INDICES OF PRINCIPAL ORDERS IN ALGEBRAIC NUMBER FIELDS

Thesis by

Melvin John Knight

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

1975

(Submitted May 16, 1975)

ACKNOWLEDGMENTS

I want to thank my wife Beth for her love and encouragement.

I would also like to thank Dr. Olga Taussky Todd for the many talks we had on this problem and the help that she gave me.

This topic was suggested to me by my adviser, Dr. Kisilevsky, and he also gave me the most important references. I appreciate the help he gave me and the opportunity I had to work with him.

I received financial support from the U.S. Department of Health, Education, and Welfare in the form of an NDEA Fellowship, from the ARCS Foundation through their Fellowship, and from the California Institute of Technology through research and teaching assistantships.

ABSTRACT

Let K be an extension of Q of degree n and $\mathfrak{O}_K$ the ring of integers of K. If θ is an algebraic integer of K and $K = Q(\theta)$, then $Z[\theta]$ is a suborder of $\mathfrak{O}_K$ of finite index. This index is called the index of θ. If k is a rational integer, the numbers θ and $\theta + k$ have equal indices. Define two numbers to be equivalent if their difference is a rational integer.

Using Schmidt's extension of Thue's Theorem it is shown that in any field of degree less than or equal to four there exist only a finite number of inequivalent numbers with index bounded by any given number. This is true for every finite extension of Q and a proof is given using a slight generalization of Schmidt's Theorem.

An application of Schmidt's Theorem to a problem on the units in a cyclic field of prime degree is given.

TABLE OF CONTENTS

INTRODUCTION

Let K be a finite extension of Q with $[K:Q] = n$. An order $\mathfrak{O}$ of K is a finitely generated Z-module which contains a basis for K over Q and is also a ring with 1. An order is called principal if it is of the form $Z[\theta]$ for some $\theta \in K$. It is well-known that K contains a unique maximal order and that it is the ring of integers of K, denoted $\mathfrak{O}_K$. It is easy to see that $Z[\theta]$ is a principal order of K if and only if $K = Q(\theta)$ and $\theta \in \mathfrak{O}_K$.

From the theory of finitely generated modules over principal ideal domains it follows that every order of K is a free Z-module and contains a free integral basis. Thus, if $\mathfrak{O}$ is an order of K, then there exist numbers $\omega_1, \dots, \omega_n$ in $\mathfrak{O}$ such that

1) $$\mathfrak{O} = \{z_1\omega_1 + \dots z_n\omega_n \mid z_i \in Z\}$$

and each number in $\mathfrak{O}$ is uniquely represented in (1). The vector $(\omega_1, \omega_2, \dots, \omega_n)$ is called an integral basis for $\mathfrak{O}$. The principal order $Z[\theta]$ has the integral basis $(1, \theta, \theta^2, \dots, \theta^{n-1})$. Such a basis is called a power basis.

Let $\mathfrak{O}' \subseteq \mathfrak{O}$ be two orders of K with bases $(\lambda_1, \lambda_2, \dots, \lambda_n)$ and $(\theta_1, \theta_2, \dots, \theta_n)$ respectively, then there exists unique integers $a_{i,j}$ satisfying

$$\lambda_i = a_{i,1}\theta_1 + a_{i,2}\theta_2 + \cdots a_{i,n}\theta_n, \qquad (i = 1, 2, \dots, n),$$

and the integral matrix $A = (a_{i,j})$ satisfies

2) $$A \begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} .$$

Since $\mathfrak{O}'$ and $\mathfrak{O}$ each have rank n, the determinant of A is not zero. The index of $\mathfrak{O}'$ as a subgroup of $\mathfrak{O}$ is $(\mathfrak{O}:\mathfrak{O}') = |\det A|$. If $\mathfrak{O}' = Z[\lambda]$ the special notation, $\text{Index}_{\mathfrak{O}}(\lambda)$, will be used for $(\mathfrak{O}:Z[\lambda])$. If $\mathfrak{O} = \mathfrak{O}_K$, then $(\mathfrak{O}:Z[\lambda])$ will be denoted by Index (λ).

The number θ is a generator of the principal order $\mathfrak{O}$ if $\mathfrak{O} = Z[\theta]$. It is easy to see that $\theta + k$ is also a generator of $\mathfrak{O}$ if k is any rational integer, so there are always an infinite number of generators of any principal order. Call two numbers equivalent if they differ by a rational integer.

The following theorem was proved by Hall [9]. The proof is given in Chapter 1.

Theorem 1: Let $[K:Q] \leq 3$. For every $c > 0$ there exist only a finite number of inequivalent $\lambda \in \mathfrak{O}_K$ satisfying

$$\text{Index}(\lambda) = c .$$

It is not difficult to show that for every order $\mathfrak{O}$ in such a field and $c > 0$ there exist only a finite number of inequivalent $\lambda \in \mathfrak{O}$ such that $\text{Index}_{\mathfrak{O}}(\lambda) = c$. This is the corollary following lemma 1 in Chapter 1. An order $\mathfrak{O}$ of an arbitrary field K with this property is said to have the bounded index property since there exist only a finite number of inequivalent $\lambda \in \mathfrak{O}$ with a given non-zero index.

The major tool required for the proof of Theorem 1 is Thue's Theorem on the integer solutions of certain diophantine equations, but this cannot be used to prove the corresponding result when $[K:Q] > 3$. The general result which is proved here uses the generalization of Thue's Theorem proved by Schmidt [13]. This result, the proof of which is given in Chapter 4, is given by the following theorem.

Theorem 2: Let K be a finite extension of Q, $\mathfrak{O}$ an order of K, and $c > 0$ constant, then there exist only a finite number of inequivalent $\lambda \in \mathfrak{O}$ satisfying

$$\mathrm{Index}_{\mathfrak{O}}(\lambda) = c .$$

In other words, every order of every finite extension of Q has the bounded index property.

The end of each proof is indicated by the symbol § near the right margin.

CHAPTER 1

A SYSTEM OF DIOPHANTINE EQUATIONS

The following lemma is useful for the proof of Theorem 1 and also shows that the theorem generalizes to every order of the field.

Lemma 1: Let K be any finite extension of Q and $\mathfrak{D}_1$, $\mathfrak{D}_2$ any two orders of K, then $\mathfrak{D}_1$ has the bounded index property if and only if $\mathfrak{D}_2$ has it.

Proof: It suffices to show that if $\mathfrak{D}_1$ does not have it then $\mathfrak{D}_2$ also will not have it. Suppose that $\{\lambda_1, \lambda_2, \ldots\}$ is an infinite set of inequivalent numbers in $\mathfrak{D}_1$ each with index in $\mathfrak{D}_1$ equal to the non-zero constant c. The result will follow from showing that a certain multiple of the λ's will all lie in the order $\mathfrak{D}_2$ and have a common non-zero index in it also, so $\mathfrak{D}_2$ will not have the bounded index property.

If $\mathfrak{D}' \subseteq \mathfrak{D}$ are two orders of a field K with $(\mathfrak{D}:\mathfrak{D}') = m$, then $m\mathfrak{D} \subseteq \mathfrak{D}'$, since the factor group $\mathfrak{D}/\mathfrak{D}'$ has order m.

Let $(\mathfrak{D}_K:\mathfrak{D}_1) = m_1$ and $(\mathfrak{D}_K:\mathfrak{D}_2) = m_2$, then for each λ_i, $i = 1, 2, \ldots$, $m_2\lambda_i \in \mathfrak{D}_2$. The set $\{m_2\lambda_1, m_2\lambda_2, \ldots\}$ is an infinite set of inequivalent numbers in $\mathfrak{D}_2$ which satisfy

$$3) \qquad \mathrm{Index}_{\mathfrak{D}_2}(m_2\lambda_i) = m_1 m_2^{\frac{(n-2)(n+1)}{2}} c \,, \quad (i = 1, 2, \ldots) .$$

It is clear that they are inequivalent because if $m_2\lambda_i - m_2\lambda_j$ is a rational integer, then $\lambda_i - \lambda_j$ must be rational, but it is also an algebraic integer, so a rational integer and λ_i is equivalent to λ_j. To calculate the index notice that $m_2\lambda_i$ is also in $Z[\lambda_i]$ and calculate Index $(m_2\lambda_i)$ two ways.

First by using the fact that $Z[m_2\lambda_i]$ is contained in $Z[\lambda_i]$

$$\begin{aligned}(\mathfrak{O}:Z[m_2\lambda_i]) &= (\mathfrak{O}:\mathfrak{O}_1)(\mathfrak{O}_1:Z[\lambda_i])(Z[\lambda_i]:Z[m_2\lambda_i]) \\ &= (m_1)(c)\left(m_2^{\frac{n(n-1)}{2}}\right) .\end{aligned}$$

The last index follows easily since the matrix of the transformation is diagonal. Similarly, $Z[m_2\lambda_i]$ is a suborder of $\mathfrak{O}_2$, so its index also satisfies

$$(\mathfrak{O}:Z[m_2\lambda_i]) = (\mathfrak{O}:\mathfrak{O}_2)(\mathfrak{O}_2:Z[m_2\lambda_i]) .$$

Combining these two equations gives (3).

Therefore, $\mathfrak{O}_2$ does not have the bounded index property and the lemma follows. §

Corollary: If $[K:Q] \leq 3$, then every order has the bounded index property.

Proof: Theorem 1 shows that $\mathfrak{O}_K$ has it, so every order must by lemma 1. §

The proof of Theorem 1 requires Thue's Theorem, which is stated here for convenience. A proof is given in Mordell [12].

Theorem 2 (Thue): The equation

$$f(x, y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n = m \neq 0 ,$$

where $n \geq 3$ and $f(x, y)$ is irreducible in the rational field, has only a finite number of integer solutions.

Proof of Theorem 1: If $n = 1$, so $K = Q$, then every integer is equivalent to 1 and the result is trivial.

Suppose now that $n = 2$. By lemma 1 it suffices to consider a principal order $\mathfrak{O} = Z[\theta]$. Every finite extension of Q has such orders. If $\lambda \in \mathfrak{O}$ with index $c > 0$, then $\lambda = a_0 + a_1\theta$ for unique integers a_0, a_1 and the matrix transforming the basis $(1, \theta)$ of $\mathfrak{O}$ into the basis $(1, \lambda)$ of $Z[\lambda]$ is

$$\begin{pmatrix} 1 & 0 \\ a_0 & a_1 \end{pmatrix} .$$

This has determinant a_1, so $|a_1| = c$ and λ is equivalent to either $c\theta_1$ or to $-c\theta_1$.

If $n = 3$ it again suffices to prove the principal order $\mathfrak{O} = Z[\theta]$ has the bounded index property, where $K = Q(\theta)$. Let θ be a root of the irreducible cubic equation

$$g(t) = t^3 + r_1t^2 + r_2t + r_3 , \tag{4)}$$

where r_1, r_2, and r_3 are integers. Every element in $\mathfrak{O}$ can be written uniquely as an integral combination of the power basis

$(1, \theta, \theta^2)$. In particular,

$$\begin{aligned} \theta^3 &= -r_3 - r_2\theta - r_1\theta^2 \\ \theta^4 &= (r_1r_3) + (r_1r_2 - r_3)\theta + (r_1^2 - r_2)\theta^2 \end{aligned} \tag{5}$$

because of (4). If $\lambda \in \mathfrak{D}$, then $\lambda = a_0 + a_1\theta + a_2\theta^2$ for some integers a_0, a_1, a_2, and using (5)

$$\lambda^2 = (a_0^2 - 2r_3a_1a_2 + r_1r_3a_2^2) + (2a_0a_1 - 2r_2a_1a_2 + [r_1r_2 - r_3]a_2^2)\theta$$
$$+ (2a_0a_2 + a_1^2 - 2r_1a_1a_2 + [r_1^2 - r_2]a_2^2)\theta^2 .$$

The determinant of the matrix A which transforms the basis $(1, \theta, \theta^2)$ is easily calculated from the expressions of $1, \lambda$, and λ^2 in terms of the basis $(1, \theta, \theta^2)$, giving

$$\det A = a_1^3 - 2r_1a_1^2a_2 + (r_1^2 + r_2)a_1a_2^2 + (r_3 - r_1r_2)a_2^3 . \tag{6}$$

Notice that a_0 does not appear in (6) since equivalent numbers have equal index. The polynomial in (6) may be written $a_2^3f(a_1/a_2)$, where $f(t) = g(t - r_1)$. Thus f is irreducible over Q since it is rationally equivalent to g.

The index of λ in $\mathfrak{D}$ is c if and only if the integers (a_1, a_2) determined by $\lambda = a_0 + a_1\theta + a_2\theta^2$ are solutions to the diophantine equation (6), where det A is either c or -c. By Thue's Theorem there are only a finite number of such integer pairs and thus only a finite number of inequivalent such λ. Thus $\mathfrak{D}$ has the bounded index property and $\mathfrak{D}_K$ must also. §

Let $K \subseteq C$ be a finite extension of Q, $\mathfrak{O} = Z[\theta]$ an order of K and $\lambda = a_0 + a_1\theta + \cdots a_{n-1}\theta^{n-1}$ any element of $\mathfrak{O}$, where $[K:Q] = n$ and each a_i is a rational integer. There are precisely n isomorphisms of K into the complex numbers. Let $\theta = \theta_1, \theta_2, \ldots, \theta_n$ denote the images of θ under these isomorphisms, so that $\lambda = \lambda_1, \lambda_2, \ldots, \lambda_n$ are the corresponding conjugates of λ. Therefore,

$$7) \qquad \lambda_i = a_0 + a_1\theta_i + \cdots a_{n-1}\theta_i^{n-1}, \qquad (i = 1, 2, \ldots, n).$$

Let $K^* = K(\theta_1, \theta_2, \ldots, \theta_n)$ and $x_1, x_2, \ldots, x_{n-1}$, Ω_1, Ω_2 be independent variables over K^*. Define the polynomial ℓ by

$$\ell(x_1, x_2, \ldots, x_{n-1} ; \Omega_1, \Omega_2) = \sum_{k=1}^{n-1} x_k \left(\frac{\Omega_1^k - \Omega_2^k}{\Omega_1 - \Omega_2} \right).$$

Since $K = Q(\theta)$, the n conjugates of θ are distinct. If θ_i, θ_j are distinct, then

$$8) \qquad \frac{\lambda_i - \lambda_j}{\theta_i - \theta_j} = \ell(a_1, a_2, \ldots, a_{n-1} ; \theta_i, \theta_j).$$

Suppose A transforms $(1, \theta, \ldots, \theta^{n-1})$ into $(1, \lambda, \ldots, \lambda^{n-1})$, then the determinant of A depends only on $a_1, \ldots, a_{n-1}$. A useful expression for this determinant was given by Dade and Taussky [5].

Lemma 2: With notation as above, let

$$9) \qquad z(x_1, x_2, \ldots, x_{n-1}) = \prod_{i<j} \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j),$$

then $z(a_1, a_2, \ldots, a_{n-1})$ is the determinant of A.

Proof: By (7) the matrix A transforms the basis $(1, \theta_i, \ldots, \theta_i^{n-1})$ to $(1, \lambda_i, \ldots, \lambda_i^{n-1})$ in the field $Q(\theta_i)$, so A satisfies the matrix equation

$$A \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & & \theta_n \\ \vdots & \vdots & & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & & \theta_n^{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & & \lambda_n \\ \vdots & \vdots & & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & & \lambda_n^{n-1} \end{pmatrix} .$$

Taking determinants in this expression gives

$$(\det A) \prod_{i<j} (\theta_i - \theta_j) = \prod_{i<j} (\lambda_i - \lambda_j) .$$

The result (9) follows from this by using (8). §

Let G be the Galois group of K^* over Q and for each $\sigma \in G$ define the action of σ on the variables $x_1, x_2, \ldots, x_{n-1}$ to be trivial, then

$$\sigma \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j) = \ell(x_1, \ldots, x_{n-1} ; \sigma\theta_i, \sigma\theta_j) .$$

Since the polynomial ℓ is symmetric in Ω_1, Ω_2 and each factor in (9) is different, each $\sigma \in G$ permutes these factors. Therefore,

$$\sigma z(x_1, \ldots, x_{n-1}) = \prod_{i<j} \sigma \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j)$$

$$= \prod_{i<j} \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j) .$$

So z is fixed by the group G, has algebraic integer coefficients and thus has rational integer coefficients.

For each choice of $1 \le i < j \le n$ let $G_{i,j}$ be the subgroup of G consisting of all $\sigma \in G$ which stabilize the set $\{\theta_i, \theta_j\}$. Thus $\sigma \in G_{i,j}$ if and only if σ fixes both θ_i and θ_j or else interchanges them. This is the subgroup of G which fixes the polynomial

$$10) \qquad \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j) .$$

Let $L_{i,j}$ be the fixed field of $G_{i,j}$. The group G induces exactly $|G| / |G_{i,j}|$ isomorphisms of $L_{i,j}$ into C given by the cosets of $G_{i,j}$ in G. This is exactly the number of factors in (9) which are conjugate to the factor given in (10).

Let

$$11) \qquad N_{L_{i,j}/Q}[\ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j)] = \Pi \sigma \ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j) ,$$

where σ .runs over a set of coset representatives of $G_{i,j}$. There are exactly $|G| / |G_{i,j}|$ factors in (11) and this polynomial is fixed by G, so it has rational integer coefficients.

Not every pair of these polynomials need be conjugate. Let S be a maximal set of pairwise non-conjugate factors $\ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j)$ of (9), so each factor in (9) is conjugate to exactly one element of S.

<u>Lemma 3</u>:

$$z(x_1, \ldots, x_{n-1}) = \prod_{S} N_{L_{i,j}/Q}[\ell(x_1, \ldots, x_{n-1} ; \theta_i, \theta_j)] .$$

Proof: Each factor of (9) is conjugate to exactly one element of S and appears only once in the product for the norm in (11). Therefore, this product is the same as (9). §

To prove that every order in a given field K over Q has the bounded index property, it is sufficient to prove it for a principal order $\mathfrak{O} = Z[\theta]$ because of lemma 1. Since each element $\lambda \in \mathfrak{O}$ may be written $\lambda = a_0 + a_1\theta + \cdots a_{n-1}\theta^{n-1}$ with uniquely determined integers $a_0, \ldots, a_{n-1}$, this element has index in $\mathfrak{O}$ equal to c if and only if

12) $$N_{L_{i,j}/Q}[\ell(a_1, \ldots, a_{n-1} ; \theta_i, \theta_j)] = c_{i,j}$$

for each polynomial in S and with the constants $c_{i,j}$ such that their product is $\pm c$. It is clear that all of these constants must be integers. Since the integers $\pm c$ have only a finite number of factorizations, the bounded index property is equivalent to the system of diophantine equations (12) having only a finite number of simultaneous integer solutions $(a_1, \ldots, a_{n-1})$ for every choice of non-zero constants $c_{i,j}$.

As an example of these lemmas, let $n = 3$ as in the proof of Theorem 1. Now equation (6) gives

$$z(a_1, a_2, a_3) = a_1^3 - 2r_1a_1^2a_2 + (r_1^2 + r_2)a_1a_2^2 + (r_3 - r_1r_2)a_2^3$$

$$= N_{K/Q}[a_1 + a_2(\theta_1 + \theta_2)]$$

with θ a root of (4).

As a second example, let $K = Q(\xi)$, ξ a primitive fifth root of one. This is a normal fourth degree field and $\mathfrak{O}_K = Z[\xi]$. The Galois group G is cyclic and generated by σ, where $\sigma(\xi) = \xi^2$. Write $\theta_1 = \xi$, $\theta_2 = \xi^2$, $\theta_3 = \xi^4$, and $\theta_4 = \xi^3$.

For the set S take

$$\{\ell(x_1, x_2, x_3 \,;\, \theta_1, \theta_2) \,,\ \ell(x_1, x_2, x_3 \,;\, \theta_1, \theta_3)\} \,.$$

The group $G_{1,2}$ is just the identity, while $G_{1,3} = \langle 1, \sigma^2 \rangle$. Therefore, $L_{1,2} = K$ and $L_{1,3} = Q(\sqrt{5}\,)$, the unique quadratic subfield of K. By lemma 3,

$$z(x_1, x_2, x_3) = N_{K/Q}\,[\ell(x_1, x_2, x_3 \,;\, \theta_1, \theta_2)]\; N_{L_{1,3}/Q}\,[\ell(x_1, x_2, x_3 \,;\, \theta_1, \theta_3)] \,.$$

Both factors have integer coefficients, the first is of fourth degree and the second is quadratic.

Notice that for each pair θ_i, θ_j the set

$$\{\ell(x_1, \ldots, x_{n-1} \,;\, \theta_i, \theta_j) \mid x_k \in Z \text{ for each } k = 1, 2, \ldots, n-1\}$$

is a Z-module. Thus, the system of norm form equations (12) is the same as a system of norms from certain modules.

Thue's Theorem may be restated in terms of modules. Let $K = Q(\alpha)$ be an extension of degree greater than 2. Thue's Theorem says that there exist only a finite number of elements in the module

$$\{x + y\alpha \mid x, y \text{ integers}\}$$

with a given non-zero norm from K to Q.

Chapter 2 gives the details of Schmidt's generalization of Thue's Theorem to more general modules.

CHAPTER 2
NORM FORM EQUATIONS

This chapter covers the material on Schmidt's Theorem [13] needed to prove Theorem 2. The proofs of some statements made here are given in [3]. Every module is assumed to be a finitely generated Z-module.

Let K be an extension of Q of degree $n = s + 2t$, where s is the number of real imbeddings and t the number of complex imbeddings of K into C, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the corresponding isomorphisms. Let $N(x_1, x_2, \ldots, x_m)$ be a norm form from K to Q; that is, for some fixed numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$ in K

$$N(x_1, \ldots, x_m) = \prod_{i=1}^{n} \sigma_i(x_1\alpha_1 + \cdots x_m\alpha_m)$$

where each variable is fixed by all of the automorphisms.

Of interest here are the integer solutions $(x_1, x_2, \ldots, x_m)$ of the norm form equation

$$(13) \qquad N(x_1, x_2, \ldots, x_m) = c$$

for some constant c.

The set of numbers of the form $x_1\alpha_1 + \cdots x_m\alpha_m$ where $x_1, x_2, \ldots, x_m$ take on all possible integer values is denoted by

$$M = \{x_1\alpha_1 + \cdots x_m\alpha_m\}$$

and is a finitely generated Z-module. It follows that M has a free Z-basis $(\beta_1, \beta_2, \ldots, \beta_k)$. The integer k is the rank of M and is less than or equal to n.

The solutions to (13) are easily found from the solutions μ of the equation

$$N_{K/Q}(\mu) = c , \qquad \mu \in M . \tag{14}$$

The integers $(x_1, x_2, \ldots, x_m)$ are found by solving a system of equations which depends on the relationship between the set $(\alpha_1, \ldots, \alpha_m)$ and the basis $(\beta_1, \ldots, \beta_k)$ of M. Therefore, it suffices to find all solutions to (14). Since only $\mu = 0$ is a solution if $c = 0$, assume $c \neq 0$ for all that follows.

Suppose now that M is full in K, i.e. that rank $M = n$. It is possible to solve (14) for all solutions in a finite number of steps. First, for a full module define the coefficient ring

$$\mathfrak{O}_M = \{\nu \in K \mid \nu\mu \in M \text{ for all } \mu \in M\} .$$

It is proved in Lemma 5 that this is an order in K. Let $U_M^{K/Q}$ be the group of units in $\mathfrak{O}_M$ with norm from K to Q equal to +1, a subgroup of index 2 or 1 in the full group of units of $\mathfrak{O}_M$ depending on whether there exists a unit with norm -1 or not.

By the Dirichlet Unit Theorem for orders, there exists a set of $r = s + t - 1$ units $\eta_1, \ldots, \eta_r$ such that every unit in $\mathfrak{O}_M$ can be written uniquely as

$$\xi \, \eta_1^{a_1} \ldots \eta_r^{a_r}$$

where ξ is a root of 1 and $a_1, \dots, a_r$ are integers. Since the units $\eta_1, \dots, \eta_r$ can be calculated in a finite number of steps, so can $U_M^{K/Q}$.

For every $\mu \in M$ the set

$$15) \qquad \mu\, U_M^{K/Q}$$

is the set of all associates of μ over $\mathfrak{O}_M$ with the same norm and is called an <u>(M, K)-family</u>.

Finally, there exists an effectively computable constant γ such that every solution to (14) has an associate over $\mathfrak{O}_M$ which is also a solution and with height bounded by γ. Each of these solutions can be calculated in a finite number of steps, so all solutions to (14) are contained in the union of a finite number of families of the form (15), where μ is one of these solutions with height bounded by γ. For full details on this method see [3, p. 122].

As an example of a norm form equation for a nonfull module take the equation

$$16) \qquad N_{K/Q}(\mu) = 3^2 \cdot 5^2 , \qquad \mu \in M$$

where $M = \{x_1\sqrt{3} + x_2\sqrt{5} + x_3\sqrt{15}\}$ and $K = Q(\sqrt{3}, \sqrt{5})$.

All solutions to (16) with $x_1x_2x_3 = 0$ can be given. If $x_1 = 0$, then μ must lie in the submodule

$$M_1 = \{x_2\sqrt{5} + x_3\sqrt{15}\} .$$

This is proportional to the full module $\{x_2 + x_3\sqrt{3}\}$ of the field

$L_1 = Q(\sqrt{3})$ and therefore

$$N_{K/Q}[(\sqrt{5})(x_2 + x_3\sqrt{3})] = 5^2[N_{L_1/Q}(x_2 + x_3\sqrt{3})]^2 .$$

Using this with (16) gives

$$N_{L_1/Q}(x_2 + x_3\sqrt{3}) = \pm 3$$

and all solutions are given by

$$x_2 + x_3\sqrt{3} = \pm\sqrt{3}(2 + \sqrt{3})^t$$

for every integer t.

If $x_2 = 0$, then μ will lie in the submodule

$$M_2 = \{x_1\sqrt{3} + x_3\sqrt{15}\}$$

which is proportional to a full module of the field $L_2 = Q(\sqrt{5})$. Again, (16) reduces to an equation from a subfield:

$$N_{L_2/Q}(x_1 + x_3\sqrt{5}) = \pm 5 .$$

The solutions to this equation are all given by

$$(x_1 + x_3\sqrt{5}) = \pm\sqrt{5}(2 + \sqrt{5})^t$$

for every integer t.

When $x_3 = 0$, μ will lie in the submodule

$$M_3 = \{x_1\sqrt{3} + x_2\sqrt{5}\}$$

and for such a μ

$$N_{K/Q}(x_1\sqrt{3} + x_2\sqrt{5}) = N_{K/Q}[(1/\sqrt{3})(3x_1 + x_2\sqrt{15})]$$

$$= \frac{1}{3^2}[N_{L_3/Q}(3x_1 + x_2\sqrt{15})]^2$$

where $L_3 = Q(\sqrt{15})$. Thus, equation (16) gives

$$N_{L_3/Q}(3x_1 + x_2\sqrt{15}) = \pm 3^2 \cdot 5 .$$

Since both 3 and 5 extend to unique nonprincipal ideals in this field, there are no solutions to this last equation.

Therefore, every solution to (16) with $x_1x_2x_3 = 0$ is given by

17) $$\pm\sqrt{3}\,(2 + \sqrt{3})^t , \qquad \pm\sqrt{5}\,(2 + \sqrt{5})^t$$

for all integer values of t. That only a finite number of other solutions exist will follow from Schmidt's Theorem. A similar example was given by Schmidt.

Let M be a module in K and L any subfield. Define the submodule

$$M^L$$

to be the set of μ in M such that for every λ in L there is a non-zero rational integer z such that $z\lambda\mu \in M$. If $\overline{M}$ denotes the vector space over Q generated by M, then M^L is the set of μ in M such that

$$\mu L \subseteq \overline{M} .$$

The last form of the definition shows that $\overline{M^L}$ is a vector space over L, since for μ in M^L and λ in L

$$(\mu\lambda)L = \mu L \subseteq \overline{M}$$

and thus $\mu\lambda$ is in $\overline{M^L}$. Because of this, $[L:Q]$ divides rank M^L.

It is easy to calculate M^L in terms of the bases for M and L. Extend the basis $(\beta_1, \ldots, \beta_k)$ of M to a basis of K, say $(\beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_n)$. Let $(\lambda_1, \ldots, \lambda_l)$ be any basis for L, then μ in M is in M^L if and only if

$$\mu\lambda_i \in \overline{M}$$

for each $1 \leq i \leq l$. This will be so if the representation of $\mu\lambda_i$ with respect to the basis $(\beta_1, \ldots, \beta_n)$ terminates with n-k zeroes. Thus, μ is in M^L if and only if the k coefficients of μ with respect to the basis $(\beta_1, \ldots, \beta_k)$ satisfy the set of $l(n-k)$ linear conditions required above. A basis for M^L can be found using these conditions.

For example, $M^Q = M$ for every module is easily seen and if the module M is full in K, then $\overline{M} = K$, so $M^K = M$. However, for any nonfull module M, $\overline{M}$ is a proper subspace of K and must have dimension over Q smaller than n. If μ were a non-zero element of M^K, then

$$\dim \mu K = n \leq \dim M^K < \dim K = n .$$

So $M^K = \{0\}$ if M is not full in K.

Let AB be the composite of the two fields A and B.

Lemma 4: For any two subfields A, B of K

$$(M^A)^B = M^{AB} .$$

Proof: Assume first that $\mu \in (M^A)^B$, then μ is an element of M^A such that

$$\mu B \subseteq \overline{M^A} .$$

Every element of AB is of the form $\alpha_1\beta_1 + \cdots + \alpha_r\beta_r$ with $\alpha_i \in$ A and $\beta_i \in$ B, so μ is in M^{AB} if and only if

$$\mu\alpha\beta \in \overline{M}$$

for every $\alpha \in$ A and $\beta \in$ B. But $\overline{M^A}$ is a vector space over A, so

$$\mu\alpha\beta \in \alpha\overline{M^A} \subseteq \overline{M^A} \subseteq \overline{M} .$$

Therefore, $(M^A)^B \subseteq M^{AB}$.

Conversely, suppose $\mu \in M^{AB}$, then

$$\mu A \subseteq \mu AB \subseteq \overline{M} .$$

Therefore, $\mu \in M^A$ and it is only necessary to show

$$\mu B \subseteq \overline{M^A} .$$

But B is a subfield of AB, so

$$\mu B \subseteq \mu AB \subseteq \overline{M^{AB}} \subseteq \overline{M^A}$$

since being in M^{AB} is more restrictive than being in M^{A}.

Thus $M^{AB} \subseteq (M^{A})^{B}$ and the lemma follows. §

With the module $M = \{x_1\sqrt{3} + x_2\sqrt{5} + x_3\sqrt{15}\}$ from the previous example (16) and the fields L_1, L_2, L_3, the submodules corresponding to these fields are M_1, M_2, and M_3 respectively. These are the same submodules which appeared in the example.

To calculate M^{L_3}, for example, extend the basis for M to the basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ of K and use the basis $\{1, \sqrt{15}\}$ for L_3. Since $1 \cdot \mu$ is in $\overline{M}$ for every μ in M, the condition for μ to be in M^{L_3} reduces to the one relation

$$\mu\sqrt{15} \in \overline{M} .$$

If μ is written as $x_1\sqrt{3} + x_2\sqrt{5} + x_3\sqrt{15}$, then $\mu\sqrt{15} \in \overline{M}$ requires rationals a, b, c such that

$$\mu\sqrt{15} = 15x_3 + 5x_2\sqrt{3} + 3x_1\sqrt{5} = a\sqrt{3} + b\sqrt{5} + c\sqrt{15} .$$

Therefore, x_3 must equal zero and $M^{L_3} = M_3$ of the example.

Let $\mathfrak{O}_M^L$ denote the ring of coefficients of M^L in L, i.e. the set of all λ in L such that $\lambda\mu \in M^L$ for all μ in M^L.

<u>Lemma 5</u>: If $M^L \neq \{0\}$, then $\mathfrak{O}_M^L$ is an order of L.

<u>Proof</u>: It is clear that $\mathfrak{O}_M^L$ is a ring with 1, so it only remains to prove that it is a full, finitely generated module in L.

Let μ be any non-zero element of M^L, then $\mu\mathfrak{O}_M^L \subseteq M^L$ and

$$\mathfrak{O}_M^L \subseteq \mu^{-1} M^L .$$

Since M^L is a finitely generated module so is $\mu^{-1} M^L$ and thus also the submodule $\mathfrak{O}_M^L$.

To show that $\mathfrak{O}_M^L$ is full in K, it suffices to show that there exists an integer $z \neq 0$ such that $z\mathfrak{O}_L \subseteq \mathfrak{O}_M^L$, where $\mathfrak{O}_L$ is the maximal order of L. For each element λ_i of a basis for $\mathfrak{O}_L$ and each μ_j of a basis for M^L there is a non-zero integer $z_{i,j}$ such that

$$z_{i,j} \lambda_i \mu_j \in M^L .$$

The integer $z = \Pi z_{i,j}$ satisfies the above conditions, so $\mathfrak{O}_M^L$ is full in L and is thus an order of L. §

The procedure used for full modules can be followed in general to some extent by using the modules M^L for each subfield. For each of the finite number of subfields L of K construct the module M^L. If M^L is not just zero, $\mathfrak{O}_M^L$ is an order of L and has a group of units as given by Dirichlet's Unit Theorem. Denote by $U_M^{L/Q}$ the subgroup of the group of all units in $\mathfrak{O}_M^L$ which consists of those units with norm from K to Q equal to +1. This group actually depends on K also, but for simplicity this dependency is assumed. As when M is a full module, the index of $U_M^{L/Q}$ in the full group of units of L is finite. The set $\mu U_M^{L/Q}$ is the set of associates of μ over $\mathfrak{O}_M^L$ which have the same norm and is called an <u>(M, L/Q)-family</u>. A family is <u>maximal</u> if it is not properly contained in any (M, L′/Q)-family for any L′ contained in K.

Every element μ of M is contained in a maximal family, since for each field L either $\mu \notin M^L$ or else it is contained in the (M, L)-family $\mu U_M^{L/Q}$ and no others. One of the finite number of families containing μ must be maximal. Of course, every μ is in $M^Q = M$.

Theorem 3 (Schmidt): There exist a finite number of maximal families which give the solutions to (14).

Applying this theorem to the equation (16), since $M^K = \{0\}$ for the nonfull module M, it is necessary to look at M^L for each subfield. It has already been calculated that $M^{L_1} = M_1$, $M^{L_2} = M_2$, $M^{L_3} = M_3$, with M_1, M_2, and M_3 the submodules given in the example. Also, it is always true that $M^Q = M$. Equation (17) gives the families of solutions for the fields M^{L_1}, M^{L_2}, and M^{L_3} and by Schmidt's Theorem there are only a finite number of maximal families altogether. It follows that there are a finite number of other families of solutions which, if any exist, will be of the form

$$\mu U_M^{Q/Q} \ .$$

However, $U_M^{Q/Q}$ is a subgroup of the group $\{1, -1\}$, so all but a finite number of solutions to (16) are given by (17).

In a general norm form equation it is always possible to calculate M^L, $\mathfrak{D}_M^L$, and $U_M^{L/Q}$ for each subfield L in a finite number of steps, but it is not known how to find all representatives for the maximal families. Still, for some modules it is possible to prove that only a finite number of solutions exist. The module M is called non-degenerate if $M^L = \{0\}$ for every subfield L except possibly for quadratic imaginary fields or Q. By Dirichlet's Unit Theorem, these are the only extensions of Q for which the group $U_M^{L/Q}$ will be finite. It follows from Schmidt's Theorem that equation (14) has only a finite number of solutions when M is non-degenerate.

It is easy to show that Schmidt's Theorem generalizes Thue's. It is necessary to prove that the equation

$$N_{K/Q}(x_1 + x_2\theta) = c \neq 0$$

has only a finite number of integer solutions, where $K = Q(\theta)$ and $[K:Q] \geq 3$. This will follow by showing that $M = \{x + y\theta\}$ is non-degenerate. Clearly $M^K = \{0\}$, so let L be any field strictly between Q and K. If $M^L \neq \{0\}$, then

$$2 \leq [L:Q] \leq \text{rank } M^L \leq \text{rank } M = 2 \text{ .}$$

The inequality between $[L:Q]$ and rank M^L is because $\overline{M^L}$ is a vector space over L. It follows that $M^L = M$. Let $L = Q(\lambda)$, then $\lambda\theta \in \overline{M}$ and

$$\lambda\theta = x + y\theta$$

for some rational numbers x, y. Since λ is not rational, this implies $\theta \in L$, contradicting the choice of L. So $M^L = \{0\}$ and M is non-degenerate.

Schmidt's Theorem has a nice extension to the more general problem

18) $$N_{K/F}(\mu) = \gamma \neq 0 , \qquad \mu \in M ,$$

when $M^F = M$. For each field L satisfying $F \subseteq L \subseteq K$ define M^L and $\mathfrak{D}_M^L$ as before, but now let

$$U_M^{L/F}$$

be the group of units in $\mathfrak{D}_M^L$ whose norm form K to F is +1. For each μ in M^L the set $\mu U_M^{L/F}$ is an <u>(M, L/F)-family</u> and a maximal family is defined as before.

<u>Lemma 6</u>: There exist a finite number of maximal families which give the solutions to (18).

<u>Proof</u>: Taking the norm of both sides of (18) from F to Q gives

$$N_{K/Q}(\mu) = N_{F/Q}(\gamma) = c \neq 0 , \qquad \mu \in M .$$

So μ lies in one of a finite number of maximal families of solutions to this equation which are of the form

$$\mu' U_M^{L/Q} ,$$

for fields L below K. The fields which appear in these families need not be above F, but since $M^F = M$,

$$M^{FL} = (M^F)^L = M^L$$

and the field FL is a field above F. It follows that the solutions to (18) are contained in a finite number of families of the form

$$\mu' U_M^{L/Q}$$

with L a field above F. It is clear that if $\mu' U_M^{L/Q}$ has any solutions, then μ' can be taken to be one. The only units of $U_M^{L/Q}$ which will give other solutions are precisely those with norm from K to F equal to +1, i.e. those in the group $U_M^{L/Q}$. §

The following lemma, a form of which was proved a different way by Győry [7], will be used in the proof of Theorem 2.

Lemma 7: Let γ_1, γ_2, and γ be any integers in K with $\gamma \neq 0$. There exist only a finite number of units u_1, u_2 in K satisfying

$$u_1\gamma_1 + u_2\gamma_2 = \gamma .$$

Proof: Every unit of K can be written uniquely as

$$\xi\eta_1^{a_1} \cdots \eta_r^{a_r} ,$$

ξ a root of one in K and $\eta_1, \ldots, \eta_r$ a fixed fundamental system of units. Let p be any prime. Those units for which $0 \leq a_i \leq p-1$ form a finite set and will be called p-power free (with respect to $\eta_1, \ldots, \eta_r$). Every unit in K is the product of a p-power free unit and a unit which a p^{th} power. Choose $p > 3$ so that the field $Q(\xi_p)$ is disjoint from K, where ξ_p is a primitive p^{th} root of 1. Then the representation is unique for each unit of K.

If the equation has an infinite number of solutions in units of K, there must be an infinite subset of solutions u_1, u_2 with p-power free parts equal to u_3, u_4 respectively, for some pair (u_3, u_4). This is clear since there are only a finite number of such pairs. Therefore, the lemma will follow from showing that for every γ_1, γ_2

and $\gamma \neq 0$ in K, there exist only a finite number of solutions x, y in units of K to the equation

$$\gamma_1 x^p + \gamma_2 y^p = \gamma .$$

This will now be proved.

If either γ_1 or γ_2 is zero, the result is obvious. If $\gamma_1\gamma_2 \neq 0$, then

$$\gamma_1^p x^p + \gamma_1^{p-1}\gamma_2 y^p = \gamma_1^{p-1}\gamma$$

and without loss of generality the equation can be assumed to be

$$x^p + \gamma_2 y^p = \gamma$$

for some integers γ_2, γ in K and $\gamma_2 \gamma \neq 0$. Also, since p^{th} powers in γ_2 can be absorbed in y, either γ_2 is not a p^{th} power or can be taken to be 1.

If γ_2 is not a p^{th} power, then $z^p + \gamma_2$ is irreducible over K, see for example [11].

If $\gamma_2 = 1$, then $(z^p + 1)/(z + 1)$ is irreducible over K. This will follow since K and $Q(\xi_p)$ are disjoint. Write ξ for ξ_p, then

$$z^p + 1 = \prod_{i=0}^{p-1} (z + \xi^i)$$

Let S be any nonempty subset of $\{0, 1, 2, \ldots, p-1\}$ such that

$$g(z) = \prod_{i \in S} (z + \xi^i)$$

is in K[z]. The coefficients of g are in $K \cap Q(\xi_p) = Q$, so the factorization is exactly the same as over Q.

So suppose first that γ_2 is not a p^{th} power. Fix a p^{th} root of γ_2 and call it β. If $E = K(\beta)$, then it is sufficient to prove that there exist only a finite number of solutions x, y in integers of K to the equation

$$N_{E/K}(x + \beta y) = \gamma .$$

Since $[E:K] = p > 3$, $M^E = \{0\}$ for $M = \{x + y\beta\}$ and there are no subfields between E and K. Also $M^K = M$ since x, y are integers of K. Thus, there exist a finite number of maximal families of solutions each of which is of the form

$$\mu\, U_M^{K/K} .$$

But $U_M^{K/K}$ is a finite group, in fact just $\{1\}$ in this case, so this gives the required result.

Now suppose $\gamma_2 = 1$, then $E = K(\xi_p)$ and the equation is

19) $$(x + y)N_{E/K}(x + \xi_p y) = \gamma .$$

Take norms from K to Q to get

$$N_{K/Q}(x + y)N_{E/Q}(x + \xi_p y) = N_{K/Q}(\gamma) = c \neq 0 ,$$

and each of the norms is an integer, so

$$N_{E/Q}(x + \xi_p y) = c'$$

where c' is one of a finite set of integer factors of c. The rank of

$M = \{x + \xi_p y\}$ is $2[K:Q]$ and $M^K = M$. Since p was chosen greater than 3, $[E:K] = p-1 > 2$, so $M^E = \{0\}$. The same argument as the one used to establish Thue's Theorem from Schmidt's shows that $M^L = \{0\}$ for every field L strictly above K.

Every solution is thus contained in a finite number of families of the form

$$\mu\, U_M^{K/Q} .$$

The integers x, y of K are determined by these numbers since $1, \xi_p$ are independent over K. If μ leads to a solution to (19) and $\mu = x_0 + \xi_p y_0$, then for $u \in U_M^{K/Q}$, $u \in K$ so

$$u\,\mu \;=\; u\,x_0 \;+\; \xi_p u\, y_0$$

and

$$(u\,x_0 + u\,y_0)\, N_{E/K}(u\,x_0 + \xi_p u\, y_0) \;=\; u^p\gamma \;.$$

Thus, the only solutions to (19) in the family are those for which $u^p = 1$ and this is only $u = 1$.

So in this case there again are only a finite number of solutions. §

CHAPTER 3

CERTAIN FIELDS WITH THE BOUNDED INDEX PROPERTY

Because of lemma 1 it is reasonable to say K has the bounded index property if any order of K has it. Let $K = Q(\theta)$, $\mathfrak{O} = Z[\theta]$ and $\theta = \theta_1, \ldots, \theta_n$, the conjugates of θ, then K has the bounded index property if and only if there only exist a finite number of integer solutions $(x_1, \ldots, x_{n-1})$ to the system of norm form equations

$$20) \quad N_{L_{i,j}/Q}\,[\ell(x_1, \ldots, x_{n-1}\ ;\ \theta_i, \theta_j)] = c_{i,j}\ , \qquad (1 \le i < j \le n)$$

for every set of non-zero constants $c_{i,j}$. The field $L_{i,j}$ is the field generated by the coefficients of $\ell(x_1, \ldots, x_{n-1}\ ;\ \theta_i, \theta_j)$.

For each pair θ_i, θ_j define the module $M_{i,j}$ to be

$$\{\ell(x_1, \ldots, x_{n-1}\ ;\ \theta_i, \theta_j) \mid x_1, \ldots, x_{n-1} \text{ integers}\}\ ,$$

so each norm form in (20) is the norm of an element from some $M_{i,j}$. However, equation (20) requires a dependency between the elements of the various modules with these norms in order for the solution $(x_1, \ldots, x_{n-1})$ to be integral.

The values of $x_1, x_2, \ldots, x_{n-1}$ are determined uniquely by the set of individual solutions $\mu_{i,j}$ to the equations

$$N_{L_{i,j}/Q}\,(\mu_{i,j}) = c_{i,j}\ , \qquad \mu_{i,j} \in M_{i,j}\ .$$

This is because $\mu_{i,j}$ is equal to

$$(\lambda_i - \lambda_j)/(\theta_i - \theta_j)$$

for some $\lambda \in \mathfrak{O}$ and if λ, ω are two numbers in $\mathfrak{O}$ such that

$$\lambda_i - \lambda_j = \omega_i - \omega_j$$

for each $i < j$, then $\lambda - \omega$ is fixed by G and λ, ω are equivalent. Thus, $x_1, x_2, \ldots, x_{n-1}$ are uniquely determined.

It will be useful to know the rank of $M_{i,j}$. Let $F_{i,j}$ be the field fixed by the group generated by all automorphisms in G which take θ_i to θ_j.

<u>Lemma 8</u>: The rank of $M_{i,j}$ is $n-[F_{i,j}:Q]$ and $M_{i,j}^{F_{i,j}} = M_{i,j}$.

<u>Proof</u>: The rank of $M_{i,j}$ is equal to the rank of $(\theta_i - \theta_j)M_{i,j}$ and equals the dimension of the vector space they generate over Q. Consider the linear transformation T from Q^{n-1} to $\overline{(\theta_i - \theta_j)M_{i,j}}$ given by

$$T(x_1, \ldots, x_{n-1}) = x_1(\theta_i - \theta_j) + \cdots x_{n-1}(\theta_i^{n-1} - \theta_j^{n-1}) .$$

If $(x_1, \ldots, x_{n-1})$ is in the null space of T, then

$$x_1\theta_i + \cdots x_{n-1}\theta_i^{n-1} = x_1\theta_j + \cdots x_{n-1}\theta_j^{n-1}$$

and this element is in $F_{i,j}$ since it is fixed by all automorphisms taking θ_i to θ_j.

Since every element of $F_{i,j}$ can be written uniquely in terms of the basis $1, \theta_i, \ldots, \theta_i^{n-1}$ of $Q(\theta_i)$, only those elements of $F_{i,j}$ whose representations have zero for the first component with respect to this basis result from an element of the null space.

Therefore, the dimension of the null space is $[F_{i,j}:Q] - 1$ and this gives the rank of $M_{i,j}$ as $n-[F_{i,j}:Q]$.

The last statement is easy since an element $\mu \in M_{i,j}$ is in $M_{i,j}^{F_{i,j}}$ if

$$\mu F_{i,j} \subseteq \overline{M_{i,j}} \ .$$

Therefore, let μ be in $M_{i,j}$ and α an element of $F_{i,j}$. It follows that there exists $\lambda \in \mathfrak{O}$ such that

$$\mu = (\lambda_i - \lambda_j)/(\theta_i - \theta_j) \ ,$$

and since α is in $F_{i,j}$ it is fixed by every automorphism of G taking θ_i to θ_j. So there is a unique ω in K such that $\omega_i = \lambda_i\alpha$ and $\omega_j = \lambda_j\alpha$. Thus

$$\mu\alpha = (\lambda_i - \lambda_j)\alpha/(\theta_i - \theta_j) = (\omega_i - \omega_j)/(\theta_i - \theta_j) \in \overline{M_{i,j}}$$

and μ is in $M_{i,j}^{F_{i,j}}$. §

Although the proof of Theorem 2 covers every finite extension of Q, it is interesting to apply Schmidt's Theorem in a different manner for fourth degree fields and certain other special fields.

The simplest fields are covered by the following theorem.

Theorem 5: The field K with $[K:Q] = n$ has the bounded index property if n is a prime and $G(K^*/Q) = C_n$, or any n if $G(K^*/Q)$ is either A_n or S_n.

Proof: If n is a prime and $G(K^*/Q) = C_n$, then K is normal and contains only Q as a proper subfield. Each of the modules $M_{i,j}$ is nonfull since their ranks are n-1 or less, so they are all non-degenerate. It follows that (20) can have only a finite number of integer solutions.

Suppose that $G(K^*/Q)$ is A_n or S_n. For $n \leq 3$ Theorem 1 is equivalent to this theorem, so assume $n \geq 4$. The system (20) reduces to one norm form equation since both A_n and S_n are 2-ply transitive for $n \geq 3$. The result will follow provided that the module $M_{1,2}$ is non-degenerate. It will be shown that for $n > 4$ the field $L_{1,2}$ contains no proper subfields except Q, so $M_{1,2}$ is non-degenerate for these fields. When $n = 4$ a simple argument will be given.

The fact that $L_{1,2}$ contains no proper subfields except Q when $n > 4$ follows from the following lemma.

Lemma 9: The group $G_{1,2}$ is maximal in $G(K^*/Q)$ when $G(K^*/Q)$ is either A_n or S_n provided n is larger than four.

Proof: Let $G = G(K^*/Q)$ and π be any element of G which is not in $G_{1,2}$. Let H be the group generated by $G_{1,2}$ and π, so it is necessary to prove $H = G$. These are permutation groups on the set $\{1, 2, \ldots, n\}$ realized by their actions on the conjugates $\theta_1, \theta_2, \ldots, \theta_n$.

Suppose σ is an arbitrary element of G and that there is a σ' in H such that

$$\sigma(1) = \sigma'(1)$$
$$\sigma(2) = \sigma'(2) ,$$

then $\sigma^{-1}\sigma'$ fixes both 1 and 2 and is thus in $G_{1,2}$. Since σ' is in H, this shows that σ must also be in H. Therefore, to prove the lemma it is only necessary to show that for every pair of distinct a, b in $\{1, 2, \ldots, n\}$ there is a σ in H with

$$\sigma(1) = a , \qquad \sigma(2) = b .$$

Let r and s be the numbers which satisfy

$$\pi(1) = r , \qquad \pi(2) = s ,$$

then since π is not in $G_{1,2}$

$$\{r, s\} \neq \{1, 2\} .$$

A number of cases arise depending on which of the numbers a, b, r, s are in the set $\{1, 2\}$ and which ones are equal to each other. In each case, since $n \geq 5$, an element σ as required above can be constructed using only π and automorphisms from $G_{1,2}$.

A case where this lemma fails for $n = 4$ will be worked out in detail. Let $r, s \notin \{1, 2\}$ and $a = 1$, $b > 2$. Suppose a permutation σ' is in H with

$$\sigma'(1) \in \{1, 2\} , \qquad \sigma'(2) \notin \{1, 2\} .$$

If $\sigma'(1) \neq 1$, then by following σ' with the even permutation $(1, 2)(r, s)$ will give another permutation in H which now fixes 1. So suppose $\sigma'(1)$ is 1 and $\sigma'(2)$ is not b, but is still larger than 2, then σ is easily constructed from σ'. Since there are at least five elements in $\{1, 2, \ldots, n\}$, there is a $c > 2$ with $m = \sigma'(2)$, b, and c distinct. So

$$\tau = (m, b, c)$$

is even and fixes both 1 and 2, and $\sigma = \tau\sigma'$ is the desired automorphism. An automorphism σ' can be easily constructed.

Since $\pi \notin G_{1,2}$ there is a number $c > 0$ with r, s, c distinct and such that either one or two of $\pi(r)$, $\pi(s)$ or $\pi(c)$ is in $\{1, 2\}$. Using τ some power of the even permutation (r, s, c) will give

$$\sigma' = \pi \tau \pi .$$

It follows that $H = G$ and $G_{1,2}$ is maximal in G. §

Since the order of the group $G_{1,2}$ is $(n-2)!$ if $G(K^{*}/Q)$ is A_n and $2(n-2)!$ for S_n, the field $L_{1,2}$ is of degree $\frac{n(n-1)}{2}$ over Q. It follows that $M_{1,2}$ is not full in $L_{1,2}$ for $n \geq 3$ and thus $M_{1,2}$ is non-degenerate, except possibly for $n = 4$.

If $n = 4$, then $L_{1,2}$ is a sixth degree extension of Q and contains only one cubic subfield L as a proper subfield. As has been shown before, $M_{1,2}$ of rank 3 implies

$$M^{L}_{1,2} = M_{1,2} \subseteq L ,$$

which is a contradiction since $M_{1,2}$ contains a generator for $L_{1,2}$. So again $M_{1,2}$ is non-degenerate. §

The following lemma is interesting by itself and is also needed to prove Theorem 6.

Lemma 10: If $L_1 = Q(\alpha_1)$ and $L_2 = Q(\alpha_2)$ are two distinct quadratic fields, then the system of norm form equations

$$21) \quad N_{L_1/Q}(x_1 + x_2\alpha_1) = c_1 , \quad N_{L_2/Q}(x_3 + x_4\alpha_2) = c_2 , \quad c_1 c_2 \neq 0$$

has only a finite number of integer solutions (x_1, x_2, x_3, x_4) satisfying the equation

$$ax_1 + bx_2 = cx_3 + dx_4$$

when neither side of the equation is identically zero.

Proof: Let $\overline{\alpha}_1, \overline{\alpha}_2$ denote the conjugates of α_1, α_2 in the appropriate fields. Since either a or b is not zero, $N_{L_1/Q}(b - a\alpha_1) \neq 0$. Similarly, $N(d - c\alpha_2) \neq 0$. Without loss of generality, assume $bd \neq 0$, then if

$$\begin{aligned} y_1 &= N_{L_1/Q}(b - a\alpha_1)x_1 \\ y_2 &= ax_1 + bx_2 \\ y_3 &= N_{L_2/Q}(d - c\alpha_2)x_3 \\ y_4 &= y_2 \end{aligned}$$

equation (21) becomes

$$N_{L_1/Q}[y_1 + y_2\alpha_1(b - a\bar{\alpha}_1)] = b^2N_{L_1/Q}(b - a\bar{\alpha}_1)c_1 \neq 0$$

$$N_{L_2/Q}[y_3 + y_2\alpha_2(d - c\bar{\alpha}_2)] = d^2N_{L_2/Q}(d - c\bar{\alpha}_1)c_2 \neq 0 ,$$

since for instance

$$\begin{aligned} y_1 + y_2\alpha(b - a\bar{\alpha}_1) &= (b - a\alpha_1)(b - a\bar{\alpha}_1)x_1 + \alpha_1(b - a\bar{\alpha}_1)(ax_1 + bx_2) \\ &= b(b - a\bar{\alpha}_1)(x_1 + x_2\alpha_1) . \end{aligned}$$

Therefore, the lemma will follow from proving the case when $x_2 = x_4$ in (21).

So assume $a = c = 0$ and $b = d = 1$ and without loss of generality that $x_2 > 0$ for all solutions. Since $(x_1 + x_2\alpha_1)$ times $(x_1 + x_2\bar{\alpha}_1)$ is a constant, any infinite set of solutions must contain a subset of solutions for which $x_1 + x_2\alpha_1$, say, goes to zero. Otherwise there would exist an infinite number of quadratic algebraic numbers with bounded height, which is impossible. Assume that there are an infinite number of integer solutions to (21) with $x_1 + x_2\alpha_1$ and $x_3 + x_2\alpha_2$ approaching zero, then since x_1/x_2 approaches $-\alpha_1$, $x_1/x_2 + \bar{\alpha}_1$ is bounded away from zero and similarly for α_2. Therefore,

$$|x_1/x_2 + \alpha_1| = \frac{|c_1|\, x_2^{-2}}{|x_1/x_2 + \bar{\alpha}_1|} < \frac{1}{x_2^{2+\epsilon}} , \qquad \epsilon > 0$$

and the corresponding inequality for α_2 with the same ϵ will have an infinite number of simultaneous integer solutions.

However, by another theorem of Schmidt's [14], it is impossible to simultaneously approximate two quadratic irrationals α_1, α_2 such that $1, \alpha_1, \alpha_2$ are independent over Q, by an infinite number of fractions x_1/x_2 and x_3/x_2 to an exponent larger than 3/2. So (21) has only a finite number of solutions.

Another proof may be given which uses only Thue's Theorem. The solutions to (21) are related to rational points on the conic

$$c_2 N_{L_1/Q}[(x_1 + x_2\alpha_1)/x_3] - c_1 N_{L_2/Q}[(x_3 + x_2\alpha_2)/x_3] = 0$$

All rational points on such a curve are given by a two parameter formula in the parameters p and q. The solutions to (21) come from these parameters if and only if the norm from the fourth degree field $Q(\alpha_1, \alpha_2)$ of the element $p + q\alpha$ is a given constant, where α is a fixed number such that $Q(\alpha) = Q(\alpha_1, \alpha_2)$. Thue's Theorem proves only a finite number of such p and q exist. §

Theorem 6: If $[K:Q] = 4$, then K has the bounded index property.

Proof: If $G(K^*/Q)$ is A_4 or S_4, Theorem 5 gives the result. Each of the remaining Galois groups is treated separately.

Case 1: $G(K^*/Q) = C_2 \times C_2$. Let $G(K^*/Q) = \{1, \sigma, \tau, \sigma\tau\}$ and $\theta = \theta_1$, $\theta_2 = \sigma\theta$, $\theta_3 = \tau\theta$, $\theta_4 = \sigma\tau\theta$, then with

$$S = \{\ell(x_1, x_2, x_3 ; \theta_1, \theta_2), \ell(x_1, x_2, x_3 ; \theta_1, \theta_3), \ell(x_1, x_2, x_3 ; \theta_1, \theta_4)\}$$

lemma 3 gives

$$z(x_1, x_2, x_3) = \prod_{\ell \in S} N_{L_{i,j}/Q}[\ell(x_1, x_2, x_3 ; \theta_i, \theta_j)] .$$

Each of the fields $L_{i,j}$ is quadratic, each module has rank 2, and the hypotheses of lemma 10 hold, so only a finite number of solutions (x_1, x_2, x_3) exist.

Case 2: $G(K^*/Q) = C_4$. Let $G(K^*/Q) = \langle\sigma\rangle$ and L the field fixed by $\langle\sigma^2\rangle$. Take θ to be one of the integers of K such that $K = Q(\theta)$ and $L = Q(\theta^2)$. Let $\theta = \theta_1$, $\theta_2 = \sigma\theta$, $\theta_3 = \sigma^2\theta$, $\theta_4 = \sigma^3\theta$, then

$$z(x_1, x_2, x_3) = N_{L_{1,2}/Q}[\ell(x_1, x_2, x_3 ; \theta_1, \theta_2)] N_{L_{1,3}/Q}[\ell(x_1, x_2, x_3 ; \theta_1, \theta_3)]$$

with $L_{1,2} = K$, $L_{1,3} = L$. Since $F_{1,2}$ is Q and $F_{1,3}$ is L, the modules $M_{1,2}$ and $M_{1,3}$ have ranks 3 and 2 respectively.

Since $M_{1,2}$ has rank 3, x_1, x_2, x_3 are uniquely determined by the element in this module, so if an infinite number of solutions exist they must belong to the module $M^L_{1,2}$ as L is the only proper subfield of K.

Since the element $\theta_1^2 + \theta_1\theta_2 + \theta_2^2$ is fixed by σ^2, but not by σ it must be a generator for L over Q. Thus, 1 and $\theta_1^2 + \theta_1\theta_2 + \theta_2^2$ form a basis for L and $L \subseteq \overline{M}_{1,2}$. It follows that

$$(\theta_1^2 + \theta_1\theta_2 + \theta_2^2) L = L \subseteq \overline{M}_{1,2}$$

so 1 and $\theta_1^2 + \theta_1\theta_2 + \theta_2^2$ are in $M^L_{1,2}$. Because $[L:Q]$ divides rank $M^L_{1,2}$, these must both be 2 and

$$M^L_{1,2} = \{x_1 + x_3(\theta_1^2 + \theta_1\theta_2 + \theta_2^2)\}$$

The system of norm form equations (20) has been reduced to

$$22)\qquad \begin{aligned} N_{L/Q}[x_1 + x_3(\theta_1^2 + \theta_1\theta_2 + \theta_2^2)] &= c_1 \\ N_{L/Q}[x_1 + x_3\theta_1^2] &= c_2 , \end{aligned}$$

since $\theta_3 = -\theta_1$ gives

$$M_{1,3} = \{x_1 + x_2(\theta_1 - \theta_1) + x_3(\theta_1^2 - \theta_1^2 + \theta_1^2)\} .$$

An infinite number of solutions can exist to the equation (22) only if $\theta_1^2 + \theta_1\theta_2 + \theta_2^2$ and θ_1^2 are conjugates, which they are not. Again K has the bounded index property.

Case 3: Dihedral Galois Group. Let $G(K^*/Q) = \langle \sigma, \tau \rangle$ where $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$. The field K can be taken to be the fixed field of τ. Let $\theta = \theta_1$, $\theta_2 = \sigma\theta$, $\theta_3 = \sigma^2\theta$, $\theta_4 = \sigma^3\theta$. The set S can be taken to be

$$\{\ell(x_1, x_2, x_3 ; \theta_1, \theta_2), \ \ell(x_1, x_2, x_3 ; \theta_1, \theta_3)\} ,$$

and $F_{1,2} = Q$, $F_{1,3}$ the quadratic subfield of K, so the rank of $M_{1,2}$ is 3 and the rank of $M_{1,3}$ is 2. Again the only possibility for an infinite number of solutions is in $M_{1,2}^L$, but $L_{1,2}$ is a fourth degree field which is disjoint from K. Thus $M_{1,2}^L$ will be full in a quadratic subfield which is distinct from $F_{1,3}$ and only a finite number of solutions can exist again by lemma 10.

These are the only Galois groups for $n = 4$ and thus the theorem is proved. §

CHAPTER 4

THE PROOF OF THEOREM 2

It turns out that lemma 7 is exactly the required tool for proving that the system of equations (20) has only a finite number of solutions. Györy [7] proved a stronger result than lemma 7 by using the results of Baker [1] and Baker and Coates [2] on the existence of a fundamental system of units of a special type. He used his result to prove that there exist only a finite number of inequivalent algebraic integers of a given bounded discriminant [6], which is equivalent to Theorem 2. The use of Baker's results gives explicit bounds on the heights of the representatives of the equivalency classes and thus a theoretical method of finding them all. This is almost always impossible in practice, but an example of a type of field for which it may be done will be given.

Schmidt's Theorem has already been used in the proof of lemma 7. The rest of the proof uses lemma 7 to get the result, following Györy's original proof.

Proof of Theorem 2: By considering the module $(\theta_i - \theta_j)M_{i,j}$ which is similar to $M_{i,j}$, equation (20) becomes

$$23) \qquad N_{K/Q}(\lambda_i - \lambda_j) = c_{i,j}\,, \qquad (1 \le i < j \le n)$$

for some $\lambda \in \mathfrak{O}$ and all non-zero constants $c_{i,j}$ has only a finite number of solutions. It has been shown that the set of values $\lambda_i - \lambda_j$ determine λ up to equivalence.

The set of solutions to any one of the equations in (23) is described by Schmidt's Theorem, but the weaker result that every number with a given norm is associated with one of a finite set of numbers will be sufficient here. Thus, there exists a finite set of numbers $\mu_1, \ldots, \mu_k$ such that

$$\lambda_i - \lambda_j \in \mu U_K$$

for every pair of distinct i,j and some μ in the set $\{\mu_1, \ldots, \mu_k\}$. The group of units U_K is the group of units with norm +1 in the maximal order of K.

Because of the finiteness of the set $\{\mu_1, \ldots, \mu_k\}$, the only way there can exist an infinite number of λ satisfying (23) is for some infinite set of such λ to exist satisfying

24) $$\lambda_i - \lambda_j \in \mu_{i,j} U_K$$

for each i, j and a fixed number $\mu_{i,j}$ in the set $\{\mu_1, \ldots, \mu_k\}$ independent of λ. It suffices to prove that only a finite number of λ exist satisfying (24).

Suppose $\lambda_1 - \lambda_2 = \epsilon_1\mu_{1,2}$, $\lambda_2 - \lambda_3 = \epsilon_2\mu_{2,3}$ and $\lambda_3 - \lambda_1 = \epsilon\mu_{3,1}$. Then since

$$(\lambda_1 - \lambda_2) + (\lambda_2 - \lambda_3) + (\lambda_3 - \lambda_1) = 0$$

it follows that

$$\epsilon_1\epsilon^{-1}\mu_{1,2} + \epsilon_2\epsilon^{-1}\mu_{2,3} + \mu_{3,1} = 0 .$$

By lemma 7, the units $\epsilon_1\epsilon^{-1}$, $\epsilon_2\epsilon^{-1}$ can have only a finite number of values and so for every λ satisfying (24)

$$\epsilon^{-1}(\lambda_1 - \lambda_2, \ \lambda_2 - \lambda_3, \ \lambda_3 - \lambda_1)$$

is one of a finite number of possible triples for some unit ϵ. This will be extended to show that for some unit ϵ

25) $$\epsilon^{-1}(\lambda_i - \lambda_j)$$

is one of a finite set of numbers for each choice of $i < j$.

Repeating the same technique with $\lambda_1, \lambda_2, \lambda_i$ for each $i \neq 1, 2$ gives for some unit η

$$\eta^{-1}(\lambda_1 - \lambda_2, \ \lambda_2 - \lambda_i, \ \lambda_i - \lambda_1) = (\alpha'_{1,2}, \alpha'_{2,i}, \alpha'_{i,1})$$

and with $i = 3$ as before

$$\epsilon^{-1}(\lambda_1 - \lambda_2, \ \lambda_2 - \lambda_3, \ \lambda_3 - \lambda_1) = (\alpha_{1,2}, \alpha_{1,3}, \alpha_{3,1})$$

for some finite set of numbers $\alpha_{1,2}, \alpha_{1,3}, \alpha_{3,1}, \alpha'_{1,2}, \alpha'_{2,i}, \alpha'_{i,1}$. Thus,

$$\lambda_1 - \lambda_2 = \eta\alpha'_{1,2} = \epsilon\alpha_{1,2}$$

and

$$\eta = \epsilon \frac{\alpha_{1,2}}{\alpha'_{1,2}} .$$

It follows that

$$\lambda_i - \lambda_1 = \eta \alpha'_{i,1} = \epsilon \frac{\alpha_{1,2}}{\alpha'_{1,2}} \alpha'_{i,1}$$

so that $\epsilon^{-1}(\lambda_i - \lambda_1)$ is also contained in a finite set of values with the same unit ϵ. This same trick will work for each $\lambda_i - \lambda_j$ by using the triple $(\lambda_1 - \lambda_i)$, $(\lambda_i - \lambda_j)$, $(\lambda_j - \lambda_1)$ and gives (25).

It only remains to show that ϵ is restricted to some finite set. However, for any integer λ in K the discriminant of λ, $D(\lambda)$ satisfies

$$D(\lambda) = \text{Index}^2(\lambda) D(K)$$

with $D(K)$ the discriminant of K, and thus

$$D(\lambda) = \prod_{i<j} (\lambda_i - \lambda_j)^2 = \epsilon^{n(n-1)} \alpha$$

with α one of a finite set of numbers depending on the numbers given by (25) for each i,j. The unit ϵ is therefore restricted to a certain finite set of values and only a finite number of λ exist satisfying (24). This proves Theorem 2. §

If K is a field such that $s + t - 1 = 1$, i.e. with unit group generated by one fundamental unit, then every number with a given index can be calculated. As an example let ξ be a primitive thirteenth root of one and $K_{13} = Q(\xi)$. Then if K is the unique fourth degree subfield of K_{13}, it is generated by $tr_{K_{13}/K}(\xi) = \xi + \xi^3 + \xi^9$ and this number and its conjugates form an integral basis for the integers of K.

Since the prime ideal (3) splits completely in K, for every $\lambda \in \mathfrak{O}_K$ the index of λ in $\mathfrak{O}_K$ is a multiple of 3 [10] and thus there is no power basis for this order. There are integers λ with index 3 and all of these will be found.

Let $\theta_1 = \xi + \xi^3 + \xi^9$, $\theta_2 = \xi^2 + \xi^5 + \xi^6$, $\theta_3 = \xi^4 + \xi^{10} + \xi^{12}$, and $\theta_4 = \xi^7 + \xi^8 + \xi^{11}$. These are the conjugates of θ_1 and form an integral basis for $\mathfrak{O}_K$. Using this basis gives $D(K) = 13^3$. This can also be shown from ramification theory since 13 is tamely ramified. Every integer λ can be written uniquely in terms of the basis $(1, \theta_1, \theta_2, \theta_3)$ as

$$\lambda = x_0 + x_1\theta_1 + x_2\theta_2 + x_3\theta_3$$

for integers x_0, x_1, x_2, x_3 and satisfies

$$26) \qquad D(\lambda) = \mathrm{Index}^2(\lambda)\, D(K) .$$

Suppose Index$(\lambda) = 3$ and number the conjugates of λ such that

$$27) \qquad \begin{aligned} (\lambda_1 - \lambda_2) &= x_1(\theta_1 - \theta_2) + x_2(\theta_2 - \theta_3) + x_3(\theta_3 - \theta_4) \\ (\lambda_1 - \lambda_3) &= x_1(\theta_1 - \theta_3) + x_2(\theta_2 - \theta_4) + x_3(\theta_3 - \theta_1) , \end{aligned}$$

then (26) becomes

$$[N_{K/Q}(\lambda_1 - \lambda_2)]^2 N_{K/Q}(\lambda_1 - \lambda_3) = 3^2 \cdot 13^3 .$$

It is easy to find every integer in λ with norm equal to 3 or to 13, since (3) splits completely into the four prime ideals generated by the conjugates of θ_1 and (13) ramifies. Thus, every number with norm 3 is an associate of θ_1, θ_2, θ_3, or θ_4 and every number with norm 13 is an associate of $\theta_1 - \theta_3$, a generator of the unique ideal above (13). It is also easy to check that the norm of each $\theta_i - \theta_j$ is a multiple of 13, so $\lambda_i - \lambda_j$ is a multiple of $\theta_1 - \theta_3$ for every pair i,j and each λ.

Thus, the norms in (28) must have either

$$N_{K/Q}(\lambda_1 - \lambda_2) = 13 \qquad N_{K/Q}(\lambda_1 - \lambda_3) = 3^2 \cdot 13$$

or

$$N_{K/Q}(\lambda_1 - \lambda_2) = 3 \cdot 13 \qquad N_{K/Q}(\lambda_1 - \lambda_3) = 13 \;,$$

since there is no unit with norm -1.

The fact that (13) ramifies from $Q(\sqrt{13})$ to K can be used to prove that every unit of K is actually in the field $Q(\sqrt{13})$. Thus, the fundamental unit for K can be chosen to be η where

$$\eta = \frac{3 + \sqrt{13}}{2} \;.$$

Pick a particular complex thirteenth root of 1 for the value of ξ which makes

$$\theta_1 + \theta_3 = \frac{-1 + \sqrt{13}}{2} \;.$$

Then an easy calculation shows

29) $$\theta_2 - \theta_4 = \eta(\theta_1 - \theta_3) \;.$$

In solving (28) the calculations are simplified by noting that $\pm\lambda$ and all conjugates of λ have the same index. Thus, a conjugate might be used in the calculation in place of λ without any specific mention of the fact. The final set of solutions must be checked to insure that the conjugates of λ and $-\lambda$ are included.

First take the case where $\lambda_1 - \lambda_2$ has norm 13. Then as above, take λ such that

$$\lambda_1 - \lambda_2 = (\theta_1 - \theta_3)\eta^a .$$

Applying σ^2 to this equality gives

$$\sigma^2(\lambda_1 - \lambda_2) = -(\lambda_1 - \lambda_2) ,$$

which with (27) implies

$$(x_1 - x_2 + x_3)(\theta_1 - \theta_2 + \theta_3 - \theta_4) = 0 .$$

Therefore, $x_1 - x_2 + x_3 = 0$ and the two norm forms are

$$N_{K/Q}[x_1(\theta_1 - \theta_3) + x_3(\theta_2 - \theta_4)] = 13$$

$$N_{K/Q}[x_1(\theta_1 + \theta_2 - \theta_3 - \theta_4) + x_3(-\theta_1 + \theta_2 + \theta_3 - \theta_4)] = 3^2 \cdot 13 .$$

These are both proportional to full modules in $Q(\sqrt{13})$. In the second form, dividing out the factor $\theta_1 - \theta_3$ and using (29) gives

$$N_{K/Q}(\theta_1 - \theta_3)N_{K/Q}[x_1(\eta + 1) + x_3(\eta - 1)] = 3^2 \cdot 13 .$$

Thus, this reduces to

$$3x_1^2 - 4x_1x_3 - 3x_3^2 = \pm 3 .$$

The sign is required since this norm is only from $Q(\sqrt{13})$ to Q.

The other norm is easier and reduces to

$$x_1^2 + 3x_1x_3 - x_3^2 = \pm 1 .$$

The only common solutions are $(x_1, x_3) = (\pm 1, 0)$, $(0, \pm 1)$, and the triples (x_1, x_2, x_3) are given by $\pm(1, 1, 0)$ and $\pm(0, 1, 1)$. The full set of solutions will be determined from these by taking conjugates.

Now suppose $\lambda_1 - \lambda_2$ has norm $3 \cdot 13$, then it is equal to $(\theta_1 - \theta_3)$ times an associate of θ_1, θ_2, θ_3, or θ_4. Therefore,

$$\lambda_1 - \lambda_2 = (\pm 1)(\theta_1 - \theta_3)\theta_i \eta^a$$

for $i = 1, 2, 3$, or 4 and some integer a. Changing λ to $-\lambda$, if necessary, will eliminate the minus sign. It is always possible to take a conjugate to get the form

30) $$\lambda_1 - \lambda_2 = (\theta_1 - \theta_3)\theta_1 \eta^a$$

or

$$\lambda_1 - \lambda_2 = (\theta_2 - \theta_4)\theta_1 \eta^a .$$

But $\theta_2 - \theta_4$ is an associate of $\theta_1 - \theta_3$, so (30) is always reachable by these transformations.

Assuming $\lambda_1 - \lambda_2$ satisfies (30) and applying σ^2 to it, it follows that

$$\theta_3(\lambda_1 - \lambda_2) + \theta_1\sigma^2(\lambda_1 - \lambda_2) = 0 .$$

With (27) this implies

$$(-8x_1 + x_3)(\theta_1 + \theta_3) + (-5x_1 - x_3)(\theta_2 + \theta_4) = 0$$

and thus $x_1 = x_3 = 0$.

Therefore, $\lambda = x_2\theta_2$ and

$$\text{Index } \lambda = x_2^6 \text{ Index } \theta_2 .$$

It just happens that θ_2 has index 3, so $x_2 = \pm 1$.

Finally, by checking all possible signs and conjugations, it follows that every λ with index 3 in this field is equivalent to, or a conjugate of a number equivalent to, either $\pm\theta_1$ or $\pm(\theta_1 + \theta_2)$. Furthermore, it can be checked that the four conjugates to each of these two sets of numbers give different orders. So there are exactly eight distinct principal orders of index 3 in this field.

A similar problem which can be partially answered using Schmidt's Theorem involves the fundamental system of units for certain fields. Brumer [4] considered cyclic extensions of prime degree over Q. Let K be such a field and let E denote the units of K with norm +1. Sometimes E is generated by a unit ϵ and its conjugates. Such a unit is called a Minkowski unit. The cyclotomic units of K form a subgroup of E of index h, where h is the class number of the field K [8]. There is always a unit η which together with its conjugates generate H.

If the Galois group of K over Q is G and is generated by σ, then E is a module over the ring

$$Z[G]/(1 + \sigma + \cdots + \sigma^{p-1}) .$$

The multiplication of an element in the module by an element of the ring is written exponentially, so that for ϵ in E with conjugates $\epsilon = \epsilon_1, \epsilon_2 = \sigma\epsilon, \ldots, \epsilon_p = \sigma^{p-1}\epsilon$ and the ring element

$$\alpha = x_0 + x_1\sigma + \cdots + x_{p-2}\sigma^{p-2}$$

the product ϵ^{α} is given by

$$\epsilon^{\alpha} = (\epsilon_1)^{x_0}(\epsilon_2)^{x_1} \cdots (\epsilon_{p-1})^{x_{p-2}} .$$

Since this ring is isomorphic to the ring of integers in K_p, denoted here by $\mathfrak{O}$, E is a module over $\mathfrak{O}$ also. The multiplication in this case is exactly as described above, except with σ replaced by ξ.

The ring $\mathfrak{O}$ is also isomorphic with H by the isomorphism sending 1 to η and this extends uniquely to an isomorphism between E and $\mathfrak{A}^{-1}$, for some integral ideal $\mathfrak{A}$ in $\mathfrak{O}$. Since the index of H in E is equal to the norm of this ideal,

$$N_{K_p/Q}(\mathfrak{A}) = h .$$

There exists a Minkowski unit if and only if E is a free $\mathfrak{O}$-module, which is exactly when the ideal $\mathfrak{A}$ is principal.

Brumer used this setup to give sufficient conditions both for a field to have such a unit and for a field not to have such a unit.

The problem considered here is to find every Minkowski unit which is generated by some fixed finite set of units in E.

Since the group H is of index h in E, every unit ϵ of E satisfies $\epsilon^h \in H$. Thus, there exists a unique number α in $\mathfrak{O}$ such that

$$\epsilon^h = \eta^{\alpha} ,$$

where η^{α} is the multiplication described above. Therefore, every unit ϵ in E can be written uniquely as η^{α} with $h\alpha$ in $\mathfrak{O}$.

Let $\epsilon_1, \ldots, \epsilon_s$ be arbitrary units in E with

$$\epsilon_i = \eta^{\alpha_i}$$

for each $1 \leq i \leq s$. If ϵ is in the group generated by these units and is a Minkowski unit, then there exist integers $a_1, \ldots, a_s$ such that $\epsilon = \eta^{\alpha}$ and

$$\alpha = a_1\alpha_1 + \cdots + a_s\alpha_s$$

is a generator of the ideal $\mathfrak{A}^{-1}$. This requires

$$N_{K_p/Q}(\alpha) = 1/h , \qquad \alpha \in M$$

with the module $M = \{x_1\alpha_1 + \cdots + x_s\alpha_s\}$. The structure of possible solutions can be given using Schmidt's Theorem.

For example, let p-1 be twice an odd number, so the quadratic subfield of K_p is imaginary, and let m be the smallest non-trivial divisor of (p-1)/2. There can only exist a finite number of Minkowski units in any group generated by fewer than m units of E. This is because the module M has rank less than m and thus less than the degree of all of the subfields of K_p, except the imaginary quadratic subfield. Therefore, M is non-degenerate and Schmidt's Theorem shows the number of solutions must be finite. The most interesting case is when $p = 2q + 1$ with q a prime, since as many as q-1 units can be allowed and still only a finite number of Minkowski units will be possible.

REFERENCES

1. Baker, A. "Contributions to the Theory of Diophantine Equations." Philos. Trans. Roy. Soc. London, ser. A, 263 (1968) : 173-208.

2. Baker, A., and Coates, J. "Integer Points on Curves of Genus 1." Proc. Cambridge Philos. Soc. 67 (1970) : 595-602.

3. Borevich, Z. I., and Shafarevich, I. R. Number Theory. Translated from the Russian. Academic Press, 1966.

4. Brumer, Armand. "On the Group of Units of an Absolutely Cyclic Number Field of Prime Degree " J. Math. Soc. Japan 21 (1969) : 357-358.

5. Dade, E. C., and Taussky, O. "On the Different in Orders in an Algebraic Number Field and Special Units Connected With It." Acta Arithmetica IX (1964) : 47-51.

6. Györy, K. "Sur les Polynômes à Coefficients Entiérs et de Discriminant Donné." Acta Arithmetica XXIII (1973) : 419-426.

7. Györy, K. "Sur l'irréductibilité d'une Classe des Polynômes II." Publ. Math. Debrecen 19 (1972) : 293-326.

8. Hasse, H. Über der Klassenzahl abelishen Zahlkörper, p. 25. Berlin, 1952.

9. Hall, Marshall. "Indices in Cubic Fields." Bull. Amer. Math. Soc. 43 (1937) : 104-109.

10. Hensel, K. "Arithmetische Untersuchungen über die gemeinsamer ausserwesentliche Discriminantenteiler einer Gattung." Jour. für Math. 113 (1894) : 128-160.

11. Lang, Serge. Algebra. Addison-Wesley, 1971.

12. Mordell, L. J. Diophantine Equations. Academic Press, 1969.

13. Schmidt, Wolfgang M. "Norm Form Equations." Annals of Mathematics 96 (1972) : 526-551.

14. Schmidt, Wolfgang M. "Simultaneous Approximation to Algebraic Numbers by Rationals." Acta Mathematica 125 (1970) : 189-201.