ON THE
UNIQUE FACTORIZATION THEOREM

By

Shukri Tahir-al-Kawwas

Submitted in Partial Fulfillment for the Requirements
of the Degree Master of Science
in the Mathematics Department of the
American University of Beirut
Beirut, Lebanon,
1964

UNIQUE FACTORIZATION

Shukri Tahir-al-Kawwas

ACKNOWLEDGEMENT

The writer wishes to express his deepest gratitude and his sincere appreciation to Dr. Amin Muwafi for suggesting the topic of this thesis and for his valuable assistance in its preparation.

He is also indebted to Miss Mona Jabbour, and would like to thank her for typing the manuscript.

ABSTRACT

The thesis is concerned with the discussion of the unique factorization theorem in different systems, mainly in the imaginary quadratic fields of the form $R(\sqrt{m})$ where m is a square free negative integer, and R denotes the real numbers. A quadratic field is called simple if the unique factorization theorem holds in that system. Necessary conditions are given for which $R(\sqrt{m})$ is simple.

A short discussion of the unique factorization for polynomials and permutations is given.

Some systems are not simple. One such example is $R(\sqrt{-5})$. The ideal theory is introduced to restore uniqueness of factorization in such fields. Some examples are given to show how this can be done by shifting the emphasis from factorization into prime factors to that of factorization into prime ideals.

TABLE OF CONTENTS

Page

CHAPTER I - INTRODUCTION

1. Definitions 1

2. Statement of the problem 2

CHAPTER II - UNIQUE FACTORIZATION IN OTHER SYSTEMS

1. Unique factorization for natural numbers... 3

2. Unique factorization for integers 4

3. A system in which the unique factorization does not hold 4

4. Factorization of polynomials 5

5. Factorization of permutations 7

CHAPTER III - UNIQUE FACTORIZATION IN IMAGINARY QUADRATIC FIELDS

1. Introduction 10

2. Gaussian numbers 10

3. The fields $R(\sqrt{-2})$, $R(\sqrt{-3})$ 11

4. The fields $R(\sqrt{m})$ 12

5. Conclusions 16

CHAPTER IV - IDEALS

1. Introduction 18

2. Arithmetic of ideals 19

3. Restoration of unique factorization in terms of ideals 20

BIBLIOGRAPHY 26

CHAPTER I

INTRODUCTION

1. Definitions.

a) Divisibility: An integer a is said to be divisible by an integer b if there exists an integer c such that

$$a = bc.$$

We write $b|a$, and say that b divides a or a is a multiple of b.

b) Primes: A non zero integer p other than ± 1 is called a prime if its only divisers are ± 1 and $\pm p$.

Later we shall see why we exclude 1 from the primes.

c) Algebraic integers: An algebraic integer is a number which satisfies an equation of the form:

$$x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_o = 0$$

where the a_i's are rational integers.

d) Units and primes in the ring of algebraicintegers:

ε is a unit if it divides 1.

An algebraic integer α is prime if it is not zero or a unit and if any factorization

$\alpha = \beta\gamma$ into algebraic integers implies that either

β or γ is a unit.

α and β are associates if $\alpha = \varepsilon\beta$.

2. Statement of the problem.

The fundamental theorem of arithmetic states that: "Every rational integer greater than one can be expressed as the product of primes. This representation is unique except possibly for the order in which the prime factors occur." This is sometimes called the unique factorization theorem for integers.

If we extend the meaning of integer to include algebraic integers in a quadratic field, the question that arises is whether the unique factorization theorem still holds. There are some quadratic fields in which uniqueness of factorization is not valid. The quadratic field $R(\sqrt{-5})$ is one example. The ideal theory is introduced to restore uniqueness of factorization in such fields. In a later chapter, we shall define an ideal, an irreducible ideal, divisibility for ideals and other arithmetics for ideals. Also we shall see that there is a completely satisfactory arithmetic for ideals. The problem will be settled by shifting the emphasis from the factorization of integers to that of ideals.

The introduction of the ideal factors is due to Kummer, but the form that we use here is due to Dedekind.

CHAPTER II

UNIQUE FACTORIZATION IN OTHER SYSTEMS

1. Unique factorization for the natural numbers.

In the set of natural numbers a prime is defined as a natural number greater than one which is divisible only by 1 and itself. The fundemental theorem of arithmetic in this set states that:

"Every positive integer greater than 1 can be expressed as the product of primes in one and only one way except possibly for the order." It is to be understood that as a special case, a "product" of primes may consist of a single prime. This agreement is to take care of the case in which the integer itself is prime. This means that the process of factorization of any positive integer will always lead to the same prime factors. With this in mind, we shall see why 1 is excluded from the list of primes. For if 1 is considered as a prime, then it will be possible for every positive integer to be factored as the product of primes in two different ways. For example, $6 = 2 \times 3$ is one factorization into primes, and $6 = 2 \times 3 \times 1$ is another. Hence 1 is not considered as a prime unless we wish to change the statement of the theorem.

A prime integer in this set may be defined as a number different from 1, having no factors in C other than 1 and itself. According to this definition 10 and 19 are primes in C, 10 x 19 = 190 is in C, and it is not prime in C. Hence there are integers in C which are not primes.

The unique factorization theorem does not hold in C, because we can find a number in C which can be expressed as a product of prime factors in two different ways:

$2530 = 9 \times 281 + 1$. Hence 2530 is in C.

$2530 = 46 \times 55$ and $2530 = 10 \times 253$.

All these factors are in C because each can be written in the form $9n+1$, where n is a positive integer. Also, all these factors are prime in C. Therefore 2530 is a number in C and it is possible to express it as the product of primes in C in the two different ways. This shows that the unique factorization theorem does not hold in C. Because of this, we see that C has some unusual properties. 10 and 46 are relatively prime in C, and each is a factor of 2530 in C, but their product is not a factor of 2530 in C. Such a property can't happen in systems where uniqueness of factorization holds.

4. Factorization of polynomials. [3, p.142].

Let F[x] denote the ring of polynomial functions in the indeterminate x over a field F. If f(x) and g(x) are

The proof of this theorem [5, p.11]+ may be found in any standard text on the theory of numbers.

2. The Unique factorization theorem for integers.

The two integers +1, -1 are factors of every integer. Thus we exclude $\pm$ 1 from the list of primes.

An integer p is said to be prime if it is different from 0, $\pm$ 1 and has no factors other than $\pm$ 1, $\pm$ p.

Any integer may be expressed as the product of primes in more than one way. For example, 10 = 2 x 5 and 10 = (-2)x(-5), and these are two different representations of 10 as a product of primes.

With these remarks in mind, the unique factorization theorem should be modified to read:
"Every integer other than 0, $\pm$ 1 is either prime or it can be expressed as a product of prime factors uniquely, except possibly for the order and the sign of the factors."
For the proof of this theorem see [5, p.13].

3. A system in which the unique factorization does not hold.

Let C denote the set of all integers of the form 9n+1, where n is a positive integer or zero

$$C = \{ 1, 10, 19, \ldots, 9n+1, \ldots \}$$

+ [5, p.11] = Page 11 of the book whose number is 5 in the entries of the bibliography. Here, and within the text hereafter, square brackets like this will have corresponding meaning.

are in F[x], then g(x) is said to be a divisor of f(x) if there is a polynomial h(x) in F[x] such that $f(x) = g(x)\ h(x)$. We say that f(x) is divisible by g(x) or it is a multiple of g(x) and write $g(x)|f(x)$.

If K is a non zero constant in F[x], that is K is a non zero polynomial of degree zero over F, then it follows that K^{-1} is in F, and

$$f(x) = K^{-1}(K\ f(x))$$

this implies that K f(x) is always a factor of f(x). Thus if

$$f(x) = g(x)\ \ h(x)$$

is any factorization of f(x), then

$$f(x) = (K\ g(x))(K^{-1}\ h(x))$$

is another.

Hence the definition of a prime polynomial must exclude all polynomials of degree zero. The polynomial p(x) of positive degree over a field F is said to be prime if p(x) can't be expressed as the product of two polynomials of positive degree over F.

Because the degree of the product of two polynomials over F is the sum of the degrees of the factors, it follows that any polynomial of degree 1 over F is prime over F.

It should be pointed out that a polynomial p(x)

may be prime over a field F_1, but ceases to be prime over another field F_2. For example the polynomial $x^2 + 1$ is prime over the field of real numbers, but it is not prime over the field of complex numbers.

Thus the unique factorization theorem for F[x] states that: [3, p.143].

"Any polynomial f(x) of positive degree over the field F can be expressed uniquely as the product of prime polynomials over F except possibly for the order of the factors."

5. Factorization of permutations. [4, p.70].

A permutation is a one to one mapping of a set onto itself. The permutation in which every element is mapped onto itself is called the identity permutation and is denoted by (1).

The product of two permutations is defined as the resultant of the two mappings.

For a set of n sumbols, there are n! possible mappings. The set of all such permutations forms a group under the product operation.

Let $S = \{a_1, a_2, \ldots, a_n\}$ be a set of n symbols. The permutation π is said to be a cycle of length r if π permutes a subset $\{a_1, a_2, \ldots, a_r\}$ of S, such that

$$a_i\pi = a_{i+1},\ i = 1, 2, \ldots, r - 1 \text{ and } a_r\pi = a_1,$$

and leaves all the other elements of S unchanged. This permutation is denoted by

$$(a_1\ a_2\ \ldots\ a_r).$$

If π is a permutation of length 2, then π is called a transposition.

Every permutation can be expressed as the product of two disjoint cycles [4, p.68], and every cycle can be written as a product of transpositions. For example the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}$$

can be written as

$$(13)(2564)$$

which can be written as

$$(13)(25)(26)(24)$$

and this is a representation of the permutation as the product of transposition. However, this representation is not unique because we could have added the transpositions (26)(26) without affecting the permutation since (26)(26) = (1) which is the identity permutation. Thus the number of transpositions, in the representation of a certain permutation as the product of transpositions, is not unique as asserted by the following theorem which is due to Cauchy [4,p.70].

"If a permutation π on n symbols can be factored into K disjoint cycles, the number of transpositions in any representation of π as a product of transpositions is either always even or always odd according as n-K is even or odd."

CHAPTER III

UNIQUE FACTORIZATIONS IN IMAGINARY QUADRATIC FIELDS

1. Introduction.

Let F be a field and θ be algebraic over F. $F(\theta)$ is defined to be the smallest field containing both F and θ, and is called a simple algebraic extension of F.

In the following discussion R denotes the field of real numbers and θ will be of the form $\sqrt{m}$, where m is a square free rational integer. That is $R(\sqrt{m})$ will denote a quadratic field. If $m < 0$, then $R(\sqrt{m})$ will denote a complex quadratic field.

$R(\sqrt{m})$ will be called simple if every integer in $R(\sqrt{m})$ can be expressed uniquely as the product of prime integers in $R(\sqrt{m})$ except possibly for the order and multiplication by units.

2. Gaussian numbers.

Consider the field $R(\sqrt{-1})$ which is called the field of Gaussian numbers. Every number in this field is of the form $a + b\sqrt{-1}$, where a and b are real numbers. The ring of Gaussian integers is the set of all numbers of the form $a + b\sqrt{-1}$, where a and b are rational integers.
It is clear that any rational integer is a Gaussian integer, but the converse is not necessarily true.

A Gaussian integer is prime if it is not zero or a unit, and its only factors are itself and the units. More precisely, p is a prime Gaussian integer if every factorization $p = \alpha\beta$ into Gaussian integers implies that either α or β is a unit.

A rational prime may be a Gaussian prime, but there are rational primes which are not Gaussian primes. For example $5 = (1 + \sqrt{-2})(1 - \sqrt{-2})$. The set of Gaussian primes G is divided into three classes [6, p.17].

1. Every positive rational prime of the form 4m + 3 and their associates in G.

2. The number 1 + i and its associates.

3. All Gaussian integers which are associated with either x + iy or x - iy, where $x > 0$, $y > 0$ x is even and $x^2 + y^2$ is a rational prime of the form 4m + 1.

The unique factorization theorem for the Gaussian integers states that [2, p.185].

"A Gaussian integer, which is not zero or a unit, can be expressed as the product of primes uniquely, except possibly for the order and multiplication by units."

3. The fields $R(\sqrt{-2})$ $R(\sqrt{-3})$.

The fields $R(\sqrt{-2})$, $R(\sqrt{-3})$ are Euclidean in the sense that if ρ and σ are integers in $R(\sqrt{m})$, with $\sigma \neq 0$, there exist integers π and δ of $R(\sqrt{m})$ such that $\rho = \sigma\pi + \delta$ with

$N(\delta) < N(\sigma)$. $N(\delta)$ being defined as the product of δ and its conjugate in $R(\sqrt{m})$.

But since every Euclidean quadratic field is simple, it follows that $R(\sqrt{-2})$ and $R(\sqrt{-3})$ are simple. [5, p.192,193].

4. The fields $R(\sqrt{m})$, $m < -3$.

The following two theorems are needed for later development in the subject. We state them here for reference.

Theorem 3.1: [1, p.154].

If $m < -3$ and if $R(\sqrt{m})$ is simple then

$$m \equiv 1 \pmod 4$$

Theorem 3.2: [1, p.154].

If $m < -3$ and $R(\sqrt{m})$ is simple, then all the following numbers are rational primes

$$N = a^2 - ab - qb^2$$

(where $q = \frac{m-1}{4}$) provided that

$$1 < N < q^2 \quad \text{and} \quad g.c.d(a,b) = 1$$

Theorem 3.3:

Let $m < -5$. If $m \equiv 1 \pmod 4$ and $q(q = \frac{m-1}{4})$ is not prime, then $R(\sqrt{m})$ is not simple.

Proof:

$$-q = 1 - 1 - q$$

therefore

$-q = N$ in theorem 3.2, with $a = b = 1$

Now

$(a,b) = 1$

and

$-q < q^2$ because $-q$ is a rational integer

also

$-q > 1$ by definition of q, and because $m < -5$.

Applying theorem 3.2 we have :

If $-q$ is not prime then $R(\sqrt{m})$ is not simple. But $-q$ is prime if and only if q is prime. Hence, if q is not prime, then $R(\sqrt{m})$ is not simple.

Theorem 3.4:

Let $m < -11$. If $m \equiv 1 \pmod 4$ and m is not prime, then $R(\sqrt{m})$ is not simple.

Proof:

Since

$m \equiv 1 \pmod 4$, it follows that

$q = \frac{m-1}{4}$ is an integer.

$m = 4q + 1$

$|m| = -1 - 4q$

$= 1 - 2 - 4q$

Therefore $|m| = N$ in theorem 3.2, with $a = 1$ and $b = 2$

Now

$(1,2) = 1$

and

$$|m| > 1 \qquad \text{because } m < -11$$

Since

$$m < -11$$

we have

$$q < -3 \quad \text{or} \quad |q| > 3.$$

Therefore

$$|q| \geq 4$$

and this implies that

$$|q|^2 \geq 4\,|q|$$

or

$$|q^2| > 4\,|q| - 1.$$

That is

$$q^2 > -4q - 1$$

or

$$q^2 > |m|$$

Therefore

$$|<|m| < q^2.$$

Applying theorem 3.2 we have:

If $|m|$ is not prime, then $R(\sqrt{m})$ is not simple. The theorem follows since $|m|$ is prime if and only if m is prime.

Theorem 3.5:

Let $m < -7$. If $m \not\equiv 5 \pmod 8$, then $R(\sqrt{m})$ is not simple.

Proof:

Suppose that $R(\sqrt{m})$ is simple, then

$$m \equiv 1 \pmod 4, \quad \text{by theorem 3.1}$$

Hence

$$m \equiv 1 \text{ or } 5 \pmod 8$$

We have to show that $m \not\equiv 1 \pmod 8$.

If $m \equiv 1 \pmod 8$, that is $m = 8u + 1$, then $q = 2u$ which is not prime when $m < -7$.

This implies that $R(\sqrt{m})$ is not simple by theorem 3.3.

Therefore

$$m \not\equiv 1 \pmod 8$$

and hence

$$m \equiv 5 \pmod 8$$

And this is a contradiction.

Hence the theorem follows.

Theorem 3.6:

Let $m < -11$. If $m \not\equiv 5 \pmod{24}$ then $R(\sqrt{m})$ is not simple.

Proof:

Suppose that $R(\sqrt{m})$ is simple, then

$$m \equiv 5 \pmod 8 \quad \text{by theorem 3.5}$$

or

$$m \equiv 5, 13 \text{ or } 21 \pmod{24}$$

we shall prove that $m \not\equiv 13$ or $21 \pmod{24}$.

1) If $m \equiv 13 \pmod{24}$, that is $m = 24u + 13$, where $u < -1$, because $m < -11$

then

$q = 6u + 3$ and this is not prime because $u < -1$.

By theorem 3.3 $R(\sqrt{m})$ is not simple.

Therefore

$$m \not\equiv 13 \pmod{24}.$$

2) If $m \equiv 21 \pmod{24}$

that is if $m = 24u + 21$, where $u < -1$, because $m < -11$, then m is not prime when $u < -1$, that is when $m < -11$. Therefore $R(\sqrt{m})$ is not simple by theorem 3.3, therefore $m \not\equiv 21 \pmod{24}$.

Therefore $m \equiv 5 \pmod{24}$, and this is a contradiction. Therefore the theorem follows.

5. Conclusions.

From the previous theorems we concluce the following

1) If $m = -1, -2, -3,$ then $R(\sqrt{m})$ is simple.

2) If $m = -5, -6,$ then $R(\sqrt{m})$ is not simple by theorem 3.1

3) If $m = -7,$ then $R(\sqrt{m})$ is simple [2, p.213]

4) If $m = -10,$ then $R(\sqrt{m})$ is not simple by theorem 3.1

5) If $m = -11,$ then $R(\sqrt{m})$ is simple [2, p.213]

6) If $m < -11,$ then for all m such that $m \not\equiv 5 \pmod{24}$ $R(\sqrt{m})$ is not simple. Thus the possible values of m, $-170 < m < -11$, for which $R(\sqrt{m})$ is simple are

$$-19, -43, -67, -91, -115, -139, -163.$$

But if $m = -91$ or -115, then by theorem 3.4 $R(\sqrt{m})$ is not simple.

If $m = -139$, then by theorem 3.3 $R(\sqrt{m})$ is not simple.

Therefore, the remaining values of m for which $R(\sqrt{m})$ is

is possibly simple are

$$-19, -43, -67, -163$$

and for these values $R(\sqrt{m})$ is simple. [1, p.156].

If $m < -170$, then there is at most one value of m for which $R(\sqrt{m})$ is simple. This fact was proved by Heilbronn and Linfoot in their book "On the imaginary quadratic corpora of class number one". Lehmer proved that if such value of m exists it should be $< -5 \times 10^9$.

CHAPTER IV

IDEALS

1. Definitions.

Let K be a number field. An ideal A in K is a nonempty subset of integers in K possessing the following property: If ρ and σ belong to A, so does $\delta\rho + \pi\sigma$, where δ and π are also integers in K.

Let $\rho_1, \rho_2, \ldots, \rho_n$ be integers of K, we say that the ideal A is generated by $\rho_1, \rho_2, \ldots, \rho_n$ if A consists of integers of the form

$$\rho_1 \sigma_1 + \rho_2 \sigma_2 + \ldots + \rho_n \sigma_n,$$

where σ_i's are integers of K. This ideal will be denoted by $[\rho_1, \rho_2, \ldots, \rho_n]$.

If A is generated by one element ρ_1 then A is called a principal ideal, and is denoted by $[\rho_1]$. The ideal [0] is the ideal consisting of 0 only. A set of integers $\delta_1, \delta_2, \ldots, \delta_m$ is said to be a basis for the ideal A if every number π of A can be uniquely represented in the form

$$c_1\delta_1 + c_2\delta_2 + \ldots + c_n\delta_n$$

where c_i are rational integers.

It is obvious that if $\delta_1, \delta_2, \ldots, \delta_m$ is a basis for A, then $\delta_1, \delta_2, \ldots, \delta_m$ generate A. But the converse

is not necessarily true. To show this consider the ideal $A = [3]$ in $R(\sqrt{-3})$. This is generated by 3, but 3 is not a basis for A, because any number in A is of the form $3a + 3b\sqrt{-3}$, where a and b are rational integers. Hence $3, 3\sqrt{-3}$ is a basis for A in $R(\sqrt{-3})$.

2. Arithmetic of ideals.

If A and B are two ideals, then A is said to be equal to B if A and B sonsist of the same elements.

If

$$A = [\rho_1, \rho_2, \ldots, \rho_n]$$

and

$$B = [\delta_1, \delta_2, \ldots, \delta_m]$$

then the product AB is defined as the ideal

$$[\rho_1\delta_1, \rho_2\delta_1, \ldots, \rho_n\delta_1, \rho_1\delta_2, \ldots, \rho_n\delta_2, \ldots, \rho_n\delta_m].$$

From this definition of product we can see that multiplication of ideals is commutative and associative. i.e.

$$AB = BA \quad \text{and} \quad A(BC) = (AB)C.$$

If A and B are two ideals, it is said that A divides B, written $A|B$, if an ideal C exists so that $B = AC$. A is then called a factor of B. A divisor is defined in a different way; A is called a divisor of B if every element of B is contained in A.

An ideal P, which is not [1] or [0] is called

irreducible if it has no factors except P and [1].

3. Restoration of unique factorization in terms of ideals.[7,253].

Let C be the set of positive integers which are $\equiv 1 \pmod 5$, that is

$$C = \{1, 6, 11, 16, \ldots\}$$

an integer a in C is said to be divisible by another integer b in C if there exists an integer c in C such that

$$a = bc$$

An integer $p \neq 1$ in C is said to be prime if its only divisors in C are 1 and p.

The unique factorization theorem does not hold in C, because it is possible to find an integer in C which can be expressed as the product of prime factors in C in two different ways.

$1806 \equiv 1 \pmod 5$, hence 1806 is in C.

$1806 = 21 \times 86$ and $1806 = 6 \times 301$.

All these factors are in C, because each is $\equiv 1 \pmod 5$.
Also, all are prime integers in C.
Therefore, 1806 is an integer in C which can be expressed as the product of two integers in C in two different ways.
Hence the unique factorization theorem does not hold in C.
The reason for this failure of the theorem lies in the

absence of the remaining positive integers from C. This failure can be remedied by introducing a new kind of numbers in C. Each of these new numbers is defined as the greatest common divisor of a pair of integers in C. That is it is defined by a pair of integers in C.

Consider

$$1806 = 21 \times 86 = 6 \times 301$$

21 is a factorof6x 301 and it is neither a factor of 6 nor a factor of 301. Therefore it is the product of two factors, one is contained in 6 and the other is contained in 301. Denote these two factors by the pairs (21,6) and (21,301) respectively. In this case, (21,6) is the greatest common divisor of 21 and 6, and the same for (21,301).

According to this notation

$$21 = (21,6)(21,301).$$

The change of the order of the integers in paranthesis has no effect, that is $(6,21) = (21,6)$.

Similarly we have:

$$86 = (86,6)(86,301)$$

$$6 = (6,21)(6,86)$$

and

$$301 = (301,21)(301,86).$$

and hence

$$1806 = 21 \times 86 = (21,6)(21,301)(86,6)(86,301)$$

$$= 6 \times 301 = (6,21)(6,86)(301,21)(301,86)$$

and the factorization is seen to be the same except for the order.

The same reasoning may be applied to the example of section 3, chapter II.

In that example

$$2530 = 46 \times 55 = 10 \times 253$$

using the same notation as above, we have

$$46 = (46,10)(46,253)$$

$$55 = (55,10)(55,253)$$

$$10 = (10,46)(10,55)$$

$$253 = (253,46)(253,55)$$

and

$$2530 = 46 \times 55 = (46,10)(46,253)(55,10)(55,253)$$

$$= 10 \times 253 = (10,46)(10,55)(253,46)(253,55).$$

The factorization is seen to be the same.

We have seen that uniqueness of factorization, in certain domains, may be restored by introducing a new kind of numbers defined by pairs of integers of the domain. Each of these numbers is the greatest common divisor of the defining pair of integers. These numbers may be called the ideal numbers of the domain.

This idea can't be extended to the fields $R(\sqrt{m})$ in which uniqueness of factorization does not hold. However, new numbers may be introduced in such fields to restore uniqueness of factorization. These numbers are not taken

to be the greatest common divisors of pairs of integers of $R(\sqrt{m})$, but as the greatest common divisors of an infinite number of integers of $R(\sqrt{m})$. That is, if A is one of these numbers, then it is defined as the greatest common divisor of the integers

$$S = \{ \alpha_1, \alpha_2, \alpha_3, \ldots \}$$

where α_i is an integer in $R(\sqrt{m})$.
A will be defined by a finite number of these integers. That is

$$A = [\beta_1, \beta_2, \ldots, \beta_n] \ , \ \beta_i \text{ in } S,$$

such that for all α in S

$$\alpha = \lambda_1 \beta_1 + \lambda_2 \beta_2 + \ldots + \lambda_n \beta_n,$$

where λ_i is an integer in $R(\sqrt{m})$.
These numbers are the ideals of $R(\sqrt{m})$ that we defined at the begining of this chapter.

To see how the introduction of ideals, in a field in which uniqueness of factorization does not hold, may restore uniqueness of factorization, consider the following example.
Consider $R(\sqrt{-5})$. It has been pointed out that this field is not simple. If we shift the emphasis from factorization into prime factors to factorization into irreducible ideals, then any ideal in $R(\sqrt{-5})$ can be factored, in one and only one way, as the product of prime ideal factors.

Example:

Consider the integer 6 in $R(\sqrt{-5})$.

6 can be factored into its prime factors in two different ways.

$$6 = 2 \times 3 \quad \text{and} \quad 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Corresponding to these two different factorizations of 6, there are two different factorizations of 6 into principal ideal factors, namely:

$$[6] = [2][3] \quad \text{and} \quad [6] = [1 + \sqrt{-5}][1 - \sqrt{-5}].$$

All these factors are not irreducible ideals

$$[2] = [2, 1 + \sqrt{-5}][2, 1 + \sqrt{-5}] = [2, 1 + \sqrt{-5}]^2$$

because

$$[2, 1 + \sqrt{-5}]^2 = [4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}]$$

by definition of multiplication. This ideal contains

$$(2 + 2\sqrt{-5}) - (-4 + 2\sqrt{-5}) = 6$$

and

$$6 - 4 = 2.$$

Hence it contains all multiples of 2 and therefore it is [2].

Similarly

$$[3] = [3, 1 + \sqrt{-5}][3, 1 - \sqrt{-5}]$$

and

$$[1 + \sqrt{-5}] = [2, 1 + \sqrt{-5}][3, 1 + \sqrt{-5}]$$

and

$$[1 - \sqrt{-5}] = [2, 1 + \sqrt{-5}][3, 1 - \sqrt{-5}].$$

All these factors are irreducible ideals [15,264].

Therefore

$$[6] = [2][3] = [2, 1 + \sqrt{-5}]^2[3, 1 + \sqrt{-5}][3, 1 - \sqrt{-5}]$$

and

$$[6] = [1 + \sqrt{-5}][1 - \sqrt{-5}] = [2, 1+ \sqrt{-5}]^2[3,1+ \sqrt{-5}][3,1- \sqrt{-5}],$$

and hence these two factorizations of [6] are not distinct, and they lead to the same irreducible ideal factors.

Hence [6] can be factored in one and only one way as the product of irreducible ideal factors except possibly for the order.

In the fields which are not simple, the unique factorization property can be restored by considering multiplication of ideal factors instead of multiplication of integers. The representation of ideals as the product of irreducible ideal factors is unique as asserted by the following theorem. [6, p.91].

"Every ideal not [0] or [1] can be factored into the product of irreducible ideals. This factorization is unique except for the order of the factors."

BIBLIOGRAPHY

1. Connel, Ian G., On Algebraic Number Fields with Unique Factorization, Math. Bull., Vol. 5, No. 2, May 1962.

2. Hardy, G. H., and Wright, E.M., The Theory of Numbers 3rd. ed. Oxford: the Clarendon Press, 1954.

3. McCay, Neal H., Introduction to Modern Algebra, Boston: Allyn and Bacon, Inc. 1960.

4. Moore, John T., Elements of Abstract Algebra, New York: The Macmillan Company 1962.

5. Niven, Ivan and Zuckerman, Herbert S., An Introduction to the Theory of Numbers, New York, London: John Willey and Sons, Inc. 1960

6. Pollard, Harry., The Theory of Algebraic Numbers, Carus Mathematical Monograph Number 9. The mathematical association of America, John willy and Sons, Inc. 1950.

7. Reid, Legh Wilbert., The Elements of the Theory of Algebraic Numbers, New York: the Macmillan Company, 1910.