UNITS IN SOME ALGEBRAIC NUMBER FIELDS

A thesis presented in partial fulfilment of

the requirements for degree of

Master of Science

in Mathematics at

Massey University

Neville Stuart Jeans

1978

ABSTRACT

Dirichlet's theorem describes the structure of the group of units of the ring of algebraic integers of any algebraic number field. This theorem shows that any unit can be written in terms of a fundamental system of units. However Dirichlet's theorem does not suggest any method by which such a fundamental system of units (or indeed any units) can be obtained.

This thesis looks at three types of algebraic number fields for which a fundamental system of units contains one unit, the so called fundamental unit. In each case properties of units and the problem of obtaining a fundamental unit are discussed.

Chapter one is an introductory chapter which summarises the basic theory relevant to algebraic number fields of arbitrary degree. Basic properties of units and Dirichlet's theorem are also given.

Chapter two looks at units of Quadratic fields, $Q(\sqrt{d})$. Units of imaginary quadratic fields are mentioned briefly but the chapter is mainly concerned with the more complicated problem of obtaining real quadratic units. The relevant theory of simple continued fractions is presented and the way in which units can be obtained from the simple continued fraction expansion of $\sqrt{d}$ is outlined. The chapter then also looks at some recent papers dealing with the length of the period of $\sqrt{d}$ and concludes by showing how units can be obtained from the simple continued fraction expansion of $(1 + \sqrt{d})/2$ when $d \equiv 1 \pmod 4$.

Chapter three looks at units of pure cubic fields. The basic properties of pure cubic units are developed and reference is made to various algorithms which can be used to obtain pure cubic units. The main purpose of this chpater is to present the results of the paper 'Determining the Fundamental Unit of a Pure Cubic Field Given any Unit' (Jeans and Hendy [1978]). However in this thesis a different approach to that of the paper is used and for two of the results sharper bounds have been obtained. Several examples are given using the algorithm which is developed from these results.

Chapter four, which is original work, investigates the quartic fields, $Q(d^{\frac{1}{4}})$, where d is a square-free negative integer. Similarities between these quartic fields and the pure cubic and real quadratic fields are developed of which the main one is a quartic analogue of the results given in the paper mentioned above.

The examples given in chapter three required multiprecision computer programs and these programs have been listed in appendix one.

ACKNOWLEDGEMENT

I would like to thank my supervisor, Dr M D Hendy for the advice and encouragement he has offered during my work on this thesis.

CONTENTS

1 INTRODUCTION

This chapter gives a short summary of the basic theory which is relevant to this thesis. While the contents of this chapter have not been derived from any particular source, texts such as Richman [1971], Adams and Goldstein [1976], Clark [1971], Maxfield and Maxfield [1971], Cohn [1962], Niven and Zuckerman [1972], and Samuel [1970] give varying degrees of coverage of the material to be summarised in this chapter.

Notation

The symbols defined below will have the same meaning through out the thesis.

Z^+	-	the set $\{1, 2, 3, 4, \ldots\}$
Z	-	the set of rational integers
Q	-	the set of rational numbers
R	-	the set of real numbers
$Z[\alpha,\beta]$	-	the module $\{a_1\alpha + a_2\beta \mid a_1, a_2 \in Z\}$
(a,b)	-	the greatest common divisor of the integers a, b.
$[\ ]$	-	the greatest integer function
i	-	the square root of minus one.

In general, Greek letters will denote algebraic numbers and letters of the Roman alphabet will denote rational integers.

Algebraic Fields

Let F be a number field, that is F is a subfield of the field of complex numbers. The polynomial

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$$

$$a_n \neq 0,\ a_i \in F,$$

is called a polynomial over F and the set of all such polynomials forms an integral domain denoted by $F[x]$. p is said to be of degree n, written deg (p) = n. A monic polynomial is one in which the leading coefficient, a_n, is unity.

A number, α, is algebraic over F if it is the zero of some polynomial $f \in F[x]$.

Theorem 1.1

If α is algebraic over F, there exists a unique polynomial $f \in F(\alpha)$ such that

i) $f(\alpha) = 0$

ii) f is monic

iii) if $g \in F[x]$ and $g(\alpha) = 0$ then $f|g$

f is called the minimal polynomial for α and the degree of α is defined to be equal to deg(f). //

Theorem 1.2

The set $F(\alpha) = \{b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} | b_i \in F,$ n = deg $(\alpha)\}$ forms a number field which is a simple extension of F. It is the smallest field that contains both α and F. //

If $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \in F(\alpha)$ then

$b_0, b_1, \ldots, b_{n-1}$ are called the coefficients of β.

Theorem 1.3

$F(\alpha)$ is a vector space over F with basis $1, \alpha, \ldots, \alpha^{n-1}$. Consequently any $\beta \in F(\alpha)$ is algebraic over F and deg $(\beta) \leq$ deg (α). $F(\alpha)$ is an algebraic extension of F. //

The minimal polynomial for α can be factored as n distinct linear factors in C,

$$f(x) = (x - \alpha)(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{n-1})$$

The $n - 1$ numbers $\alpha_1, \alpha_2 \ldots, \alpha_{n-1}$ are called the conjugates of α.

Theorem 1.4

Let $\beta \in F(\alpha)$. Then $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ where $n = \deg(\alpha)$ and $b_j \in F$. Let g be the minimal polynomial for β. Define

$$\beta_j = b_0 + b_1\alpha_j + b_2\alpha_j + \ldots + b_{n-1}\alpha_j^{n-1}, \quad j = 1, 2, \ldots, n - 1 \quad (1)$$

where the α_j are the conjugates of α.

Let $h(x) = (x - \beta)(x - \beta_1) \ldots (x - \beta_{n-1})$

Then
i) each β_j is either equal to β or is a conjugate of β.
ii) h is a monic polynomial and $h \in F[x]$*.
iii) $h = g^p$ where deg (g) x p = deg (α), $p \in Z^+$
iv) $N(\beta) = \beta\beta_1\beta_2 \ldots \beta_{n-1}$, called the norm function (with respect to $F(\alpha)$) is a multiplicative homomorphism from $F(\alpha)$ into F
v) $N(\beta) = (-1)^n a_o$, where a_o is the constant term of the polynomial h. //

---

* i) and ii) follow from consideration of the automorphisms of $F(\alpha, \alpha_1, \ldots, \alpha_{n-1})$, the splitting field for f over F.

Algebraic Numbers, Number Fields and Integers

If we take F = Q in the previous section then any α algebraic over Q is called an algebraic number, $Q(\alpha)$ is called an algebraic number field, and for any $\beta \in Q(\alpha)$ $N(\beta)$ is necessarily a rational number.

Example 1.1

As an illustration of theorem 1.4, consider $\beta = 3 + 5\sqrt{2}$, whose minimal polynomial over Q is

$$f(x) = x^2 - 6x - 41$$

If we consider β to be an element of $Q(\sqrt{2})$ then

$$\beta_1 = 3 - 5\sqrt{2} ,$$

$$h_1(x) = x^2 - 6x - 41 = f(x) ,$$

and $$N_1(\beta) = -41$$

If we consider β to be an element of $Q(2^{\frac{1}{4}})$ then

$$\beta_1 = 3 - 5\sqrt{2} ,$$

$$\beta_2 = 3 + 5\sqrt{2} = \beta ,$$

$$\beta_3 = 3 - 5\sqrt{2} = \beta_1 ,$$

$$h_2(x) = x^4 - 12x^3 - 46x^2 + 492x + 1681$$

$$= (f(x))^2$$

and $$N_2(\beta) = 1681 = (N_1(\beta))^2$$ //

An algebraic integer is an algebraic number whose minimal polynomial has integer coefficients. Consequently the norm of an algebraic integer is a rational integer.

Theorem 1.5.

The algebraic integers of an algebraic number field, $Q(\alpha)$, form an integral domain (denoted by $Z(\alpha)$). $Z(\alpha)$ is often referred to as the ring of algebraic integers of $Q(\alpha)$. //

Recalling h as defined in theorem 1.4 we have that for $\beta \in Q(\alpha)$,

$\beta \in Z(\alpha) \Leftrightarrow$ h has integer coefficients.

This fact is used when we determine the form of the algebraic integers of a particular $Q(\alpha)$.

The only rational numbers which are also algebraic integers are the rational integers, Z, and for any ring of algebraic integers, $Z(\alpha)$, we have $Z \subseteq Z(\alpha)$.

An integral basis of $Q(\alpha)$ is a set of elements $\theta_1, \theta_2, \ldots, \theta_k \in Z(\alpha)$ such that every $\beta \in Z(\alpha)$ can be written uniquely in the form $\beta = m_1\theta_1 + m_2\theta_2 + \ldots + m_k\theta_k$ where $m_1, m_2, \ldots, m_k \in Z$. Every $Z(\alpha)$ has an integral basis and an integral basis of $Z(\alpha)$ is also a basis of $Q(\alpha)$.

If $\theta_1, \theta_2, \ldots, \theta_n$ is a basis of $Q(\alpha)$ and if θ_j has conjugates $\theta_j^{(1)}, \theta_j^{(2)}, \ldots, \theta_j^{(n-1)}$ then the discriminant of the basis is the determinant,

$$\Delta = \begin{vmatrix} \theta_1 & \theta_2 & \theta_3 & \cdots & \theta_n \\ \theta_1^{(1)} & \theta_2^{(1)} & \theta_3^{(1)} & \cdots & \theta_n^{(1)} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \theta_1^{(n-1)} & \theta_2^{(n-1)} & \theta_3^{(n-1)} & \cdots & \theta_n^{(n-1)} \end{vmatrix}^2$$

The discriminant of a basis of $Q(\alpha)$ is a rational number. If the basis is also an integral basis of $Q(\alpha)$ then the discriminant of the basis is a rational integer. Each integral basis of $Q(\alpha)$ has the same discriminant. Thus the discriminant of any integral basis of $Q(\alpha)$ is also called the discriminant of the field $Q(\alpha)$.

Example 1.2

Let $\alpha = \sqrt{d}$, d a square-free integer. In chapter two we will see that

i) $1, \sqrt{d}$ forms an integral basis when $d \equiv 2, 3 \pmod 4$

ii) $1, (1 + \sqrt{d})/2$ forms an integral basis when $d \equiv 1 \pmod 4$

Thus when $d \equiv 2, 3 \pmod 4$

$$\Delta = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d$$

and when $d \equiv 1 \pmod 4$

$$\Delta = \begin{vmatrix} 1 & (1+\sqrt{d})/2 \\ 1 & (1-\sqrt{d})/2 \end{vmatrix}^2 = d$$

Units of the Ring of Algebraic Integers of $Q(\alpha)$

If $\beta \in Z(\alpha)$ and $\beta \neq 0$ then $\beta^{-1} \in Q(\alpha)$. If we also have that $\beta^{-1} \in Z(\alpha)$, then β is called a unit of $Z(\alpha)$.

Theorem 1.6

$\beta \in Z(\alpha)$ is a unit $\Leftrightarrow$ $N(\beta) = \pm 1$.

Proof

Let the minimal polynomial for β be

$$f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0, \quad a_j \in Z$$

Then $a_0 \neq 0$ (otherwise f would not be minimal) and $f(\beta) = 0$. Thus we have

$$0 = 1/a_0 + a_{m-1}\beta^{-1}/a_0 + \ldots + a_1(\beta^{-1})^{m-1}/a_0 + (\beta^{-1})^m$$

The polynomial

$$f_1(x) = x^m + a_1 x^{m-1}/a_0 + \ldots + 1/a_0$$

is the minimal polynomial for β^{-1} and clearly $\beta^{-1} \in Z(\alpha)$ precisely when $a_0 = \pm 1$. The theorem now follows since $N(\beta)$ is a power of a_0 multiplied by ± 1. (Theorem 1.4 v)). //

The inverse of β is given by

$$\beta^{-1} = \beta_1\beta_2 \ldots \beta_{m-1}(N(\beta))^{-1}$$

where the β_j are as defined in (1).

If β and γ are algebraic integers of $Q(\alpha)$ and (β/γ) is a unit then we say that β and γ are associates.

The units of $Z(\alpha)$ form a multiplicative group whose structure is described in the following theorem due to Dirichlet.

Theorem 1.7

Let α be an algebraic number and f its minimal polynomial. Suppose that f has r real roots and 2s non-real roots, that is $\deg(\alpha) = r + 2s$. Then there exist units $\eta_1, \eta_2, \ldots, \eta_t$, where $t = r + s - 1$, such that every unit, η, of $Z(\alpha)$ may be written as

$$\eta = \xi\eta_1^{a_1}\eta_2^{a_2} \ldots \eta_t^{a_t}, \quad a_j \in Z$$

where ξ is some root of unity contained in $Z(\alpha)$.

Proof

[Samuel, 1970, p60], [Delone and Faddeev, 1964, p28] //

The number of possible values for ξ is finite and in the case that α is real or α has real conjugates the only values for ξ are ± 1.

The set of units $\eta_1, \eta_2, \ldots, \eta_t$ is referred to as a fundamental system of units of $Z(\alpha)$. Such a system is not unique since if $\eta_1, \eta_2, \ldots, \eta_t$ is a fundamental system then so is $\eta_1^{-1}, \eta_2, \ldots, \eta_t$.

When $t = 1$, we can write any unit of $Z(\alpha)$ as $\xi\eta_1^{a_1}$ for some unit $\eta_1 \in Z(\alpha)$. In such a case we call η_1 a fundamental unit. It is easily shown that η_1 must be such that there is no unit whose magnitude lies between 1 and $|\eta_1|$, and that the only other fundamental units are of the form $\xi\eta_1^{\pm 1}$. Consequently there are only a finite

number of fundamental units when $t = 1$. (If α is real or has a real conjugate then there are four fundamental units). It is usual to define precisely one of these units as the fundamental unit of $Z(\alpha)$.

Example 1.3

Let α be a real quadratic irrational, then $t = 1$ and there is one unit in any fundamental system. Let $\eta_1 \in Z(\alpha)$ be the smallest unit greater than unity.

Then each of η_1, η_1^{-1}, $-\eta_1$ and $-\eta_1^{-1}$ is a fundamental unit. We take η_1 as the fundamental unit. //

When t is greater than one, the situation is more complex. Firstly, there are always units whose magnitudes are arbitrarily close to unity and, secondly, from any given fundamental system of units it is possible to derive an infinite number of distinct fundamental systems. For example, the set $\eta_1, \eta_2, \ldots, \eta_t$ give rise to the systems $\eta_1\eta_2^p, \eta_2, \ldots, \eta_t$, where p is any integer. Consequently, a fundamental system cannot be characterised when $t > 1$ in a manner similar to the case when $t = 1$.

In the following three chapters we shall confine our attention to cases where $t = 0, 1$.

The problem of finding all the units of $Z(\alpha)$ is effectively solved by finding a fundamental system of units. Dirichlet's theorem offers no help in this area and we have to look to other areas of mathematics (for example, continued fractions) to find algorithms which can be used to calculate units in algebraic number

fields and theory which enables us to determine whether or not a system of units is fundamental.