AN ABSTRACT OF THE THESIS OF

DALE MORRELL MASSEY (Name) for the M.S. (Degree) in Mathematics (Major)

Date thesis is presented August 9, 1966

Title A STUDY OF FACTORIZATION IN Ra(\sqrt{6}) AND Ra(\sqrt{-21})

Abstract approved Redacted for Privacy

Major professor

Various properties of the integers in two quadratic number fields will be examined. Among these will be the property of unique prime factorization. When unique prime factorization breaks down, as will be the case in one of the quadratic number fields, the concept of ideal numbers will be introduced. It will be demonstrated that unique prime factorization is restored.
A STUDY OF FACTORIZATION IN $Ra(\sqrt{6})$ AND $Ra(\sqrt{-21})$

by

DALE MORRELL MASSEY

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1967
APPROVED:

Redacted for Privacy

Professor of Mathematics
In Charge of Major

Redacted for Privacy

Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented    August 9, 1966

Typed by Carol Baker
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. THE NUMBERS $\mathbb{R}a(\sqrt{6})$</td>
<td>3</td>
</tr>
<tr>
<td>III. THE NUMBERS $\mathbb{R}a(\sqrt{-21})$</td>
<td>32</td>
</tr>
<tr>
<td>IV. THE IDEAL NUMBERS IN $\mathbb{R}a(\sqrt{-21})$</td>
<td>41</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>51</td>
</tr>
</tbody>
</table>
A STUDY OF FACTORIZATION IN $\text{Ra}(\sqrt{6})$ AND $\text{Ra}(\sqrt{-21})$

I. INTRODUCTION

The purpose of this paper is to investigate some of the properties of two number fields. An algebraic number is one which satisfies a polynomial equation with rational coefficients. Among the infinite number of rational equations satisfied by our algebraic number, we will consider the one of least degree. A number which satisfies an irreducible quadratic equation is called a quadratic number. The system of algebraic numbers will be denoted $\text{Ra}(\sqrt{m})$. The algebraic numbers will be expressed as $a+b\sqrt{m}$, where $a$ and $b$ range independently over the field of rational numbers. The two number fields being considered are, one in which $m = 6$, the other in which $m = -21$. The paper will show that in each of these fields there is a particular subset which is an integral domain. The elements of this subset will be called integers. It will be demonstrated that the integers in $\text{Ra}(\sqrt{6})$ can be uniquely factored into prime factors. The integers in $\text{Ra}(\sqrt{-21})$ do not possess the property of unique prime factorization. The concept of ideal numbers will be introduced which will restore unique prime factorization in $\text{Ra}(\sqrt{-21})$.

In the paper properties of groups, rings, integral domains and fields will be used without these properties having been defined.

It will also be assumed that the properties of the complex
number field are known as well as certain results from number theory 
and algebra such as:

1.1 Every composite rational integer has a unique factorization 
into a finite number of prime factors.

1.2 If $a$ is a rational integer, $a^2$ is congruent to 0 or 1 
mod 4, and in particular,

\[ a \equiv 0 \mod 2 \quad a^2 \equiv 0 \mod 4 \]
\[ a \equiv 1 \mod 2, \quad a^2 \equiv 1 \mod 4 \]
II. THE NUMBERS \( Ra(\sqrt{6}) \)

Let \( px^2 + qx + r = 0 \) be an irreducible quadratic equation. We can assume without loss of generality that \( p, q \) and \( r \) are rational integers. If this is not the case, we can multiply through by the lowest common denominator. Let \( \rho \) be one of its roots.

**Definition 2.1.** The set of numbers \( a + b\rho \), where \( a \) and \( b \) range independently over the field of rational numbers, will be called \( Ra(\rho) \).

**Theorem 2.1.** There exists a rational integer \( m \) without a repeated prime factor such that \( Ra(\rho) = Ra(\sqrt{m}) \).

**Proof:**

a. Let \( q^2 - 4pr = m \).

Then \( \rho = \frac{-q + \sqrt{m}}{2p} \), \( \sqrt{m} = 2pp + q \).

Suppose \( a \in Ra(\rho) \). Then \( a = a + b\rho \). Now

\[
\begin{align*}
a + b\rho &= a + b\left( \frac{-q}{2p} + \frac{\sqrt{m}}{2p} \right) = \left( a - \frac{bq}{2p} \right) + \frac{b}{2p} \sqrt{m}.
\end{align*}
\]

Hence \( a \) can be expressed as \( c + d\sqrt{m} \) which is an element of \( Ra(\sqrt{m}) \). Since \( a \in Ra(\rho) \) implies \( a \in Ra(\sqrt{m}) \),

\( Ra(\rho) \) is a subset of \( Ra(\sqrt{m}) \).
b. Suppose \( \beta \in \text{Ra}(\sqrt{m}) \). Then \( \beta = a_1 + b_1 \sqrt{m} \). Now
\[
a_1 + b_1 \sqrt{m} = a_1 + b_1 (2pp + q) = (a_1 + b_1 q) + (2bp)\rho .
\]
Hence \( \beta \) can be expressed as \( c_1 + d_1 \rho \) which is an element of \( \text{Ra}(\rho) \). Since \( \beta \in \text{Ra}(\sqrt{m}) \) implies \( \beta \in \text{Ra}(\rho) \), \( \text{Ra}(\sqrt{m}) \) is a subset of \( \text{Ra}(\rho) \).

c. The conclusions derived in parts (a) and (b) tell us that \( \text{Ra}(\rho) = \text{Ra}(\sqrt{m}) \). A similar argument results when
\[
\rho = \frac{-q - \sqrt{m}}{2p} .
\]

**Theorem 2.2.** \( \text{Ra}(\sqrt{6}) \) is a field.

**Proof:**

a. The set is closed under addition and multiplication, for if
we take \( a = a + b\sqrt{6} \) and \( \beta = c + d\sqrt{6} \) we have
\[
a + \beta = (a+c) + (b+d) \sqrt{6}
\]
\[
a \cdot \beta = (ac + 6bd) + (ad + bc)\sqrt{6}
\]
and \( a, b, c \) and \( d \) are rational numbers. So
are the coefficients \( a+c, b+d, \) and so on.

b. Both operations are associative and commutative, and
multiplication is distributive over addition since \( \text{Ra}(\sqrt{6}) \)
is a subset of the complex field.
c. \(0 = 0+0\sqrt{6}\) and \(1 = 1+0\sqrt{6}\) are in \(\text{Ra}(\sqrt{6})\).

d. If \(a+b\sqrt{6}\) is in \(\text{Ra}(\sqrt{6})\) so is \(-a-b\sqrt{6}\).

e. Considering \(a+b\sqrt{6} \neq 0\) in \(\text{Ra}(\sqrt{6})\) there exists an inverse \(\frac{1}{a+b\sqrt{6}}\) in \(\text{Ra}(\sqrt{6})\) with \(a\) and \(b\) rational numbers. For \(\frac{1}{a+b\sqrt{6}} = \frac{a-b\sqrt{6}}{a^2-6b^2}\). If \(a^2-6b^2 = 0\), either \(a^2 = b^2 = 0\) which by hypothesis is impossible, or \(b^2 \neq 0\). Then \(\frac{a^2}{b^2} = 6\) or \(\frac{a}{b} = \sqrt{6}\) which is impossible since this would mean \(\sqrt{6}\) is rational. Therefore \(a^2-6b^2 \neq 0\) and \(\frac{1}{a+b\sqrt{6}} = \frac{a}{a^2-6b^2} - \frac{b}{a^2-6b^2} \sqrt{6}\) exists and is in \(\text{Ra}(\sqrt{6})\).

Let \(a = a+b\sqrt{6}\) be any number of \(\text{Ra}(\sqrt{6})\) with \(a\) and \(b\) rational. Then \(a\) satisfies the equation, \(x^2-2ax+a^2-6b^2 = 0\). This is to say that every number of \(\text{Ra}(\sqrt{6})\) satisfies a quadratic equation with rational coefficients. The equation is called the principal equation of \(a\). Its constant term, \(a^2-6b^2\), is called the norm of \(a\) and is denoted \(N(a)\). The remaining root of the principal equation is \(\bar{a} = a-b\sqrt{6}\) and is called the conjugate of \(a\). If \(b = 0\), the conjugate of \(a\) is \(a\). This is to say that a rational number of \(\text{Ra}(\sqrt{6})\) is its own conjugate. We observe that the norm mentioned above is formed by the product of two conjugate numbers.
Example:

1. \( N(a+b\sqrt{6}) = (a+b\sqrt{6})(a-b\sqrt{6}) = a^2 - 6b^2 \).

2. \( N(3+\sqrt{6}) = (3+\sqrt{6})(3-\sqrt{6}) = 3 \).

3. \( N(7) = 7 \cdot 7 = 49 \).

**Theorem 2.3.** The norm of the product of two numbers of \( \mathbb{R}a(\sqrt{6}) \) is equal to the product of their norms.

**Proof:**

Let \( a = a+b\sqrt{6} \), \( \beta = c+d\sqrt{6} \) be two numbers of \( \mathbb{R}a(\sqrt{6}) \). Then

\[
N[(a+b\sqrt{6})(c+d\sqrt{6})] = N[(ac+6bd) + (ad+bc)\sqrt{6}]
\]

\[
= \{(ac+6bd) + (ad+bc)\sqrt{6}\} \cdot \{(ac+6bd) - (ad+bc)\sqrt{6}\}
\]

\[
= (ac+6bd)^2 - 6(ad+bc)^2
\]

\[
= a^2c^2 - 6a^2d^2 - 6b^2c^2 + 36b^2d^2
\]

\[
= (a^2 - 6b^2)(c^2 - 6d^2)
\]

\[
= N(a+b\sqrt{6}) \cdot N(c+d\sqrt{6}) .
\]

Example:

\[
N[(4+\sqrt{6})(1-\sqrt{6})] = N[-2-3\sqrt{6}] = (-2-3\sqrt{6})(-2+3\sqrt{6}) = -50 .
\]
Also \[ N(4+\sqrt{6})(1-\sqrt{6}) = N(4+\sqrt{6}) \cdot N(1-\sqrt{6}) \]

\[ = (4+\sqrt{6})(4-\sqrt{6})(1-\sqrt{6})(1+\sqrt{6}) \]

\[ = -50. \]

**Definition 2.2.** In order for \( a \) to be an algebraic integer, the rational equation of lowest degree, \( x^2 + px + q = 0 \), satisfied by \( a \) shall have coefficients which are integers.

**Definition 2.3.** The set of all numbers of \( \text{Ra}(\sqrt{6}) \), the coefficients of whose principal equations are rational integers (the coefficient of \( x^2 \) being 1) constitute the integral domain \( \text{Ra}[\sqrt{6}] \) of \( \text{Ra}(\sqrt{6}) \).

**Theorem 2.4.** Every rational integer is in \( \text{Ra}[\sqrt{6}] \). Every number of \( \text{Ra}[\sqrt{6}] \) which is rational is a rational integer.

**Proof:**

Let \( a = a + b\sqrt{6} \) be a number in \( \text{Ra}[\sqrt{6}] \) with \( a \) and \( b \) rational integers. If \( b = 0 \), \( a = a \) where \( a \) is a rational integer whose principal equation is

\[ x^2 - 2ax + a^2 = 0 \]

and its coefficients are rational integers.

Conversely, if \( a = a + b\sqrt{6} \) is rational, \( b = 0 \) and \( a \)
in Ra[√6] implies the principal equation

\[ x^2 - 2ax + a^2 = 0 \]

of \( a \) has rational integral coefficients. If \( a^2 \) is a rational integer so is \( a = a \).

**Theorem 2.5.** The conjugate of a number of Ra[√6] is in Ra[√6].

**Proof:**

This is true since both \( a \) and \( \bar{a} \) have the same principal equation.

**Theorem 2.6.** A number of Ra(√6) is in Ra[√6] if and only if it is of the form \( a + b\sqrt{6} \) where \( a \) and \( b \) are rational integers.

**Proof:**

Let \( a \) be a number of Ra(√6). Then \( a = \frac{a_1 + b_1 \sqrt{6}}{c_1} \)

where \( a_1, b_1 \) and \( c_1 \) are rational integers with no common factor.

We may assume \( c_1 \) to be positive without loss of generality.

The principal equation of \( a \) is

\[ x^2 - \frac{2a_1}{c_1} x + \frac{a_1^2 - 6b_1^2}{c_1^2} = 0. \]
If \( a \) is in \( \text{Ra}[\sqrt{6}] \),

(1) \( \frac{2a_1}{c_1} \) is a rational integer;

(2) \( \frac{a_1^2 - 6b_1^2}{c_1} \) is a rational integer.

Then one of the following three cases must occur:

(i) \( c_1 \neq 1 \) and \( c_1 \neq 2 \) 
(ii) \( c_1 = 2 \) 
(iii) \( c_1 = 1 \).

If \( c_1 \neq 1 \) and \( c_1 \neq 2 \), then by (1) \( a_1 \) and \( c_1 \) have a common factor which by (2) would be contained in \( b_1 \) also. This is a contradiction since \( a_1, b_1 \) and \( c_1 \) were assumed to be rational integers with no common factor.

If \( c_1 = 2 \), \( c_1^2 = 4 \) and from (2)

\[
a_1^2 - 6b_1^2 = 0 \mod 4
\]

\[
a_1^2 = 6b_1^2 \mod 4.
\]

If \( b_1 = 0 \mod 2 \) then \( b_1^2 = 0 \mod 4 \) and \( a_1^2 = 0 \mod 4 \) hence \( a_1 \equiv 0 \mod 2 \) and \( a_1, b_1 \) and \( c_1 \) would have a common factor 2 which is contrary to our hypothesis.

If \( b_1 = 1 \mod 2 \) then \( b_1^2 = 1 \mod 4 \) and \( a_1^2 = 2 \mod 4 \) which is impossible. Therefore \( c_1 = 1 \) and \( a \) and \( b \) are
rational integers.

Conversely, if \( a = a + b\sqrt{6} \), with \( a \) and \( b \) rational integers, then \( 2a \) and \( a^2 - 6b^2 \) are rational integers and the principal equation of \( a \) has rational coefficients.

**Theorem 2.7.** The set of integers in \( \mathbb{R}[\sqrt{6}] \) is closed under addition, subtraction and multiplication.

**Proof:** Let \( a_1 + b_1\sqrt{6} \) and \( a_2 + b_2\sqrt{6} \) be two integers in \( \mathbb{R}[\sqrt{6}] \) where \( a_1, a_2, b_1 \) and \( b_2 \) are rational integers.

(i) \( (a_1 + b_1\sqrt{6}) \pm (a_2 + b_2\sqrt{6}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{6} \) which is in \( \mathbb{R}[\sqrt{6}] \) since \( (a_1 \pm a_2) \) and \( (b_1 \pm b_2) \) are rational integers.

(ii) \( (a_1 + b_1\sqrt{6})(a_2 + b_2\sqrt{6}) = (a_1a_2 + 6b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{6} \) which is in \( \mathbb{R}[\sqrt{6}] \) since \( (a_1a_2 + 6b_1b_2) \) and \( (a_1b_2 + a_2b_1) \) are rational integers.

**Definition 2.4.** Any two integers \( \theta_1 \) and \( \theta_2 \) in \( \mathbb{R}[\sqrt{6}] \) are said to form a basis if every integer in \( \mathbb{R}[\sqrt{6}] \) can be represented as \( a_1\theta_1 + a_2\theta_2 \) where \( a_1 \) and \( a_2 \) are rational integers.

**Theorem 2.8.** If \( \theta_1, \theta_2 \) is a basis in \( \mathbb{R}[\sqrt{m}] \), the necessary and sufficient condition that \( \theta'_1 = a_{11}\theta_1 + a_{12}\theta_2 \) and \( \theta'_2 = a_{21}\theta_1 + a_{22}\theta_2 \), where the \( a_{ij} \)'s are rational integers, shall be also a basis of
Ra[$\sqrt{6}$] is

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \pm 1.$$  

Proof:

Let $\theta_1, \theta_2$ and $\theta'_1, \theta'_2$ be two bases in Ra[$\sqrt{6}$]. Since $\theta_1, \theta_2$ form a basis for Ra[$\sqrt{m}$] we have

$$(1) \quad \theta'_1 = a_{11} \theta_1 + a_{12} \theta_2 \quad \theta'_2 = a_{21} \theta_1 + a_{22} \theta_2$$

where the $a_{ij}$'s are rational integers. $\theta'_1, \theta'_2$ form a basis for Ra[$\sqrt{6}$], hence we have

$$(2) \quad \theta_1 = b_{11} \theta'_1 + b_{12} \theta'_2 \quad \theta_2 = b_{21} \theta'_1 + b_{22} \theta'_2$$

where the $b_{ij}$'s are rational integers.

Substituting the values of $\theta'_1$ and $\theta'_2$ we have

$$(3) \quad \theta_1 = (b_{11}a_{11} + b_{12}a_{21})\theta_1 + (b_{11}a_{12} + b_{12}a_{22})\theta_2 \quad \theta_2 = (b_{21}a_{11} + b_{22}a_{21})\theta_1 + (b_{21}a_{12} + b_{22}a_{22})\theta_2.$$
So since $\theta_1$ and $\theta_2$ are linearly independent,

\[
\begin{align*}
 b_{11}a_{11} + b_{12}a_{21} &= 1 \\
 b_{11}a_{12} + b_{12}a_{22} &= 0 \\
 b_{21}a_{11} + b_{22}a_{21} &= 0 \\
 b_{21}a_{12} + b_{22}a_{22} &= 1 .
\end{align*}
\]

From these equations, it follows that

\[
\begin{bmatrix}
 b_{11} & b_{12} \\
 b_{21} & b_{22}
\end{bmatrix}
\begin{bmatrix}
 a_{11} & a_{12} \\
 a_{21} & a_{22}
\end{bmatrix}
= \begin{bmatrix}
 1 & 0 \\
 0 & 1
\end{bmatrix} .
\]

Hence

\[
\begin{vmatrix}
 b_{11} & b_{12} \\
 b_{21} & b_{22}
\end{vmatrix}
\begin{vmatrix}
 a_{11} & a_{12} \\
 a_{21} & a_{22}
\end{vmatrix}
= 1 .
\]

The determinant of each matrix on the left divides 1 so is either +1 or -1. Thus

\[
\begin{vmatrix}
 a_{11} & a_{12} \\
 a_{21} & a_{22}
\end{vmatrix}
= \pm 1
\]

is a necessary condition for $\begin{pmatrix} \theta_1' \\ \theta_2' \end{pmatrix}$ to be a basis.

The condition is also sufficient; for, solving (1) for $\theta_1$ and $\theta_2$ we have
\[ \theta_1 = \pm (a_{22} \theta_1' - a_{12} \theta_2') \]

\[ \theta_2 = \pm (a_{21} \theta_1' - a_{11} \theta_2') \]

since \( a_{11} a_{22} - a_{12} a_{21} = \pm 1 \).

Since \( \theta_1, \theta_2 \) is a basis, if \( \theta \) is in \( \text{Ra}[\sqrt{6}] \) we have

\[ \theta = c_{11} \theta_1 + c_{12} \theta_2 = \pm (c_{11} a_{22} + c_{12} a_{21}) \theta_1' \pm (c_{11} a_{12} + c_{12} a_{11}) \theta_2' \]

where \( c_{11} \) and \( c_{12} \) are rational integers.

**Theorem 2.9.** The numbers \( 1, \sqrt{6} \) form a basis in \( \text{Ra}[\sqrt{6}] \).

**Proof:**

If \( a = a + b \sqrt{6} \) is in \( \text{Ra}[\sqrt{6}] \), then there exist unique rational integers \( x \) and \( y \) such that \( a + b \sqrt{6} = x + y \sqrt{6} \).

To show that \( x \) and \( y \) are unique let us assume that

\[ a + b \sqrt{6} = x_1 + y_1 \sqrt{6} \quad \text{and} \quad a + b \sqrt{6} = x_2 + y_2 \sqrt{6}. \]

This implies that

\[ (x_1 - x_2) + (y_1 - y_2) \sqrt{6} = 0 \quad \text{so} \quad x_1 - x_2 = 0 \quad \text{and} \quad y_1 - y_2 = 0. \]

Hence \( x_1 = x_2 \) and \( y_1 = y_2 \).

**Definition 2.5.** If \( \theta_1 \) and \( \theta_2 \) form a basis in \( \text{Ra}[\sqrt{6}] \) and \( \alpha \) and \( \beta \) are any two numbers of \( \text{Ra}[\sqrt{6}] \), the discriminant of the numbers \( \alpha \) and \( \beta \) is
\[ \Delta(a, \beta) = \begin{vmatrix} a_1 \theta_1 + b_1 \theta_2 & a_2 \theta_1 + b_2 \theta_2 \\ a_1 \overline{\theta_1} + b_1 \overline{\theta_2} & a_2 \overline{\theta_1} + b_2 \overline{\theta_2} \end{vmatrix}^2. \]

**Theorem 2.10.** \( \Delta(\theta_1, \theta_2) \) where \( \theta_1, \theta_2 \) is a basis is invariant under change of basis.

**Proof:** From definition 2.5

\[ \Delta(a, \beta) = \begin{vmatrix} \theta_1 & \theta_2 \\ \theta_1 & \theta_2 \end{vmatrix}^2 \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}. \]

From Theorem 2.8 \( a, \beta \) form a basis in \( Ra[\sqrt{6}] \) if and only if

\[ \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \pm 1. \]

Hence \( \Delta(a, \beta) = \begin{vmatrix} \theta_1 & \theta_2 \\ \theta_1 & \theta_2 \end{vmatrix}^2 = \Delta(\theta_1, \theta_2). \)

**Definition 2.6.** \( \Delta(\theta_1, \theta_2) \) is called the discriminant of \( Ra[\sqrt{6}] \) and denoted \( \Delta[\sqrt{6}] \).

**Theorem 2.11.** \( \Delta[\sqrt{6}] = 24. \)

**Proof:**

Use \((1, \sqrt{6})\) as a basis. Then
\[ \Delta[\sqrt{6}] = \begin{vmatrix} 1 & \sqrt{6} \\ 1 & -\sqrt{6} \end{vmatrix} = (-\sqrt{6} - \sqrt{6})^2 = (-2\sqrt{6})^2 = 24. \]

**Definition 2.7.** Any integer \( a \) is divisible by an integer, \( \beta \), when there exists an integer, \( \gamma \), such that \( a = \beta \gamma \) with \( a, \beta \) and \( \gamma \) in \( \mathbb{R}[\sqrt{6}] \). We say that \( \beta \) and \( \gamma \) are divisors or factors of \( a \) and \( a \) is a multiple of \( \beta \) and \( \gamma \). \( \beta \) divides \( a \) is denoted \( \beta | a \).

**Example 1:** \(-6+\sqrt{6}\) is divisible by \(3+2\sqrt{6}\) since

\[-6+\sqrt{6} = (3+2\sqrt{6})(2-\sqrt{6}) .\]

**Example 2:** \(5+3\sqrt{6}\) is not divisible by \(-2+3\sqrt{6}\).

Consider \(5+3\sqrt{6} = (-2+3\sqrt{6})(a+b\sqrt{6})\)

\[= (-2a+18b) + (3a-2b)\sqrt{6}.\]

Upon equating coefficients, \(a = \frac{32}{25}\) and \(b = \frac{21}{50}\).

**Theorem 2.12.** If \( a \) is divisible by \( \beta \), then \( N(a) \) is divisible by \( N(\beta) \).

**Proof:**

\(\beta | a \) implies that \( a = \beta \gamma \) where \( a, \beta \) and \( \gamma \) are in \( \mathbb{R}[\sqrt{6}] \). By Theorem 2.3
\[
N(a) = N(\beta \gamma) = N(\beta) \cdot N(\gamma).
\]

Hence by definition 2.7 \( N(\beta) \mid N(a) \).

**Definition 2.8.** An integer which divides 1 is called a unit of \( \mathbb{R}a[\sqrt{6}] \).

**Theorem 2.13.** An integer in \( \mathbb{R}a[\sqrt{6}] \) is a unit if and only if its norm is \( \pm 1 \).

**Proof:**

Let \( a+b\sqrt{6} \) be a unit in \( \mathbb{R}a[\sqrt{6}] \). By definition 2.8

\[
a+b\sqrt{6} \mid 1 \text{ so } (a+b\sqrt{6})(c+d\sqrt{6}) = 1 \text{ where } c+d\sqrt{6} \text{ is in } \mathbb{R}a[\sqrt{6}].
\]

By theorem 2.3, \( N(a+b\sqrt{6}) \cdot N(c+d\sqrt{6}) = 1 \) and \( N(a+b\sqrt{6}) \mid 1 \).

Now \( |N(a+b\sqrt{6})| \leq 1 \) and \( -1 \leq N(a+b\sqrt{6}) \leq 1 \). Since \( N(a+b\sqrt{6}) \) is a non-zero integer, \( N(a+b\sqrt{6}) = \pm 1 \).

Conversely, if \( N(a+b\sqrt{6}) = \pm 1 \) then \( (a+b\sqrt{6})(a-b\sqrt{6}) = \pm 1 \).

Hence \( (a+b\sqrt{6})(a-b\sqrt{6})\gamma = \pm \gamma \) where \( \gamma \) is in \( \mathbb{R}a[\sqrt{6}] \). If \( \gamma = 1 \) then \( a+b\sqrt{6} \mid 1 \).

Let \( \epsilon = a+b\sqrt{6} \) be a unit in \( \mathbb{R}a[\sqrt{6}] \) where \( a \) and \( b \) are rational integers. Now

\[
N(\epsilon) = \pm 1
\]

that is

\[
a^2 - 6b^2 = \pm 1.
\]
It is possible to obtain many solutions for \( a \) and \( b \) some of which are:

\[
\begin{align*}
\text{a} &= \pm 1, \quad \text{b} = 0 \quad \epsilon = \pm 1 \\
\text{a} &= \pm 5, \quad \text{b} = \pm 2 \quad \epsilon = \pm 5 \pm 2\sqrt{6} \\
\text{a} &= \pm 49, \quad \text{b} = \pm 20 \quad \epsilon = \pm 49 \pm 20\sqrt{6}.
\end{align*}
\]

It will be demonstrated that \( Ra[\sqrt{6}] \) has an infinite number of units, each of which can, however, be represented as a power of the unit \( 5+2\sqrt{6} \), multiplied by \( \pm 1 \). We call \( 5+2\sqrt{6} \) the fundamental unit.

**Theorem 2.14.** All units of \( Ra[\sqrt{6}] \) have the form \( \pm(5+2\sqrt{6})^n \), where \( n \) is a positive or negative integer or 0, and all numbers of this form are units of \( Ra[\sqrt{6}] \).

**Proof:**

Let \( \epsilon = 5+2\sqrt{6} \).

\[
N(\epsilon^n) = [N(\epsilon)]^n = (1)^n = 1 .
\]

Hence every positive power of \( \epsilon \) is a unit. Moreover, since \( \epsilon^n \cdot \epsilon^{-n} = \epsilon^0 = 1 \), \( \epsilon^{-n} \) is a unit also; hence all negative powers of \( \epsilon \) are units. Since \( \epsilon = 5+2\sqrt{6} > 1 \), \( \epsilon^n > 1 \) when \( n \) is positive. Thus two different positive powers give different units.
Also since $\epsilon^{-n} = \frac{1}{\epsilon^n}$, $\epsilon^{-1} < 1$ and hence $\epsilon^n < 1$ when $n$ is a negative integer. Thus two different negative powers give different units. Also no negative power of $\epsilon$ is equal to any positive power of $\epsilon$. Therefore every power of $\epsilon$ is a unit of $\text{Ra}[\sqrt{6}]$ and two different powers give different units.

Conversely, let $a+b\sqrt{6}$ be any unit in $\text{Ra}[\sqrt{6}]$. Then $a-b\sqrt{6}$, $-a+b\sqrt{6}$ and $-a-b\sqrt{6}$ will also be units of $\text{Ra}[\sqrt{6}]$. We denote $a+b\sqrt{6}$ by $\eta_1$ where $a$ and $b$ are positive rational integers, and the remaining three by $\overline{\eta_1}$, $-\eta_1$ and $-\overline{\eta_1}$.

Since $\eta_1 \geq 1$, then either

1. $\eta_1 = \epsilon^n$ or
2. $\epsilon^n < \eta_1 < \epsilon^{n+1}$

where $n \geq 0$. From (2) $1 < \frac{\eta_1}{\epsilon^n} < \epsilon$ where $\frac{\eta_1}{\epsilon^n}$ is a unit. If we let $\frac{\eta_1}{\epsilon^n} = x+y\sqrt{6}$, $N(x+y\sqrt{6}) = \pm 1$. Since $x+y\sqrt{6} > 1$, $|x-y\sqrt{6}| < 1$ and

$$-1 < x-y\sqrt{6} < 1.$$  

Using this result together with the result of (2),

$$0 < x < 3+\sqrt{6}.$$  

Since $x$ is a rational integer, $0 < x < 6$. In solving the above inequalities for $y$

$$0 < y\sqrt{6} < 3+\sqrt{6}.$$
Since $y$ is a rational integer, $0 < y < 3$.

$x + y\sqrt{6}$ by supposition is a unit and the possibilities for $x$ and $y$ indicate that we check the norms of the following:

\[
\begin{align*}
1 + \sqrt{6} & ; & N(1 + \sqrt{6}) &= -5 \\
1 + 2\sqrt{6} & ; & N(1 + 2\sqrt{6}) &= -23 \\
2 + \sqrt{6} & ; & N(2 + \sqrt{6}) &= -2 \\
2 + 2\sqrt{6} & ; & N(2 + 2\sqrt{6}) &= -20 \\
3 + \sqrt{6} & ; & N(3 + \sqrt{6}) &= 3 \\
3 + 2\sqrt{6} & ; & N(3 + 2\sqrt{6}) &= -15 \\
4 + \sqrt{6} & ; & N(4 + \sqrt{6}) &= 10 \\
4 + 2\sqrt{6} & ; & N(4 + 2\sqrt{6}) &= -8 \\
5 + \sqrt{6} & ; & N(5 + \sqrt{6}) &= 19 \\
\end{align*}
\]

Since $N(x + y\sqrt{6}) \neq \pm 1$, (2) cannot exist. Thus

\[
\eta_1 = \epsilon^n ; \quad n \geq 0.
\]

Also

\[
-\eta_1 = -\epsilon^n.
\]

Since $\eta_1\overline{\eta_1} = \pm 1$, \[
\eta_1 = \pm \frac{1}{\epsilon_n} = \pm \epsilon^{-n} \text{ and } -\overline{\eta_1} = \pm \epsilon^{-n} \text{ therefore}
\]
\[
\eta = \pm \epsilon^n \text{ where } n \text{ is positive, negative or 0.}
\]

**Definition 2.9.** Any two integers of $\text{Ra}[^{\sqrt{6}}]$ which differ only by a unit factor are called **associates**.
It has been demonstrated that $\text{Ra}[\sqrt{6}]$ contains an infinite number of units. Therefore one can expect each integer of $\text{Ra}[\sqrt{6}]$ to be associated with an infinite number of integers in $\text{Ra}[\sqrt{6}]$. If $a$ is a factor of $\mu$, and $n$ any positive or negative rational integer, the infinitely many integers $\pm \epsilon^n a$ that are associated with $a$, are also factors of $\mu$. In the case of $\text{Ra}[\sqrt{6}]$ the associates of any integer can be found by multiplying the integer by $\pm(5+2\sqrt{6})^n$ where $n$ is a positive or negative rational integer or 0. Hence in all questions of divisibility, associated integers are considered as identical; that is, two factors, one of which can be changed into the other by multiplication by a unit, are looked upon as the same.

**Definition 2.10.** An integer in $\text{Ra}[\sqrt{6}]$ that is not a unit and has no divisors other than its associates and the units, is called a **prime** number in $\text{Ra}[\sqrt{6}]$.

**Definition 2.11.** An integer in $\text{Ra}[\sqrt{6}]$ with divisors other than its associates and the units is called a **composite** number.

**Example 1.** $3+\sqrt{6}$ is a prime number in $\text{Ra}[\sqrt{6}]$.

$$3+\sqrt{6} = (a+b\sqrt{6})(c+d\sqrt{6}).$$

By theorem 2.3

$$3 = (a^2-6b^2)(c^2-6d^2).$$
Either

(1) \( a^2 - 6b^2 = 3 \)  
(2) \( a^2 - 6b^2 = -3 \)

\( c^2 - 6d^2 = 1 \)  
\( c^2 - 6d^2 = -1 \)

Both (1) and (2) indicate that \( c+d\sqrt{6} \) is a unit. So

\[ 3+\sqrt{6} = (3-\sqrt{6})(5+2\sqrt{6}) = (-3+\sqrt{6})(-5-2\sqrt{6}). \]

This factorization can be looked upon as essentially the same since the corresponding factors are associated. It is interesting to note that the process of finding the divisors of \( 3+\sqrt{6} \) gives us the divisors of its associates and also the divisors of every other integer whose norm is \( 3 \) as well as their associates.

\[ (5+2\sqrt{6}) (3+\sqrt{6}) = 27 + 11\sqrt{6} \]
\[ -(5+2\sqrt{6}) (3+\sqrt{6}) = -27 - 11\sqrt{6} \]
\[ (5+2\sqrt{6})^{-2}(3+\sqrt{6}) = 27 - 11\sqrt{6} \]
\[ -(5+2\sqrt{6})^{-2}(3+\sqrt{6}) = -27 + 11\sqrt{6} \]

\( N(27+11\sqrt{6}) = 3 \) and \(-27-11\sqrt{6} \), \( 27-11\sqrt{6} \) and \(-26+11\sqrt{6} \) are associates of \( 27+11\sqrt{6} \).

**Example 2.** \( 4-\sqrt{6} \) is a composite number in \( \mathbb{R}[\sqrt{6}] \).

\[ 4-\sqrt{6} = (a+b\sqrt{6})(c+d\sqrt{6}). \]
By theorem 2.3

\[ 10 = (a^2 - 6b^2)(c^2 - 6d^2) . \]

Either

\[
\begin{align*}
(1) & \quad a^2 - 6b^2 = 5 \\
(2) & \quad a^2 - 6b^2 = -5 \\
(3) & \quad a^2 - 6b^2 = \pm 10 \\
(4) & \quad c^2 - 6d^2 = 2 \\
(5) & \quad c^2 - 6d^2 = -2 \\
(6) & \quad c^2 - 6d^2 = \pm 1
\end{align*}
\]

(3) gives \( c + d\sqrt{6} \) as a unit. Some solutions of (2) are

\[
\begin{align*}
a &= \pm 7 & b &= \pm 3 \\
a &= \pm 1 & b &= \pm 1 \\
c &= \pm 2 & d &= \pm 1 \\
c &= \pm 22 & d &= \pm 9
\end{align*}
\]

\[ 4 - \sqrt{6} = (7 - 3\sqrt{6})(-2 + \sqrt{6}) \]

\[ = (-7 + 3\sqrt{6})(2 + \sqrt{6}) \]

\[ = (1 + \sqrt{6})(-2 + \sqrt{6}) \]

\[ = (-1 - \sqrt{6})(2 - \sqrt{6}) . \]

Looking at the fundamental unit \( \epsilon = 5 + 2\sqrt{6} \), all these factorizations can be derived from any particular one by multiplying the factors by suitable units and hence are not different; that is

\[
(5 + 2\sqrt{6})^0 (1 + \sqrt{6}) = 1 + \sqrt{6}
\]

\[-(5 + 2\sqrt{6})^0 (1 + \sqrt{6}) = -1 + \sqrt{6} \]
Now

\[(5+2\sqrt{6})^{-1}(1+\sqrt{6}) = -7+3\sqrt{6}\]

\[-(5+2\sqrt{6})(1+\sqrt{6}) = 7-3\sqrt{6}\]

\[(5+2\sqrt{6})^0 (2+\sqrt{6}) = 2+\sqrt{6}\]

\[-(5+2\sqrt{6})^0 (2+\sqrt{6}) = -2-\sqrt{6}\]

\[(5+2\sqrt{6})^{-1}(2+\sqrt{6}) = -2+\sqrt{6}\]

\[-(5+2\sqrt{6})^{-1}(2+\sqrt{6}) = 2-\sqrt{6}\]

Now

\[4-\sqrt{6} = \left[ \pm \epsilon \right] n(1+\sqrt{6})\left[ \pm \epsilon \right] n(2+\sqrt{6}).\]

In trying to factor \(1+\sqrt{6}\) and \(2+\sqrt{6}\), we find them to be prime numbers and therefore \(4-\sqrt{6}\) has been resolved into its prime factors.

**Theorem 2.15.** If \(a\) be any integer in \(\mathbb{R}[\sqrt{6}]\) and \(\beta\) any integer of \(\mathbb{R}[\sqrt{6}]\) different from 0, there exists an integer \(\mu\) in \(\mathbb{R}[\sqrt{6}]\) such that

\[|N(a-\mu\beta)| < |N(\beta)|.\]

**Proof:**

Let \(a = a+b\sqrt{6}\) in \(\mathbb{R}[\sqrt{6}]\) where

\[a = r+r_1 \quad \quad \quad \quad b = s+s_1\]

\(r\) and \(s\) being the rational integers nearest to \(a\) and \(b\).
respectively so that
\[ |r_1| \leq \frac{1}{2}, \quad |s_1| \leq \frac{1}{2}. \]

In choosing \( \mu = r+s\sqrt{6} \) we run into difficulty.

\[ \frac{a}{\beta} - \mu = r_1 + s_1\sqrt{6} \]

\[ |N(\frac{a}{\beta} - \mu)| = |N(r_1 + s_1\sqrt{6})| = |r_1^2 - 6s_1^2|. \]

It is apparent that \( \mu \) must be selected according to the values of \( r_1 \) and \( s_1 \), for if \( r_1 = \frac{1}{3} \) and \( s_1 = \frac{1}{2} \)

\[ |r_1^2 - 6s_1^2| = \left| \frac{25}{18} \right| \not\leq 1. \]

Consider selecting \( \mu \) in the following ways:

1. \( \mu = r+s\sqrt{6} \) if \( |s_1| < \frac{1}{\sqrt{6}} \) and \( |r_1| \leq \frac{1}{2} \)

2. \( \mu = r+1+s\sqrt{6} \) if \( \frac{1}{\sqrt{6}} \leq |s_1| < \frac{\sqrt{5}}{2\sqrt{6}} \) and \( 0 \leq r_1 \leq \frac{1}{2} \)

3. \( \mu = r-1+s\sqrt{6} \) if \( \frac{1}{\sqrt{6}} < |s_1| < \frac{\sqrt{5}}{2\sqrt{6}} \) and \( 0 \leq r_1 \leq \frac{1}{2} \)

4. \( \mu = r-1+s\sqrt{6} \) if \( \frac{1}{\sqrt{6}} \leq |s_1| < \frac{\sqrt{5}}{2\sqrt{6}} \) and \( -\frac{1}{2} \leq r_1 \leq 0 \)

5. \( \mu = r+1+s\sqrt{6} \) if \( \frac{1}{\sqrt{6}} \leq |s_1| < \frac{\sqrt{5}}{2\sqrt{6}} \) and \( -\frac{1}{2} \leq r_1 \leq 0 \)

\[ s \] cannot assume the value \( \frac{\sqrt{5}}{2\sqrt{6}} \) since \( b = s+s_1 \), and \( b \) is a rational number with \( \frac{\sqrt{5}}{s} \) a rational integer.
Since it is possible to choose $\mu$ according to the values of $r_1$ and $s_1$ we have

$$|N\left(\frac{a}{b} - \mu\right)| < 1$$

and multiplying by $|N(\beta)|$

$$|N(a - \beta \mu)| < |N(\beta)| .$$

**Definition 2.12.** If $a$, $\beta$ and $\gamma$ are integers in $Ra[\sqrt{6}]$ and $\gamma \mid a$, $\gamma \mid \beta$ then $\gamma$ is a **common divisor** of $a$ and $\beta$. If in addition every common divisor of $a$ and $\beta$ divides $\gamma$, $\gamma$ is called the **greatest common divisor** of $a$ and $\beta$ and denoted $(a, \beta)$.

**Theorem 2.16.** If $a$ and $\beta$ are any two integers in $Ra[\sqrt{6}]$ there exist two integers $\gamma$ and $\xi$ in $Ra[\sqrt{6}]$ such that

$$a \gamma + \beta \xi = \delta$$

where $\delta$ is the greatest common divisor of $a$ and $\beta$ and is unique up to an associate.

**Proof:**

We may assume that $N(a) > N(\beta)$ without limiting the generality of the proof.
By theorem 2.15 there exist two integers \( \eta \) and \( \rho \) in \( \mathbb{R}[\sqrt{6}] \) such that

\[
a = \eta \beta + \rho
\]

Continuing the process

\[
\beta = \eta_1 \rho + \rho_1
\]

\[
\rho = \eta_2 \rho_1 + \rho_2
\]

\[
\ldots
\]

\[
\rho_{k-3} = \eta_{k-1} \rho_{k-2} + \rho_{k-1}
\]

\[
\rho_{k-2} = \eta_{k} \rho_{k-1} + \rho_{k}
\]

In a finite number of steps we will arrive at a \( \rho_k \) whose norm is 0, since

\[
|N(\beta)| > |N(\rho)| > |N(\rho_1)| > \ldots > |N(\rho_{k-1})| > |N(\rho_k)|
\]

form a sequence of decreasing positive integers.

Since \( |N(\rho_k)| = 0 \), \( \rho_k = 0 \).

We may eliminate from these equations successively

\( \rho_{k-2}, \rho_{k-3}, \ldots, \rho \) to obtain
\[ \delta = \rho_{k-1} = a\gamma + \beta\xi . \]

If \( \rho_k = 0 \), \( \rho_{k-2} = \delta \eta_k \) so \( \delta \) divides \( \rho_{k-2} \) and 
\[ \rho_{k-3} = \eta_{k-1} \delta \eta_k + \delta = \delta(\eta_k \eta_{k-1} + 1) \] so \( \delta \) divides \( \rho_{k-3} \). Continuing this process, the left member of each of the above equations is divisible by \( \delta \). Therefore \( \delta \) is a common divisor of \( a \) and \( \beta \). Since \( \delta = a\gamma + \beta\xi \) any common divisor of \( a \) and \( \beta \) divides \( \delta \) so \( \delta \) is the greatest common divisor of \( a \) and \( \beta \).

To show \( \delta \) unique, suppose \( \delta_1 \) is also a greatest common divisor of \( a \) and \( \beta \).

Then \( \delta = \mu \delta_1 \) and \( \delta_1 = \mu_1 \delta \) so \( \delta = \mu\mu_1 \delta \). Since 
\[ N(\delta) = N(\mu)N(\mu_1)N(\delta) \text{ and } N(\delta) \neq 0 \]
\[ N(\mu)N(\mu_1) = 1. \]

Hence \( \mu \) and \( \mu_1 \) are units and \( \delta \) and \( \delta_1 \) are associates.

**Definition 2.13.** Two integers are said to be **relatively prime** if every common divisor is a unit.

**Corollary 2.16.** If \( a \) and \( \beta \) are relatively prime, there exist integers \( \mu \) and \( \eta \) such that 
\[ \mu a + \eta \beta = 1 . \]
Proof:

By definition 2.13 and theorem 2.16 there exist integers \( \mu_1 \) and \( \eta_1 \) such that

\[
\mu_1 a + \eta_1 \beta = \epsilon; \quad \epsilon \text{ a unit.}
\]

Then \( \frac{1}{\epsilon} \mu_1 a + \frac{1}{\epsilon} \eta_1 \beta = \frac{1}{\epsilon} \cdot \epsilon \), and since the units are closed under division and the integers closed under multiplication it follows that

\[
\mu a + \eta \beta = 1.
\]

Theorem 2.17. If the product of two integers, \( a \) and \( \beta \), of \( \text{Ra}[\sqrt{6}] \) be divisible by a prime number \( \pi \), at least one of the integers, \( a \) or \( \beta \), is divisible by \( \pi \).

Proof:

Let \( a \beta = \gamma \pi \) with \( \gamma \) in \( \text{Ra}[\sqrt{6}] \) and suppose \( a \) is not divisible by \( \pi \). \( a \) and \( \pi \) are prime to each other so by theorem 2.16 \( a \xi + \pi \eta = 1 \) with \( \xi \) and \( \eta \) in \( \text{Ra}[\sqrt{6}] \). Multiplying by \( \beta; \beta a \xi + \beta \pi \eta = \beta \) and \( \gamma \pi \xi + \beta \pi \eta = \pi (\gamma \xi + \beta \eta) = \beta. \) Hence \( \beta \) is divisible by \( \pi \).

Corollary 2.17. If the product of any number of integers in \( \text{Ra}[\sqrt{6}] \) be divisible by a prime number \( \pi \), at least one of the integers is
divisible by \( \pi \).

**Proof:**

Let \( a_1 a_2 \cdots a_k \) be the product of \( k \) integers in \( \mathbb{R}[\sqrt{6}] \) which is divisible by \( \pi \).

Consider two integers \( a_i \) and \( a_1 a_2 \cdots a_{i-1} a_i a_{i+1} \cdots a_k \) of the product. By theorem 2.17, either \( a_i \) or \( a_1 a_2 \cdots a_{i-1} a_i a_{i+1} \cdots a_k \) is divisible by \( \pi \). If \( \pi | a_i \) proof is done.

If \( \pi | a_1 a_2 \cdots a_{i-1} a_i a_{i+1} \cdots a_k \) we can express this product as the product of \( a_{i-1} \) and \( a_1 a_2 \cdots a_{i-2} a_{i+1} \cdots a_k \). If \( \pi | a_{i-1} \) proof is done. If \( \pi | a_1 a_2 \cdots a_{i-2} a_{i+1} \cdots a_k \) we can continue to break up this product into two integers one of which is divisible by \( \pi \). In this way it can be shown that \( \pi \) divides at least one integer of \( a_1 a_2 \cdots a_k \).

**Theorem 2.18.** Every integer in \( \mathbb{R}[\sqrt{6}] \) can be represented in one and only one way as the product of prime numbers.

**Proof:** Let \( P(n) \) be the proposition that every integer \( a \neq 0 \) in \( \mathbb{R}[\sqrt{6}] \) where \( |N(a)| = n \) (a natural number) is either a unit, or a prime, or can be factored into a finite number of primes.

If \( n = 1 \), \( a \) is a unit and \( P(1) \) is true.

If \( a \) is a prime, then \( P(n) \) is true for all \( n \).

If \( a \) is composite, \( a = \beta \gamma \) where \( \beta \) and \( \gamma \) are integers...
in $\mathbb{R}[\sqrt{6}]$ neither of which is a unit nor an associate of $a$.

$|N(\beta)| \neq 1$, $|N(\gamma)| \neq 1$ and both $|N(\beta)|$ and $|N(\gamma)|$ are less than $|N(a)|$ since $|N(a)| = |N(\beta)| \cdot |N(\gamma)|$ and the norms are rational integers.

Now suppose that every composite integer $\psi$ of $\mathbb{R}[\sqrt{6}]$ with $|N(\psi)| < |N(a)| < n$ has a finite prime decomposition. $\beta$ and $\gamma$ could then be expressed as

$$\beta = \beta_1 \beta_2 \cdots \beta_m, \quad \gamma = \gamma_1 \gamma_2 \cdots \gamma_n$$

where $\beta_1 \beta_2 \cdots \beta_m$ and $\gamma_1 \gamma_2 \cdots \gamma_n$ are prime numbers. Thus $a = \beta_1 \beta_2 \cdots \beta_m \gamma_1 \gamma_2 \cdots \gamma_n$ which is a product of a finite number of primes. Thus $P(n)$ is true for all $n \geq 1$.

**Theorem 2.18. (continued)** The decomposition of a composite integer into primes is unique.

**Proof:**

Suppose there are two prime decompositions of $a$,

$$a = \pi_1 \pi_2 \cdots \pi_r = \lambda_1 \lambda_2 \cdots \lambda_s.$$

By corollary 2.17 at least one of $\pi_i$ say $\pi_1$ divides some $\lambda_i$ say $\lambda_1$. Then $\lambda_1 = \epsilon_1 \pi_1$ where $\epsilon_1$ is a unit and

$$\pi_2 \pi_3 \cdots \pi_r = \epsilon_1 \lambda_2 \lambda_3 \cdots \lambda_s.$$
Then $\pi_2$ divides some $\lambda_i$, say $\lambda_2$ and

$$\pi_3 \pi_4 \cdots \pi_r = \epsilon_1 \epsilon_2 \epsilon_3 \epsilon_4 \cdots \epsilon_s \lambda_3 \lambda_4 \cdots \lambda_s.$$ 

If $r < s$, after $r$ steps we have

$$1 = \epsilon_1 \epsilon_2 \cdots \epsilon_r \epsilon_{r+1} \cdots \epsilon_s \lambda_3 \lambda_4 \cdots \lambda_s.$$ 

This implies $N(\lambda_{r+1}) \cdots N(\lambda_s) = 1$. This is impossible as each $\lambda_i$ is a prime and hence $N(\lambda_i)$ is a rational integer not equal to $\pm 1$. Similarly $r > s$ is impossible.

Then $r = s$ and $1 = \epsilon_1 \epsilon_2 \cdots \epsilon_s$ and the prime factorization of a composite integer in $\mathbb{R}a[\sqrt{6}]$ is unique up to associates.
III. THE NUMBERS \( \text{Ra}(\sqrt{-21}) \)

Theorem 3.1. The set \( \text{Ra}(\sqrt{-21}) = a + b\sqrt{-21} \), where \( a \) and \( b \) range independently over the field of rational numbers, is a field. \(^2\)

Theorem 3.2. The numbers \( a \) and \( \overline{a} \) of \( \text{Ra}(\sqrt{-21}) \) satisfy a quadratic equation with rational coefficients.

Proof:

\[
\text{a satisfies } x^2 - 2ax + a^2 + 21b^2 = 0 \text{ as does } \overline{a}.
\]

Definition 3.1. \( N(a) = a \overline{a} \).

Theorem 3.3. For every number \( a \neq 0 \) of \( \text{Ra}(\sqrt{-21}) \), \( N(a) \) is a positive rational number.

Proof:

Let \( a = a + b\sqrt{-21} \) where \( a \) and \( b \) are rational numbers.

Then

\[
N(a) = a \overline{a} = a^2 + 21b^2.
\]

This is a rational number since \( a \) and \( b \) are rational, and positive

\(^2\)

The proof of this theorem as well as those of a number of others in this chapter are essentially no different from the proofs of the corresponding theorems of \( \text{Ra}(\sqrt{-6}) \) and will be omitted for sake of brevity. Only major theorems and definitions will be restated.
since \( a^2 \) and \( b^2 \) are squares of real numbers not both zero.

**Theorem 3.4.** \( N(a\beta) = N(a)N(\beta) \), \( a \) and \( \beta \) being numbers of \( Ra(\sqrt{-21}) \).

**Definition 3.2.** \( a \) is an integer of \( Ra(\sqrt{-21}) \) if its principal equation has rational integral coefficients. The set of integers will be denoted by \( Ra[\sqrt{-21}] \).

**Theorem 3.5.** Every rational integer is in \( Ra[\sqrt{-21}] \). Every number of \( Ra[\sqrt{-21}] \), which is rational, is a rational integer.

**Theorem 3.6.** If \( a \) is in \( Ra[\sqrt{-21}] \), so is \( \bar{a} \).

**Theorem 3.7.** A number of \( Ra(\sqrt{-21}) \) is in \( Ra[\sqrt{-21}] \) if and only if it is of the form \( a + b\sqrt{-21} \) where \( a \) and \( b \) are rational integers.

**Proof:**

Let \( a = \frac{a_1 + b_1\sqrt{-21}}{c_1} \) be a number of \( Ra(\sqrt{-21}) \) with \( a_1 \), \( b_1 \) and \( c_1 \) being rational integers with no common factor. \( c_1 \) can be assumed to be positive without loss of generality. The principal equation of \( a \) is

\[
x^2 - \frac{2a_1}{c_1} x + \frac{a_1^2 + 21b_1^2}{c_1^2} = 0
\]

and if \( a \) is in \( Ra[\sqrt{-21}] \)
are rational integers. One of the following cases must hold

(i) $c_1 \neq 1$ and $c_1 \neq 2$,  (ii) $c_1 = 2$,  (iii) $c_1 = 1$.

If $c_1 \neq 1$ and $c_1 \neq 2$, then by (1) $a_1$ and $c_1$ have a common factor which by (2) is also a factor of $b_1$ contrary to the hypothesis that $a_1$, $b_1$ and $c_1$ are rational integers with no common factor.

If $c_1 = 2$, then $c_1^2 = 4$. From (2) $a_1^2 + 21b_1^2 \equiv 0 \mod 4$.

Then $a_1^2 \equiv -21b_1^2 \mod 4$. If $b_1 \equiv 0 \mod 2$ then $b_1^2 \equiv 0 \mod 4$ and $a_1^2 \equiv 0 \mod 4$ hence $a_1 \equiv 0 \mod 2$ and we have $a_1$, $b_1$ and $c_1$ all with factor $2$ contrary to hypothesis. If $b_1 \equiv 1 \mod 2$ then $b_1^2 \equiv 1 \mod 4$ and $a_1^2 \equiv 3 \mod 4$ which is impossible.

Hence $c_1 = 1$ and $a$ and $b$ are rational integers.

Conversely, if $a = a + b\sqrt{-21}$, and $a$ and $b$ are rational integers, then $2a$ and $a^2 + 21b^2$ are rational integers and the principal equation of $a$ has rational coefficients.

Theorem 3.8. The numbers $1$ and $\sqrt{-21}$ form a basis for $\mathbb{R}[\sqrt{-21}]$.

This theorem is an immediate consequence of theorem 3.7.

We can show that $\mathbb{R}\sqrt{-21}$ is closed under addition, subtraction
and multiplication. Together with theorems 3.1 and 3.5 and the fact that multiplication is complex number multiplication and allows no proper divisors of zero, we can conclude that \( \text{Ra}[\sqrt{-21}] \) is an integral domain.

**Theorem 3.9.** If \( \theta_1 \) and \( \theta_2 \) form a basis of \( \text{Ra}[\sqrt{-21}] \), the necessary and sufficient condition that

\[
\begin{align*}
\theta'_1 &= a_{11}\theta_1 + a_{12}\theta_2 \\
\theta'_2 &= a_{21}\theta_1 + a_{22}\theta_2
\end{align*}
\]

where the \( a_{ij} \)'s are rational integers, is also a basis of \( \text{Ra}[\sqrt{-21}] \) is

\[
\begin{vmatrix}
a_{11} & a_{12} \\
a_{21} & a_{22}
\end{vmatrix} = \pm 1
\]

**Theorem 3.10.** If \( \theta_1 \) and \( \theta_2 \) form a basis in \( \text{Ra}[\sqrt{-21}] \) and \( \alpha \) and \( \beta \) are any two numbers of \( \text{Ra}[\sqrt{-21}] \), the discriminant of the numbers \( \alpha \) and \( \beta \) is

\[
\Delta(\alpha, \beta) = \begin{vmatrix}
\theta_1 & \theta_2 \\
-\theta_2 & \theta_1
\end{vmatrix}^2
\]

and is invariant under change of basis.
Theorem 3.11. \( \Delta[\sqrt{-21}] = -84 \).

Proof:

Use \((1, \sqrt{-21})\) as a basis. Then

\[
\Delta[\sqrt{-21}] = \begin{vmatrix} 1 & \sqrt{-21} \\ 1 & -\sqrt{-21} \end{vmatrix}^2 = (-\sqrt{-21} - \sqrt{-21})^2 = (-2\sqrt{-21})^2 = -84.
\]

Definition 3.3. Any integer \( a \) is said to be divisible by an integer \( \beta \), when there exists an integer, \( \gamma \), such that \( a = \beta \gamma \); \( a, \beta, \gamma \) are numbers of \( \mathbb{R}[\sqrt{-21}] \). We say that \( \beta \) and \( \gamma \) are divisors or factors of \( a \) and \( a \) is a multiple of \( \beta \) and \( \gamma \).

Example: \( 27 + \sqrt{-21} \) is divisible by \( 2 + \sqrt{-21} \) since

\[ 27 + \sqrt{-21} = (2 + \sqrt{-21})(3 - \sqrt{-21}). \]

Example: \( 1 + \sqrt{-21} \) is not divisible by \( 1 - \sqrt{-21} \).

Consider

\[ 1 + \sqrt{-21} = (1 - \sqrt{-21})(a + b\sqrt{-21}) \]

\[ 1 + \sqrt{-21} = (a + 21b) + (b-a)\sqrt{-21}. \]

Upon equating coefficients, \( a = -\frac{10}{11} \) and \( b = \frac{1}{11} \). This tells us there are no integral values of \( a \) and \( b \) for which the above equation will hold. Hence \( 1 + \sqrt{-21} \) is not divisible by \( 1 - \sqrt{-21} \).
Theorem 3.12. If $a$ and $\beta$ are numbers in $\mathbb{R}a[\sqrt{-21}]$ and $a$ divides $\beta$ then $N(a)$ divides $N(\beta)$.

Definition 3.4. The units of $\mathbb{R}a[\sqrt{-21}]$ are those integers in $\mathbb{R}a[\sqrt{-21}]$ which divide 1. The units are also those integers whose norms are 1.

Theorem 3.13. The units in $\mathbb{R}a[\sqrt{-21}]$ are 1 and -1.

Proof:

Let $\epsilon = a + b\sqrt{-21}$ be a unit in $\mathbb{R}a[\sqrt{-21}]$ where $a$ and $b$ are rational integers. Then $N(\epsilon) = a^2 + 21b^2 = 1$ and $a$ and $b$ are rational integers so $a = \pm 1$ and $b = 0$.

Definition 3.5. An integer of $\mathbb{R}a[\sqrt{-21}]$ that is not a unit and has no divisors other than its associates and the units, is called a prime number of $\mathbb{R}a[\sqrt{-21}]$.

Definition 3.6. An integer of $\mathbb{R}a[\sqrt{-21}]$ with divisors other than its associates and the units is called a composite number.

Example 1: Determine whether 2 is a prime or composite number of $\mathbb{R}a[\sqrt{-21}]$.

Let $2 = (a + b\sqrt{-21})(c + d\sqrt{-21})$ with $a$, $b$, $c$ and $d$ rational integers. Then by theorem 2.3
\[ 4 = (a^2 + 21b^2)(c^2 + 21d^2) \]

and either

\[ a^2 + 21b^2 = 2 \quad \quad \quad \quad a^2 + 21b^2 = 4 \]

or

\[ c^2 + 21d^2 = 2 \quad \quad \quad \quad c^2 + 21d^2 = 1 \]

The case on the left is impossible and that on the right says that \( c + d \sqrt{-21} \) is a unit. Hence 2 is prime in \( \mathbb{R}[\sqrt{-21}] \).

**Example 2:** 11 is a prime number in \( \mathbb{R}[\sqrt{-21}] \).

Let \( 11 = (a + b \sqrt{-21})(c + d \sqrt{-21}) \) with \( a, b, c \) and \( d \) rational integers. By theorem 2.3

\[ 121 = (a^2 + 21b^2)(c^2 + 21d^2) \]

and either

\[ a^2 + 21b^2 = 11 \quad \quad \quad \quad a^2 + 21b^2 = 121 \]

or

\[ c^2 + 21d^2 = 11 \quad \quad \quad \quad c^2 + 21d^2 = 1 \]

The case on the left is impossible and that on the right says that \( c + d \sqrt{-21} \) is a unit. Hence 11 is a prime in \( \mathbb{R}[\sqrt{-21}] \).

**Example 3:** \( 1 + \sqrt{-21} \) is a prime number in \( \mathbb{R}[\sqrt{-21}] \).

Let \( 1 + \sqrt{-21} = (a + b \sqrt{-21})(c + d \sqrt{-21}) \) with \( a, b, c \) and \( d \)
rational integers. By theorem 2.3

\[22 = (a^2 + 21b^2)(c^2 + 21d^2)\]

and either

\[
\begin{align*}
a^2 + 21b^2 &= 11 & a^2 + 21b^2 &= 22 \\
c^2 + 21d^2 &= 2 & c^2 + 21d^2 &= 1
\end{align*}
\]

The case on the left is impossible and that on the right says that 
\(c + d\sqrt{-21}\) is a unit. Hence \(1 + \sqrt{-21}\) is a prime in \(Ra[\sqrt{-21}]\).

**Example 4:** \(1 - \sqrt{-21}\) is a prime number in \(Ra[\sqrt{-21}]\).

Since \(1 - \sqrt{-21}\) is the conjugate of \(1 + \sqrt{-21}\) the norms of each are the same. Therefore \(1 - \sqrt{-21}\) is a prime in \(Ra[\sqrt{-21}]\).

In the work with \(Ra[\sqrt{6}]\), unique factorization was shown to hold. It can be shown that the analogous theorems are not true in \(Ra[\sqrt{-21}]\), but it will suffice to show at least one composite integer in \(Ra[\sqrt{-21}]\) which doesn't have unique prime factorization.

Consider

\[22 = 2 \cdot 11 = (1 + \sqrt{-21})(1 - \sqrt{-21})\]

It is clear that neither factor in the first pair is an associate of a number in the second pair. It has been shown that \(2, 11, 1 + \sqrt{-21}\) and \(1 - \sqrt{-21}\) are prime numbers in \(Ra[\sqrt{-21}]\). Thus 22 has
two distinct prime factorizations. This example illustrates the fact that unique factorization does not hold for the composite integers of $\text{Ra}[\sqrt{-21}]$. The concept of ideal numbers will be introduced, and unique factorization will be restored in terms of ideal factors.
IV. THE IDEAL NUMBERS IN $Ra(\sqrt{-21})$

**Definition 4.1.** An ideal in $Ra[\sqrt{-21}]$ is an infinite system of integers composed of all linear combinations of any finite number of integers, the coefficients being any integers of $Ra[\sqrt{-21}]$.

If $a_1, a_2, \ldots, a_n$ is a set of $n$ integers in $Ra[\sqrt{-21}]$, then the set of integers $\eta_1 a_1 + \eta_2 a_2 + \cdots + \eta_n a_n$, where $\eta_1, \eta_2, \ldots, \eta_n$ are any integers in $Ra[\sqrt{-21}]$, is an ideal. Such an ideal is denoted $A = (a_1, a_2, \ldots, a_n)$. An ideal which consists of all multiples of an integer $a$ by integers of the domain is called a principal ideal and denoted $(a)$.

**Definition 4.2.** Two ideals $A$ and $B$ are equal, and we write $A = B$, when every number of one is a number of the other.

We see that $A = B$ if and only if every integer defining $A$ is a linear combination of the integers defining $B$ and every integer defining $B$ is a linear combination of the integers defining $A$, using the integers of $Ra[\sqrt{-21}]$ as coefficients in both cases.

**Definition 4.3.** If $(a_1, a_2, \ldots, a_n)$ is an ideal, any one of the $a$'s may be eliminated from the symbol of the ideal if it is a linear combination of those remaining. Likewise we may introduce into the symbol of the ideal any integer which is a linear combination of those already there.
Example 1: \( (2, 1+\sqrt{-21}) = (2, 1-\sqrt{-21}) \).

\( (2, 1+\sqrt{-21}) = (2, 1+\sqrt{-21}, 1-\sqrt{-21}) \)

since

\[ 1-\sqrt{-21} = 2(-\sqrt{-21}) + 1+\sqrt{-21} = (2, 1-\sqrt{-21}) \]

since

\[ 1+\sqrt{-21} = 2(\sqrt{-21}) + 1-\sqrt{-21} \]

Therefore

\( (2, 1+\sqrt{-21}) = (2, 1-\sqrt{-21}). \)

Example 2: \( (11, 1+\sqrt{-21}) \neq (11, 1-\sqrt{-21}) \).

If \( 1+\sqrt{-21} \) is a number of \( (11, 1-\sqrt{-21}) \) then \( x+y\sqrt{-21} \)
and \( a+b\sqrt{-21} \) must exist as two integers of \( \mathbb{R}[\sqrt{-21}] \) such that

\[ 1+\sqrt{-21} = (x+y\sqrt{-21})11 + (a+b\sqrt{-21})(1-\sqrt{-21}). \]

Then

\[ 11x+a+21b = 1 \]
\[ 11y-a+b = 1. \]

The result of combining, \( 11x+11y+22b = 2 \), is impossible since
\( x, y \) and \( b \) are rational integers. Hence the required integers

\( 1+\sqrt{-21} \) is not a number of the ideal \( (11, 1+\sqrt{-21}) \)
and therefore the two ideals are unequal.
Example 3: \( (2, 1 + \sqrt{-21}) \neq (1) \).

There exist \( x + y\sqrt{-21} \) and \( a + b\sqrt{-21} \) in \( \mathbb{R}[\sqrt{-21}] \) such that

\[
1 = (x + y\sqrt{-21})^2 + (a + b\sqrt{-21})(1 + \sqrt{-21}).
\]

Then

\[
2x + a - 21b = 1 \quad 2y + a + b = 0.
\]

The result of combining, \( 2x - 2y - 22b = 1 \), is impossible by reasoning similar to example 2. Therefore the two ideals are unequal.

Definition 4.4. If \( A \) and \( B \) are two ideals, the product \( AB \) is the set formed by multiplying every number of \( A \) by every number of \( B \) and then taking all possible linear combinations of these products, using as coefficients the integers of \( \mathbb{R}[\sqrt{-21}] \).

If \( A = (a_1, a_2, \ldots, a_m) \) and \( B = (\beta_1, \beta_2, \ldots, \beta_n) \) then \( AB \) is the set of numbers given by

\[
(a_1\beta_1, a_1\beta_2, \ldots, a_1\beta_n, a_2\beta_1, \ldots, a_2\beta_n, \ldots, a_m\beta_1, \ldots, a_m\beta_n).
\]

We observe that the product of ideals is an ideal of the same domain and that ideal multiplication is both commutative and associative.
Example 1: \((2, 1+\sqrt{-21})(2, 1+\sqrt{-21}) = (2)\).

\[(2, 1+\sqrt{-21})(2, 1+\sqrt{-21}) = (4, 2+2\sqrt{-21}, 2+2\sqrt{-21}, -20+2\sqrt{-21})\]

\[= (4, 2+2\sqrt{-21}, -20+2\sqrt{-21}, 2)\]

since \(2+2\sqrt{-21}-(20+2\sqrt{-21})-4(4) = 2\). Since all numbers in the symbol are multiples of 2

\((2, 1+\sqrt{-21})^2 = (2, 1+\sqrt{-21})(2, 1+\sqrt{-21}) = (2)\).

Example 2: \((11, 1+\sqrt{-21})(11, 1-\sqrt{-21}) = (11)\).

\[(11, 1+\sqrt{-21})(11, 1-\sqrt{-21}) = (121, 11-11\sqrt{-21}, 11+11\sqrt{-21}, 22)\]

\[= (121, 11-11\sqrt{-21}, 11+11\sqrt{-21}, 22, 11)\]

since \(121-5(22) = 11\). Hence all numbers in the symbol are multiples of 11 and the result follows.

It can also be shown that

\[(1)\quad (2, 1+\sqrt{-21})(11, 1+\sqrt{-21}) = (1+\sqrt{-21})\]

and

\[(2)\quad (2, 1+\sqrt{-21})(11, 1-\sqrt{-21}) = (1-\sqrt{-21})\).

Definition 4.5. An ideal \(A\) is said to be divisible by an ideal \(B\), when there exists an ideal \(C\) such that \(A = BC\); \(B\) and \(C\) are said to be divisors or factors of \(A\).
Definition 4.6. An ideal which divides every ideal of the domain is called a unit ideal.

Theorem 4.1. The only unit ideal in $Ra[\sqrt{-21}]$ is $(1)$.

Proof:

The ideal $(1)$ is the set of all multiples of $1$ by numbers of $Ra[\sqrt{-21}]$ and therefore is the set $Ra[\sqrt{-21}]$. Since any ideal of $Ra[\sqrt{-21}]$ consists of numbers from $Ra[\sqrt{-21}]$, every ideal is divisible by $(1)$.

Let $A = (a_1^2, a_2^2, \ldots, a_n^2)$ be an ideal of $Ra[\sqrt{-21}]$ which divides every ideal in the domain. Since it divides $(1)$, we have $(1) = AB$ where $B = (\beta_1^2, \beta_2^2, \ldots, \beta_m^2)$ is an ideal of the domain. Then

$$(1) = (a_1^2, a_2^2, \ldots, a_n^2)(\beta_1^2, \beta_2^2, \ldots, \beta_m^2)$$

$$= (a_1 \beta_1, \ldots, a_m \beta_m, \ldots, a_n \beta_1, \ldots, a_n \beta_m);$$

hence

$$1 = \lambda_1 a_1 \beta_1 + \lambda_2 a_1 \beta_2 + \cdots + \lambda_m a_n \beta_m$$

$$= \eta_1 a_1 + \eta_2 a_2 + \cdots + \eta_m a_n$$

where $\lambda_1, \lambda_2, \ldots, \lambda_m$ and hence $\eta_1, \eta_2, \ldots, \eta_m$ are integers of $Ra[\sqrt{-21}]$. Therefore $1$ is a number of $A$ and
A = (a_1, a_2, \ldots, a_n, 1) = (1).

The ideal (1) is therefore the only ideal which divides every ideal of \( Ra[\sqrt{-21}] \). Hence (1) is the only unit ideal in \( Ra[\sqrt{-21}] \).

**Definition 4.7.** An ideal different from (1) divisible only by itself and (1) is called a prime ideal. An ideal with divisors other than itself and (1) is called a composite ideal.

Example: \( (2, 1+\sqrt{-21}) \) is a prime ideal.

If this is not the case there would be two ideals

\[ A = (a_1, a_2, \ldots, a_m) \quad \text{and} \quad B = (\beta_1, \beta_2, \ldots, \beta_n), \]

neither of which is (1) such that

\[ (2, 1+\sqrt{-21}) = AB. \]

\[ AB = (a_1 \beta_1, a_1 \beta_2, \ldots, a_1 \beta_n, a_2 \beta_1, \ldots, a_2 \beta_n, \ldots, a_m \beta_1, \ldots, a_m \beta_n), \]

\[ AB = \{ \gamma_1 a_1 \beta_1 + \gamma_2 a_1 \beta_2 + \cdots + \gamma_m a_m \beta_n \} \]

where the \( \gamma \)'s are numbers of \( Ra[\sqrt{-21}] \). Now \( AB \subset A \) since \( AB \) can be written as a linear combination of \( A \), namely \( (\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_m a_m) \) where the \( \lambda \)'s are numbers of \( Ra[\sqrt{-21}] \). By definition of equality \( 2 \) and \( 1+\sqrt{-21} \) are in \( AB \). Since \( AB \subset A \), \( 2 \) and \( 1+\sqrt{-21} \) are in \( A \).

Let \( a_i = a + b\sqrt{-21} \) be any of the integers of \( a_1, a_2, \ldots, a_m \). Then \( a_i = b(1+\sqrt{-21}) + a - b \) and \( a - b \) is a rational integer so
\[ a_i = b(1+\sqrt{-21}) + 2c \]

or

\[ a_i = b(1+\sqrt{-21}) + 2c + 1 \]

where \( c \) is a rational integer.

In the first case \( a_i \) is a linear combination of \( 2, 1+\sqrt{-21} \) and so may be omitted from the symbol for \( A \). In the second case we have

\[ a_i - b(1+\sqrt{-21}) - 2c = 1 \]

and \( 1 \) may be inserted in the symbol for \( A \), in which case \( A = (1) \).

Since \( a_i \) was arbitrary, either all of the numbers \( a_1, a_2, \ldots, a_m \) are linear combinations of \( 2 \) and \( 1+\sqrt{-21} \), in which case we have

\[ A = (2, 1+\sqrt{-21}), \]

or some number of \( A \) is not a linear combination of \( 2 \) and \( 1+\sqrt{-21} \), in which case \( 1 \) may be introduced into the symbol for \( A \) and

\[ A = (1) \cdot \]

The same is true for \( B \). So either
\[(2, 1 + \sqrt{-21}) = (1)(1) = (1)\]
or
\[= (2, 1 + \sqrt{-21})^2\]
or
\[= (2, 1 + \sqrt{-21})(1)\]
or
\[= (1)(2, 1 + \sqrt{-21}).\]

It was shown in example 3 on page 43 that \((2, 1 + \sqrt{-21}) \neq (1)\). Also \((2, 1 + \sqrt{-21}) \neq (2, 1 + \sqrt{-21})^2\) since by example 1 on page 44 \((2, 1 + \sqrt{-21})^2 = (2)\) and \(1 + \sqrt{-21}\) is not a multiple of 2. Thus \((2, 1 + \sqrt{-21}) \neq (2)\). The only divisors of \((2, 1 + \sqrt{-21})\) are therefore the ideal itself and \((1)\). Hence \((2, 1 + \sqrt{-21})\) is a prime ideal.

**Definition 4.8.** An ideal \(G\) is the greatest common divisor of the ideals \(A\) and \(B\) if \(G | A\) and \(G | B\) and if every common divisor of \(A\) and \(B\) divides \(G\).

**Definition 4.9.** Two ideals are relatively prime if their greatest common divisor is \((1)\).

**Example 1:** \(G\) the greatest common divisor of \((2, 1 + \sqrt{-21})\) and \((6, 3 - \sqrt{-21})\) is the set

\[\gamma_1(2) + \gamma_2(1 + \sqrt{-21}) + \gamma_3(6) + \gamma_4(3 - \sqrt{-21})\]
where the $\gamma$'s are integers of $\mathbb{R}[\sqrt{-21}]$. Thus

$$G = (2, 1+\sqrt{-21}, 6, 3-\sqrt{-21})$$

$$= (2, 1+\sqrt{-21}, 3-\sqrt{-21})$$

$$= (2, 1+\sqrt{-21})$$

since $3-\sqrt{-21} = 2(2) - (1+\sqrt{-21})$.

Example 2: $(2, 1+\sqrt{-21})$ and $(11, 1+\sqrt{-21})$ are relatively prime.

$$G = (2, 1+\sqrt{-21}, 11, 1+\sqrt{-21})$$

$$= (2, 1+\sqrt{-21}, 11)$$

$$= (2, 1+\sqrt{-21}, 11, 1)$$

$$= (1).$$

In Chapter II it was shown that in $\mathbb{R}[\sqrt{-21}]$ the integer 22 factors into two sets of prime integers $2 \cdot 11$ and $(1+\sqrt{-21})(1-\sqrt{-21})$.

Now consider $(22) = (2)(11) = (1+\sqrt{-21})(1-\sqrt{-21})$. The ideal $(2)$ is not prime for

$$(2) = (2, 1+\sqrt{-21})^2.$$
Similarly

\((11) = (11, 1+\sqrt{-21})(11, 1-\sqrt{-21})\)

\((1+\sqrt{-21}) = (2, 1+\sqrt{-21})(11, 1+\sqrt{-21})\)

\((1-\sqrt{-21}) = (2, 1+\sqrt{-21})(11, 1-\sqrt{-21})\).

It was shown in an example that \((2, 1+\sqrt{-21})\) is a prime ideal. In a similar manner \((11, 1+\sqrt{-21})\) and \((11, 1-\sqrt{-21})\) can be shown to be prime. So

\[(2)(11) = (2, 1+\sqrt{-21})^2(11, 1+\sqrt{-21})(11, 1-\sqrt{-21})\]

and

\[(1+\sqrt{-21})(1-\sqrt{-21}) = (2, 1+\sqrt{-21})(11, 1+\sqrt{-21})(2, 1+\sqrt{-21})(11, 1-\sqrt{-21})\].

Thus \((22)\) has this decomposition into prime ideal factors which are unique. Hence it has been shown that the introduction of the concept of an ideal number in \(\mathbb{R}[\sqrt{-21}]\) has accomplished, at least in the particular example used, what we desired; namely the restoration of the unique factorization law.

