FACTORING ALGEBRAIC INTEGERS

By

VERLIN F. KOPER

Bachelor of Science
Southwestern State College
Weatherford, Oklahoma
1961

Master of Arts
University of Missouri
Columbia, Missouri
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
July, 1971

FACTORING ALGEBRAIC INTEGERS

Thesis Approved:

Gerald H. Goff
Thesis Adviser
John Jewett
R. J. Alciatore
W. Ware Morsden
Dennis Berthold
D. Dunham
Dean of the Graduate College

ACKNOWLEDGEMENTS

To Professor Gerald Goff, my thesis adviser, my thanks for his personalized effort to help and guide me with this dissertation, not just during regular school hours but at many other times as well.

I also wish to thank Professor John Jewett for serving as my committee chairman. For their suggestions and cooperation my gratitude goes to the other members of my committee: Dr. Dennis Bertholf, Dr. Robert Alciatore and Dr. Ware Marsden.

Linda, my wife, has now completed her fifth year of giving her encouragement and support as a graduate student's wife. She and our son, Seth, have made many sacrifices during this time, all of which I sincerely appreciate.

TABLE OF CONTENTS

CHAPTER I

HISTORY OF ALGEBRAIC NUMBER THEORY

Number theory and in particular algebraic number theory has traditionally been a reservoir of ideas in the development of algebra. An excellent example of this can be seen in the work of the German mathematician, E. Kummer (1810, 1893). In his unsuccessful attempt to prove Fermat's last theorem he extended the domain of number theory to include not only the rational but also the algebraic numbers and eventually to ideals of algebraic integers. It was Dedekind who first introduced the notions of algebraic integer and ideal [4] but it was Kummer who did most of the original work with these ideas in relation to Fermat's last theorem.

Fermat's last theorem states that the equation $x^n + y^n = z^n$ has no solution in positive integers if $n > 2$. In 1843 Kummer thought he had a proof of this theorem, however Lejeunne-Dirichlet picked out the error in his reasoning, namely that unique factorization may no longer hold in algebraic number fields [5]. This failure caused Kummer to attack the problem with redoubled vigor. A few years later he found a substitute for the fundamental theorem of arithmetic which was unique factorization of ideals, the theory of which later gained importance in many parts of mathematics. It is this theory with which this dissertation is essentially concerned.

The algebraic number fields in which Kummer was interested were the minimal field extensions of the rationals to include a primitive p^{th} root of unity, θ, where p was a prime. It so happens that if $p < 23$ the field extension does have the unique factorization property [6]. Therefore the proof of Fermat's theorem which Kummer submitted to Dirichlet would have been valid in the case where the exponent is a prime less than 23.

Since Kummer there have been numerous criteria developed by which Fermat's theorem has been proven for exponents at least up to 600 [5].

Borevich and Shafarevich [7] give a "proof" of part of Fermat's theorem using the false assumption of unique factorization. The part they prove is that if p is a prime, the equation $x^p + y^p = z^p$ has no solution in rational integers not divisible by p. LeVeque [8] proves Fermat's last theorem for the special case of $n = 3$ using algebraic number theory.

CHAPTER II

AN INVESTIGATION OF THE FUNDAMENTAL THEOREM OF ARITHMETIC IN RELATION TO AN EXPANDED DEFINITION OF AN INTEGER

Some basic definitions and results are needed.

Definition 2.1. A nonempty set of elements F forms a field F if there are two binary operations $+$ and $\cdot$ defined in F such that:

(1) F is an abelian group with respect to $+$.

(2) F with the additive identity omitted forms an abelian group with respect to $\cdot$.

(3) $a(b+c) = ab+ac$ for all $a, b, c \in F$.

Definition 2.2. A polynomial is monic if the coefficient of the highest powered term is 1.

Definition 2.3. A polynomial $p(x)$ with coefficients in a field F is irreducible over F if when $p(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are polynomials with coefficients in F, then one of $a(x)$ or $b(x)$ is a constant.

Definition 2.4. The polynomial $p(x)$ is a minimal polynomial for the number θ if:

(1) θ is a zero of $p(x)$.

(2) $p(x)$ is monic.

(3) $p(x)$ is irreducible.

As examples, $x - 1/2$ and $x^2 + 1$ are minimal polynomials for $1/2$ and i respectively.

Throughout this chapter the primary concern will be with the field of rational numbers which will be denoted by R. If the reader finds it more readable to think of the arbitrary field F as the field of rational numbers R in the above definitions and in future work in this chapter, then nothing will be lost in so doing.

It should be noted that a set of numbers K is a field if when α and β belong to K then so do $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, and α/β, if $\beta \neq 0$.

Let the set of all polynomials with coefficients in a field F be denoted by $F[x]$.

Definition 2.5. θ is algebraic over the field F if θ is a zero of a polynomial of $F[x]$.

Definition 2.6. θ is an algebraic number if θ is algebraic over the field R.

Definition 2.7. θ is an algebraic integer if it is an algebraic number over R and its minimal polynomial has only rational integers as coefficients.

As an illustration of the preceding definitions, it is seen that $x^2 - 5$ is a member of $R[x]$ and since $\sqrt{5}$ is a zero of $x^2 - 5$, it is an algebraic number. Further, since $x^2 - 5$ is monic, irreducible and has rational integer coefficients $\sqrt{5}$ is an algebraic integer.

Every rational integer $(\ldots, -1, 0, 1, 2, \ldots)$ is an algebraic integer and hence the rational integers are a subset of the algebraic integers. Rational numbers of the form a/b with $b > 1$ and $(a, b) = 1$ are algebraic numbers but not algebraic integers since $x - a/b$ is the minimal polynomial for a/b but does not have rational integer coefficients. Since it can be shown (see Herstein, [10]) that $x^2 + x + 1$ is irreducible, $\frac{1 \pm i\sqrt{3}}{2}$ are both algebraic integers.

As can be seen, there could be confusion between the terms rational integer and algebraic integer. The convention of the literature will be adopted where the term integer will be used in its broad sense of algebraic integer and the term rational integer is used for members of the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Pollard [9] proves that there exists numbers which are not algebraic numbers and in particular proves that the number represented by the series $\sum_{m=1}^{\infty} (-1)^m 2^{-m!}$ is not an algebraic number. Numbers which are not algebraic numbers are called transcendental. An interesting occurence is that the algebraic numbers are countable whereas the transcendental numbers are not. An easy proof of this occurs if one notes that the set of all complex and real numbers are uncountable whereas the set of polynomials in $R[x]$ and hence the set of algebraic numbers are countable, since R is countable.

In the material which follows, the following theorems are needed.

Definition 2.8. A polynomial in $R[x]$ is primitive if it has rational integer coefficients and the greatest common divisor of the set of coefficients is 1.

Theorem 2.9. The product of primitive polynomials is primitive.

Proof: See Herstein [10].

Theorem 2.10. If a polynomial with rational integral coefficients can be factored over R, it can be factored into polynomials with rational integral coefficients.

Proof: See Herstein [10].

Theorem 2.11. If β is a root of a monic polynomial equation with rational integer coefficients then β is an algebraic integer.

Proof: Let $p(x)$ be the above described polynomial, then if $p(x)$ is irreducible we are done. If $p(x)$ is reducible, then by Theorem 2.10 one can write $p(x) = (a_r x^r + \ldots + a_0)(b_q x^q + \ldots + b_0)$ where $r+q$ is the degree of $p(x)$, $p > 0$, $q > 0$ with $a_0, \ldots, a_r$, $b_0, \ldots, b_q$ all rational integers. Since $a_r b_q x^{r+q}$ is the highest powered term of $p(x)$ it must occur that $a_r b_q$ is 1 and since a_r and b_q are rational integers, without loss of generality, they are both 1. $a_r x^r + \ldots + a_0$ and $b_q x^q + \ldots + b_0$ are therefore both monic. Since β is a zero of $p(x)$ it must be a zero of one of the above monic factors of $p(x)$. Repeating the preceding argument it is seen that in a finite number of steps one must arrive at a monic polynomial with rational integral coefficients which is irreducible and has β as a zero. Hence β is an algebraic integer.

The Basic Problem of Algebraic Number Theory

The basic problem of algebraic number theory is to extend the meaning of integer and to determine if there is a valid analog to the fundamental theorem of arithmetic. It has been defined what is meant by an algebraic integer so next is the investigation of the fundamental theorem of arithmetic with respect to algebraic integers.

First, two definitions are needed.

Definition 2.12. Let ϵ be an integer (algebraic) then ϵ is a unit if there is an integer β such that $\epsilon\beta = 1$. α and β are associates if and only if $\alpha = \epsilon\beta$ for some unit ϵ.

Theorem 2.13. A finite product of units is again a unit.

Proof: It will be shown in Theorem 3.10 using only preceding work that the finite product of integers is again an integer. Assuming this for now, let $\epsilon_1, \ldots, \epsilon_n$ be units. There are then integers $\beta_1, \ldots, \beta_n$ such that $\epsilon_i\beta_i = 1$ for $i = 1, \ldots, n$. Now by the assumption the product $\beta_1\beta_2 \cdots \beta_n$ is an integer and

$$(\epsilon_1 \cdots \epsilon_n)(\beta_1 \cdots \beta_n) = \epsilon_1\beta_1 \cdots \epsilon_n\beta_n = 1 .$$

Therefore the product $\epsilon_1 \cdots \epsilon_n$ is a unit.

Definition 2.14. Let p be an integer then p is a prime if p is not zero or a unit and $p = ab$ with a and b integers implies that either a or b is a unit.

Fundamental Theorem of Arithmetic. Each integer not zero or a unit can be factored into the product of primes which are uniquely

determined to within order and multiplication by units.

With the new broader definition of integer as an algebraic integer it can be seen that the Fundamental Theorem of Arithmetic does not hold if one considers the set of all algebraic integers, simply because there are no primes in the set of all algebraic integers. To verify that there are no primes let α be an algebraic integer different from zero or a unit with minimal polynomial $p(x)$. Now $p(x^2)$ is a monic polynomial with rational integer coefficients and $\sqrt{\alpha}$ is a zero of $p(x^2)$, hence by Theorem 2.11, $\sqrt{\alpha}$ is an algebraic integer. Note that $\sqrt{\alpha}$ is not a unit. For, if it were there would be a product of units being a nonunit, since $\alpha = \sqrt{\alpha}\,\sqrt{\alpha}$, which is not possible by Theorem 2.13. Hence α can be written as the product of two nonunit algebraic integers and is therefore not prime.

As an example to the above one usually thinks of 3 as a prime however in the set of all algebraic integers it is not. Since $\sqrt{3}$ is a zero of $x^2 - 3$ one sees that $\sqrt{3}$ is an integer. Further 3 is not zero or a unit since if $3 \cdot \alpha = 1$ then α is $1/3$ but as noted earlier, $1/3$ is not an algebraic integer. Theorem 2.13 may be used to argue that $\sqrt{3}$ is not a unit or it can be assumed that there is an α such that $\alpha \cdot \sqrt{3} = 1$ and then show that $3x^2 - 1$ is the irreducible polynomial over R for α and hence α is not an algebraic integer since its minimal polynomial is not monic.

A much more interesting situation occurs when one restricts their attention to a simple algebraic extension of R.

Definition 2.15. If θ is algebraic over a field F then $K = F(\theta)$ is the smallest field containing both F and θ. K is called either a

simple algebraic extension of F or an algebraic extension of degree 1.

Even though it is not important to this discussion, if it is of concern to the reader, it will be proven in Theorem 3.20 that any finite algebraic extension of the field of rational numbers is a simple algebraic extension.

Definition 2.16. An algebraic number field is any simple algebraic extension of the field of rational numbers.

I should be useful to now consider in some detail $R(\sqrt{-5})$ in relation to the fundamental theorem of arithmetic.

Consider $\{a+b\sqrt{-5} \mid a, b \in R\}$. Since there is closure of addition, subtraction, multiplication and nonzero division this set is a field. It contains R and $\sqrt{-5}$ and since any field which does so must contain all sums and products of such elements, it follows that $\{a+b\sqrt{-5} \mid a, b \in R\}$ is the simple algebraic extension of R to include $\sqrt{-5}$ and therefore

$$R(\sqrt{-5}) = \{a+b\sqrt{-5} \mid a, b \in R\}.$$

It will next be shown that $3, 7, 1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are all prime integers in $R(\sqrt{-5})$ but notice

$$21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

and hence the fundamental theorem of arithmetic does not hold in $R(\sqrt{-5})$.

To confirm that $3, 7, 1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are all prime notice first that they are respectively zeros of the monic primitive

polynomials $x-3$, $x-7$, $x^2-2x+21$ and $x^2-2x+21$ and hence are algebraic integers by Theorem 2.11.

Next it will be shown that the only algebraic integers in $R(\sqrt{-5})$ are of the form $a+b\sqrt{-5}$ with a and b rational integers. Suppose that $a+b\sqrt{-5}$ is an algebraic integer with a and b rational numbers, one can then write $a+b\sqrt{-5} = \frac{\ell+m\sqrt{-5}}{n}$ with ℓ, m and n rational integers, $n>0$ and $((\ell,m),n)=1$. Now since $a+b\sqrt{-5}$ is a zero of a quadratic polynomial, $\frac{\ell+m\sqrt{-5}}{n}$ must be a zero of x^2+fx+c for some choice of rational integers f and c if it is to be an algebraic integer. Therefore one must have

$$(\ell+m\sqrt{-5})^2 + fn(\ell+m\sqrt{-5}) + cn^2 = 0 \quad \text{or}$$

$$* \quad \ell^2 - 5m^2 + fn\ell + cn^2 = 0 \quad \text{and} \quad m(2\ell+fn) = 0 \ .$$

Now if $m=0$ then $a+b\sqrt{-5} = \ell/n$ which is not an algebraic integer unless n divides ℓ, but since by hypothesis $((\ell,m),n) = ((\ell,0),n) = 1$, one sees that n is 1 and hence both a and b are rational integers. Next if $m \neq 0$ by the second equation of *, $fn = -2\ell$ so that the first equation of * becomes:

$$-5m^2 - \ell^2 + cn^2 = 0 \ .$$

Now let $(\ell,n)=d$, then d^2 divides $-5m^2$. Therefore d divides m but by hypothesis $((\ell,m),n)=1$ hence $d=1$. Therefore ℓ and n have no common factors larger than 1 but since $fn=-2\ell$ this implies that ℓ divides f which in turn implies $n=1$ or 2 since $n>0$. If $n=1$ then a and b are integers. If $n=2$ then $\frac{\ell+m\sqrt{-5}}{2}$ satisfies the quadratic equation

$$x^2 - \ell x + \frac{\ell^2 + 5m^2}{4} = 0$$

and consequently is an algebraic integer only if $\ell^2 + 5m^2 \equiv 0 \bmod 4$ which implies $\ell^2 + m^2 \equiv 0 \bmod 4$. Now since $(\ell, n) = 1 = (\ell, 2)$ this implies ℓ is odd. Let $\ell = 2t + 1$, the congruence then becomes:

$$4t^2 + 4t + 1 + m^2 \equiv 0 \bmod 4 .$$

This in turn becomes:

$$1 + m^2 \equiv 0 \bmod 4 .$$

Now if m is even the above is impossible. If m is odd, $m = 2p + 1$ and the congruence then becomes

$$1 + 4p^2 + 4p + 1 \equiv 0 \bmod 4$$

which says $2 \equiv 0 \bmod 4$ an impossibility. It now follows that $n = 1$ and hence $a + b\sqrt{-5}$ is such that a and b are rational integers if $a + b\sqrt{-5}$ is an algebraic integer.

It is next shown that $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ are not units, in fact it is shown that ± 1 are the only units in $R(\sqrt{-5})$.

If $\alpha = a + b\sqrt{-5}$ is an algebraic integer in $R(\sqrt{-5})$, define $N(\alpha) = a^2 + 5b^2$. With α and β both algebraic integers in $R(\sqrt{-5})$, it is easily seen that $N(\alpha\beta) = N(\alpha)N(\beta)$. An algebraic integer α is a unit in $R(\sqrt{-5})$ if and only if $N(\alpha) = 1$. The proof is as follows. Let α be a unit in $R(\sqrt{-5})$, there is then an integer β in $R(\sqrt{-5})$ such that $\alpha\beta = 1$. Now $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$ and since $N(\alpha)$ and $N(\beta)$ are positive rational integers, by definition of $N(\alpha)$ and $N(\beta)$, it is seen that $N(\alpha) = 1$. Now if $N(\alpha) = 1$ then $a^2 + 5b^2 = 1$, but a and b

rational integers implies b must be zero for the equation to be satisfied, hence $a = \pm 1$ and therefore $\alpha = 1$ or -1, both of which are units. Now $N(3) = 9$, $N(7) = 21$, $N(1+\sqrt{-5}) = 21$ $N(1-2\sqrt{-5}) = 21$ and hence none of $3, 7, 1+2\sqrt{-5}$ or $1-2\sqrt{-5}$ are units.

There is now only to show that $3, 7, 1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are all prime in the field $R(\sqrt{-5})$.

Suppose $3 = \alpha \cdot \beta$ where α, β are integers in $R(\sqrt{-5})$ which are not units. Then $9 = N(3) = N(\alpha\beta) = N(\alpha)N(\beta)$, and hence $N(\alpha) = 3$ and $N(\beta) = 3$ since $N(\alpha)$ and $N(\beta)$ are positive rational integers not equal to 1. If $\alpha = a + b\sqrt{-5}$, it follows that $a^2 + 5b^2 = 3$ which is impossible since if $b \neq 0$ then $a^2 + 5b^2 > 3$ and if $b = 0$ then $a^2 = 3$. Which is not possible since a is a rational integer. Similarly, $7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ are also prime.

The original goal has been reached and is now restated for emphasis.

In the algebraic number field $R(\sqrt{-5})$ the fundamental theorem of arithmetic does not hold since $3, 7, 1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ are all prime integers in $R(\sqrt{-5})$ and yet,

$$21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5}).$$

It is therefore seen that there is no possibility for the fundamental theorem of arithmetic to hold in all simple algebraic extensions of R. However, according to Shanks [6], if θ is a primitive p^{th} root of unity where p is a prime, then the fundamental theorem of arithmetic does hold in $R(\theta)$ for $p < 23$.

It will also be shown that the fundamental theorem of arithmetic will hold when certain collections of algebraic integers called ideals are considered. This will require further development.

CHAPTER III

PRELIMINARY CONCEPTS TO IDEAL THEORY

Symmetric Polynomials

In Theorem 2.13 it was needed that the finite product of integers is an integer. In what follows it shall be proven that the sum, difference and product of algebraic integers are again algebraic integers.

Definition 3.1. A polynomial $P(x_1, \ldots, x_n)$ is symmetric in its n variables if it is unchanged by any of the n! permutations of the variables $x_1, \ldots, x_n$.

Definition 3.2. Given a set $x_1, \ldots, x_n$ then the set of σ_i, $i = 1, \ldots n$ given below are called the elementary symmetric functions.

$$\sigma_1 = x_1 + x_2 + \ldots + x_n$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_ix_j + \ldots + x_{n-1}x_n \quad \text{where} \quad 1 \leq i < j \leq n$$

$$\vdots$$

$$\sigma_i = \text{sum of all products of } i \text{ different } x_j,\ j = 1, 2, \ldots, n$$

$$\vdots$$

$$\sigma_n = x_1x_2 \cdots x_n$$

Theorem 3.3. If $f_n(z) = (z - x_1)(z - x_2) \cdots (z - x_n)$ then $f_n(z) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots (-1)^n \sigma_n$

Proof: Induct on n. For $n=1$ the result is obvious therefore assume true for all $k<n$ then

$$f_n(z) = f_{n-1}(z)(z-x_n)$$

$$= \left(z^{n-1} - \sigma_1' z^{n-2} + \ldots + (-1)^r \sigma_r' z^{n-r-1} + \ldots + (-1)^{n-1}\sigma_{n-1}'\right)(z-x_n)$$

where σ_r' = sum of all products of r different x_j, $j=1,2,\ldots,n-1$. Now look at the term involving z^{n-r} in $f_n(z)$ and confirm that its coefficient is indeed $(-1)^r\sigma_r$. That term is given by:

$$(-1)^{r-1}\sigma_{r-1}' z^{n-r}(-x_n) + (-1)^r\sigma_r' z^{n-r-1}(z) = (-1)^r z^{n-r}(\sigma_r' + \sigma_{r-1}' x_n)$$

$$= (-1)^r\sigma_r z^{n-r}.$$

Theorem 3.4. Any polynomial $P(x_1,\ldots,x_n)$ which is symmetric in $x_1,\ldots,x_n$ is equal to a polynomial with rational integral coefficients in the coefficients of P and the elementary symmetric functions $\sigma_1,\sigma_2,\ldots,\sigma_n$. Examples:

$$x_1^2+x_2^2+x_3^2 = (x_1+x_2+x_3)^2 - 2(x_1x_2+x_1x_3+x_2x_3) = \sigma_1^2 - 2\sigma_2$$

$$\sqrt{2}\,x_1^3x_2 + \sqrt{2}\,x_1x_2^3 = \sqrt{2}\,(x_1+x_2)^2(x_1x_2) - 2\sqrt{2}\,(x_1x_2)^2$$

$$= 1(\sqrt{2}\,\sigma_1^2\sigma_2) - 2(\sqrt{2}\,\sigma_2^2)$$

Proof: A polynomial $P(x_1,\ldots,x_n)$ is homogeneous if for every summand $cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ in P, $k=k_1+k_2+\ldots+k_n$ is the same fixed rational integer. An example is: $P(x_1,x_2)=x_1^3x_2+x_1x_2^3+x_1^4+x_2^4$.

The proof shall be restricted to proving the theorem for a homogeneous polynomial P, since if P is not homogeneous it is a sum of homogeneous functions. If each of these homogeneous polynomials is equal to a polynomial with rational integral coefficients in the coefficients of P and the elementary symmetric functions then their sum is such a polynomial.

Further, it is assumed that if both $h = a x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ and $L = b x_1^{\ell_1} x_2^{\ell_2} \dots x_n^{\ell_n}$ are summands of P then the permutations $(k_1, k_2, \dots, k_n)$ and $(\ell_1, \ell_2, \dots, \ell_n)$ are different for if not h and L can be combined into a single term of P. Now h is called a higher term than L if the first nonzero number in the sequence $k_1 - \ell_1, k_2 - \ell_2, \dots, k_n - \ell_n$ is positive.

If h is the highest term of P then $k_1 \geq k_2 \geq \dots \geq k_n$. For if $k_1 < k_2$ then since P is symmetric $a x_1^{k_2} x_2^{k_1} x_3^{k_3} \dots x_n^{k_n}$ is also a summand of P and hence h would not be the highest term in P. Similarly, if $k_i < k_{i+1}$, $i < n$ then since P is symmetric

$$a x_1^{k_1} \dots x_{i-1}^{k_{i-1}} x_i^{k_{i+1}} x_{i+1}^{k_i} x_{i+2}^{k_{i+2}} \dots x_n^{k_n}$$

is a summand of P which is higher than h, a contradiction to the choice of h.

If the highest term in another homogeneous symmetric polynomial P' is $h' = a' x_1^{k'_1} \dots x_n^{k'_n}$ then the highest term in the product PP' is $hh' = a a' x_1^{k_1+k'_1} \dots x_n^{k_n+k'_n}$. Hence, the highest term in a product of homogeneous symmetric polynomials is the product of their highest terms. Now the highest terms in $\sigma_1, \sigma_2, \dots, \sigma_n$ are $x_1, x_1x_2, x_1x_2x_3, \dots, x_1x_2 \cdots x_n$ respectively. Hence the highest term

in $\sigma_1^{q_1}\sigma_2^{q_2}\cdots\sigma_n^{q_n}$ is $x_1^{q_1+\cdots+q_n}x_2^{q_2+\cdots+q_n}\cdots x_n^{q_n}$. Thus the highest term in

$$\Sigma_0 = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$$

is $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ which is h. Hence $P_1 = P - \Sigma_0$ is either identically zero or a homogeneous symmetric polynomial of the same degree k as P and having a highest term h_1 not as high as h. If $P_1 \not\equiv 0$ repeat the argument to get $P_2 = P_1 - \Sigma_1$, where

$$\Sigma_1 = h_1 = a_1x_1^{p_1}\cdots x_n^{p_n} = a_1\sigma_1^{p_1-p_2}\sigma_2^{p_2-p_3}\cdots\sigma_n^{p_n}$$

and P_2 is a symmetric polynomial of the same degree k as P_1 whose highest term h_2 is not as high as h_1 or $P_2 \equiv 0$. Since all terms of P were of degree k and there are only a finite number of such terms there must finally be a Σ_t such that $P_t - \Sigma_t \equiv 0$. Hence $P = \Sigma_0 + P_1 = \Sigma_0 + (\Sigma_1 + P_2) = \cdots = \Sigma_0 + \Sigma_1 + \ldots + \Sigma_t$. Each of the Σ_i, $i = 0, \ldots, t$ are polynomials in $\sigma_1, \ldots, \sigma_n$ and the coefficients of P and therefore P is a polynomial in elementary symmetric functions and the coefficients of P with rational integer coefficients.

It should be noted that if P has rational integer coefficients then the above theorem tells us that P is equal to a polynomial in the elementary symmetric functions with rational integer coefficients.

Theorem 3.5. Let f(x) be a polynomial of degree n over a field F of complex numbers with roots of $r_1, r_2, \ldots, r_n$ and let $P(x_1, \ldots, x_n)$ be a symmetric polynomial with coefficients in F. Then $P(r_1, \ldots, r_n)$ is an element of F.

Proof: Since the coefficients are in a field, it may be assumed that $f(x)$ has a leading coefficient of one, hence

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \ldots + a_0 \\ &= (x - r_1)(x - r_2)\cdots(x - r_n) \\ &= x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n \sigma_n . \end{aligned}$$

Now since a_i, $i = 0, 1, \ldots, n-1$ are elements of F and by the above equalities it is seen that $a_{n-1} = -\sigma_1, \ldots, a_0 = (-1)^n \sigma_n$ and hence the σ_i, $i = 1, \ldots, n$ are all elements of the field F. Theorem 3.4 implies that $P(r_1, \ldots, r_n)$ is a polynomial with rational integer coefficients in the symmetric functions and the coefficients of P which are also in F and hence $P(r_1, \ldots, r_n)$ is in F.

As an example of Theorem 3.5 let $F = R$, $f(x) = x^2 + x + 1$ and $P(x_1, x_2) = 2x_1^2 + 2x_2^2$. Now

$$r_1 = \frac{-1 + i\sqrt{3}}{2} \quad \text{and} \quad r_2 = \frac{-1 - i\sqrt{3}}{2}$$

with

$$P(r_1, r_2) = 2\left(\frac{-1 + i\sqrt{3}}{2}\right)^2 + 2\left(\frac{-1 - i\sqrt{3}}{2}\right)^2 = -2$$

an element of R as predicted.

If α is an algebraic number and $p(x)$ is the minimal polynomial of α (monic, irreducible, $p(\alpha) = 0$) then $p(x)$ is referred to as the defining polynomial of α. If α is an algebraic integer then its defining polynomial will have rational integer coefficients.

Theorem 3.6. The sum of two algebraic integers is an algebraic integer.

Proof: Let $\alpha = \alpha_1$ and $\beta = \beta_1$ be algebraic integers and have as their defining polynomials

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

and

$$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0 = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$$

respectively. Since

$$f(x-\beta_j) = (x-\beta_j)^n + a_{n-1}(x-\beta_j)^{n-1} + \ldots + a_0$$

it is seen that

$$p(x,\beta_1,\ldots,\beta_m) = \prod_{j=1}^{m} f(x-\beta_j)$$

is symmetric in $\beta_1,\ldots,\beta_m$. Therefore every coefficient must be symmetric in $\beta_1,\ldots,\beta_m$. Suppose not, then for some i such that $0 \leq i \leq mn$ the coefficient $h(\beta_1,\ldots,\beta_m)$ of x^i is not symmetric in $\beta_1,\ldots,\beta_m$. Therefore $h(\beta_1,\ldots,\beta_m) \neq h(\beta_q,\ldots,\beta_r)$ for some permutation $\beta_q,\ldots,\beta_r$ of $\beta_1,\ldots,\beta_m$. Polynomials are equal if and only if corresponding coefficients are equal and hence the above implies $p(x,\beta_1,\ldots,\beta_m) \neq p(x,\beta_q,\ldots,\beta_r)$. A contradiction to the fact that

$$p(x,\beta_1,\ldots,\beta_m) = \prod_{j=1}^{m} f(x-\beta_i)$$

is symmetric in $\beta_1,\ldots,\beta_m$.

Since each coefficient is a symmetric function in $\beta_1,\ldots,\beta_m$ and $\beta_1,\ldots,\beta_m$ are roots of a polynomial of degree m, Theorem 3.5 gives that each coefficient is an element of R.

Except for sign, the coefficients of $g(x)$ are the elementary symmetric functions of $\beta_1,\ldots,\beta_m$ according to Theorem 3.3 and since by hypothesis the coefficients of $g(x)$ are rational integers, the elementary symmetric functions in $\beta_1,\ldots,\beta_m$ are rational integers. Since each coefficient of $p(x,\beta_1,\ldots,\beta_m)$ is symmetric in $\beta_1,\ldots,\beta_m$, Theorem 3.4 implies that each coefficient is a polynomial with rational integer coefficients of the elementary symmetric functions in $\beta_1,\ldots,\beta_m$. Now, since each elementary symmetric function is a rational integer it follows that each coefficient of $p(x,\beta_1,\ldots,\beta_m)$ is a rational integer.

Hence $\alpha + \beta$ is a zero of a monic polynomial with rational integer coefficients, namely $p(x,\beta_1,\ldots,\beta_m)$ and therefore by Theorem 2.11 is an algebraic integer.

Corollary 3.7. The sum of two algebraic numbers is an algebraic number.

Proof: In the proof of Theorem 3.6 let the coefficients of $f(x)$ and $g(x)$ be rational numbers.

Theorem 3.8. The difference of two algebraic integers are algebraic integers.

Proof: Let α and β be algebraic integers with $g(x)$ the defining polynomial of β then $-\beta$ is a zero of the polynomial $g(-x)$ and therefore after multiplication of $g(-x)$ by either $+1$ or -1 it is seen that

$-\beta$ is an algebraic integer by Theorem 2.11. Theorem 3.6 implies that $\alpha + (-\beta) = \alpha - \beta$ is an algebraic integer.

Corollary 3.9. The difference of two algebraic numbers is an algebraic number.

Theorem 3.10. The product of two algebraic integers is an algebraic integer.

Proof: Let $\alpha = \alpha_1$ and $\beta = \beta_1$ be algebraic integers and have as their defining polynomials

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

and

$$g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0 = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m)$$

respectively. Let

$$P(x, \alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = \prod_{j=1}^{m} \prod_{i=1}^{n} (x - \alpha_i\beta_j) .$$

By Theorem 3.3 the coefficients of the polynomial P are the elementary symmetric functions except for sign in the quantities $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_n\beta_m$. Let $\beta_q, \ldots, \beta_r$ be a permutation of $\beta_1, \ldots, \beta_m$ then the set $\alpha_1\beta_q, \ldots, \alpha_1\beta_r, \alpha_2\beta_q, \ldots, \alpha_n\beta_r$ is a permutation of $\alpha_1\beta_1, \ldots, \alpha_n\beta_m$ and hence

$$P(x, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = P(x, \alpha_1, \ldots, \alpha_n, \beta_q, \ldots, \beta_r) .$$

Likewise for any permutation $\alpha_t, \ldots, \alpha_w$ of $\alpha_1, \ldots, \alpha_n$

$$P(x,\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m) = P(x,\alpha_t,\ldots,\alpha_w,\beta_1,\ldots,\beta_m) .$$

Let $h(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m)$ be a coefficient of P, since polynomials are equal if and only if corresponding coefficients are equal and P is symmetric in the α_i and β_j, one must have h symmetric in the α_i and β_j. Theorem 3.4 gives that h can be written as a polynomial in the elementary symmetric functions of $\beta_1,\ldots,\beta_m$ with coefficients of rational integers and functions of $\alpha_1,\ldots,\alpha_n$. Since h is also symmetric in $\alpha_1,\ldots,\alpha_n$, each of the coefficients of the polynomial in the elementary symmetric functions of $\beta_1,\ldots,\beta_m$ can be written as polynomials of the symmetric functions of $\alpha_1,\ldots,\alpha_n$ with rational integer coefficients according to Theorem 3.4. Now every symmetric function of $\alpha_1,\ldots,\alpha_n$ is an a_i, except for sign, by Theorem 3.3 and hence is a rational integer. Likewise each symmetric function of $\beta_1,\ldots,\beta_m$ is a b_i, except for sign, by Theorem 3.3 and hence is a rational integer. Now since $h(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m)$ is a polynomial in the symmetric functions of $\beta_1,\ldots,\beta_m$ with coefficients which are polynomials with rational integer coefficients in the elementary symmetric functions of $\alpha_1,\ldots,\alpha_n$ and $h(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m)$ is a rational integer. Therefore, $P(x,\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_m)$ is a monic polynomial with rational integer coefficients which has $\alpha\beta$ as a zero. Hence $\alpha\beta$ is an algebraic integer.

Corollary 3.11. The product of two algebraic numbers is an algebraic number.

The objective of proving that the sum, difference and product of algebraic integers are again algebraic integers has now been

accomplished. If in addition to Corollaries 3.7, 3.9 and 3.11 it was also known that the nonzero quotient of two algebraic numbers is an algebraic number it would then follow that the set of all algebraic numbers is a field.

Theorem 3.12. The set of all algebraic numbers is a field.

Proof: Let α and β be algebraic numbers with $\beta \neq 0$. Let $g(x)$ be the defining polynomial of β, then $\frac{1}{\beta}$ is a zero of $x^m g(\frac{1}{x})$, where m is the degree of $g(x)$, and hence $\frac{1}{\beta}$ is an algebraic number. Corollary 3.11 implies $\alpha \cdot \frac{1}{\beta}$ is an algebraic number and hence $\frac{\alpha}{\beta}$ is an algebraic number. Corollary's 3.7, 3.9 and 3.11 complete the proof.

Field Extensions

In Definition 2.15, a simple algebraic field extension was defined. A characterization of the set of elements in the extension will now be given.

Theorem 3.13. If θ is algebraic over a field F then the algebraic extension of F to include θ, $F(\theta)$ is

$$K = \left\{ \frac{f(\theta)}{g(\theta)} \mid f(x), g(x) \in F[x], g(\theta) \neq 0 \right\} .$$

Proof: The sum, difference, product and nonzero quotient of rational functions (quotient of two polynomials) is a rational function of the required form. Both F and θ belong to K and hence K is a field which contains F and θ. The fact that it is the smallest such field follows from the requirement of closure of addition, subtraction,

multiplication and non-zero division and hence, the necessity of containing all numbers of the form $\frac{f(\theta)}{g(\theta)}$ where $f(x)$ and $g(x)$ are polynomials over the field F.

With the use of the above theorem, it will be shown that a better characterization of $F(\theta)$ can be obtained; namely, that every element of $F(\theta)$ can be written as a polynomial in θ.

Definition 3.14. If θ is an algebraic number with minimal polynomial $p(x)$ of degree n, then θ is said to be of degree n over F.

Theorem 3.15. If θ is of degree n over F and α is any element of $F(\theta)$ then α can be written uniquely in the form

$$\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$$

where a_i, $i = 0, \ldots, n-1$ are elements of F.

Proof: By Theorem 3.13, $\alpha = \frac{f(\theta)}{g(\theta)}$ for some polynomials $f(x)$ and $g(x)$ in $F[x]$ with $g(\theta) \neq 0$. Let $p(x)$ be the defining polynomial of θ, then since $p(x)$ is irreducible $g(x) \nmid p(x)$ unless $g(x) = p(x)$. This cannot happen since $g(\theta) \neq 0$ and $p(\theta) = 0$. If $p(x) \mid g(x)$ this implies $g(\theta) = 0$ which cannot happen, hence $p(x)$ and $g(x)$ are relatively prime. Hence, there are polynomials $h(x)$ and $t(x)$ in $F[x]$ such that $h(x)p(x) + t(x)g(x) = 1$. Since $p(\theta) = 0$, $\frac{1}{g(\theta)} = t(\theta)$. Therefore $\alpha = f(\theta)t(\theta)$. Now by the division algorithm for polynomials over $F[x]$, $f(x)t(x) = q(x)p(x) + r(x)$ where $q(x)$ and $r(x)$ are in $F[x]$ and the degree of $r(x)$ is $n-1$ or less. Hence $\alpha = f(\theta)t(\theta) = q(\theta)p(\theta) + r(\theta) = r(\theta)$ and since $r(x) \in F[x]$ is of degree

$n-1$ or less, it follows that $\alpha = r(\theta) = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$ where the a_i are in F.

To show uniqueness suppose $h(x)$ is in $F[x]$ with $h(\theta) = \alpha$ and degree of $h(x)$ less than n, then θ is a zero of the polynomial $h(x) - r(x)$, a contradiction since the minimal polynomial of θ is of degree n and $h(x) - r(x)$ is of degree less than n.

After two definitions and two more lemmas it will be possible to prove a comment made in Chapter II concerning the fact that every multiple algebraic extension is a simple algebraic extension.

Definition 3.16. Let $\alpha_1, \ldots, \alpha_n$ be numbers algebraic over a field F, then the smallest field $K = F(\alpha_1, \ldots, \alpha_n)$ containing F and $\alpha_1, \ldots, \alpha_n$ is called a multiple or finite algebraic extension of F.

Definition 3.17. Let $\alpha = \alpha_1$ be an algebraic number and $p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ its minimal polynomial, then $\alpha_1, \alpha_2, \ldots, \alpha_n$ are called the conjugates of α.

Lemma 3.18. If θ is algebraic over F, θ has a unique minimal polynomial $p(x)$ and if $g(x)$ is a polynomial such that $g(\theta) = 0$ then $p(x)$ is a factor of $g(x)$.

Proof: By the division algorithm for polynomials, $g(x) = q(x)\,p(x) + h(x)$ where the degree of $h(x)$ is less than $p(x)$. Since $p(\theta) = 0$ and $g(\theta) = 0$, it follows that $h(\theta) = 0$ and hence $h(x) \equiv 0$, since $p(x)$ is the minimal polynomial for θ. So $p(x)$ is a factor of $g(x)$. To show the uniqueness of $p(x)$, assume that $g(x)$ is also a minimal polynomial for θ and considering $p(x) = k(x)\,g(x) + r(x)$ it will follow that

$g(x)$ is a factor of $p(x)$ and therefore $p(x) = \epsilon g(x)$ where ϵ is a unit in $F[x]$. Since the units in $F[x]$ are the units in F and both $p(x)$ and $g(x)$ are monic by definition of a minimal polynomial, then $p(x) = g(x)$.

Lemma 3.19. If $f(x)$ is irreducible in $F[x]$ and of degree n then $f(x)$ has n distinct zeros.

Proof: Suppose $f(x) = (x - r)^2 g(x)$ and is monic then $f'(x) = 2(x - r)\, g(x) + (x - r)^2 g'(x)$. Notice that r is an algebraic number and that $f(x)$ is its minimal polynomial, also since the coefficients of $f(x)$ are in F so are the coefficients of $f'(x)$. Hence $f'(x)$ is a polynomial of degree $n - 1$ in $F[x]$ with r as a zero, a contradiction to the uniqueness of a minimal polynomial for an algebraic number.

Theorem 3.20. A multiple algebraic extension of a number field F is a simple algebraic extension.

Proof: It need only be shown that if α and β are algebraic over F there is some θ which is algebraic over F for which $F(\theta) = F(\alpha, \beta)$. Once this is done, mathematical induction will extend the result to any finite algebraic extension of F.

Let $\alpha = \alpha_1$ and $\beta = \beta_1$ with $\alpha \neq \beta$ be algebraic over F with conjugates over F of $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ respectively. By Lemma 3.19, $\beta_k \neq \beta_1$ for $k = 2, \ldots, m$ and $\alpha_i \neq \alpha_j$ for $i \neq j$ and therefore the set of $X_{ij} = \dfrac{\alpha_1 - \alpha_i}{\beta_j - \beta_1}$, $i \neq j$, $j \neq 1$, $i = 1, \ldots, n$ and $j = 2, \ldots, m$ is a finite set. This means there is a value b in F such that $b \neq \dfrac{\alpha_1 - \alpha_i}{\beta_j - \beta_1}$ for any i or $j \neq 1$. Rearranging this gives

$\alpha_i + b\beta_j \neq \alpha + b\beta$ for all i and $j \neq 1$. Let $\theta = \alpha + b\beta$ and it shall be shown that $F(\theta) = F(\alpha, \beta)$.

$F(\theta)$ is a subset of $F(\alpha, \beta)$ since by Theorem 3.13 every α in $F(\theta)$ can be written as

$$\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} = a_0 + a_1(\alpha + b\beta) + \ldots + a_{n-1}(\alpha + b\beta)^{n-1}$$

which is clearly in $F(\alpha, \beta)$.

To show the set inclusion the other direction, first show that β is in $F(\theta)$. Let $f(x)$ and $g(x)$ be the minimal polynomials for α and β respectively then $f(\theta - b\beta) = f(\alpha) = 0$ and $g(\beta) = 0$ and therefore $f(\theta - bx)$ and $g(x)$ have a zero in common. Further, since the only zeros of $f(x)$ are $\alpha_1, \ldots, \alpha_n$, the only zeros of $f(\theta - bx)$ are when $\theta - bx = \alpha_i$, $i = 1, \ldots, n$ which by the choice of b only occurs when $x = \beta$, hence the only zero common to $f(\theta - bx)$ and $g(x)$ is β. Let the minimal polynomial of β in $F(\theta)$ be $h(x)$. Notice that $h(x)$ has coefficients in $F(\theta)$ not just F. If $h(x)$ has degree higher than one then $h(x)$ is a factor of both $f(\theta - bx)$ and $g(x)$ over $F(\theta)$ by Lemma 3.19 and hence $f(\theta - bx)$ and $g(x)$ would have more than one root in common, a contradiction. Therefore, $h(x) = dx + e$ with d and e in $F(\theta)$, further $h(\beta) = 0$ which gives $\beta = \frac{-e}{d}$ an element of $F(\theta)$.

Now since β, b and θ are all in $F(\theta)$ it follows that $\theta - b\beta = \alpha$ is in $F(\theta)$. Therefore since both α and β are in $F(\theta)$ it follows that $F(\theta)$ is a subset of $F(\alpha, \beta)$. With set inclusion in both directions, then $F(\theta) = F(\alpha, \beta)$.

Theorem 3.21. If θ is an algebraic number, there is a non-zero rational integer b such that $b\theta$ is an algebraic integer.

Proof: Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be the defining polynomial of θ. All the coefficients are rational numbers and hence there is an integer b such that ba_i, $i = 0, \ldots, n-1$, is a rational integer. Considering the monic polynomial $g(x) = x^n + ba_{n-1}x^{n-1} + \ldots + b^n a_0$ which has rational integer coefficients then $b\theta$ is a zero of $g(x)$, since $g(b\theta) = b^n(\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0) = b^n \cdot 0 = 0$. Hence $b\theta$ is an algebraic integer.

Theorem 3.22. For every algebraic number field $R(\theta)$ there is a rational integer b such that $R(\theta) = R(b\theta)$ with $b\theta$ an algebraic integer.

Proof: Let θ be of degree n over R and α be in $R(\theta)$ with b the rational integer of Theorem 3.21 such that $b\theta$ is an algebraic integer. Theorem 3.15 implies that $\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$ but

$$a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1} = a_0 + \frac{a_1}{b}(b\theta) + \ldots + \frac{a_{n-1}}{b^{n-1}}(b\theta)^{n-1}$$

which is in $R(b\theta)$. Therefore $R(\theta)$ is a subset of $R(b\theta)$ and since $R(b\theta)$ is a subset of $R(\theta)$ then $R(\theta) = R(b\theta)$.

The preceding theorems now enable one to consider only simple algebraic extensions of R to include an algebraic integer as opposed to having to work with multiple extensions to include algebraic numbers. That is, if $\alpha_1, \ldots, \alpha_n$ are algebraic numbers then there is an algebraic integer θ such that $R(\alpha_1, \ldots, \alpha_n) = R(\theta)$.

Properties of the Norm

Several characteristics of algebraic integers can be developed through the definition of a norm. For convient reference the following definition is repeated.

Definition 3.23. Let $\alpha = \alpha_1$ be an algebraic number with $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ its defining polynomial. The set of numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the conjugates of the algebraic number α.

Definition 3.24. Let α be an element of $R(\theta)$ where θ is of degree n over R. With $r(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, the polynomial of Theorem 3.15, such that $\alpha = r(\theta)$ and θ_i, $i = 1, \ldots, n$ being the conjugates of θ. The field conjugates of α are defined as the set of numbers $\alpha^{(i)} = r(\theta_i)$ $i = 1, \ldots, n$.

A relationship between the conjugates of α and the field conjugates of α is seen in the following theorem.

Theorem 3.25. Let α be an algebraic number in $R(\theta)$, then the set of field conjugates is either identical with the set of conjugates of α or is $\frac{n}{m}$ repetitions of the set of conjugates of α where n is the degree of θ and m is the degree of α. Also if $f(x)$ is a monic polynomial with the field conjugates of α as its roots and $g(x)$ is the defining polynomial of α then $[g(x)]^{n/m} = f(x)$.

Proof: Consider $f(x) = (x-\alpha^{(1)})(x-\alpha^{(2)})\cdots(x-\alpha^{(n)})$ with the notation as in Definition 3.24. By Theorem 3.4, the coefficients of $f(x)$ are, except possibly for sign, the elementary symmetric functions in $\alpha^{(i)}$, $i = 1, \ldots, n$ and hence are symmetric polynomials in the

θ_i, $i = 1, \ldots, n$ and hence are rational numbers. Let $g(x)$ be the minimal polynomial for α, then since $\alpha = r(\theta) = r(\theta_1) = \alpha^{(1)}$ it follows by Lemma 3.18 that $g(x)$ is a factor of $f(x)$. Therefore, write $f(x) = [g(x)]^s h(x)$ where $g(x)$ and $h(x)$ are relatively prime.

Notice that every field conjugate of α is a conjugate of α since if $g(x)$ is the minimal polynomial for α then $g(r(x))$ has θ as a zero. Lemma 3.18 then gives that the minimal polynomial for θ, $p(x)$, is a factor of $g(r(x))$ and hence every θ_i, $i = 1, \ldots, n$ is a zero of $g(r(x))$. Equivalently every $\alpha^{(i)} = r(\theta_i)$, $i = 1, \ldots, n$ is a zero of $g(x)$.

Now to prove that $h(x) \equiv 1$, suppose it is not. First, if $h(x) \equiv c$ then c must be 1 since $f(x)$ is monic and so is $g(x)$, next suppose $h(x) \not\equiv c$ then for some fixed j, $\alpha^{(j)}$ must be a zero of $h(x)$ but since $p(x)$ is a minimal polynomial for α it is also a minimal polynomial for $\alpha_1, \alpha_2, \ldots, \alpha_n$ and hence of $\alpha^{(j)}$. By Lemma 3.18 $g(x)$ is a factor of $h(x)$, a contradiction to our way of writing $f(x)$. Hence $h(x) \equiv 1$ and therefore $f(x) = [g(x)]^s$.

It is then seen that since $f(x)$ is of degree n and if the minimal polynomial for α, that is $g(x)$ is of degree m then $s = \frac{n}{m}$. That is, s is the degree of θ divided by the degree of α.

Definition 3.26. The norm of the algebraic number α, written $N(\alpha)$, is the product of its field conjugates.

In Theorem 3.25 the function $f(x)$ defined such that $f(x) = (x - \alpha^{(1)}) \cdots (x - \alpha^{(n)})$ is called the field polynomial for α where $\alpha^{(i)}$, $i = 1, \ldots, n$ are the field conjugates of α. Notice that the constant term of the field polynomial is $(-1)^n N(\alpha)$. Also recall that $f(x) = [g(x)]^{n/m}$ where $g(x)$ is the minimal polynomial for α and $\frac{n}{m}$

is a rational integer and hence if $g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ then the norm of α is just a rational integral power of the constant term a_0 of the defining polynomial for α. Further, if α is an algebraic integer then a_0 is a rational integer and hence $N(\alpha)$ is a rational integer. This gives the following theorem.

Theorem 3.27. If α is an algebraic integer then $N(\alpha)$ is a rational integer.

Theorem 3.28. $N(\alpha\beta) = N(\alpha)N(\beta)$

Proof: Let α and β be in $R(\theta)$ where θ is of degree n over R. Theorem 3.15 implies that one can write α and β uniquely as follows:

$$\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$$

$$\beta = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$$

Let the minimal polynomial for θ be $x^n + c_{n-1}x^{n-1} + \ldots + c_0$, then $\theta_i^n = -(c_{n-1}\theta_i^{n-1} + \ldots + c_0)$ for $i = 1, \ldots, n$ and θ_i the conjugates of θ. Taking the product $\alpha\beta$ and repeatedly using $\theta^n = -(c_{n-1}\theta^{n-1} + \ldots + c_0)$ the unique representation of $\alpha\beta$ as a polynomial in θ of degree less than n is obtained, but the coefficients of this polynomial are the same as the coefficients of the polynomial representing $\alpha^{(i)}\beta^{(i)}$ $i = 1, \ldots, n$. For clarification,

$$\alpha^{(i)}\beta^{(i)} = (a_0 + a_1\theta_i + \ldots + a_{n-1}\theta_i^{n-1})(b_0 + b_1\theta_i + \ldots + b_{n-1}\theta_i^{n-1})$$

and through repeated use of $\theta_i^n = -(c_{n-1}\theta_i^{n-1} + \ldots + c_0)$ the unique representation of $\alpha^{(i)}\beta^{(i)}$ is obtained and the coefficients of this

polynomial in θ_i is the same as the coefficients of the unique representation of $\alpha\beta$ as a polynomial in θ. That is, if $\alpha\beta = r(\theta)$ then $\alpha^{(i)}\beta^{(i)} = r(\theta_i)$ and hence since $(\alpha\beta)^{(i)} = r(\theta_i)$ then $(\alpha\beta)^{(i)} = \alpha^{(i)}\beta^{(i)}$.

Now if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are the field conjugates of α and β respectively in $R(\theta)$ then the field conjugates of $\alpha\beta$ are $\alpha^{(1)}\beta^{(1)}, \alpha^{(2)}\beta^{(2)}, \ldots, \alpha^{(n)}\beta^{(n)}$. Therefore

$$N(\alpha\beta) = (\alpha\beta)^{(1)}(\alpha\beta)^{(2)} \cdots (\alpha\beta)^{(n)} = \alpha^{(1)}\beta^{(1)} \cdots \alpha^{(n)}\beta^{(n)} = N(\alpha)\,N(\beta).$$

Theorem 3.29. An algebraic integer α is a unit if and only if $N(\alpha) = \pm 1$.

Proof: α a unit implies there is an algebraic integer β in $R(\theta)$ such that $\alpha\beta = 1$. Therefore $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$ but since $N(\alpha)$ and $N(\beta)$ must be rational integers by Theorem 3.27 this implies they must be ± 1. Hence $N(\alpha) = \pm 1$.

If $N(\alpha) = \pm 1$ then $\alpha^{(1)} \cdot \alpha^{(2)} \cdots \alpha^{(n)} = \pm 1$ where $\alpha^{(i)}$ $i = 1, \ldots, n$ are the field conjugates of α. Let $\alpha^{(1)} = \alpha$ and then α is a unit since $\alpha^{(2)} \cdots \alpha^{(n)}$ is an algebraic integer (every field conjugate of α is a conjuate of α).

Theorem 3.30. An algebraic integer α is a prime in $R(\theta)$ if $N(\alpha)$ is a rational prime.

Proof: Let $N(\alpha)$ be a rational prime and $\alpha = \beta\delta$ with β and δ algebraic integers, then $N(\alpha) = N(\beta)N(\delta)$. The norm of α a rational prime implies that one of $N(\beta)$ or $N(\delta)$ is ± 1 and hence a unit. Therefore α is a prime.

Definition 3.31. The set of all algebraic integers in $R(\theta)$ will be denoted by $R[\theta]$.

Theorem 3.32. If α is in $R[\theta]$ and is not zero or a unit then α can be factored into a product of primes in $R[\theta]$.

Proof: If α is not prime write $\alpha = \beta \cdot \delta$ where neither β nor δ is a unit. Repeat this for β and δ and continue in this way. The process must stop since otherwise $\alpha = \mu_1 \cdot \mu_2 \cdots \mu_n$ where n is arbitrarily large and the μ_i are nonunits. Hence $|N(\mu_i)| > 1$ for $i = 1, \ldots, n$ and therefore $N(\mu_1 \cdots \mu_n) = N(\mu_1) \cdots N(\mu_n)$ would become arbitrarily large, a contradiction to the fact that $N(\alpha)$ is finite.

Theorem 3.33. There are infinitely many primes in $R[\theta]$.

Proof: The proof is analogous to Euclid's proof of the similar theorem for rational primes.

First, there is at least one prime in $R[\theta]$, since 3 is in $R[\theta]$, Theorem 3.32 implies 3 is a product of primes in $R[\theta]$. Notice that it is not claimed that 3 itself is a prime but that there is a prime factor of 3 in $R[\theta]$.

Suppose there is a finite number of primes in $R[\theta]$, say $p_1, p_2, \ldots, p_n$. Now consider the number $r = p_1 \cdot p_2 \cdots p_n + 1$, this number is an algebraic integer in $R[\theta]$ since we have closure of multiplication and addition of algebraic integers. Now r is nonzero and nonunit and in $R[\theta]$ therefore r has a prime factor q. Now $q \neq p_i$, $i = 1, \ldots, n$ since it would be necessary for q to divide 1 which it does not since q is a prime and 1 is a unit. Therefore there is a

prime in $R[\theta]$ different from $p_1, \ldots, p_n$ a contradiction to the assumption of only a finite number of primes in $R[\theta]$.

Bases

Definition 3.34. Let F be a field of numbers and K an extension of F, then a set of numbers $x_1, x_2, \ldots, x_n$ in K is linearly dependent over F if there exists $c_1, c_2, \ldots, c_n$ in F, not all zero such that $c_1 x_1 + c_2 x_2 + \ldots + c_n x_n = 0$. If no such set exists the set $x_1, x_2, \ldots, x_n$ is called a linearly independent set.

Definition 3.35. Let F be a field of numbers and K an extension of F, then a set of numbers $y_1, y_2, \ldots, y_m$ is a basis for K over F if for every z in K there exists a unique set of numbers $d_1, d_2, \ldots, d_m$ in F such that $z = d_1 y_1 + d_2 y_2 + \ldots + d_m y_m$.

Notice that a basis is a linearly independent set, for if not, $0 = c_1 y_1 + c_2 y_2 + \ldots + c_m y_m$ where not all the c_i are zero but also $0 = 0 \cdot y_1 + 0 \cdot y_2 + \ldots + 0 \cdot y_m$ a contradiction to the unique representation requirement of the definition of a basis.

Lemma 3.36. If $m < n$ and if the a_{ij} are in a number field F, then the system of equations $\sum_{j=1}^{n} a_{ij} x_j = 0$, $i = 1, 2, \ldots, m$ has a solution $x_j = a_j$, $j = 1, \ldots, n$ in F, where not all the a_j are zero.

Proof: Refer to Hahn [11].

Theorem 3.37. If the extension K of the field of numbers F has a basis of m elements over F, then any n numbers in K where $n > m$, are linearly dependent over F.

Proof: Let $y_1, y_2, \ldots, y_m$ be a basis and $x_1, x_2, \ldots, x_n$ be any set of elements in K. Then $x_i = \sum_{j=1}^{m} a_{ij} y_j$, $i = 1, 2, \ldots, n$. By Lemma 3.36 the system $\sum_{i=1}^{n} a_{ij} z_i = 0$, $j = 1, \ldots, m$ has a nontrivial solution $z_i = c_i$, $i = 1, \ldots, n$ hence

$$\sum_{i=1}^{n} c_i x_i = \sum_{i=1}^{n} c_i \sum_{j=1}^{m} a_{ij} y_j = \sum_{j=1}^{m} y_j \sum_{i=1}^{n} a_{ij} c_i = 0.$$

Therefore, there is a set of c_i, $i = 1, \ldots, n$ not all zero, such that $c_1 x_1 + c_2 x_2 + \ldots + c_n x_n = 0$ and hence $x_1, x_2, \ldots, x_n$ is a linearly dependent set.

Theorem 3.38. If $y_1, y_2, \ldots, y_m$ and $z_1, \ldots, z_p$ are both bases for K over F then $m = p$.

Proof: If $m \neq p$ then without loss of generality let $m > p$. Theorem 3.37 then implies that $y_1, y_2, \ldots, y_m$ are linearly dependent and hence not a basis, a contradiction to the hypothesis. Hence $m = p$.

Definition 3.39. If K is an extension of the field of numbers F and K has a basis consisting of n elements then K is called a finite extension of F which has degree n over F.

Theorem 3.40. If K is a finite extension of F then every α in K is algebraic over F.

Proof: Let K have degree n over F then by Theorem 3.37 the set of numbers $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over F. Therefore there are numbers a_i, $i = 0, \ldots, n$ in F, not all zero, such that $a_0 + a_1 \alpha + \ldots + a_n \alpha^n = 0$. Hence α is a root of a polynomial in $F[x]$ and is therefore algebraic over F.

Theorem 3.41. An extension K of a number field F is of finite degree if and only if K is a simple algebraic extension of F.

Proof: First let K be a finite extension of F, then K has a basis $x_1, x_2, \ldots, x_n$ over F and therefore $K = F(x_1, x_2, \ldots, x_n)$. Further by Theorem 3.40 every x_i, $i = 1, \ldots, n$ is algebraic over F and hence by Theorem 3.20, K is a simple algebraic extension of F. That is, $K = F(\theta)$ for some θ which is algebraic over F.

Next let K be a simple algebraic extension of F, say $F(\theta)$ where θ is of degree n over F. By Theorem 3.15 every element of $K = F(\theta)$ can be written uniquely in the form $a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$ where a_i, $i = 0, \ldots, n-1$ are elements of F, hence $1, \theta, \ldots, \theta^{n-1}$ is a basis for K. Therefore K is a finite extension of F of degree n over F.

Notice that it has been shown that if the field of rational numbers R is considered, then every finite field extension K of R is a simple algebraic extension of R. That is there is a number θ which is algebraic over R such that $K = R(\theta)$. Further by Theorem 3.22 there is an algebraic integer α such that $K = R(\alpha)$. Comparing the definition of the degree of an algebraic number θ and the degree of K over R it is seen that they are the same. That is, if θ is of degree n over R then $R(\theta)$ is of degree n over R.

Definition 3.42. Let $R(\theta)$ be of degree n and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements of $R(\theta)$. Let $\alpha_i^{(j)}$, $j = 1, \ldots, n$ be the field conjugates of α_i, $i = 1, 2, \ldots, n$. The discriminant of the set $\alpha_1, \alpha_2, \ldots, \alpha_n$, denoted by $\Delta[\alpha_1, \ldots, \alpha_n]$ is defined by the square of the determinant

$$\begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ \alpha_1^{(2)} & \cdot & & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \\ \alpha_1^{(n)} & \cdots & & \alpha_n^{(n)} \end{vmatrix} .$$

That is $\Delta[\alpha_1,\ldots,\alpha_n] = |\alpha_i^{(j)}|^2$.

Theorem 3.43. $\Delta[\alpha_1,\ldots,\alpha_n]$ is a rational integer if $\alpha_1,\ldots,\alpha_n$ are all in $R[\theta]$.

Proof: From linear algebra it is known that the determinant of a product of square matrices is the product of the determinant of the transpose of the first and the determinant of the second. Hence

$$\Delta[\alpha_1,\ldots,\alpha_n] = \begin{vmatrix} \alpha_1^{(1)} & \cdots & \alpha_1^{(n)} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_n^{(1)} & \cdots & \alpha_n^{(n)} \end{vmatrix} \cdot \begin{vmatrix} \alpha_1^{(1)} & \cdots & \alpha_n^{(1)} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_1^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}$$

$$= \begin{vmatrix} \alpha_1^{(1)2} + \ldots + \alpha_1^{(n)2} & \cdots & \alpha_1^{(1)}\alpha_n^{(1)} + \ldots + \alpha_1^{(n)}\alpha_n^{(n)} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_n^{(1)}\alpha_1^{(1)} + \ldots + \alpha_n^{(n)}\alpha_1^{(n)} & \cdots & \alpha_1^{(n)2} + \ldots + \alpha_n^{(n)2} \end{vmatrix} .$$

As in the proof of Theorem 3.28, the conjugate of the product is the product of the conjugates, hence:

$$\alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \ldots + \alpha^{(n)}\beta^{(n)} = (\alpha\beta)^{(1)} + (\alpha\beta)^{(2)} + \ldots + (\alpha\beta)^{(n)} .$$

This sum is a rational integer for let $x^m + a_{m-1}x^{m-1} + \ldots + a_0$ be the defining polynomial for the algebraic integer $\alpha\beta$ then the sum of the conjugates of $\alpha\beta$ is $-a_{m-1}$, a rational integer by Theorem 3.3. The field conjugates of $\alpha\beta$ are just $\frac{n}{m}$ (a rational integer) repetitions of the conjugates of $\alpha\beta$ by Theorem 3.25 and hence their sum is also a rational integer.

Since every entry in the above determinant for the discriminant is a rational integer then its value is a rational integer.

Definition 3.44. An integral basis for $R(\theta)$ is a set $\alpha_1, \ldots, \alpha_n$ of algebraic integers in $R[\theta]$ such that if $\alpha \in R[\theta]$, α can be written uniquely as

$$\alpha = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n .$$

Where b_i, $i = 1, \ldots, n$ are rational integers.

Theorem 3.45. An integral basis for $R(\theta)$ is a basis for $R(\theta)$.

Proof: Let x be in $R(\theta)$ then by Theorem 3.21 there is a nonzero rational integer b such that bx is an algebraic integer. Hence $bx = b_1\alpha_1 + \ldots + b_n\alpha_n$ for some choice of rational integers b_i, $i = 1, \ldots, n$. Therefore $x = \frac{b_1}{b}\alpha_1 + \ldots + \frac{b_n}{b}\alpha_n$. Now the set $\alpha_1, \ldots, \alpha_n$ is an independent set over R for if not, there are rational numbers $c_1, c_2, \ldots, c_n$ not all zero such that $c_1\alpha_1 + \ldots + c_n\alpha_n = 0$. Let d be the least common denominator of the c_i's then dc_i, $i = 1, \ldots, n$ is a rational integer. Therefore $dc_1\alpha_1 + \ldots + dc_n\alpha_n = 0$ but by definition of an integral basis this

implies $d c_i = 0$, $i = 1, \ldots, n$ and therefore since $d \neq 0$ this implies $c_i = 0$, $i = 1, \ldots, n$.

Basis of an Ideal

The following definition of an ideal in $R(\theta)$ is the same as the usual algebra definition of an ideal if you consider as your ring the ring of algebraic integers in $R(\theta)$, that is, $R[\theta]$.

Definition 3.46. A nonempty set of algebraic integers A in $R[\theta]$ is an ideal of $R(\theta)$ if for every pair of algebraic integers α, β in A then $\alpha x + \beta y$ is also in A for all x, y in $R[\theta]$.

Recalling $R(\sqrt{-5})$ of Chapter II consider the subset $A = \{z \mid z = 3x, x \in R[\sqrt{-5}]\}$. A is an ideal and contains such elements as $3(7) = 21$, $3(1 + 2\sqrt{-5}) = 3 + 6\sqrt{-5}$, in fact 3 times any algebraic integer in $R(\sqrt{-5})$. Another example would be

$$\{z \mid z = 3x + (1 - 2\sqrt{-5})y, x \text{ and } y \text{ in } R[\sqrt{-5}]\}.$$

Notice that in Chapter II it was shown that $3, 7, 1 + 2\sqrt{-5}$, $1 - 2\sqrt{-5}$ were all algebraic integers in $R(\sqrt{-5})$.

Definition 3.46. A basis for an ideal A in $R(\theta)$ is any set $b_1, \ldots, b_m$ of algebraic integers in A such that every α in A can be uniquely represented in the form $\alpha = c_1 b_1 + \ldots + c_m b_m$ where the c_i are rational integers.

The goal of this section is to prove that every ideal in a simple algebraic extension has a basis.

Theorem 3.47. The discriminent of any basis of $R(\theta)$ is non-zero.

Proof: Let $\alpha_1, \ldots, \alpha_n$ and $b_1, \ldots, b_n$ both be bases for $R(\theta)$, then

$$b_k = \sum_{j=1}^{n} c_{jk}\alpha_j , \quad k = 1, \ldots, n$$

for some choice of the c_{jk} in R. It shall now be shown that $\Delta[b_1, \ldots, b_n] = |c_{jk}|^2 \Delta[\alpha_1, \ldots, \alpha_n]$.

By the comment following 3.41 and since there are n elements in a basis, θ is of degree n over R. Hence Theorem 3.15 implies $\alpha_j = \alpha_j(\theta) = a_{j0} + a_{j1}\theta + \ldots + a_{jn-1}\theta^{n-1}$ and the definition of a field conjugate gives $\alpha_j^{(i)} = \alpha_j(\theta_i)$ where θ_i is the i^{th} conjugate of θ. But,

$$\begin{aligned} b_j &= c_{j1}\alpha_1 + \ldots + c_{jn}\alpha_n \\ &= c_{j1}\alpha_1(\theta) + \ldots + c_{jn}\alpha_n(\theta) \quad j = 1, \ldots, n \end{aligned}$$

which is a function of θ of degree at most $n-1$. Hence by the uniqueness of representation from Theorem 3.15 of b_j it is seen that

$$\begin{aligned} b_j^{(i)} = b_j(\theta_i) &= c_{j1}\alpha_1(\theta_i) + \ldots + c_{jn}\alpha_n(\theta_i) \\ &= c_{j1}\alpha_1^{(i)} + \ldots + c_{jn}\alpha_n^{(i)} . \end{aligned}$$

Hence,

$$\begin{vmatrix} b_1^{(1)} & \ldots & b_1^{(n)} \\ \vdots & & \vdots \\ b_n^{(1)} & \ldots & b_n^{(n)} \end{vmatrix} = \begin{vmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \ldots & c_{nn} \end{vmatrix} \cdot \begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_1^{(1)} \\ \vdots & & \vdots \\ \alpha_n^{(1)} & \ldots & \alpha_n^{(n)} \end{vmatrix} .$$

which implies $\Delta[b_1,\ldots,b_n] = |c_{jk}|^2 \Delta[\alpha_1,\ldots,\alpha_n]$.

The next part of the proof is to show that $|c_{jk}| \neq 0$. Suppose $|c_{jk}| = 0$ then by linear algebra, see Hahn [11], considering the α_j as variables the system of equations $\sum_{j=1}^{n} c_{jk}\alpha_j = 0$, $k=1,\ldots,n$ has a nontrivial solution and hence $\alpha_1,\ldots,\alpha_n$ is a linearly dependent set and therefore not a basis.

It now only remains to show that the discriminant of a particular base is nonzero since the discriminant of any other base will just be a nonzero constant times the nonzero discriminant of this particular base.

Theorem 3.15 implies that $1,\theta,\ldots,\theta^{n-1}$ is a basis for $R(\theta)$. Let $\theta_1 = \theta,\theta_2,\ldots,\theta_n$ be the conjugates of θ then since $\theta^i = 1\cdot\theta^i = r(\theta)$, (the $r(\theta)$ of Definition 3.24), $i=0,\ldots,n-1$ it is seen that $(\theta^i)^{(j)} = 1\cdot(\theta_j)^i$. That is $(\theta^i)^{(j)} = (\theta^{(j)})^i$ or the j^{th} field conjugate of θ^i is the i^{th} power of the j^{th} conjugate of θ. Hence

$$\Delta[1,\theta,\ldots,\theta^{n-1}] = \begin{vmatrix} 1 & \theta^{(1)} & \ldots & \left(\theta^{(1)}\right)^{n-1} \\ \vdots & & & \vdots \\ 1 & \theta^{(n)} & \ldots & \left(\theta^{(n)}\right)^{n-1} \end{vmatrix}^2 .$$

Hence $\Delta[1,\theta,\ldots,\theta^{n-1}]$ is the square of the Vandermonde determinant and hence its value is $\prod_{1\leq i<j\leq n} (\theta^{(i)}-\theta^{(j)})^2$, [11].

Lemma 3.19 implies $\theta^{(i)} \neq \theta^{(j)}$ for $i\neq j$ since θ is a root of an irreducible polynomial over R of degree n. Hence

$$\prod_{1\leq i<j\leq n} (\theta^{(i)}-\theta^{(j)})^2 \neq 0.$$

It has therefore been shown that $\Delta[1,\theta,\ldots,\theta^{n-1}] \neq 0$ which proves the theorem.

Corollary 3.48. If $\alpha_1,\ldots,\alpha_n$ is a basis of $R(\theta)$ and $b_1,\ldots,b_n$ are in $R(\theta)$ such that $b_k = \sum_{j=1}^{n} c_{jk}\alpha_j$, $k = 1,\ldots,n$ then $\Delta[b_1,\ldots,b_n] = |c_{jk}|^2 \Delta[\alpha_1,\ldots,\alpha_n]$.

Proof: The proof is as in Theorem 3.47 since that proof did not depend on $b_1,\ldots,b_n$ being a basis.

Theorem 3.49. $R(\theta)$ has an integral basis

Proof: Without loss of generality it may be assumed by Theorem 3.22 that θ is an algebraic integer of degree n over R. Consider the set of bases consisting of algebraic integers of $R(\theta)$ and choose one whose discriminant in absolute value is a minimum. This can be done since there is at least one basis of algebraic integers; namely, $1,\theta,\ldots,\theta^{n-1}$ and Theorem 3.43 implies that the discriminant of algebraic integers is a rational integer. Let $b_1, b_2,\ldots,b_n$ be a basis of algebraic integers whose discriminant in absolute value is a minimum. Note that $\Delta[b_1,\ldots,b_n] \neq 0$ by Theorem 3.47.

It shall now be shown that $b_1,\ldots,b_n$ is an integral basis. Suppose it is not an integral basis then there is an algebraic integer t in $R(\theta)$ such that $t = c_1 b_1 + \ldots + c_n b_n$ for some unique choice of c_i in R but not all the c_i are rational integers. Without loss of generality, let c_1 be a nonrational integer then $c_1 = d + r$ where d is a rational integer and r is a rational number such that $0 < r < 1$. It is now asserted that $t - d\,b_1, b_2,\ldots,b_n$ is a basis of algebraic integers. First t, d, b_1 are all algebraic integers hence $t - d\,b_1$ is

an algebraic integer and the b_i, $i=2,\ldots,n$ were given to be algebraic integers. Suppose $t-db_1, b_2, \ldots, b_n$ is not a basis, then there are r_i not all zero in R such that

$$r_1(t-db_1) + r_2b_2 + \ldots + r_nb_n = 0$$

and therefore

$$r_1(c_1b_1 + \ldots + c_nb_n - db_1) + r_2b_2 + \ldots + r_nb_n = 0$$

which in turn gives

$$r_1(c_1-d)b_1 + (r_1c_2 + r_2)b_2 + \ldots + (r_1c_n + r_n)b_n = 0 .$$

But $b_1,\ldots,b_n$ a basis implies $r_1(c_1-d)=0$ and $r_1c_i+r_i=0$, $i=2,\ldots,n$. By the choice of d, $c_1-d\neq 0$ hence $r_1=0$ but this in turn implies $r_i=0$, $i=2,\ldots,n$, which contradicts the assumption that $t-db_1, b_2, \ldots, b_n$ is not a basis. Hence it is a basis.

Now by Corollary 3.48, since $t-db_1 = (c_1-d)b_1+c_2b_2+\ldots+c_nb_n$ and $b_i = 1\cdot b_i$, $i=2,\ldots,n$:

$$\Delta[t-db_1, b_2, \ldots, b_n] = \begin{vmatrix} c_1-d & c_2 & c_3 & \ldots & c_n \\ 0 & 1 & 0 & \ldots & 0 \\ \cdot & & 1 & & \cdot \\ \cdot & & & \cdot & \cdot \\ \cdot & & & & \cdot \\ & & & & 0 \\ 0 & & \ldots & 0 & 1 \end{vmatrix}^2 \Delta[b_1, b_2, \ldots, b_n]$$

$$= (c_1-d)^2\,\Delta[b_1,\ldots,b_n]$$

$$= r^2\,\Delta[b_1,\ldots,b_n] .$$

But $0 < r < 1$ which implies $\Delta[t - d b_1, b_2, \ldots, b_n] < \Delta[b_1, \ldots, b_n]$ a contradiction to the choice of the basis $b_1, \ldots, b_n$. Hence the assumption that $b_1, \ldots, b_n$ is not an integral basis is false, and it is an integral basis. Therefore $R(\theta)$ has an integral basis.

The necessary theorems have been shown so that it is now possible to accomplish the stated objective of this section by proving that every ideal has a basis. As a convenience in notation let the zero ideal, (0), represent the ideal of $R(\theta)$ consisting only of zero.

Theorem 3.50. Every nonzero ideal A in $R(\theta)$ has a basis of n elements, where n is the degree of θ over R.

Proof: First it will be shown that if A has a basis then that basis has n elements. Suppose A has a basis $b_1, \ldots, b_m$. This is an independent set in $R(\theta)$ for suppose not, then there exist c_i in R, not all zero, such that $c_1 b_1 + \ldots + c_n b_n = 0$. Multiply by the greatest common denominator, d, of the c_i, this gives $d c_1 b_1 + \ldots + d c_n b_n = 0$ with the $d c_i$ all rational integers not all of which are zero. This is a contradiction to $b_1, \ldots, b_m$ being a basis for A. Since $b_1, \ldots, b_m$ is an independent set in $R(\theta)$ Theorem 3.37 implies $m \leq n$.

Now show $m = n$. Assume $m < n$. By Theorem 3.49 $R(\theta)$ has an integral basis $t_1, \ldots, t_n$. Choose $\alpha \neq 0$ from A. $\alpha t_1, \ldots, \alpha t_n$ is then in A by the definition of an ideal. Further, $\alpha t_1, \ldots, \alpha t_n$ is easily seen to be a basis for $R(\theta)$ and hence $\Delta[\alpha t_1, \ldots, \alpha t_n] \neq 0$ by Theorem 3.47. Also, since $b_1, \ldots, b_m$ is a basis for A there are rational integers e_{ij} such that $\alpha t_i = \sum_{j=1}^{n} e_{ij} b_j$,

$i = 1, \ldots, n$ where $b_j = 0$ for $j = m+1, \ldots, n$. Corollary 3.48 then gives

$$\Delta[\alpha t_1, \ldots, \alpha t_n] = |e_{ij}|^2 \Delta[b_1, \ldots, b_m, 0, \ldots, 0]$$

$$= |e_{ij}|^2 \cdot 0$$

$$= 0$$

This is a contradiction to $\Delta[\alpha t_1, \ldots, \alpha t_n] \neq 0$. Hence $m = n$.

The proof that A has a basis is similar to the proof that $R(\theta)$ has an integral basis.

Consider the set of all bases for $R(\theta)$ such that every element in each basis is in A. $\alpha t_1, \ldots, \alpha t_n$ from above is such a base. Theorem 3.43 and Theorem 3.47 imply that the absolute value of the discriminant of any such basis is a positive rational integer. Let $b_1, \ldots, b_n$ be a basis in this set where $|\Delta[b_1, \ldots, b_n]|$ is a minimum. It shall now be shown that $b_1, \ldots, b_n$ is a basis for A.

First, each b_i is an element of A by the choice of the set of bases considered. Now assume it is not a basis for A. There is then a t in A such that $t = c_1 b_1 + \ldots + c_n b_n$ for some unique choice of c_i in R but not all the c_i are rational integers. Without loss of generality let c_1 be a nonrational integer then $c_1 = d + r$ where d is a rational integer and r is a rational number such that $0 < r < 1$.

Secondly, it is asserted that $t - d b_1, b_2, \ldots, b_n$ is a basis of algebraic integers in A. Now, t, b_1 in A and d a rational integer implies $t - db$ is in A by definition of an ideal. Further, $b_2, \ldots, b_n$ were originally chosen in A. Suppose $t - d b_1, b_2, \ldots, b_n$ is not a basis for $R(\theta)$ then there are r_i in R, not all zero, such that

$r_1(t - d\,b_1) + r_2 b_2 + \ldots + r_n b_n = 0$. Substituting for t and rearranging it follows that $r_1(c_1 - d)b_1 + (r_1 c_2 + r_2)b_2 + \ldots + (r_1 c_n + r_n)b_n = 0$. But $b_1, \ldots, b_n$ a basis for $R(\theta)$ implies $r_1(c_1 - d) = 0$ hence $r_1 = 0$ which in turn implies $r_i = 0$, $i = 2, \ldots, n$. A contradiction to the assumption that $t - d\,b_1, b_2, \ldots, b_n$ is not a basis, hence it is a basis.

Now by Corollary 3.48, since $t - d\,b_1 = (c_1 - d)b_1 + c_2 b_2 + \ldots + c_n b_n$ and $b_i = 1 \cdot b_i$, $i = 2, \ldots, n$ it is seen that

$$\Delta[t - d\,b_1, b_2, \ldots, b_n] = \begin{vmatrix} c_1 - d & c_2 & c_3 & \ldots & c_n \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & & 1 & & \vdots \\ \vdots & & & \ddots & \vdots \\ \vdots & & & & 0 \\ 0 & \ldots & & 0 & 1 \end{vmatrix} \Delta[b_1, b_2, \ldots, b_n]$$

$$= (c_1 - d)^2 \Delta[b_1, \ldots, b_n]$$

$$= r^2 \Delta[b_1, \ldots, b_n] .$$

But $0 < r < 1$ which implies $\Delta[t - d\,b_1, b_2, \ldots, b_n] < \Delta[b_1, \ldots, b_n]$ a contradiction to the choice of the basis $b_1, \ldots, b_n$. Hence the assumption that $b_1, \ldots, b_n$ is not a basis for A is false. Therefore A has a basis.

CHAPTER IV

FUNDAMENTAL THEOREM OF IDEALS

The major goal of this chapter is to prove a theorem relating to ideals which is analogous to the fundamental theorem of arithmetic.

In order that the material be somewhat self contained in this chapter a previous definition and theorem are restated.

Definition 4.1. A nonempty subset A of $R[\theta]$ is an ideal of $R(\theta)$ if for every pair of algebraic integers α, β in A then $\alpha x + \beta y$ is also in A for all x, y in $R[\theta]$.

The reader should notice that this is equivalent to saying that A is an additive subgroup of $R[\theta]$ such that ra is in A for every r in $R[\theta]$ and a in A. Also one should recall that R represents the rational numbers, $R(\theta)$ represents the field extension of R to include the algebraic number θ and $R[\theta]$ represents the algebraic integers in $R(\theta)$.

The following theorem was proven as Theorem 3.50.

Theorem 4.2. Every nonzero ideal A in $R(\theta)$ has a basis of n elements, where n is the degree of θ over R.

One should also recall that according to the definition of a basis for an ideal this basis is actually an integral basis.

Given a set of algebraic integers $\beta_1,\ldots,\beta_n$ in $R[\theta]$ then the set of all numbers of the form $d_1\beta_1 + \ldots + d_n\beta_n$ where the d_i are algebraic integers is easily seen to form an ideal of $R(\theta)$. The set $\beta_1,\ldots,\beta_n$ is said to form a generating set for an ideal B which is written $B = (\beta_1,\beta_2,\ldots,\beta_n)$.

Let A be an ideal of $R(\theta)$ then since it has an integral basis $\alpha_1,\ldots,\alpha_n$ with the α_i in A, one can consider $\alpha_1,\ldots,\alpha_n$ as a generating set for A and write $A = (\alpha_1,\ldots,\alpha_n)$. That is, every element a in A can be written as $a = b_1\alpha_1 + \ldots + b_n\alpha_n$ where the b_i are rational integers. Further, for every choice of algebraic integers $c_1,\ldots,c_n$ it is seen that $c_1\alpha_1 + \ldots + c_n\alpha_n$ is in A since A is an ideal. Hence every ideal A of $R(\theta)$ can be written as $A = (\alpha_1,\ldots,\alpha_n)$.

Notice that if $B = (\beta_1,\ldots,\beta_n)$ then $\beta_1,\ldots,\beta_n$ is not necessarily a basis for the ideal B.

Theorem 4.3. If $A = (\alpha_1,\ldots,\alpha_n)$ and $B = (\beta_1,\ldots,\beta_p)$ are ideals of $R(\theta)$ then $A = B$ if and only if for every α_i, $\alpha_i = b_{i1}\beta_1 + \ldots + b_{ip}\beta_p$ and for every β_j, $\beta_j = a_{j1}\alpha_1 + \ldots + a_{jn}\alpha_n$ for some choice of algebraic integers $b_{i1},\ldots,b_{ip}$, $a_{j1},\ldots,a_{jn}$.

Proof: If $A = B$, it is then obvious that the condition must hold. If the condition holds pick an arbitrary element a in A, then for some choice of algebraic integers $c_1,\ldots,c_n$

$$a = \sum_{i=1}^{n} c_i\alpha_i = \sum_{i=1}^{n} c_i \sum_{j=1}^{p} b_{ij}\beta_j = \sum_{i=1}^{n}\sum_{j=1}^{p} c_i b_{ij}\beta_j$$

which is an element of B. Therefore A is a subset of B. Similarly B is a subset of A, hence $A = B$.

Definition 4.4. An ideal A is a principal ideal if it is generated by a single algebraic integer.

Theorem 4.5. $(\alpha) = (\beta)$ if and only if α and β are associates.

Proof: If $(\alpha) = (\beta)$ then there are algebraic integers a and b such that $\alpha = b\beta$ and $\beta = a\alpha$. Therefore $\alpha = b(a\alpha) = (ba)\alpha$ and hence $ba = 1$. Hence by definition of a unit both a and b are units. Therefore α and β are associates.

If α and β are associates then $\alpha = b\beta$ and $\beta = a\alpha$ where b and a are units and hence algebraic integers. Theorem 4.3. then gives that $(\alpha) = (\beta)$.

Definition 4.6. The product of two ideals $A = (\alpha_1, \ldots, \alpha_n)$ and $B = (\beta_1, \beta_2, \ldots, \beta_t)$ is given by

$$AB = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_t, \alpha_2\beta_1, \ldots, \alpha_2\beta_t, \ldots, \alpha_n\beta_1, \ldots, \alpha_n\beta_t)$$

or alternately

$$AB = \{x \mid x \text{ is a finite sum of the form } \Sigma a_i b_i,\ a_i \text{ in } A,\ b_i \text{ in } B\}.$$

The two forms are equivalent for consider

$$h = c_{11}\alpha_1\beta_1 + c_{12}\alpha_1\beta_2 + \ldots + c_{ij}\alpha_i\beta_j + \ldots + c_{nt}\alpha_n\beta_t.$$

It is known that A is an ideal and hence $c_{ij}\alpha_i = \alpha_i'$ is in A and therefore $h = \alpha_1'\beta_1 + \ldots + \alpha_n'\beta_t$ which is of the form $\sum_{i=1}^{p} a_i b_i$.

Verification the other direction follows but is more difficult notationally.

The product is well defined as can be verified by the use of Theorem 4.3.

Two other consequences which follow immediately from the definition are the associative property, namely $A(BC) = (AB)C$ and the commutative property, $AB = BA$.

Definition 4.7. A is a divisor or factor of B, written $A|B$, if and only if there is an ideal C such that $B = AC$, A, B, C ideals in $R(\theta)$.

Theorem 4.8. IF $A|B$ then B is a subset of A.

Proof: IF $A|B$ then there is an ideal C such that $B = AC$. Let $A = (\alpha_1, \ldots, \alpha_n)$, $B = (\beta_1, \ldots, \beta_t)$, $C = (\epsilon_1, \ldots, \epsilon_p)$ then

$$(\beta_1, \ldots, \beta_t) = (\alpha_1\epsilon_1, \alpha_1\epsilon_2, \ldots, \alpha_i\epsilon_j, \ldots, \alpha_n\epsilon_p) .$$

Therefore every β_k is of the form

$$c_{11}\alpha_1\epsilon_1 + \ldots + c_{np}\alpha_n\epsilon_p = (c_{11}\epsilon_1)\alpha_1 + \ldots + (c_{np}\epsilon_p)\alpha_n$$

and hence an element of A. Hence $B \subset A$.

The converse of this theorem is also true, however its formal statement as a theorem and its proof will be delayed until Theorem 4.28.

Theorem 4.9. A nonzero rational integer t belongs to at most a finite number of ideals in $R(\theta)$.

Proof: If t does not belong to any ideals then the theorem is true. Suppose t is in at least one ideal, then every such ideal A can be expressed in the form $A = (\alpha_1, \ldots, \alpha_n)$ by Theorem 4.2. where n is the degree of $R(\theta)$. Let $b_1, \ldots, b_n$ be an integral basis for $R[\theta]$. Then $\alpha_i = c_{i1}b_1 + \ldots + c_{in}b_n$ with the c_{ij} being rational integers. Now there exists rational integers q_{ij} and r_{ij} such that $c_{ij} = tq_{ij} + r_{ij}$ with $0 \leq r_{ij} < t$. Note that it can be assumed that $t > 0$ since if t is in A then so is -t. Hence

$$\begin{aligned}\alpha_i &= (tq_{i1} + r_{i1})b_1 + \ldots + (tq_{in} + r_{in})b_n \\ &= t(q_{i1}b_1 + \ldots + q_{in}b_n) + r_{i1}b_1 + \ldots + r_{in}b_n \\ &= tx_i + \beta_i .\end{aligned}$$

Since the b_i's are fixed and $0 \leq r_{ij} < t$ there are only a finite number of choices for β_i no matter how many sets of $\alpha_1, \ldots, \alpha_n$ are chosen. It shall now be shown that $A = (\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n, t)$ and hence there will be only a finite number of ideals containing t since there are only a finite number of choices for $\beta_1, \ldots, \beta_n, t$ for a fixed t. Now

$$\begin{aligned}A &= (\alpha_1, \ldots, \alpha_n) \\ &= (\alpha_1, \ldots, \alpha_n, t) \quad \text{since t is in A} \\ &= (tx_1 + \beta_1, \ldots, tx_n + \beta_n, t) \\ &= (\beta_1, \ldots, \beta_n, t)\end{aligned}$$

by Theorem 4.3 since

$$\beta_i = (tx_i + \beta_i) - x_i t, \quad t = t, \quad \text{and} \quad tx_i + \beta_i = x_i(t) + 1(\beta_i)$$

Theorem 4.10. An ideal $A \neq (0)$ has only a finite number of factors.

Proof: This will be proven if it can be shown that A is a subset of only a finite number of ideals and then invoking Theorem 4.8. Since if A has infinitely many factors then each of these factors are ideals which contain A and hence there would be infinitely many ideals which would contain A.

Let $\alpha \neq 0$ be in A and $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be the minimal polynomial for α then $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha = -a_0 \neq 0$. Now $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha$ is in A since A is an ideal and each of the coefficients a_i are rational integers and hence in $R[\theta]$. Therefore the rational integer $-a_0$ is in A. By Theorem 4.9 there can only be a finite number of ideals which contain $-a_0$, therefore only a finite number of ideals which contain A.

Definition 4.11. An ideal $A \neq (0)$ or (1) is called a prime or maximal ideal if and only if for every ideal B such that $A \subset B$, then $B = A$ or $B = (1)$.

Theorem 4.12. A is a prime ideal if and only if $ab \in A$ implies either a or b is in A, where a and b are algebraic integers, $A \neq (0)$.

Proof: Suppose A is prime (maximal) and $A = (\alpha_1, \ldots, \alpha_n)$. Let $ab \in A$, if $b \in A$ then the theorem is true. If b is not in A then consider $B = (\alpha_1, \ldots, \alpha_n, b)$, it follows that $A \subset B$. A maximal implies $B = A$ or $B = (1)$. $B \neq A$ since $b \in B$ but $b \notin A$ therefore $B = (1)$. Now $1 \in B$ therefore

$$1 = c_1\alpha_1 + \ldots + c_n\alpha_n + db$$

which implies that

$$a = (ac_1)\alpha_1 + \ldots + (ac_n)\alpha_n + d(ab).$$

Since $\alpha_1, \ldots, \alpha_n, ab$ are in A so is a. Hence the conclusion follows.

Suppose $ab \in A$ implies a or b is in A. Let B be an ideal such that $A \subset B$ and $A \neq B$ then show $B = (1)$. If $A \neq B$ there is an $\alpha \in B$ such that $\alpha \notin A$ and there is a nonzero rational integer t in both A and B. As in the proof of Theorem 4.9, $\alpha = tx_1 + r_1b_1 + \ldots + r_nb_n$ where there are only a finite number of choices for the r_i and $b_1, \ldots, b_n$ is an integral basis for $R[\theta]$. Therefore, considering powers of α there are exponents p and q with $p > q$ such that $\alpha^p - \alpha^q = tx_p - tx_q$. That is, the set of coefficients of the b_i are the same for distinct powers of α. Now $t \in A$ implies $tx_1 - tx_q \in A$ which in turn implies that $\alpha^q(\alpha^{p-q} - 1) \in A$. $\alpha^q \notin A$ since if it were then one of its factors α^r would be in A by the hypothesis and hence one could arrive at the conclusion inductively that $\alpha \in A$. Therefore by the hypothesis $\alpha^{p-q} - 1 \in A$. $A \subset B$ implies $\alpha^{p-q} - 1$ is in B. Letting $\alpha^{p-q} - 1 = \beta$ it is seen that $-1 = \beta - \alpha^{p-q}$ is in B and hence $1 \in B$. Therefore $B = (1)$.

Theorem 4.13. If P is a prime ideal and $AB \subset P$ then $A \subset P$ or $B \subset P$, A, B ideals.

Proof: If $A \subset P$ then the theorem is true. Suppose $A \not\subset P$ then there is an α in A which is not in P. Let β be an arbitrary element

in B then $\alpha\beta \in AB$ and hence $\alpha\beta$ is in P. P a prime ideal implies β is in P by Theorem 4.12. Therefore $B \subset P$.

Theorem 4.14. If A is an ideal different from (0) or (1) then $A \supset P_1P_2 \cdots P_r$ for some finite collection of prime ideals P_i and further $A \subset P_i$, $i = 1, \ldots, r$.

Proof: If A is prime then the theorem is true. If A is not prime then Theorem 4.12 implies there is a product bc in A such that neither b nor c is in A. If $A = (\alpha_1, \ldots, \alpha_n)$ then consider $B = (\alpha_1, \ldots, \alpha_n, b)$ and $C = (\alpha_1, \ldots, \alpha_n, c)$ Now A is a proper subset of both B and C. Also if $x \in BC$ then

$$x = \sum_{i,j=1}^{n} a_{ij}\alpha_i\alpha_j + \sum_{i=1}^{n} b_i b\alpha_i + \sum_{i=1}^{n} c_i c\alpha_i + d(bc) .$$

Since either an α_i or bc is in each summand and A is an ideal, then each summand is an element of A and hence x is in A. Therefore $A \supset BC$. Repeat the procedure for B and C. This process will stop after a finite number of times since there are only a finite number of factors by Theorem 4.10 and hence only a finite number of ideals which contain A by Theorem 4.8. Hence A will contain a finite product of prime ideals with A contained in each.

Definition 4.15. If P is a prime ideal then

$$P^{-1} = \{x \in R(\theta) \mid xp \in R[\theta] \text{ for all } p \in P\} .$$

Theorem 4.16. If P is a prime ideal then P^{-1} contains an element which is not an algebraic integer.

Proof: Let $\alpha \neq 0$ be in P and consider the ideal (α). Theorem 4.14 implies $(\alpha) \supset P_1 \cdots P_r$ where the P_i are prime. If there are several choices for the product $P_1 \cdots P_r$ choose one where r is a minimum. $P \supset (\alpha)$ therefore by Theorem 4.13 some $P_i \subset P$. Without loss of generality let it be P_1. Since P_1 is maximal and $P \neq (1)$ this implies $P_1 = P$. Now since r was chosen to be a minimum, $(\alpha) \not\supset P_2 \cdots P_r$, where $P_2 = (1)$ if $r = 1$. Hence there is a nonzero element β in $P_2 \cdots P_r$ which is not in (α). Therefore $\frac{\beta}{\alpha}$ is not an algebraic integer since for every algebraic integer a, $a\alpha \neq \beta$ which implies there is no integer a such that $\frac{\beta}{\alpha} = a$. However since $\beta \in P_2 \cdots P_r$ it follows that $(\alpha) \supset P_1 \cdots P_r = P P_2 \cdots P_r \supset P(\beta)$. Therefore if ϵ is in P, $\epsilon\beta = b\alpha$ for some algebraic integer b which implies $\epsilon\frac{\beta}{\alpha}$ is in $R[\theta]$ for all ϵ in P. Hence $\frac{\beta}{\alpha}$ is in P^{-1} and $\frac{\beta}{\alpha}$ is the nonalgebraic integer in P^{-1} as asserted.

Theorem 4.17. If P is a prime ideal with x and y in P^{-1} then $x+y \in P^{-1}$ and $\epsilon x \in P^{-1}$ for every algebraic integer ϵ.

Proof: Let $\alpha \in P$ then $(x+y)\alpha = x\alpha + y\alpha$. Each of the summands on the right side of the equation is in $R[\theta]$ by definition of P^{-1} and hence their sum is in $R[\theta]$. Hence $x+y \in P^{-1}$.

Now $(\epsilon x)\alpha = \epsilon(x\alpha)$ and since $x\alpha$ is in $R[\theta]$ and ϵ is in $R[\theta]$ it is seen that $(\epsilon x)\alpha$ is in $R[\theta]$. Hence ϵx is in P^{-1}.

Definition 4.18. Let H be a nonempty set in $R(\theta)$ then H is a fractional ideal if there is an ideal K in $R[\theta]$ and an element b in $R(\theta)$ such that $H = bK$ where $bK = \{bk \mid k \in K\}$.

Note that if α and β are arbitrary algebraic integers and h_1, h_2 are in H then

$$\alpha h_1 + \beta h_2 = \alpha(b k_1) + \beta(b k_2) = b(\alpha k_1 + \alpha k_2) \varepsilon\, bK = H .$$

Theorem 4.19. If P is a prime ideal then P^{-1} is a fractional ideal. In fact $P^{-1} = \frac{1}{b} K$ where $b \neq 0$ is in P and $K = \{b x | x \varepsilon P^{-1}\}$.

Proof: Since P is prime $P \neq (0)$ and therefore there is an element b in P such that $b \neq 0$. Let $K = \{b x | x \varepsilon P^{-1}\}$. The definition of P^{-1} implies $b x \varepsilon R[\theta]$ and therefore K is a set of algebraic integers. Now to show K is an ideal

$$\begin{aligned} \alpha(b x_1) + \beta(b x_2) &= b(\alpha x_1) + b(\beta x_2) \\ &= b x_1' + b x_2' \,, \; x_1', x_2' \varepsilon P^{-1} \quad \text{by Thm. 4.17} \\ &= b(x_1' + x_2') \\ &= b x'' \qquad\qquad x'' \varepsilon P^{-1} \quad \text{by Thm. 4.17.} \end{aligned}$$

Therefore K is an ideal. Hence since

$$\frac{1}{b} K = \{\frac{1}{b}(b x) | x \varepsilon P^{-1}\} = \{x | x \varepsilon P^{-1}\} = P^{-1}$$

it is seen that P^{-1} is a fractional ideal.

Definition 4.20. If A is an ideal and B a fractional ideal with $B = d L$ where $d \varepsilon R(\theta)$ and L is an ideal then define $A B = d(A L)$

Notice that if P is a prime ideal this implies that if $P^{-1} = \frac{1}{b} K$ then

$$A P^{-1} = \{x | x \text{ is a finite sum of the form } \Sigma\, a_i \frac{k_i}{b} \,, \; a_i \varepsilon A, \; k_i \varepsilon K\}$$

Theorem 4.21. If A and B are ideals with $A \subset B$ then $AC \subset BC$ for every fractional ideal C.

Proof: Let $C = cL$ where $c \in R(\theta)$ and L is an ideal then $x \in AC$ implies $x = \sum_{i=1}^{c} a_i(c\ell_i)$ where $a_i \in A$ and $\ell_i \in L$ but $a_i \in A$ implies $a_i \in B$ therefore x is a finite sum of the form $\sum_{i=1}^{n} b_i(c\ell_i)$ with $b_i \in B$. Hence x is in BC. Therefore $AC \subset BC$.

Note that an ideal is also a fractional ideal and hence if C is an ideal in the above theorem then the theorem is still true.

Theorem 4.22. If P is a prime ideal then $PP^{-1} = (1)$.

Proof: Since P^{-1} is a fractional ideal $P^{-1} = \frac{1}{b}K$ for b and K as in Theorem 4.19. It will first be shown that PP^{-1} is an ideal. If $\alpha \in PP^{-1}$ then

$$\alpha = \sum_{i=1}^{r} \beta_i \frac{k_i}{b} = \sum_{i=1}^{r} \frac{\beta_i b x_i}{b} = \sum_{i=1}^{r} \beta_i x_i$$

which is in $R[\theta]$ where the β_i are in P, the $k_i = bx_i$ are in K, and the x_i are in P^{-1}. Therefore $PP^{-1} \subset R[\theta]$. Now consider

$$\alpha \sum_{i=1}^{r} \beta_i \frac{k_i}{b} + \epsilon \sum_{j=1}^{t} \beta_j' \frac{k_j'}{b} = \sum_{i=1}^{r} (\alpha\beta_i) \frac{k_i}{b} + \sum_{j=1}^{t} (\epsilon\beta_j') \frac{k_j'}{b}$$

where α, ϵ are arbitrary algebraic integers, the β_i and the β_j' are in P and the k_i and k_j' are in K. The $\alpha\beta_i$ and $\epsilon\beta_j'$ are elements of P since P is an ideal. Therefore, since each of the sums are finite and of the required form their sum is still finite and is of the same form and hence is an element of PP^{-1}. Therefore PP^{-1} is an ideal.

Next it shall be shown that $P \subset PP^{-1}$. $1 \in P^{-1}$ by definition of P^{-1}. Therefore let α be an arbitrary element in P then $\alpha = \alpha \cdot \frac{b \cdot 1}{b}$ which is a finite sum of the form $\sum_{i=1}^{r} \beta_i \frac{k_i}{b}$ and hence $\alpha \in PP^{-1}$. Hence $P \subset PP^{-1}$.

Now with P maximal, $P \subset PP^{-1}$ and PP^{-1} an ideal it is seen that $PP^{-1} = (1) = R[\theta]$ or $PP^{-1} = P$. Suppose $PP^{-1} = P$, as will be shown this cannot happen.

By Theorem 4.2 P has an integral basis $\omega_1, \ldots, \omega_n$ and by Theorem 4.16 there is an element r in P^{-1} which is not an algebraic integer. The products $r\omega_i$, $i = 1, \ldots, n$ are in P since it is assumed that $PP^{-1} = P$. Therefore $r\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$ for $i = 1, 2, \ldots, n$ where the a_{ij} are rational integers. Replacing ω_i by the variable x_i it is seen that the following system has a solution $x_i = \omega_i$, $i = 1, \ldots, n$ which is nontrivial since $P \neq (0)$ and hence $\omega_1 \neq 0$.

$$
\begin{aligned}
(a_{11} - r)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0 \\
a_{21}x_1 + (a_{22} - r)x_2 + \ldots + a_{2n}x_n &= 0 \\
&\vdots \\
a_{n1}x_1 + a_{n2}x_2 + \ldots + (a_{nn} - r)x_n &= 0
\end{aligned}
$$

Therefore by linear algebra the determinant of coefficients is 0. That is

$$
\begin{vmatrix}
a_{11} - r & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} - r & \cdots & a_{2n} \\
\vdots & & & \\
a_{n-1} & a_{n2} & \cdots & a_{nn} - r
\end{vmatrix} = 0 .
$$

Replacing r by the variable x and expanding one obtains an n^{th} degree polynomial with rational integer coefficients such that the coefficient of x^n is either 1 or -1. Hence r is a solution to a monic polynomial with integer coefficients and is therefore an algebraic integer. A contradiction to the choice of r and hence $PP^{-1} \neq P$. Therefore

$$PP^{-1} = (1) = R[\theta].$$

Theorem 4.23. If A and P are ideals with P prime and $A \subset P$ then AP^{-1} is an ideal.

Proof: $A \subset P$ implies $AP^{-1} \subset PP^{-1} = (1)$. Hence $AP^{-1} \subset R[\theta]$. By the note following Definition 4.20 $AP^{-1} = \frac{1}{b}(AK)$ where K is an ideal, hence AP^{-1} is a fractional ideal containing only algebraic integers and is therefore an ideal.

Theorem 4.24. Every ideal A not (0) or (1) is a product of prime ideals.

Proof: By Theorem 4.14, A contains a product of prime ideals. Choose a product so that the number of factors is a minimum. That is, $A \supset P_1P_2 \cdots P_n$ with n a minimum. Proof of the theorem will be by induction on n.

If $n = 1$ and B is any ideal such that $B \neq (1)$ and $B \supset P_1$ then $B = P_1$ since P_1 is maximal and $B \neq (1)$ and hence B is a product of maximal ideals. Letting $B = A$ the theorem is true for $n = 1$.

Suppose that for $r < n$, any ideal $B \neq (1)$ with $B \supset P_1 \cdots P_r$ with r the minimum such r then $B = P_1 \cdots P_r$.

Now let $A \supset P_1 \cdots P_n$ then

$$A P_n^{-1} \supset P_1 \cdots P_{n-1}(1) = P_1 \cdots P_{n-1}$$

by Theorem 4.21 together with $P_n P_n^{-1} = (1)$ by Theorem 4.22. Now $A P_n^{-1}$ is an ideal by Theorem 4.23 since $A \subset P_n$ by Theorem 4.14. Also $n-1$ is the minimum number of factors such that $A P_n^{-1} \supset P_1 \cdots P_{n-1}$. If not, $A P_n^{-1} \supset P_1 \cdots P_{n-1}$ implies $A \supset P_1 \cdots P_n$ and hence n would not be the minimum number of factors as was assumed at the beginning of the proof. Therefore by the induction hypothesis $A P_n^{-1} = P_1 \cdots P_{n-1}$ and hence $A = P_1 \cdots P_n$.

Theorem 4.25. If A and B are ideals with $A \subset B$, $A = P_1 \cdots P_n$, $B = Q_1 \cdots Q_t$, $P_i \neq (1)$, $Q_j \neq (1)$ and P_i, Q_j prime ideals then each Q_j occurs among the $P_1, P_2, \ldots, P_n$ at least as many times as it does as a factor of B.

Proof: Since Q_1 is a factor of B then $B \subset Q_1$ by Theorem 4.14. Hence $Q_1 \supset B \supset A \supset P_1 \cdots P_n$ and by Theorem 4.13 some $P_i \subset Q_1$. Without loss of generality let $P_1 \subset Q_1$. P_1 maximal and $Q_1 \neq (1)$ implies $P_1 = Q_1$. Therefore $Q_1 \cdots Q_t \supset P_1 \cdots P_n$ implies $Q_2 \cdots Q_t \supset P_2 \cdots P_n$.

Note that $t \leq n$ for if not, after the above procedure is applied n times, it can be concluded that $Q_{n+1} \cdots Q_t \supset (1)$. Therefore $Q_t \supset Q_{n+1} \cdots Q_t \supset (1)$ but $Q_t \neq (1)$.

Therefore, inductively it is seen that $P_i = Q_i$, $i = 1, \ldots, t$.

Theorem 4.26. The Fundamental Theorem of Ideals. An ideal not (0) or (1) in $R(\theta)$ can be represented uniquely except for order

as a product of prime ideals.

Proof: Let A be an ideal not (0) or (1) and suppose $A = P_1 \cdots P_n = Q_1 \cdots Q_t$. Let $A = P_1 \cdots P_n$ and $B = Q_1 \cdots Q_t$ in Theorem 4.25 then $A \subset B$ and $B \subset A$ hence $n = t$ and $P_1 = Q_1', \ldots, P_n = Q_t'$ for some arrangement $Q_1', \ldots, Q_t'$ of $Q_1, \ldots, Q_t$.

It shall now be shown that the above theorem is indeed a valid analog to the Fundamental Theorem of Arithmetic.

Replace the word integer by ideal in Definition 2.12 and Definition 2.14 to get the analogous definitions for a unit and a "prime" ideal respectively. Note that if A is an ideal then $A(1) = (1)A = A$ and that $(0)A = A(0) = (0)$ and hence the ideals (1) and (0) act as mulitplicative identity and zero respectively.

Substitution into the definition gives the following. Let A be an ideal then A is a unit if there is an ideal B such that $AB = (1)$. Let A be an ideal then A is a "prime" if $A \neq (0)$ or a unit and if $A = BC$ with B and C ideals implies that either B or C is a unit.

The idea of a unit has not been used in this chapter, however the concept of a prime ideal has been used but with a different definition than that above. It is now necessary to show that the definition of a prime ideal that has been used in this chapter implies the characterization of a "prime" ideal given in the preceding paragraph.

Now, (1) is a unit in the set of ideals of $R(\theta)$ and in fact it is the only unit. Notice that $(1) = (a)$ if a is an associate of 1, that is a is a unit. Suppose $A \neq (1)$ is a unit, then there is a B such that $AB = (1)$. However, $AB \subset A$ therefore $(1) \subset A$ which implies $A = (1)$, a contradiction.

Next it shall be shown that each definition of a prime ideal implies the other and hence an equivalent.

Assume that if P is a prime ideal and $P \subset A$ with A an ideal then $A = P$ or $A = (1)$. Now suppose $P = AB$ and neither A nor B is (1), then $P = AB$ implies that either A or B is a subset of P by Theorem 4.13 and that $(1) = ABP^{-1}$. Without loss of generality let $B \subset P$ then BP^{-1} is an ideal by Theorem 4.23. Now $BP^{-1} \neq (0)$ or (1) since $ABP^{-1} = (1)$. Therefore by the same argument as given two paragraphs before it is a contradiction that $A(BP^{-1}) = (1)$ with neither of the factors being (1). Therefore the supposition that neither A nor B is (1) is false and hence either A or B is (1). Hence the definition of a prime ideal which was used earlier in this chapter implies that if P is "prime" and $P = AB$ then A or B is a unit. The converse is also true. For assume that if P is a "prime" ideal and $P = AB$ then A or B is (1). Let $P \subset A$ then by Theorem 4.28 which will be proven shortly $A \mid P$ and hence $P = AB$ for some ideal B. Now by the definition being assumed A or B must be (1). If $A = (1)$ then the characterization follows. If $A \neq (1)$ then $B = (1)$ and hence $P = A(1) = A$.

Therefore the two concepts of a prime ideal are equivalent.

One of the main benefits of the Fundamental Theorem of Ideals is that it enables one to give a characterization of when unique factorization occurs in $R[\theta]$ in terms of the types of ideals which occur in $R[\theta]$.

Suppose the principal ideal (α) is a prime ideal, then α must be a prime algebraic integer in $R[\theta]$ for if not, $\alpha = \beta\delta$ where neither of β and δ are units. Therefore $(\alpha) = (\beta)(\delta)$ where $(\beta) \neq (1)$ and

$(\delta) \neq (1)$ hence (α) is not a prime ideal. A contradiction, hence α must be prime in $R[\theta]$. Now if every ideal A in $R[\theta]$ is a principal ideal one can write $A = (\alpha)$ and further A has a unique representation except for order as a product of prime ideals. That is, $(\alpha) = (\beta_1)(\beta_2)\cdots(\beta_n)$. As shown above, $\beta_1, \ldots, \beta_n$ are each prime algebraic integers in $R[\theta]$. Also $(\beta_i) = (\gamma)$ if and only if β_i and γ are associates by Theorem 4.5. Hence one can write the algebraic integer α uniquely as a product of primes in $R[\theta]$ except for order and multiplication by units as $\alpha = \beta_1\beta_2\cdots\beta_n$. This proves the sufficiency of Theorem 4.29. In order to prove the necessity several more theorems are needed.

Theorem 4.27. If A is an ideal then there is an ideal B such that $AB = (\alpha)$ where α is a rational integer.

Proof: If $A = (0)$ or (1) then the theorem is true. Suppose $A \neq (0)$ or (1) then let $A = P_1 \cdots P_n$ be the unique factorization of A into prime ideals. Now choose $b_i \in P_i$, $i = 1, \ldots, n$ such that b_i is a rational integer. This can be done since if $\beta \in P_i$ with $\beta \neq 0$, then $N(\beta)$ is in P_i and $N(\beta)$ is a rational integer. Then, as in Theorem 4.19, one can represent P_i^{-1} as $\frac{1}{b_i} K_i$, $i = 1, \ldots, n$ where K_i is an ideal. Therefore $A P_n^{-1} \cdots P_1^{-1} = (1)$ which implies $A\left(\frac{1}{b_n} K_n\right) \cdots \left(\frac{1}{b_1} K_1\right) = (1)$ and hence $\frac{1}{b_n \cdots b_1} A K_n \cdots K_1 = (1)$ which gives $A(K_n \cdots K_1) = (b_n \cdots b_1)$. Hence $K_n \cdots K_1$ is the required ideal and $b_n \cdots b_1$ is the rational integer α.

Theorem 4.28. If A and B are ideals and $B \subset A$ then $A \mid B$.

Proof: $B \subset A$ implies $BD \subset AD$ for every ideal D. Choose D such that $AD = (\alpha)$ for some rational integer α. Let $BD = (\beta_1, \ldots, \beta_n)$ then since $BD \subset AD$ $\beta_i = \epsilon_i \alpha$ for some algebraic integer ϵ_i, $i = 1, \ldots, n$. Hence $BD = (\alpha)(\epsilon_1, \ldots, \epsilon_n) = AD(\epsilon_1, \ldots, \epsilon_n)$. Therefore $Q_1 \cdots Q_t \, B = Q_1 \cdots Q_t \, A(\epsilon_1, \ldots, \epsilon_n)$ where $D = Q_1 \cdots Q_t$ is the unique factorization of D into prime ideals. Hence

$$Q_t^{-1} \cdots Q_1^{-1} Q_1 \cdots Q_t \, B = Q_t^{-1} \cdots Q_1^{-1} Q_1 \cdots Q_t \, A(\epsilon_1, \ldots, \epsilon_n)$$

and therefore $B = A(\epsilon_1, \ldots, \epsilon_n)$. That is, A is a factor of B.

Theorem 4.29. Let unique factorization (The Fundamental Theorem of Arithmetic) hold in $R[\theta]$ and let δ be a prime in $R[\theta]$ then (δ) is a prime ideal in $R[\theta]$.

Proof: Suppose $(\delta) = AB$ with neither A nor B being (1). Then there exists $\alpha \in A$, $\beta \in B$ such that $\delta \nmid \alpha$ and $\delta \nmid \beta$ but $a\delta = \alpha\beta$ for some algebraic integer a. To verify that there exist such α and β suppose without loss of generality that $\delta \mid \alpha$ for every α in A then $A = (c\delta)$. Now $(\delta) = (c\delta)B$ implies $(1) = (c)B$ which in turn implies there is a γ in B such that $c\gamma = 1$. Hence γ is a unit which implies $B = (1)$, a contradiction. Further, α is not a unit in $R[\theta]$ for if so $\epsilon\alpha = 1$ for some algebraic integer ϵ and hence $1 \in A$ and therefore $A = (1)$, a contradiction. Likewise for β. Since $a\delta = \alpha\beta$ this implies $\delta \mid \alpha\beta$. Now $\alpha\beta$ has a unique factorization into primes and since δ is a prime δ must be one of the prime factors. But α and β each have a unique factorization and therefore the product of these two factorizations must be the same as the factorization for $\alpha\beta$ except for the order and multiplication by units. Therefore δ must be a

factor of either α or β. Hence one of A or B must be (1) and therefore (δ) is a prime ideal.

Theorem 4.30. Unique factorization holds for the algebraic integers $R[\theta]$ if and only if every ideal in $R[\theta]$ is a principal ideal.

Proof: Assume unique factorization holds in $R[\theta]$. One now needs only to show that every prime ideal is a principal ideal since every ideal is a product of prime ideals and the product of principal ideals is a principal ideal.

Let P be a prime ideal and $\alpha \in P$. Since unique factorization holds, $\alpha = \beta_1\beta_2\cdots\beta_n$ where the β_i are prime algebraic integers. Now $(\alpha) = (\beta_1)(\beta_2)\cdots(\beta_n)$ and $P \supset (\alpha)$ which implies by Theorem 4.28 that $P \mid (\beta_1)(\beta_2)\cdots(\beta_n)$. Therefore $AP = (\beta_1)\cdots(\beta_n)$ for some A. Now A has a unique factorization of prime ideals, $A = Q_1\cdots Q_t$ and each of $(\beta_1),\ldots,(\beta_n)$ on prime ideals by Theorem 4.28. Hence $Q_1\cdots Q_t P$ and $(\beta_1)\cdots(\beta_n)$ are two prime factorizations of AP. Uniqueness of factorization gives $P = (\beta_k)$ for some k. Therefore P is a principal ideal.

If every ideal is a principal ideal then unique factorization holds as was shown in the paragraph preceding Theorem 4.27.

It was shown in Chapter II that $R[\sqrt{-5}]$ does not enjoy unique factorization. One can now show this by considering the ideal $(3, 1+2\sqrt{-5})$ and invoking Theorem 4.30 as follows.

As was shown in Chapter II both 3 and $1+2\sqrt{-5}$ are prime algebraic integers in $R(\sqrt{-5})$. Suppose that $(3, 1+2\sqrt{-5})$ is a principal ideal then there exists an algebraic integer β such that $(\beta) = (3, 1+2\sqrt{-5})$. Then $\beta \mid 3$ and $\beta \mid 1+2\sqrt{-5}$ but since both 3 and

$1+2\sqrt{-5}$ are prime this implies β is a unit. β a unit implies $(\beta)=(1)$. Also, as shown in Chapter II every element of $R[\sqrt{-5}]$ is of the form $3x+y\sqrt{-5}$ where x and y are rational integers. Therefore if $(1) = (3, 1+2\sqrt{-5})$ there must be rational integers a, b, c, d such that

$$3(a+b\sqrt{-5}) + (1+2\sqrt{-5})(c+d\sqrt{-5}) = 1$$

and hence

$$3a + c - 10d + \sqrt{-5}\,(3b+d+2c) = 1 .$$

Therefore one must have $3a + c - 10d = 1$ and $3b + d + 2c = 0$. Add these two equations to get $3(a+b-3d+c) = 1$. This cannot happen since 3 times a rational integer cannot be 1. Hence $(3, 1+2\sqrt{-5})$ is not a principle ideal and therefore by Theorem 4.30 unique factorization does not hold in $R[\sqrt{-5}]$.

CHAPTER V

FACTORIZATION IN QUADRATIC FIELDS

In the preceding chapters $R(\sqrt{-5})$ has been used as an example. It was determined that $R[\sqrt{-5}]$ does not enjoy unique factorization. This chapter is concerned with when $R[\sqrt{D}]$, D a rational integer, does or does not enjoy unique factorization.

Definition 5.1. If D is a rational integer other than 0 or 1 which has no square rational integer factors then D is called square free.

Through a number of published mathematical papers (see Chatland and Davenport [20] and Hardy and Wright [15]) it has been shown that the only square free rational integers, D, such that $R[\sqrt{D}]$ is a Euclidean domain and hence enjoys unique factorization (as will be shown) are the values $D = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

To prove that $d = -11, -7, -3, -2, -1$ are the only square free negative rational integers such that $R[\sqrt{D}]$ is a Euclidean domain is within the intended scope of this dissertation and will be done. However, to prove that the only positive square free D are the ones listed above such that $R[\sqrt{D}]$ is a Euclidean domain is a very long task, requiring the publishings of several mathematicians.

Using the definition that the norm of α, $N(\alpha)$, is the product of the field conjugates of α the following theorem gives a criteria as to when all ideals are principal in $R[\theta]$. Hence, a criteria as to when unique factorization holds in $R[\theta]$ by Theorem 4.30.

Theorem 5.2. Every ideal in $R[\theta]$ is principal if and only if for all algebraic integers a, b in $R[\theta]$, neither of which are zero and $b \nmid a$, then there exists algebraic integers α and β such that $0 < |N(\alpha a - \beta b)| < |N(b)|$.

Proof: Suppose every ideal of $R[\theta]$ is principal. Let a, b satisfy the conditions listed in the theorem. The ideal $A = (a, b)$ is principal and hence $(a, b) = (r)$ for some algebraic integer r. Now $b = \delta r$ for some δ in $R[\theta]$ hence $N(b) = N(\delta)N(r)$. Further b and r are not associates since if so $b \mid r$, but $r \mid a$ and therefore $b \mid a$, a contradiction to the assumption. Hence $|N(\delta)| > 1$, therefore $|N(b)| > |N(r)|$. Now r is in (a, b) therefore $r = \alpha a + (-\beta)b$ for some algebraic integers α and β. Hence $|N(\alpha a - \beta b)| = |N(r)| < N(b)$. Also $N(r) \neq 0$ since $N(b) \neq 0$ $(b \neq 0)$. Therefore $0 < |N(\alpha a - \beta b)| < |N(b)|$.

Now let the criteria be satisfied and A be a nonzero ideal of $R[\theta]$. For every δ in A, $N(\delta)$ is a rational integer, therefore one may choose b in A such that $|N(b)|$ is the minimum positive rational integer of $\{|N(x)| \mid x \in A\}$. Assert that $A = (b)$. For suppose that a is in A and $a \neq \delta b$, that is $b \nmid a$, then by the criteria there exist algebraic integers α and β such that $0 < |N(\alpha a - \beta b)| < N(b)$. A contradiction since $\alpha a - \beta b$ is in A and has norm less than $|N(b)|$ which is a contradiction to the choice of b.

When the special case of $\alpha = 1$ occurs in the preceding theorem, $R[\theta]$ is referred to as a Euclidean domain. However, the usual way of defining $R[\theta]$ as a Euclidean domain is as follows.

Definition 5.3. $R[\theta]$ is a Euclidean domain if there is a function E (referred to as a Euclidean norm) from $R[\theta] - \{0\}$ to the positive rational integers such that:

(1) $E(ab) = E(a)E(b)$, $a, b \in R[\theta] - \{0\}$

(2) Given $b \neq 0$ and a in $R[\theta]$ there exist q, r in $R[\theta]$ such that $a = bq + r$ and either $r = 0$ or $E(r) < E(b)$.

Theorem 5.4. The absolute value of the norm, $|N|$, is a Euclidean norm for $R[\theta]$ if and only if for every $b \neq 0$ and a in $R[\theta]$ there exists an algebraic integer q such that $|N(a - bq)| < |N(b)|$.

Proof: Suppose $|N|$ is a Euclidean norm for $R[\theta]$. (Note that since $N(\alpha\beta) = N(\alpha)N(\beta)$, it is a reasonable candidate.) Let $b \neq 0$ and a be arbitrary in $R[\theta]$. $|N|$ a Euclidean norm implies there exist q and r in $R[\theta]$ such that $a = bq + r$ with $r = 0$ or $|N(r)| < |N(b)|$. Therefore in either case $|N(a - bq)| = |N(r)| < |N(b)|$.

Now assume the criteria, $|N(\alpha\beta)| = |N(\alpha)|\,|N(\beta)|$, and part (1) of the definition of a Euclidean norm is satisfied. Let $r = a - bq$, that is $a = bq + r$. Hence $r = 0$ or by assumption, $|N(a - bq)| = |N(r)| < |N(b)|$. Hence $|N|$ is a Euclidean norm.

The following theorem is a result of combining Theorems 5.2, 5.4 and 4.30 after noting that if $b \nmid a$ in Theorem 5.4, then

$0 < |N(a - bq)| < |N(b)|$.

Theorem 5.5. If $|N|$ is a Euclidean norm for $R[\theta]$ then unique factorization holds in $R[\theta]$.

Proof: Follows directly from Theorem 5.2, 5.4 and 4.30 with $\alpha = 1$, $\beta = q$ in Theorem 5.4.

Notice that this theorem is not an if and only if theorem, that is, it may be possible (in fact it does happen) that $R[\theta]$ may enjoy unique factorization even though $|N|$ is not a Euclidean norm for $R[\theta]$.

The remainder of the chapter will be devoted to quadratic field extensions of the rational numbers.

Definition 5.6. If D is a nonsquare rational integer then $R(\sqrt{D})$ is called a quadratic field extension of the rational numbers.

Since $R(\sqrt{D})$ is the smallest field containing both R and $\sqrt{D}$ it follows that $R(\sqrt{D}) = \{x + y\sqrt{D} \mid x, y \in R\}$.

In the study of quadratic field extensions one restricts oneself to those values of D which are square free. For suppose that $D = m^2 D'$, then

$$R(\sqrt{D}) = \{x + y\sqrt{D} \mid x, y \in R\} = \{x + ym\sqrt{D'} \mid x, y \in R\} = R(\sqrt{D'})$$

since every rational number can be written in the form ym where y is a rational number and m is a fixed integer. Also notice that if D is the square of a rational integer then $R(\sqrt{D}) = R$ since $\sqrt{D}$ is a rational integer and hence the smallest field which contains R and the rational integer $\sqrt{D}$ is R itself.

Hence it shall be assumed throughout the rest of this chapter that when considering $R(\sqrt{D})$, D is a square free rational integer.

In a quadratic field, $R(\sqrt{D})$, the norm of $a+b\sqrt{D}$ is such that $N(a+b\sqrt{D}) = a^2 - Db^2$. Since D square free implies that $x^2 - D = 0$ is the minimal polynomial for $\sqrt{D}$ then, the conjugates of $\sqrt{D}$ are $\sqrt{D}$ and $-\sqrt{D}$. This gives, by Definition 3.24, that the field conjugates of $a+b\sqrt{D}$ are $a+b\sqrt{D}$ and $a+b(-\sqrt{D})$. The product $(a+b\sqrt{D})(a+b(-\sqrt{D})) = a^2 - Db^2$ by definition is the norm of $a+b\sqrt{D}$. An algebra calculation will verify that $N(\frac{\alpha}{\beta}) = \frac{N(\alpha)}{N(\beta)}$ for any α, β in $R(\theta)$ such that $\beta \neq 0$.

Theorem 5.4 can now be worded in the following way.

Theorem 5.7. The absolute value of the norm, $|N|$, is a Euclidean norm for $R[\theta]$ if and only if for every $b \neq 0$ and a which are in $R[\theta]$, there exists an algebraic integer q such that $|N(\frac{a}{b} - q)| < 1$.

Theorem 5.8. Let $D \not\equiv 1 \bmod 4$ then $a+b\sqrt{D}$ is an algebraic integer if and only if a and b are rational integers. If $D \equiv 1 \bmod 4$ then $a+b\sqrt{D}$ is an algebraic integer if and only if $a+b\sqrt{D} = \frac{\ell + m\sqrt{D}}{2}$ where ℓ and m are rational integers and ℓ and m have the same parity.

Proof: Since $\frac{\ell + m\sqrt{D}}{n}$, with ℓ, m, n rational integers satisfies $x^2 - \frac{2\ell}{n}x + \frac{\ell^2 - m^2 D}{n^2} = 0$ and hence $\frac{\ell + m\sqrt{D}}{n}$ is an algebraic integer if and only if $n \mid 2\ell$ and $n^2 \mid \ell^2 - m^2 D$. Without loss of generality, let $(\ell, m, n) = 1$.

Let p be an odd prime such that $p|n$ where $n|2\ell$ and $n^2|\ell^2 - m^2 D$. Then $p|\ell$ and hence implies $p^2|\ell^2$. Since $p^2|\ell^2 - m^2 D$ and D is square free this implies $p|m$. Hence $(\ell, m, n) \geq p$, a contradiction. Hence no odd prime can be a factor of n if $\frac{\ell + m\sqrt{D}}{n}$ is an algebraic integer. Suppose $4|n$ then $2|\ell$ and as above, this leads to the contradiction that $(\ell, m, n) \geq 2$. Therefore, since neither 4 nor an odd prime can be a factor of n, n must be 1 or 2.

If $n = 1$ there are no restrictions on D.

If $n = 2$ then $4|\ell^2 - m^2 D$ which implies $\ell^2 - m^2 D \equiv 0 \bmod 4$. Now D square free implies $4 \nmid D$ and therefore ℓ^2 and m^2 must be of the same parity if $\ell^2 - m^2 D \equiv 0 \bmod 4$. If ℓ and m are even then $(\ell, m, n) \geq 2$, a contradiction to the assumption. If ℓ and m are odd, $\ell^2 \equiv m^2 \equiv 1 \bmod 4$, therefore $\ell^2 - m^2 D \equiv 1 - D \equiv 0 \bmod 4$ or $D \equiv 1 \bmod 4$. The contrapositive gives that if $D \not\equiv 1 \bmod 4$ then $n = 1$ when $\frac{\ell + m\sqrt{D}}{n}$ is an algebraic integer.

If $D \equiv 1 \bmod 4$ then $\frac{e + f\sqrt{D}}{2}$ is an algebraic integer if both e and f are rational integers of the same parity. For if they are of the same parity and $D \equiv 1 \bmod 4$ then $e^2 - f^2 D \equiv 0 \bmod 4$ and hence, $2^2|e^2 - f^2 D$ and $2|2e$ which by the first part of the proof assures that $\frac{e + f\sqrt{D}}{2}$ is an algebraic integer.

Theorem 5.9. If D is a square free negative rational integer then $D = -1, -2, -3, -7, -11$ are the only values of D for which $R[\sqrt{D}]$ is a Euclidean domain.

Proof: Suppose $D \not\equiv 1 \bmod 4$ and consider $\frac{1 + \sqrt{D}}{2}$ with D a square free negative rational integer. Then with $a = 1 + \sqrt{D}$ and $b = 2$

Theorem 5.7 implies that if $R[\sqrt{D}]$ is a Euclidean domain there exists an algebraic integer $x+y\sqrt{D}$ (x, y are rational integers by Theorem 5.8) such that $|N(\frac{1+\sqrt{D}}{2} - (x+y\sqrt{D}))| < 1$. Now

$$\begin{aligned}\frac{1}{4} - \frac{1}{4}D &\leq \left(\frac{1}{2} - x\right)^2 - D\left(\frac{1}{2} - y\right)^2 \\ &= \left|\left(\frac{1}{2} - x\right)^2 - D\left(\frac{1}{2} - y\right)^2\right| \\ &= \left|N\left(\frac{1+\sqrt{D}}{2} - (x+y\sqrt{D})\right)\right| .\end{aligned}$$

Therefore if $\left|N\left(\frac{1+\sqrt{D}}{2} - (x+y\sqrt{D})\right)\right| < 1$ then $\frac{1}{4} - \frac{1}{4}D < 1$ which implies $D > -3$. Hence $D = -2$ or -1 are the only possible cases for which $R[\sqrt{D}]$ can be a Euclidean domain if $D \not\equiv 1 \bmod 4$ and D is a square free negative rational integer.

Now it shall be shown that $D = -1$ or -2 does give a Euclidean domain by the use of Theorem 5.7. Choose arbitrary a and b from $R[\sqrt{D}]$ such that $b \neq 0$. Then $\frac{a}{b} = u+v\sqrt{D}$. Choose rational integers x and y such that $|u-x| \leq \frac{1}{2}$ and $|v-y| \leq \frac{1}{2}$ then $x+y\sqrt{D}$ is an algebraic integer. Also,

$$\begin{aligned}|N(u+v\sqrt{D} - (x+y\sqrt{D}))| &= |(u-x)^2 - (v-y)^2 D| \\ &= (u-x)^2 - D(v-y)^2 \\ &\leq \frac{1}{4} - \frac{1}{4}D \\ &< 1 \text{ for } D = -1 \text{ or } -2 .\end{aligned}$$

Hence $R[\sqrt{D}]$ is a Euclidean domain for $D = -1$ and -2 by Theorem 5.7.

Suppose $D \equiv 1 \bmod 4$ and consider $\frac{1+\sqrt{D}}{4}$ with D a square free negative rational integer, then by Theorem 5.7 with $a = 1+\sqrt{D}$ and $b = 4$, there must exist an algebraic integer $\frac{x+y\sqrt{D}}{2}$, with x and y rational integers of the same parity, such that $\left|N\left(\frac{1+\sqrt{D}}{4}\right) - \left(\frac{x+y\sqrt{D}}{2}\right)\right| < 1$. Now

$$\frac{1}{16} - \frac{1}{16}D \leq \left(\frac{1}{4} - \frac{x}{2}\right)^2 - D\left(\frac{1}{4} - \frac{y}{2}\right)^2$$

$$= \left|N\left(\frac{1+\sqrt{D}}{4} - \left(\frac{x+y\sqrt{D}}{2}\right)\right)\right| .$$

Therefore, if $\left|N\left(\frac{1+\sqrt{D}}{4} - \left(\frac{x+y\sqrt{D}}{2}\right)\right)\right| < 1$ then $\frac{1}{16} - \frac{1}{16}D < 1$, which implies $D > -15$. But $D \equiv 1 \bmod 4$ therefore $D = -3, -7$ or -11. Hence $D = -3, -7$ or -11 are the only possible cases for which $R[\sqrt{D}]$ can be a Euclidean domain if $D \equiv 1 \bmod 4$ and D is a square free negative rational integer.

Now it shall be shown that $D = -3, -7$ or -11 does give a Euclidean domain by the use of Theorem 5.7. Choose arbitrary a and b from $R[\sqrt{D}]$ such that $b \neq 0$. Then $\frac{a}{b} = u+v\sqrt{D}$. Choose a rational integer y such that $|2v - y| \leq \frac{1}{2}$, then choose a rational integer x of the same parity such that $|2u - x| \leq 1$. Then $\frac{x+y\sqrt{D}}{2}$ is an algebraic integer in $R[\sqrt{D}]$ by Theorem 5.8. Now

$$\left|N\left(u+v\sqrt{D} - \left(\frac{x+y\sqrt{D}}{2}\right)\right)\right| = \left(u - \frac{x}{2}\right)^2 - D\left(v - \frac{y}{2}\right)^2$$

$$= \left(\frac{2u-x}{2}\right)^2 - D\left(\frac{2v-y}{2}\right)^2$$

$$\leq \left(\frac{1}{2}\right)^2 - D\left(\frac{\frac{1}{2}}{2}\right)^2$$

$$= \frac{1}{4} - \frac{1}{16} D$$

$$< 1 \text{ for } D = -3 \text{ or } -7 \text{ or } -11.$$

Hence $R[\sqrt{D}]$ is a Euclidean domain for $D = -3, -7$ and -11 by Theorem 5.7.

As was mentioned at the first of this chapter, it has been shown through a sequence of papers that the only square free positive rational integers D such that $R[\sqrt{D}]$ is a Euclidean domain are the values, $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$. Hardy and Wright [15] prove that $R[\sqrt{D}]$ is a Euclidean domain for $D = 2, 3, 5, 6, 7, 13, 17, 21$ and 29 using a method similar to the proof that $R[\sqrt{-2}]$ and $R[\sqrt{-1}]$ are Euclidean domains in Theorem 5.9. For the other values of D, H. Chatland [16] gives a bibliography of where the proofs might be found. Chatland's article mistakenly lists $R[\sqrt{97}]$ as a Euclidean domain, however in a later paper Barnes and Swinnerton-Dyer [18] proved that this is not the case.

As was proven earlier, if $R[\sqrt{D}]$ is a Euclidean domain then unique factorization holds in $R[\sqrt{D}]$. Now if $R[\sqrt{D}]$ is not a Euclidean domain then one can make no assertion as to whether or not unique factorization holds in $R[\sqrt{D}]$ simply on the basis that $R[\sqrt{D}]$ is not a Euclidean domain. Bolker [13] asserts that the following set of numbers is a complete listing of those square free rational integers $D < 100$ for which unique factorization holds in $R[\sqrt{D}]$: $\{-163, -67, -43, -19, -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 22, 23, 29, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97\}$.

In the above set, there are nine negative values. Stark [17] proved in 1967 that there are no other negative values of D for which

unique factorization holds. Bolker claims that it is not yet known whether or not unique factorization holds for infinitely many positive D.

CHAPTER VI

SUMMARY AND CONCLUSION

This dissertation was written so that it is within the grasp of the good undergraduate student which has had first courses in number theory, modern algebra and linear algebra. If the need should arise it could, with addition of problems and motivational paragraphs, be material for a seminar on the advanced undergraduate level. Used as such, it should strengthen the student's perception of both number theory and algebra. The basic work of the dissertation deals with the set of rational numbers, a concrete concept of the undergraduate student at this level. The student should learn that there is an extended concept of an integer and that with this extended concept one sometimes, but not always, has unique factorization.

Chapter I gives a brief history of the inception of algebraic number theory. Chapter II gives an introduction of what is involved when speaking of algebraic integers and unique factorization. Chapter III is a necessary background chapter on such topics as field extensions, symmetric polynomials and bases. Unfortunately it is not unified nor does it give the student an intuitive feel for the subject of factorization of algebraic integers. Chapter IV returns to the heart of the matter by characterizing those algebraic number fields in which unique factorization holds through the use of ideals. Chapter V uses the theory of Chapter IV on the specific case of quadratic field extensions. There

is a complete characterization of all those square free negative rational integral values of D for which unique factorization occurs in $R[\sqrt{D}]$.

Chapter V will give the advanced reader who wishes to do further research on the subject a direction to proceed. Namely, to complete the characterization of all those square free rational integral values of D for which unique factorization holds in $R[\sqrt{D}]$. This has been done through a series of papers, a beginning list of which can be found in Chapter V. The compilation of these into a comprehensive work could possibly be a worthwhile paper.

A SELECTED BIBLIOGRAPHY

[1] Dickson, L. E. History of the Theory of Numbers, Washington, Carnegie Institute, Vol. I, II, III, 1919.

[2] Motzkin, T. The Euclidean Algorithm, Bulletin American Mathematical Society, Vol. 55 (1949), pp. 1142-1146.

[3] Vandiver, H. S. Fermat's Last Theorem, American Mathematical Monthly, Vol. 53 (1946), pp. 555-578.

[4] Weiss, E. Algebraic Number Theory, McGraw-Hill, New York, N. Y., 1963.

[5] Ore, O. Number Theory and its History, McGraw-Hill, New York, N. Y., 1948.

[6] Shanks, D. Solved and Unsolved Problems in Number Theory, Spartan Books, Washington, D. C., Vol. I, 1962.

[7] Borevich and Shafarevich, Number Theory, Academic Press, New York and London, 1966.

[8] LeVeque, W. J. Topics in Number Theory, Vol. II, Addison-Wesley Publishing Company, Inc., 1956.

[9] Pollard, H. The Theory of Algebraic Numbers Carus Mathematical Monograph No. 9, Buffalo, N. Y.: Mathematical Association of America, 1950, John Wiley and Sons, Inc., New York.

[10] Herstein, I. N. Topics in Algebra, Blaisdell Publishing Company, Waltham, Massachusetts, 1964.

[11] Hohn, F. E. Elementary Matrix Algebra, 2nd edition, The Macmillan Company, New York, 1958 and 1964.

[12] Robinson, A. Numbers and Ideals, Holden-Day, San Francisco, 1965.

[13] Bolker, E. D. Elementary Number Theory, W. A. Benjamin, Inc., New York, 1970.

[14] Eichler, M. Introduction to the Theory of Algebraic Numbers and Functions, Academic Press, Inc., New York, 1966.

[15] Hardy and Wright, An Introduction to the Theory of Numbers, 4th edition, Oxford, 1960.

[16] Chatland, H. On the Euclidean Algorithm in Quadratic Number Fields, Bulletin American Mathematical Society, Vol. 55 (1949), pp. 948-953.

[17] Stark, H. There is no Tenth Complex Quadratic Field with Class Number One, Proc. Nat. Acad. Sci. U.S.A., Vol. 57 (1967), pp. 216-221.

[18] Barnes and Swinnerton-Dyer, Acta Mathematica, Vol. 87 (1952), pp. 259-323.

[19] Dubois and Steger, A Note on Division Algorithms in Imaginary Quadratic Number Fields, Canadian Journal of Mathematics, Vol. 10 (1958), pp. 285-286.

[20] Chatland and Davenport, Euclid's Algorithm in Real Quadratic Fields, Canadian Journal of Mathematics, Vol. 2 (1950), pp. 289-296.

[21] Dickson, L. E. New First Course in the Theory of Equations, John Wiley and Sons, New York, 1939.

VITA[2]

Verlin F. Koper

Candidate for the Degree of

Doctor of Education

Thesis: FACTORING ALGEBRAIC INTEGERS

Major Field: Higher Education

Biographical:

Personal Data: Born in Hobart, Oklahoma, December 9, 1938, the son of Fred and Lorene Koper.

Education: Attended Rocky grade school and graduated from Rocky highschool, Rocky, Oklahoma, in 1957; received the Bachelor of Science degree from Southwestern State College, Weatherford, Oklahoma in 1961 with a double major of mathematics and physics; attended Sayre Junior College for the spring semester of 1958; attended the University of Missouri, Columbia, Missouri, from the fall semester of 1961 until the end of summer school in 1964; received the Master of Arts degree in mathematics at the end of the spring semester in 1963 from the University of Missouri; attended Oklahoma State University and completed requirements for the Doctor of Education degree between the fall semester of 1969 and the end of summer school in 1971.

Professional Experience: Taught mathematics as a graduate assistant in mathematics at the University of Missouri, Columbia, Missouri, from the fall semester 1961 until the end of summer school in 1964. Also taught as an extension instructor for the University of Missouri at their Normandy campus; was an instructor and then an assistant professor of mathematics at Southwestern State College, Weatherford, Oklahoma from the fall semester of 1964 until the end of summer school, 1969; and have taught as a graduate assistant at Oklahoma State University from the fall semester of 1969 through the spring semester of 1971.