AN ABSTRACT OF THE THESIS OF

ROGER ARLIE KNOBEL for the M. S. in Mathematics
(Name) (Degree) (Major)

Date thesis is presented August 4, 1966

Title A STUDY OF FACTORIZATION IN $I(\sqrt{-7})$ AND $I(\sqrt{-23})$

Abstract approved [redacted]
(Major professor)

This thesis studies the question of factorization in two quadratic integral domains, $I(\sqrt{-7})$ and $I(\sqrt{-23})$. In the first chapter the definition of quadratic numbers is given. It is proved that $Ra(\sqrt{m})$ is a quadratic number field. The second chapter concerns the integral domain, $I(\sqrt{-7})$, and it is shown that the Unique Factorization Theorem holds. The third chapter studies the integral domain, $I(\sqrt{-23})$, and it is shown that the Unique Factorization Theorem fails. The fourth chapter develops the concept of ideals in order to restore the Unique Factorization Theorem in $I(\sqrt{-23})$.

A STUDY OF FACTORIZATION IN $I(\sqrt{-7})$ AND $I(\sqrt{-23})$

by

ROGER ARLIE KNOBEL

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1967

APPROVED:

[redacted]

Professor of Mathematics

In Charge of Major

[redacted]

Chairman of Department of Mathematics

[redacted]

Dean of Graduate School

Date thesis is presented August 4, 1966

Typed by Carol Baker

TABLE OF CONTENTS

A STUDY OF FACTORIZATION IN $I(\sqrt{-7})$ AND $I(\sqrt{-23})$

1. INTRODUCTION

A number which is a solution of a quadratic equation with rational coefficients is called a quadratic number. The set of numbers of the form, $a+b\sqrt{m}$, where a and b are rational numbers and m is a non-zero integer with distinct factors, is denoted by $Ra(\sqrt{m})$. Theorem 1.1 shows that the numbers of $Ra(\sqrt{m})$ are quadratic numbers.

Theorem 1.1. If $\alpha \epsilon Ra(\sqrt{m})$, then α satisfies a quadratic equation with rational coefficients.

Proof:

Let $\alpha = a+b\sqrt{m}$ be a number of $Ra(\sqrt{m})$. Then α satisfies the following equivalent equations. $[x-(a+b\sqrt{m})]\ [x-(a-b\sqrt{m})] = 0$, $x^2-2ax+a^2-mb^2 = 0$. Since a and b are rational and m is a non-zero integer, then $-2a$ and a^2-mb^2 are rational. So, by the definition of a quadratic number, α is a quadratic number.

Theorem 1.2. $Ra(\sqrt{m})$ is a field.

Proof:

That $Ra(\sqrt{m})$ is an abelian group relative to addition is evident. Since $Ra(\sqrt{m})$ is a subset of the complex number field, the commutative and associative laws of multiplication hold, and also the distributive law. 1 is the identity element for multiplication. This only leaves closure and inverses for multiplication to be shown.

To prove that $Ra(\sqrt{m})$ is closed under multiplication consider $a_1+b_1\sqrt{m}$ and $a_2+b_2\sqrt{m}$ as two numbers of $Ra(\sqrt{m})$. By the distributive law, commutative and associative laws of multiplication and addition, the following is obtained.

$(a_1+b_1\sqrt{m})(a_2+b_2\sqrt{m}) = (a_1a_2+b_1b_2m) + (a_1b_2+a_2b_1)\sqrt{m}$, which is an element of $Ra(\sqrt{m})$.

To obtain the multiplicative inverse of $\alpha = a+b\sqrt{m}$, $\alpha \neq 0$, the following procedure is used.

$$\beta = \frac{1}{a+b\sqrt{m}} = \frac{1}{a+b\sqrt{m}} \; \frac{a-b\sqrt{m}}{a-b\sqrt{m}} = \frac{a}{a^2-b^2m} + \frac{-b}{a^2-b^2m}\sqrt{m}$$

To prove that β is the inverse of α, it is noted that $\alpha\beta = \beta\alpha = 1$. It is only necessary, therefore, to prove that $a^2-b^2m \neq 0$. Suppose $a^2-b^2m = 0$. Then either (i) $a = 0$ and $b = 0$ or (ii) $b \neq 0$. In case (i), if $a = b = 0$, then $\alpha = a+b\sqrt{m} = 0$. In case (ii), $b \neq 0$ and $a^2-b^2m = 0$, then $b^2m = a$ and so $\sqrt{m} = \pm\frac{a}{b}$, which is a rational number. In either case a contradiction is reached and so $a^2-b^2m \neq 0$ and β is the multiplicative inverse of α.

The results of theorems 1.1 and 1.2 show that $Ra(\sqrt{m})$ is a quadratic number field.

The quadratic numbers that are solutions of a quadratic equation with integral coefficients and unity as the coefficient of the squared term are called quadratic integers. The set of quadratic integers which is a subset of $Ra(\sqrt{m})$ is denoted by $I(\sqrt{m})$. It will be shown later in the text that $I(\sqrt{-7})$ and $I(\sqrt{-23})$ are quadratic integral domains.

The integral domain $I(\sqrt{-7})$ is studied in Chapter 2 and it will be shown that the Unique Factorization Theorem is satisfied in $I(\sqrt{-7})$.

In Chapter 3 it will be shown that the Unique Factorization Theorem does not hold true in the integral domain $I(\sqrt{-23})$.

The concept of ideals is introduced in Chapter 4. It is then shown that unique factorization can be restored in terms of the ideals of $I(\sqrt{-23})$.

Throughout the text the symbol I will denote the set of integers and Ra the set of rational numbers.

2. THE QUADRATIC NUMBER FIELD $Ra(\sqrt{-7})$

2.1 The Numbers of $Ra(\sqrt{-7})$

It was shown by theorems 1.1 and 1.2 that $Ra(\sqrt{-7})$ is a quadratic number field. The following definitions and theorems give the background material for finding the primes and units of $I(\sqrt{-7})$ and proving theorems which are necessary to prove the Unique Factorization Theorem.

Definition 2.11. If $\alpha = a+b\sqrt{-7}$, then the conjugate of α, denoted by $\bar{\alpha}$, is $a-b\sqrt{-7}$.

Definition 2.12. The norm of α, denoted by $N(\alpha)$, is $\alpha\bar{\alpha}$.

Theorem 2.11. $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$ and $\overline{\alpha+\beta} = \bar{\alpha}+\bar{\beta}$.

Proof:

$$\bar{\alpha}\bar{\beta} = (a-b\sqrt{-7})(c-d\sqrt{-7}) = (ac-7bd)-(ad+bc)\sqrt{-7} = \overline{\alpha\beta}$$

$$\bar{\alpha}+\bar{\beta} = (a-b\sqrt{-7}) + (c-d\sqrt{-7}) = (a+c)-(b+d)\sqrt{-7} = \overline{\alpha+\beta}$$

Theorem 2.12. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof:

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)\,N(\beta)\ .$$

Theorem 2.13. If $\alpha \epsilon Ra(\sqrt{-7})$, then $N(\alpha) \geq 0$.

Proof:

If $\alpha = a+b\sqrt{-7}$, then $N(\alpha) = (a+b\sqrt{-7})(a-b\sqrt{-7}) = a^2+7b^2 \geq 0$.

Theorem 2.14. $\alpha = 0$ if and only if $N(\alpha) = 0$.

Proof:

If $\alpha = 0$, then $N(\alpha) = 0$.

Let $\alpha = a+b\sqrt{-7}$, then $\alpha = 0$ implies $\bar{\alpha} = 0$. So $N(\alpha) = \alpha\bar{\alpha} = 0$.

If $N(\alpha) = 0$, then $\alpha = 0$.

$N(\alpha) = a^2+7b^2 = 0$ implies that $a = b = 0$ since a and b are rational numbers.

2.2 Integers of $Ra(\sqrt{-7})$

The subset of $Ra(\sqrt{-7})$ whose members are solutions of the quadratic equation, $x^2-2ax+a^2+7b^2 = 0$, where $-2a$ and a^2+7b^2 are integers, is denoted by $I(\sqrt{-7})$. The members of $I(\sqrt{-7})$ are called quadratic integers.

Theorem 2.21. If α is an integer, then α is an element of $I(\sqrt{-7})$.

Proof:

$\alpha = a \epsilon I$ is a solution of $x^2 - 2ax + a^2 = x^2 - 2ax + a^2 + 7 \cdot 0 = 0$. Hence $\alpha \epsilon I(\sqrt{-7})$.

<u>Theorem 2. 22.</u> If α is in $I(\sqrt{-7})$, then $\alpha = \frac{a+b\sqrt{-7}}{2}$, where a and b are both even or odd integers.

Proof:

If α is in $I(\sqrt{-7})$, then α is a solution of $x^2 - 2ax + a^2 + 7b^2 = 0$, where $2a$ and $a^2 + 7b^2$ are integers. But $\alpha + \bar{\alpha} = 2a$ and $\alpha\bar{\alpha} = a^2 + 7b^2$, so $\alpha + \bar{\alpha}$ is an integer and $\alpha\bar{\alpha}$ is also an integer.

Let $\alpha = \frac{a_1 + b_1\sqrt{-7}}{c_1}$, where a_1, b_1, and c_1 are integers and $(a_1, b_1, c_1) = 1$. Then $\alpha + \bar{\alpha} = \frac{2a_1}{c_1}$ and $\alpha\bar{\alpha} = \frac{a_1^2 + 7b_1^2}{c_1^2}$.

Suppose $c_1 \neq 2$ and $c_1 \neq 1$, then $\frac{2a_1}{c_1}$ is an integer which implies that $c_1 | 2a_1$. Hence $(a_1, c_1) = d$, where $d \neq 1$ because $c_1 \neq 2$ and $c_1 \neq 1$. Also $\frac{a_1^2 + 7b_1^2}{c_1^2}$ is an integer, which implies $c_1^2 | (a_1^2 + 7b_1^2)$. Since $(a_1, c_1) = d$ implies $(a_1^2, c_1^2) = d^2$, it follows that $d^2 | (a_1^2 + 7b_1^2)$. Since $d^2 | a_1^2$, then $d^2 | 7b_1^2$. But 7 has no square factors and d^2 has only square prime factors, so $d^2 | b_1^2$, which implies $d | b_1$. Hence it has been shown that $(a_1, b_1, c_1) = d$, where $d \neq 1$. This contradicts the fact that $(a_1, b_1, c_1) = 1$. Therefore $c_1 = 1$ and $c_1 = 2$.

Suppose $c_1 = 2$, then $\frac{2a_1}{c_1} = \frac{2a_1}{2} = a_1$, which is an integer. If $\frac{a_1^2 + 7b_1^2}{c_1^2} = \frac{a_1^2 + 7b_1^2}{4}$ is an integer, then $a_1^2 + 7b_1^2 \equiv 0 \mod 4$. If a_1 is odd, then $a_1^2 \equiv 1 \mod 4$ and $7b^2 \equiv -1 \mod 4$. But $-1 \equiv 7 \mod 4$ and so $7b^2 \equiv 7 \mod 4$. Therefore $b_1^2 \equiv 1 \mod 4$, $b_1 \equiv 1 \mod 2$; that is, b_1 is an odd integer. If a_1 and b_1 are both odd integers, then $\frac{a_1 + b_1\sqrt{-7}}{2}$ is a quadratic integer of $I(\sqrt{-7})$.

Suppose $c_1 = 1$, then $\frac{2a_1}{c_1} = 2a_1$ is an integer. Also $\frac{a_1^2+7b_1^2}{c_1^2} = a_1^2+7b_1^2$ is an integer. Hence $a_1 + b_1\sqrt{-7} = \frac{2a_1+2b_1\sqrt{-7}}{2}$ is an integer and therefore $\frac{a+b\sqrt{-7}}{2}$ is a quadratic integer of $I(\sqrt{-7})$, if a and b are both even.

<u>Theorem 2.23.</u> $I(\sqrt{-7})$ is an integral domain.

Proof:

It is evident that $I(\sqrt{-7})$ is an abelian group under addition. The commutative and associative laws of multiplication follow from the fact that $I(\sqrt{-7})$ is a subset of the quadratic number field $Ra(\sqrt{-7})$. 1 is the multiplicative identity and is an element of $I(\sqrt{-7})$ since all integers are elements of $I(\sqrt{-7})$. Hence $I(\sqrt{-7})$

is an abelian monoid under multiplication. The remaining property of an integral domain to be proved is the cancellation law for multiplication. Suppose $\alpha\beta = \alpha\gamma$, $\alpha \neq 0$, then $\alpha\beta - \alpha\gamma = 0$, and $\alpha(\beta - \gamma) = 0$. Since α, β, γ are in the complex number field, $\alpha \neq 0$, and the last result shows that $\beta - \gamma = 0$. Hence $\beta = \gamma$.

2.3 Basis of $I(\sqrt{-7})$

Two integers, α and $\beta \in I(\sqrt{-7})$, form a basis of $I(\sqrt{-7})$ if every number of $I(\sqrt{-7})$ can be represented in the form, $a\alpha + b\beta$, where $a, b \in I$.

Theorem 2.31. 1 and $\frac{1+\sqrt{-7}}{2}$ form a basis of $I(\sqrt{-7})$.

Proof:

Let $\frac{x+y\sqrt{-7}}{2} \in I(\sqrt{-7})$ and write

$$\frac{x+y\sqrt{-7}}{2} = a(1) + b\left(\frac{1+\sqrt{-7}}{2}\right) = \frac{2a+b}{2} + \frac{b}{2}\sqrt{-7}.$$

From the above equation and equality of complex numbers it follows that $x = \frac{2a+b}{2}$ and $y = b$. Solving for a and b gives $a = \frac{x-y}{2}$ which is in I since x and y are both even or odd integers and $b = y$ is in I. Therefore $\frac{x+y\sqrt{-7}}{2} = \frac{x-y}{2}(1) + y\left(\frac{1+\sqrt{-7}}{2}\right)$.

We shall let $\omega = \frac{1+\sqrt{-7}}{2}$.

In the remaining sections of $I(\sqrt{-7})$, the numbers of $I(\sqrt{-7})$

will be expressed by $a+b\omega$, where $a, b \in I$. The following theorem is proved here in order to ease computations which are necessary later in the text.

Theorem 2.32. $\omega\bar{\omega} = 2$, $\omega + \bar{\omega} = 1$, $\omega^2 = -2+\omega$.

Proof:

$$\omega\bar{\omega} = \frac{1+\sqrt{-7}}{2} \cdot \frac{1-\sqrt{-7}}{2} = \frac{8}{4} = 2$$

$$\omega + \bar{\omega} = \frac{1+\sqrt{-7}}{2} + \frac{1-\sqrt{-7}}{2} = \frac{2}{2} = 1$$

$$\omega^2 = \left(\frac{1+\sqrt{-7}}{2}\right)^2 = \frac{-6+2\sqrt{-7}}{4} = \frac{-3+\sqrt{-7}}{2} = \frac{-3-1}{2} + 1 \cdot \omega = -2+\omega$$

Theorem 2.33. If $a+b\omega$ is in $I(\sqrt{-7})$, then $N(a+b\omega) = a^2+ab+2b^2$.

Proof:

$$N(a+b\omega) = (a+b\omega)\overline{(a+b\omega)} = (a+b\omega)(a+b\bar{\omega})$$

$$= a^2+ab(\omega+\bar{\omega})+b^2\omega\bar{\omega} = a^2+ab+2b^2$$

2.4 Units of $I(\sqrt{-7})$

Definition 2.41: For all β and α in $I(\sqrt{-7})$, β divides α, written $\beta \mid \alpha$, if and only if there exist γ in $I(\sqrt{-7})$ such that $\alpha = \beta\gamma$.

Example: $-2+5\omega \mid -38+7\omega$ because $-38+7\omega = (-2+5\omega)(-1+4\omega)$.

Definition 2.42: A quadratic integer, ϵ, in $I(\sqrt{-7})$ is a unit of $I(\sqrt{-7})$ if $\epsilon \mid \beta$, for all β in $I(\sqrt{-7})$.

Theorem 2.41. The units of $I(\sqrt{-7})$ are 1 and -1.

Proof:

If ϵ is a unit of $I(\sqrt{-7})$, then $\epsilon \mid 1$. Therefore there exists β in $I(\sqrt{-7})$ such that $1 = \beta\epsilon$. Hence $N(1) = N(\beta\epsilon) = N(\beta)N(\epsilon) = 1$. Since $N(\beta) \geq 0$ and $N(\epsilon) \geq 0$ are integers, it follows that $N(\epsilon) = 1$. Now $N(\epsilon) = N(\frac{a+b\sqrt{-7}}{2}) = \frac{a^2+7b^2}{4} = 1$. Hence $a^2+7b^2 = 4$ and this shows that $7b^2 \leq 4$, $b^2 \leq \frac{4}{7}$, or that $b = 0$. Then $a^2 = 4$ so that $a = \pm 2$. Therefore $\epsilon = \frac{\pm 2+0\sqrt{-7}}{2} = \pm 1$.

Definition 2.43: Associates in $I(\sqrt{-7})$ are quadratic integers which differ by a unit factor.

2.5 Prime Numbers of $I(\sqrt{-7})$

Definition 2.51: A prime number of $I(\sqrt{-7})$ is an integer of $I(\sqrt{-7})$ that is not a unit and has no divisors other than its associates and the units.

Example: 3 is prime in $I(\sqrt{-7})$.

If $\alpha\beta = 3$, then $N(\alpha)N(\beta) = N(3) = 9$. This gives two cases to consider since the norm of an integer of $I(\sqrt{-7})$ is a non-negative integer.

Case (i) $N(\alpha) = 1$ and $N(\beta) = 9$.

In this case, $N(\alpha) = 1$ implies that α is a unit.

Case (ii) $N(\alpha) = 3$ and $N(\beta) = 3$.

If $\alpha = a+b\omega$, then $N(\alpha) = a^2+ab+2b^2 = 3$. Then $(a+\frac{b}{2})^2 + \frac{7b^2}{4} = 3$ which implies that $\frac{7b^2}{4} \leq 3$. Then $b^2 \leq 1$ and so $b = 0$ or $b = \pm 1$. If $b = 0$, then there exists no a in I such that $a^2 = 3$. If $b = \pm 1$, then there exists no a in I such that $(a \pm \frac{1}{2})^2 = \frac{5}{4}$. Hence there is no α in $I(\sqrt{-7})$ such that its norm is 3. So the only possible factorization of 3 is as in the first case.

3 is a prime since the only factors of 3 are its associates or the units.

Example: ω is a prime in $I(\sqrt{-7})$.

Suppose $\alpha\beta = \omega$. Then $N(\alpha)N(\beta) = N(\omega) = 2$. Since $N(\alpha) \geq 0$ and $N(\beta) \geq 0$ are integers, then $N(\alpha) = 1$ and $N(\beta) = 2$. But $N(\alpha) = 1$ means α is a unit. Hence ω is prime because its only factors are its associates or the units.

2.6 Unique Factorization in $I(\sqrt{-7})$

In this section, four theorems will be proved. These results will lead to the proof of theorem 2.65, the Unique Factorization Theorem in $I(\sqrt{-7})$, which states that every integer of $I(\sqrt{-7})$ can be represented in one and only one way as a product of prime numbers.

Example: $-6-3\omega = 3\omega^3$.

$$3\omega^3 = 3\omega(\omega^2) = 3\omega(-2+\omega) = -6\omega+3(-2+\omega) = -6\omega-6+3\omega = -6-3\omega.$$

It was shown in section 2.5 that 3 and ω are prime in $I(\sqrt{-7})$.

Theorem 2.61. If α and β are numbers of $I(\sqrt{-7})$ and $\beta \neq 0$, then there exists in $I(\sqrt{-7})$ a number μ such that $N(\alpha-\mu\beta) < N(\beta)$.

Proof:

Let $\frac{\alpha}{\beta} = c+d\omega = (r+r_1)+(s+s_1)\omega$, where r and s are integers nearest to c and d respectively. Hence $|r_1| \leq \frac{1}{2}$ and $|s_1| \leq \frac{1}{2}$. If $|r_1| = \frac{1}{2}$ and $|s_1| = \frac{1}{2}$, then r_1 and s_1 are chosen so that they are opposite in sign.

The following argument will show that $\mu = r+s\omega$ will fulfill the required conditions of the theorem.

Since $\frac{\alpha}{\beta} = (r+s\omega) + (r_1+s_1\omega)$ or $\frac{\alpha}{\beta}-\mu = r_1+s_1\omega$, then $N(\frac{\alpha}{\beta}-\mu) = N(r_1+s_1\omega)$. But $N(r_1+s_1\omega)=r_1^2+r_1s_1+2s_1^2 \leq \frac{1}{4}-\frac{1}{4}+2\cdot\frac{1}{4} = \frac{1}{2}$.

Hence $N(\frac{\alpha}{\beta}-\mu) < 1$ so $N(\alpha-\mu\beta) < N(\beta)$.

<u>Theorem 2.62.</u> Let α_0, β_0 be numbers of $I(\sqrt{-7})$ with $(\alpha_0, \beta_0) = 1$. Define $\alpha_n = \beta_{n-1}$ and $\beta_n = \alpha_{n-1} - \mu_{n-1}\beta_{n-1}$, where μ_{n-1} is determined as in theorem 2.61, then $(\alpha_n, \beta_n) = 1$.

Proof: (by induction)

Let S be the set of positive integers n for which the theorem is true.

Then $1 \in S$. For $\alpha_1 = \beta_0$ and $\beta_1 = \alpha_0 - \mu_0\beta_0$. Suppose $(\alpha_1, \beta_1) = c$. Then $c \mid \alpha_1$ implies that $c \mid \beta_0$. Moreover, $c \mid \beta_1$ implies that $c \mid (\alpha_0 - \mu_0\beta_0)$. But then $c \mid \alpha_0$ since $c \mid \mu\beta_0$. Hence $c \mid \alpha_0$ and $c \mid \beta_0$, and therefore $c = 1$.

Assume $k \in S$. Consider, $\alpha_{k+1} = \beta_k$ and $\beta_{k+1} = \alpha_k - \mu_k\beta_k$, where $(\alpha_k, \beta_k) = 1$. Suppose $(\alpha_{k+1}, \beta_{k+1}) = c$. Then $c \mid \alpha_{k+1}$ implies $c \mid \beta_k$, and $c \mid \beta_{k+1}$ implies $c \mid (\alpha_k - \mu_k\beta_k)$. So $c \mid \alpha_k$, since $c \mid \mu_k\beta_k$. Therefore $c \mid \alpha_k$ and $c \mid \beta_k$ and hence $c = 1$. So $(\alpha_{k+1}, \beta_{k+1}) = 1$ which means that if $k \in S$, then $k+1 \in S$. By the Axiom of Mathematical Induction, S is the set of all positive integers.

<u>Theorem 2.63.</u> If α and β are numbers in $I(\sqrt{-7})$ with $(\alpha, \beta) = 1$, then there exist ξ and η in $I(\sqrt{-7})$ such that $\alpha\xi + \beta\eta = 1$.

Proof:

There are two cases to prove. Case (i) is if α or β is a unit and case (ii) if α and β are not units.

Case (i) α or β is a unit.

Suppose $\alpha = 1$, then $\xi + \beta\eta = 1$ implies that $\beta\eta = 1 - \xi$. The conditions of the theorem are satisfied if $\eta = 1$ and $\xi = \bar{\beta}$.

Case (ii) α and β are not units.

In this argument suppose that $N(\beta) \leq N(\alpha)$. By theorem 2.61 there exist μ such that $N(\alpha - \mu\beta) < N(\beta)$. Let $\alpha_1 = \beta$ and $\beta_1 = \alpha - \mu\beta$. By theorem 2.62, it is seen that $(\alpha_1, \beta_1) = 1$.

If there exists ξ_1 and η_1 such that $\alpha_1\xi_1 + \beta_1\eta_1 = 1$, $\beta(\xi_1) + (\alpha - \mu\beta)\,\eta_1 = 1$, and so $\alpha\eta_1 + \beta(\xi_1 - \mu\eta_1) = 1$, then $\xi = \eta_1$ and $\eta = \xi_1 - \mu\eta_1$. If α_1 or β_1 is a unit, then ξ_1 and η_1 can be determined as in case (i).

If α_1 or β_1 is not a unit, then the process is repeated as in the first part of case (ii). Each time the process is continued, $N(\beta_n) > N(\alpha_n - \mu_n\beta_n)$ by theorem 2.61 and the following sequence of decreasing integers is formed: $N(\alpha) \geq N(\beta) > N(\alpha - \mu\beta) > N(\alpha_1 - \mu_1\beta_1) > \cdots > N(\beta_n) > N(\alpha_n - \mu_n\beta_n)$, where $N(\alpha_n - \mu_n\beta_n) = 0$. A norm of zero must eventually occur, since each norm is a non-negative integer strictly smaller than the preceding one, and the existence of an infinite sequence of non-negative integers which would never end would contradict the well-ordering axiom.

$N(\alpha_n - \mu_n\beta_n) = 0$ implies that $\alpha_n = \mu_n\beta_n$. Then $\beta_n | \alpha_n$. But $(\alpha_n, \beta_n) = 1$ by theorem 2.62. Hence $\beta_n = \epsilon$, where ϵ is a unit.

Hence there exists ξ_n and η_n such that $\alpha_n\xi_n + \beta_n\eta_n = 1$, but $\beta_n = \epsilon$, so $\alpha_n\xi_n + \epsilon\eta_n = 1$. Let $\xi_n = 1$ and $\eta_n = \frac{1-\alpha_n}{\epsilon}$. As seen from above, each ξ_i and η_i can be determined by ξ_{i+1} and η_{i+1} since $\xi_i = \eta_{i+1}$ and $\eta_i = \xi_{i+1} - \mu_i\eta_{i+1}$.

Theorem 2.64. If α and β are numbers of $I(\sqrt{-7})$, π is a prime in $I(\sqrt{-7})$, and $\pi | \alpha\beta$, then $\pi | \alpha$ or $\pi | \beta$.

Proof:

$\pi | \alpha\beta$ implies that there exists a γ in $I(\sqrt{-7})$ such that $\alpha\beta = \gamma\pi$. Suppose π does not divide α. Then $(\pi, \alpha) = 1$ and there exists ξ and η in $I(\sqrt{-7})$ such that $\alpha\xi + \pi\eta = 1$ by theorem 2.63. Hence $\beta\alpha\xi + \beta\pi\eta = \beta$ or since $\beta\alpha = \gamma\pi$, then $\gamma\pi\xi + \beta\pi\eta = \beta$. This implies that $\pi(\gamma\xi + \beta\eta) = \beta$ which shows that $\pi | \beta$ since $\gamma\xi + \beta\eta$ is a number in $I(\sqrt{-7})$.

Corollary 2.641. If $\pi | \alpha_1\alpha_2 \cdots \alpha_n$, then $\pi | \alpha_i$ for at least one i in $\{1, 2, 3, \cdots, n\}$.

Proof:

Suppose π does not divide α_i for $i = 1, 2, 3, \cdots, n-1$. Then by theorem 2.64, $\pi | \alpha_n$.

Theorem 2.65. Every number of $I(\sqrt{-7})$ can be represented in one and only one way as the product of prime numbers.

Proof:

Let α be a number of $I(\sqrt{-7})$. If α is not prime, then there exists β and γ in $I(\sqrt{-7})$ and neither are units such that $\alpha = \beta\gamma$. $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Since $N(\beta)$ and $N(\gamma)$ are positive integers, then $N(\beta) < N(\alpha)$.

If β is not a prime number, then $\beta = \beta_1\gamma_1$, where β_1 and γ_1 are elements of $I(\sqrt{-7})$ and neither are units. So $N(\beta) = N(\beta_1\gamma_1) = N(\beta_1)N(\gamma_1)$ and since $N(\beta_1)$ and $N(\gamma_1)$ are positive integers, then $N(\beta_1) < N(\beta)$. Now $\alpha = \beta_1\gamma_1\gamma$.

Continuing this process, $\alpha = \beta_n\gamma_n\gamma_{n-1}\cdots\gamma_1\gamma$. If β_n is not prime, then $\beta_n = \beta_{n+1}\gamma_{n+1}$, where β_{n+1} and γ_{n+1} are in $I(\sqrt{-7})$ and neither are units. $N(\beta_n) = N(\beta_{n+1})N(\gamma_{n+1})$ implies that $N(\beta_{n+1}) < N(\beta_n)$ since $N(\beta_{n+1})$ and $N(\gamma_{n+1})$ are positive integers.

After a finite number of factorizations, the following sequence of strictly decreasing positive integers is formed: $N(\beta) > N(\beta_1) > N(\beta_2) > \cdots > N(\beta_n) > N(\beta_{n+1})$. A prime number must be reached. If a prime number was not reached, then the above decreasing sequence of positive integers would continue indefinitely which contradicts the well-ordering axiom.

Thus α can be expressed as a product of some prime number π and some number α_1 in $I(\sqrt{-7})$. That is, $\alpha = \pi\alpha_1$.

If α_1 is not a prime number, then using the same argument as above, α_1 can be factored into $\alpha_1 = \pi_2\alpha_2$, where π_2 is a prime.

Hence $\alpha = \pi_1\pi_2\alpha_2$. This process is continued until a prime number π_n is reached in the sequence, $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$.

Thus $\alpha = \pi_1\pi_2 \cdots \pi_n$, which shows each integer of $I(\sqrt{-7})$ can be factored into prime numbers.

This representation of α as a product of primes is unique. Suppose there is another prime factorization of α; that is, $\alpha = \rho_1\rho_2\cdots\rho_m$, where ρ_i is a prime number for $i = 1, 2, \cdots, m$. Then $\pi_1\pi_2\cdots\pi_n = \rho_1\rho_2 \cdots \rho_m$.

Corollary 2. 641 says that if $\pi_1 | \rho_1\rho_2\cdots\rho_m$, then $\pi_1 | \rho_i$ for some i in $\{1, 2, \cdots, m\}$. For convenience, suppose the primes are arranged such that $i = 1$, then $\rho_1 = \epsilon\pi_1$, since ρ_1 is a prime. Hence $\pi_1\pi_2\cdots\pi_n = \epsilon\pi_1\rho_2\rho_3 \cdots \rho_m$ or $\pi_2\pi_3 \cdots \pi_n = \epsilon\rho_2\rho_3 \cdots \rho_m$.

Similarly, $\pi_j | \rho_2\rho_3 \cdots \rho_m$, for j in $\{2, 3, \cdots, n\}$, then $\pi_j | \rho_k$ for some k in $\{2, 3, \cdots, m\}$. Suppose $j = k$, then $\rho_k = \epsilon\pi_k$. Then $\pi_k\pi_{k+1}\cdots\pi_n = \epsilon\pi_k\rho_{k+1} \cdots \rho_m$ or

$\pi_{k+1} \cdots \pi_n = \epsilon \rho_{k+1} \cdots \rho_m$.

Suppose $n > m$, then $\pi_m | \rho_m$ implies that $\rho_m = \epsilon \pi_m$. So $\pi_m \pi_{m+1} \cdots \pi_n = \rho_m$ implies $\pi_m \pi_{m+1} \cdots \pi_n = \epsilon \pi_m$ or $\pi_{m+1} \cdots \pi_n = \epsilon$. This last equation is absurd since primes are not units. So n is not greater than m.

By assuming $m > n$ a contradiction is reached which is similar to the above argument so m is not greater than n. Hence $m = n$.

Thus $\alpha = \pi_1 \pi_2 \cdots \pi_n = \rho_1 \rho_2 \cdots \rho_n$, where $\rho_i = \epsilon \pi_i$ for $i = 1, 2, 3, \cdots, n$. So α has a unique representation of primes.

3. THE QUADRATIC NUMBER FIELD $Ra(\sqrt{-23})$

3.1 The Numbers of $Ra(\sqrt{-23})$

The numbers of $Ra(\sqrt{-23})$ satisfy the quadratic equation $x^2-2ax+a^2+23b^2 = 0$, where $-2a$ and a^2+23b^2 are rational numbers. The set $Ra(\sqrt{-23})$ is a quadratic number field as proved by theorems 1.1 and 1.2.

The proofs of the theorems in this section are similar to the proofs in section 2.1 by replacing -7 with -23. So the proofs have been omitted.

Definition 3.1. The conjugate of $\alpha = a+b\sqrt{-23}$ is $a-b\sqrt{-23}$, denoted by $\bar{\alpha}$.

Definition 3.2. The norm of α is $\alpha\bar{\alpha}$, denoted by $N(\alpha)$.

Theorem 3.11. $\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta}$ and $\overline{\alpha+\beta} = \bar{\alpha}+\bar{\beta}$.

Theorem 3.12. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Theorem 3.13. If $\alpha \epsilon Ra(\sqrt{-23})$, then $N(\alpha) \geq 0$.

Proof:

Suppose $\alpha = a+b\sqrt{-23}$. Then

$N(\alpha) = (a+b\sqrt{-23})(a-b\sqrt{-23}) = a^2+23b^2 \geq 0$.

3.2 Integers of $Ra(\sqrt{-23})$

The subset of $Ra(\sqrt{-23})$ whose members are solutions of the quadratic equation, $x^2-2ax+a^2+23b^2=0$, where $-2a$ and a^2+23b^2 are integers is denoted by $I(\sqrt{-23})$. The members of $I(\sqrt{-23})$ are called quadratic integers.

Theorem 3.21. If α is in I, then α is in $I(\sqrt{-23})$.

Proof:

$\alpha = a \in I$ is a solution of $x^2-2ax+a^2 = x^2-2ax+a^2+23\cdot 0 = 0$. So $\alpha \in I(\sqrt{-23})$.

Theorem 3.22. If $\alpha \in I(\sqrt{-23})$, then $\alpha = \dfrac{a+b\sqrt{-23}}{2}$, where a and b are both even or odd integers.

Proof:

If α be a number in $I(\sqrt{-23})$, then α is a solution of $x^2-2ax+a^2+23b^2=0$. Hence $\alpha+\bar{\alpha}=2a$ is an integer and $\alpha\bar{\alpha}=a^2+23b^2$ is an integer.

Let $\alpha = \dfrac{a_1+b_1\sqrt{-23}}{c_1}$, where a_1, b_1, and c_1 are integers and $(a_1, b_1, c_1) = 1$. Then $\alpha+\bar{\alpha} = \dfrac{2a_1}{c_1}$ and $\alpha\bar{\alpha} = \dfrac{a_1^2+23b_1^2}{c_1^2}$.

Suppose $c_1 \neq 2$ and $c_1 \neq 1$. $\dfrac{2a_1}{c_1}$ is an integer which implies that $c_1 \mid 2a_1$. Therefore $(a_1, c_1) = d$, where $d \neq 1$

because $c_1 \neq 2$ and $c_1 \neq 1$. Also $\frac{a_1^2 + 23b_1^2}{c_1^2}$ is an integer, which implies $c_1^2 | (a_1^2 + 23b_1^2)$. $(a_1, c_1) = d$ implies $(a_1^2, c_1^2) = d^2$, so it follows that $d^2 | (a_1^2 + 23b_1^2)$. Since $d^2 | a_1^2$, then $d^2 | 23b_1^2$. But 23 has no square factors and d^2 has only square prime factors, so $d^2 | b_1^2$, which implies $d | b_1$. Therefore $(a_1, b_1, c_1) = d$, where $d \neq 1$. But this contradicts the fact that $(a_1, b_1, c_1) = 1$. Therefore $c_1 = 1$ or $c_1 = 2$.

Suppose $c_1 = 2$, then $\frac{2a_1}{c_1} = \frac{2a_1}{2} = a_1$ is an integer. If $\frac{a_1^2 + 23b_1^2}{4}$ is an integer, then $a_1^2 + 23b_1^2 \equiv 0 \mod 4$. If a_1 is odd, $a_1^2 \equiv 1 \mod 4$, then $23b_1^2 \equiv -1 \mod 4$, but $-1 \equiv 23 \mod 4$ so $23b_1^2 \equiv 23 \mod 4$ or $b_1^2 \equiv 1 \mod 4$. Hence $b_1^2 \equiv 1 \mod 4$ implies that $b_1 \equiv 1 \mod 2$; that is, b_1 is an odd integer. So $\frac{a_1 + b_1\sqrt{-23}}{2}$ is a quadratic integer of $I(\sqrt{-23})$, if a_1 and b_1 are both odd integers.

Suppose $c_1 = 1$, then $\frac{2a_1}{c_1} = 2a_1$ is an integer and $\frac{a_1^2 + 23b_1^2}{c_1^2} = a_1^2 + 23b_1^2$ is an integer. So $a_1 + b_1\sqrt{-23} = \frac{2a_1 + 2b_1\sqrt{-23}}{2} = \frac{a + b\sqrt{-23}}{2}$ is a quadratic integer of $I(\sqrt{-23})$, if a and b are both even integers.

<u>Theorem 3.23.</u> $I(\sqrt{-23})$ is an integral domain.

Proof:

The proof is similar to theorem 2. 23.

3. 3 Basis of $I(\sqrt{-23})$

Theorem 3. 31. 1 and $\frac{1+\sqrt{-23}}{2}$ form a basis for $I(\sqrt{-23})$.

Proof:

Let $\frac{x+y\sqrt{-23}}{2} \in I(\sqrt{-23})$ and write

$\frac{x+y\sqrt{-23}}{2} = a(1) + b(\frac{1+\sqrt{-23}}{2}) = \frac{2a+b}{2} + \frac{b}{2}\sqrt{-23}$. Then $x = \frac{2a+b}{2}$ and $y = b$ or, solving for a and b; $a = \frac{x-y}{2}$ and $b = y$. Since x and y are both even or odd integers, then $\frac{x-y}{2} = a$ is in I and b is in I. So $\frac{x+y\sqrt{-23}}{2} = \frac{x-y}{2}(1) + y(\frac{1+\sqrt{-23}}{2})$.

We shall write $\frac{1+\sqrt{-23}}{2} = \theta$.

Theorem 3. 32. $\theta\bar{\theta} = 6$, $\theta + \bar{\theta} = 1$, and $\theta^2 = -6 + \theta$.

Proof:

$$\theta\bar{\theta} = \frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2} = \frac{1+23}{4} = 6$$

$$\theta + \bar{\theta} = \frac{1+\sqrt{-23}}{2} + \frac{1-\sqrt{-23}}{2} = \frac{2}{2} = 1$$

$$\theta^2 = (\frac{1+\sqrt{-23}}{2})^2 = \frac{-11+\sqrt{-23}}{2} = \frac{-11-1}{2} + 1\cdot\theta = -6 + \theta .$$

Theorem 3. 33. If $a+b\theta \in I(\sqrt{-23})$, then $N(a+b\theta) = a^2+ab+6b^2$.

Proof:

$$N(a+b\theta) = (a+b\theta)\overline{(a+b\theta)} = (a+b\theta)(a+b\overline{\theta})$$

$$= a^2+ab(\theta + \overline{\theta}) + b^2\theta\,\overline{\theta}$$

$$= a^2 + ab + 6b^2 \quad .$$

3.4 The Units of $I(\sqrt{-23})$

The definitions of $\beta \mid \alpha$ and units in $I(\sqrt{-23})$ are the same as in $I(\sqrt{-7})$.

Theorem 3.41. The units of $I(\sqrt{-23})$ are 1 and -1.

Proof:

If ϵ is a unit of $I(\sqrt{-23})$, then $\epsilon \mid 1$. Hence there exists a β in $I(\sqrt{-23})$ such that $1 = \beta\epsilon$, $N(1) = N(\beta\epsilon) = N(\beta)N(\epsilon) = 1$. Since $N(\beta)$ and $N(\epsilon)$ are non-negative integers as seen by theorems 3.13 and 3.33, it follows that $N(\epsilon) = 1$.

Now $N(\epsilon) = N(\frac{a+b\sqrt{-23}}{2}) = \frac{a^2+23b^2}{4} = 1$. But $a^2+23b^2 = 4$ implies that $23b^2 \leq 4$. Hence $b^2 \leq \frac{4}{23}$, and so $b = 0$. Then $a^2 = 4$; that is, $a = \pm 2$, and so $\epsilon = \frac{\pm 2 + 0\sqrt{-23}}{2} = \pm 1$.

Definition 3.41. Associates are integers in $I(\sqrt{-23})$ that differ by a unit factor.

3.5 Prime Numbers of $I(\sqrt{-23})$

Definition 3.51. A prime number of $I(\sqrt{-23})$ is an integer that is not a unit and has no divisors other than its associates and the units.

Example: 2 is a prime in $I(\sqrt{-23})$

Let $\alpha\beta = 2$, then $N(\alpha\beta) = N(\alpha)N(\beta) = N(2)$ and $N(2) = 4$, so $N(\alpha)N(\beta) = 4$. This result gives two cases to consider since the norm of an integer in $I(\sqrt{-23})$ is a non-negative integer.

Case (i) $N(\alpha) = 1$ and $N(\beta) = 4$.

In this case $N(\alpha) = 1$ implies that α is a unit.

Case (ii) $N(\alpha) = 2$ and $N(\beta) = 2$.

In this case, let $\alpha = a+b\theta$, then $2 = a^2+ab+6b^2$ which yields $2 = (a+\frac{b}{2})^2 + \frac{23}{4}b^2$. Hence $\frac{23}{4}b^2 \leq 2$, $b^2 \leq \frac{8}{23}$, and so $b = 0$. This gives $a^2 = 2$ which implies a is not an integer. So there does not exist the number α such that $N(\alpha) = 2$.

So the only divisors of 2 are the units or its associates which means 2 is prime.

Example: 3 is a prime in $I(\sqrt{-23})$

Using an argument similar to that above, let $\alpha\beta = 3$. Then $N(\alpha)N(\beta) = 9$, which results in two cases.

Case (i) $N(\alpha) = 1$ and $N(\beta) = 9$.

In this case $N(\alpha) = 1$ implies α is a unit.

Case (ii) $N(\alpha) = 3$ and $N(\beta) = 3$.

In this case, $(a + \frac{b}{2})^2 + \frac{23}{4}b^2 = 3$ which gives $b^2 \leq \frac{12}{24}$, $b = 0$, $a^2 = 3$, and so a is not an integer. So there exist no numbers in $I(\sqrt{-23})$ with a norm of 3.

Hence 3 is a prime in $I(\sqrt{-23})$.

Example: θ and $\overline{\theta}$ are prime

Let $\alpha\beta = \theta$. Then $N(\alpha)\,N(\beta) = N(\theta) = 6$. This means that $N(\alpha) = 1$ and $N(\beta) = 6$ or $N(\alpha) = 2$ and $N(\beta) = 3$. If $N(\alpha) = 1$, then α is a unit. But there exists no α in $I(\sqrt{-23})$ such that $N(\alpha) = 2$, as shown above. Hence θ is a prime. Similarly it can be shown that $\overline{\theta}$ is prime.

3.6 Failure of Unique Factorization in $I(\sqrt{-23})$

To have the Unique Factorization Theorem hold true in $I(\sqrt{-23})$ every integer of $I(\sqrt{-23})$ must have a unique representation of prime factors. This is not the case for the integral domain $I(\sqrt{-23})$ as illustrated by the following example.

Example: $6 = 2 \cdot 3 = \theta\overline{\theta}$

$2, 3, \theta, \overline{\theta}$ were shown to be prime in $I(\sqrt{-23})$ in section 3.5.

This is the only possible prime factorization of 6, as proved in the following. Suppose $\alpha\beta = 6$, then $N(\alpha)N(\beta) = N(6) = 36$. Four cases result from this last statement.

(i) $N(\alpha)N(\beta) = 2 \cdot 18$. But there exists no $\alpha \in I(\sqrt{-23})$ such that $N(\alpha) = 2$, as shown in section 3.5.

(ii) $N(\alpha)N(\beta) = 3 \cdot 12$. Again there exists no $\alpha \in I(\sqrt{-23})$ such that $N(\alpha) = 3$, as shown in section 3.5.

(iii) $N(\alpha)N(\beta) = 4 \cdot 9$. If $\alpha = a+b\theta$ and $N(\alpha) = 4$, then $4 = a^2+ab+6b^2 = (a+\frac{b}{2})^2 + \frac{23b^2}{4}$. The last statement shows that $\frac{23b^2}{4} \leq 4$, which implies that $b^2 \leq \frac{16}{23}$ and so $b = 0$. Hence $a^2 = 4$ or $a = \pm 2$. So $\alpha = 2$ and $\beta = 3$. (2 and -2 are associates so only $\alpha = 2$ is considered.)

(iv) $N(\alpha)N(\beta) = 6 \cdot 6$. Again if $\alpha = a+b\theta$ and $N(\alpha) = 6$, then $6 = a^2+ab+6b^2 = (a+\frac{b}{2})^2 + \frac{23b^2}{4}$. So $b^2 \leq \frac{24}{23}$ or $b = \pm 1, 0$. If $b = 1$, then $a = -1$ or $a = 0$. The possibilities for α is $-1+\theta$ or θ. If $b = -1$, then $a = 1$ or $a = 0$. So $\alpha = 1-\theta = \overline{\theta}$ or $\alpha = -\theta$. $\alpha = -1+\theta \Rightarrow \beta = -\theta$ or $\alpha = 1-\theta \Rightarrow \beta = \theta$. But these are associates, so it is only necessary to consider $\alpha = 1-\theta = \overline{\theta}$ and $\beta = \theta$.

It has been shown that 6, an integer in $I(\sqrt{-23})$, has two different prime factorizations. So the Unique Factorization Theorem fails in $I(\sqrt{-23})$.

The remaining part of this chapter will show how some of the theorems used to prove the Unique Factorization Theorem in $I(\sqrt{-7})$ fail in $I(\sqrt{-23})$.

Suppose theorem 2.61 is restated in terms of the integers of $I(\sqrt{-23})$; that is, if α and β are numbers of $I(\sqrt{-23})$ and $\beta \neq 0$, then there exists in $I(\sqrt{-23})$ a number μ such that $N(\alpha-\mu\beta) < N(\beta)$.

Let $\frac{\alpha}{\beta} = c+d\theta = (r+r_1)+(s+s_1)\theta$, where r and s are integers nearest to c and d, respectively. Then $|r_1| \leq \frac{1}{2}$ and $|s_1| \leq \frac{1}{2}$. If $|r_1| = \frac{1}{2}$ and $|s_1| = \frac{1}{2}$, then choose r_1 and s_1 so that they are opposite in sign. If $\mu = r+s\theta$, then $\frac{\alpha}{\beta}-\mu = r_1+s_1\theta$. So $N(\frac{\alpha}{\beta}-\mu) = N(r_1+s_1\theta) = r_1^2+r_1s_1+6s_1^2$, and so $r_1^2+r_1s_1+6s_1^2 \leq \frac{1}{4} - \frac{1}{4} + 6\cdot \frac{1}{4} \leq \frac{3}{2}$. Hence $N(\frac{\alpha}{\beta}-\mu) < 1$ cannot be concluded. But $N(\alpha-\mu\beta) < N(\beta)$ is necessary in order to prove the analog of theorem 2.63 in $I(\sqrt{-23})$.

Example: Let $\alpha = 3$, $\beta = \theta$, and $\mu = x+y\theta$, then $\frac{\alpha}{\beta} = \frac{1}{2} - \frac{1}{2}\theta$.

$$N(\frac{\alpha}{\beta}-\mu) = N[(\frac{1}{2}-\frac{1}{2}\theta)-(x+y\theta)] = N[(\frac{1}{2}-x)+(-\frac{1}{2}-y)\theta] = (\frac{1}{2}-x)^2+(\frac{1}{2}-x)(-\frac{1}{2}-y)+(-\frac{1}{2}-y)^2 6.$$

Rewriting the last expression as the sum of two positive numbers, $[(\frac{1}{2}-x) + (-\frac{1}{2}-y)]^2 + \frac{23}{4}(-\frac{1}{2}-y)^2$. Since $\frac{23}{4}(-\frac{1}{2}-y)^2 > 1$ for all y in I, the last expression is greater than one.

If theorem 2.63 is restated for the integral domain $I(\sqrt{-23})$, then it fails to be true as shown by the following example.

Example: If $\alpha = 3$ and $\beta = \theta$, where $(3, \theta) = 1$, there exist no $\xi = a+b\theta$ and $\eta = c+d\theta$ in $I(\sqrt{-23})$ such that $3\xi + \theta\eta = 1$. Writing $3\xi + \theta\eta = 1$ as $3(a+b\theta) + \theta(c+d\theta) = 1$ and then $(3a-6d) + (3b+c+d)\theta = 1$ implies that $3a-6d = 1$. The last equation shows $3 \mid (3a-6d)$ which implies $3 \mid 1$. Hence a and d are not integers. So ξ and η do not exist in $I(\sqrt{-23})$.

If the product of two integers is divisible by a prime number, at least one of the integers is divisible by that prime does not hold in $I(\sqrt{-23})$. Consider the following example.

Example: It is known that $6 = \theta\,\overline{\theta}$. Also $2 \mid 6$ but 2 does not divide θ or $\overline{\theta}$ since θ and $\overline{\theta}$ are prime. Also 2 was shown to be prime in $I(\sqrt{-23})$.

4. IDEALS IN $I(\sqrt{-23})$

4.1 Introduction of Ideals

In order to restore the Unique Factorization Theorem in $I(\sqrt{-23})$, it is necessary to introduce the concept of ideals in $I(\sqrt{-23})$. The definitions and theorems in this section will give the necessary background to work with ideals. Capital letters will represent ideals.

Definition 4.11. $A = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is an ideal in $I(\sqrt{-23})$, where $\alpha_i \in I(\sqrt{-23})$ and $i \in \{1, 2, \cdots, n\}$, if $\beta \in A$, then $\beta = \alpha_1\xi_1 + \alpha_2\xi_2 + \cdots + \alpha_n\xi_n$, where $\xi_i \in I(\sqrt{-23})$ for $i \in \{1, 2, \cdots, n\}$.

The following theorem shows that every ideal in $I(\sqrt{-23})$ can be generated by at most two numbers of $I(\sqrt{-23})$. This will ease the computations in the following theorems.

Theorem 4.11. If A is an ideal, then ω_1 and ω_2 exist in $I(\sqrt{-23})$ such that for all α in A, $\alpha = k_1\omega_1 + k_2\omega_2$, where $k_1, k_2 \in I$.

Proof:

If $\alpha_i \neq 0$ is in A, then $N(\alpha_i)$ is in A since we may write $N(\alpha_i) = \xi_1\alpha_1 + \xi_2\alpha_2 + \cdots \xi_i\alpha_i + \cdots + \xi_n\alpha_n$, with $\xi_i = \bar{\alpha}_i$ and $\xi_j = 0$ if $j \neq i$.

So A contains positive integers. Let ω_1 be the smallest positive integer in A.

Of all numbers $\ell_1 + \ell_2\theta$ in A, where $\ell_2 \neq 0$ and ℓ_2, ℓ_1 are integers, choose as ω_2 one for which $\ell_2 > 0$ and minimal. Then write $\omega_2 = \ell_1 + \ell_2\theta$.

If $\alpha = a_1 + a_2\theta$ is in A, then express $a_2 = \ell_2 k_2 + r_2$, where $0 \leq r_2 < \ell_2$. Hence $\alpha = a_1 + (\ell_2 k_2 + r_2)\theta = a_1 + k_2(\ell_2\theta) + r_2\theta$ or $\alpha = a_1 + k_2(\omega_2 - \ell_1) + r_2\theta$. Subtracting $k_2\omega_2$ from both sides of the last equation, $\alpha - k_2\omega_2 = (a_1 - k_2\ell_1) + r_2\theta$. Since $\alpha - k_2\omega_2$ is in A, then $r_2 = 0$. If $r_2 \neq 0$, then $0 < r_2 < \ell_2$ which means ℓ_2 was not minimal as selected above. So $\alpha - k_2\omega_2 = a_1 - k_2\ell_1$.

Let $a_1 - k_2\ell_1 = b$, then we can write $b = \omega_1 k_1 + r_1$ where $0 \leq r_1 < \omega_1$. If $r_1 \neq 0$, then $0 < r_1 < \omega_1$, which means ω_1 was not minimal as selected above. So $r_1 = 0$, then $b = \omega_1 k_1$. Therefore $\alpha - k_2\omega_2 = \omega_1 k_1$ or $\alpha = k_1\omega_1 + k_2\omega_2$.

<u>Definition 4.12:</u> Let A and B be ideals. Then <u>$A = B$</u> if and only if every element α of A is also an element of B and every element β of B is an element of A.

<u>Definition 4.13.</u> Let $A = (\alpha_1, \alpha_2)$ and $B = (\beta_1, \beta_2)$. Then <u>AB</u> $= (\alpha_1\beta_1, \alpha_2\beta_1, \alpha_1\beta_2, \alpha_2\beta_2)$.

<u>Definition 4.14:</u> Ideal B <u>divides</u> ideal A, written as $B|A$, if

there exists C such that $A = BC$.

<u>Theorem 4.12.</u> If $B|A$, then every element α of A is in B.

Proof:

If $B|A$, then there exists C such that $A = BC$. Let $A = (\alpha_1, \alpha_2)$, $B = (\beta_1, \beta_2)$, and $C = (\gamma_1, \gamma_2)$. Then $A = BC = (\beta_1\gamma_1, \beta_2\gamma_1, \beta_1\gamma_2, \beta_2\gamma_2)$. If α is in A, then $\alpha = \xi_1\beta_1\gamma_1 + \xi_2\beta_2\gamma_1 + \xi_3\beta_1\gamma_2 + \xi_4\beta_2\gamma_2$, for ξ_1, ξ_2, ξ_3, and ξ_4 in $I(\sqrt{-23})$. Rewriting the last expression as, $\alpha = (\xi_1\gamma_1+\xi_3\gamma_2)\beta_1 + (\xi_2\gamma_1+\xi_4\gamma_2)\beta_2$ shows that α is an element of B.

<u>Corollary 4.121.</u> If $B|A$ and $A|B$, then $A = B$.

Proof:

If $B|A$, then every element α of A is in B. If $A|B$, then every element β of B is in A. So by the definition of equality of ideals, $A = B$.

<u>4.2 Unit Ideal in $I(\sqrt{-23})$</u>

<u>Definition 4.21.</u> A <u>unit</u> <u>ideal</u> is an ideal which divides all ideals.

<u>Theorem 4.21.</u> (1) is the unit ideal.

Existence: Let $A = (\alpha_1, \alpha_2)$.

$A(1) = (\alpha_1, \alpha_2)(1) = (\alpha_1 \cdot 1, \alpha_2 \cdot 1) = (\alpha_1, \alpha_2) = A$. Hence $(1)|A$.

So (1) is a unit ideal.

Uniqueness: Suppose B is a unit ideal, then $B|A, \forall A$. If $A = (1)$, then $B|(1)$. Since $(1)|B$ and corollary 4.121, $(1) = B$.

4.3 Prime Ideals in $I(\sqrt{-23})$

Definition 4.31. An ideal A, which is not the unit ideal, is prime if and only if A is divisible only by itself and the unit ideal.

Example: $(2, \theta)$ is a prime ideal.

Suppose $(2, \theta)$ is not a prime ideal, then there exists A and B, where neither is the unit ideal, such that $AB = (2, \theta)$.

Let $A = (\alpha_1, \alpha_2)$ and $B = (\beta_1, \beta_2)$. Then $AB = (2, \theta)$ implies that $A = (\alpha_1, \alpha_2, 2, \theta)$ and $B = (\beta_1, \beta_2, 2, \theta)$ by theorem 4.12.

Let $\alpha_i = \dfrac{a+b\sqrt{-23}}{2}$ be any of the integers in A. Then $\alpha_i = b(\dfrac{1+\sqrt{-23}}{2}) + \dfrac{a-b}{2}$ or $\alpha_i = b\theta + \dfrac{a-b}{2}$. For α_i to be an integer of $I(\sqrt{-23})$, then $\dfrac{a-b}{2}$ is an integer. This implies that $\dfrac{a-b}{2} = 2c$ or $\dfrac{a-b}{2} = 2c+1$, where c is in I.

Suppose $\alpha_i = b\theta + 2c$, then α_1 and α_2 can be expressed as a linear combination of θ and 2. Hence $A = (2, \theta)$.

Now suppose that $\alpha_i = b\theta + 2c+1$. Then $\alpha_i - b\theta - 2c = 1$ which implies 1 is a linear combination of α_i, θ, and 2. So $A = (\alpha_1, \alpha_2, 2, \theta, 1)$. But every element of A can be expressed in terms of 1, so $A = (1)$.

Using an argument similar to that as above, it can be shown that $B = (2, \theta)$ or $B = (1)$.

Therefore the possible factorizations of $(2, \theta)$ are as follows.

Case (i) $(2, \theta) = (1)(1) = (1)$.

Case (ii) $(2, \theta) = (2, \theta)(2, \theta)$.

Case (iii) $(2, \theta) = (1)(2, \theta)$.

In case (i), it will be shown that $(2, \theta) \neq (1)$. Suppose it is true that $(2, \theta) = (1)$. That means $1 = 2(a+b\theta) + \theta(c+d\theta)$, $1 = (2a-6d) + (2b+c+d)\theta$, which implies that $1 = 2a-6d$. But $2a-6d = 1$ implies $2|1$ which is absurd. So there does not exist $a+b\theta$ and $c+d\theta$ such that 1 is a linear combination of 2 and θ. Hence $(2, \theta) \neq (1)$.

Also case (ii) is not true; that is, $(2, \theta) \neq (2, \theta)(2, \theta)$. Suppose $(2, \theta) = (2, \theta)(2, \theta)$. Multiplying, $(2, \theta)(2, \theta) = (4, 2\theta, 2\theta, \theta^2) = (4, 2\theta, -6+\theta)$. But $2\theta = 4(-3+\theta)+(-6+\theta)(-2)$, so $(4, 2\theta, -6+\theta) = (4, -6+\theta)$. If $(2, \theta) = (4, -6+\theta)$, then every element of $(2, \theta)$ is an element of $(4, -6+\theta)$, and every element of $(4, -6+\theta)$ is an element of $(2, \theta)$. Suppose θ is in $(4, -6+\theta)$, then $\theta = 4(a+b\theta)+(-6+\theta)(c+d\theta)$, or simplifying, $\theta = (4a-6c-6d) + (4b-5d+c)\theta$. This implies $0 = 2a-3c-3d$ and

$1 = 4b-5d+c$. Adding these two equations, $1 = 2a+4b-2c-8d$, which implies $2|1$. Hence $a+b\theta$ and $c+d\theta$ do not exist to represent θ as a linear combination of 4 and $-6+\theta$. Therefore θ is not an element of $(4, -6+\theta)$. So $(2, \theta) \neq (4, -6+\theta)$, which implies $(2, \theta) \neq (2, \theta)(2, \theta)$.

Case (iii) contradicts the assumption that neither A or B is the unit ideal.

So the assumption that $(2, \theta)$ was not prime yields three cases which proved to be false. Hence the assumption is false, so $(2, \theta)$ is prime in $I(\sqrt{-23})$.

Example: $(2, 1-\theta)$ is a prime ideal.

The proof of this example is similar to the proof of $(2, \theta)$ is a prime ideal.

Example: $(3, \theta)$ is a prime ideal.

Suppose $(3, \theta)$ is not prime, then there exists A and B, where neither is the unit ideal, such that $AB = (3, \theta)$.

Let $A = (\alpha_1, \alpha_2)$ and $B = (\beta_1, \beta_2)$. Then $AB = (3, \theta)$ implies that $A = (\alpha_1, \alpha_2, 3, \theta)$ and $B = (\beta_1, \beta_2, 3, \theta)$ by theorem 4.12.

Let $\alpha_i = \frac{a+b\sqrt{-23}}{2}$ be any of the elements of A. Rewriting α_i in the form, $\alpha_i = b(\frac{1+\sqrt{-23}}{2}) + \frac{a-b}{2}$ or $\alpha_i = b\theta + \frac{a-b}{2}$. Since α_i is an integer of $I(\sqrt{-23})$, then $\frac{a-b}{2}$ is an integer and of the form $3c$, $3c+1$, or $3c+2$, where c is an integer.

Suppose $\alpha_i = b\theta+3c$, then α_1 and α_2 can be expressed as a linear combination of θ and 3. Hence $A = (\alpha_1, \alpha_2, 3, \theta) = (3, \theta)$.

If $\alpha_i = b\theta+3c+1$, then $\alpha_i-b\theta-3c = 1$, which implies 1 is a linear combination of α_i, θ, and 3. So $A = (\alpha_1, \alpha_2, 3, \theta) = (\alpha_1, \alpha_2, 3, \theta, 1)$. But each element of A can be expressed in terms of 1, so $A = (1)$.

The last form of α_i is $\alpha_i = b\theta+3c+2$. Then $\alpha_i-b\theta-3c = 2$, which implies that 2 is an element of A. So $A = (\alpha_1, \alpha_2, 3, \theta) = (\alpha_1, \alpha_2, 3, \theta, 2)$. But 1 is a linear combination of the elements of $(\alpha_1, \alpha_2, 3, \theta, 2)$, so $A = (\alpha_1, \alpha_2, 3, \theta, 2, 1)$. Since each element of A can be expressed in terms of 1, then $A = (1)$.

It also follows that $B = (3, \theta)$ or $B = (1)$.

Therefore the possible factorizations of $(3, \theta)$ areas follows:

Case (i) $(3, \theta) = (1)(1) = (1)$.

Case (ii) $(3, \theta) = (3, \theta)(3, \theta)$.

Case (iii) $(3, \theta) = (1)(3, \theta)$.

Consider case (i), $(3, \theta) = (1)$. Suppose $(3, \theta) = (1)$, then $1 = 3(a+b\theta) + \theta(c+d\theta)$ or rewriting as $1 = (3a-6d)+(3b+c+d)\theta$ yields $1 = 3a-6d$. Hence $3 | 1$ which implies there exist no $a+b\theta$ and

$c+d\theta$ which expresses 1 as a linear combination of 3 and θ. Hence $(3,\theta) \neq (1)$.

In case (ii), $(3,\theta) = (3,\theta)(3,\theta)$ will be shown to be false. Consider the product $(3,\theta)(3,\theta) = (9, 3\theta, 3\theta, \theta^2) = (9, 3\theta, -6+\theta)$. But $3\theta = 9(4+\theta) + (-6+\theta)(-6)$, so $(9, 3\theta, -6+\theta) = (9, -6+\theta)$. Hence $(3,\theta)(3,\theta) = (9, -6+\theta)$. If $(3,\theta) = (3,\theta)(3,\theta) = (9, -6+\theta)$, then θ is an element of $(9, -6+\theta)$. That is, $\theta = 9(a+b\theta) + (-6+\theta)(c+d\theta)$ or rewriting as $\theta = (9a-6c-6d) + (9b-5d+c)\theta$. The last equation implies that $0 = 3a-2c-2d$ and $1 = 9b-5d+c$. Multiply both sides of $0 = 3a-2c-2d$ by 2 to obtain $0 = 6a-4c-4d$ and add to $1 = 9b-5d+c$ to yield $1 = 6a+9b-3c-9d$. The last equation implies $3 \mid 1$. Hence there does not exist $a+b\theta$ and $c+d\theta$ which expresses θ as a linear combination of 9 and $-6+\theta$. Therefore θ is not an element of $(9, -6+\theta)$ which implies that $(3,\theta)(3,\theta) \neq (3,\theta)$.

Case (iii), $(3,\theta) = (1)(3,\theta)$, contradicts the assumption that neither A or B is a unit.

Therefore the assumption that $(3,\theta)$ is not a prime resulted into three cases of factorizations in which each case proved to be false. Hence $(3,\theta)$ is a prime in $I(\sqrt{-23})$.

Example: $(3, 1-\theta)$ is a prime ideal.

The proof is similar to the proof that $(3,\theta)$ is a prime ideal.

4.4 Restoration of the Unique Factorization Theorem

In section 3.6 it was shown that $6 = 2 \cdot 3 = \theta \overline{\theta}$, where $2, 3, \theta$ and $\overline{\theta}$ are prime numbers in $I(\sqrt{-23})$. In this section, 6 is considered as the ideal (6) and is factored into prime ideals. Since 6 was factored into primes by two ways, then the following product of ideals are considered, $(2)(3)$ and $(\theta)(\overline{\theta})$.

Consider the ideal (6) factored as the following: $(6) = (2)(3)$.

The following argument will show that $(2) = (2, \theta)(2, 1-\theta)$ and $(3) = (3, \theta)(3, 1-\theta)$, where $(2, \theta), (2, 1-\theta), (3, \theta)$, and $(3, 1-\theta)$ are prime ideals in $I(\sqrt{-23})$.

First, consider $(2) = (2, \theta)(2, 1-\theta)$.

$(2, \theta)(2, 1-\theta) = (4, 2-2\theta, 2\theta, 6) = (4, 2-2\theta, 2\theta, 6, 2)$. The last ideal follows from the fact that $2 = (-1)4 + 0(2-2\theta) + 0 \cdot 2\theta + 1 \cdot 6$. It is evident that all the elements of $(4, 2-2\theta, 2\theta, 6, 2)$ can be written in terms of 2, so $(4, 2-2\theta, 2\theta, 6, 2) = (2)$.

Second, consider $(3) = (3, \theta)(3, 1-\theta)$.

$(3, \theta)(3, 1-\theta) = (9, 3-3\theta, 3\theta, 6) = (9, 3-3\theta, 3\theta, 6, 3)$, since $3 = 1 \cdot (9) + 0(3-3\theta) + 0(3\theta) + (-1)(6)$. All the elements of $(9, 3-3\theta, 3\theta, 6, 3)$ can be written in terms of 3, so this ideal is (3). Hence $(3, \theta)(3, 1-\theta) = (3)$.

The above shows that a prime factorization of (6) is

$(6) = (2, \theta)(2, 1-\theta)(3, \theta)(3, 1-\theta)$.

The factorization, $(6) = (\theta)(1-\theta)$, is also possible since $\theta(1-\theta) = \theta\overline{\theta} = 6$.

Consider the product, $(2,\theta)(3,\theta) = (6, 2\theta, 3\theta, -6+\theta)$. Since $\theta = 6\cdot 0+(-1)2\theta+1(3\theta)+0(-6+\theta)$, then θ is an element of the ideal, $(6, 2\theta, 3\theta, -6+\theta)$. That is, $(6, 2\theta, 3\theta, -6+\theta) = (6, 2\theta, 3\theta, -6+\theta, \theta)$. But each element of $(6, 2\theta, 3\theta, -6+\theta, \theta)$ can be written in terms of θ. Therefore $(2,\theta)(3,\theta) = (6, 2\theta, 3\theta, -6+\theta, \theta) = (\theta)$.

Next consider the product, $(2, 1-\theta)(3, 1-\theta) = (6, 2-2\theta, 3-3\theta, -5-\theta)$. Since $1-\theta = 0\cdot 6+(-1)(2-2\theta)+(1)(3-3\theta)+(0)(5+\theta)$, then $(6, 2-2\theta, 3-3\theta, -5-\theta) = (6, 2-2\theta, 3-3\theta, -5-\theta, 1-\theta)$. Each element of $(6, 2-2\theta, 3-3\theta, -5-\theta, 1-\theta)$ can be expressed in terms of $1-\theta$, so $(2, 1-\theta)(3, 1-\theta) = (6, 2-2\theta, 3-3\theta, -5-\theta, 1-\theta) = (1-\theta)$.

Hence it has been shown that $(\theta) = (2,\theta)(3,\theta)$ and $(1-\theta) = (2, 1-\theta)(3, 1-\theta)$. So the factorization of $(6) = (\theta)(1-\theta)$ is also $(2,\theta)(3,\theta)(2,1-\theta)(3,1-\theta)$, where this last representation consists of prime ideals. But this factorization is exactly the same as (6) factored first as $(2)(3)$ and then as a product of prime ideals.

If the integer 6 in $I(\sqrt{-23})$ is considered as the ideal (6), then unique prime factorization of 6 can be restored.

To restore unique factorization in $I(\sqrt{-23})$, the integer α in $I(\sqrt{-23})$ is considered as the ideal (α). Then the properties of ideals can be used to factor (α) uniquely as a product of prime ideals.

BIBLIOGRAPHY

1. Birkhoff, Garrett and Saunders MacLane. A survey of modern algebra. New York, Macmillan, 1963. 472 p.

2. Cohn, Harvey. A second course in number theory. New York, Wiley, 1962. 276 p.

3. LeVeque, William. Elementary theory of numbers. Reading, Mass., Addison-Wesley, 1962. 132 p.

4. MacDuffee, C.C. Introduction to abstract algebra. New York, Wiley, 1940. 303 p.

5. Moore, John. Elements of abstract algebra. New York, Macmillan, 1962. 203 p.

6. Reid, Legh. The elements of the theory of algebraic numbers. New York, Macmillan, 1910. 454 p.

7. Weyl, H. Algebràic theory of numbers. Princeton, N.J., Princeton University Press, 1940. 223 p.