

This dissertation has been 65-9918  
microfilmed exactly as received

NYMANN, James Eugene, 1938-  
IDEAL STRUCTURE OF RELATIVE QUADRATIC  
FIELDS ARISING FROM FIXED POINTS OF THE  
HILBERT MODULAR GROUP.

University of Arizona, Ph.D., 1965  
Mathematics

University Microfilms, Inc., Ann Arbor, Michigan

Ideal Structure of Relative Quadratic Fields  
Arising from Fixed Points of the Hilbert Modular Group

by  
James E. <sup>August</sup> Nymann

---

A Dissertation Submitted to the Faculty of the  
DEPARTMENT OF MATHEMATICS  
In Partial Fulfillment of the Requirements  
for the Degree of  
DOCTOR OF PHILOSOPHY  
In the Graduate College  
THE UNIVERSITY OF ARIZONA

1965

THE UNIVERSITY OF ARIZONA

GRADUATE COLLEGE

I hereby recommend that this dissertation prepared under my direction by James E. Nymann entitled "Ideal Structure of Relative Quadratic Fields Arising from Fixed Points of the Hilbert Modular Group" be accepted as fulfilling the dissertation requirement of the degree of Doctor of Philosophy

Harry Cole  
Dissertation Director

23 April 65  
Date

After inspection of the dissertation, the following members of the Final Examination Committee concur in its approval and recommend its acceptance:\*

Ronald Jacobowitz  
Louis C. Hen  
Donald S. Rogers  
Mark ...

April 26, 1965  
April 25, 1965  
April 23, 1965  
April 26, 1965

\*This approval and acceptance is contingent on the candidate's adequate performance and defense of this dissertation at the final oral examination. The inclusion of this sheet bound into the library copy of the dissertation is evidence of satisfactory performance at the final examination.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: James E. Hyman

## ACKNOWLEDGMENTS

The author would like to express his appreciation to Professor Harvey Cohn whose assistance and kindly encouragement were of extreme value in the development of this paper.

This paper was prepared partially under the sponsorship of the National Science Foundation Grant number GP-2141.

## ABSTRACT

The principal result gives a Minkowskian bound on the norms of ideals in ideal classes of certain fourth degree extensions of the rationals. Let  $K_1$  denote a real quadratic extension of the rationals with class number 1 and let  $\mu_0 = \tau^2 - 4\epsilon \ll 0$ , where  $\tau$  and  $\epsilon$  (unit) are integers in  $K_1$ . Then  $K_2 = K_1(\sqrt{\mu_0})$  will be called a fixed point field. The main result states:

Every ideal class of a fixed point field contains an ideal of norm less than or equal to  $N^{\frac{1}{2}}(\mu_0)/4H_1$ , where  $H_1 = \inf \{x: x = \text{Im}z\text{Im}z' \text{ for } (z, z') \text{ a fixed point in the fundamental domain of the Hilbert modular group for } K_1\}$ .

The above result is obtained by using a generalization of the classical result of Fermat, which states that the solvability of  $x^2 + 1 \equiv 0 \pmod{m}$  implies the solvability of  $x^2 + y^2 = m$  in rational integers. Using the notation above, this generalization, which is due to H. Cohn, states:

The solvability of  $\xi^2 - \tau\xi + \epsilon \equiv 0 \pmod{\gamma}$  implies the solvability of  $\xi_1^2 - \tau\xi_1\xi_2 + \epsilon\xi_2^2 = \gamma\gamma_2$  in integers

in  $K_1$  with  $|N(\gamma_2)| \leq N^{\frac{1}{2}}(\mu_0)/4H_1$ .

With the aid of the Minkowskian bound the class number of several fixed point fields is determined.

It is also proven that all fixed point fields are normal. A theorem characterizing units in fixed point fields is also given.

## TABLE OF CONTENTS

	Page
TITLE PAGE	1
STATEMENT BY AUTHOR	11
ACKNOWLEDGMENTS	111
ABSTRACT	iv
CHAPTER:	
I.  The Hilbert Modular Group	
1.  Definitions	1
2.  Fixed Points	3
II. Relative Quadratic Fields	
3.  Basis Theorem	8
4.  Discriminant	11
5.  Factorization of Primes	14
6.  Galois Group	21
III. Fixed Point Fields	
7.  Normality of Fixed Point Fields	23
8.  Existence of Fixed Point Fields	27
9.  Minkowskian Bound	29
10. Units	32
IV.  Class Number of Fixed Point Fields	
11. Determination of Class Number	35
12. Class Number Unequal to 1	40
13. Concluding Remarks	44
TABLE I	45
TABLE II	47
REFERENCES	48

1. Definitions

The Hilbert modular group  $H$  for a totally real field  $K$  of degree  $n$  over the rationals  $\mathbb{Q}$  with conjugate fields  $K', K'', \dots, K^{(n-1)}$  is the group of transformations  $T$  such that

$$(1) \quad T(z, z', \dots, z^{(n-1)}) = \left( \frac{\alpha z + \beta}{\gamma z + \delta}, \frac{\alpha' z' + \beta'}{\gamma' z' + \delta'}, \dots, \frac{\alpha^{(n-1)} z^{(n-1)} + \beta^{(n-1)}}{\gamma^{(n-1)} z^{(n-1)} + \delta^{(n-1)}} \right)$$

where  $(z, z', \dots, z^{(n-1)}) \in UxU'x \dots xU^{(n-1)}$ ,  $U, U', \dots, U^{(n-1)}$  denote  $n$  copies of the upper half of the complex plane,

$\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$  (the integers in  $K$ ) and  $\alpha\delta - \beta\gamma = \epsilon$  (a totally positive unit). In the following  $z$  will be used instead of  $(z, z', \dots, z^{(n-1)})$  and (1) will be written

$$T(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$$

$R \subset UxU'x \dots xU^{(n-1)}$  will be said to be a fundamental domain for the Hilbert modular group  $H$  if for every  $z \in UxU'x \dots xU^{(n-1)}$  there exists a  $T \in H$  such that  $T(z) \in R$  and if  $z_1, z_2 \in R$  are such that  $T(z_1) = T(z_2)$  for some  $T \in H$  then  $z_1$  and  $z_2$  are on the boundary of  $R$ .  $H_0 = H_0(K)$  will be defined to be  $\inf \{x: x = \text{Im}z \cdot \text{Im}z' \dots \text{Im}z^{(n-1)} \text{ for } (z, z', \dots, z^{(n-1)}) \text{ belonging to the fundamental domain of the Hilbert modular group over } K\}$ .

The following theorem due to H. Cohn [ 2 ] , which gives a lower bound for  $H_0$  in the quadratic case, will be used below.

THEOREM 1. If  $K$  is a real quadratic field with class number 1, then  $H_0 > \frac{2}{d}$  where  $d$  is the discriminant of  $K$ .

In the following  $K$  will be assumed to have class number 1. This is done so that we will have  $H_0 > 0$ , as shown by Maass [ 5 ] .

## 2. Fixed Points

A point  $z$  will be said to be a fixed point of the Hilbert modular group  $H$  if there exists a  $T \in H$  such that  $T(z) = z$  and  $T$  is not the identity element of  $H$ . We will let  $H_1 = H_1(K) = \inf \{x: x = \text{Im}z \cdot \text{Im}z' \cdots \text{Im}z^{(n-1)} \text{ with } (z, z', \dots, z^{(n-1)}) \text{ a fixed point belonging to the fundamental domain of the Hilbert modular group.}\}$  It is clear that  $H_1 \supseteq H_0$ . The following lemma characterizes fixed points.

LEMMA 1. The most general fixed point is

$$(2) \quad z_0 = \frac{-\xi + i\sqrt{\Delta} \text{sgn}\gamma}{2\gamma}$$

where for a unit  $\epsilon$  and  $\tau \in \mathcal{O}_K$ ,

$$(3) \quad \Delta = 4\epsilon - \tau^2 \gg 0$$

$$(4) \quad \xi^2 + \Delta \equiv 0 \pmod{4\gamma}.$$

Proof. If  $z_0$  is as given in the lemma, the transformation that leaves  $z_0$  fixed is given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \epsilon \end{pmatrix} = \begin{pmatrix} \frac{\tau - \xi}{2\gamma} & \frac{\xi^2 + \Delta}{4\gamma} \\ \gamma & \frac{\tau + \xi}{2} \end{pmatrix}$$

which are all in  $0_K$  since (3) and (4) give us  $\xi^2 \equiv \tau^2 \pmod{4}$  and hence  $\xi \equiv \tau \pmod{2}$ .

Now suppose  $\frac{\alpha z_0 + \beta}{\gamma z_0 + \delta} = z_0$ . Then  $\gamma z_0^2 + (\delta - \alpha)z_0 - \beta = 0$  and

$$z_0 = \frac{-\delta + \alpha \pm \sqrt{\delta^2 - 2\alpha\delta + \alpha^2 + 4\gamma\beta}}{2\gamma}.$$

Therefore for  $z_0$  to be in the upper half plane

$$z_0 = \frac{-\xi + i\sqrt{\Delta} \operatorname{sgn} \gamma}{2\gamma}$$

where  $\Delta = 4\epsilon - (\delta + \alpha)^2 = 4\epsilon - \tau^2 \rightarrow 0$  and  $\xi = \delta - \alpha$  and  $\xi^2 + \Delta = (\delta - \alpha)^2 + 4\epsilon - (\delta + \alpha)^2 = 4\epsilon - 4\alpha\delta = 4\beta\gamma \equiv 0 \pmod{4\gamma}$ .

With the aid of this lemma we are able to prove the following theorem due to H. Cohn [2] which will be of great importance in determining the class number of certain relative quadratic fields.

**THEOREM 2.** Let  $\tau$  and  $\epsilon$  (unit) belong to  $0_K$  and let  $\Delta = 4\epsilon - \tau^2 \rightarrow 0$ . If  $\gamma \in 0_K$  is such that

$$(5) \quad \xi^2 + \Delta \equiv 0 \pmod{4\gamma}$$

is solvable, then there exists  $\xi_1, \xi_2, \gamma_2 \in 0_K$  such that

$$(6) \quad \frac{\xi_1^2 + \Delta \xi_2^2}{4} = \gamma \gamma_2 \quad \text{and}$$

$$(7) \quad |N(\gamma_2)| = \frac{N^{\frac{1}{2}}(\Delta)}{2^{n_{H_1}}}.$$

Proof. Let  $z_0$  be a fixed point as given in lemma 1. Then there exists a  $V \in H$  such that  $V(z_0)$  is in the fundamental domain. We can say

$$z_1 = V(z_0) = \frac{\lambda z_0 + \mu}{\nu z_0 + \rho}, \lambda\rho - \mu\nu = \eta \quad (\text{a totally positive unit})$$

and  $\text{Im}z_1 \cdot \text{Im}z_1' \cdots \text{Im}z_1^{(n-1)} \geq H_1$ , since  $z_1$  is a fixed point of  $VTV^{-1}$ , where  $T$  is the transformation which leaves  $z_0$  fixed.

Thus

$$\text{Im}z_1 = \text{Im} \left[ \frac{(\lambda z_0 + \mu)(\nu \bar{z}_0 + \rho)}{|\nu z_0 + \rho|^2} \right] = \frac{(\lambda\rho - \mu\nu)\text{Im}z_0}{|\nu z_0 + \rho|^2} = \frac{\eta\sqrt{\Delta}\text{sgn}\gamma}{2\gamma|\nu z_0 + \rho|^2}$$

or

$$(8) \quad \text{Im}z_1 = \frac{\eta^2\gamma\sqrt{\Delta}\text{sgn}\gamma}{\Phi}$$

where

$$\begin{aligned} \Phi &= 4\gamma^2 \left| \nu \left( \frac{-\xi + i\sqrt{\Delta}\text{sgn}\gamma}{2\gamma} \right) + \rho \right|^2 \\ &= 4\gamma^2 \left[ \left| \frac{-\nu\xi + 2\gamma\rho}{2\gamma} \right|^2 + \left| \frac{\nu\sqrt{\Delta}\text{sgn}\gamma}{2\gamma} \right|^2 \right] \\ &= (-\nu\hat{\xi} + 2\gamma\rho)^2 + \Delta\nu^2 \\ &= \hat{\xi}_1^2 + \Delta\hat{\xi}_2^2. \end{aligned}$$

Since  $z_1$  is also a fixed point, we have by lemma 1

$$z_1 = \frac{-\hat{\xi}_1 + i\sqrt{\Delta_1}\text{sgn}\gamma_1}{2\gamma_1}, \quad \text{where} \quad \left| \frac{\sqrt{\Delta_1}}{2\gamma_1} \cdot \frac{\sqrt{\Delta_1'}}{2\gamma_1'} \cdots \frac{\sqrt{\Delta_1^{(n-1)}}}{2\gamma_1^{(n-1)}} \right| = H_1$$

or  $|N(\gamma_1)| = \frac{N^2(\Delta_1)}{2n\eta_1}$ . Since  $\Delta = 4\epsilon - \tau^2 = \det(T) - (\text{tr}(T))^2$   
 $= \det(VTV^{-1}) - (\text{tr}(VTV^{-1}))^2 = 4\epsilon_1 - \tau_1^2 = \Delta_1$  we have  
 (9)  $\text{Im}z_1 = \frac{\sqrt{\Delta} \text{sgn}\gamma_1}{\gamma_1}$ .

Comparing (8) and (9) we obtain

$$\frac{\sqrt{\Delta} \text{sgn}\gamma_1}{2\gamma_1} = \frac{\eta_2 \gamma \sqrt{\Delta} \text{sgn}\gamma}{\phi} \quad \text{or}$$

$$\frac{\phi}{4} = \gamma \left( \eta \gamma_1 \frac{\text{sgn}\gamma}{\text{sgn}\gamma_1} \right) = \gamma \eta \gamma_1 \quad \text{since } \gamma \text{ and } \gamma_1 \text{ have the same sign.}$$

Hence, on setting  $\gamma_2 = \eta \gamma_1$ , the proof is completed.

By replacing  $\xi$  by  $\tau - 2\xi$  the congruence (5) becomes  
 $\tau^2 - 4\tau\xi + 4\xi^2 + 4\epsilon - \tau^2 \equiv 0 \pmod{4\gamma}$  or  $\xi^2 - \tau\xi + \epsilon \equiv 0 \pmod{\gamma}$ .  
 Also by replacing  $\xi_1$  by  $2\xi_1 - \tau\xi_2$  and  $\xi_2$  by  $\xi_2$  (6) becomes

$$\frac{4\xi_1^2 - 4\tau\xi_1\xi_2 + \tau^2\xi_2^2 + 4\epsilon\xi_2^2 - \tau^2\xi_2^2}{4} = \gamma\gamma_2$$

or  $\xi_1^2 - \tau\xi_1\xi_2 + \epsilon\xi_2^2 = \gamma\gamma_2$ .

Thus we are allowed to restate theorem 2 as follows:

**THEOREM 2A.** Let  $\tau$  and  $\epsilon$  (unit) belong to  $O_K$  and let  $\Delta = 4\epsilon - \tau^2 \neq 0$ . Then the solvability of

(10)  $\xi^2 - \tau\xi + \epsilon \equiv 0 \pmod{\gamma}$  in  $O_K$

implies the solvability of

$$(11) \quad \xi_1^2 - \tau \xi_1 \xi_2 + \epsilon \xi_2^2 = \gamma \gamma_2 \quad \text{in } \mathcal{O}_K$$

with

$$|N(\gamma_2)| \leq \frac{N^{\frac{1}{2}}(\Delta)}{2^{nH_1}}$$

Let us observe the consequences of this theorem for  $n = 1$ , i.e.  $K = \mathbb{Q}$ . Then the only admissible  $\epsilon$  is 1 and  $\tau$  must be 0 or 1. We consider the case  $\tau = 0$ . Then the theorem states that the solvability of  $\xi^2 + 1 \equiv 0 \pmod{\gamma}$  implies the solvability of  $\xi_1^2 + \xi_2^2 = \gamma \gamma_2$  with  $\xi, \gamma, \xi_1, \xi_2, \gamma_2$  rational integers and

$$|N(\gamma_2)| = |\gamma_2| \leq \frac{N^{\frac{1}{2}}(4)}{2^{H_1}} = \frac{2}{\sqrt{3}} < 2$$

since  $H_1(\mathbb{Q}) = \sqrt{3}/2$ . Therefore  $\gamma_2 = 1$ . Hence theorem 2A is seen to be a generalization of the classical result of Fermat that the solvability of  $x^2 + 1 \equiv 0 \pmod{m}$  implies the solvability of  $x^2 + y^2 = m$  for  $m$  a positive rational integer. This result in turn can be used to prove, in a very simple manner, that  $\mathbb{Q}(\sqrt{-1})$  has class number 1. In section 8 a theorem will be proven, using theorem 2A, which will aid in determining the class number of certain imaginary fourth degree extensions of the rationals.

### 3. Basis Theorem

In the following  $K_1$  will denote a quadratic extension of the rationals having class number one, i.e.  $K_1 = \mathbb{Q}(\sqrt{m})$  where  $m$  is a square-free rational integer and  $\mathbb{Q}(\sqrt{m})$  has unique factorization. If  $\mu$  is a square-free integer in  $K_1$ ,  $K_2$  will denote  $K_1(\sqrt{\mu})$ . The following basis theorem will be needed to determine the factorization in  $\mathcal{O}_{K_2}$  of the primes in  $\mathcal{O}_{K_1}$ .

THEOREM 3. Let  $(2) = (\lambda_1)^{l_1} (\lambda_2)^{l_2}$  and  $(\mu) = (\lambda_1)^{a_1} (\lambda_2)^{a_2} (\pi_1) \cdots (\pi_r)$  in  $\mathcal{O}_{K_1}$ . Let  $g_1$  and  $g_2$  be the largest rational integers such that

$$(12) \quad \nu^2 \equiv \mu \pmod{\lambda_1^{2g_1} \lambda_2^{2g_2}} \quad 0 \leq g_1 \leq l_1, \quad 0 \leq g_2 \leq l_2$$

is solvable. If  $\nu_1$  is a solution of (12), then  $1, \Omega$  is an integral basis for  $K_2$  over  $K_1$  where

$$(13) \quad \Omega = \frac{\nu_1 + \sqrt{\mu}}{\lambda_1^{g_1} \lambda_2^{g_2}}.$$

Hence  $1, \omega, \Omega, \omega\Omega$  is an integral basis for  $K_2$  over  $\mathbb{Q}$ , where  $1, \omega$  is an integral basis for  $K_1$  over  $\mathbb{Q}$ .

Proof.  $N_{K_2/K_1}(\Omega) = \frac{\nu_1^2 - \mu}{\lambda_1^{2\varepsilon_1} \lambda_2^{2\varepsilon_2}}$  is an integer

in  $K_1$  by (12).

$T_{K_2/K_1}(\Omega) = \frac{2\nu_1}{\lambda_1^{\varepsilon_1} \lambda_2^{\varepsilon_2}}$  is an integer

in  $K_1$  since  $\lambda_1^{\varepsilon_1} \lambda_2^{\varepsilon_2} \mid 2$ . Hence  $\Omega$  is an integer in  $K_2$ .

Let  $A = \frac{\alpha + \beta\sqrt{\mu}}{\gamma}$  be an arbitrary integer in  $K_2$  where  $\alpha, \beta, \gamma$  are integers in  $K_1$  and  $(\alpha, \beta, \gamma) = 1$ . Then

$$(14) \quad N_{K_2/K_1}(A) = \frac{\alpha^2 - \beta^2\mu}{\gamma^2} \quad \text{and}$$

$$(15) \quad T_{K_2/K_1}(A) = \frac{2\alpha}{\gamma}$$

are integers in  $K_1$ . Therefore  $\gamma \mid 2\alpha$  and  $\gamma^2 \mid \alpha^2 - \beta^2\mu$ . Suppose  $\pi \mid (\gamma, \alpha)$ , then  $\pi^2 \mid \beta^2\mu$ . Therefore  $\pi^2 \mid \mu$  since  $\pi \nmid \beta$ . This is a contradiction since  $\mu$  was assumed to be square-free. Hence  $(\gamma, \alpha) = 1$ , and from (15)  $\gamma \mid 2$ .

Also from (14)  $\alpha^2 \equiv \beta^2\mu \pmod{\gamma^2}$ . Now  $(\gamma, \beta) = 1$  since otherwise  $(\alpha, \beta, \gamma) \neq 1$ . Therefore there exists  $\rho \in \mathcal{O}_{K_1}$  such that  $\rho\beta \equiv 1 \pmod{\gamma^2}$ . Hence  $\nu^2 \equiv \mu \pmod{\gamma^2}$  is solvable with  $\nu = \rho\alpha$ . Therefore  $A = \frac{\alpha_1 + \beta_1\sqrt{\mu}}{\lambda_1^{\varepsilon_1} \lambda_2^{\varepsilon_2}}$  where  $\varepsilon_1$  and  $\varepsilon_2$

are as given in the theorem.

Note that  $\lambda_1^{\mathfrak{E}_1} \lambda_2^{\mathfrak{E}_2}$  is the "worst possible" denominator for an integer in  $\mathcal{O}_{K_2}$ . Now

$$A - \beta_1 \Omega = \frac{\alpha_1 - \beta_1 \nu_1}{\lambda_1^{\mathfrak{E}_1} \lambda_2^{\mathfrak{E}_2}}$$

is in  $\mathcal{O}_{K_2} \cap K_1$ . Therefore it is in  $\mathcal{O}_{K_1}$ , and hence

$$A = \frac{\alpha_1 - \beta_1 \nu_1}{\lambda_1^{\mathfrak{E}_1} \lambda_2^{\mathfrak{E}_2}} + \beta_1 \Omega.$$

Henceforth we will write  $\Omega = \frac{\nu_1 + \sqrt{\mu}}{\gamma_1}$  where  $\gamma_1$

denotes the denominator as given in the basis theorem.

4. Discriminant

When  $A \in K_2$ ,  $A^S$  will denote the image of  $A$  under the automorphism of  $K_2$  which sends  $\sqrt{\mu}$  into  $-\sqrt{\mu}$ , and  $A^{\bar{S}}$  will denote the image of  $A$  under the isomorphism of  $K_2$  which sends  $\sqrt{m}$  into  $-\sqrt{m}$ .

THEOREM 4. The discriminant of  $K_2$  is

$$\frac{16d^2 N(\mu)}{N^2(\gamma_1)}$$

where  $d$  is the discriminant of  $K_1$  and  $\gamma_1$  is as defined above.

Proof.

$$\text{Discriminant} = \begin{vmatrix} 1 & \omega & \Omega & \omega\Omega \\ 1 & \omega^S & \Omega^S & \omega^S\Omega^S \\ 1 & \omega & \Omega^{\bar{S}} & \omega\Omega^{\bar{S}} \\ 1 & \omega^S & \Omega^{S\bar{S}} & \omega^S\Omega^{S\bar{S}} \end{vmatrix}^2$$

$$\begin{vmatrix} 1 & \omega & \Omega & \omega\Omega \\ 1 & \omega^S & \Omega^S & \omega^S\Omega^S \\ 0 & 0 & \Omega - \Omega^S & \omega(\Omega - \Omega^S) \\ 0 & 0 & \Omega^S - \Omega^{S\bar{S}} & \omega^S(\Omega^S - \Omega^{S\bar{S}}) \end{vmatrix}^2$$

$$\begin{aligned}
&= [(\omega^s - \omega)^2 (\Omega - \Omega^s) (\Omega^s - \Omega^{ss})]^2 \\
&= \left[ d \frac{2\sqrt{\mu}}{\gamma_1} \frac{2\sqrt{\mu^s}}{\gamma_1^s} \right]^2 = \frac{16d^2 N(\mu)}{N^2(\gamma_1)}.
\end{aligned}$$

The relative different of  $K_2$  is defined to be the ideal  $(A_1 - A_1^s, A_2 - A_2^s, \dots)$ , where  $A_1$  runs through all elements of  $O_{K_2}$ . The relative discriminant  $\delta$  of  $K_2$  is defined to be the square of the relative different.

THEOREM 5. 
$$\delta = \left( \frac{4\mu}{\gamma_1^2} \right).$$

Proof. 
$$\begin{aligned}
\delta &= (A_1 - A_1^s, A_2 - A_2^s, \dots)^2 \\
&= \left( \frac{2\beta_1\sqrt{\mu}}{\gamma_1}, \frac{2\beta_2\sqrt{\mu}}{\gamma_1}, \dots \right)^2 \\
&= \left( \frac{2\sqrt{\mu}}{\gamma_1} \right)^2 (\beta_1, \beta_2, \dots)^2 \\
&= \left( \frac{4\mu}{\gamma_1^2} \right)
\end{aligned}$$

THEOREM 6. (1) Let  $\pi$  be a prime in  $O_{K_1}$  such that  $\pi \nmid 2$ . Then the relative discriminant of  $K_2$  is divisible by  $\pi$  if and only if  $\pi \mid \mu$ .

(ii) If  $\lambda^k \parallel 2$  in  $\mathcal{O}_{K_1}$  and  $\lambda \nmid \mu$  then the relative discriminant of  $K_2$  is relatively prime to  $\lambda$  if and only if

$$(16) \quad \mu \equiv \nu^2 \pmod{\lambda^{2k}} \quad \text{is solvable in } \mathcal{O}_{K_1}.$$

Proof. The first part is obvious. For the second part suppose (16) is solvable. Then by the basis theorem  $\lambda^k \mid \gamma_1$ , and  $\lambda \nmid \delta$ . Conversely, if  $\lambda \nmid \frac{\mu}{\gamma_1^2}$ , then  $\lambda^k \mid \gamma_1$ . Hence by the basis theorem  $\mu \equiv \nu^2 \pmod{\lambda^{2k}}$  is solvable.

5. Factorization

As the following theorems will show, the ideal factorization of primes in relative quadratic fields is analogous to the factorization in quadratic fields. Here the relative discriminant  $\delta$  plays the important role.

THEOREM 7. Let  $\pi$  be a prime in  $K_1$  such that  $\pi \nmid \mu$ . Then  $(\pi) = P_1 P_2$  in  $K_2$  if and only if

$$(17) \quad \mu \equiv \alpha^2 \pmod{\pi}$$

is solvable in  $O_{K_1}$ , in which case

$$\begin{aligned} P_1 &= (\pi, \alpha + \sqrt{\mu}) \\ P_2 &= (\pi, \alpha - \sqrt{\mu}). \end{aligned}$$

Proof. Note that  $(\alpha, \pi) = 1$ , since if  $\pi \mid \alpha$ , then  $\pi \mid \mu$  which is contrary to the hypotheses. Therefore  $P_1 \neq P_2$ , for if  $P_1 = P_2$ , then  $P_1 = (\pi, \alpha + \sqrt{\mu}, \alpha - \sqrt{\mu}, 2\alpha) = (1) = P_2$  which is impossible.

$$\begin{aligned} \text{Now } P_1 P_2 &= (\pi^2, \pi(\alpha + \sqrt{\mu}), \pi(\alpha - \sqrt{\mu}), \mu - \alpha^2, 2\pi\alpha) \\ &= (\pi)(\pi, \alpha + \sqrt{\mu}, \alpha - \sqrt{\mu}, (\mu - \alpha^2)/\pi, 2\alpha) = (\pi) \text{ since } (\pi, 2\alpha) = 1. \end{aligned}$$

Conversely, suppose  $(\pi) = P_1 P_2$ . Taking relative norms we have  $(\pi)^2 = P_1 P_2 P_1^S P_2^S$ , but also  $(\pi)^2 = P_1 P_2 P_1 P_2$ . Hence  $P_1 P_2 = P_1^S P_2^S$ . Therefore either

$$(18) \quad P_1 = P_1^S \quad \text{and} \quad P_2 = P_2^S$$

or

$$(19) \quad P_1 = P_2^S \quad \text{and} \quad P_2 = P_1^S.$$

Now there must be an element  $\alpha + \beta\Omega$  in  $P_1$  such that

$P_1 = (\pi, \alpha + \beta\Omega)$  and  $(\pi, \beta) = 1$ . For if  $\pi \nmid \beta$  for all elements in  $P_1$ , we would have  $P_1 \subseteq (\pi, \alpha)$ , an ideal in  $K_1$ .

Now if (18) holds

$$P_1 = (\pi, \alpha + \beta\Omega, \alpha + \beta\Omega^S, 2\beta\sqrt{\mu}/\gamma_1) = (1)$$

which is impossible. Therefore (19) must be true, i.e.  $P_2 = P_1^S$ .

Let

$$A = \frac{\alpha + \beta\sqrt{\mu}}{\gamma_1} \in P_1 \quad \text{with} \quad (\pi, \beta) = 1, \quad \text{then}$$

$$A^S = \frac{\alpha - \beta\sqrt{\mu}}{\gamma_1} \in P_1^S = P_2.$$

Since  $P_1 P_1^S = (\pi)$ ,  $AA^S = \frac{\alpha^2 - \beta^2\mu}{\gamma_1^2} \equiv 0 \pmod{\pi}$  or

$\alpha^2 \equiv \beta^2\mu \pmod{\pi}$ . Since  $(\pi, \beta) = 1$ ,  $\beta$  has an inverse  $\xi$   $\pmod{\pi}$  and  $(\xi\alpha)^2 \equiv \mu \pmod{\pi}$ .

THEOREM 8. Let  $\lambda \nmid 2$  in  $O_{K_1}$ , and let  $(\delta, \lambda) = 1$ .

Then  $(\lambda) = L_1 L_2$  if and only if

$$(20) \quad \mu \equiv \alpha^2 \pmod{\lambda^{2\ell} + 1}$$

is solvable in  $O_{K_1}$ . Moreover, in this case

$$(21) \quad \begin{cases} L_1 = \left( \lambda, \frac{\alpha + \sqrt{\mu}}{\lambda^\ell} \right) \\ L_2 = \left( \lambda, \frac{\alpha - \sqrt{\mu}}{\lambda^\ell} \right) \end{cases}$$

Proof. By reasoning similar to that used in theorem 8, we find that, if  $L_1$  and  $L_2$  are as given in (21),  $L_1 \neq L_2$ .

Now suppose (20) is solvable and  $L_1$  and  $L_2$  are given by (21), then

$$\begin{aligned} L_1 L_2 &= \left( \lambda^2, \lambda \left( \frac{\alpha + \sqrt{\mu}}{\lambda^i} \right), \lambda \left( \frac{\alpha - \sqrt{\mu}}{\lambda^i} \right), \frac{\alpha^2 - \mu}{\lambda^{2i}} \right) \\ &= (\lambda) \left( \lambda, \frac{\alpha + \sqrt{\mu}}{\lambda^i}, \frac{\alpha - \sqrt{\mu}}{\lambda^i}, \frac{\alpha^2 - \mu}{\lambda^{2i+1}}, \frac{2\sqrt{\mu}}{\lambda^i} \right) \\ &= (\lambda) \end{aligned}$$

since  $\left( \lambda, \frac{2\sqrt{\mu}}{\lambda^i} \right) = 1$ .

Conversely suppose  $(\lambda) = L_1 L_2$ . Then  $(\lambda)^2 = L_1 L_2 L_1^S L_2^S$  and  $(\lambda)^2 = L_1 L_2 L_1 L_2$ . Hence either

$$(22) \quad L_1 = L_1^S \quad \text{and} \quad L_2 = L_2^S$$

or

$$(23) \quad L_1 = L_2^S \quad \text{and} \quad L_2 = L_1^S.$$

As in the proof of theorem 8 there exists an element

$\alpha + \beta\delta$  in  $L_1$  such that  $L_1 = (\lambda, \alpha + \beta\delta)$  and  $(\beta, \lambda) = 1$ .

Now if (22) holds

$$L_1 = \left( \lambda, \alpha + \beta\delta, \alpha + \beta\delta^S, \frac{2\beta\sqrt{\mu}}{\gamma_1}, \frac{4\beta^2\mu}{\gamma_1^2} \right).$$

But  $\delta = \frac{4\mu}{\gamma_1^2}$  and  $(\delta, \lambda) = 1$ , and  $(\beta^2, \lambda) = 1$ ; thus  $L_1 = (1)$ ,

which is impossible. Hence (23) holds and  $(\lambda) = L_1 L_1^S$ .

Let  $A = \frac{\rho + \sigma\sqrt{\mu}}{\gamma_1}$  belong to  $L_1$  where  $\lambda \nmid A$ . We now have

$$(24) \quad AA^S = \frac{\rho^2 - \sigma^2\mu}{\gamma_1^2} \equiv 0 \pmod{\lambda}.$$

Since  $\lambda \nmid A$ ,  $(\sigma, \lambda) = 1$ . Hence there exists  $\xi \in \mathcal{O}_{K_1}$  such that  $\xi\sigma \equiv 1 \pmod{\lambda}$ . Thus from (24) we obtain

$$(25) \quad \frac{(\xi\sigma)^2 - \mu}{\gamma_1^2} \equiv 0 \pmod{\lambda}.$$

Since  $(\delta, \lambda) = 1$ , theorems 6 (ii) and 3 show that  $\lambda^\delta \parallel \gamma_1$ ; therefore (25) yields  $(\xi\sigma)^2 \equiv \mu \pmod{\lambda^{2\delta+1}}$ .

**THEOREM 9.** If  $\pi$  is a prime in  $\mathcal{O}_{K_1}$  such that  $\pi \mid \mu$  and  $\pi \nmid 2$ , then  $(\pi) = P^2$  in  $K_2$  where

$$(26) \quad P = (\pi, \sqrt{\mu}).$$

Proof. Let  $P$  be given as in (26). Then

$$P^2 = (\pi^2, \pi\sqrt{\mu}, \mu) = (\pi)(\pi, \sqrt{\mu}, \mu/\pi) = (\pi)$$
 because  $(\pi, \mu/\pi) = 1$  since  $\mu$  is square-free.

The factorization of primes which are factors of 2 and  $\delta$  is somewhat more difficult and requires the following lemma.

LEMMA 2. Let  $\lambda$  be a prime factor of 2 in  $O_{K_1}$  such that  $\lambda^2 \parallel 2$  and  $\lambda^6 \parallel \gamma_1$ . Then if  $g = \lambda$ ,

$$(27) \quad \nu^2 \equiv \mu \pmod{\lambda^{2g+1}}$$

is solvable in  $O_{K_1}$ .

Proof. Case I.  $g = 0$ .

Suppose first  $\lambda = 2$ ; then  $m \equiv 5 \pmod{8}$ . Let  $1, \omega = \frac{1+\sqrt{m}}{2}$  denote the integral basis for  $O_{K_1}$ . Let  $u = a+b\omega$  and  $\nu = x+y\omega$ . Then (27) becomes

$$x^2 + y^2 \left( \frac{1+m+2\sqrt{m}}{4} \right) + 2xy\omega - (a+b\omega) \equiv 0 \pmod{2}$$

or

$$x^2 + \left( \frac{m-1}{4} \right) y^2 - a + (y^2 - b)\omega \equiv 0 \pmod{2}.$$

Since  $\frac{m-1}{4} \equiv 1 \pmod{2}$ , to solve (27) we must solve

$$\begin{cases} x^2 + y^2 - a \equiv 0 \pmod{2} \\ y^2 - b \equiv 0 \pmod{2} \end{cases}$$

simultaneously in rational integers  $x$  and  $y$ , and this is clearly possible.

If  $\lambda \neq 2$ , then  $\lambda \equiv 0$  or  $1 \pmod{\lambda}$  and (27) is clearly solvable.

Case II.  $g = 1$ .

Since  $g = 1$ , there exists  $\nu_1$  such that

$$\nu_1^2 \equiv \mu \pmod{\lambda^2}.$$

Let  $\frac{v_1^2 - \mu}{\lambda^2} = \sigma$ . Since  $\sigma \equiv 0$  or  $1 \pmod{\lambda}$ , there exists

$\rho \in \mathcal{O}_{K_1}$  such that  $\rho^2 \equiv \sigma \pmod{\lambda}$ . Let  $v_2 = v_1 + \rho\lambda$ . Then

$$\frac{v_2^2 - \mu}{\lambda^3} = \frac{v_1^2 - \mu + 2\rho v_1 \lambda + \rho^2 \lambda^2}{\lambda^3} = \frac{\sigma - \rho^2}{\lambda} + \frac{2\rho v_1}{\lambda^2}$$

which is in  $\mathcal{O}_{K_1}$ . Hence (27) is solvable with  $v = v_2$ .

**THEOREM 10.** Let  $\lambda | (2, \delta)$  in  $\mathcal{O}_{K_1}$ . Then  $(\lambda) = L^2$  in  $K_2$  where  $L = (\lambda, \sqrt{\mu})$  if  $\lambda | \mu$  and  $L = (\lambda, \Omega)$  if  $\lambda \nmid \mu$  and the  $v_1$  in  $\Omega$  is taken to be such that  $v_1^2 \equiv \mu \pmod{\lambda^{2g+1}}$ .

Proof. Suppose  $\lambda | \mu$  and  $L = (\lambda, \sqrt{\mu})$ . Then  $L^2 = (\lambda^2, \lambda\sqrt{\mu}, \mu) = (\lambda)(\lambda, \sqrt{\mu}, \mu/\lambda) = (\lambda)$  since  $(\lambda, \mu/\lambda) = 1$ .

Suppose  $\lambda \nmid \mu$ . Then since  $\lambda | \delta$  we have  $\lambda | 4/\gamma_1^2$  and hence  $g < l$ . Therefore by lemma 2 there exists an integer  $v_1$  in  $K_1$  such that

$$(28) \quad v_1^2 \equiv \mu \pmod{\lambda^{2g+1}}.$$

Let  $L = (\lambda, \Omega)$  where the  $v_1$  in  $\Omega$  is given in (28). Then

$$L^S = (\lambda, \Omega^S) \text{ and } \Omega - \Omega^S = \frac{2\sqrt{\mu}}{\gamma_1} \equiv 0 \pmod{\lambda} \text{ since } g < l.$$

Hence  $L = L^S$  and

$$L^2 = LL^S = \left( \lambda^2, \lambda\Omega, \lambda\Omega^S, \frac{v_1^2 - \mu}{\gamma_1^2} \right) = (\lambda) \left( \lambda, \Omega, \Omega^S, \frac{v_1^2 - \mu}{\gamma_1^2} \right) = (\lambda)$$

because  $\left( \lambda, \frac{v_1^2 - \mu}{\lambda\gamma_1^2} \right) = 1$ , for if  $\lambda | \frac{v_1^2 - \mu}{\lambda\gamma_1^2}$  we would have

$\nu_1^2 \equiv \mu \pmod{\lambda^{2g+2}}$  which contradicts the definition of  $g$ .

Theorems 7, 8, 9, and 10 can now be combined to give the following theorem illustrating how the prime ideals in  $\mathcal{O}_{K_1}$  factor in  $\mathcal{O}_{K_2}$ .

**THEOREM 11.** Let  $\pi$  denote a prime in  $K_1$  such that  $\pi \nmid 2$  and let  $\lambda$  denote a prime in  $K_1$  such that  $\lambda^g \parallel 2$ . Then:

$$(\pi) = \begin{cases} (\pi) & \text{if } \pi \nmid \mu \text{ and } \alpha^2 \equiv \mu \pmod{\pi} \\ & \text{is unsolvable in } \mathcal{O}_{K_1}. \\ (\pi, \alpha + \sqrt{\mu})(\pi, \alpha - \sqrt{\mu}) & \text{if } \pi \nmid \mu \text{ and } \alpha^2 \equiv \mu \pmod{\pi}. \\ (\pi, \sqrt{\mu})^2 & \text{if } \pi \mid \mu. \end{cases}$$
  

$$(\lambda) = \begin{cases} (\lambda) & \text{if } \lambda \nmid \delta \text{ and } \alpha^2 \equiv \mu \pmod{\lambda^{2g+1}} \\ & \text{is unsolvable in } \mathcal{O}_{K_1}. \\ (\lambda, \frac{\alpha + \sqrt{\mu}}{\lambda^g})(\lambda, \frac{\alpha - \sqrt{\mu}}{\lambda^g}) & \text{if } \lambda \nmid \delta \text{ and } \alpha^2 \equiv \mu \pmod{\lambda^{2g+1}}. \\ (\lambda, \sqrt{\mu})^2 & \text{if } \lambda \mid \mu. \\ (\lambda, \Omega)^2 & \text{if } \lambda \mid \delta \text{ and } \lambda \nmid \mu, \text{ where the } \nu_1 \\ & \text{in } \Omega \text{ is such that} \\ & \nu_1^2 \equiv \mu \pmod{\lambda^{2g+1}}. \end{cases}$$

## 6. Galois Group

We proceed now to the task of determining the Galois group  $\mathcal{G}(K_2/\mathbb{Q})$  of the field  $K_2$ .

**THEOREM 12.**  $K_2$  is a normal field (i.e.  $\sqrt{\mu^s} \in K_2$ ) if and only if  $\mu^s = \mu\rho^2$  where  $\rho \in K_1$ .

Proof. Suppose  $\mu^s = \mu\rho^2$ . Then  $\sqrt{\mu^s} = \rho\sqrt{\mu} \in K_2$ .

Suppose  $\sqrt{\mu^s} \in K_2$ . Then  $\sqrt{\mu^s} = \alpha + \beta\sqrt{\mu}$ , where  $\alpha, \beta \in K_1$ . Hence  $\mu^s = \alpha^2 + \beta^2\mu + 2\alpha\beta\sqrt{\mu} \in K_1$  and  $\alpha = 0$  or  $\beta = 0$ . If  $\beta = 0$ ,  $\mu^s = \alpha^2$  and  $\mu = (\alpha^s)^2$  which is impossible since  $\mu$  is square-free. Therefore  $\alpha = 0$  and  $\mu^s = \beta^2\mu$ .

**COROLLARY 1.**  $K_2$  is a normal field if and only if  $N(\mu) = \alpha^2$  for some  $\alpha \in K_1$ .

Proof. If  $K_2$  is normal  $\mu^s = \mu\rho^2$  for some  $\rho \in K_1$  and  $N(\mu) = \mu\mu^s = (\mu\rho)^2$ .

If  $N(\mu) = \alpha^2$ , then  $\mu^s = \alpha^2/\mu = \mu(\alpha/\mu)^2$  and  $K_2$  is normal.

**THEOREM 13.** If  $K_2$  is normal, then  $\mathcal{G}(K_2/\mathbb{Q}) = \{1, s, S, sS\}$   $s^2 = S^2 = 1$ ,  $sS = Ss$ .

Proof. Clearly  $s, S \in \mathfrak{S}(K_2/Q)$  and  $s^2 = S^2 = 1$ . Since  $K_2$  is normal  $\mu^S = \mu\rho^2$  for some  $\rho \in K_1$  and we have

$$\begin{aligned} (\alpha + \beta\sqrt{\mu})^{SS} &= (\alpha^S + \beta^S \rho\sqrt{\mu})^S = \alpha^S - \beta^S \rho\sqrt{\mu} = \alpha^S - \beta^S \sqrt{\mu^S} \\ &= (\alpha - \beta\sqrt{\mu})^S = (\alpha + \beta\sqrt{\mu})^{SS}. \end{aligned}$$

Therefore  $sS = Ss$ . Also the number of elements in  $\mathfrak{S}(K_2/Q)$  is 4 since  $K_2$  is a normal fourth degree extension of  $Q$ .

The following theorem will not be needed in the future material, but is included in order to complete the discussion of the Galois group of  $K_2$ .

**THEOREM 14.** If  $K_2$  is not normal and  $N = K_2(\sqrt{\mu^S})$  (the splitting field for  $(x^2 - \mu)(x^2 - \mu^S)$ ), then  
 $\mathfrak{S}(N/Q) = \{1, (13), (24), (13)(24), (1234), (1432), (12)(34), (14)(23)\}$ .

Proof. Let  $x_1 = \sqrt{\mu}$ ,  $x_2 = \sqrt{\mu^S}$ ,  $x_3 = -\sqrt{\mu}$ ,  $x_4 = -\sqrt{\mu^S}$ . Any  $Q$  automorphism of  $N$  must permute  $x_1, x_2, x_3, x_4$ , and must leave the rational number  $x_1x_3 + x_2x_4$  fixed. Also there must be 8 automorphisms since  $N$  is an eighth degree extension of  $Q$ . The theorem follows immediately.

## 7. Normality of Fixed Point Fields

The fields with which we shall be concerned in the following will be called fixed point fields and are defined as follows: Let  $K_1$  denote a real quadratic extension of  $\mathbb{Q}$  with class number 1, and let  $\mu_0 = \tau^2 - 4\epsilon \neq 0$ , where  $\epsilon$  is a unit and  $\tau \in \mathcal{O}_{K_1}$ . Then  $K_2 = K_1(\sqrt{\mu_0})$  will be called a fixed point field. Note that  $\mu_0$  has exactly the same form as  $-\Delta$  in theorem 2A. There  $\Delta$  arose from fixed points of the Hilbert modular group; hence, the name fixed point field.

In general  $\mu_0$  will not be square-free, but we may write  $\mu_0 = \sigma^2 \mu$  where  $\mu$  is square-free. Then  $K_2 = K_1(\sqrt{\mu_0}) = K_1(\sqrt{\mu})$ , and we see  $K_2$  is a relative quadratic field as discussed in Chapter II. Hence the theorems in sections 3 thru 6 apply to fixed point fields.

Continuing with the ideas pursued in section 6, now applied to fixed point fields, we prove the following theorem.

**THEOREM 15.** If  $K_2$  is a fixed point field, then  $K_2$  is a normal field.

Proof. We begin by making two observations which will not only be used in the proof of this theorem but

also in later proofs.

$$-\mu_0 = 4\epsilon - \tau^2 \leq 4\epsilon \quad \text{and} \quad -\mu_0^s = 4\epsilon^s - (\tau^s)^2 \leq 4\epsilon^s$$

give us

$$(29) \quad N(\mu_0) \leq 16.$$

Also  $\tau^2 < 4\epsilon$  and  $(\tau^s)^2 < 4\epsilon^s$  yield  $N^2(\tau) < 16$  or

$$(30) \quad |N(\tau)| < 4.$$

From corollary 1 it suffices to show that  $N(\mu)$  is the square of an element in  $K_1$ . Since  $\mu_0 = \sigma^2 \mu$ ,  $N(\mu_0) = N^2(\sigma)N(\mu)$  and it will suffice to show  $N(\mu_0)$  is the square of an element in  $K_1$ . From

$$(31) \quad 0 \leq N(\mu_0) = (\tau^2 - 4\epsilon)((\tau^s)^2 - 4\epsilon^s) = N^2(\tau) - 4T(\tau^2\epsilon^s) + 16 \leq 16$$

we see  $T(\tau^2\epsilon^s) \geq 0$ . If  $\tau = 0$ ,  $N(\mu_0) = 4^2$  and we are done.

When  $\tau \neq 0$  the proof breaks into several cases.

Case 1.  $m \neq 4n+1$

Let  $\tau^2\epsilon^s = a+b\sqrt{m}$  where  $a$  and  $b$  are rational integers.

Then  $T(\tau^2\epsilon^s) = 2a$  and by (31) we have

$$(32) \quad 16 \geq N(\mu_0) = N^2(\tau) - 8a + 16 > 0.$$

Case 1a.  $|N(\tau)| = 1$

Then by (32) we have  $16 \geq N(\mu_0) = 17 - 8a > 0$ .

Hence  $a = 1$  or  $2$  and  $N(\mu_0) = 3^2$  or  $1^2$ .

$$\text{Case 1b.} \quad |N(\tau)| = 2$$

Then by (32),  $16 \geq N(\mu_0) = 20 - 3a > 0$  and  $a = 1$  or  $2$ .

If  $a = 2$ ,  $N(\mu_0) = 2^2$ . Since  $N(\tau^2 \in \mathbb{S}) = a^2 - b^2m = 4$ , if  $a = 1$ , then  $-b^2m = 3$  which is impossible. Hence  $a$  cannot be 1.

$$\text{Case 1c.} \quad |N(\tau)| = 3$$

Then  $16 \geq N(\mu_0) = 25 - 8a > 0$  and  $a = 2$  or  $3$ .

Thus  $N(\mu_0) = 3^2$  or  $1^2$ .

$$\text{Case 2.} \quad m = 4n+1$$

Let  $\tau^2 \in \mathbb{S} = a + b \left( \frac{1 + \sqrt{m}}{2} \right)$  where  $a$  and  $b$  are rational integers. Then  $N(\tau^2 \in \mathbb{S}) = 2a + b$  and (31) becomes

$$(33) \quad 16 \geq N(\mu_0) = N^2(\tau) - 4(2a + b) + 16 > 0.$$

$$\text{Case 2a.} \quad |N(\tau)| = 1$$

Then (33) becomes  $16 \geq N(\mu_0) = 17 - 4(2a + b) > 0$  and

$2a + b = 1, 2, 3$ , or  $4$ . If  $2a + b = 2$  or  $4$ ,  $N(\mu_0) = 3^2$  or  $1^2$ .

Suppose  $2a + b = 1$ . Then  $N(\tau^2 \in \mathbb{S}) = \frac{(2a + b)^2 - mb^2}{4} = 1$  and

$-mb^2 = 3$  which is impossible. Therefore  $2a + b = 1$  is excluded, which leaves only the possibility  $2a + b = 3$ . In this case

$N(\tau^2 \in \mathbb{S}) = \frac{9 - mb^2}{4} = 1$  or  $mb^2 = 5$ . Hence  $m = 5$  and

$$N(\mu_0) = (\sqrt{5})^2.$$

$$\text{Case 2b.} \quad |N(\tau)| = 2$$

In this case  $16 \geq N(\mu_0) = 20 - 4(2a + b) > 0$  and

$2a+b = 1, 2, 3$  or  $4$ . But  $N(\tau^2 \epsilon^s) = \frac{(2a+b)^2 - mb^2}{4} = 4$  or  $(2a+b)^2 = 16 + mb^2$ . Hence  $2a+b \geq 4$ ; thus  $2a+b = 4$  and  $N(\mu_0) = 2^2$ .

Case 2c.  $|N(\tau)| = 3$

We then have  $16 \geq N(\mu_0) = 25 - 4(2a+b) > 0$  and

$2a+b = 3, 4, 5$  or  $6$ . Also  $N(\tau^2 \epsilon^s) = \frac{(2a+b)^2 - mb^2}{4} = 9$  or  $(2a+b)^2 = 36 + mb^2$  which requires  $2a+b \geq 6$ . Hence  $2a+b = 6$  and  $N(\mu_0) = 1$ . The proof of the theorem is now complete.

If  $K_2$  is a fixed point field and  $A \in K_2$ , the above theorem together with theorem 12 allows us to say  $A^{SS} = A^{SS}$ .

8. Existence of Fixed Point Fields

It is natural at this point to ask about the existence and abundance of fixed point fields, i.e. for a fixed positive integer  $m$  such that  $Q(\sqrt{m})$  has class number 1, how many  $\mu$  exist such that  $\mu$  is the square-free kernel of  $\mu_0 = \tau^2 - 4\epsilon = 0$ . For  $\epsilon = 1$  it is clear that  $\tau = 0$  and 1 are admissible values for  $\tau$  and thus  $K_1(\sqrt{-3})$  (if 3 is not a perfect square in  $K_1$ ) and  $K_1(\sqrt{-4}) = K_1(\sqrt{-1})$  are always fixed point fields. Hence for fixed  $m$ , fixed point fields exist. We proceed now to partially answer the question of abundance.

Since  $\tau^2 \ll 4\epsilon$  we see that  $\epsilon$  must be a totally positive unit. If we let  $\epsilon_0$  denote the fundamental unit of  $K_1 = Q(\sqrt{m})$  then

$$(34) \quad \mu_0 = \tau^2 - 4\epsilon^n = \begin{cases} \epsilon_0^{2k} [(\tau/\epsilon_0^k)^2 - 4] & \text{if } n = 2k \\ \epsilon_0^{2k} [(\tau/\epsilon_0^k)^2 - 4\epsilon_0] & \text{if } n = 2k+1. \end{cases}$$

The quantities that appear in brackets in (34) are admissible values for a different  $\mu_0$  which gives rise to the same fixed point field. Thus in seeking admissible values for  $\mu_0$  we may restrict the values of  $\epsilon$  to 1 and  $\epsilon_0$  if  $\epsilon_0$  is totally positive and to 1 alone if  $\epsilon_0$  is not totally positive. (If  $\epsilon_0$  were not totally positive  $n$  could not be odd in (34).)

For fixed  $\epsilon$  we now show that there are only a finite number of values for  $\tau$  that give rise to an admissible  $\mu_0$ . Let  $\tau = x+y\omega$  ( $1, \omega$  is an integral basis for  $K_1$ ), where  $x$  and  $y$  are rational integers. Then  $x$  and  $y$  must satisfy

$$(35) \quad \begin{aligned} -2\sqrt{\epsilon} &= x+y\omega < 2\sqrt{\epsilon} \\ -2\sqrt{\epsilon^s} &< x+y\omega^s < 2\sqrt{\epsilon^s}. \end{aligned}$$

Now if  $(x,y)$  is a solution to (35),  $(x,y)$  must be a lattice point in the interior of the parallelogram determined by the four lines

$$\begin{aligned} x+y\omega &= 2\sqrt{\epsilon} \\ x+y\omega &= -2\sqrt{\epsilon} \\ x+y\omega^s &= 2\sqrt{\epsilon^s} \\ x+y\omega^s &= -2\sqrt{\epsilon^s}. \end{aligned}$$

Thus we see that for fixed  $\epsilon$ , there are only a finite number of admissible values for  $\tau$ . This proves the following theorem.

**THEOREM 16.** For a fixed  $m$ , there are a (non-zero) finite number of fixed point fields.

Table I on page 45 gives a listing of all admissible values of  $\mu_0$  for selected values of  $m$ .

## 9. Minkowskian Bound

In determining the class number of a particular algebraic number field, much work can be eliminated by being able to say that every ideal class contains an ideal with norm less than or equal to some fixed number. Such a number is often called a Minkowskian bound on the norms of ideals in ideal classes. The following theorem, which appears on page 190 of [ 7 ], will be used to determine a Minkowskian bound for fixed point fields.

**THEOREM 17.** Every ideal class of an algebraic number field contains infinitely many prime ideals.

**THEOREM 18.** If  $K_2$  is a fixed point field, then every ideal class of  $K_2$  contains an ideal  $\psi$  such that

$$N[\psi] \leq \frac{N^{\frac{1}{2}}(\mu_0)}{4H_1}$$

Proof. Let  $\mu_0 = \tau^2 - 4\epsilon \neq 0$  and also let  $\mu_0 = \sigma^2\mu$  where  $\mu$  is square-free. Then  $K_2 = K_1(\sqrt{\mu})$  is a fixed point field. Let  $\mathcal{Q}$  be an ideal class of  $K_2$ . The theorem is clearly true if  $\mathcal{Q}$  is the class of principal ideals, so we may assume  $\mathcal{Q}$  is not the identity class.

Let  $P \in \mathcal{Q}$  where  $P$  is a prime ideal such that  $P \nmid (2\mu_0)$ . This is possible by theorem 17. Now, by theorem 11,  $PP^S = (\pi)$  where  $\pi$  is a prime in  $\mathcal{O}_{K_1}$  which does not divide  $(2\mu_0)$ . Again by theorem 11, there exists an integer  $\alpha$  in  $K_1$  such that  $\alpha^2 \equiv \mu_0 \pmod{\pi}$ . Hence if  $\rho = \alpha$

$$(36) \quad \rho^2 \equiv \mu_0 \pmod{\pi}.$$

Since  $(\pi, 2) = 1$ , by the Chinese Remainder Theorem there exists a  $\rho_1 \in \mathcal{O}_{K_1}$  such that  $\rho_1 \equiv \rho \pmod{\pi}$  and  $\rho_1 \equiv \tau \pmod{2}$ . Hence  $\rho_1 = \tau - 2\xi$  for some integer  $\xi$  in  $K_1$ . From (36) we have

$$\rho_1^2 \equiv \rho^2 \equiv 4\xi^2 - 4\tau\xi + \tau^2 \equiv \mu_0 = \tau^2 - 4\epsilon \pmod{\pi}.$$

Hence  $\xi^2 - \tau\xi + \epsilon \equiv 0 \pmod{\pi}$ . Now from theorem 2A there exist integers  $\hat{\xi}_1, \hat{\xi}_2, \gamma_2$  in  $K_1$  such that

$$(37) \quad \hat{\xi}_1^2 - \tau \hat{\xi}_1 \hat{\xi}_2 + \epsilon \hat{\xi}_2^2 = \pi \gamma_2$$

with

$$N(\gamma_2) = \frac{N^{\frac{1}{2}}(\mu_0)}{4H_1}$$

Or, rewriting (37) we have

$$(\hat{\xi}_1 - \hat{\xi}_2 X)(\hat{\xi}_1 - \hat{\xi}_2 X)^S = (\pi)(\gamma_2) = PP^S(\gamma_2)$$

where  $X = \frac{\tau + \sqrt{\mu_0}}{2}$ , an integer in  $K_2$ . Hence  $P \mid (\hat{\xi}_1 - \hat{\xi}_2 X)$  or  $P \mid (\hat{\xi}_1 - \hat{\xi}_2 X)^S$ . Without loss of generality we may assume

$P | (\xi_1 - \xi_2 X)$ . Then  $(\xi_1 - \xi_2 X) = P\Gamma$  and  $PP^S \Gamma \Gamma^S = (\pi)(\gamma_2)$ . Clearly  $\Gamma \in \mathcal{O}^{-1}$  and  $\Gamma^S \in \mathcal{O}$ , since  $\Gamma \Gamma^S = (\gamma_2)$ . We also have  $N_{K_2/Q}[\Gamma^S] = N_{K_1/Q}[(\gamma_2)] = |N_{K_1/Q}(\gamma_2)| = \frac{N^{\frac{1}{2}}(\mu_0)}{4H_1}$

The following corollary is an immediate consequence of theorem 18.

COROLLARY 2. If  $\frac{N^{\frac{1}{2}}(\mu_0)}{4H_1} < 2$ , then  $K_2$  has class number 1.

We conclude this section by giving a simple, but important, application of theorem 18. R. DeVore has shown [3] that for the field  $Q(\sqrt{5})$ ,  $H_0 = \sqrt{5}/4$ . This result was proven by showing that  $H_0 \geq \sqrt{5}/4$  and that  $H_0 \leq \sqrt{5}/4$ . It will now be shown, using theorem 18, that  $H_0 \leq \sqrt{5}/4$ . Let  $m = 5$ ,  $\epsilon = 1$ , and  $\tau = \frac{1+\sqrt{5}}{2}$ . Then  $\mu_0 = \frac{-5+\sqrt{5}}{2}$  is totally negative. Since  $H_1 \geq H_0$  we have, if  $H_0 > \sqrt{5}/4$ ,

$$\frac{N^{\frac{1}{2}}(\mu_0)}{4H_1} \leq \frac{\sqrt{5}}{4H_0} < 1.$$

Hence, by theorem 18, we would be led to the absurd statement that every ideal class of  $K_1 \left( \sqrt{\frac{-5+\sqrt{5}}{2}} \right)$  contains an ideal of norm strictly less than 1. Hence  $H_0 \leq \sqrt{5}/4$ . This gives another proof of (the easier) half of DeVore's result.

10. Units

The following theorem serves to characterize units in fixed point fields. It should be noted that the proof in no way depends on Dirichlet's unit theorem. The proof does, however, require some knowledge of the structure of units in real quadratic fields. This may be found in [ 1 ]

THEOREM 19. If  $K_2$  is a fixed point field, all units are of the form  $\zeta_k^{n_1} \epsilon_0^{n_2}$  where

$$\epsilon_0 = \begin{cases} \sqrt{-\epsilon_0} & \text{if } \mu = -\epsilon_0. \\ \epsilon_0 & \text{if } \mu \neq -\epsilon_0. \end{cases}$$

$\epsilon_0$  denotes the fundamental unit of  $K_1$  and  $\zeta_k$  is a primitive  $k^{\text{th}}$  root of unity.  $n_1$  (determined (mod  $k$ )) and  $n_2$  are rational integers. Furthermore

$$k = \begin{cases} 12 & \text{if } \mu = -1 \text{ and } m = 3 \\ 4 & \text{if } \mu = -1 \text{ and } m \neq 3 \\ 10 & \text{if } \mu = -\frac{5 + \sqrt{5}}{2} \\ 6 & \text{if } \mu = -3 \\ 2 & \text{otherwise} \end{cases}$$

Proof. Let  $E$  be an arbitrary unit in  $K_2$ . Clearly  $|E| = |E^S|$  and  $|E^S| = |E^{SS}|$ , since  $A^S$  is the complex conjugate of  $A$ . Also  $|EE^S E^{SS} E^{SSS}| = |E|^2 |E^S|^2 = 1$ .

Hence  $|E||E^S| = 1$ .

Consider the set  $U = \{x: x = \log |E|, \text{ and } E \text{ is a unit in } K_2\}$ .  $U$  forms an additive subgroup of the real numbers. Suppose the elements of  $U$  become arbitrarily close to 0. Then  $|E|$  becomes arbitrarily close to 1 and  $|E|^2 = |EE^S| = |\epsilon_0^t|$  becomes arbitrarily close to 1, which contradicts the definition of  $\epsilon_0$  (the fundamental unit of  $K_1$ ). Hence  $U$  is not dense and it must contain a smallest positive element. Thus there exists a unit  $E_0$  in  $O_{K_2}$  such that each element in  $U$  can be written as  $n \log |E_0|$  where  $n$  is a rational integer. Therefore for any unit  $E$  in  $K_2$ ,  $|E| = |E_0|^n$  or  $E = E_0^n \zeta$  where  $|\zeta| = 1$ ; also  $|E^S| = |E_0^S|^n$  or  $E^S = (E_0^S)^n \zeta^S$  where  $|\zeta^S| = 1$ . Thus, since  $\zeta$  and all its conjugates lie on the unit circle,  $\zeta$  is a root of unity (as shown on page 122 of [4]). Now  $|E_0 E_0^S| = |\epsilon_0^t|$  with  $t = 1$  or  $2$ , for if  $t \geq 3$ ,  $E_1 = E_0 / \epsilon_0$  would be such that

$$|E_1 E_1^S| = |\epsilon_0^{t-2}| < |\epsilon_0^t| = |E_0 E_0^S| \text{ or } 1 < |E_1| < |E_0|$$

which contradicts the definition of  $E_0$ . If  $t = 2$ ,  $|E_0 / \epsilon_0| = 1$  and  $E_0$  can be chosen to be  $\epsilon_0$ . If  $t = 1$ , then  $|E_0|^2 = |\epsilon_0|$  and  $E_0 = \sqrt{\epsilon_0} \theta$  where  $|\theta| = 1$ .  $\theta$  must be real, so  $\theta = \pm 1$ .  $\theta = 1$  can be eliminated since  $\sqrt{\epsilon_0}$  cannot be in a fixed point field. Thus  $E_0 = \sqrt{-\epsilon_0}$ . If  $\sqrt{-\epsilon_0} \in K_2$ , then  $\alpha + \beta \sqrt{\mu} = \sqrt{-\epsilon_0}$ , where  $\alpha, \beta \in K_1$ . Hence  $\alpha^2 + \mu \beta^2 + 2\alpha\beta\sqrt{\mu} = -\epsilon_0$ . Thus  $\alpha\beta = 0$

and  $\beta \neq 0$ . Therefore  $\alpha = 0$  and  $\beta^2 = -\epsilon_0/\mu$ . Now  $-\epsilon_0/\mu$  is not a perfect square unless  $-\epsilon_0/\mu = 1$ , or  $\mu = -\epsilon_0$ .

In order that  $\zeta_k$  (a primitive  $k^{\text{th}}$  root of unity) be in  $K_2$ ,  $\phi(k)$  must be 2 or 4. Hence 2, 3, 4, 5, 6, 10, 12, are the only possibilities for  $k$  and

$$\begin{aligned}\zeta_2 &= -1 \\ \zeta_3 &= -\frac{1}{2} + \frac{\sqrt{-3}}{2} \\ \zeta_4 &= \sqrt{-1} \\ \zeta_5 &= \frac{\sqrt{5}-1}{4} + \frac{\sqrt{-\frac{5+\sqrt{5}}{2}}}{2} \\ \zeta_6 &= \frac{1}{2} + \frac{\sqrt{-3}}{2} \\ \zeta_{10} &= -\zeta_5 \\ \zeta_{12} &= \frac{\sqrt{3}}{2} + \frac{\sqrt{-1}}{2}.\end{aligned}$$

In order that  $\zeta_{12} \in K_2$ , we must have  $m = 3$  and  $\mu = -1$ .

In order that  $\zeta_6 \in K_2$ , we must have  $\mu = -3$  and if  $\zeta_{12} \notin K_2$  we must also have  $m \neq 3$ .

In order that  $\zeta_5 \in K_2$ , we must have ( $m = 5$  and)  $\mu = -\frac{5+\sqrt{5}}{2}$

In order that  $\zeta_4 \in K_2$ , we must have  $\mu = -1$  and if  $\zeta_{12} \notin K_2$  we must also have  $m \neq 3$ .

Also,  $\zeta_3 \in K_2$  if and only if  $\zeta_6 \in K_2$  and  $\zeta_5 \in K_2$  if and only if  $\zeta_{10} \in K_2$ . The theorem follows immediately.

11. Determination of Class Number

The following theorem gives necessary conditions for an algebraic number to be an element of a fixed point field. It will be used in showing certain ideals to be non-principal.

THEOREM 20. If  $A \in K_2$ , where  $K_2$  is a fixed point field, then  $N_{K_2/K_1}(A) \neq 0$ .

Proof. Let  $A = \alpha + \beta\sqrt{\mu}$  where  $\alpha, \beta \in K_1$ . Then  $N_{K_2/K_1}(A) = \alpha^2 - \mu\beta^2 > 0$  since  $\mu < 0$  and

$$N_{K_2/K_1}(A)^s = (\alpha^s)^2 - \mu^s(\beta^s)^2 > 0 \text{ since } \mu^s < 0. \text{ Hence}$$

$N_{K_2/K_1}(A)$  is totally positive.

Included in Table II on page 47 is the class number of specific fixed point fields. These have been determined using many of the preceding theorems. The following three examples illustrate many of the techniques which have been used.

Example 1. Let  $m = 5$ ,  $\tau = 0$  and  $\epsilon = 1$ . Then  $\mu_0 = -4$  and  $\mu = -1$ , i.e.  $K_2 = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$ . Since  $H_1 = \frac{\sqrt{5}}{4}$

we have

$$\frac{N^{\frac{1}{2}}(\mu_0)}{4H_1} \leq \frac{4\sqrt{5}}{5} < 2.$$

Hence by corollary 2,  $K_2$  has class number 1.

Example 2. Let  $m = 3$ ,  $\tau = 0$ ,  $\epsilon = \epsilon_0 = 2 + \sqrt{3}$ .  
Then  $\mu_0 = -4\epsilon_0$ , and  $\mu = -\epsilon_0$ , i.e.  $K_2 = Q(\sqrt{3}, \sqrt{-2-\sqrt{3}})$ .  
From theorem 1,  $H_1 < 2/d = 1/6$ . Hence

$$\frac{N^{\frac{1}{2}}(\mu_0)}{4H_1} < 6.$$

Therefore from theorem 18 every ideal class of  $K_2$  contains an ideal of norm less than or equal to 5. But since 5 does not factor in  $K_1 = Q(\sqrt{3})$  there are no ideals of norm 5 and the classes which contain factors of 2 and 3 generate the group of ideal classes.

Since  $(2) = (1 + \sqrt{3})^2$  in  $O_{K_1}$  and  $\nu^2 \equiv -\epsilon_0 \pmod{2}$  is unsolvable in  $O_{K_1}$ .  $\gamma_1 = 1$ ,  $\Omega = \sqrt{\mu}$  and  $\delta = 4\mu$ .

Hence from theorem 11 we have

$$(2) = (1 + \sqrt{3})^2 = (1 + \sqrt{3}, 1 + \sqrt{-\epsilon_0})^4 = L^4$$

$$(3) = (\sqrt{3})^2 = (\sqrt{3}, 1 + \sqrt{-\epsilon_0})^2 (\sqrt{3}, 1 - \sqrt{-\epsilon_0})^2 = P_1^2 P_2^2$$

If  $L$  were a principal ideal generated by  $A$ , then we would have  $N_{K_2/K_1}(A) = (1 + \sqrt{3})\epsilon_0^k$  which is not totally positive, contradicting theorem 20. Hence  $L$  cannot be principal.

Similarly  $P_1$  and  $P_2$  are not principal. But  $L^2$  and  $P_1P_2$  are principal and

$$\begin{aligned} P_1L &= (3+\sqrt{3}, \sqrt{3}(1+\sqrt{-\epsilon_0}), (1+\sqrt{3})(1+\sqrt{-\epsilon_0}), (1+\sqrt{-\epsilon_0})^2) \\ &= (1+\sqrt{-\epsilon_0})(1-\sqrt{-\epsilon_0}, \sqrt{3}, 1+\sqrt{3}, 1+\sqrt{-\epsilon_0}) \\ &= (1+\sqrt{-\epsilon_0}) \end{aligned}$$

since  $(\sqrt{3}, 1+\sqrt{3}) = 1$ . Hence  $P_1$ ,  $P_2$  and  $L$  all belong to the same ideal class and thus  $K_2$  has class number 2.

Example 3. Let  $m = 11$ ,  $\tau = 1$  and  $\epsilon = 1$ . Then  $\mu_0 = -3 = \mu$  and  $K_2 = \mathbb{Q}(\sqrt{11}, \sqrt{-3})$ . Since  $\nu = 1$  satisfies  $\nu^2 \equiv \mu \pmod{4}$ ,  $\delta = -3$  and  $\Omega = \frac{1+\sqrt{-3}}{2}$ . From theorem 1,  $H_1 > 2/d = 1/22$  and hence  $\frac{N(\mu_0)}{4H_1} < 17$ . Therefore from theorem 18 every ideal class of  $K_2$  contains an ideal with norm 16 or less. Hence the classes which contain factors of primes less than 16 generate the group of ideal classes.

Since  $(2) = (\lambda)^2$  in  $\mathcal{O}_{K_1}$ , where  $\lambda = 3+\sqrt{11}$ , by theorem 18,  $(\lambda)$  factors in  $\mathcal{O}_{K_2}$  if and only if

$$(38) \quad \alpha^2 \equiv -3 \pmod{\lambda^5}$$

is solvable in  $\mathcal{O}_{K_1}$ . If we let  $\alpha = x+y\sqrt{11}$ , then after expanding and multiplying through by  $\lambda$ , (38) becomes

$$(39) \quad 3x^2+33y^2+9-22xy = (6xy-x^2-11y^2-3)\sqrt{11} \equiv 0 \pmod{8}.$$

Now (39) is solvable if and only if

$$(40) \quad 3x^2 + y^2 + 2xy + 1 \equiv 0 \pmod{8}$$

and

$$(41) \quad 6xy - x^2 - 3y^2 - 3 \equiv 0 \pmod{8}$$

have a common solution in rational integers  $x$  and  $y$ . But

(41) implies  $x \not\equiv y \pmod{2}$  and then (40) becomes

$$3x^2 + 2xy + y^2 + 1 = 2x^2 + (x+y)^2 + 1 \equiv 2x^2 + 2 \equiv 0 \pmod{8}$$

which is impossible. Thus  $(\lambda)$  does not factor in  $O_{K_2}$ .

(3) does not factor in  $O_{K_1}$ , but  $(3) = (\sqrt{-3})^2$  in  $O_{K_2}$ .

(5) =  $(4 + \sqrt{11})(4 - \sqrt{11})$  in  $O_{K_1}$ , but the congruences  $\alpha^2 \equiv -3 \pmod{4 \pm \sqrt{11}}$  are seen to be impossible by testing a complete residue system  $\pmod{4 \pm \sqrt{11}}$  (e.g. 0, 1, 2, 3, 4). Therefore neither of the factors of (5) factor further in  $O_{K_2}$ .

It is easily verified that the factorization of (7) is

$$\begin{aligned} (7) &= (2 + \sqrt{11})(2 - \sqrt{11}) \\ &= (2 + \sqrt{11}, 2 + \sqrt{-3})(2 + \sqrt{11}, 2 - \sqrt{-3})(2 - \sqrt{11}, 2 + \sqrt{-3})(2 - \sqrt{11}, 2 - \sqrt{-3}). \end{aligned}$$

(11) =  $(\sqrt{11})^2$  in  $O_{K_1}$  and  $\alpha^2 \equiv -3 \pmod{\sqrt{11}}$  is unsolvable in  $O_{K_1}$ ; hence  $(\sqrt{11})$  does not factor in  $O_{K_2}$ .

(13) does not factor in  $O_{K_1}$ . Therefore any factor of (13) would have norm  $13^2$  which is bigger than  $\frac{N^{\frac{1}{2}}(\mathcal{L}_0)}{4H_1}$ . Hence the class containing a factor of (13) contains an ideal of norm less than  $\frac{N^{\frac{1}{2}}(\mathcal{L}_0)}{4H_1}$ .

All the above ideals are principal with the possible exception of the factors of (7). As in example 2 these are

not principal since  $\epsilon_0 = 10+3\sqrt{11}$  is totally positive and  $2+\sqrt{11}$  is not totally positive. If we let  $P_1, P_2, P_3, P_4$  denote the four factors of (7) listed in the above order, we see  $P_1P_3 = (2+\sqrt{-3})$  and  $P_2P_4 = (2-\sqrt{-3})$ . Therefore since  $P_1P_2 = (2+\sqrt{11})$  and  $P_3P_4 = (2-\sqrt{11})$ ,  $P_1 \sim P_4$  and  $P_2 \sim P_3$ . Hence all non-principal ideals are equivalent to  $P_1$  or  $P_2$ . Now  $P_1^3$  cannot be principal because if  $P_1^3 = (A)$ , then  $N_{K_2/K_1}^3(A) = (2+\sqrt{11})^3 \epsilon_0^k$  which is not totally positive, contradicting theorem 20. Hence the order of the group cannot be 3 and thus  $K_2$  has class number 2.

In Example 3 it was shown that the non-principal ideals of smallest norm were the factors of (7). Therefore if  $H_1 > 3/28$  we would have  $\frac{N^{\frac{1}{2}}(\mu_0)}{4H_1} < 7$  and we would be led, by theorem 18, to the false conclusion that  $Q(\sqrt{11}, \sqrt{-3})$  has class number 1. Hence for  $m = 11$ ,  $H_1 \leq 3/28$ . In the same manner the following upper bounds for  $H_1$  have been determined for the values of  $m$  listed below.

$m = 3$	$H_1 \leq 1/2$	$m = 17$	$H_1 \leq 1/2$
$m = 6$	$H_1 \leq 1/4$	$m = 21$	$H_1 \leq 1/5$
$m = 7$	$H_1 \leq 1/4$	$m = 33$	$H_1 \leq 1/2$
$m = 11$	$H_1 \leq 3/28$	$m = 41$	$H_1 \leq 1/2$
$m = 14$	$H_1 \leq 3/28$		

12. Class Number Unequal to 1

In Table II on page 47 it is seen that many fixed point fields do not have class number 1. The following theorems attempt to "explain" why certain fields fail to have class number 1.

THEOREM 21. Let  $\epsilon_0$  (the fundamental unit in  $K_1$ ) have norm +1. If there exists a prime  $\pi$  in  $\mathcal{O}_{K_1}$  such that  $N(\pi) = -p$  and  $(\pi) = P_1 P_2$  in  $\mathcal{O}_{K_2}$ , then  $P_1$  and  $P_2$  are not principal. (Hence  $K_2$  does not have class number 1.)

Proof. Suppose  $P_1 = (A)$ . Then

$$(42) \quad N_{K_2/K_1}(A) = \pi \epsilon_0^n$$

but  $\pi \epsilon_0^n$  is not totally positive since its norm is negative. Hence by theorem 20 (42) is impossible. Therefore  $P_1$  cannot be principal.

As the hypotheses show, the following theorem can be applied not only to fixed point fields, but also to certain other relative quadratic fields.

THEOREM 22. Let  $K_1 = \mathbb{Q}(\sqrt{m})$  where  $m \not\equiv 5 \pmod{8}$  and  $K_1$  has class number 1. Let  $K_2 = K_1(\sqrt{\mu})$  where  $\mu$  is a totally negative square-free integer in  $K_1$  and  $N(\mu) \neq 2$ . If  $\delta = 4\mu$ , then  $K_2$  has even class number.

Proof. Since  $m \not\equiv 5 \pmod{8}$ , (2) factors in  $\mathcal{O}_{K_1}$ . If  $\lambda$  denotes a factor of 2,  $\lambda | \delta = 4\mu$  and hence  $(\lambda) = L^2$  in  $\mathcal{O}_{K_2}$ . Suppose  $L = (A)$ , then  $N_{K_2/\mathbb{Q}}(A) = 2$ . Let  $A = \alpha + \beta\sqrt{\mu}$ , where  $\alpha, \beta \in \mathcal{O}_{K_1}$  ( $\Omega = \sqrt{\mu}$  since  $\delta = 4\mu$ ). Then

$$(43) \quad N_{K_2/K_1}(A) = \alpha^2 - \mu\beta^2 = 2\sqrt{-\mu}|\alpha\beta|$$

and

$$(44) \quad N_{K_2/K_1}(A)^s = (\alpha^s)^2 - \mu^s(\beta^s)^2 = 2\sqrt{-\mu^s}|\alpha^s\beta^s|$$

since  $\mu \ll 0$ . Multiplying (43) and (44) we obtain

$$(45) \quad N_{K_2/\mathbb{Q}}(A) \geq 4N^{\frac{1}{2}}(\mu)|N(\alpha\beta)|.$$

Now if  $\alpha\beta \neq 0$  we see from (45) that  $N_{K_2/\mathbb{Q}}(A) \geq 4$  which is impossible. Clearly  $\beta \neq 0$  and if  $\alpha = 0$  (43) and (45) give  $N_{K_2/\mathbb{Q}}(A) = N^2(\beta)N(\mu)$  which cannot be 2 since  $N(\mu) \neq 2$ . Thus  $L$  cannot be principal and since  $L^2$  is principal the class containing  $L$  has period 2. Therefore  $K_2$  has even class number.

COROLLARY 3. If  $K_2$  is a fixed point field with  $m \equiv 1 \pmod{8}$  and  $\mu = -1$ , then  $K_2$  has even class number.

Proof. In  $K_1$ ,  $(2) = (\lambda)(\lambda^s)$  where  $(\lambda, \lambda^s) = 1$ . If  $\rho \in \mathcal{O}_{K_1}$  were such that  $\rho^2 \equiv -1 \pmod{\lambda^2}$ , then  $(\rho^s)^2 \equiv -1 \pmod{(\lambda^s)^2}$ , and by the Chinese Remainder Theorem

$$(46) \quad \alpha^2 \equiv -1 \pmod{4}$$

would be solvable. Let  $\alpha = x+y\omega$  where  $\omega = \frac{1+\sqrt{m}}{2}$  and also let  $m = 8n+1$ . Then (46) becomes

$$(47) \quad x^2+2ny^2+1 + (2xy+y^2)\omega \equiv 0 \pmod{4}.$$

Now (47) is solvable if and only if

$$(48) \quad x^2+2ny^2+1 \equiv 0 \pmod{4}$$

and

$$(49) \quad 2xy+y^2 \equiv 0 \pmod{4}$$

have a common solution in rational integers  $x$  and  $y$ . But

(49) implies  $y \equiv 0 \pmod{2}$  and then (48) becomes

$x^2+1 \equiv 0 \pmod{4}$  which is impossible. Hence (46) is

unsolvable and thus  $\delta = 4\mu$ . Therefore by theorem 22,

$K_2$  has even class number.

COROLLARY 4. Let  $K_2$  be a fixed point field with  $m \not\equiv 1 \pmod{4}$  and  $\mu = a+b\sqrt{m}$ . If  $b$  is odd and  $N(\mu) \neq 2$ , then  $K_2$  has even class number.

Proof. Since  $m \not\equiv 1 \pmod{4}$ ,  $(2) = (\lambda)^2$  in  $O_{K_1}$ . If  $\alpha = x+y\sqrt{m}$ , then  $\alpha^2 \equiv \mu \pmod{\lambda^2}$  is solvable in  $O_{K_1}$  if and only if

$$(50) \quad x^2 + my^2 - a + (2xy - b)\sqrt{m} \equiv 0 \pmod{2}$$

is solvable in rational integers  $x$  and  $y$ . But since  $b$  is odd  $2xy - b \equiv 1 \pmod{2}$  and hence (50) is impossible.

Since  $\alpha^2 \equiv \mu \pmod{\lambda^2}$  is unsolvable in  $O_{K_1}$ ,  $\delta = 4\mu$  and by theorem 22,  $K_2$  has even class number.

### 13. Concluding Remarks

The theorems in the previous section do not cover all the cases in Table II, where the class number is unequal to 1. It is expected that more inclusive theorems can be found, which give sufficient conditions for failure of unique factorization in fixed point fields.

The general definition of the Hilbert modular group and the statement of theorem 2 suggest that the definition of a fixed point field might be generalized to allow  $K_1$  to be a totally real field with unique factorization and of arbitrary (finite) degree over the rationals. With this generalization it appears that, after making the appropriate changes in the theorems in section 5, the proof of theorem 18 will carry over. The essential properties used in the proof depend on the fact that  $K_2$  was a quadratic extension of  $K_1$  and that  $K_1$  was a field chosen so that theorem 2A would apply. It does not seem reasonable, however, to expect theorem 15 to carry over, since  $K_1$  may not be normal. Theorem 19 also would not be expected to generalize since its proof depended on knowing the structure of units in  $K_1$ .

Besides generalizing the definition of a fixed point field, it is hoped that in the future other useful properties of fixed point fields can be established.

TABLE I

Admissible Values of  $\mu_0$  for Selected Values of  $m$ 

$m$	$\epsilon$	$\tau$	$\mu_0$	$\sigma$	$\mu$
2	1	0	-4	2	-1
		1	-3	1	-3
		$\sqrt{2}$	-2	$\sqrt{2}$	-1
3	1	0	-4	2	-1
		1	-3	$\sqrt{3}$	-1
		$\sqrt{3}$	-1	1	-1
	$2+\sqrt{3}$	0	$-4(2+\sqrt{3})$	2	$-(2+\sqrt{3})$
		1	$-7-4\sqrt{3}$	$2+\sqrt{3}$	-1
$2+\sqrt{3}$		-1	1	-1	
	$1+\sqrt{3}$	$-2(2+\sqrt{3})$	$1+\sqrt{3}$	-1	
5	1	0	-4	2	-1
		1	-3	1	-3
		$(1\pm\sqrt{5})/2$	$(-5\pm\sqrt{5})/2$	1	$(-5\pm\sqrt{5})/2$
6	1	0	-4	2	-1
		1	-3	$3-\sqrt{6}$	$-(5+2\sqrt{6})$
	$5+2\sqrt{6}$	0	$-4(5+2\sqrt{6})$	2	$-(5+2\sqrt{6})$
		$2+\sqrt{6}$	$-2(5+2\sqrt{6})$	$2+\sqrt{6}$	-1
	$3+\sqrt{6}$	$-(5+2\sqrt{6})$	1	$-(5+2\sqrt{6})$	
7	1	0	-4	2	-1
		1	-3	1	-3
	$8+3\sqrt{7}$	0	$-4(8+3\sqrt{7})$	2	$-(8+3\sqrt{7})$
$3+\sqrt{7}$		$-2(8+3\sqrt{7})$	$3+\sqrt{7}$	-1	

TABLE I (Continued)

$m$	$\epsilon$	$\tau$	$\mu_0$	$\sigma$	$\mu$
11	1	0	-4	2	-1
		1	-3	1	-3
	$10+3\sqrt{11}$	0	$-4(10+3\sqrt{11})$	2	$-(10+3\sqrt{11})$
		$3+\sqrt{11}$	$-2(10+3\sqrt{11})$	$3+\sqrt{11}$	-1
13	1	0	-4	2	-1
		1	-3	1	-3
14	1	0	-4	2	-1
		1	-3	1	-3
	$15+4\sqrt{14}$	0	$-4(15+4\sqrt{14})$	2	$-(15+4\sqrt{14})$
		$4+\sqrt{14}$	$-2(15+4\sqrt{14})$	$4+\sqrt{14}$	-1
17	1	0	-4	2	-1
		1	-3	1	-3
21	1	0	-4	2	-1
		1	-3	$(3-\sqrt{21})/2$	$-(5+\sqrt{21})/2$
	$(5+\sqrt{21})/2$	0	$-4(5+\sqrt{21})/2$	2	$-(5+\sqrt{21})/2$
		$(3+\sqrt{21})/2$	$-(5+\sqrt{21})/2$	1	$-(5+\sqrt{21})/2$
33	1	0	-4	2	-1
		1	-3	$6+\sqrt{33}$	$-(23+4\sqrt{33})$
	$23+4\sqrt{33}$	0	$-4(23+4\sqrt{33})$	2	$-(23+4\sqrt{33})$
		$6+\sqrt{33}$	$-(23+4\sqrt{33})$	1	$-(23+4\sqrt{33})$
41	1	0	-4	2	-1
		1	-3	1	-3

TABLE II

## Class Number of Specific Fixed Point Fields

Fixed Point Fields	$\delta$	Class Number
$Q(\sqrt{2}, \sqrt{-1})$	$\lambda^2 \mu$	1
$Q(\sqrt{2}, \sqrt{-3})$	$\mu$	1
$Q(\sqrt{3}, \sqrt{-1})$	$\mu$	1
$Q(\sqrt{3}, \sqrt{-2-\sqrt{3}})$	$4\mu$	2
$Q(\sqrt{5}, \sqrt{-1})$	$4\mu$	1
$Q(\sqrt{5}, \sqrt{-3})$	$\mu$	1
$Q(\sqrt{5}, \sqrt{(-5 \pm \sqrt{5})/2})$	$\mu$	1
$Q(\sqrt{6}, \sqrt{-1})$	$\lambda^2 \mu$	2
$Q(\sqrt{6}, \sqrt{-5-2\sqrt{6}})$	$\mu$	1
$Q(\sqrt{7}, \sqrt{-1})$	$\mu$	1
$Q(\sqrt{7}, \sqrt{-3})$	$\mu$	2
$Q(\sqrt{11}, \sqrt{-1})$	$\mu$	1
$Q(\sqrt{11}, \sqrt{-3})$	$\mu$	2
$Q(\sqrt{13}, \sqrt{-1})$	$4\mu$	1
$Q(\sqrt{17}, \sqrt{-1})$	$4\mu$	2
$Q(\sqrt{17}, \sqrt{-3})$	$\mu$	1
$Q(\sqrt{21}, \sqrt{-1})$	$4\mu$	2
$Q(\sqrt{21}, \sqrt{(-5-\sqrt{21})/2})$	$\mu$	1
$Q(\sqrt{33}, \sqrt{-23-4\sqrt{33}})$	$\mu$	1
$Q(\sqrt{41}, \sqrt{-3})$	$\mu$	1

## REFERENCES

- [ 1 ] H. Cohn, A Second Course in Number Theory, Wiley, New York, 1962.
- [ 2 ] H. Cohn, "On the Shape of the Fundamental Domain of the Hilbert Modular Group", Proc. Symposium of Recent Developments in Number Theory, (1963), A. M. S. Providence, Rhode Island, 1965.
- [ 3 ] R. DeVore, The Lowest Points in the Fundamental Domains of the Hilbert Modular Groups for  $\mathbb{Q}(\sqrt{5})$  and  $\mathbb{Q}(\sqrt{2})$ , Ph.D. Dissertation, University of Arizona, 1964.
- [ 4 ] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Akademische Verlag, Leipzig, 1923.
- [ 5 ] H. Maass, Über Gruppen von hyperabelschen Transformationen, Sitzber, Heidelberg, Akad. der Wiss., 1940.
- [ 6 ] J. Sommer, Introduction a la Théorie des Nombres Algébriques, Hermann, Paris, 1911.
- [ 7 ] H. Weyl, Algebraic Theory of Numbers, Annals of Math. Study Number 1., Princeton Press, 1940.