

ALGEBRAIC INTEGERS, UNITS AND
INTEGRAL BASES

By

ROBERT EDWARD DAHLIN

Bachelor of Applied Mathematics
University of Minnesota
Minneapolis, Minnesota
1960

Master of Science
University of Minnesota
Minneapolis, Minnesota
1963

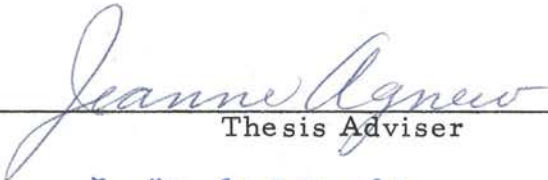
Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
May, 1972

Thesis
19720
0131a
cop 2

AUG 10 1973

ALGEBRAIC INTEGERS, UNITS AND
INTEGRAL BASES

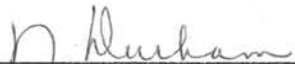
Thesis Approved:



Thesis Adviser

E. K. M. S. Jackson





Dean of the Graduate College

PREFACE

The goal of this thesis is to write a segment of mathematics that would fit between a first course in elementary number theory and a course in algebraic number theory. Current books titled algebraic number theory are an abstract generalization of the material presented in this thesis. The transition from elementary number theory to such abstract treatments of algebraic number theory is too difficult for the average undergraduate student. This thesis provides an intermediate step discussing algebraic number fields and the domain of algebraic integers therein. All the fields discussed are finite algebraic extensions of the rational numbers. Examples are used to demonstrate the theory.

The level of this material is for a senior mathematics major. In addition to a course in elementary number theory he should have had a course in linear algebra. Abstract algebra would be helpful but not necessary if the linear algebra course was fairly sophisticated and complete. A student could not, of course, go on to a complete study of algebraic number theory without a thorough knowledge of abstract algebra.

The thesis is divided into five chapters. The first chapter introduces the concept of an algebraic integer. Then some elementary facts concerning algebraic integers and their minimal polynomials are proved. The second chapter deals with finite algebraic extensions of

the rational numbers. The norm and trace of a number in a finite algebraic extension are defined. The properties of norm and trace, used frequently in Chapters III and IV, are developed. Chapter III derives the integral basis theorem and develops some techniques for computing such a basis. Examples are given demonstrating how the various concepts can be used as aids for calculating an integral basis of a finite algebraic extension. The main topic in Chapter IV is the proof of Dirichlet's theorem on the structure of the group of units in a finite algebraic extension. This theorem is usually proved using results from the theory of ideals. The proof in this paper does not use these results but uses only the concepts already developed and some elementary counting techniques. Dirichlet's theorem is demonstrated by an example in which a fundamental unit is calculated for a cubic extension. The final chapter presents some examples of how algebraic number theory can be used to find solutions to Diophantine equations. The paper concludes with some remarks about related topics and current developments.

Items such as theorems, definitions or examples are numbered consecutively throughout the paper.

I would like to take this opportunity to express my thanks for the assistance, guidance and time given to me by the members of my committee: Dr. Jeanne L. Agnew, my thesis advisor, Dr. E. K. McLachlan, my committee chairman, and Dr. W. Ware Marsden.

In addition I would like to thank the University of Wisconsin, Superior, for giving me time and financial support for this project.

Finally, I would like to express my appreciation and gratitude to my wife, Priscilla, and our children, Peter, Mark and Rachel, for

their understanding, patience, and the sacrifices they made that I might write this dissertation.

TABLE OF CONTENTS

Chapter	Page
I. INTRODUCTION	1
II. ALGEBRAIC NUMBER FIELDS	15
III. RINGS OF ALGEBRAIC INTEGERS	34
IV. UNITS	54
V. CONCLUSION	85
A SELECTED BIBLIOGRAPHY	90

CHAPTER I

INTRODUCTION

The Diophantine equation

$$x^2 - y^2 = 17$$

might be solved by the following method:

$$x^2 - y^2 = (x+y)(x-y) .$$

Since x and y are integers $x+y$ and $x-y$ must be factors of 17.

A solution may be obtained by setting

$$x+y = 17$$

$$x-y = 1$$

or $x=9$ and $y=8$. Three other solutions may be achieved by changing the signs or order of the factors of 17. Since the only factors of 17 are ± 1 and ± 17 there cannot be any other solutions.

A similar approach to the Diophantine equation

$$x^2 - 2y^2 = 17$$

fails. Since

$$x^2 - 2y^2 = (x + \sqrt{2}y)(x - \sqrt{2}y) .$$

The factors $(x + \sqrt{2}y)$ and $(x - \sqrt{2}y)$ are not integers, when x and

y are integers, unless $y=0$. Example 91 will show that this equation not only has a solution, but has infinitely many solutions. One can see that a solution to this equation is $x=7$ and $y=4$. Thus one might say that

$$17 = (7 + 4\sqrt{2})(7 - 4\sqrt{2})$$

is a factorization of 17. What is needed is a set of numbers which contain the integers and numbers such as $7 \pm 4\sqrt{2}$.

Definition 1. Let θ be a root of the polynomial

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0.$$

When $a_{n-1}, a_{n-2}, \dots, a_1, a_0$ are integers, θ is called an algebraic integer. When the coefficients are rational, θ is called an algebraic number.

Algebraic numbers can be real or complex. The purpose of this dissertation is to present methods of representing algebraic integers and computing with these integers. Throughout this material Z will stand for the integers and Q the rationals. Since the integers are themselves algebraic integers they will be referred to as the rational integers to distinguish them from the other algebraic integers. The set of polynomials in x with rational coefficients will be denoted by $Q[x]$. The subset of $Q[x]$ that consists of polynomials with coefficients that are rational integers is denoted by $Z[x]$. Consider the polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad a_n \neq 0.$$

The degree of this polynomial is n , a_n is the leading coefficient, and when $a_n = 1$ the polynomial is called monic. Note that the constant polynomial a_0 has degree zero except when $a_0 = 0$. Degree is not defined for the zero polynomial. The rules for working with polynomials that one learns in a high school or college algebra course will be assumed. The following theorem is a formal statement of the usual division process one learns for polynomials.

Theorem 2. If $p(x)$ and $f(x) \neq 0$ are polynomials in $Q[x]$ there exist unique polynomials $q(x)$ and $r(x)$ in $Q[x]$ such that $p(x) = q(x)f(x) + r(x)$, where either the degree of $r(x)$ is less than the degree of $f(x)$, or $r(x)$ is the zero polynomial.

When the polynomial $r(x)$ in Theorem 2 is the zero polynomial then $f(x)$ is said to divide $p(x)$. A polynomial in $Q[x]$ is called irreducible in $Q[x]$ if it cannot be expressed as the product of two polynomials in $Q[x]$ each with degree greater than zero. Note, constant multiples of irreducible polynomials are irreducible. Irreducible polynomials in $Q[x]$ have many properties that are similar to prime numbers in Z . The following theorem is an example of this.

Theorem 3. If $f(x)$ and $g(x)$ in $Q[x]$ have no common divisors other than constants, then there exist $h(x)$ and $k(x)$ in $Q[x]$ such that

$$h(x)f(x) + k(x)g(x) = 1.$$

A detailed account of Theorems 2 and 3 as well as their proofs can be found in most theory of equation texts. The proofs of these

theorems rely on the fact that the coefficients are members of a field. No other properties of \mathbb{Q} are used, thus \mathbb{Q} could be replaced by the real numbers, the complex numbers or any other field. There will be occasions when other fields are used. Since \mathbb{Z} is not a field Theorems 2 and 3 do not hold for polynomials in $\mathbb{Z}[x]$, However, polynomials in $\mathbb{Z}[x]$ are also polynomials in $\mathbb{Q}[x]$, so that, with care these theorems can be used. The following example illustrates the fact that given a polynomial $f(x)$ in $\mathbb{Q}[x]$ there is a rational integer k such that $kf(x)$ is in $\mathbb{Z}[x]$.

Example 4. Consider the following polynomial in $\mathbb{Q}[x]$

$$f(x) = \frac{2}{3}x^3 + \frac{4}{3}x^2 + \frac{2}{5}x + \frac{2}{9}$$

then

$$45f(x) = 30x^3 + 60x^2 + 27x + 10.$$

Note that 45 is simply the least common multiple of 3, 3, 5, and 9; the denominators of the coefficients. Another fact is that the greatest common divisor of the numerators 2, 4, 2 and 2 is equal to the greatest common divisor of 30, 60, 27 and 10, the coefficients of $45f(x)$..

It is easily seen that in general any polynomial in $\mathbb{Q}[x]$ can be multiplied by a rational integer to obtain a new polynomial in $\mathbb{Z}[x]$. In addition the greatest common divisor of numerators of the rational coefficients is equal to the greatest common divisor of the integral coefficients. This fact is assumed in the proof of Theorem 7. The following lemma is needed in the proof of Theorem 6.

Lemma 5. Let $f(x) = g(x)h(x)$ with all the coefficients rational integers. If p is a rational prime that divides all the coefficients of $f(x)$ then p must divide all the coefficients of $g(x)$ or of $h(x)$.

Proof. Let

$$g(x) = \sum_{j=0}^n a_j x^j \quad h(x) = \sum_{i=0}^m b_i x^i$$

then the coefficient of x^r in $f(x)$ is

$$\sum_{s=0}^r a_{r-s} b_s$$

where $a_j = 0$ when $j > n$ and $b_i = 0$ when $i > m$. Suppose the conclusion of the lemma is false. Let k be the smallest subscript such that $p \nmid a_k$ and t be the smallest subscript such that $p \nmid b_t$. Consider the coefficient of x^{t+k} in $f(x)$,

$$\sum_{s=0}^{t+k} a_{t+k-s} b_s.$$

By the choice of k and t , $p \mid a_{t+k-s} b_s$ for every s from 0 to $t+k$ except for $s=t$, $p \nmid a_k b_t$. Thus p cannot divide the coefficient of x^{t+k} in $f(x)$. The hypothesis of the lemma is contradicted, so the lemma is proved by contraposition.

The next theorems will show that Definition 1 is not inconsistent, that is, it is not possible, by considering different polynomials for which θ is a root, to say that sometimes θ is an algebraic integer and sometimes it is not.

Theorem 6. If a monic polynomial $f(x)$ with rational integral coefficients can be factored into two monic polynomials $g(x)$ and $h(x)$ in $\mathbb{Q}[x]$, then the coefficients of $h(x)$ and $g(x)$ are rational integers.

Proof. Let

$$g(x) = x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \frac{a_{n-2}}{b_{n-2}} x^{n-2} + \dots + \frac{a_1}{b_1} x + \frac{a_0}{b_0}$$

and

$$h(x) = x^n + \frac{c_{n-1}}{d_{n-1}} x^{n-1} + \frac{c_{n-2}}{d_{n-2}} x^{n-2} + \dots + \frac{c_1}{d_1} x + \frac{c_0}{d_0}$$

where a_i, b_i, c_i, d_i are in \mathbb{Z} and $(a_i, b_i) = 1 = (c_j, d_j)$. Let s be the least common multiple of b_0, b_1, \dots, b_{n-1} and t be the least common multiple of d_0, d_1, \dots, d_{n-1} . Then as in Example 4 $sg(x)$ and $th(x)$ are in $\mathbb{Z}[x]$ also the greatest common divisor of the coefficients of $sg(x)$ is 1 and $th(x)$ is 1. The proof will be completed when it is shown that $s=t=1$. Since $f(x) = g(x)h(x)$ then $stf(x) = (sg(x))(th(x))$. Suppose p is prime and $p|st$ then p divides all the coefficients of $stf(x)$. From Lemma 5, p must divide all the coefficients of $sg(x)$ or $th(x)$, but this is impossible, thus there is no prime that divides st . Since st is not divisible by a prime and s and t are positive rational integers $s=t=1$.

It is possible to prove a more general theorem than Theorem 6. The restriction that $f(x)$, $g(x)$ and $h(x)$ are monic can be omitted and the same conclusion obtained. Such generality is not needed here, so the theorem is not included.

The next theorem is very important. The results are used extensively throughout the remainder of the paper.

Theorem 7. An algebraic number θ is the root of a unique irreducible monic polynomial $f(x)$ in $\mathbb{Q}[x]$. All other polynomials in $\mathbb{Q}[x]$ for which θ is a root are divisible by $f(x)$.

Proof. Since any polynomial in $\mathbb{Q}[x]$ may be divided by its leading coefficient without affecting the roots only monic polynomials need be considered. From all the (monic) polynomials for which θ is a root, pick $f(x)$ such that the degree of $f(x)$ is less than or equal to the degree of any of the others. Suppose $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$ where the degrees of $g(x)$ and $h(x)$ are less than the degree of $f(x)$. Now $f(\theta) = g(\theta)h(\theta) = 0$ implies θ is a root of $g(x)$ or $h(x)$ contradicting the choice of $f(x)$. Thus $f(x)$ is irreducible. Consider any polynomial $g(x)$ in $\mathbb{Q}[x]$ with θ as a root. From Theorem 2 $g(x) = f(x)k(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $f(x)$ or $r(x)$ is zero. Now $g(\theta) = f(\theta)k(\theta) + r(\theta)$ implies $r(\theta) = 0$. The choice of $f(x)$ implies $r(x)$ is the zero polynomial, thus $f(x)$ divides $g(x)$. Since $f(x)$ divides all other polynomials with θ as a root, the only irreducible polynomials with θ as a root are constant multiples of $f(x)$. Thus $f(x)$ is the unique monic polynomial satisfying the conclusion of the theorem.

Definition 8. The polynomial $f(x)$ in Theorem 6 is called the minimal polynomial of θ , and the degree of $f(x)$ is called the degree of θ .

Theorem 6 implies the minimal polynomial of an algebraic integer is in $\mathbb{Z}[x]$. If a is a rational number then $x - a$ is the minimal polynomial of a . Thus the only rational numbers that are algebraic integers are the rational integers.

The next few theorems will reveal some facts about the roots of polynomials and how the roots and coefficients of a polynomial are related.

Definition 9. If

$$f(x) = \sum_{i=0}^n a_i x^i$$

then the derivative, $f'(x)$, is defined as

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1}.$$

Although no use of limits was made to define the derivative, all the results from elementary calculus regarding the derivatives of polynomials can be obtained, and they will be used freely.

Theorem 10. If θ is a root of $f(x)$ then $f(x) = (x - \theta)g(x)$. The coefficients of $g(x)$ may be complex numbers.

Proof. Theorem 2 with \mathbb{Q} replaced by the field of complex numbers gives

$$f(x) = (x - \theta)g(x) + r$$

where r is a constant. Now $r = f(\theta) - (\theta - \theta)g(\theta) = 0$ and the theorem is proved.

Definition 11. A root θ of $f(x)$ has multiplicity k if $f(x) = (x - \theta)^k g(x)$ and θ is not a root of $g(x)$. If $k=1$ the root is simple.

Theorem 12. If θ is a root of multiplicity k for $f(x)$ and $k > 1$, then θ is a root of $f'(x)$.

Proof. From the definition

$$f(x) = (x - \theta)^k g(x)$$

thus

$$f'(x) = (x - \theta)^{k-1} g(x) + (x - \theta)^k g'(x)$$

so

$$f'(\theta) = 0 \text{ and the theorem is proved.}$$

Theorem 13. If $f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$ then all the roots of $f(x)$ are simple.

Proof. Again, as in Theorem 7, only monic polynomials need be considered. If θ is a root of $f(x)$ then $f(x)$ is the minimal polynomial of θ . The degree of $f'(x)$ is less than the degree of $f(x)$ so that θ is not a root of $f'(x)$. Thus by Theorem 12, θ is a simple root.

A polynomial in n variables is said to be symmetric if the variables can be permuted without changing the polynomial. For example

$$h(x, y, z) = 3x^2 y^2 z^2 + xy + yz + xz + x + y + z$$

is symmetric since

$$\begin{aligned} h(x, y, z) &= h(y, x, z) = h(y, z, x) = h(z, x, y) \\ &= h(z, y, x) = h(x, z, y). \end{aligned}$$

But $g(x, y, z) = x + y + z^2$ is not symmetric since

$$g(x, y, z) \neq g(z, x, y) = z + x + y^2.$$

The polynomials

$$s_1 = x_1 + x_2 + x_3 + \dots + x_n$$

$$s_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n$$

$$s_3 = x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n$$

...

$$s_n = x_1x_2 \dots x_n$$

are called the elementary symmetric functions in n variables. If

x_1, x_2, \dots, x_n are roots of the polynomial

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} + x^n$$

then $f(x)$ can be factored

$$f(x) = (x - x_1)(x - x_2)(x - x_3) \dots (x - x_n).$$

Multiplying out the second form and equating the coefficients gives

$$a_0 = (-1)^n s_n$$

$$a_1 = (-1)^{n-1} s_{n-1}$$

...

$$a_{n-1} = -s_1.$$

This simple relation between the elementary symmetric functions of

the roots and the coefficients of a polynomial is very useful. If the roots of $f(x)$ are bounded by M then $|a_i| \leq \binom{n}{i} M^i$, where $\binom{n}{i}$ is the binomial coefficient.

Theorem 14. A symmetric polynomial in n variables with coefficients in a ring R can be written as a polynomial in the n elementary symmetric functions with coefficients in R .

The proof can be found in Clark [6]. The usual proof of this theorem yields a method of finding the polynomial. The theorem can also be proved by double induction on n and the degree of the polynomial. The following example demonstrates another method and also gives a result to be used later.

Example 15. Consider the square of the Vandermonde determinant

$$\Delta(x, y, z) = \begin{vmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{vmatrix}^2 = (x-y)^2(x-z)^2(y-z)^2.$$

This function is symmetric in x , y and z . Let the elementary symmetric functions of x , y and z be

$$a = x + y + z$$

$$b = xy + xz + yz$$

$$c = xyz.$$

$\Delta(x, y, z)$ is homogeneous of degree six, that is, each term has degree six. The combinations of a , b , and c which give degree six are c^2 , b^3 , a^6 , abc , b^2a^2 , ba^4 and ca^3 .

Assume

$$\Delta = Ac^2 + Bb^3 + Ca^6 + Dabc + Eb^2a^2 + Fba^4 + Gca^3 .$$

It would be possible to find the values of A, B, C, D, E, F, and G by expanding the equation in terms of x, y, and z and equating coefficients of like x, y, z terms. Since this is very tedious seven different values of (x, y, z) are chosen to determine a set of linear equations for A, B, C, D, E, F and G. The values are tabulated:

x	y	z	a	b	c	Δ
1	0	0	1	0	0	0
1	1	0	2	1	0	0
1	-1	0	0	-1	0	4
2	-1	-1	0	-3	2	0
2	1	0	3	2	0	4
1	2	3	6	11	6	4
1	-1	2	2	-1	-2	36

This gives the equations

$$0 = C$$

$$0 = B + 64C + 4E + 16F$$

$$4 = -B$$

$$0 = 4A - 27B$$

$$4 = 8B + 279C + 36E + 162F$$

$$4 = 36A + 1331B + 46656C + 396D + 4356E + 14255F + 1296G$$

$$36 = 4A - B + 64C + 4D + 4E - 16F - 16G .$$

Solving the equations gives

$$A = -27, B = -4, C = 0, D = 18, E = 1, F = 0, G = -4$$

or

$$\Delta = b^2a^2 + 18abc - 27c^2 - 4b^3 - 4ca^3.$$

This chapter concludes with the theorem that demonstrates that the set of algebraic numbers and the set of algebraic integers are closed with respect to the arithmetic operations of addition and multiplication.

Theorem 16. The product, sum or difference of algebraic numbers is an algebraic number. If the numbers are algebraic integers then the results are algebraic integers.

Proof. Let α and β be algebraic numbers with minimal polynomials $h(x)$ and $k(x)$. Let $\alpha = \alpha_1, \dots, \alpha_n$ be the n distinct roots of $h(x)$ and $\beta = \beta_1, \dots, \beta_m$ be the m distinct roots of $k(x)$. Form the polynomials

$$s(x) = \prod (x - \alpha_j - \beta_i)$$

$$d(x) = \prod (x - \alpha_j + \beta_i)$$

$$p(x) = \prod (x - \alpha_j \beta_i).$$

Where $i = 1, 2, \dots, m$, and $j = 1, 2, \dots, n$. These polynomials are symmetric in $\alpha_1, \alpha_2, \dots, \alpha_n$ and in β_1, \dots, β_m . Theorem 14 implies that $s(x)$, $d(x)$ and $p(x)$ can be expressed as polynomials in the elementary symmetric functions of $\alpha_1, \dots, \alpha_n$ and β_1, \dots, β_m , but these are the coefficients of $h(x)$ and $k(x)$. Thus $s(x)$, $d(x)$ and $p(x)$ are polynomials with coefficients from the same domain as $h(x)$ and $k(x)$. The roots of $s(x)$, $d(x)$ and $p(x)$ are thus algebraic

numbers or algebraic integers depending on whether α and β are algebraic numbers or algebraic integers. Finally $\alpha + \beta$ is a root of $s(x)$, $\alpha - \beta$ is a root of $d(x)$ and $\alpha\beta$ is a root of $p(x)$. Note however, that these three polynomials are not necessarily the minimal polynomial of the sum, difference and product of α and β .

Theorem 16 implies that the set of algebraic numbers and the set of algebraic integers form a subring of the complex numbers. One could show that the inverse of an algebraic number is an algebraic number and thus the set of algebraic numbers forms a subfield of the complex numbers. This result will appear in the next chapter where certain algebraic number fields will be studied.

CHAPTER II

ALGEBRAIC NUMBER FIELDS

The object of this chapter is to present some basic facts about fields of algebraic numbers. Consider two fields H and K where H is a subfield of K . Then K can be thought of as a vector space over H , with vector addition ordinary addition in K and scalar multiplication ordinary multiplication in K . The field K is called an extension of H . The dimension of the vector space K over H is the degree of the extension K over H .

Example 17. The set of numbers

$$\{a + b\sqrt{-1} : a, b \in \mathbb{Q}\}$$

forms an extension of \mathbb{Q} . The numbers 1 and $\sqrt{-1}$ form a basis, thus the degree of the extension is two.

Theorem 18. If K is an extension of \mathbb{Q} and the degree of the extension is finite, then the members of K are algebraic numbers.

Proof. Let the degree of K over \mathbb{Q} be n and let θ be in K . Then $1, \theta, \theta^2, \dots, \theta^n$ are $n+1$ vectors in K and must be dependent. This means there exist a_0, a_1, \dots, a_n in \mathbb{Q} not all of which are zero such that

$$a_0 + a_1\theta + a_2\theta^2 + \dots + a_n\theta^n = 0.$$

Thus θ is a root of

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

a polynomial in $Q[x]$, which implies θ is an algebraic number.

Because of this theorem finite extensions are often called algebraic extensions. The next theorem is quite useful later. It is proved here in a general setting.

Theorem 19. Let H , B and K be fields such that $H \subset B \subset K$, the degree of B over H is m , and the degree of K over B is n . Then the degree of K over H is mn .

Proof. Let b_1, b_2, \dots, b_m be a basis of the vector space B over H and k_1, k_2, \dots, k_n be a basis of the vector space K over B . The products $b_i k_j$ $i=1, 2, \dots, m; j=1, \dots, n$ form a set of mn vectors in K . The theorem will be proved if this set can be shown to be a basis of the vector space K over H . Consider

$$\sum_{j=1}^n \sum_{i=1}^m h_{ij} b_i k_j = 0 \quad h_{ij} \in H$$

Then

$$\sum_{i=1}^m h_{ij} b_i \quad j = 1, 2, \dots, n.$$

is in B . Since k_1, k_2, \dots, k_n is a basis of K over B

$$\sum_{j=1}^n \left(\sum_{i=1}^m h_{ij} b_i \right) k_j = 0$$

implies

$$\sum_{i=1}^m h_{ij} b_i = 0 \quad j = 1, 2, \dots, n.$$

This last equation implies $h_{ij} = 0$ for $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n$ since b_1, b_2, \dots, b_m is a basis for B over H . Thus the set of vectors $b_i k_j$ is independent. Let x be in K . There exist y_j in B for $j = 1, 2, \dots, n$ such that

$$x = \sum_{j=1}^n y_j k_j.$$

For each y_j in B there exist h_{ij} in H , $i = 1, 2, \dots, m$ such that

$$y_j = \sum_{i=1}^m h_{ij} b_i \quad j = 1, 2, \dots, n.$$

Thus

$$x = \sum_{j=1}^n \sum_{i=1}^m h_{ij} b_i k_j.$$

Hence the set of vectors $b_i k_j$ form a basis for K over H .

Let θ be an algebraic number with minimal polynomial $f(x)$. For any $g(x)$ in $\mathbb{Q}[x]$, $g(\theta)$ is the value of $g(x)$ at θ . From Theorem 16, $g(\theta)$ is an algebraic number. Let $\mathbb{Q}[\theta]$ be the set of values at θ for the polynomials in $\mathbb{Q}[x]$. The numbers in $\mathbb{Q}[\theta]$ can be thought of as polynomials in θ .

Theorem 20. Let θ be an algebraic number. Then $\mathbb{Q}[\theta]$ is a field.

Proof. $Q[\theta]$ is a subset of the complex numbers (including Q), thus all that is needed to complete the proof is closure and inverses under addition and multiplication. Let $g(\theta)$ and $h(\theta)$ be in $Q[\theta]$ where $g(x)$ and $h(x)$ are in $Q[x]$. Then $g(x) + h(x)$, $g(x)h(x)$ and $-g(x)$ are in $Q[x]$ so $g(\theta) + h(\theta)$, $g(\theta)h(\theta)$ and $-g(\theta)$ are in $Q[\theta]$. All that remains to be shown is that if $g(\theta) \neq 0$, then $g(\theta)$ has a multiplicative inverse in $Q[\theta]$. If $f(x)$ is the minimal polynomial of θ , it follows from Theorem 2 and the fact that $f(x)$ is irreducible that $f(x)$ and $g(x)$ have no common factor. Theorem 3 implies there exists $k(x)$ and $r(x)$ in $Q[x]$ such that $g(x)k(x) + h(x)f(x) = 1$. Thus $1 = g(\theta)k(\theta) + h(\theta)f(\theta) = g(\theta)k(\theta)$ since $f(\theta) = 0$. So $k(\theta)$ is the multiplicative inverse of $g(\theta)$.

Different polynomials in $Q[x]$ may have the same value at θ . The following theorem will pick out one polynomial for each number in $Q[\theta]$.

Theorem 21. Let θ be an algebraic number of degree n . Then

$$Q[\theta] = \{g(\theta) : g(x) \text{ is in } Q[x] \text{ and either the degree of } g(x) \text{ is less than } n \text{ or } g(x) \text{ is the zero polynomial}\} .$$

For each element of $Q[\theta]$ this polynomial is unique.

Proof. Let $f(x)$ be the minimal polynomial of θ . The degree of $f(x)$ is n , the degree of θ . Let $h(x)$ be in $Q[x]$. Then from Theorem 2 $h(x) = f(x)q(x) + r(x)$ where the degree of $r(x)$ is less than n or $r(x)$ is the zero polynomial. The value of $h(x)$ at θ is then $h(\theta) = f(\theta)q(\theta) + r(\theta) = r(\theta)$. This proves the first part of the theorem. If $h(x)$ and $k(x)$ have the same value at θ and both have degree less

than n , then $k(x) - h(x)$ has θ as a root. The degree of $h(x) - k(x)$ is less than n . This contradicts the degree of θ being n unless $h(x) = k(x)$.

Corollary 22. The numbers $1, \theta, \theta^2, \dots, \theta^{n-1}$ form a basis for $\mathbb{Q}[\theta]$ over \mathbb{Q} . The degree of θ is the degree of the extension $\mathbb{Q}[\theta]$ over \mathbb{Q} .

Proof. From the theorem each element of $\mathbb{Q}[\theta]$ is a unique linear combination of $1, \theta, \dots, \theta^{n-1}$, with coefficients in \mathbb{Q} , thus $1, \theta, \dots, \theta^{n-1}$ is a basis for $\mathbb{Q}[\theta]$ over \mathbb{Q} and the dimension of the vector space is n .

Example 23. Consider

$$f(x) = x^3 - \frac{3}{2}x^2 + \frac{15}{4}x + \frac{27}{8}.$$

If $f(x)$ is reducible one of the factors must be linear since $f(x)$ is cubic. The root of a linear factor must be rational. Thus to show that $f(x)$ is irreducible one must show $f(x)$ does not have a rational root. From elementary theory of equations if $f(x)$ has a rational root the numerator of that root divides 27 and the denominator divides 8. Testing all of the possibilities shows $f(x)$ has no rational roots thus $f(x)$ is irreducible. Let α be a root of $f(x)$, then $f(x)$ is the minimal polynomial of α and α is an algebraic number of degree 3. The numbers in $\mathbb{Q}[\alpha]$ can all be expressed in the form

$$a + b\alpha + c\alpha^2 \quad a, b, c \in \mathbb{Q}.$$

Corollary 22 and Theorem 18 imply all the elements of $\mathbb{Q}[\theta]$ are algebraic numbers. Thus $\mathbb{Q}[\theta]$ is referred to as an algebraic number field. Let ψ be in $\mathbb{Q}[\theta]$ and consider the set $1, \psi, \psi^2, \dots, \psi^k$. For some $k > 0$ this set is dependent while $1, \psi, \psi^2, \dots, \psi^{k-1}$ is independent over \mathbb{Q} . Just as in the proof of Theorem 18, the minimal polynomial of ψ must have degree k . This leads to the following result.

Theorem 24. Let ψ be in $\mathbb{Q}[\theta]$. If the degree of ψ equals the degree of θ then $\mathbb{Q}[\psi] = \mathbb{Q}[\theta]$.

Proof. Let the degree of θ be n . The numbers $1, \psi, \psi^2, \dots, \psi^{n-1}$ form a basis for $\mathbb{Q}[\theta]$ since they are n independent elements. They are also a basis for $\mathbb{Q}[\psi]$. Thus $\mathbb{Q}[\psi] = \mathbb{Q}[\theta]$.

Let ζ be the root of a polynomial with coefficients in $\mathbb{Q}[\theta]$. Then a new field $\mathbb{Q}[\theta][\zeta]$ can be formed in the same manner $\mathbb{Q}[\theta]$ was formed. It can be shown that there is an algebraic number ψ such that $\mathbb{Q}[\psi] = \mathbb{Q}[\theta][\zeta]$. A proof can be found in Clark [6]. This result implies the numbers in $\mathbb{Q}[\theta][\zeta]$ are also algebraic numbers.

Theorem 25. If θ is an algebraic number there is a rational integer $m \neq 0$ such that $m\theta$ is an algebraic integer, and $\mathbb{Q}[m\theta] = \mathbb{Q}[\theta]$.

Proof. Let the minimal polynomial of θ be

$$f(x) = x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \dots + \frac{a_0}{b_0} \quad a_j, b_j \in \mathbb{Z}$$

where $(a_j, b_j) = 1 \quad j = 0, 1, \dots, n-1$. Let m be the least common multiple of b_0, b_1, \dots, b_{n-1} . Define $g(x) = m^n f(x/m)$. Clearly $g(x)$ is monic and $g(x)$ is in $Z[x]$. If $g(x)$ is reducible then $f(x)$ is. Since $f(x)$ is irreducible $g(x)$ is irreducible. Finally $g(m\theta) = m^n f(\theta) = 0$ so $g(x)$ is the minimal polynomial of $m\theta$ and $m\theta$ is an algebraic integer of degree n in $Q[\theta]$. Thus Theorem 24 implies $Q[m\theta] = Q[\theta]$.

Thus an algebraic field extension $Q[\theta]$ may always be defined in terms of an algebraic integer.

Example 26. Consider the algebraic field extension $Q[\alpha]$ from Example 23. The least common multiple of the denominators of the minimal polynomial of α is 8. Let $\beta = 8\alpha$ then the minimal polynomial of β is

$$\begin{aligned} g(x) &= 512 \left(\frac{x^3}{512} - \frac{3x^2}{128} + \frac{15x}{32} + \frac{27}{8} \right) \\ &= x^3 - 12x^2 + 240x + 1728. \end{aligned}$$

Each of the roots of $g(x)$ is 8 times a root of the minimal polynomial of α .

When $Q[\theta]$ is regarded as a vector space over Q a linear transformation from $Q[\theta]$ to $Q[\theta]$ can be defined for each element of $Q[\theta]$ in the following way: Let Ψ be in $Q[\theta]$, define $F_\Psi: Q[\theta] \rightarrow Q[\theta]$ by $F_\Psi(\zeta) = \Psi\zeta$ for each ζ in $Q[\theta]$. Then, for ζ_1, ζ_2 in $Q[\theta]$ and a in Q ,

$$F_\Psi(\zeta_1 + \zeta_2) = (\zeta_1 + \zeta_2)\Psi = \zeta_1\Psi + \zeta_2\Psi = F_\Psi(\zeta_1) + F_\Psi(\zeta_2)$$

$$F_\Psi(a\zeta_1) = (a\zeta_1)\Psi = a(\zeta_1\Psi) = aF_\Psi(\zeta_1).$$

For each basis of $\mathbb{Q}[\theta]$ there is a matrix representation of F_ψ . Although changing the basis changes the matrix representation of F_ψ , there are some quantities which are independent of which matrix represents F_ψ . Three of these quantities are the trace, the determinant and the characteristic polynomial of the matrix. These facts are proved in Zelinsky [19].

Definition 27. Let ψ be in $\mathbb{Q}[\theta]$ and F_ψ the corresponding linear transformation. The trace, determinant and characteristic polynomial of a matrix representation of F_ψ are called the trace, norm and characteristic polynomial of ψ respectively. The norm will be denoted by $N(\psi)$ and the trace by $T(\psi)$.

It is important to note the linear transformation F_ψ depends on the algebraic number field from which ψ is chosen. The following examples and theorems demonstrate how the norm, trace and characteristic polynomial of an algebraic number are related to the field from which ψ is chosen.

Example 28. Let α be the algebraic number of Examples 23 and 24. Then

$$\alpha^3 = -\frac{27}{8} - \frac{15}{4}\alpha + \frac{3}{2}\alpha^2.$$

With $1, \alpha, \alpha^2$ as a basis for $\mathbb{Q}[\alpha]$ a matrix representation of F_α and F_β where $\beta = 8\alpha$ can be calculated in the following manner:

$$F_\alpha(1) = \alpha = 0 + \alpha + 0$$

$$F_\alpha(\alpha) = \alpha^2 = 0 + 0 + \alpha^2$$

$$F_\alpha(\alpha^2) = \alpha^3 = -\frac{27}{8} - \frac{15}{4}\alpha + \frac{3}{2}\alpha^2.$$

The values for F_β are simply 8 times the values for F_α . The matrix for F_α is

$$A = \begin{pmatrix} 0 & 0 & -\frac{27}{8} \\ 1 & 0 & -\frac{15}{4} \\ 0 & 1 & \frac{3}{2} \end{pmatrix}$$

and the matrix for F_β is $8A$. Thus $N(\alpha) = \det A = -\frac{27}{8}$, $T(\alpha) = \frac{3}{2}$, $N(\beta) = 8^3 \det A = -1728$ and $T(\beta) = 8T(\alpha) = 12$. Note the characteristic polynomial of β is

$$\begin{aligned} \det(xI - 8A) &= \begin{vmatrix} x & 0 & 27 \\ -8 & x & 30 \\ 0 & -8 & x-12 \end{vmatrix} \\ &= x^3 - 12x^2 + 240x + 1728 \end{aligned}$$

where I is the identity matrix. From Example 24 $\det(xI - 8A) = g(x)$ the minimal polynomial of β . The exact relationship between the characteristic polynomial and the minimal polynomial of an algebraic number will be shown in Theorem 31.

If θ , ψ and ζ are numbers from an algebraic number field then $F_{\theta\psi}(\zeta) = \zeta(\theta\psi) = (\zeta\theta)\psi = F_\psi(\zeta\theta) = F_\psi(F_\theta(\zeta))$ and

$$F_{\theta+\psi}(\zeta) = \zeta(\theta+\psi) = \zeta\theta + \zeta\psi = F_\theta(\zeta) + F_\psi(\zeta) = (F_\theta + F_\psi)(\zeta).$$

From the properties of matrices and their relationships to linear transformations the following theorem can be established.

Theorem 29. Let ψ and ζ be in $\mathbb{Q}[\theta]$, then $N(\psi\zeta) = N(\psi)N(\zeta)$ and $T(\psi + \zeta) = T(\psi) + T(\zeta)$.

The next two theorems use Theorem 19 to show how the degree of an algebraic number in $\mathbb{Q}[\theta]$ is related to the degree of θ and how the minimal polynomial of a number is related to its characteristic polynomial.

Theorem 30. Let ψ be in $\mathbb{Q}[\theta]$. Then the degree of ψ divides the degree of θ .

Proof. The set $1, \psi, \psi^2, \dots, \psi^{m-1}$ where m is the degree of ψ is a set of independent vectors in $\mathbb{Q}[\theta]$. Thus $\mathbb{Q}[\psi]$ is a subspace of $\mathbb{Q}[\theta]$. Now $\mathbb{Q} \subset \mathbb{Q}[\psi] \subset \mathbb{Q}[\theta]$ are fields satisfying the hypothesis of Theorem 19. The degree of $\mathbb{Q}[\psi]$ over \mathbb{Q} is m the degree of ψ and the degree of $\mathbb{Q}[\theta]$ over \mathbb{Q} is the degree of θ . Theorem 19 implies the degree of ψ divides the degree of θ .

Theorem 31. Let ψ be in $\mathbb{Q}[\theta]$ and the degrees of ψ and θ be m and n . Then the characteristic polynomial of ψ is the minimal polynomial of ψ raised to the power $k = n/m$.

Proof. The fields $\mathbb{Q} \subset \mathbb{Q}[\psi] \subset \mathbb{Q}[\theta]$ satisfy the hypotheses of Theorem 19. The numbers $1, \psi, \psi^2, \dots, \psi^{m-1}$ form a basis for $\mathbb{Q}[\psi]$ over \mathbb{Q} . Let $\zeta_1, \zeta_2, \dots, \zeta_k$ be a basis for $\mathbb{Q}[\theta]$ over $\mathbb{Q}[\psi]$. Note that the scalars for $\mathbb{Q}[\theta]$ over $\mathbb{Q}[\psi]$ are members of $\mathbb{Q}[\psi]$, not \mathbb{Q} . From Theorem 19 the numbers $\zeta_i \psi^j$ $i = 1, 2, \dots, k$ $j = 0, 1, 2, \dots, m-1$ form a basis for $\mathbb{Q}[\theta]$ over \mathbb{Q} . Let the minimal polynomial for ψ be

$$f(x) = x^m + b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \dots + b_0$$

then

$$\psi^m = -b_0 - b_1\psi - b_2\psi^2 - \dots - b_{m-1}\psi^{m-1}.$$

Now

$$F_\psi(\zeta_1) = 0 + \zeta_1\psi + 0 + \dots + 0$$

$$F_\psi(\zeta_1\psi) = 0 + 0 + \zeta_1\psi^2 + 0 + \dots + 0$$

...

$$F_\psi(\zeta_k\psi^{m-1}) = \zeta_k\psi^m = 0 + \dots + 0 - b_0\zeta_k - b_1\zeta_k\psi - \dots - b_{m-1}\zeta_k\psi^{m-1}$$

where each equation has enough zeros to make n terms. The matrix A of F_ψ contains k copies of the matrix

$$B = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & 0 & \dots & 0 & -b_2 \\ 0 & 0 & 1 & \dots & 0 & -b_3 \\ \dots & & & & & \\ 0 & 0 & 0 & \dots & 1 & -b_{m-1} \end{pmatrix}$$

down the main diagonal with zeros elsewhere. The characteristic polynomial of ψ is thus

$$\det(xI - A) = \left(\det(xI - B)\right)^k = \left(f(x)\right)^k.$$

Corollary 32. Let ψ be in $\mathbb{Q}[\theta]$ where the degree of θ is n and the characteristic polynomial of ψ is

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0.$$

Then $N(\Psi) = (-1)^n a_0$ and $T(\Psi) = -a_{n-1}$. Let $\Psi = \Psi_1, \Psi_2, \dots, \Psi_m$ be the roots of the minimal polynomial of Ψ , then $N(\Psi) = (\Psi_1 \Psi_2 \cdots \Psi_m)^k$ and $T(\Psi) = k(\Psi_1 + \Psi_2 + \dots + \Psi_m)$ where $k = n/m$.

Proof. The first conclusion follows from the rules for computing determinants. The second from the relations between the roots of a polynomial and its coefficients.

The next corollary will be a very useful tool.

Corollary 33. Let Ψ be in $\mathbb{Q}[\theta]$. If Ψ is an algebraic integer then the norm and trace of Ψ are rational integers.

Proof. If Ψ is an algebraic integer then $-a_{n-1}$ and $(-1)^n a_0$ in Corollary 32 are rational integers.

The results of Theorem 31 and the two corollaries were demonstrated in Example 28.

Let $\theta = \theta_1, \theta_2, \dots, \theta_n$ be all the roots of the minimal polynomial of θ . Then each root defines an algebraic number field $\mathbb{Q}[\theta_j]$ $j = 1, 2, \dots, n$. These fields are not necessarily distinct. Let Ψ be in $\mathbb{Q}[\theta]$ and let $g(x)$ be the unique polynomial of Theorem 21 that corresponds to Ψ . Then there is a correspondence between elements of $\mathbb{Q}[\theta]$ and $\mathbb{Q}[\theta_j]$ given by $\Psi = g(\theta) \rightarrow \Psi_j = g(\theta_j)$. This correspondence clearly preserves arithmetic operations. That is, if $\Psi + \xi = \zeta$ then $\Psi_j + \xi_j = \zeta_j$ and if $\Psi\xi = \lambda$ then $\Psi_j \xi_j = \lambda_j$. The fields $\mathbb{Q}[\theta_j]$ $j = 1, 2, \dots, n$ are called the conjugate fields and the numbers $\Psi_1, \Psi_2, \dots, \Psi_n$ are called the conjugates of Ψ with respect to those fields.

Theorem 34. Let ψ be in $Q[\theta]$. Then the conjugates of ψ are the roots of the minimal polynomial of ψ .

Proof. Let $\psi_j = g(\theta_j)$ and let $f(x)$ and $h(x)$ be the minimal polynomials of θ and ψ respectively. Now $h(\psi) = h(g(\theta)) = 0$. Thus $f(x)$ divides $h(g(x))$. Therefore $h(\psi_j) = h(g(\theta_j)) = 0$.

It follows from Theorems 31 and 34 that the conjugates of ψ are the roots of the minimal polynomial of ψ repeated enough times to make n numbers where n is the number of conjugate fields.

Example 35. Let $f(x) = x^4 - 3$ and $\sigma = \sqrt[4]{3}$. The conjugates of σ are $\sigma_1 = \sqrt[4]{3}$, $\sigma_2 = -\sqrt[4]{3}$, $\sigma_3 = \sqrt{-1} \sqrt[4]{3}$ and $\sigma_4 = -\sqrt{-1} \sqrt[4]{3}$. A basis for $Q[\sigma]$ is $1, \sigma, \sigma^2, \sigma^3$ or $1, \sqrt[4]{3}, \sqrt{3}, \sqrt[4]{27}$. Let $\tau_i = 1 + \sigma_i^2$ or $\tau_1 = 1 + \sqrt{3}$, $\tau_2 = 1 - \sqrt{3}$, $\tau_3 = 1 + \sqrt{3}$, $\tau_4 = 1 - \sqrt{3}$. The minimal polynomial of τ is clearly $x^2 - 2x - 2$. As another example of Theorem 31 a matrix representation for F_τ is determined. Note $\sigma^4 = 3$.

$$F_\tau(1) = \tau = 1 + 0 + \sigma^2 + 0$$

$$F_\tau(\sigma) = \tau\sigma = 0 + 1 + 0 + \sigma^3$$

$$F_\tau(\sigma^2) = \tau\sigma^2 = 3 + 0 + 1\sigma^2 + 0$$

$$F_\tau(\sigma^3) = \tau\sigma^3 = 0 + 3\sigma + 0 + 1\sigma^3$$

The basis used in Theorem 31 is not the basis used here. The basis used in the proof of the theorem demonstrated the desired result, but, from a computational point of view, it is difficult to discover and use that particular basis. The matrix of F_τ is

$$A = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 3 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} .$$

The characteristic polynomial of τ is $\det(xI - A)$

$$\begin{vmatrix} x-1 & 0 & -3 & 0 \\ 0 & x-1 & 0 & -3 \\ -1 & 0 & x-1 & 0 \\ 0 & -1 & 0 & x-1 \end{vmatrix} = (x^2 - 2x - 2)^2 ,$$

Also $T(\tau) = 4 = 2(\tau_1 + \tau_2)$ and $N(\tau) = 4 = (\tau_1\tau_2)^2$ where τ_1 and τ_2 are the distinct roots of the minimal polynomial of τ .

There is one concept left to be discussed in this chapter.

Definition 36. Let $Q[\theta]$ be an algebraic number field of degree n over Q . Let $\psi_1, \psi_2, \dots, \psi_n$ be in $Q[\theta]$ and let $\psi_{i1}, \psi_{i2}, \dots, \psi_{in}$ be the conjugates of ψ_i . The number

$$\Delta(\psi_1, \psi_2, \dots, \psi_n) = \begin{vmatrix} \psi_{11} & \psi_{21} & \psi_{31} & \cdots & \psi_{n1} \\ \psi_{12} & \psi_{22} & \psi_{32} & \cdots & \psi_{n2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \psi_{1n} & \psi_{2n} & \psi_{3n} & \cdots & \psi_{nn} \end{vmatrix}^2$$

is called the discriminant of $\psi_1, \psi_2, \dots, \psi_n$.

The discriminant is a symmetric function in each of the conjugates of ψ_i . Theorem 14 implies the discriminant is a rational number. If

all the ψ_i are algebraic integers then the discriminant is a rational integer. The discriminant of $1, \theta, \theta^2, \dots, \theta^{n-1}$ will be used frequently in Chapter III.

Example 37. Consider the algebraic number field $\mathbb{Q}[\alpha]$ of Example 23 where α is a root of $x^3 - \frac{3}{2}x^2 + \frac{15}{4}x + \frac{27}{8}$.

$$\Delta(1, \alpha, \alpha^2) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{vmatrix}^2$$

where $\alpha_1, \alpha_2, \alpha_3$ are the conjugates of α . From Example 15

$$\Delta(1, \alpha, \alpha^2) = b^2 a^2 + 18abc - 27c^2 - 4b^3 - 4ca^3 \quad \text{where}$$

$$a = \alpha_1 + \alpha_2 + \alpha_3 = T(\alpha) = \frac{3}{2}$$

$$b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \frac{15}{4}$$

$$c = \alpha_1\alpha_2\alpha_3 = N(\alpha) = -\frac{27}{8}$$

Thus $\Delta(1, \alpha, \alpha^2) = -783$. The discriminant of $1, \beta, \beta^2$ where $\beta = 8\alpha$

can be computed in the same manner using results of Example 26

$\Delta(1, \beta, \beta^2) = -205258752$. Note that $\Delta(1, \alpha, \alpha^2)$ is in \mathbb{Z} but not all of the algebraic numbers $1, \alpha, \alpha^2$ are algebraic integers.

Theorem 38. Let $\psi_1, \psi_2, \dots, \psi_n$ be in $\mathbb{Q}[\theta]$ where the degree of θ is n . If

$$\xi_i = \sum_{j=1}^n a_{ij} \psi_j \quad a_{ij} \in \mathbb{Q}$$

$i=1,2,\dots,n$ then $\Delta(\xi_1, \xi_2, \dots, \xi_n) = |A|^2 \Delta(\psi_1, \psi_2, \dots, \psi_n)$. Where $|A|$ is $\det(a_{ij})$.

Proof. Let ψ_{ij} be the j^{th} conjugates of ψ_i and ξ_i respectively. Let B and C be the matrices with entries ψ_{ij} and ξ_{ij} respectively. Then $C = AB$ and

$$\Delta(\xi_1, \xi_2, \dots, \xi_n) = |C|^2 = |AB|^2 = |A|^2 |B|^2 = |A|^2 \Delta(\psi_1, \psi_2, \dots, \psi_n)$$

Example 39. The matrix relating $1, \alpha, \alpha^2$ and $1, \beta, \beta^2$ in Example 37 is

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 64 \end{pmatrix}.$$

$$|A|^2 = (512)^2 = 272144 \text{ and}$$

$$\Delta(1, \beta, \beta^2) = -205258752 = (272144)(-783) = (512)^2 \Delta(1, \alpha, \alpha^2).$$

Theorem 40. The discriminant of any basis of $Q[\theta]$ is never zero.

Proof. Given any two bases of $Q[\theta]$ there exists a matrix A relating them as in Theorem 38. Furthermore A is nonsingular. Thus if one basis with a nonzero discriminant can be found, Theorem 38 will imply that the discriminant of every other basis is not zero. Consider the basis $1, \theta, \theta^2, \dots, \theta^{n-1}$. Let θ_j be the j^{th} conjugate of θ then

$$\Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \begin{vmatrix} 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \dots & \theta_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1} \end{vmatrix}^2$$

This is the square of the Vandermonde determinant thus

$$\Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = (\theta_1 - \theta_2)^2 (\theta_1 - \theta_3)^2 \dots (\theta_{n-1} - \theta_n)^2.$$

Since all the θ_j are distinct the discriminant is not zero.

Note also that all the discriminants of bases of $\mathbb{Q}[\theta]$ have the same sign. If all the conjugate fields of $\mathbb{Q}[\theta]$ are real fields then all the θ_j are real and the discriminant is the square of a real number. Thus the discriminant of a basis must be positive if all the conjugate fields are real.

Theorem 41. Let $\mathbb{Q}[\theta]$ be an algebraic number field and $f(x)$ the minimal polynomial of θ . Then

$$\Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(f'(\theta)).$$

Where n is the degree of $f(x)$ and $f'(x)$ is the derivative of $f(x)$.

Proof. Let θ_j be the j^{th} conjugate of θ , then

$$f(x) = \prod_{j=1}^n (x - \theta_j)$$

and

$$f'(x) = \sum_{i=1}^n \left(\prod_{j \neq i} (x - \theta_j) \right).$$

Now from Corollary 32

$$\begin{aligned} N(f'(\theta)) &= \prod_{k=1}^n f'(\theta_k) \\ &= \prod_{k=1}^n \left(\sum_{i=1}^n \left\{ \prod_{j \neq i} (\theta_k - \theta_j) \right\} \right) \\ &= \prod_{k=1}^n \left(\prod_{j \neq k} (\theta_k - \theta_j) \right) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{k < j} (\theta_k - \theta_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}). \end{aligned}$$

In the next to the last step half of the $n(n-1)$ terms are reversed in order.

Example 42. Let p be a prime number. It can be shown that

$$f(x) = x^{p-1} + x^{p-2} + x^{p-3} + \dots + x + 1$$

is irreducible [6]. This polynomial is called the p^{th} cyclotomic polynomial. Let ω be a root of $f(x)$ then

$$\Delta(1, \omega, \omega^2, \dots, \omega^{p-2}) = (-1)^{\frac{p-1}{2}} N(f'(\omega))$$

The norm of $f'(\omega)$ is computed in the same manner as in Example 28.

Let F be the linear transformation of $\mathbb{Q}[\omega]$ determined by $f'(\omega)$.

Note that

$$f'(\omega) = 1 + 2\omega + 3\omega^2 + \dots + (p-1)\omega^{p-2}$$

and

$$\omega^{p-1} = -1 - \omega - \omega^2 - \dots - \omega^{p-2}.$$

Now

$$F(1) = f'(\omega) = 1 + 2\omega + 3\omega^2 + \dots + (p-1)\omega^{p-2}$$

$$F(\omega) = f'(\omega)\omega = 1 - p + (2-p)\omega + (3-p)\omega^2 + \dots - \omega^{p-2}$$

$$F(\omega^2) = f'(\omega)\omega^2 = 1 + (2-p)\omega + (3-p)\omega^2 + \dots - \omega^{p-2}$$

...

$$F(\omega^{p-2}) = f'(\omega)\omega^{p-2} = 1 + \omega + \omega^2 + \dots - \omega^{p-2}.$$

So the matrix of F is

$$A = \begin{pmatrix} 1 & 2 & 3 & \dots & p-1 \\ 1-p & 2-p & 3-p & \dots & -1 \\ 1 & 2-p & 3-p & \dots & -1 \\ 1 & 2 & 3-p & \dots & -1 \\ \dots & & & & \\ 1 & 2 & 3 & \dots & -1 \end{pmatrix}$$

The determinant of A is the norm of $f'(\omega)$. It can be shown that the determinant of A is p^{p-2} thus

$$\Delta(1, \omega, \omega^2, \dots, \omega^{p-2}) = (-1)^{\frac{p-1}{2}} N(f'(\omega)) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

CHAPTER III

RINGS OF ALGEBRAIC INTEGERS

The main theme of this chapter is to develop some theorems regarding the structure of the set of algebraic integers contained in some algebraic number field. It follows from Theorem 16 that the set of all algebraic integers in a given algebraic number field forms a ring, in fact it forms an integral domain. An algebraic number field is quadratic or cubic if the degree of the extension is two or three respectively. Many of the results in this chapter will pertain to quadratic and cubic extensions, although Theorem 47, the main theorem of the chapter, relates to extensions of arbitrary degree. More exhaustive results on quadratic extensions can be found in Reid [14], and on cubic extensions in Delone and Faddeev [7].

Example 43. Consider $\mathbb{Q}[\sqrt{6}]$ where $x^2 - 6$ is the minimal polynomial of $\sqrt{6}$. The numbers in $\mathbb{Q}[\sqrt{6}]$ are of the form $a + b\sqrt{6}$ a, b in \mathbb{Q} . Suppose $\theta = a + b\sqrt{6}$ is an algebraic integer. If $b = 0$ then $\theta = a$ is in \mathbb{Z} , or θ is a rational integer. If $b \neq 0$ then θ has degree two and the characteristic polynomial of θ is the minimal polynomial of θ . Computing F_θ

$$F_\theta(1) = \theta = a + b\sqrt{6}$$

$$F_\theta(6) = \sqrt{6}\theta = 6b + a\sqrt{6} .$$

Thus the minimal polynomial of θ is

$$\begin{vmatrix} x-a & -b \\ -6b & x-a \end{vmatrix} = x^2 - 2ax + a^2 - 6b^2.$$

For θ to be an algebraic integer $2a$ and $a^2 - 6b^2$ must be in \mathbb{Z} .

Clearly if a is in \mathbb{Z} then b must be in \mathbb{Z} . If $a = \frac{r}{2}$ for an odd rational integer r then

$$a^2 - 6b^2 = \frac{r^2}{4} - 6b^2 = \frac{r^2 - 24b^2}{4}$$

is in \mathbb{Z} . This implies

$$r^2 - 24b^2 \equiv 0 \pmod{4}$$

or $r^2 \equiv 0 \pmod{4}$. Since r is odd this is impossible. Thus the algebraic integers in $\mathbb{Q}[\sqrt{6}]$ are all numbers of the form $a + b\sqrt{6}$ with a and b in \mathbb{Z} .

If $\mathbb{Q}[\theta]$ is a quadratic extension of \mathbb{Q} then θ is the root of a quadratic equation. Thus there are a, b, c and d in \mathbb{Z} such that $\theta = \frac{a+b\sqrt{d}}{c}$ where $b \neq 0, c \neq 0$ and d is square free. The numbers 1 and θ form a basis for $\mathbb{Q}[\theta]$, thus $\sqrt{d} = -\frac{a}{b}1 + \frac{c}{b}\theta \in \mathbb{Q}[\theta]$. Since the degree of \sqrt{d} is two, Theorem 24 implies $\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{d}]$. Thus all quadratic extensions can be expressed in the form $\mathbb{Q}[\sqrt{d}]$ where d is a square free rational integer.

Theorem 44. The algebraic integers in $\mathbb{Q}[\sqrt{d}]$ where d is a square free rational integer are of the form

$$a + b\sqrt{d} \quad \text{if } d \equiv 2, 3 \pmod{4}$$

or

$$a + b \left(\frac{1 + \sqrt{d}}{2} \right) \quad \text{if } d \equiv 1 \pmod{4}$$

where $a, b \in \mathbb{Z}$.

Proof. Let $\theta = r + s\sqrt{d}$ be in $\mathbb{Q}[\sqrt{d}]$. As in Example 43. The minimal polynomial of θ ($s \neq 0$) is

$$x^2 - 2rx + r^2 + s^2d$$

If θ is an algebraic integer $2r$ and $r^2 + s^2d$ are in \mathbb{Z} . If $d \equiv 2$ or $3 \pmod{4}$ then r and s are in \mathbb{Z} by the same reasoning as in Example 43. If $d \equiv 1 \pmod{4}$ then $2r$ and $2s$ are both odd or both even rational integers. Thus $\theta = r + s\sqrt{d} = (r - s) + (2s) \frac{1 + \sqrt{d}}{2}$ where $r - s$ and $2s$ are in \mathbb{Z} .

This theorem states that the ring of integers in a quadratic extension forms a free \mathbb{Z} module with two generators. The next theorems generalize this result to extensions of arbitrary degree.

Theorem 45. Let θ be an algebraic integer of degree n and let $\Delta = \Delta(1, \theta, \dots, \theta^{n-1})$. Then all the algebraic integers in $\mathbb{Q}[\theta]$ can be expressed in the form

$$\frac{1}{\Delta} \sum_{j=0}^{n-1} a_j \theta^j \quad a_j \in \mathbb{Z}.$$

Proof. Let θ_i be the i th conjugate of θ . Consider an algebraic integer ψ in $\mathbb{Q}[\psi]$ then

$$\psi = \sum_{j=0}^{n-1} r_j \theta^j \quad r_j \in \mathbb{Q}.$$

Now the object is to show the r_j can be written as a rational number with denominator Δ . This is done by setting up a system of n equations for r_0, r_1, \dots, r_{n-1} with coefficients in Z . From Corollary 33 the trace of an algebraic integer is in Z . Calculating the traces of $\psi \theta^j$ from Corollary 32 gives

$$T(\psi) = \sum_{i=1}^n \left(\sum_{j=0}^{n-1} r_j \theta_i^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=1}^n \theta_i^j \right) r_j$$

$$T(\psi\theta) = \sum_{i=1}^n \left(\sum_{j=0}^{n-1} r_j \theta_i^{j+1} \right) = \sum_{j=0}^{n-1} \left(\sum_{i=1}^n \theta_i^{j+1} \right) r_j$$

...

$$T(\psi\theta^{n-1}) = \sum_{i=1}^n \left(\sum_{j=0}^{n-1} r_j \theta_i^{j+n-1} \right) = \sum_{j=0}^{n-1} \left(\sum_{i=1}^n \theta_i^{j+n-1} \right) r_j.$$

The coefficients of the r_j are symmetric functions in $\theta_1, \theta_2, \dots, \theta_n$. Theorem 14 states that these coefficients can be written as polynomials in the elementary symmetric functions of $\theta_1, \theta_2, \dots, \theta_n$. Since θ is an algebraic integer, the elementary symmetric function of $\theta_1, \theta_2, \dots, \theta_n$ are in Z . Thus the coefficients of r_j are rational integers. The r_j 's can be expressed as the ratio of determinants according to Cramer's rule if the determinant of coefficients is not zero. The determinant of the coefficients is

$$\begin{array}{cccccc}
 n & \sum_{i=1}^n \theta_i & \sum_{i=1}^n \theta_i^2 & \dots & \sum_{i=1}^n \theta_i^{n-1} \\
 \sum_{i=1}^n \theta_i & \sum_{i=1}^n \theta_i^2 & \sum_{i=1}^n \theta_i^3 & \dots & \sum_{i=1}^n \theta_i^n \\
 \dots & & & & \\
 \sum_{i=1}^n \theta_i^{n-1} & \sum_{i=1}^n \theta_i^n & \sum_{i=1}^n \theta_i^{n+1} & \dots & \sum_{i=1}^n \theta_i^{2n-2}
 \end{array}$$

$$= \begin{array}{c}
 \left| \begin{array}{ccccc}
 1 & 1 & 1 & \dots & 1 \\
 \theta_1 & \theta_2 & \theta_3 & \dots & \theta_n \\
 \theta_1^2 & \theta_2^2 & \theta_3^2 & \dots & \theta_n^2 \\
 \dots & & & & \\
 \theta_1^{n-1} & \theta_2^{n-1} & \theta_3^{n-1} & \dots & \theta_n^{n-1}
 \end{array} \right| \left| \begin{array}{ccccc}
 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\
 1 & \theta_2 & \theta_2^2 & \dots & \theta_2^{n-1} \\
 1 & \theta_3 & \theta_3^2 & \dots & \theta_3^{n-1} \\
 \dots & & & & \\
 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1}
 \end{array} \right|
 \end{array}$$

$$= \left| \begin{array}{ccccc}
 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\
 1 & \theta_2 & \theta_2^2 & \dots & \theta_2^{n-1} \\
 1 & \theta_3 & \theta_3^2 & \dots & \theta_3^{n-1} \\
 \dots & & & & \\
 1 & \theta_n & \theta_n^2 & \dots & \theta_n^{n-1}
 \end{array} \right|^2 = \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}) = \Delta.$$

Theorem 40 implies $\Delta \neq 0$. Thus from Cramer's rule the r_j can be expressed as the ratio of determinants. The denominator determinant is Δ . The numerator determinant has only numbers from Z as entries thus the value of that determinant is in Z . Thus r_j has the desired form.

Note that the theorem did not say that numbers of the form

$$\frac{1}{\Delta} \sum_{j=0}^{n-1} a_j \theta^j \quad a_j \in Z$$

are always algebraic integers.

Example 46. From Example 37 with $\Delta = -205258752$ let $a_0 = 1$ and $a_1 = a_2 = \dots = a_{n-1} = 0$. Then $\frac{1}{\Delta}$ is a number of the form in Theorem 45 that is not an algebraic integer.

Theorem 47. Let $Q[\theta]$ be an algebraic number field where θ has degree n . There exist algebraic integers $\rho_1, \rho_2, \dots, \rho_n$ in $Q[\theta]$ such that any algebraic integer ψ in $Q[\theta]$ can be expressed uniquely in the form

$$\psi = \sum_{j=1}^n z_j \rho_j \quad z_m \in Z.$$

Proof. Theorem 25 implies that θ can be assumed to be an algebraic integer without any loss of generality. Let $\Delta = \Delta(1, \theta, \theta^2, \dots, \theta^{n-1})$ as in Theorem 45. Consider algebraic integers in $Q[\theta]$ of the form

$$\begin{aligned}
\rho_1 &= \frac{a_{10}}{\Delta} \\
\rho_2 &= \frac{a_{20} + a_{21}\theta}{\Delta} \\
&\dots \\
\rho_n &= \frac{a_{n0} + a_{n1}\theta + \dots + a_{n,n-1}\theta^{n-1}}{\Delta}
\end{aligned} \tag{48}$$

where a_{ij} is in Z . Since $\theta^j = \frac{\Delta}{\Delta} \theta^j$ there is an algebraic integer ρ_j for each j in Equation 48 with $a_{j,j-1} \neq 0$. Choose ρ_j from the algebraic integers of the form in Equation 48 such that $|a_{j,j-1}|$ is the smallest positive rational integer, $j = 1, 2, \dots, n$. The theorem will be proved when it is shown that $\rho_1, \rho_2, \dots, \rho_n$ satisfy the conclusion of the theorem. Let ψ be an algebraic integer in $Q[\theta]$ then Theorem 45 implies

$$\psi = \frac{b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1}}{\Delta} \quad b_j \in Z.$$

From the division algorithm $b_{n-1} = z_n a_{n,n-1} + r_{n-1}$ where $0 \leq r_{n-1} < |a_{n,n-1}|$. Now $\psi - z_n \rho_n$ is an algebraic integer and

$$\psi - z_n \rho_n = \frac{1}{\Delta} \sum_{j=0}^{n-1} (b_j - z_n a_{nj}) \theta^j.$$

Thus the coefficient of θ^{n-1} is $\frac{r_{n-1}}{\Delta}$, Since $r_{n-1} < |a_{n,n-1}|$ it must be that $r_{n-1} = 0$ because ρ_n was the algebraic integer of this form with the coefficient of θ^{n-1} least in numerical value. This process is now repeated, that is $(b_{n-2} - z_n a_{n,n-2}) = z_{n-1} a_{n-1,n-2} + r_{n-2}$

where $0 \leq r_{n-2} < |a_{n-1, n-2}|$. Examination of the algebraic integer $\psi - z_n \rho_n - z_{n-1} \rho_{n-1}$ shows $r_{n-2} = 0$. This process is repeated until $\psi - z_n \rho_n - z_{n-1} \rho_{n-1} - \dots - z_1 \rho_1 = 0$ or

$$\psi = \sum_{j=1}^n z_j \rho_j \quad z_j \in Z.$$

Thus all the algebraic integers in $Q[\theta]$ can be expressed in the desired form. In particular $1, \theta, \theta^2, \dots, \theta^{n-1}$ can be, thus $\rho_1, \rho_2, \dots, \rho_n$ must be a basis for $Q[\theta]$. This implies that the z_j are unique.

Definition 49. Let $Q[\theta]$ be an algebraic number field and have degree n . The algebraic integers $\rho_1, \rho_2, \dots, \rho_n$ are called an integral basis for $Q[\theta]$ if they are a basis for $Q[\theta]$ and every algebraic integer ψ in $Q[\theta]$ can be expressed in the form

$$\psi = \sum_{i=1}^n z_i \rho_i \quad z_i \in Z.$$

Every algebraic number field $Q[\theta]$ has an integral basis (Theorem 47). For a quadratic extension Theorem 44 completely describes the situation. In general finding an integral basis for a given extension is a difficult task. However it can be shown that the discriminant of an integral basis is minimal.

Theorem 50. Let $\psi_1, \psi_2, \dots, \psi_n$ be algebraic integers that form a basis for $Q[\theta]$, and let $\rho_1, \rho_2, \dots, \rho_n$ be an integral basis for $Q[\theta]$. Then $|\Delta(\psi_1, \psi_2, \dots, \psi_n)| \geq |\Delta(\rho_1, \rho_2, \dots, \rho_n)|$. Equality occurs if and only if $\psi_1, \psi_2, \dots, \psi_n$ is an integral basis for $Q[\theta]$.

Proof. Since $\rho_1, \rho_2, \dots, \rho_n$ is an integral basis there exists z_{ij} in Z such that

$$\psi_i = \sum_{j=1}^n z_{ij} \rho_j \quad i = 1, 2, \dots, n.$$

Let A be the matrix with z_{ij} as entries. From Theorem 38

$$\Delta(\psi_1, \psi_2, \dots, \psi_n) = (\det A)^2 \Delta(\rho_1, \rho_2, \dots, \rho_n)$$

Since the z_{ij} are in Z $\det A$ is in Z . Theorem 40 implies $\det A \neq 0$. Thus $(\det A)^2 \geq 1$ which implies

$$|\Delta(\psi_1, \psi_2, \dots, \psi_n)| \geq |\Delta(\rho_1, \rho_2, \dots, \rho_n)|.$$

The numbers $\psi_1, \psi_2, \dots, \psi_n$ are an integral basis if and only if A^{-1} has entries in Z . This is true if and only if $\det A$ and $\det A^{-1}$ are both in Z . Since $\det A^{-1} = (\det A)^{-1}$ it follows that $|\det A| = 1$ and

$$\Delta(\psi_1, \psi_2, \dots, \psi_n) = \Delta(\rho_1, \rho_2, \dots, \rho_n).$$

The number $\Delta(\rho_1, \rho_2, \dots, \rho_n)$ is called the discriminant of $\mathbb{Q}[\theta]$.

Example 51. Consider $\mathbb{Q}[\sqrt{d}]$. If $d \equiv 2$ or $3 \pmod{4}$ then $1, \sqrt{d}$ form an integral basis and the discriminant of $\mathbb{Q}[\sqrt{d}]$ is

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

If $d \equiv 1 \pmod{4}$ then $1, \frac{1+\sqrt{d}}{2}$ forms an integral basis and the discriminant is

$$\Delta\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

Thus the discriminant of $\mathbb{Q}[\sqrt{d}]$ is $4d$ when $d \equiv 2, 3 \pmod{4}$, or is d if $d \equiv 1 \pmod{4}$.

Let ξ be an algebraic integer in $\mathbb{Q}[\theta]$ with representation according to Theorem 45

$$\xi = \frac{1}{\Delta} \sum_{j=0}^{s-1} a_j \theta^j \quad a_j \in \mathbb{Z}$$

where $s-1 < n-1$, That is assume $a_s = a_{s+1} = \dots = a_{n-1} = 0$.

Then the corresponding representation of ξ according to Theorem 47 is

$$\xi = \sum_{j=1}^s z_j \rho_j \quad z_j \in \mathbb{Z}.$$

In other words $z_{s+1} = z_{s+2} = \dots = z_n = 0$. This follows from the way the z_j were calculated in the proof of Theorem 47. This fact will be used to discover many relations among the a_{ij} 's of Equation 48 when $\rho_1, \rho_2, \dots, \rho_n$ is an integral basis. Note that ρ_1 in Equation 48 is in \mathbb{Q} thus if ρ_1 is to be an algebraic integer $\Delta | a_{10}$. Thus the smallest nonzero $|a_{10}|$ is Δ so ρ_1 can always be chosen as 1. Now

$$\theta^j = \frac{\Delta}{\Delta} \theta^j = \sum_{i=1}^{j+1} z_i \rho_i \quad j = 1, 2, \dots, n-1.$$

Calculating z_{j+1} as in the proof of Theorem 47 gives $\Delta = z_{j+1} a_{j+1,j}$.

Thus $a_{j+1,j} | \Delta$ for $j=1,2,\dots,n-1$. Let $\Delta_j = \frac{\Delta}{a_{j,j-1}}$. The number $\theta \rho_j$ is an algebraic integer for $j=1,\dots,n$. Now

$$\theta \rho_j = \frac{a_{j0} \theta + a_{j1} \theta^2 + \dots + a_{j,j-1} \theta^j}{\Delta}$$

and

$$\theta \rho_j = \sum_{i=1}^{j+1} z_i \rho_i.$$

Thus $a_{j,j-1} = z_{j+1} a_{j+1,j}$ or $a_{j+1,j} | a_{j,j-1}$ for $j=1,2,\dots,n-1$.

Since $\Delta = \Delta_j a_{j,j-1} = \Delta_{j+1} a_{j+1,j}$ the fact that $a_{j+1,j} | a_{j,j-1}$ implies $\Delta_j | \Delta_{j+1}$. Induction on j will be used to show that for $1 \leq j \leq n$ $a_{j,j-1} | a_{jk}$ $k=0,1,2,\dots,j-1$. For $j=1$ $a_{10} | a_{10}$. Suppose the statement is true for $j=1,2,\dots,s$. Now

$$\theta \rho_s = \sum_{i=1}^{s+1} z_i \rho_i$$

or

$$z_{s+1} \rho_{s+1} - \theta \rho_s = \sum_{i=1}^s z_i \rho_i.$$

Then since $z_{s+1} = \frac{a_{s,s-1}}{a_{s+1,s}}$

$$\frac{\Delta}{a_{s+1,s}} \rho_{s+1} = \frac{\Delta \theta}{a_{s,s-1}} \rho_s + \sum_{i=1}^s z_i \frac{\Delta}{a_{s,s-1}} \rho_i.$$

Using Equation 48 to write this equation as a polynomial in θ , the left side is

$$\frac{a_{s+1,0}}{a_{s+1,s}} + \frac{a_{s+1,1}}{a_{s+1,s}} \theta + \frac{a_{s+1,2}}{a_{s+1,s}} \theta^2 + \dots + \frac{a_{s+1,s}}{a_{s+1,s}} \theta^s,$$

while the right hand side is

$$\begin{aligned} & \frac{a_{s,0}}{a_{s,s-1}} \theta + \frac{a_{s,1}}{a_{s,s-1}} \theta^2 + \dots + \frac{a_{s,s-1}}{a_{s,s-1}} \theta^s \\ & + \sum_{i=1}^s \frac{z_i a_{i,i-1}}{a_{s,s-1}} \left(\frac{a_{i,0}}{a_{i,i-1}} + \frac{a_{i,1}}{a_{i,i-1}} \theta + \dots + \frac{a_{i,i-1}}{a_{i,i-1}} \theta^{i-1} \right). \end{aligned}$$

The coefficients of θ^i on the left side must equal the right side since $1, \theta, \theta^2, \dots, \theta^{n-1}$ is a basis. All the coefficients on the right hand side are rational integers by the induction hypothesis. Thus the coefficients on the left hand side are also in Z , and the induction is completed. Summing up, $Q[\theta]$ has an integral basis of the form

$$\rho_j = \frac{h_j(\theta)}{\Delta_j} \quad j = 1, 2, \dots, n \quad (51)$$

where $h_j(x)$ is a monic polynomial in $Z[x]$ of degree $j-1$. Also $\Delta_j | \Delta_{j+1}$ and

$$\Delta(\rho_1, \rho_2, \dots, \rho_n) \prod_{j=1}^n \Delta_j^2 = \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}).$$

Since $|a_{j,j-1}|$ is picked to be smallest, then $|\Delta_j|$ must be picked largest. Finally $\rho_1 = 1$.

Example 52. Consider $Q[\omega]$ where ω is a root of the p th cyclotomic polynomial as in Example 42. Now

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1).$$

Since the second factor on the right hand side is the minimal polynomial of ω it follows that $\omega^p = 1$. Thus $(\omega^j)^p = \omega^{jp} = (\omega^p)^j = 1$ so ω^j is a root of $x^p - 1$. The only root of $x - 1$ is 1 thus $\omega, \omega^2, \omega^3, \dots, \omega^{p-1}$ must be the $p - 1$ roots of the minimal polynomial of ω . No two of those powers of ω are equal because of the properties of the minimal polynomial. Thus $N(\omega^j) = -1$ and $T(\omega^j) = -1$ for $j = 1, 2, \dots, p-1$. Consider the number $\lambda = 1 - \omega$. The matrix of F_λ for the basis $1, \omega, \dots, \omega^{p-2}$ is found from

$$F_\lambda(1) = 1 - \omega$$

$$F_\lambda(\omega) = 0 + \omega - \omega^2$$

...

$$F_\lambda(\omega^{p-3}) = 0 + 0 + \dots + 0 + \omega^{p-3} - \omega^{p-2}$$

$$F_\lambda(\omega^{p-2}) = 1 + \omega + \omega^2 + \dots + \omega^{p-3} + 2\omega^{p-2}.$$

Thus $N(\lambda) = p$ and $T(\lambda) = p$. The next two lemmas will be used to prove that $1, \omega, \omega^2, \dots, \omega^{p-2}$ form an integral basis for $\mathbb{Q}[\omega]$.

Lemma. Let ψ be an algebraic integer in $\mathbb{Q}[\omega]$. If $\psi\lambda$ is in \mathbb{Z} then $p \mid \psi\lambda$.

Proof. The matrix of $F_{\psi\lambda}$ with respect to the basis $1, \omega, \omega^2, \dots, \omega^{p-2}$ is a diagonal matrix since $F_{\psi\lambda}(\omega^j) = \psi\lambda\omega^j$, $j = 0, 1, \dots, p-2$ and $\psi\lambda$ is in \mathbb{Z} . Thus

$$N(\psi\lambda) = (\psi\lambda)^{p-1} = N(\psi)N(\lambda) = N(\psi)p.$$

Since $N(\psi)$ is in \mathbb{Z} it follows that $p \mid \psi\lambda$.

Lemma. Let ξ be an algebraic integer in $\mathbb{Q}[\omega]$, then $p \mid T(\xi\lambda)$.

Proof. Since $\xi\lambda$ is an algebraic integer $T(\xi\lambda)$ is in \mathbb{Z} . The previous lemma can be applied if $T(\xi\lambda)$ can be shown to be the product of λ and some algebraic integer in $\mathbb{Q}[\omega]$. Let the conjugates of ξ be $\xi_1, \xi_2, \dots, \xi_{p-1}$. The conjugates of λ are $1-\omega, 1-\omega^2, \dots, 1-\omega^{p-1}$. Note that

$$1 - \omega^j = (1 - \omega) \sum_{k=1}^{j-1} \omega^k = \lambda \sum_{k=1}^{j-1} \omega^k.$$

Thus

$$T(\xi\lambda) = \sum_{j=1}^{p-1} \xi_j (1 - \omega^j) = \lambda \left(\sum_{j=1}^{p-1} \xi_j \sum_{k=1}^{j-1} \omega^k \right).$$

Since

$$\sum_{j=1}^{p-1} \xi_j \sum_{k=1}^{j-1} \omega^k$$

is an algebraic integer in $\mathbb{Q}[\omega]$ the proof is complete.

Now to show that $1, \omega, \dots, \omega^{p-2}$ forms an integral basis for $\mathbb{Q}[\omega]$ consider an algebraic integer ξ in $\mathbb{Q}[\omega]$. Then

$$\xi = \sum_{i=0}^{p-2} a_i \omega^i \quad a_i \in \mathbb{Q}.$$

The proof will be complete when it is shown that the a_i are in \mathbb{Z} . Now

$$\begin{aligned}
T(\xi\lambda) &= T\left(\sum_{i=0}^{p-2} a_i \omega^i (1-\omega)\right) \\
&= T\left(\sum_{i=0}^{p-2} a_i (\omega^i - \omega^{i+1})\right) \\
&= \sum_{i=0}^{p-2} a_i (T(\omega^i) - T(\omega^{i+1})) \\
&= a_0 T(\lambda) = a_0 p
\end{aligned}$$

So $a_0 = \frac{T(\xi\lambda)}{p}$ but $p \mid T(\xi\lambda)$ thus a_0 is in Z . Now $\omega^p = 1$ so $\omega^{p-1} = \omega^{-1}$ is an algebraic integer in $Q[\omega]$. Consider

$$(\xi - a_0)\omega^{-1} = \sum_{i=1}^{p-2} a_i \omega^{i-1}.$$

The trace of $(\xi - a_0)\omega^{-1}\lambda$ and the second lemma can be used to show a_1 is in Z just as a_0 is. This process can be repeated to show all a_i are in Z . Thus $1, \omega, \omega^2, \dots, \omega^{p-2}$ is an integral basis for $Q[\omega]$.

The rest of the chapter is one long example demonstrating a method for finding an integral basis.

Example 53. Consider $Q[\alpha]$ from Example 23. The number α is not an algebraic integer. In Example 26 the number $\beta = 8\alpha$ is an algebraic integer and $1, \beta, \beta^2$ form a basis for $Q[\alpha]$. From Example 37 $\Delta(1, \beta, \beta^2) = -205258752 = -(2)^{18}(3)^3(29) = \Delta$. The minimal polynomial of β is $g(x) = x^3 - 12x^2 + 240x + 1728$. Basis elements exist with the form of Equation 51, that is

$$\begin{aligned} \rho_1 &= 1 \\ \rho_2 &= \frac{a+\beta}{\Delta_2} & a, b, c \in Z \\ \rho_3 &= \frac{b+c\beta+\beta^2}{\Delta_3} . \end{aligned}$$

Since $\Delta(1, \rho_2, \rho_3) = \Delta(1, \rho_2+h, \rho_3+k_1, \rho_2+k_2)$ for h, k_1 and k_2 in Z it follows from Theorem 50 that $1, \rho_2+h, \rho_3+k_1, \rho_2+k_2$ is an integral basis if $1, \rho_2, \rho_3$ is an integral basis. By making the appropriate choice for h, k_1 and k_2 the numbers a, b and c can be chosen such that

$$|a| < |\Delta_2| \quad |b| < |\Delta_3| \quad |c| < |\Delta_3| \quad (54)$$

without loss of generality. Since

$$\begin{aligned} 1 &= 1 \\ \rho_2 &= \frac{a}{\Delta_2} + \frac{1}{\Delta_2}\beta \\ \rho_2^2 &= \frac{a^2}{\Delta_2^2} + \frac{2a}{\Delta_2^2}\beta + \frac{1}{\Delta_2^2}\beta^2 \end{aligned}$$

Theorem 38 implies $\Delta(1, \rho_2, \rho_2^2) = \left(\frac{1}{\Delta_2}\right)^6 \Delta(1, \beta, \beta^2)$. Hence $\Delta_2^6 |2^{18} 3^3 29$. Since Δ_2 is to be as large as possible the first candidate for Δ_2 is $2^3 = 8$. Let F_2 be the linear transformation corresponding to β_2 then

$$F_2(1) = \frac{a}{\Delta_2} + \frac{1}{\Delta_2}\beta$$

$$F_2(\beta) = 0 + \frac{a}{\Delta_2}\beta + \frac{1}{\Delta_2}\beta^2$$

$$F_2(\beta^2) = -\frac{1728}{\Delta_2} - \frac{240}{\Delta_2}\beta + \frac{a+12}{\Delta_2}\beta^2.$$

The characteristic polynomial of ρ_2 is

$$\begin{vmatrix} x - \frac{a}{\Delta_2} & -\frac{1}{\Delta_2} & 0 \\ 0 & x - \frac{a}{\Delta_2} & -\frac{1}{\Delta_2} \\ \frac{1728}{\Delta_2} & \frac{240}{\Delta_2} & x - \frac{a+12}{\Delta_2} \end{vmatrix}$$

$$= x^3 - \frac{3a+12}{\Delta_2}x^2 + \frac{3a^2+24a+240}{\Delta_2^2}x - \frac{a^3+12a^2+240a-1728}{\Delta_2^3}.$$

The coefficients of this polynomial must be in \mathbb{Z} if ρ_2 is to be an algebraic integer. Thus

$$3a + 12 \equiv 0 \pmod{\Delta_2}$$

$$3a^2 + 24a + 240 \equiv 0 \pmod{\Delta_2^2} \tag{55}$$

$$a^3 + 12a^2 + 240a - 1728 \equiv 0 \pmod{\Delta_2^3}.$$

A solution can be found with $\Delta_2 = 8$ namely $a = 4$. Thus

$$\rho_2 = \frac{4 + \beta}{8}$$

and the minimal polynomial of ρ_2 is

$$x^3 - 24x^2 + 384x - 512 .$$

Finally, $\Delta(1, \rho_2, \rho_2^2) = -3^3 \cdot 29$. Now $\beta = -4 + 8\rho_2$ so

$$\rho_3 = \frac{b + c(-4 + 8\rho_2) + \beta^2}{\Delta} .$$

Expressing $1, \beta, \beta^2$ in terms of $1, \rho_2, \rho_3$ gives

$$1 = 1$$

$$\beta = -4 + 8\rho_2$$

$$\beta^2 = 4c - b - 8\rho_2 + \Delta_3 \rho_3 .$$

From Theorem 38 $\Delta(1, \beta, \beta^2) = -2^{18} 3^3 \cdot 29 = (8 \Delta_3)^2 \Delta(1, \rho_2, \rho_3)$. Thus $\Delta_3 \mid 2^6 3$. The largest candidate for Δ_3 is therefore $2^6 3 = 192$. Let F_3 be the linear transformation corresponding to ρ_3 then

$$F_3(1) = \frac{b}{\Delta_3} + \frac{c}{\Delta_3} \beta + \frac{1}{\Delta_3} \beta^2$$

$$F_3(\beta) = -\frac{1728}{\Delta_3} + \frac{b-240}{\Delta_3} \beta + \frac{c+12}{\Delta_3} \beta^2$$

$$F_3(\beta^2) = -\frac{1728(c+12)}{\Delta_3} - \frac{240(c+12) + 1728}{\Delta_3} \beta + \frac{b-240 + 12(c+12)}{\Delta_3} \beta^2 .$$

The characteristic polynomial of ρ_3 is

$$\left| \begin{array}{ccc}
 x - \frac{b}{\Delta_3} & - \frac{c}{\Delta_3} & - \frac{1}{\Delta_3} \\
 \frac{1728}{\Delta_3} & x - \frac{b-240}{\Delta_3} & - \frac{c+12}{\Delta_3} \\
 \frac{1728c+20736}{\Delta_3} & \frac{240c+4608}{\Delta_3} & x - \frac{b+12c-96}{\Delta_3}
 \end{array} \right|$$

$$\begin{aligned}
 &= x^3 - \frac{3b+12c-336}{\Delta_3} x^2 \\
 &+ \frac{3b^2 - 672b + 99072 + 24bc + 8064c + 240c^2}{\Delta_3^2} x \\
 &+ \frac{-b^3 + 336b^2 - 12b^2c - 99072b - 240c^2b + 1728c^3}{\Delta_3^3} \\
 &+ \frac{414720c - 8064bc - 2985964}{\Delta_3^3} .
 \end{aligned}$$

Since these coefficients must be in \mathbb{Z} for ρ_3 to be an algebraic integer three congruences are obtained. The first is

$$3b + 12c - 336 \equiv 0 \pmod{\Delta_3} .$$

For $\Delta_3 = 192$ this congruence becomes

$$b + 4c \equiv 112 \pmod{64} \quad \text{or} \quad b \equiv 48 - 4c \pmod{64} .$$

The general solution to this congruence is

$$\begin{aligned} b &= 4s \\ c &= 16t - s + 12 \end{aligned} \tag{55}$$

for any s and t in Z . Inequality 54 implies that b and c are bounded by 192. Two possibilities arise: either there is a b and c given by Equation 55 that makes all the coefficients of the characteristic equation of ρ_3 rational integers or $\Delta_3 \neq 192$. Trial and error shows that $b=48$ and $c=0$ makes all the coefficients in Z . Thus

$$\rho_3 = \frac{48 + \beta^2}{192}.$$

The minimal polynomial of ρ_3 is $x^3 + x^2 + 2x - 1$. From Theorem 38 $\Delta(1, \beta, \beta^2) = \left(\frac{1}{8} \cdot \frac{1}{192}\right)^2 \Delta(1, \rho_2, \rho_3)$. Thus $\Delta(1, \rho_2, \rho_3) = -3 \cdot 29$ is the discriminant of $Q[\alpha]$. Finally the integral basis can be given in terms of α where $\alpha = 8\beta$

$$\begin{aligned} \rho_1 &= 1 \\ \rho_2 &= \frac{1 + 2\alpha}{2} \\ \rho_3 &= \frac{3 + 4\alpha^2}{12}. \end{aligned}$$

The methods used in this example could, in principle, be applied to any algebraic extension. For some special types of extensions, simultaneous congruences have been found that give an integral basis. None of these systems have led to methods of attacking the general case different from the one used in the example. Two of these special cases are the cubic extension done in 1894 [7] and the pure extension done in 1930 [4].

CHAPTER IV

UNITS

The main goal of this chapter is to develop Dirichlet's fundamental theorem on units. This is an existence theorem concerning the structure of the set of units in the ring of algebraic integers contained in an algebraic number field. The theorem only proves the existence of certain numbers; it does not say how to find these numbers. As with integral bases, algorithms for units have been worked out for quadratic and cubic extensions. The chapter begins with the definition of a unit and some elementary properties.

Definition 56. An algebraic integer is called a unit if its multiplicative inverse is also an algebraic integer.

From the definition it is clear that the inverse of a unit is a unit. If μ_1 and μ_2 are units in $\mathbb{Q}[\theta]$ then $\mu_1\mu_2$ and $\mu_1^{-1}\mu_2^{-1}$ are algebraic integers in $\mathbb{Q}[\theta]$. Now $(\mu_1\mu_2)(\mu_1^{-1}\mu_2^{-1}) = 1$ thus $\mu_1\mu_2$ is a unit in $\mathbb{Q}[\theta]$. So the set of units in $\mathbb{Q}[\theta]$ forms a group under multiplication.

Theorem 57. Let μ be an algebraic integer in $\mathbb{Q}[\theta]$. Then μ is a unit if and only if $N(\mu) = \pm 1$.

Proof. If μ is a unit then μ^{-1} is a unit. Now by Corollary 33, $N(\mu)$ and $N(\mu^{-1})$ are in \mathbb{Z} since μ and μ^{-1} are algebraic integers. The

number 1 in $\mathbb{Q}[\theta]$ corresponds to the identity transformation thus $N(1) = 1$. Now

$$N(\mu)N(\mu^{-1}) = N(\mu\mu^{-1}) = N(1) = 1$$

Thus $N(\mu) \mid 1$ or $N(\mu) = \pm 1$. Conversely, suppose $N(\mu) = \pm 1$. Let the conjugates of μ be $\mu = \mu_1, \mu_2, \dots, \mu_n$ then $\pm 1 = N(\mu) = \mu_1\mu_2 \cdots \mu_n$ or $\mu^{-1} = \pm\mu_2\mu_3 \cdots \mu_n$. Since $\mu_2, \mu_3, \dots, \mu_n$ are roots of the minimal polynomial of μ they are also algebraic integers hence their product, μ^{-1} , is an algebraic integer. Thus μ is a unit.

Theorem 58. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ with constant term ± 1 . Then the roots of $f(x)$ are units.

Proof. If $f(x)$ is irreducible then $f(x)$ is the minimal polynomial of its roots and the theorem follows from Corollary 32. If $f(x)$ is reducible then by Theorem 6 the irreducible factors are monic with constant term ± 1 . Now Corollary 32 may be applied to the irreducible factors of $f(x)$ and the theorem is proved.

Definition 59. A root of the polynomial $x^n - 1$ is called an n^{th} root of unity. If ω is an n^{th} root of unity but not a k^{th} root of unity for $k < n$ then ω is a primitive n^{th} root of unity.

Theorem 58 implies that roots of unity are units. De Moivre's theorem gives an expression for the n^{th} roots of unity:

$$\exp\left\{\frac{2\pi k\sqrt{-1}}{n}\right\} = \cos \frac{2\pi k}{n} + \sqrt{-1} \sin \frac{2\pi k}{n} \quad (60)$$

where $k = 1, 2, \dots, n$.

Let $\varphi(n)$ be the Euler totient. Then the definition of roots of unity and De Moivre's theorem imply the following theorem.

Theorem 61. There are $\varphi(n)$ primitive n^{th} roots of unity. If $(k, n) = d$ then $\exp\left\{\frac{2\pi k\sqrt{-1}}{n}\right\}$ is a primitive n/d^{th} root of unity. If $h|n$ then an h^{th} root of unity is an n^{th} root of unity.

Let $\omega_1, \omega_2, \dots, \omega_{\varphi(n)}$ be the primitive n^{th} roots of unity. Then

$$\phi_n(x) = \prod_{j=1}^{\varphi(n)} (x - \omega_j)$$

is called the n^{th} cyclotomic polynomial. It can be shown that $\phi_n(x)$ is the minimal polynomial for the primitive n^{th} roots of unity.

Examples 42 and 52 dealt with roots of p^{th} cyclotomic polynomials where p is a prime number. A more detailed discussion of cyclotomic polynomials can be found in Clark [6].

The next theorem is one of many in this chapter that makes use of counting techniques in the proof.

Theorem 62. Let M be a positive number. Then there are only finitely many algebraic integers ψ of degree n or less such that $|\psi_j| < M$ where ψ_j are the conjugates of ψ .

Proof. Let

$$f(x) = \sum_{i=0}^k a_i x^i \quad a_i \in \mathbb{Z}$$

be the minimal polynomial of $\psi_1, \psi_2, \dots, \psi_k$. Where $k \leq n$ and $|\psi_j| < M \quad j = 1, 2, \dots, k$. The $|a_i|$ are the elementary symmetric

functions of $\psi_1, \psi_2, \dots, \psi_k$. Thus

$$|a_i| \leq \binom{k}{i} M^i \quad i = 0, 1, 2, \dots, k$$

where $\binom{k}{i}$ is the binomial coefficient. Since the a_i are bounded and in \mathbb{Z} there are only finitely many numbers that a_i can be. Thus there can only be finitely many polynomials with roots bounded by M . Since there are only finitely many polynomials there are only finitely many ψ as in the theorem.

Theorem 63. Let ψ be an algebraic integer. Then ψ is a root of unity if and only if all the conjugates of ψ have absolute value one.

Proof. Equation 60 implies that all the roots of unity have absolute value one. Since the conjugates of roots of unity are also roots of unity it follows that all the conjugates of a root of unity have absolute value one. Conversely let ψ be an algebraic integer such that all its conjugates have absolute value one. Now ψ is in $\mathbb{Q}[\psi]$ and since $\mathbb{Q}[\psi]$ is closed under multiplication the algebraic integers ψ^k are in $\mathbb{Q}[\psi]$ for $k=1, 2, \dots$. From Theorem 30 the degree of ψ^k is less than or equal to the degree of ψ . If ψ_j is a conjugate of ψ then ψ_j^k is a conjugate of ψ^k . Since $|\psi_j| = 1$, $|\psi_j^k| = 1$. Thus from Theorem 62 the sequence $\psi, \psi^2, \psi^3, \dots$ can have only finitely many distinct values. Therefore for some u and v with $u > v$ $\psi^u = \psi^v$. Thus $\psi^{u-v} = 1$ or ψ is a $u-v$ th root of unity.

These last two theorems imply that the number of roots of unity in a given algebraic number field is finite.

Theorem 64. The set of roots of unity in $Q[\theta]$ forms a cyclic group. That is, there is a root of unity ω in $Q[\theta]$ such that $\omega, \omega^2, \dots, \omega^k = 1$ is the complete set of roots of unity in $Q[\theta]$.

Proof. Since there are only finitely many roots of unity in $Q[\theta]$ there is a maximum n for which there is an n^{th} root of unity in $Q[\theta]$. Let that maximum value be k . From Equation 60 all the k^{th} roots of unity are in $Q[\theta]$. That is, if ω is a primitive k^{th} root of unity in $Q[\theta]$, then $\omega, \omega^2, \dots, \omega^k = 1$ are all in $Q[\theta]$. The theorem will be proved if it is shown that there can not be any other roots of unity other than k^{th} roots of unity in $Q[\theta]$. Suppose ν is a root of unity in $Q[\theta]$ and ν is not a k^{th} root of unity. Then ν is an h^{th} primitive root of unity where $h \nmid k$ and $h < k$. Then $\omega\nu$ is an m^{th} root of unity in $Q[\theta]$ where m is the least common multiple of h and k . Thus $m > k$ contradicting the maximum property of k . Therefore there is no other roots of unity in $Q[\theta]$ other than the k^{th} roots.

Theorem 65. Let $Q[\theta]$ be an algebraic number field. If θ has a real conjugate then the only roots of unity in $Q[\theta]$ are $+1$ and -1 .

Proof. Let ω be a root of unity in $Q[\theta]$. Let θ_j be a real conjugate of θ then $Q[\theta_j]$ is a field of real numbers. If ω_j is the conjugate of ω in $Q[\theta_j]$ then ω_j is real. The conjugates of roots of unity are roots of unity. Thus ω_j is a real root of unity that is $\omega_j = \pm 1$. Since the minimal polynomial of ± 1 is $x \mp 1$ it follows that $\omega = \pm 1$.

Corollary 66. If the degree of θ is odd then 1 and -1 are the only roots of unity in $Q[\theta]$.

Proof. The degree of θ is odd implies θ has a real conjugate.

There is one more result before beginning a long sequence of theorems leading to Dirichlet's theorem. This theorem proves one case not covered in the proof of Dirichlet's theorem.

Theorem 67. Let $-d$ be square free and $d < 0$ then all the units in $\mathbb{Q}[\sqrt{d}]$ consist of:

- i) the 4th roots of unity if $d = -1$
- ii) the 6th roots of unity if $d = -3$
- iii) 1 and -1 otherwise.

Proof. From Theorem 57 the units of $\mathbb{Q}[\sqrt{d}]$ are those algebraic integers with norm ± 1 . An integral basis for $\mathbb{Q}[\sqrt{d}]$ is given in Theorem 44. If $d = -1$ an algebraic integer in $\mathbb{Q}[\sqrt{d}]$ has the form

$$a + b\sqrt{-1} \quad a, b \in \mathbb{Z}.$$

Thus $N(a + b\sqrt{-1}) = a^2 + b^2 = \pm 1$ implies only 1, -1 , $\sqrt{-1}$ and $-\sqrt{-1}$ are units in $\mathbb{Q}[\sqrt{-1}]$. If $d = -3$ the algebraic integers have the form

$$a + b\left(\frac{1 + \sqrt{-3}}{2}\right) \quad a, b \in \mathbb{Z}.$$

Now

$$N\left(a + b\left(\frac{1 + \sqrt{-3}}{2}\right)\right) = a^2 + ab + b^2 = \pm 1$$

has six solutions giving the sixth roots of unity. If $d \equiv 2, 3 \pmod{4}$ then the integers of $\mathbb{Q}[\sqrt{d}]$ have the form

$$a + b\sqrt{d} \quad a, b \in \mathbb{Z}.$$

Then

$$N(a + b\sqrt{d}) = a^2 - b^2d = \pm 1$$

has no solutions for $d < -1$ except $a = \pm 1$ $b = 0$. If $d \equiv 1 \pmod{4}$ then the integers have the form

$$a + b\left(\frac{1 + \sqrt{d}}{2}\right) \quad a, b \in \mathbb{Z}.$$

Now

$$N\left[a + b\left(\frac{1 + \sqrt{d}}{2}\right)\right] = a^2 + ab + \frac{1-d}{4}b^2 = \pm 1$$

implies $b = 0$ since $d < -3$. So the only units are ± 1 .

Note that if $a + b\sqrt{-1}$ is a root of a polynomial in $\mathbb{Q}[x]$ then $a - b\sqrt{-1}$ is also a root of that polynomial. For the remainder of this chapter let θ be an algebraic number and let the degree of θ be $n = r + 2s$ where r is the number of real conjugates and $2s$ the number of complex conjugates. When $r = 1$ and $s = 0$ then $\mathbb{Q}[\theta] = \mathbb{Q}$ and when $r = 0$ and $s = 1$ the units are described in Theorem 67, thus it is also assumed that $r + s > 1$. When the conjugates are numbered they shall always be numbered such that the last s conjugates shall consist of one member from each pair of complex conjugates. That is, if $a + b\sqrt{-1}$ is among the last s conjugate then $a - b\sqrt{-1}$ will be among the first $r + s$ conjugates. Instead of the n conjugates sometimes n real numbers consisting of the r real conjugates the s real parts and s imaginary parts of the complex conjugates will be used.

The following lemma will be needed in the proof of Theorem 70.

Lemma 68. If k , m and n are positive rational integers such that $n > m$ then there is an h in Z such that $h > 0$ and

$$(k+1)^n > h^m > k^n \quad (69)$$

Proof. Consider the real function

$$f(x) = (x+1)^{n/m} - x^{n/m}.$$

It follows from elementary calculus that $f(x)$ is increasing for $x > 0$. Since $f(0) = 1$ it follows that $f(k) > 1$. Therefore there is an h in Z such that $(k+1)^{n/m} > h > k^{n/m}$ so there exists an h as in Equation 69.

In Theorem 70 and the following corollaries the order of the first $r+s$ conjugates is arbitrary.

Theorem 70. Let A and B be real numbers such that $B > A > 0$ and let t be in Z such that $1 \leq t < r+s$. Then there is a ξ in $Q[\theta]$ and a real number C such that

$$\begin{aligned} |N(\xi)| &< C \\ |\xi_i| &< A \text{ for } i = 1, 2, \dots, t \\ |\xi_i| &> B \text{ for } i = t+1, \dots, r+s \end{aligned}$$

where ξ_i $i = 1, 2, \dots, n$ are the conjugates of ξ . The number C does not depend on the choice of A , B or t .

Proof. Let $\rho_1, \rho_2, \dots, \rho_n$ be an integral basis for $Q[\theta]$ and let ρ_{ij} be the j^{th} conjugate of ρ_i . Set

$$M = \max_j \sum_{i=1}^n |\rho_{ij}|$$

and for each j , $j = 1, 2, \dots, n$ define n real numbers

$$u_{ij} = \begin{cases} \text{the real part of } \rho_{ij} & i = 1, 2, \dots, r+s \\ \text{the imaginary part of } \rho_{ij} & i = r+s+1, \dots, n. \end{cases}$$

Consider for $j = 1, 2, \dots, n$

$$v_j = \sum_{i=1}^n x_i u_{ij} \quad x_i \in Z.$$

Let $0 \leq x_i \leq k$ then there are $(k+1)^n$ possible values for v_j for each j . Now

$$\begin{aligned} |v_j| &= \left| \sum_{i=1}^n x_i u_{ij} \right| \leq \sum_{i=1}^n |x_i u_{ij}| \\ &\leq k \sum_{i=1}^n |u_{ij}| \leq k \sum_{i=1}^n |\rho_{ij}| \\ &\leq k M \quad j = 1, 2, \dots, n. \end{aligned}$$

Consider v_j for the following values of j : $j = 1, 2, \dots, t$ and those j from $r+s+1, \dots, n$ which have a complex conjugate among the first t conjugates. That is if θ_g and θ_i are a complex pair of conjugate such that $1 \leq g \leq t$ then $r+s < i \leq n$ and g and i are both acceptable values for j . Let J be the set of acceptable values for j and let m be the number of elements in J . Then $t \leq m \leq t+s < r+s+s = n$. since $t < r+s$. Note that m , n and k satisfy the hypotheses of Lemma 68 thus there is an $h > 0$ as in Inequality 69. Partition the closed interval $[-Mk, Mk]$ into h

subintervals in the following way

$$\left[-Mk, -Mk + \frac{2Mk}{h}\right), \left[-Mk + \frac{2Mk}{h}, -Mk + \frac{4Mk}{h}\right), \dots, \left[Mk - \frac{2Mk}{h}, Mk\right].$$

For the numbers v_j in $[-Mk, Mk]$, consider those v_j such that j is in J . The set of m values for v_j can belong to the h subintervals of $[-Mk, Mk]$ in h^m different ways. Now for each j in J there are $(k+1)^n$ values v_j . From Equation 69 $(k+1)^n > h^m$. Thus there must be two sets of values for the v_j that belong to the h subintervals in the same way. Let these two sets be given by

$$v_j' = \sum_{i=1}^n x_i' u_{ij}$$

and

$$v_j'' = \sum_{i=1}^n x_i'' u_{ij}.$$

Summarizing the properties of v_j' and v_j'' :

$$|x_i' - x_i''| \leq k \quad j = 1, 2, \dots, n$$

$$|v_j' - v_j''| \leq \frac{2kM}{h} \quad j \in J.$$

The x_i' and x_i'' will be used to define a number ξ . Then it will be shown that for a suitable k the number ξ will have the desired properties. Let

$$\xi = \sum_{i=1}^n (x_i' - x_i'') \rho_i.$$

For the j in J such that $Q[\theta_j]$ is a real extension, $\rho_{ij} = u_{ij}$ and

$$\begin{aligned}
|\xi_j| &= \left| \sum_{i=1}^n (x_i' - x_i'') \rho_{ij} \right| \\
&= \left| \sum_{i=1}^n x_i' u_{ij} - \sum_{i=1}^n x_i'' u_{ij} \right| \\
&= |v_j' - v_j''| < \frac{2kM}{h} .
\end{aligned}$$

If $Q[\theta_j]$ is a complex extension, then $\rho_{ij} = u_{ij} - u_{ik} \sqrt{-1}$ where k is such that $Q[\theta_k]$ is the complex conjugate extension of $Q[\theta_j]$. Note that if j is in J then k is in J . Now

$$\begin{aligned}
|\xi_j| &= \left| \sum_{i=1}^n (x_i' - x_i'') \rho_{ij} \right| \\
&= \left| \sum_{i=1}^n x_i' (u_{ij} - u_{ik} \sqrt{-1}) - x_i'' (u_{ij} - u_{ik} \sqrt{-1}) \right| \\
&\leq |v_j' - v_j''| + |\sqrt{-1} (v_k' - v_k'')| \\
&\leq \frac{2kM}{h} + \frac{2kM}{h} .
\end{aligned}$$

thus

$$|\xi_j| \leq \frac{4kM}{h} \quad j = 1, 2, \dots, t$$

whether the j^{th} extension is real or complex. From Inequality 69, $h^m > k^n$. Thus

$$|\xi_j| \leq 4Mk^{1 - \frac{n}{m}}, \quad j \in J .$$

Since $n > m$ $k^{1 - \frac{n}{m}} \rightarrow 0$ as $k \rightarrow \infty$, there is a k_1 such that

$$|\xi_j| \leq 4Mk^{1 - \frac{n}{m}} < A \quad j = 1, 2, \dots, t$$

for all $k > k_1$. Now for j not in J

$$\begin{aligned} |\xi_j| &= \left| \sum_{i=1}^n (x_i' - x_i'') \rho_{ij} \right| \leq \sum_{i=1}^n |x_i' - x_i''| |\rho_{ij}| \\ &\leq \sum_{i=1}^n k |\rho_{ij}| \leq kM. \end{aligned}$$

Thus

$$|N(\xi)| = \left| \prod_{j=1}^n \xi_j \right| = \prod_{j=1}^n |\xi_j|$$

which can be written in the form

$$\begin{aligned} |N(\xi)| &= \prod_{j \in J} |\xi_k| \prod_{q \notin J} |\xi_q| \\ &\leq (4Mk^{1-\frac{n}{m}})^m (kM)^{n-m} \\ &\leq 4^m M^n < (4M)^n. \end{aligned}$$

Let $C = (4M)^n$ then C depends only on the basis $\rho_1, \rho_2, \dots, \rho_n$ chosen for $Q[\theta]$. To obtain a better estimate for $|\xi_j|$ for $j = t+1, t+2, \dots, s+r$ consider

$$\begin{aligned} |N(\xi)| &= \left(\prod_{\substack{q=1 \\ q \neq j}}^n |\xi_q| \right) |\xi_j| \\ &\leq \left(4Mk^{1-\frac{n}{m}} \right)^m (kM)^{n-m-1} |\xi_j| \\ &= 4^m M^{n-1} k^{-1} |\xi_j|. \end{aligned}$$

Since $N(\xi)$ is in Z , $N(\xi) \geq 1$ thus

$$|\xi_j| \geq (4^m M^{n-1})^{-1} k.$$

Thus there is a k_2 such that for $k > k_2$

$$|\xi_j| \geq (4^m M^{n-1})^{-1} k > B \quad j = t+1, \dots, r+s.$$

Now if $k > k_1 + k_2$ then for $j = 1, 2, \dots, n$

$$|\xi_j| < A \quad j \in J$$

$$|\xi_j| > B \quad j \notin J.$$

Thus the desired ξ exists and the theorem is finally proved.

Corollary 71. There exists a sequence of algebraic integers

$\langle \xi_i \rangle$ in $Q[\theta]$ such that

$$|\xi_{ij}| > |\xi_{i+1j}| \quad j = 1, 2, \dots, t$$

$$|\xi_{ij}| < |\xi_{i+1j}| \quad j = t+1, t+2, \dots, r+s$$

and $|N(\xi_i)| < C$. Where t and C are as in Theorem 70 and ξ_{ij} is the j^{th} conjugate of ξ_i .

Proof. Let $\xi_1 = \xi$ from Theorem 70. Then define ξ_{i+1} inductively by Theorem 70 where

$$A_{i+1} = \min_j |\xi_{ij}| \quad j = 1, 2, \dots, t$$

$$B_{i+1} = \max_j |\xi_{ij}| \quad j = t+1, t+2, \dots, r+s.$$

Note that it is not possible for any of the A_i to be zero since $A_i = 0$ implies some $\xi_{i-1j} = 0$ but the only conjugates of zero are zero and

$|\xi_{i-1t+1}| > B_i$ is contradicted. It follows from Theorem 70 that the sequence $\langle \xi_i \rangle$ has the desired properties.

Corollary 72. There exists a sequence of algebraic integers $\langle \psi_i \rangle$ in $Q[\theta]$ such that

$$|\psi_{ij}| > |\psi_{i+1j}| \quad j = 1, 2, \dots, t$$

$$|\psi_{ij}| < |\psi_{i+1j}| \quad j = t+1, t+2, \dots, r+s$$

where t is as in Theorem 70 and for all positive i, k in Z

$$N(\psi_i) = N(\psi_k).$$

Proof. Consider the sequence $\langle \xi_i \rangle$ of Corollary 71. The norms of ξ_i are in Z and bounded by C . Thus there are only finitely many values the norm can have. Thus there is a subsequence $\langle \psi_i \rangle$ of $\langle \xi_i \rangle$ where all the norms are equal.

Theorem 73. There is a unit in $Q[\theta]$ other than a root of unity.

Proof. Consider the sequence $\langle \psi_i \rangle$ of Corollary 72. Let $g = |N(\psi_i)|$ and $\rho_1, \rho_2, \dots, \rho_n$ be an integral basis of $Q[\theta]$. Now

$$\psi_i = \sum_{j=1}^n a_{ij} \rho_j \quad a_{ij} \in Z$$

for $i = 1, 2, 3, \dots$. Partition the set of ψ_i by the following rule:

ψ_i and ψ_k are in the same class if

$$a_{ij} \equiv a_{kj} \pmod{g} \quad j = 1, 2, \dots, n.$$

The partition has at most g^n classes. Thus some class has at least two elements. Let ψ_i and ψ_k be in the same class then

$$a_{ij} = a_{kj} + b_j g \quad j = 1, 2, \dots, n.$$

Since $N(\psi_k) = \pm g$ there is an algebraic integer γ in $Q[\theta]$ such that $\psi_k \gamma = g$. Now

$$\begin{aligned} \psi_i &= \sum_{j=1}^n a_{ij} \rho_j = \sum_{j=1}^n (a_{kj} + b_j g) \rho_j \\ &= \sum_{j=1}^n (a_{kj} + b_j \psi_k \gamma) \rho_j \\ &= \sum_{j=1}^n a_{kj} \rho_j + \gamma \sum_{j=1}^n b_j \psi_k \rho_j \\ &= \psi_k + \psi_k \gamma \sum_{j=1}^n b_j \rho_j \\ &= \psi_k \left(1 + \gamma \sum_{j=1}^n b_j \rho_j \right). \end{aligned}$$

Since $1, \gamma, b_j$ and ρ_j are algebraic integers

$$\varepsilon = 1 + \gamma \sum_{j=1}^n b_j \rho_j$$

is also an algebraic integer. Now $N(\psi_i) = N(\varepsilon \psi_k) = N(\varepsilon) N(\psi_k)$. Since $N(\psi_i) = N(\psi_k)$ it follows that $N(\varepsilon) = 1$. Thus by Theorem 57 ε is a unit. From Corollary 72 it follows that none of the corresponding conjugates of ψ_i and ψ_k have the same absolute values. Since $\varepsilon = \psi_i / \psi_k$ none of the conjugates of ε have absolute value one. It follows from Theorem 63 that ε is not a root of unity.

Corollary 74. For any t of the first $r+s$ conjugate fields $Q[\theta_j]$ there is a unit ϵ in $Q[\theta]$ such that $|\epsilon_j| < 1$ for those t conjugate fields, and $|\epsilon_j| > 1$ for the remaining $r+s-t$ conjugate fields. Here $1 \leq t < r+s$.

Proof. Without loss of generality let the conjugate fields $Q[\theta_j]$ be numbered so the first t are the fields such that $|\epsilon_j| < 1$ is desired. Consider the $\epsilon = \psi_i/\psi_k$ of Theorem 73. If $i > k$ then from Corollary 72

$$\begin{aligned} |\psi_{ij}| &< |\psi_{kj}| & j = 1, 2, \dots, t \\ |\psi_{ij}| &> |\psi_{kj}| & j = t+1, t+2, \dots, r+s. \end{aligned}$$

Then $\epsilon = \psi_i/\psi_k$ satisfies the conclusion of the corollary. If $k > i$ then ϵ^{-1} is also a unit and it satisfies the conclusion of the corollary.

Definition 75. A set of units $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ in $Q[\theta]$ is said to be independent if

$$\prod_{i=1}^k \epsilon_i^{a_i} = 1 \quad a_i \in \mathbb{Z}$$

implies $a_i = 0 \quad i = 1, 2, \dots, k$. If the set is not independent then it is dependent.

The next few theorems develop some methods of determining independence for a set of units. Clearly a set of one unit is dependent if and only if that unit is a root of unity. Thus any set of units containing a root of unity is a dependent set.

The following discussion gives an equivalent form for independence that will be used frequently. Consider the set of units $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ such that

$$\prod_{i=1}^k \varepsilon_i^{q_i/b_i} = 1 \quad q_i, b_i \in \mathbb{Z}. \quad b_i \neq 0.$$

Let m be the least common multiple of the b_i . Then mq_i/b_i is in \mathbb{Z} and

$$\prod \varepsilon_i^{mq_i/b_i} = 1^m = 1.$$

If $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ is an independent set then $mq_i/b_i = 0$ implies $q_i = 0$ for $i = 1, 2, \dots, k$. Conversely if there is some $q_j \neq 0$ then $mq_j/b_j \neq 0$ and the set is dependent. Thus in Definition 75 a_i in \mathbb{Z} could be replaced by a_i in \mathbb{Q} .

The following lemma is needed in the proof of the next theorem. The greatest integer function is denoted by $[x]$.

Lemma 76. Let c be an irrational real number and h and k be in \mathbb{Z} . If $hc - [hc] = kc - [kc]$ then $h = k$.

Proof. If $hc - [hc] = kc - [kc]$ then $[hc] - [kc] = hc - kc = (h - k)c$. Now $[hc] - [kc]$ and $(h - k)$ are in \mathbb{Z} . Thus c must be rational unless $h - k = 0$ or $h = k$.

Note this lemma implies for fixed c the set $\{hc - [hc] : h \in \mathbb{Z}\}$ is infinite if c is irrational and finite if c is rational.

Theorem 77. Let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ be units in $Q[\theta]$ and ε_{ij} the j^{th} conjugate of ε_i . If

$$\sum_{i=1}^k a_i \log |\varepsilon_{ij}| = 0 \quad j = 1, 2, \dots, r+s$$

for nontrivial real a_i then $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ is a dependent set.

Proof. Since any set of units containing roots of unity is a dependent set, assume that none of the units are roots of unity. One unit forms an independent set. Suppose that for $2 \leq q$

$$\sum_{i=1}^{q-1} b_i \log |\varepsilon_{ij}| = 0 \quad j = 1, 2, \dots, r+s \quad (78)$$

has only the trivial solution for the b_i . Also suppose that

$$\sum_{i=1}^q a_i \log |\varepsilon_{ij}| = 0 \quad j = 1, 2, \dots, r+s \quad (79)$$

has a nontrivial solution for the a_i . Now $a_q \neq 0$ otherwise the assumption of Equation 78 is contradicted. Then

$$\log |\varepsilon_{qj}| = - \sum_{i=1}^{q-1} \frac{a_i}{a_q} \log |\varepsilon_{ij}| \quad j = 1, 2, \dots, r+s$$

Consider the set S of units in $Q[\theta]$ such that η is in S if and only if there are real c_i such that

$$\log |\eta_j| = \sum_{i=1}^{q-1} c_i \log |\varepsilon_{ij}| \quad j = 1, 2, \dots, r+s.$$

The set S is not empty since ε_q is in S . The object now is to show

that for all η in S the c_i are rational. If c_i is irrational then $0 < mc_i - [mc_i] < 1$ for all m in Z . For $j = 1, 2, \dots, r+s$

$$\begin{aligned} \sum_{i=1}^{q-1} (mc_i - [mc_i]) \log |\epsilon_{ij}| &= \sum_{i=1}^{q-1} mc_i \log |\epsilon_{ij}| - \sum_{i=1}^{q-1} [mc_i] \log |\epsilon_{ij}| \\ &= m \log |\eta_j| - \sum_{i=1}^{q-1} \log |\epsilon_{ij}|^{[mc_i]} \\ &= \log |\eta_j^m| - \log \left| \prod_{i=1}^{q-1} \epsilon_{ij}^{[mc_i]} \right|. \end{aligned}$$

Now $\prod_{i=1}^{q-1} \epsilon_{ij}^{[mc_i]}$ is a unit and so is its inverse. Let

$$\mu^{-1} = \prod_{i=1}^{q-1} \epsilon_{ij}^{[mc_i]}$$

then for $j = 1, 2, \dots, r+s$

$$\log |\eta_j^m \mu| = \sum_{i=1}^{q-1} (mc_i - [mc_i]) \log |\epsilon_{ij}|.$$

Thus if η is in S so is $\eta^m \mu$ for all m in Z . If the c_i corresponding to η are irrational then for each m in Z the unit $\eta^m \mu$ has a distinct representation according to Lemma 76. Each distinct representation gives a distinct unit otherwise the assumption for Equation 78 is contradicted. Now $0 < mc_i - [mc_i] < 1$ implies

$$\begin{aligned} \log |\eta_j^m \mu_j| &\leq \sum_{i=1}^{q-1} \log |\epsilon_{ij}| \quad j = 1, 2, \dots, r+s \\ &\leq \log M \end{aligned}$$

where

$$M = \max \prod_{i=1}^{q-1} |\epsilon_{ij}| .$$

Since log is a monotone function the first $r+s$ conjugates of η^m_μ are bounded by M . Since each of the last s conjugates with one of the first $r+s$ conjugates forms a complex conjugate pair, the last s conjugates are also bounded by M . Theorem 62 implies there cannot be an infinite number of elements of the form η^m_μ with conjugates bounded by M . Thus the c_i cannot be irrational. So the a_i in Equation 79 are rational which implies

$$\left| \prod_{i=1}^q \epsilon_{ij}^{a_i} \right| = 1 \quad j = 1, 2, \dots, n .$$

Note that the last s equations are repetitions of some s of the first $r+s$. Theorem 63 implies $\prod_{i=1}^q \epsilon_i^{a_i}$ is a root of unity. Thus there is a positive b in Z such that

$$\prod_{i=1}^q \epsilon_i^{a_i b} = 1 .$$

Since $a_q b \neq 0$, $\epsilon_1, \epsilon_2, \dots, \epsilon_q$ is a dependent set. Thus the theorem is proved by induction.

Theorem 80. Any $r+s$ units in $Q[\theta]$ are dependent.

Proof. Let $\epsilon_1, \epsilon_2, \dots, \epsilon_{r+s}$ be any $r+s$ units in $Q[\theta]$ and ϵ_{ij} the j^{th} conjugate of ϵ_i . Then

$$|N(\epsilon_i)| = \left| \prod_{j=1}^n \epsilon_{ij} \right| = \prod_{j=1}^n |\epsilon_{ij}| = 1 \quad i = 1, 2, \dots, r+s.$$

Each of the last s conjugates has its corresponding complex conjugate among the first $r+s$ conjugates. Since the members of a complex conjugate pair have the same absolute value

$$|N(\epsilon_i)| = \prod_{j=1}^{r+s} |\epsilon_{ij}^{a_j}| = 1 \quad i = 1, 2, \dots, r+s$$

where a_j is one if ϵ_{ij} is a real conjugate and two if complex. Thus

$$\sum_{j=1}^{r+s} a_j \log |\epsilon_{ij}| = 0 \quad i = 1, 2, \dots, r+s.$$

This is a system of $r+s$ equations in the $r+s$ a_j which has a nontrivial solution. This implies the system with the coefficient matrix transposed also has a nontrivial solution. Thus there is a nontrivial solution c_1, c_2, \dots, c_{r+s} to

$$\sum_{i=1}^{r+s} c_i \log |\epsilon_{ij}| = 0 \quad j = 1, 2, \dots, r+s$$

Theorem 77 implies that $\epsilon_1, \epsilon_2, \dots, \epsilon_{r+s}$ is a dependent set.

Theorem 81. There exist $r+s-1$ independent units in $Q[\theta]$.

Proof. The method of proof will be to show that given k independent units where k is less than $r+s-1$ it is possible to find another unit to add to the set and still have an independent set. Theorem 73 proved there is one independent unit. Consider k independent units $\epsilon_1, \epsilon_2, \dots, \epsilon_k$. From Theorem 77

$$\sum_{i=1}^k a_i \log |\varepsilon_{ij}| = 0 \quad i=1, 2, \dots, r+s$$

has only the trivial solution. Thus there must be k of those $r+s$ equations which have only the trivial solution for the a_i . Suppose they are the first k , then

$$\begin{vmatrix} \log |\varepsilon_{11}| & \log |\varepsilon_{12}| & \dots & \log |\varepsilon_{1k}| \\ \log |\varepsilon_{21}| & \log |\varepsilon_{22}| & \dots & \log |\varepsilon_{2k}| \\ \dots & \dots & \dots & \dots \\ \log |\varepsilon_{k1}| & \log |\varepsilon_{k2}| & \dots & \log |\varepsilon_{kk}| \end{vmatrix} \neq 0. \quad (82)$$

Consider the following determinant

$$\begin{vmatrix} \log |\varepsilon_{11}| & \log |\varepsilon_{12}| & \dots & \log |\varepsilon_{1,k+1}| \\ \log |\varepsilon_{21}| & \log |\varepsilon_{22}| & \dots & \log |\varepsilon_{2,k+1}| \\ \dots & \dots & \dots & \dots \\ \log |\varepsilon_{k1}| & \log |\varepsilon_{k2}| & \dots & \log |\varepsilon_{k,k+1}| \\ b_1 & b_2 & \dots & b_{k+1} \end{vmatrix} = A_1 b_1 + A_2 b_2 + \dots + A_{k+1} b_{k+1} \quad (83)$$

where A_i is the cofactor of b_i . Equation 82 implies $A_{k+1} \neq 0$.

Since $k < r+s-1$ Corollary 74 implies there is a unit ε_{k+1} in $Q[\theta]$

such that $|\varepsilon_{k+1j}| < 1$ if $A_j \leq 0$ and $|\varepsilon_{k+1j}| > 1$ if $A_j > 0$.

Substituting $\log|\epsilon_{k+1,j}|$ for b_j in equation 83 gives

$$\sum_{j=1}^{k+1} A_j b_j = \sum_{j=1}^{k+1} A_j \log|\epsilon_{k+1,j}|.$$

Now $\log|\epsilon_{k+1,j}|$ has the same sign as A_j when $A_j \neq 0$. Since $A_{k+1} \neq 0$

$$\sum_{j=1}^{k+1} A_j \log|\epsilon_{k+1,j}| > 0.$$

Thus the determinant in equation 83 with $b_j = \log|\epsilon_{k+1,j}|$ is not zero. From Theorem 77 the units $\epsilon_1, \epsilon_2, \dots, \epsilon_{k+1}$ are independent. When $k = r + s - 1$ Corollary 74 cannot be applied to find an additional unit. Thus up to $r + s - 1$ independent units can be found

Theorem 84. Let $\epsilon_1, \epsilon_2, \dots, \epsilon_{r+s-1}$ be a set of independent units in $Q[\theta]$. Then there is an m in Z such that every unit η in $Q[\theta]$ can be written in the form

$$\eta = \omega \prod_{j=1}^{r+s-1} \epsilon_j^{b_j/m} \quad b_j \in Z$$

and ω is a root of unity.

Proof. Let S be the set of units in $Q[\theta]$ of the form

$$\eta = \mu \prod_{j=1}^{r+s-1} \epsilon_j^{a_j/c_j} \quad \left| \frac{a_j}{c_j} \right| \leq 1$$

where μ is a root of unity a_j and c_j are in Z and $(a_j, c_j) = 1$. Now ϵ_j is in S thus $S \neq \emptyset$. Since $|\mu| = 1$ $\log|\mu| = 0$ and

$$\left| \log |\eta_i| \right| = \left| \sum_{j=1}^{r+s-1} a_j/c_j \log |\epsilon_{ji}| \right| \quad i=1, 2, \dots, r+s$$

$$\leq \sum_{j=1}^{r+s-1} \left| \log |\epsilon_{ji}| \right| = M$$

The conjugates of all η in S are bounded by M , thus S is finite by Theorem 62. Theorem 77 implies the a_j and c_j are unique. Let m be the least common multiple of the c_j . Let η be any unit in $\mathbb{Q}[\theta]$ then $\eta, \epsilon_1, \epsilon_2, \dots, \epsilon_{r+s-1}$ is a dependent set, so there are $z, z_1, z_2, \dots, z_{r+s-1}$ in \mathbb{Z} such that

$$\eta^z \prod_{i=1}^{r+s-1} \epsilon_i^{z_i} = 1.$$

Now

$$\left(\eta \prod_{i=1}^{r+s-1} \epsilon_i^{z_i/z} \right)^z = 1.$$

Let

$$\omega = \eta \prod_{i=1}^{r+s-1} \epsilon_i^{z_i/z}.$$

Then ω is a root of unity and

$$\eta = \omega \prod_{i=1}^{r+s-1} \epsilon_i^{-z_i/z}$$

After the $\epsilon_i^{-z_i/z}$ have been written in lowest terms let y be the least common denominator and y_i the appropriate numerator, then

$$\eta = \omega \prod_{i=1}^{r+s-1} \epsilon_i^{y_i/y}.$$

Now $y_i/y - [y_i/y] \leq 1$, and $[y_i/y]$ is in \mathbb{Z} so $\epsilon_i^{[y_i/y]}$ is in $\mathbb{Q}[\theta]$.

$$\omega \prod_{i=1}^{r+s-1} \epsilon_i^{y_i/y} \prod_{i=1}^{r+s-1} \epsilon_i^{-[y_i/y]} = \omega \prod_{i=1}^{r+s-1} \epsilon_i^{y_i/y - [y_i/y]}$$

is the product of units and thus a unit. The exponents are bounded by one thus this unit is in S . The least common multiple of the denominators of the exponents of ϵ_i is y thus $y \mid m$. Let $xy = m$ and $b_j = y_j x$ then

$$\eta = \omega \prod_{i=1}^{r+s-1} \epsilon_i^{b_i/m}.$$

The following theorem was first proved by Dirichlet in 1846,

Theorem 85. Let θ be an algebraic number of degree $n = r + 2s \geq 1$. Then there are units $\mu_1, \mu_2, \dots, \mu_k$ in $\mathbb{Q}[\theta]$ where $k = r + s - 1$ such that any unit η in $\mathbb{Q}[\theta]$ can be represented in the form

$$\eta = \omega \prod_{j=1}^k \mu_j^{z_j} \quad z_j \in \mathbb{Z}.$$

Where the z_j are unique and ω is a root of unity.

Proof. The cases when $n = 1$ and $n = 2s = 2$ were done in Theorem 67. Consider $r + s > 1$. Let $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ be independent units and m the rational integer in Theorem 84. Consider units of the form

$$\begin{aligned}
\mu_1 &= \epsilon_1^{b_{11}/m} \\
\mu_2 &= \epsilon_1^{b_{21}/m} \epsilon_2^{b_{22}/m} \\
&\dots \\
\mu_k &= \prod_{j=1}^k \epsilon_j^{b_{kj}/m}
\end{aligned} \tag{86}$$

where b_{ij} are in Z . Clearly there are units with $b_{ii} \neq 0$ for each equation in 86. Pick μ_i with $b_{ii} \neq 0$ as in equation 86 such that $|b_{ii}|$ is minimum for each i , $i = 1, 2, \dots, k$. Let η be a unit in $Q[\theta]$, from Theorem 84

$$\eta = \omega \prod_j^k \epsilon_j^{a_j/m} \quad a_j \in Z.$$

From the division algorithm $a_k = z_k b_{kk} + r_k$ and $0 \leq r_k < |b_{kk}|$. Now μ_k is a unit so $\eta \mu_k^{-z_k}$ is a unit in $Q[\theta]$ also and

$$\eta \mu_k^{-z_k} = \omega \prod_{j=1}^k \epsilon_j^{(a_j - z_k b_{kj})/m}.$$

Thus $r_k = 0$ otherwise the choice of μ_k is contradicted. Similarly $a_{k-1} - z_k b_{kj-1} = z_{k-1} b_{k-1k-1} + r_{k-1}$ where $0 \leq r_{k-1} < |b_{k-1k-1}|$. Again $r_{k-1} = 0$ otherwise the choice of μ_{k-1} is contradicted. This process can be repeated until $z_k, z_{k-1}, z_{k-2}, \dots, z_1$ are determined. Then

$$\eta = \omega \prod_{j=1}^k \mu_j^{z_j}.$$

To show the z_j are unique it is necessary to show that $\mu_1, \mu_2, \dots, \mu_k$ form an independent set. Let c_1, c_2, \dots, c_k be in z such that

$$\prod_{j=1}^k \mu_j^{c_j} = 1$$

Now

$$\prod_{j=1}^k \mu_j^{c_j} = \prod_{j=1}^k \epsilon_j^{d_j}$$

where

$$d_j = \frac{1}{m} \sum_{i=1}^k c_i b_{ij} \quad j = 1, 2, \dots, k$$

then $d_j = 0$, $j = 1, 2, \dots, k$ since $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ is an independent set of units. Suppose h is the largest subscript such that $c_h \neq 0$ then

$$d_h = \frac{1}{m} \sum_{i=h}^k c_i b_{ih} = \frac{c_h b_{hh}}{m}$$

Since $d_h = 0$ and $b_{hh} \neq 0$, $c_h \neq 0$ gives a contradiction. Thus $c_j = 0$, $j = 1, 2, \dots, k$ and the set $\mu_1, \mu_2, \dots, \mu_k$ is independent.

The units $\mu_1, \mu_2, \dots, \mu_k$ of Theorem 85 are called a set of fundamental units for $Q[\theta]$.

Example 87. Consider $Q[\alpha]$ from Example 23. From Example 53 the discriminant of $Q[\alpha]$ is $-3 \cdot 29$. This implies that two of the three conjugate fields are complex and $r + s - 1 = 1$. Thus there is one fundamental unit in $Q[\alpha]$. From Theorem 65 the roots of unity in $Q[\alpha]$ are 1 and -1 . From Example 53 ρ_3 has minimal

polynomial $x^3 + x^2 + 2x - 1$. Thus $N(\rho_3) = 1$ and ρ_3 is a unit in $Q[\alpha]$. Now

$$\rho_3 = \pm \mu^n$$

for some n in Z where μ is a fundamental unit. Since $\rho_3^{-1} = \pm \mu^{-n}$ only positive n need be considered. Now the object will be to find an n^{th} root of $\pm \rho_3$ in $Q[\alpha]$ for the largest possible value of n . This process is done by extracting p^{th} roots of ρ_3 , where p is prime, until no more roots can be extracted. First consider $\rho_3 = \pm \mu^2$. Since $N(\rho_3) = 1 = N(\pm \mu^2) = N(\pm 1)N(\mu)^2 = \pm N(\mu)^2$ only the plus sign needs to be considered. Suppose μ has minimal polynomial $x^3 + ax^2 + bx + c$. The elementary symmetric functions of the conjugates of ρ_3 are also symmetric functions of the conjugates of μ . Thus if the conjugates of μ are μ_1, μ_2, μ_3 and of ρ_3 are $\rho_{31}, \rho_{32}, \rho_{33}$ then

$$1 = -(\rho_{31} + \rho_{32} + \rho_{33}) = -(\mu_1^2 + \mu_2^2 + \mu_3^2)$$

$$2 = \rho_{31}\rho_{32} + \rho_{31}\rho_{33} + \rho_{32}\rho_{33} = \mu_1^2\mu_2^2 + \mu_1^2\mu_3^2 + \mu_2^2\mu_3^2$$

$$-1 = -(\rho_{31}\rho_{32}\rho_{33}) = -(\mu_1^2\mu_2^2\mu_3^2).$$

Since

$$\mu_1 + \mu_2 + \mu_3 = -a$$

$$\mu_1\mu_2 + \mu_1\mu_3 + \mu_2\mu_3 = b$$

$$\mu_1\mu_2\mu_3 = -c$$

it follows that

$$\begin{aligned} 1 &= -(a^2 - 2b) \\ 2 &= b^2 - 2ac \\ -1 &= -c^2 \end{aligned}$$

Eliminating c and a :

$$\begin{aligned} b^2 - 2 &= 2ca \\ b^4 - 4b^2 - 4 &= 4c^2 a^2 = 4(2b - 1) \\ b^4 - 4b^2 - 8b + 8 &= 0. \end{aligned}$$

This has no rational solutions for b . Thus ρ_3 has no square root in $\mathbb{Q}[\alpha]$.

Suppose $\rho_3 = \pm\mu^p$ for odd prime p . Again only the plus sign needs to be considered. In fact $N(\rho_3) = N(\mu)^p$ implies $N(\mu) = 1$. Suppose μ has minimal polynomial $x^3 + ax^2 + bx + 1$. Proceeding as before

$$\begin{aligned} 1 &= -(\mu_1^p + \mu_2^p + \mu_3^p) \\ 2 &= \mu_1^p \mu_2^p + \mu_1^p \mu_3^p = \mu_2^p \mu_3^p \\ -1 &= -1 \end{aligned}$$

The complete expansion of the right hand side in terms of a and b for a general odd prime p is too complex to work with. The following procedure will reduce the possibilities for p . Now

$$(\mu_1 + \mu_2 + \mu_3)^p = \mu_1^p + \mu_2^p + \mu_3^p + ph(\mu_1, \mu_2, \mu_3)$$

where $h(\mu_1, \mu_2, \mu_3)$ is a symmetric polynomial in μ_1, μ_2, μ_3 and

hence in Z . The factor of p comes from the binomial coefficients in the expansion of $(\mu_1 + \mu_2 + \mu_3)^p$. Thus

$$1 \equiv -(-a)^p \equiv a \pmod{p}.$$

Similarly

$$2 \equiv b^p \equiv b \pmod{p}.$$

Now

$$\mu^p \pm 1 = \rho_3 \pm 1$$

Thus $\rho_3 \pm 1$ is the product of algebraic integers in $Q[\alpha]$ one of which is $\mu \pm 1$. This implies $N(\mu \pm 1)$ divides $N(\rho_3 \pm 1)$ in Z . Computing norms as in Example 28 with $1, \rho_3, \rho_3^2$ as a basis for $Q[\alpha]$

$$N(\rho_3 \pm 1) = \begin{vmatrix} \pm 1 & 1 & 0 \\ 0 & \pm 1 & 1 \\ 1 & -2 & -1 \pm 1 \end{vmatrix} = \pm 3.$$

The norm for $\mu \pm 1$ is computed with $1, \mu, \mu^2$ as a basis

$$N(\mu \pm 1) = \begin{vmatrix} \pm 1 & 1 & 0 \\ 0 & \pm 1 & 1 \\ 1 & -b & -a \pm 1 \end{vmatrix} = 1 - a \pm 1 \pm b.$$

Summing up the conditions on a and b

$$a \equiv 1 \pmod{p}$$

$$b \equiv 2 \pmod{p}$$

$$2 - a + b \mid 3$$

$$-a - b \mid -3 .$$

Now $2 - a + b \equiv 3 \pmod{p}$ and $-a - b \equiv -3 \pmod{p}$. Thus the only solution for these four conditions is $a=1$ and $b=2$. This solution gives μ the same minimal polynomial as ρ_3 . This is not possible since $\rho_3^3 \neq \rho_3$. Thus ρ_3 is a fundamental unit for $\mathbb{Q}[\alpha]$.

CHAPTER V

CONCLUSION

The concept of an algebraic integer arose in part as an aid to solving certain Diophantine equations. The following examples give some indication of how this is done. The first example is due to Fermat and makes use of the properties of norm and conjugate.

Example 88. Consider the Diophantine equation $y^2 + 2 = x^3$. Let $y + \sqrt{-2}$ and $a + b\sqrt{-2}$ be algebraic integers in $\mathbb{Q}[\sqrt{-2}]$ such that

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3. \quad (89)$$

Then

$$N(y + \sqrt{-2}) = N(a + b\sqrt{-2})^3$$

Or

$$y^2 + 2 = \left(N(a + b\sqrt{-2}) \right)^3.$$

Thus $x = N(a + b\sqrt{-2}) = a^2 + 2b^2$ gives an equation equivalent to the original problem. The equation that corresponds to Equation 89 with the conjugates of $y + \sqrt{-2}$ and $a + b\sqrt{-2}$ is

$$y - \sqrt{-2} = (a - b\sqrt{-2})^3 \quad (90)$$

Eliminating y from Equations 89 and 90 gives

$$1 = b(3a^2 - 2b^2).$$

Since 1 factors into 1^2 or $(-1)^2$ there are two possible systems of equations to solve for a and b . The system

$$-1 = b \quad \text{and} \quad -1 = 3a^2 - 2b^2$$

has no solution in \mathbb{Z} . The alternative choice

$$1 = b \quad \text{and} \quad 1 = 3a^2 - 2b^2$$

has the solution $b=1$ and $a=\pm 1$. Thus $x = 1+2 = 3$ and $y = \pm 5$.

This next example concludes the discussion begun on page 1 of the thesis.

Example 91. Consider the Diophantine equation $x^2 - 2y^2 = 17$. This is equivalent to finding all the algebraic integers in $\mathbb{Q}[\sqrt{2}]$ with norm 17. It has already been noted that the number $7+4\sqrt{2}$ has norm 17. If μ is a unit in $\mathbb{Q}[\sqrt{2}]$ then

$$N(\mu(7+4\sqrt{2})) = N(\mu)N(7+4\sqrt{2}) = 17.$$

Since there is an infinite number of units with norm 1 in $\mathbb{Q}[\sqrt{2}]$ there is an infinite number of solutions to $x^2 - 2y^2 = 17$. A fundamental unit for $\mathbb{Q}[\sqrt{2}]$ is $1+\sqrt{2}$. Now $N(1+\sqrt{2}) = -1$ thus the units with norm plus one are

$$\pm(1+\sqrt{2})^{2n} = \pm(3+2\sqrt{2})^n \quad n \in \mathbb{Z}.$$

So

$$\pm(7+4\sqrt{2})(3+2\sqrt{2})^n \quad n \in \mathbb{Z}$$

are algebraic integers in $\mathbb{Q}[\sqrt{2}]$ with norm 17. If $\pm(7+4\sqrt{2})(3+2\sqrt{2})^n$ is expanded and written in the form $a+b\sqrt{2}$ then a, b is a solution for $x^2 - 2y^2 = 17$.

Many Diophantine equations can be transformed into an equivalent problem of finding all the algebraic integers in a given algebraic number field with some fixed norm. This method is discussed in Borevich and Shafarevich [5]. One of the earliest problems to be approached through algebraic number theory was Fermat's conjecture:

$$x^n + y^n = z^n \quad xyz \neq 0 \quad n > 2$$

has no solution in \mathbb{Z} for x, y and z . The problem is still unsolved, but many interesting facts and ideas came to light as a result of efforts to solve Fermat's problem. One of these facts concerns the factoring of algebraic integers.

If α, β and γ are algebraic integers such that $\alpha\beta = \gamma$ then α and β are called factors of γ or α divides γ . Just as in factoring in \mathbb{Z} , every algebraic integer ψ in $\mathbb{Q}[\theta]$ has as factors all the units in $\mathbb{Q}[\theta]$ and numbers of the form $\mu\psi$ where μ is a unit in $\mathbb{Q}[\theta]$. If ψ has no other factors then ψ is called prime.

Theorem 92. If ψ is an algebraic integer in $\mathbb{Q}[\theta]$ and $N(\psi) = p$ where p is a prime in \mathbb{Z} then ψ is a prime in $\mathbb{Q}[\theta]$.

Proof. Suppose $\alpha\beta = \psi$ where α and β are algebraic integers in $\mathbb{Q}[\theta]$ then

$$N(\alpha\beta) = N(\alpha)N(\beta) = N(\psi) = p.$$

Since $N(\alpha)$ and $N(\beta)$ are in \mathbb{Z} one of them is ± 1 . Suppose

$N(\alpha) = \pm 1$ then α is a unit. Thus $\beta = \alpha^{-1}\psi$ where α^{-1} is a unit.

Example 93. Consider the algebraic integers in $\mathbb{Q}[\sqrt{-5}]$. The following discussion demonstrates a method for proving a number is a prime in $\mathbb{Q}[\sqrt{-5}]$. Consider $1 - \sqrt{-5}$. Suppose

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1 - \sqrt{-5}$$

Then

$$N(a + b\sqrt{-5})N(c + d\sqrt{-5}) = N(1 - \sqrt{-5})$$

or

$$(a^2 + 5b^2)(c^2 + 5d^2) = 6$$

Thus $a^2 + 5b^2$ is a factor of 6. If $a^2 + 5b^2 = 1$ then $a + b\sqrt{-5}$ is a unit. If $a^2 + 5b^2 = 6$ the other number is a unit. Neither $a^2 + 5b^2 = 2$ nor $a^2 + 5b^2 = 3$ has a solution. Thus $1 - \sqrt{-5}$ is a prime. Similarly $1 + \sqrt{-5}$, 2 and 3 can be shown to be prime in $\mathbb{Q}[\sqrt{-5}]$. Now

$$2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$$

Since ± 1 are the only units in $\mathbb{Q}[\sqrt{-5}]$ the number 6 has two distinct factorizations into primes.

For a time some mathematicians thought they had solved Fermat's problem. Then they discovered that factorization was not unique in the algebraic number field they used. Attempts to repair proofs led to ideal theory. Factoring algebraic integers is discussed in Koper [11].

The problem of finding units in algebraic number fields still interests mathematicians. In 1969 Bernstein developed an algorithm for finding independent units in certain types of algebraic number

fields [3]. This algorithm gives a method for finding a complete set of independent units for the given field. The algorithm is a variation of the continued fraction algorithm used for finding units in quadratic and cubic extensions. However Bernstein was not able to determine whether the units obtained were fundamental.

A SELECTED BIBLIOGRAPHY

- 1 Albert, A. A. "The Integers of Normal Quartic Fields." Annals of Mathematics, Vol. 31, 2nd series (1930), pp. 381-418.
- 2 Albert, A. A. "A Determination of the Integers in All Cubic Fields." Annals of Math, Vol. 31, 2nd series (1930), pp. 550-566.
- 3 Bernstein, Leon and Hasse, Helmut. An Explicit Formula for the Units of an Algebraic Number Field of Degree ≥ 2 . Pacific Journal of Mathematics, Vol. 30, No. 2 (1969), pp. 293-365.
- 4 Berwick, W. E. H. Integral Bases. Stechert-Hafner Service Agency, New York and London, 1964.
- 5 Borevich and Shafarevich. Number Theory. New York and London: Academic Press, 1966.
- 6 Clark, Allen. Elements of Abstract Algebra. Belmont, California: Wadsworth Publishing Company, 1971.
- 7 Delone, B. N. and Faddeev, D. K. The Theory of Irrationalities of the Third Degree. Providence: American Mathematical Society, 1964.
- 8 Dickson, L. E. History of the Theory of Numbers. Washington, Carnegie Institute, Vol. I, II, III, 1919.
- 9 Grosswald, Emil. Topics from the Theory of Numbers. New York: The Macmillan Company, 1966.
- 10 Hancock, Harris. Foundations of the Theory of Algebraic Numbers, Vol. I and II, New York: Dover Publications, Inc., 1931.
- 11 Koper, Verlin F. "Factoring Algebraic Integers." (unpublished Doctoral thesis, Oklahoma State University, 1971).
- 12 Mordell, L. J. Diophantine Equations. New York and London: Academic Press, 1969.
- 13 Pollard, H. The Theory of Algebraic Numbers. Carus Mathematical Monograph No. 9, New York: Mathematical Association of America, 1950, New York: John Wiley and Sons, Inc.
- 14 Reid, L. W. Elements of the Theory of Algebraic Numbers. New York: The Macmillan Company, 1910.

- 15 Samuel, Pierre. Algebraic Theory of Numbers. Boston: Houghton Mifflin Company, 1970.
- 16 Stark, Harold M. An Introduction to Number Theory. Chicago: Markham Publishing Company, 1970.
- 17 Uspensky, J. V. A Method for Finding Units in Cubic Extensions With Negative Discriminant. Translation American Mathematical Society, Vol. 33 (1931), pp. 1-22.
- 18 Zariski, Oscar and Samuel, Pierre. Commutative Algebra, Vol. I, Princeton: D. Van Nostrand Company, Inc., 1958.
- 19 Zelinsky, Daniel. A First Course in Linear Algebra. New York: Academic Press, 1968.

VITA

Robert Edward Dahlin

Candidate for the Degree of

Doctor of Education

Thesis: ALGEBRAIC INTEGERS, UNITS AND INTEGRAL BASES

Major Field: Higher Education

Biographical:

Personal Data: Born in St. Paul, Minnesota, October 2, 1934,
the son of Mr. and Mrs. Arthur B. Dahlin.

Education: Graduated from John A. Johnson High School,
St. Paul, Minnesota in June 1952; attended the University
of Minnesota from 1955-1963; received the Bachelor of
Applied Mathematics degree from the University of
Minnesota in 1960; received the Master of Science degree
from the University of Minnesota in 1963 with a major in
mathematics; completed requirements for the Doctor of
Education degree at Oklahoma State University in May,
1972.

Professional Experience: Graduate teaching assistant, Institute
of Technology, University of Minnesota, 1960-63;
Instructor, Department of Mathematics, Wisconsin State
University, Superior, 1963-65; Assistant Professor,
Department of Mathematics, University of Wisconsin,
Superior, 1967 to present; Member of the Mathematical
Association of America since 1969.