts of class field theory is that the degree of the extension CF(K) over K is equal to the class number of K.

The class number is an indication of how far the ring int K (the integers of K) is removed from being a principal ideal domain. In fact, h(K) is 1 if and only if int K is a principal ideal domain, in which case K is its own Hilbert Class Field. It is well known that while every ideal J of K when lifted to CF(K) becomes principal, CF(K) itself frequently contains non-principal ideals. This gives rise to the classical problem of class field towers. That is to ask, is the chain

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots ,$$

where each K_n is the Hilbert Class Field of K_{n-1}, necessarily finite? Clearly an affirmative answer to this question would imply that each such tower would have a principal ideal domain as one of its terms. However, this question was answered negatively by Golod and Safarevic in 1964. [5].

Generally it is extremely difficult to calculate the Hilbert Class Field of an algebraic number field. One criterion that may be used is that the Galois group G(CF(K)/K) is isomorphic to the

ideal class group I/H. Thus in those cases where this group has already been determined, considerations of extensions of K having this as Galois group may aid in the determination of the Hilbert Class Field of K, since if such an extension is found to be unramified, the uniqueness of $CF(K)$ insures the desired result.

Nevertheless, several inherent difficulties remain. Even when the composition of the ideal class group and consequently the class number is known, the actual production of the abelian unramified extension is problematic. Moreover for a wide range of fields even the class number itself has not yet been computed. Several tables of class numbers for quadratic, cubic, and cyclotomic fields are exhibited by Borevich and Shafarevich in [3]. All class numbers quoted in this thesis are taken from that reference.

As has already been indicated, the problem of calculating class fields involves proving that no prime of K can ramify in certain extensions under consideration. One method of achieving this is through the use of discriminants.

Let $L = K(\theta)$ be a finite separable extension of K and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ denote the n distinct K-isomorphisms of L into the algebraic closure of K. Let $\theta_j = \sigma_j(\theta)$, and

$$d_{L/K}(1,\theta,\ldots,\theta^{n-1}) = \begin{vmatrix} 1 & \theta & \theta^2 & \ldots & \theta^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ \vdots & & & & \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (\theta_i - \theta_j)^2$$

Definition 5. The element $d_{L/K}(1,\theta,\ldots,\theta^{n-1})$ will be called here the number discriminant of θ.

Discriminants are of importance in determining class fields since, according to Dedekind, any finite prime P of K that ramifies in L must divide every number discriminant $d_{L/K}(1,\theta,\ldots,\theta^{n-1})$. Thus in searching for unramified extensions L of K it is sufficient to show that there exist relatively prime number discriminants for two elements of L or to prove that those primes of K which divide any given number discriminant remain unramified in L. Both these methods will be employed in the following chapters.

We must consider cyclotomic fields since a cyclotomic extension of some algebraic number fields will yield the Hilbert Class Field $CF(K)$.

Definition 6. An extension of the rational field obtained by adjoining a primitive n-th root of unity is termed a cyclotomic number field.

Definition 7. $K(\alpha)$ is a cyclotomic extension of K if α is a primitive element for a subfield of a cyclotomic number field.

Let ζ_n be a primitive n-th root of unity. If K is an algebraic number field that meets $Q(\zeta_n)$ at Q, then $K(\zeta_n)$ is an extension of degree $\phi(n)$ over K. In particular, for $n = p$ (a prime) and any K which does not contain any subfield of $Q(\zeta_p)$ other than Q, $(K(\zeta_p):K) = p-1$. While every cyclotomic number field is abelian, only those for which $n = 2, 4, p^e$, and $2p^e$ with p an odd prime are cyclic.

The defining equation for $K(\zeta_p)$ is $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. If k is a subfield of $Q(\zeta_p)$ with index m, then $k = Q(\theta_p)$ where θ_p is of the form $\zeta_p + \zeta_p^{a} + \zeta_p^{a^2} + \cdots + \zeta_p^{a^{m-1}}$, $2 \leq a < p$, and conversely. For instance $Q(\zeta_p+\zeta_p^{-1})$ has index 2 in $Q(\zeta_p)$. Since $\overline{\zeta}_p = \zeta_p^{-1}$, $\zeta_p+\zeta_p^{-1}$ and all its conjugates are real. Thus $Q(\zeta_p+\zeta_p^{-1})$ is real as well as all its subfields. Since $Q(\zeta_p)$ is cyclic, $Q(\zeta_p+\zeta_p^{-1})$ is its only subfield of index 2. Thus all the subfields of $Q(\zeta_p)$ of odd degree are contained in $Q(\zeta_p+\zeta_p^{-1})$ and hence are real. When $p \equiv 1 \pmod 4$, $Q(\sqrt{p})$ is contained in $Q(\zeta_p)$ and $\sqrt{p}$ has defining equation $X^2 + X - (p-1)/4=0$, while for $p \equiv 3 \pmod 4$, $Q(\sqrt{-p})$ is the quadratic

subfield of $Q(\zeta_p)$ with defining equation $X^2 + X + (p+1)/4 = 0$.

Definition 8. Let $f(X) = 0$ be the defining equation of the integer β of $L = K(\beta)$ over K. The integer $f'(\beta)$ of L is called the number different of β over K.

The number discriminant of an integer is (within a sign) the norm of the number different. Further any prime P of L which is ramified over K divides every number different. Other useful facts are that

$$d(1,\zeta_p,\ldots,\zeta_p^{p-2}) = (-1)^{\binom{p-1}{2}} p^{p-2},$$

and that $f'(\zeta_p)$ divides p.

Thus the only primes P of $L = K(\zeta_p)$ which can ramify over K must divide p. Therefore when $H = K(\theta_p)$ is a subfield of L, the only primes of H which can ramify over K are those primes which are divisors of p, since if a prime ramifies in a subfield of L it must also ramify in L.

Since localization methods will be used to exhibit the Hilbert Class Field for some algebraic number fields, we consider some local field theory --- primarily that related to Q_p, the completion of the field Q of rational numbers with respect to a

p-adic valuation.

Definition 9. Let x be any rational number other than zero. Then for any prime p, $x = p^{\alpha}(a/b)$ where p divides neither of the integers a or b. Let

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-\alpha} & \text{if } x \neq 0. \end{cases}$$

The non-negative real valued function $|x| \to |x|_p$ is called the p-adic valuation on Q.

The function thus defined is clearly a valuation. Moreover for a p-adic valuation condition (iiia) may be replaced by the stronger

(iiib) $|a+b|_p \leq \max(|a|_p, |b|_p)$.

A p-adic valuation is non-archimedian as can be seen from (iiib) which yields $|a+1|_p \leq \max(|a|_p, |1|_p) = 1$ when $|a|_p \leq 1$. The ring of integers of Q_p is denoted by $O_p = \{a \text{ in } Q_p : |a|_p \leq 1\}$ while $P = \{a \text{ in } Q_p : |a|_p < 1\}$ is the unique prime ideal of Q_p. Since Q_p has only one prime ideal, consideration of the ramification which may occur in $Q_p(\alpha)$ is much simpler than that in an algebraic number field.

Definition 10. $Q_p(\alpha)/Q_p$ is totally ramified if P, the unique prime ideal of Q_p, has ramification

index in $Q_p(\alpha)$ equal to the degree of the extension.

From $(X-1)\Phi_p(X) \equiv (X-1)^p \pmod{p}$ it follows that $\Phi_p(X) \equiv (X-1)^{p-1} \pmod{p}$ where $\Phi_p(X)$ is the p-th cyclotomic polynomial and hence $Q_p(\zeta_p)$ is totally ramified by Kummer's Theorem.

Definition 11. $Q_p(\alpha)/Q_p$ is tamely ramified if p does not divide the degree of the extension.

Since the degree of $Q_p(\zeta_p)$ over Q_p is p-1, $Q_p(\zeta_p)/Q_p$ is tamely ramified.

We state one form of Hensel's Lemma.

Let R be a Dedekind Domain with quotient field k and let P be an integral prime ideal of R. Suppose that f(X) is a polynomial of R[X] such that for some a in R, $f(a) \equiv 0 \pmod{P}$ and $f'(a) \not\equiv 0 \pmod{P}$. Then f(X) = 0 has at least one (non-repeated) root in the local field k_p.

Hensel's Lemma implies that Q_p contains the (p-1)-th roots of 1 since

$$X^{p-1}-1 \equiv (X-1)(X-2)\ldots(X-(p-1)) \pmod{p}$$

so that $\Phi_{p-1}(X)$ must split completely in Q_p.

For our purpose one of the most crucial

aspects of local field theory is that the ramification index of a rational prime p of Q in an extension $Q(\alpha)$ is the same as the ramification index of the unique prime ideal P of $Q_p(\alpha)$ as has been shown by Artin.

CHAPTER II

DISCRIMINANTS DETERMINE CLASS FIELDS

In this section we shall see that the class field of $Q(\sqrt{m})$, for certain composite m, can be determined solely by consideration of relative number discriminants. We will list those fields with $|m| < 500$ to which the particular propositions apply.

Theorem 1. Let $m = pq > 0$ where p and q are distinct positive prime numbers with $p \equiv 1 \pmod 4$, and suppose $Q(\sqrt{m})$ has class number $h = 2$. Then

$$CF(Q(\sqrt{m})) = Q(\sqrt{p},\sqrt{q}).$$

Proof. We have already seen that a necessary condition that a finite prime of $K = Q(\sqrt{m})$ ramify in an extension of K is that it divide every relative number discriminant. Clearly $L = Q(\sqrt{p},\sqrt{q})$ is an extension of K of degree 2. Further $(1+\sqrt{p})/2$ and either $(1+\sqrt{q})/2$ or $\sqrt{q}$ (depending on whether or not $q \equiv 1 \pmod 4$) are

integral. Now we have the relative number discriminants for L/K:

$$d(1, (1+\sqrt{p})/2) = p$$

$$d(1, \sqrt{q}) = 4q$$

$$d(1, (1+\sqrt{q})/2) = q.$$

Since p and $4q$ are relatively prime, it is impossible for any finite prime of K to ramify in the extension L. Moreover since L is real, the archimedian primes of K also are unramified. Hence $Q(\sqrt{p},\sqrt{q})$ is unramified of degree $h = 2$ over $Q(\sqrt{m})$ and thus must be the Hilbert Class Field of $K = Q(\sqrt{m})$.

This theorem can be applied to a rather long list of real quadratic number fields. When $p \equiv 1 \pmod 4$ with $m = pq$, $Q(\sqrt{m})$ has class number 2 for the following m and hence for these m we have $CF(Q(\sqrt{m})) = Q(\sqrt{p},\sqrt{q})$.

m	p	q
10	5	2
15	5	3
26	13	2
34	17	2
35	5	7
39	13	3
51	17	3
55	5	11
58	29	2
65	5	13
74	37	2
85	5	17
87	29	3
91	13	7
95	5	19
106	53	2
111	37	3
115	5	23
119	17	7
122	61	2
123	41	3
143	13	11
146	73	2
155	5	31
159	53	3
178	89	2
183	61	3
185	5	37
187	17	11
194	97	2
202	101	2
203	29	7
205	5	41
215	5	43
218	109	2
221	13	17
247	13	19
259	37	7
265	5	53
267	89	3
287	41	7
295	5	59
298	149	2
299	13	23
303	101	3
305	5	61
314	157	2
319	29	11
327	109	3
335	5	67
339	113	3
355	5	71
362	181	2
365	5	73
371	53	7
377	13	29
386	193	2
391	17	23
394	197	2
395	5	79
403	13	31
407	37	11
411	137	3
415	5	83
447	149	3
451	41	11
458	229	2
466	233	2
471	157	3
481	13	37
482	241	2
485	5	97
493	19	29

Modification of the conditions placed on m yield several corollaries to the above theorem. The first of these concerns imaginary quadratic fields.

Corollary 1. Let $m = pq > 0$ where p and q are distinct positive prime numbers with $p \neq 2$ and such that $Q(\sqrt{-m})$ has class number 2. Then

$$CF(Q(\sqrt{-m})) = Q(\sqrt{p},\sqrt{-q}) \quad \text{if} \quad p \equiv 1 \pmod 4$$

$$CF(Q(\sqrt{-m})) = Q(\sqrt{-p},\sqrt{q}) \quad \text{if} \quad p \equiv 3 \pmod 4.$$

Proof. The finite primes of $Q(\sqrt{-m})$ other than p cannot ramify in the extension since we have

$$d(1, (1+\sqrt{p})/2) = p \quad \text{if} \quad p \equiv 1 \pmod 4$$

$$d(1, (1+\sqrt{-p})/2 = -p \quad \text{if} \quad p \equiv 3 \pmod 4.$$

But neither can the (repeated) prime factor of p in $Q(\sqrt{-m})$ ramify in the extension since $p \neq 2$ and $d(1, \sqrt{q}) = 4q$. The archimedian primes of $Q(\sqrt{-m})$ are already complex and hence are no cause for concern. The result follows as in the theorem.

As examples of this we have $CF(Q(\sqrt{-m})) = Q(\sqrt{p},\sqrt{-q})$ or $Q(\sqrt{-p},\sqrt{q})$ for the following m.

m	p	q	m	p	q
6	3	2	91	7	13
10	5	2	115	5	23
15	3	5	123	3	41
22	11	2	187	11	17
35	5	7	235	5	47
51	3	17	267	3	89
58	29	2	403	31	13
			427	7	61

Returning again to the case of the real quadratic fields we have

Corollary 2. Let $m = pqr > 0$ where p, q, and r are distinct positive prime numbers with $p \equiv 1 \pmod 4$ and neither q nor $r \equiv 1 \pmod 4$. Suppose that the class number of $Q(\sqrt{m})$ is 2. Then

$$CF(Q(\sqrt{m})) = Q(\sqrt{p},\sqrt{qr}).$$

Proof. For the integers $(1+\sqrt{p})/2$, $\sqrt{qr}$, and $(1+\sqrt{qr})/2$ of $Q(\sqrt{p},\sqrt{qr})$ we have the relative number discriminants over $Q(\sqrt{m})$ equal to p, $4qr$, and qr respectively. Since p and $4qr$ are relatively prime and since $Q(\sqrt{p},\sqrt{qr})$ contains only real infinite primes, $Q(\sqrt{p},\sqrt{qr})$ is an unramified extension of degree 2 over $Q(\sqrt{m})$ and hence its Hilbert Class Field.

As a result of this corollary we have

$CF(Q(\sqrt{m})) = Q(\sqrt{p},\sqrt{qr})$ for the following m.

m	p	q	r	m	p	q	r
30	5	2	3	285	5	3	19
70	5	2	7	286	13	2	11
78	13	2	3	310	5	2	31
102	17	2	3	318	53	2	3
105	5	3	7	345	5	3	23
110	5	2	11	357	17	3	7
165	5	3	11	366	61	2	3
174	29	2	3	374	17	2	11
182	13	2	7	385	5	7	11
190	5	2	19	406	29	2	7
222	37	2	3	429	13	3	11
230	5	2	23	430	5	2	43
238	17	2	7	465	5	3	31
246	41	2	3	470	5	2	47
273	13	3	7	494	13	2	19

Further changes in the hypotheses of the theorem give the final result of this section as

Corollary 3. Let $m = 2pq > 0$ where p and q are distinct odd positive primes with $p,q \equiv 3 \pmod 4$. Moreover let the class number of $Q(\sqrt{m})$ be 2. Then

$$CF(Q(\sqrt{m})) = Q(\sqrt{2},\sqrt{pq}).$$

Proof. Since $p,q \equiv 3 \pmod 4$ we have $pq \equiv 1 \pmod 4$. Thus $(1+\sqrt{pq})/2$ and $\sqrt{2}$ are integers of $Q(\sqrt{2},\sqrt{pq})$ with $d(1, (1+\sqrt{pq})/2) = pq$ while $d(1, \sqrt{2}) = 4$. Moreover all archimedian

primes remain real. Hence the conclusion follows immediately.

Since the class number of $Q(\sqrt{m})$ is 2 for the following m, we have $CF(Q(\sqrt{m})) = Q(\sqrt{2},\sqrt{pq})$ for these m.

m	2 p q	m	2 p q
42	2 3 7	282	2 3 47
66	2 3 11	354	2 3 59
114	2 3 19	402	2 3 67
138	2 3 23	418	2 11 19
154	2 7 11	426	2 3 71
186	2 3 31	474	2 3 79
258	2 3 43	498	2 3 83
266	2 7 19		

CHAPTER III

HILBERT CLASS FIELDS THROUGH LOCALIZATION TECHNIQUES

We now turn our attention to a more interesting class of fields --- the pure fields, that is, those of the form $Q(\sqrt[n]{a})$. Since the rationals do not contain the n-th roots of unity for $n \neq 2$ the pure fields are never normal over the rationals when $n \neq 2$. In order to determine the class fields of certain of these we will employ localization techniques. The lemmas that follow are the foundation of the technique.

Lemma A. Let p be a positive rational prime number and ζ_p a primitive p-th root of unity. Then $Q_p(\zeta_p) = Q_p(\sqrt[p-1]{-p})$ where Q_p denotes the field of p-adic rational numbers.

Proof. Since $Q_p(\zeta_p)/Q_p$ is tamely and totally ramified we have that $Q_p(\zeta_p) = Q_p(\sqrt[p-1]{\varepsilon p})$ for some unit ε of Q_p. But in fact, $-p = -u(1-\zeta)^{p-1}$ where $-u \equiv -(p-1)! \equiv 1 \bmod (1-\zeta)$. But then by

Hensel's Lemma there exists a unit ε in Q_p such that $\varepsilon^{p-1} = -u$.

Corollary. $Q_p(\sqrt[p-1]{-p})/Q_p$ is cyclic, and tamely and totally ramified.

Proof. Q_p contains the (p-1)-th roots of unity.

Lemma B. If h is an odd divisor of p-1, then $Q_p(\sqrt[h]{p}) = Q_p(\theta)$ where θ is a primitive element for the h-th degree subfield of $Q(\zeta_p)$.

Proof. Clearly $Q_p(\sqrt[h]{p}) = Q_p(\sqrt[h]{-p})$ since h is odd. $Q_p(\zeta_p)$ is a cyclic extension of Q_p and thus contains only one subfield of degree h. This, together with Lemma A, yields the conclusion.

We are now in a position to prove our first theorem concerning some fields which are not normal over the rationals. Direct application of this theorem will enable us to actually display the Hilbert Class Field of certain fields of this type for which the class number is known.

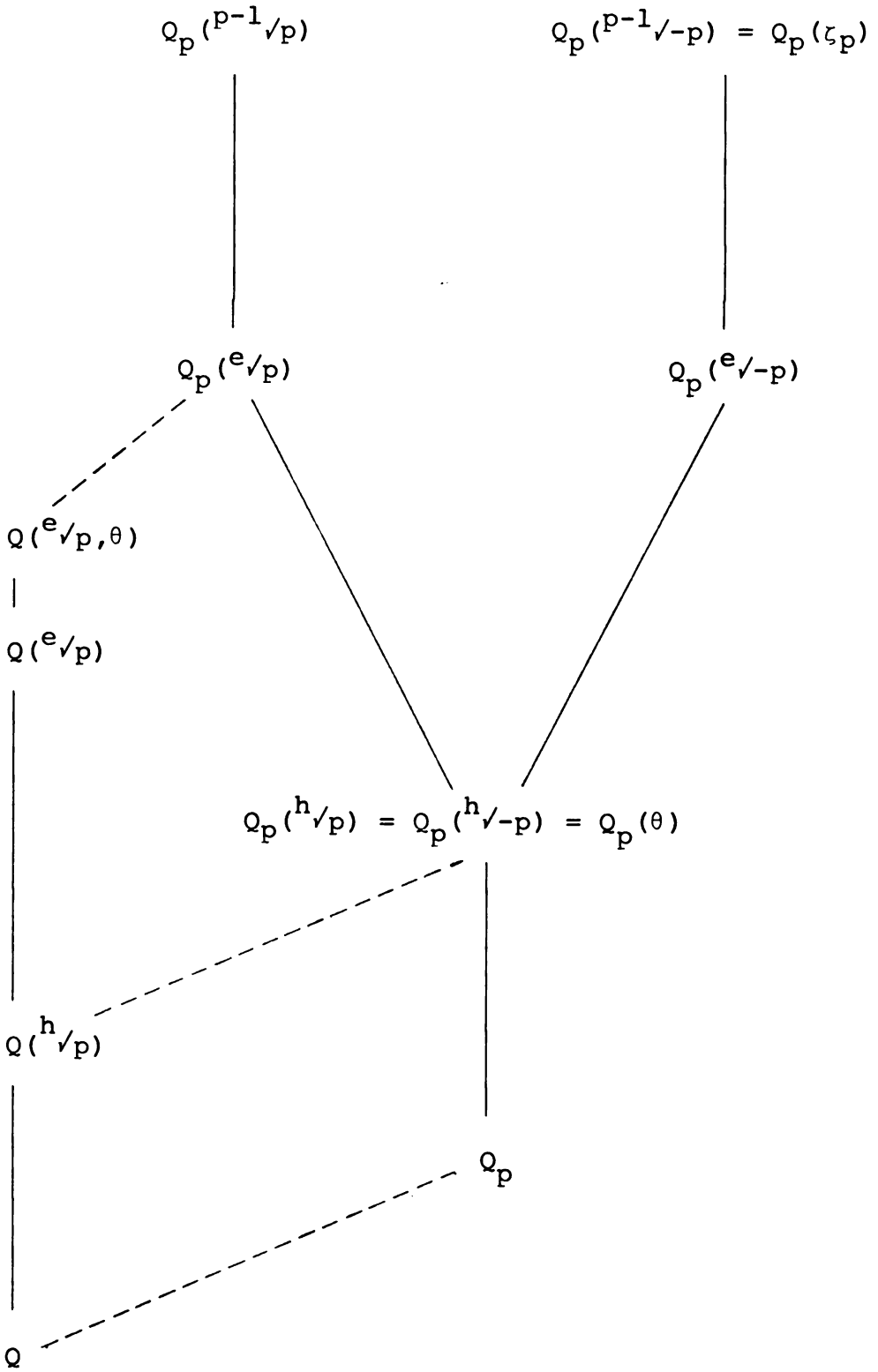
Theorem 2. Let the class number h of $Q(\sqrt[e]{p})$ be odd and let h be a divisor of e. Then if $p \equiv 1 \pmod{e}$ we have

$$CF(Q(\sqrt[e]{p})) = Q(\sqrt[e]{p},\theta)$$

where θ is a primitive element for the unique subfield of degree h of the cyclotomic field $Q(\zeta_p)$.

Proof. Since the discriminant of the number ζ_p over Q is a power of p, it is clear that the only finite prime of $Q(\sqrt[e]{p})$ that can ramify in the extension $Q(\sqrt[e]{p},\zeta_p)$ and hence in $Q(\sqrt[e]{p},\theta)$ is $\sqrt[e]{p}$. But not even $\sqrt[e]{p}$ can ramify. For by Hensel's Lemma, Q_p contains the $(p-1)$-th roots of unity and hence also the e-th roots of unity. Thus, locally, $Q_p(\sqrt[e]{p})/Q_p$ is normal, in fact, cyclic. Since h is odd and divides e, $Q_p(\sqrt[e]{p})$ contains $Q_p(\sqrt[h]{p})$. On the other hand, $Q_p(\sqrt[h]{p}) = Q_p(\theta)$ by Lemma B. The fact that global ramification can be determined by local ramification indicates that the ramification index of p in $Q(\sqrt[e]{p},\theta)$ as well as in $Q(\sqrt[e]{p})$ is e. Hence $\sqrt[e]{p}$ does not ramify in the given extension.

Consideration of the following diagram should help clarify the preceding statements.


$Q_p(\sqrt[p-1]{p})$
$Q_p(\sqrt[p-1]{-p}) = Q_p(\zeta_p)$
$Q_p(\sqrt[e]{p})$
$Q_p(\sqrt[e]{-p})$
$Q(\sqrt[e]{p},\theta)$
$Q(\sqrt[e]{p})$
$Q_p(\sqrt[h]{p}) = Q_p(\sqrt[h]{-p}) = Q_p(\theta)$
$Q(\sqrt[h]{p})$
Q_p
Q

Now that we have disposed of the finite primes we will consider the infinite primes $P_\infty^{(i)}$ in $Q(\sqrt[e]{p})$. The only $P_\infty^{(i)}$ which could ramify in the extension are those associated with the real archimedian valuations $\phi^{(i)}$ of $Q(\sqrt[e]{p})$. Now since $Q(\theta)/Q$ is galois and of odd degree h, $Q(\theta)$ is a real field. Hence θ and all its conjugates are also real. Thus the extensions of the real $\phi^{(i)}$ are real in $Q(\sqrt[e]{p},\theta)$, and hence none of the $P_\infty^{(i)}$ ramify.

Thus $Q(\sqrt[e]{p},\theta)$ is an abelian unramified extension of $Q(\sqrt[e]{p})$ of degree h and is therefore the Hilbert Class Field.

We have now arrived at a position from which we can specify the Hilbert Class Field for specific pure fields. Since $k = Q(\sqrt[3]{p})$ has class number 3 for $p = 7, 13, 19, 31,$ and 37 [3] the Hilbert Class Field of k is $k(\theta)$ where θ is a primitive element for the cubic subfield of $Q(\zeta_p)$. In particular we have

$$CF(Q(\sqrt[3]{7}))=Q(\sqrt[3]{7},\zeta_7+\zeta_7^6)$$

$$CF(Q(\sqrt[3]{13}))=Q(\sqrt[3]{13},\zeta_{13}+\zeta_{13}^5+\zeta_{13}^8+\zeta_{13}^{12})$$

$$CF(Q(\sqrt[3]{19}))=Q(\sqrt[3]{19},\zeta_{19}+\zeta^7+\zeta^8+\zeta^{11}+\zeta^{12}+\zeta^{18})$$

$$CF(Q(\sqrt[3]{31}))=Q(\sqrt[3]{31},\zeta_{31}+\zeta^2+\zeta^4+\zeta^8+\zeta^{15}+\zeta^{16}+\zeta^{23}+\zeta^{27}+\zeta^{29}+\zeta^{30})$$

$$CF(Q(\sqrt[3]{37}))=Q(\sqrt[3]{37},\zeta_{37}+\zeta^6+\zeta^8+\zeta^{10}+\zeta^{11}+\zeta^{14}+\zeta^{23}+\zeta^{26}+\zeta^{27}+\zeta^{29}+\zeta^{31}+\zeta^{36}).$$

We note the corresponding defining equations which yield these extensions.

$$\text{Irr}(\theta, Q(\sqrt[3]{7})) = X^3 + X^2 - 2X - 1$$

$$\text{Irr}(\theta, Q(\sqrt[3]{13})) = X^3 + X^2 - 4X + 1$$

$$\text{Irr}(\theta, Q(\sqrt[3]{19})) = X^3 + X^2 - 6X - 7$$

$$\text{Irr}(\theta, Q(\sqrt[3]{31})) = X^3 + X^2 - 10X - 8$$

$$\text{Irr}(\theta, Q(\sqrt[3]{37})) = X^3 + X^2 - 12X + 11$$

We continue with

Lemma C. If e is even and $p \equiv 1 \pmod{2e}$, then $Q_p(\sqrt[e]{p}) = Q_p(\sqrt[e]{-p})$.

Proof. We have already seen that Q_p contains the $(p-1)$-th roots of unity. Thus under the hypotheses, Q_p contains the $2e$-th roots of unity and hence also the e-th roots of -1. The conclusion is immediate.

Lemma D. $Q_p(\zeta_p)$ contains $Q_p(\sqrt[e]{p})$ when both e is even and $p \equiv 1 \pmod{2e}$.

Proof. We first note that since $p \equiv 1 \pmod{2e}$, $Q_p(\sqrt[p-1]{-p})$ contains $Q_p(\sqrt[e]{-p})$. Then Lemma C followed by Lemma A yields

$$Q_p(\sqrt[e]{p}) = Q_p(\sqrt[e]{-p}) = Q_p(\theta) \subset Q_p(\zeta_p)$$

where θ is a primitive element for the e-th degree

subfield of $Q(\zeta_p)$.

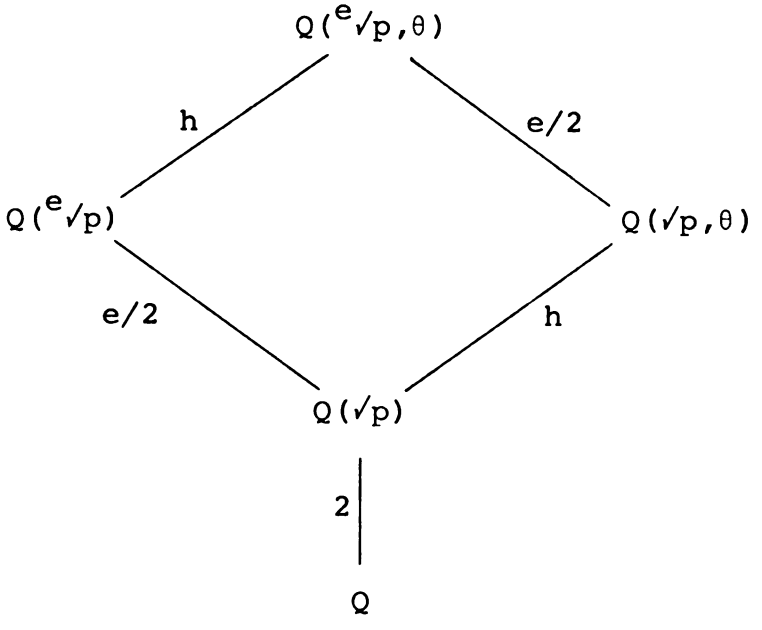
The preceding lemmas enable us to prove

Theorem 3. Let $p \equiv 1 \pmod{2e}$ and suppose $Q(\sqrt[e]{p})$ has class number h with $e \equiv 0 \pmod{2h}$. Then

$$CF(Q(\sqrt[e]{p})) = Q(\sqrt[e]{p},\theta)$$

where θ is a primitive element for the h-th degree extension of $Q(\sqrt{p})$ in $Q(\zeta_p)$.

Proof. The stated hypotheses imply that $p \equiv 1 \pmod{4}$. Since $Q(\zeta_p)$ contains $Q(\sqrt{p})$ when $p \equiv 1 \pmod{4}$, $Q(\sqrt[e]{p},\theta)$ is an extension of $Q(\sqrt[e]{p})$ of degree h.



Clearly $\sqrt[e]{p}$ is the only finite prime of $Q(\sqrt[e]{p})$ that can possibly ramify in $Q(\sqrt[e]{p},\theta)$. To see that this in fact cannot occur, we again localize at p. From Lemma D we have that $Q_p(\zeta_p)$ contains $Q_p(\sqrt[e]{p})$ with the unique subfield $Q_p(\sqrt{p},\theta) = Q_p(\sqrt[2h]{p})$ of degree $2h$. Since $e \equiv 0 \pmod{2h}$, $Q_p(\sqrt[e]{p})$ contains $Q_p(\sqrt{p},\theta)$.

The following diagram illustrates the above containments.

$$
\begin{array}{c}
Q_p(\zeta_p) = Q_p(\sqrt[p-1]{-p}) \\
\Big| \quad (p-1)/2 = 2m \\
Q_p(\sqrt[e]{p}) = Q_p(\sqrt[e]{-p}) \\
\Big| \quad e/2h \\
Q_p(\sqrt[2h]{p}) = Q_p(\sqrt{p},\theta) \\
\Big| \quad h \\
Q_p(\sqrt{p}) \\
\Big| \quad 2 \\
Q_p
\end{array}
$$

The local ramification index e of p in $Q_p(\sqrt[e]{p})$ indicates that the global ramification index of p in $Q(\sqrt[e]{p},\theta)$ must also be e. Hence $\sqrt[e]{p}$ does not ramify in the extension.

Since the degree of $Q(\zeta_p)/Q(\theta)$ is even, $Q(\theta)$ is real. Thus all the conjugates of θ are real, and hence the infinite primes of $Q(\sqrt[e]{p})$ have ramification index 1 in $Q(\sqrt[e]{p},\theta)$. Thus the Hilbert Class Field of $Q(\sqrt[e]{p})$ is indeed $Q(\sqrt[e]{p},\theta)$.

Clearly Theorems 2 and 3 are also valid for $Q(\sqrt[e]{p^a})$ where a and e are relatively prime since in that case $Q(\sqrt[e]{p}) = Q(\sqrt[e]{p^a})$.

When $p \equiv 1 \pmod 4$, $Q(\zeta_p)$ does <u>not</u> contain $Q(\sqrt{-p})$. Thus the hypothesis $e \equiv 0 \pmod{2h}$ of Theorem 3 can be omitted to obtain

<u>Corollary 1</u>. Let $p \equiv 1 \pmod{2e}$ with $e \equiv 0 \pmod 2$, and suppose that $Q(\sqrt[e]{-p})$ has class number h where h divides e. Then

$$CF(Q(\sqrt[e]{-p})) = Q(\sqrt[e]{-p},\theta)$$

where θ is a primitive element for the h-th degree subfield of $Q(\zeta_p)$.

Proof. Since e is even the archimedian

primes in $Q(\sqrt[e]{-p})$ are already complex and therefore cannot further ramify. Moreover the hypotheses imply that $p \equiv 1 \pmod 4$. Since $p \equiv 1 \pmod{2e}$, $Q_p(\sqrt[e]{-p})$ is cyclic over Q_p by Lemma C. Application of Lemma A yields $Q_p(\theta) = Q_p(\sqrt[h]{-p})$ as the unique subfield of $Q_p(\sqrt[e]{-p})$ of degree h.

As a special application of the above we have

Corollary 2. Let $p \equiv 1 \pmod 4$ be such that $Q(\sqrt{-p})$ has class number 2. Then

$$CF(Q(\sqrt{-p})) = Q(\sqrt{-p},\sqrt{p}) = Q(i,\sqrt{p}).$$

Proof. $Q(\sqrt{p})$ is the quadratic subfield of $Q(\zeta_p)$ when $p \equiv 1 \pmod 4$.

For $p = 5$, 13, and 37, $Q(\sqrt{-p})$ has class number 2. Hence

$$CF(Q(\sqrt{-5})) = Q(i, \sqrt{5})$$
$$CF(Q(\sqrt{-13})) = Q(i,\sqrt{13})$$
$$CF(Q(\sqrt{-37})) = Q(i,\sqrt{37}).$$

The radicands of the pure fields we have considered up to this point have all been primes.

The theory can be extended to include certain composite radicands. To begin this we shall deal with cubic extensions of the rationals.

Lemma E. Let a,b be in Q_p^* (the multiplicative group of the non-zero elements of Q_p) but not in Q_p^{*3}. Then when a/b is an element of Q_p^{*3}, $Q_p(\sqrt[3]{a}) = Q_p(\sqrt[3]{b})$.

Proof. Clear.

Lemma F. Let the rational integer r be a cubic residue modulo p with p a positive rational prime distinct from 3. Then $Q_p(\sqrt[3]{p}) = Q_p(\sqrt[3]{rp})$.

Proof. By Hensel's Lemma, r is in Q_p^{*3} and $rp/p = r$.

Theorem 4. Let $p \equiv 1 \pmod 3$ and let r be a cubic residue modulo p. Suppose $h(Q(\sqrt[3]{rp})) = 3$. Then

$$CF(Q(\sqrt[3]{rp})) = Q(\sqrt[3]{rp},\theta)$$

where θ is a primitive element for the cubic subfield of $Q(\zeta_p)$.

Proof. As we have observed before, $\sqrt[3]{p}$ is the only finite prime that could ramify in the

extension $Q(\sqrt[3]{rp},\theta)$ of $Q(\sqrt[3]{rp})$. Localizing at p we see that since $p \equiv 1 \pmod 3$, Q_p contains the cube roots of unity. Hence $Q_p(\sqrt[3]{p})/Q_p$ is cyclic and from Lemma F it follows that $Q_p(\sqrt[3]{rp})/Q_p$ is also cyclic since r is a cubic residue modulo p. Moreover, application of Lemmas F and B yield $Q_p(\sqrt[3]{rp}) = Q_p(\theta)$. Thus globally p has ramification index 3 in $Q(\sqrt[3]{rp},\theta)$ which is also its index in $Q(\sqrt[3]{rp})$.

Since $Q(\theta)/Q$ is galois and of odd degree, $Q(\theta)$ is a real field. Therefore the real archimedian primes of $Q(\sqrt[3]{rp})$ extend to real primes in $Q(\sqrt[3]{rp},\theta)$. Hence $Q(\sqrt[3]{rp},\theta)$ is an abelian unramified extension of $Q(\sqrt[3]{rp})$ of degree 3 and is therefore the Hilbert Class Field.

For instance note that $Q(\sqrt[3]{42})$ has class number 3. Thus $CF(Q(\sqrt[3]{42})) = Q(\sqrt[3]{42},\theta)$ where θ is a primitive element for the cubic subfield of $Q(\zeta_p)$. That is, $CF(Q(\sqrt[3]{42})) = Q(\sqrt[3]{42},\zeta_7+\zeta_7^6)$, with defining equation $Irr(\theta, Q(\sqrt[3]{42})) = X^3 + X^2 - 2X - 1$.

It can readily be seen that in Lemmas E and F and in Theorem 4, the prime 3 can be replaced by any odd $q \neq p$ so that we have

Theorem 4a. Let $p \equiv 1 \pmod q$ and

$q \equiv 1 \pmod 2$. Further let r be a q-th power residue modulo p, and suppose that $h(Q(\sqrt[q]{rp})) = q$. Then

$$CF(Q(\sqrt[q]{rp})) = Q(\sqrt[q]{rp},\theta)$$

where θ is a primitive element for the q-th degree subfield of $Q(\zeta_p)$.

A very slight modification in the hypotheses yields

Theorem 4b. Let $p \equiv 1 \pmod{2q}$ with $q \equiv 0 \pmod 2$ and let the positive rational integer r be a q-th power residue modulo p. Suppose that $h(Q(\sqrt[q]{-rp})) = q$. Then

$$CF(Q(\sqrt[q]{-rp})) = Q(\sqrt[q]{-rp},\theta)$$

where θ is a primitive element for the q-th degree subfield of $Q(\zeta_p)$.

Proof. Since r is a q-th power residue we have $Q_p(\sqrt[q]{-rp}) = Q_p(\sqrt[q]{-p})$, while the first corollary to Theorem 3 assures us that $Q_p(\sqrt[q]{-p}) = Q_p(\sqrt[q]{-p},\theta)$. Hence the finite primes of $Q(\sqrt[q]{-rp})$ do not ramify in $Q(\sqrt[q]{-rp},\theta)$. Since the

archimedian primes of $Q(\sqrt[q]{-rp})$ are complex, no ramification can occur.

Similarly we have

Theorem 4c. Let $p \equiv 1 \pmod{2q}$ with $q \equiv 0 \pmod{2}$ and let $r > 0$ be a q-th power residue modulo p. Suppose that $h(Q(\sqrt[q]{rp})) = q$. Then

$$CF(Q(\sqrt[q]{rp})) = Q(\sqrt[q]{rp},\theta)$$

θ as before.

Proof. We need only note that since $p \equiv 1 \pmod{2q}$ Q_p contains the q-th roots of -1. Thus $Q_p(\sqrt[q]{rp}) = Q_p(\sqrt[q]{-rp}) = Q_p(\sqrt[q]{-p}) = Q_p(\sqrt[q]{-p},\theta)$. The last equality is a result of Lemma A. Regarding the infinite primes, we need only observe that since $(p-1)/q$ is even, $Q(\theta)$ must be real.

BIBLIOGRAPHY

BIBLIOGRAPHY

1 Bachman, George, Introduction to p-adic Numbers and Valuation Theory, Academic Press, New York, 1964.

2 Borel,A., Chowla,S., Herz,C.S., Iwasawa,K., and Serre,J-P., Seminar on Complex Multiplication, Springer-Verlag, Berlin, 1966.

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

4 Furtwangler, Philip, "Allgemeiner Existenzbeweis fur den Klassenkorper eines beliebigen algebraischen Zahlkorpers", Mathematische Annalen, 63, 1909, pp.1-37.

5 Golod,E.S., and Safarevic,I.R., "On Class Field Towers" (Russian), Izv. Akad. Nauk. SSSR 28, 1964, pp.261-272, English translation in Am. Math. Soc. Transl. (2) 48, pp.91-102.

6 Weiss, Edwin, Algebraic Number Theory, McGraw-Hill Book Company, New York, 1963.