AN ABSTRACT OF THE THESIS OF

Adelbert Frederick Hackert for the M.S. in Mathematics
(Name) (Degree) (Major)

Date thesis is presented August 9, 1965

Title QUADRATIC INTEGRAL DOMAINS IN Ra($\sqrt{5}$) AND Ra($\sqrt{-13}$)

Abstract approved Redacted for Privacy
(Major professor)

Some of the properties of the numbers of two quadratic number fields are explored. Among these properties is the existence of unique prime factorization of the integers of the field and the importance of the concept of ideal numbers in restoring unique factorization when it does not exist. Some consideration is given to the relationship between the nature of the ideals of an integral domain and the existence of unique factorization in that domain.

QUADRATIC INTEGRAL DOMAINS IN $Ra(\sqrt{5})$ AND $Ra(\sqrt{-13})$

by

ADELBERT FREDERICK HACKERT

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1966

APPROVED:

Redacted for Privacy

Professor of Mathematics

In Charge of Major

Redacted for Privacy

Chairman of Mathematics Departments

Redacted for Privacy

Dean of Graduate School

Date thesis is presented August 9, 1965

Typed by Carol Baker

TABLE OF CONTENTS

QUADRATIC INTEGRAL DOMAINS IN Ra $(\sqrt{5})$ AND Ra $(\sqrt{-13})$

I. INTRODUCTION

An algebraic number is defined to be a complex number which satisfies a polynomial equation with rational coefficients. Every algebraic number satisfies many such polynomial equations, but among these is one of least degree (3, p. 1-2). The degree of this equation determines the degree of the number. A number which satisfies an irreducible quadratic equation is therefore called a quadratic number.

Suppose ρ is a quadratic number. We are first interested in the set of numbers $a_1 + b_1\rho$, where a_1 and b_1 are rational numbers. For every ρ there exists some rational integer m, without a repeated prime factor, such that the set $a + b\sqrt{m}$ is identical to the set $a_1 + b_1\rho$ (3, p. 280-283).

The purpose of this paper is to consider two such sets, one in which $m = 5$, the other in which $m = -13$. The paper will show that these sets are fields, and that in each field there is a particular subset which is an integral domain, and whose elements will be called integers.[1] In the first set unique factorization of these integers into prime factors will be demonstrated. In the second set this property is absent, so ideal numbers will be introduced, which will restore

[1] To avoid confusion, the term <u>integer</u> will be used in reference to a number of quadratic integral domain, while the ordinary integers of arithmetic will be called <u>rational integers</u>.

the unique factorization.

In the development, the following definitions will be used:

1.1 A group is a mathematical system composed of a set of elements with a well defined binary operation and:

1. The system is closed under the operation.

2. The operation is associative. That is

$$(a + b) + c = a + (b + c)$$

for every element a, b and c of the set.

3. There exists an identity element $\underline{0}$ such that

$$a + \underline{0} = \underline{0} + a = a$$

for every element a of the set.

4. Every element a has an inverse $\bar{a}$ such that

$$a + \bar{a} = \bar{a} + a = \underline{0}$$

1.2. An abelian group is one in which the operation is commutative. That is

$$a + b = b + a$$

for every element a, b of the group.

1.3. A ring is a mathematical system consisting of a set of elements closed under two well defined binary operations, addition (+) and multiplication (×) and subject to the following:

1. The elements form an abelian group relative to addition.

2. Multiplication is associative.

3. Multiplication is distributive over addition. That is, for every element a, b and c in the system

$$a \times (b + c) = a \times b + a \times c .$$

1.4. An <u>integral domain</u> is a ring in which:

1. The operation multiplication is commutative.

2. There exists an identity element for multiplication.

3. There are no proper divisors of zero.

1.5. A <u>field</u> is an integral domain in which every element except the additive identity has an inverse under multiplication.

It will be assumed that the complex number system has been developed and shown to be a field and that sufficient background to establish the following specific properties from number theory and algebra have been developed.

1.6a. The natural numbers are well ordered.

1.6b. Every composite rational integer has a unique factorization into a finite number of prime factors.

1.6c. If a is a rational integer, a^2 is congruent to 0 or 1 mod 4, and in particular for

$$a \equiv 1 \bmod 2, \quad a^2 \equiv 1 \bmod 4$$

$$a \equiv 0 \bmod 2, \quad a^2 \equiv 0 \bmod 4$$

and conversely.

1.6d. In an integral domain $ab = ac$ and $a \neq 0$ implies $b = c$ for all b and c.

II. THE NUMBERS Ra ($\sqrt{5}$)

Definition 2. 1. The set of numbers $a + b\sqrt{5}$, where a and b range independently over the field of rational numbers, will be called Ra ($\sqrt{5}$).

Theorem 2. 1. Ra ($\sqrt{5}$) is a field.

Proof: a. The set is closed under addition and multiplication, for if we take $\alpha = a + b\sqrt{5}$ and $\beta = c + d\sqrt{5}$ we have

$$\alpha + \beta = (a + c) + (b + d)\sqrt{5}$$

$$\alpha \cdot \beta = (ac + 5bd) + (ad + bc)\sqrt{5}$$

and a, b, c and d are rational numbers. Then so are the coefficients $a + c$, $b + d$, and so on.

b. Both operations are associative and commutative, and multiplication distributes over addition since Ra ($\sqrt{5}$) is a subset of the complex field.

c. $0 = 0 + 0\sqrt{5}$ and $1 = 1 + 0\sqrt{5}$ are in Ra($\sqrt{5}$).

d. If $a + b\sqrt{5}$ is in Ra($\sqrt{5}$) so is $-a - b\sqrt{5}$.

e. Each element $a + b\sqrt{5}$ with not both a and b equal to 0 has a multiplicative inverse in Ra($\sqrt{5}$). For

$$\frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} .$$

If $a^2 - 5b^2 = 0$ either $a^2 = b^2 = 0$, which by hypothesis is impossible, or $b^2 \neq 0$. Then $5 = a^2/b^2$ and $\sqrt{5} = a/b$ which is impossible since that would mean $\sqrt{5}$ is rational. Therefore $a^2 - 5b^2 \neq 0$ and we have

$$\frac{1}{a + b\sqrt{5}} = \frac{a}{a^2 - 5b^2} - \frac{b\sqrt{5}}{a^2 - 5b^2},$$

an element of $Ra(\sqrt{5})$.

Definition 2.2. The number $\bar{\alpha} = a - b\sqrt{5}$ is called the conjugate of $\alpha = a + b\sqrt{5}$. The product $\alpha\bar{\alpha} = a^2 - 5b^2$ is called the norm of α and is denoted $N(\alpha)$.

From this definition the following properties are clearly true.

a. $\bar{\bar{\alpha}} = \alpha$.

b. $\bar{\alpha} = \alpha$ if α is a rational number.

c. $N(\bar{\alpha}) = N(\alpha)$.

Theorem 2.2. α and $\bar{\alpha}$ are the two roots of a unique monic quadratic equation with rational coefficients.

Proof of existence: Let $\alpha = a + b\sqrt{5}$

$$\bar{\alpha} = a - b\sqrt{5}.$$

Then α and $\bar{\alpha}$ satisfy the equation

$$(x - a)^2 - 5b^2 = x^2 - 2ax + a^2 - 5b^2 = 0$$

and the coefficients $2a$ and $a^2 - 5b^2$ are rational since a and b are.

Proof of uniqueness: Case I, $b = 0$. Then $\alpha = a$ and $\bar{\alpha} = a$. The equation must have equal rational roots and so it is of the form

$$(x - r)^2 = 0$$

with r a rational integer. Since a satisfies this equation $(a - r)^2 = 0$, $r = a$ and the equation must be

$$(x - a)^2 = 0$$

so the equation is unique.

Case II, $b \neq 0$.

Lemma. $\alpha = a + b\sqrt{5}$, $b \neq 0$ does not satisfy a rational linear equation of the form

$$x - r = 0 .$$

Suppose the contrary. Then

$$a + b\sqrt{5} = r ,$$

$$\sqrt{5} = \frac{r - a}{b} ,$$

which cannot be since $\sqrt{5}$ is irrational. Hence the lemma.

Suppose α satisfies two monic rational quadratic equations

$$x^2 + p_1x + q_1 = 0 \quad \text{and} \quad x^2 + p_2x + q_2 = 0.$$

Then α satisfies the equation formed by subtracting the second of these from the first;

$$(p_1 - p_2)x + q_1 - q_2 = 0 .$$

This equation must be identically zero, otherwise it contradicts the above lemma. Therefore $p_1 = p_2$ and $q_1 = q_2$ and the two equations are identical.

Definition 2.3. The equation of theorem 2.2 is called the principal equation of α.

Corollary 2.2. The constant term of the principal equation of α is $N(\alpha)$.

Theorem 2.3. The conjugate of the product (sum) of two numbers of $Ra(\sqrt{5})$ is equal to the product (sum) of the conjugates.

Proof: Let $\alpha = a_1 + b_1\sqrt{5}$ and $\beta = a_2 + b_2\sqrt{5}$. Then

$$\overline{\alpha\beta} = a_1a_2 + 5b_1b_2 - (a_1b_2 + a_2b_1)\sqrt{5}$$

$$= a_1a_2 - a_1b_2\sqrt{5} + 5b_1b_2 - a_2b_1\sqrt{5}$$

$$= a_1(a_2 - b_2\sqrt{5}) - b_1\sqrt{5}(a_2 - b_2\sqrt{5})$$

$$= (a_1 - b_1\sqrt{5})(a_2 - b_2\sqrt{5})$$

$$= \overline{\alpha} \cdot \overline{\beta} .$$

And $\overline{\alpha + \beta} = a_1 + a_2 - (b_1 + b_2)\sqrt{5}$

$$= a_1 - b_1\sqrt{5} + a_2 - b_2\sqrt{5}$$

$$= \overline{\alpha} + \overline{\beta} .$$

Theorem 2.4. The norm of the product of two numbers of $Ra(\sqrt{5})$ is equal to the product of their norms.

Proof: Let α and β be two numbers of $Ra(\sqrt{5})$. Then

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta}$$

$$= \alpha\beta \cdot \overline{\alpha}\overline{\beta} \qquad \text{by theorem 2.3}$$

$$= \alpha\overline{\alpha} \cdot \beta\overline{\beta} \qquad \text{by theorem 2.1}$$

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

Corollary 2.4. If α, β are two numbers of $Ra(\sqrt{5})$ and $\beta \neq 0$, then

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)} .$$

By definition 2.2, if $\beta \neq 0$, then $N(\beta) \neq 0$. If

$$N\left(\frac{\alpha}{\beta}\right) \neq \frac{N(\alpha)}{N(\beta)}$$

$N(\alpha)$ and $N(\beta)$ are rational integers by definition 2.2, so

$$N\left(\frac{\alpha}{\beta}\right) \cdot N(\beta) \neq N(\alpha)$$

$$N\left(\frac{\alpha}{\beta} \cdot \beta\right) \neq N(\alpha)$$

$$N(\alpha) \neq N(\alpha).$$

Definition 2.4. A number of $Ra(\sqrt{5})$ is an integer of $Ra(\sqrt{5})$ if its principle equation has rational integral coefficients. The set of integers of $Ra(\sqrt{5})$ will be denoted $Ra[\sqrt{5}]$.

Theorem 2.5. Every rational integer is in $Ra[\sqrt{5}]$. Every number of $Ra[\sqrt{5}]$ which is rational is a rational integer.

Proof: If a is a rational integer, the principal equation of a is

$$x^2 - 2ax + a^2 = 0$$

and its coefficients are rational integers.

If $\alpha = a + b\sqrt{5}$ is rational, $b = 0$ and α in $Ra[\sqrt{5}]$ implies the principal equation

$$x^2 - 2ax + a^2 = 0$$

of α has rational integral coefficients. But if a^2 is a rational integer so is $\alpha = a$.

Theorem 2.6. If α is in $Ra[\sqrt{5}]$, then so is $\bar{\alpha}$.

This is so since both have the same principal equation.

Theorem 2.7. A number of $Ra(\sqrt{5})$ is in $Ra[\sqrt{5}]$ if and only if it is of the form $a + b\sqrt{5}$ where a and b are rational integers, or where both a and b are halves of odd rational integers.

Proof: Let α be a number of $Ra(\sqrt{5})$. Then

$$\alpha = \frac{a_1 + b_1\sqrt{5}}{c_1}$$

where a_1, b_1 and c_1 are rational integers with no common factor and $b_1 \neq 0$ to avoid the previous case where α is rational. Now c_1 may be considered positive without loss of generality. The principal equation of α is

$$x^2 - \frac{2a_1}{c_1}x + \frac{a_1^2 - 5b_1^2}{c_1^2} = 0 .$$

If in addition α is in $Ra[\sqrt{5}]$,

(1) $\qquad \dfrac{2a_1}{c_1}$ is a rational integer;

(2) $$\frac{a_1^2 - 5b_1^2}{c_1^2} \text{ is a rational integer .}$$

Then one of the following is true:

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

If $c_1 \neq 1$ or 2, then by (1) a_1 and c_1 have a common factor and by (2) this factor is also a factor of b_1 contrary to the hypothesis that a_1, b_1 and c_1 are relatively prime.

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

$$a_1^2 - 5b_1^2 \equiv 0 \mod 4,$$

$$a_1^2 \equiv 5b_1^2 \mod 4,$$

If $b_1 \equiv 0 \mod 2$, $b_1^2 \equiv 0 \mod 4$ and $a_1^2 \equiv 0 \mod 4$ by property 1.6c. So $a_1 \equiv 0 \mod 2$, which makes a_1, b_1 and c_1 even in contradiction to hypothesis. If $b_1 \equiv 1 \mod 2$, $b_1^2 \equiv 1 \mod 4$, so $a_1^2 \equiv 1 \mod 4$. Then $a_1 \equiv 1 \mod 2$. Thus, for this case, for $a + b\sqrt{5}$ to be an integer a and b must be halves of odd rational integers.

If $c_1 = 1$, $\alpha = a_1 + b_1\sqrt{5}$ is an integer since $2a_1$ and $a_1^2 - 5b_1^2$ are rational integers for all rational integral values of a_1 and b_1.

Thus it follows that any number $a + b\sqrt{5}$ of $Ra[\sqrt{5}]$ must have a and b rational integers or both a and b halves of rational integers.

Conversely any number of this form is in $Ra[\sqrt{5}]$ for the equation

$$x^2 - 2ax + a^2 - 5b^2 = 0$$

has rational integral coefficients if a and b are rational integers, and if a and b are halves of odd integers $2a$ is a rational integer and

$$a^2 - 5b^2 = \frac{n^2 - 5m^2}{4}$$

where $n \equiv m \equiv 1 \bmod 2$. So $n^2 \equiv m^2 \equiv 5m^2 \equiv 1 \bmod 4$, and $n^2 - 5m^2 \equiv 0 \bmod 4$. Thus $a^2 - 5b^2$ is a rational integer.

Definition 2.5. Two linearly independent numbers θ_1 and θ_2 form a basis for $Ra[\sqrt{5}]$ if every member of $Ra[\sqrt{5}]$ is given in the form $a\theta_1 + b\theta_2$ where a and b range independently over the rational integers.

Theorem 2.8. The numbers 1 and $\theta = \frac{1}{2} + \frac{1}{2}\sqrt{5}$ form a basis for $Ra[\sqrt{5}]$.

Proof: Consider the sets $S_1 = a_1 + b_1\sqrt{5}$ and

$S_2 = a_2 + b_2(\frac{1}{2} + \frac{1}{2}\sqrt{5})$ where a_1 and b_1 are rational integers or halves of odd rational integers and a_2 and b_2 are rational integers. By theorem 2.7, S_1 is $Ra[\sqrt{5}]$.

If a number of S_1 equals a number of S_2, that is

$$a_1 + b_1\sqrt{5} = a_2 + \frac{b_2}{2} + \frac{b_2\sqrt{5}}{2} ,$$

$$2a_1 + 2b_1\sqrt{5} = 2a_2 + b_2 + b_2\sqrt{5} ;$$

$$2a_1 = 2a_2 + b_2 , \qquad \text{(i)}$$

$$b_2 = 2b_1 , \qquad \text{(ii)}$$

$$a_2 = a_1 - b_1 . \qquad \text{(iii)}$$

If a_1 and b_1 are rational integers or halves of odd rational integers, then by (ii) and (iii), a_2 and b_2 are rational integers. So $S_1 \subseteq S_2$.

If a_2 and b_2 are rational integers and b_2 is even, a_1 and b_1 are rational integers by (i) and (ii). If b_2 is odd, $2a_1$ and $2b_1$ are odd rational integers so a_1 and b_1 are halves of odd integers and $S_2 \subseteq S_1$. Therefore $S_1 = S_2$ and $(1, \theta)$ is a basis for $Ra[\sqrt{5}]$.

Theorem 2.9. $Ra[\sqrt{5}]$ is closed under addition, subtraction and multiplication.

Proof: Let $\alpha = a_1 + b_1\theta$, and $\beta = a_2 + b_2\theta$ be two numbers of $Ra[\sqrt{5}]$.

$$\alpha \pm \beta = (a_1 \pm a_2) + (b_1 \pm b_2)\theta.$$

$$\alpha\beta = a_1a_2 + b_1b_2\theta^2 + (a_1b_2 + a_2b_1)\theta.$$

And

$$\theta^2 = (\frac{1}{2}+\frac{1}{2}\sqrt{5})^2 = \frac{3}{2}+\sqrt{\frac{5}{2}} = 1+\frac{1}{2}+\frac{1}{2}\sqrt{5} = \theta + 1.$$

So

$$\alpha\beta = a_1a_2+b_1b_2+(a_1b_2+a_2b_1+b_1b_2)\theta.$$

From theorems 2. 1, 2. 5 and 2. 9 and the fact that we are using complex number multiplication so can have no proper divisors of zero it follows that $Ra[\sqrt{5}]$ is an integral domain.

Theorem 2. 10. If θ_1, θ_2 is a basis of $Ra[\sqrt{5}]$, the necessary and sufficient condition that

$$\theta_1^* = a_{11}\theta_1 + a_{12}\theta_2$$

$$\theta_2^* = a_{21}\theta_1 + a_{22}\theta_2$$

with a_{11}, a_{12}, a_{21} and a_{22} rational integers be a basis also is

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

Proof: If θ_1^*, θ_2^* is a basis,

$$\theta_1 = b_{11}\theta_1^* + b_{12}\theta_2^*$$

$$\theta_2 = b_{21}\theta_1^* + b_{22}\theta_2^*$$

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

$$\theta_1 = (a_{11}b_{11} + a_{21}b_{12})\theta_1 + (a_{12}b_{11} + a_{22}b_{12})\theta_2,$$

$$\theta_2 = (a_{11}b_{21} + a_{21}b_{22})\theta_1 + (a_{12}b_{21} + a_{22}b_{22})\theta_2.$$

So, since θ_1 and θ_2 are linearly independent,

$$a_{11}b_{11} + a_{21}b_{12} = 1 \qquad a_{12}b_{11} + a_{22}b_{12} = 0$$

$$a_{11}b_{21} + a_{21}b_{22} = 0 \qquad a_{12}b_{21} + a_{22}b_{22} = 1 .$$

From these four equations, it follows

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Hence

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

and 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 θ_1^*, θ_2^* to be a basis.

Since θ_1, θ_2 is a basis, if θ_1^* and θ_2^* are in $Ra[\sqrt{5}]$, we have

$$\theta_1^* = a_{11}\theta_1 + a_{12}\theta_2$$

$$\theta_2^* = a_{21}\theta_1 + a_{22}\theta_2$$

where the a_{ij}'s are rational integers. Then

$$\theta_1 = \frac{\begin{vmatrix} \theta_1^* & a_{12} \\ \theta_2^* & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}} \qquad \theta_2 = \frac{\begin{vmatrix} a_{11} & \theta_1^* \\ a_{21} & \theta_2^* \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}} .$$

If

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

both θ_1 and θ_2 and thus all numbers of $Ra[\sqrt{5}]$ can be expressed as linear combinations of θ_1^* and θ_2^* with rational integral coefficients. This establishes the sufficiency condition of the theorem.

Definition 2.6. If θ_1 and θ_2 form a basis for $Ra[\sqrt{5}]$ and α and β are any two numbers of the domain, the discriminant of the numbers α and β is

$$\Delta(\alpha, \beta) = \begin{vmatrix} a_1\theta_1 + b_1\theta_2 & a_2\theta_1 + b_2\theta_2 \\ a_1\overline{\theta}_1 + b_1\overline{\theta}_2 & a_2\overline{\theta}_1 + b_2\overline{\theta}_2 \end{vmatrix}^2$$

Theorem 2.11. $\Delta(\theta_1, \theta_2)$ where θ_1, θ_2 is a basis is invariant under change of basis.

Proof: From definition 2.6

$$\Delta(\alpha, \beta) = \begin{vmatrix} \theta_1 & \theta_2 \\ \overline{\theta}_1 & \overline{\theta}_2 \end{vmatrix}^2 \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}^2$$

and

$$\Delta(\theta_1, \theta_2) = \begin{vmatrix} \theta_1 & \theta_2 \\ \overline{\theta}_1 & \overline{\theta}_2 \end{vmatrix}^2 .$$

By theorem 2.10, if α, β is a basis θ_1^*, θ_2^*, then $a_1b_2 - a_2b_1 = \pm 1$. So

$$\Delta(\theta_1^*, \theta_2^*) = \begin{vmatrix} \theta_1 & \theta_2 \\ \overline{\theta}_1 & \overline{\theta}_2 \end{vmatrix}^2 = \Delta(\theta_1 \theta_2) .$$

Definition 2.7. $\Delta(\theta_1, \theta_2)$ will be called the discriminant of Ra[$\sqrt{5}$] and denoted $\Delta[\sqrt{5}]$.

Theorem 2.12. $\Delta[\sqrt{5}] = 5$.

Proof: Take $(1, \frac{1}{2} + \frac{1}{2}\sqrt{5})$ as a basis. Then

$$\Delta[\sqrt{5}] = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{5} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{5} \end{vmatrix}^2 = (\frac{1}{2} - \frac{1}{2}\sqrt{5} - \frac{1}{2} - \frac{1}{2}\sqrt{5})^2 = (-\sqrt{5})^2 = 5.$$

Theorem 2.13. A necessary and sufficient condition that θ_1, θ_2 be a basis for Ra[$\sqrt{5}$] is that $\Delta(\theta_1, \theta_2) = 5$.

Proof: That this is a necessary condition follows immediately from the last two theorems.

To prove it also sufficient, let α and β be two linearly independent numbers of Ra[$\sqrt{5}$] which do not form a basis. Then

$$\alpha = a_1\theta_1 + a_2\theta_2;$$

$$\beta = b_1\theta_1 + b_2\theta_2$$

where θ_1, θ_2 is a basis and

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \neq \pm 1.$$

Since a_1, a_2, b_1 and b_2 are rational integers and α and β are linearly independent it follows that

$$\left\| \begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix} \right\| > 1 ,$$

$$\left| \begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix} \right|^2 > 1 ,$$

$$\Delta(\alpha, \beta) = \left| \begin{matrix} \theta_1 & \theta_2 \\ \bar{\theta}_1 & \bar{\theta}_2 \end{matrix} \right|^2 \left| \begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix} \right|^2 > 5 \cdot 1 .$$

Example: $a + b\sqrt{5}$, $c + d\sqrt{5}$ is a basis for $Ra[\sqrt{5}]$ if and only if

$$\left| \begin{matrix} a + b\sqrt{5} & c + d\sqrt{5} \\ a - b\sqrt{5} & c - d\sqrt{5} \end{matrix} \right|^2 = [ac-5bd+(bc-ad)\sqrt{5}-ac+5bd-(ad-bc)\sqrt{5}]^2 ,$$

$$= [2(bc-ad)\sqrt{5}]^2 ,$$

$$= 20(bc-ad)^2 = 5$$

or

$$(bc - ad)^2 = \frac{1}{4}$$

The pair a and b must be rational integers or both halves of odd rational integers and likewise for the pair c and d. So any of an infinite number of values will do, in particular the values

$$\frac{5}{2} + \frac{1}{2}\sqrt{5} \qquad \frac{3}{2} + \frac{1}{2}\sqrt{5}.$$

Definition 2. 8. For α, β in Ra[$\sqrt{5}$], α is divisible by β, denoted $\beta | \alpha$, when there exists γ in Ra[$\sqrt{5}$] such that

$$\alpha = \beta\gamma$$

β and γ are called divisors or factors of α, and α is called a multiple of β and γ.

Theorem 2. 14.

a. If α is a multiple of β and β is a multiple of γ, then α is a multiple of γ.

b. If each integer of a sequence $\alpha_1, \alpha_2, \cdots, \alpha_n$ of integers is a multiple of the one that succeeds it, each integer is a multiple of every integer which follows it for any rational integer $n \geq 2$.

c. If two integers α and β, are multiples of a third integer γ, then $\alpha\xi + \beta\eta$ is a multiple of γ where ξ and η are any integers of Ra[$\sqrt{5}$].

Proof:

a. $\beta | \alpha$ and $\gamma | \beta$ implies $\alpha = \xi\beta$ and $\beta = \eta\gamma$ where ξ and η are integers. So $\alpha = \xi\eta\gamma$ and the integers being closed under multiplication, α is a multiple of γ.

b. For $n = 2$ the theorem is obviously true. Assume the theorem is true for sequences with k terms, $k \geq 2$. Let $\alpha_1, \alpha_2, \cdots, \alpha_k, \alpha_{k+1}$ be a sequence where $\alpha_{i+1} | \alpha_i$, $i = 1 \cdots k$. Then

$$\alpha_i = \lambda_i \alpha_k \qquad i = 1 \cdots k-1 \tag{1}$$

by the induction hypothesis. Also by hypothesis

$$\alpha_k = \lambda_k \alpha_{k+1} \tag{2}$$

So from (1) and (2)

$$\alpha_i = \lambda_i (\lambda_k \alpha_{k+1}) \quad \text{for} \quad i = 1 \cdots k-1,$$

$$\text{or} \quad \alpha_i = \mu_i \alpha_{k+1} \quad \text{for} \quad i = 1 \cdots k-1$$

and taking $\mu_k = \lambda_k$ in (2)

$$\alpha_k = \mu_k \alpha_{k+1} .$$

So

$$\alpha_i = \mu_i \alpha_{k+1} \qquad \text{for } i = 1 \cdots k . \tag{3}$$

Also by induction hypothesis, each α_i is a multiple of each α_{i+j} where $i = 1 \cdots k-1$ and $i+j \leq k$ so from this and (3) each α_j is a multiple of α_{i+j} where $i = 1 \cdots k$ and $i+j \leq k+1$.

Since the theorem is true for $n = 2$ and is true for $n = k+1$ whenever it is true for $n = k$, then it is true for all $n \geq 2$.

c. $\alpha = \rho_1 \gamma$, $\beta = \rho_2 \gamma$, ρ_1, ρ_2 integers;

$$\alpha\xi + \beta\eta = \rho_1 \alpha\xi + \rho_2 \alpha\eta ,$$

$$= (\rho_1 \xi + \rho_2 \eta)\gamma$$

and $\alpha\xi + \beta\eta$ is a multiple of γ.

Theorem 2.15. If α is divisible by β, $N(\alpha)$ is divisible by $N(\beta)$.

Proof: $$\alpha = \beta\gamma,$$

$$N(\alpha) = N(\beta)N(\gamma) \quad \text{by theorem 2.4.}$$

and $N(\alpha)$, $N(\beta)N(\gamma)$ being rational integers it follows that $N(\beta) | N(\alpha)$.

Definition 2.9. An integer which divides 1 is called a unit of $Ra[\sqrt{5}]$.

Theorem 2.16. A necessary and sufficient condition that an integer be a unit is that its norm be ± 1.

Proof: If ϵ is a unit it divides 1 so by theorem 2.15, $N(\epsilon)$ divides $N(1) = 1$. Therefore $N(\epsilon) = \pm 1$.

Conversely, if ϵ is an integer and $N(\epsilon) = \pm 1$, then $\epsilon\bar{\epsilon} = 1$ or $\epsilon\bar{\epsilon} = -1$. In the first case ϵ is a unit by definition. In the second case $\epsilon | (-1)$ and $-1 | 1$ so by theorem 2.14a $\epsilon | 1$ and ϵ is a unit.

Corollary 2.16. The product of two units and the quotient of two units are units.

Theorem 2.17. There are an infinite number of units of $Ra[\sqrt{5}]$.

Proof: Consider $\epsilon = \frac{1}{2} + \frac{1}{2}\sqrt{5}$ which is an integer of $Ra[\sqrt{5}]$. $N(\epsilon) = \frac{1}{4} - \frac{5}{4} = -1$ so ϵ is a unit. Every positive power of ϵ is a unit for

$$N(\epsilon^n) = [N(\epsilon)]^n = (-1)^n = +1 \text{ or } -1$$

according as n is even or odd.

Now, $\epsilon, \epsilon^2, \epsilon^3, \cdots$ are all different or for some $n > m$ we have $\epsilon^n = \epsilon^m$. In the latter case $\epsilon^{n-m} = 1$ which is impossible since $\epsilon > 1$. Therefore every positive integral power of ϵ is a unique unit.

Theorem 2.18. A number of $Ra[\sqrt{5}]$ is a unit if and only if it is of the form $\pm\epsilon^n$ where $\epsilon = \frac{1}{2}(1 + \sqrt{5})$ and n is any rational integer.

Proof: Theorem 2.17 establishes the proof that ϵ^n is a unit for $n > 0$. If $n = 0$, $\epsilon^n = 1$, a unit. If $n < 0$, then $\epsilon^n = \frac{1}{\epsilon^m}$ where $m = -n > 0$ and is thus a unit since the quotient of two units is a unit.

To show that all units are of the form $\pm\epsilon^n$, let ϵ_1 be a unit. Then $-\epsilon_1, \bar{\epsilon}_1$ and $-\bar{\epsilon}_1$ are units. If $\epsilon_1 = a+b\sqrt{5}$ where a and b are rational integers or halves of odd rational integers,

$$-\epsilon_1 = -a-b\sqrt{5},$$

$$\bar{\epsilon}_1 = a-b\sqrt{5},$$

$$-\bar{\epsilon}_1 = -a+b\sqrt{5}.$$

One of the above four units has both coefficients positive and so is positive and greater than 1. There will be no lack of generality if we suppose that one to be $a+b\sqrt{5}$ and designate it ϵ_1. The other three units will be $-\epsilon_1$, $\bar{\epsilon}_1$ and $-\bar{\epsilon}_1$ respectively.

Either $\epsilon_1 = \epsilon^n$ or $\epsilon^n < \epsilon_1 < \epsilon^{n+1}$ where n is a non negative rational integer. If the latter case is true, then

$$1 < \frac{\epsilon_1}{\epsilon^n} < \epsilon . \tag{1}$$

Since the quotient of two units is a unit we may write

$$\frac{\epsilon_1}{\epsilon^n} = x + y\sqrt{5}$$

where x and y are rational integers or halves of odd rational integers. Then

$$(x+y\sqrt{5})(x-y\sqrt{5}) = \pm 1 \qquad \text{by theorem 2.16.}$$

Since by (1) $$x + y\sqrt{5} > 1 ,$$

$$|x - y\sqrt{5}| < 1$$

or $$-1 < x - y\sqrt{5} < 1 . \tag{2}$$

From (1) and (2) $0 < 2x < \frac{3}{2} + \frac{\sqrt{5}}{2}$.

To satisfy this, since x is a rational integer or half an odd rational integer, its value must be $\frac{1}{2}$ or 1. But from (1), if $x = \frac{1}{2}$, y must be positive and half an odd rational integer. No such value will satisfy (1). If $x = 1$, y must be positive and a rational integer and again no such value will satisfy (1).

Thus it is impossible that

$$\epsilon^n < \epsilon_1 < \epsilon^{n+1}$$

holds. So

$$\epsilon_1 = \epsilon^n .$$

Then $$-\epsilon_1 = -\epsilon^n .$$

And since $\epsilon_1 \bar{\epsilon}_1 = \pm 1$,

$$\bar{\epsilon} = \pm \frac{1}{\epsilon_1} = \pm \frac{1}{\epsilon^n} = \pm \epsilon^{-n} .$$

Finally

$$-\bar{\epsilon} = -\epsilon^{-n} .$$

Hence the theorem.

Definition 2.10. An integer of $Ra[\sqrt{5}]$ which differs from α by only a unit factor is called an associate of α. If an integer is not a unit nor zero and has no factors except units or its associates, it is called a prime. An integer is composite if it has factors other than units and its associates.

Theorem 2.19. If α and $\beta \neq 0$ are integers of $Ra[\sqrt{5}]$ there exist integers μ and ρ of the domain such that

$$\alpha = \beta\mu + \rho \qquad |N(\rho)| < |N(\beta)| \ .$$

Proof: Let $\frac{\alpha}{\beta} = a + b\theta$ where $\theta = \frac{1}{2}(1+\sqrt{5})$ and $a = r + r_1$, $b = s + s_1$, r and s being rational integers nearest to a and b so that

$$|r_1| \leq \frac{1}{2}, \qquad |s_1| \leq \frac{1}{2} \ .$$

Set $\mu = r + s\theta$, then

$$\frac{\alpha}{\beta} - \mu = r_1 + s_1\theta,$$

$$|N(\frac{\alpha}{\beta} - \mu)| = |r_1^2 + r_1 s_1 - s_1^2| \leq \frac{1}{2} < 1 \ .$$

Then multiplying by $|N(\beta)|$ which is not zero since $\beta \neq 0$

$$|N(\beta)|\,|N(\frac{\alpha}{\beta} - \mu)| = |N(\alpha - \beta\mu| < N(\beta)$$

and setting $\alpha - \beta\mu = \rho$ we have

$$\alpha = \beta\mu + \rho \qquad |N(\rho)| < |N(\beta)|.$$

Definition 2.11. If α, β and δ are integers of $Ra[\sqrt{5}]$ and $\delta | \alpha$, $\delta | \beta$ then δ is a common divisor of α and β. If in addition every common divisor of α and β divides δ, δ is called the greatest common divisor of α and β and denoted (a, β).

Theroem 2.20. If α and β are any two integers of $Ra[\sqrt{5}]$ not both zero there exists a greatest common divisor δ of α and β such that

$$\alpha\mu + \beta\eta = \delta$$

where μ and η are integers. δ is unique up to associates.

Proof: If $\alpha = 0$, $\beta \neq 0$ then $\delta = \beta$. If $\alpha = \beta$, then $\delta = \alpha = \beta$. If $\alpha \neq \beta$ and neither one is zero we may, without loss of generality, assume $|N(\alpha)| > |N(\beta)|$. Then by theorem 2.19 there exists integers ρ and σ such that

$$\alpha = \beta\rho + \sigma, \qquad \text{where} \quad |N(\sigma)| < |N(\beta)|$$

and by continuing the process

$$\beta = \sigma\rho_1 + \sigma_1, \qquad |N(\sigma_1)| < |N(\beta)|,$$

$$\sigma = \sigma_1\rho_2 + \sigma_2, \qquad |N(\sigma_2)| < |N(\sigma_1)|,$$

$$\vdots$$

$$\sigma_{k-3} = \sigma_{k-2}\rho_{k-1} + \sigma_{k-1}, \qquad |N(\sigma_{k-1})| < |N(\sigma_{k-2})|,$$

$$\sigma_{k-2} = \sigma_{k-1}\rho_k + \sigma_k, \qquad |N(\sigma_k)| < |N(\sigma_{k-1})|.$$

$|N(\alpha)|$ is a non negative integer when α is an integer, so in a finite number of steps the process will result in a σ_k such that $|N(\sigma_k)| = 0$. Then $\sigma_k = 0$ and we may eliminate from these equations successively $\sigma_{k-2}, \sigma_{k-3}, \cdots, \sigma$ to obtain

$$\delta = \sigma_{k-1} = \alpha\mu + \beta\eta .$$

If $\sigma_k = 0$, $\sigma_{k-2} = \delta\rho_k$, so δ divides σ_{k-2}, and

$$\begin{aligned} \sigma_{k-3} &= \delta\,\rho_k\rho_{k-1} + \delta , \\ &= \delta(\rho_k\rho_{k-1} + 1), \end{aligned}$$

so δ divides σ_{k-3}. Continuing, we see that the left member of each of the above series of equations is a multiple of δ. Therefore δ is a common divisor of α and β.

Since $\delta = \alpha\mu + \beta\eta$, any common divisor of α and β divides δ, so δ is a greatest common divisor of α and β.

That δ is the only greatest common divisor may be seen by assuming δ_1 is also a greatest common divisor of α and β. Then

$$\delta = \kappa_1\delta_1 \qquad \delta_1 = \kappa_2\delta$$

by definition 2.11, and

$$\delta = \kappa_1\kappa_2\delta .$$

Then $\quad N(\delta) = N(\kappa_1)N(\kappa_2)N(\delta)$ and $N(\delta) \neq 0$ so

$$1 = N(\kappa_1)N(\kappa_2),$$

κ_1 and κ_2 are units and δ and δ_1 are associates.

Example: To find the g.c.d. of $-2 + 2\sqrt{5}$ and $13 - 7\sqrt{5}$, note that

$$|N(-2 + 2\sqrt{5})| = 16, \quad |N(13 - 7\sqrt{5}| = 76$$

and

$$\frac{13 - 7\sqrt{5}}{-2 + 2\sqrt{5}} = \frac{-11 + 3\sqrt{5}}{4} = -3 + \sqrt{5} + \frac{1 - \sqrt{5}}{4}$$

or

$$13 - 7\sqrt{5} = (-2 + 2\sqrt{5})(-3 + \sqrt{5}) + (-3 + \sqrt{5})$$

and

$$|N(-3 + \sqrt{5})| = 4$$

so

$$|N(-3 + \sqrt{5})| < |N(-2 + 2\sqrt{5})|.$$

In the same manner

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

So $-3 + \sqrt{5}$ is the g.c.d.. We may write

$$(1)\ (13 - 7\sqrt{5}) + (3 - \sqrt{5})(-2 + 2\sqrt{5}) = -3 + \sqrt{5}.$$

Definition 2.12. Two integers are said to be relatively prime if every common divisor is a unit.

Corollary 2.20. If α and β are relatively prime, there exist integers μ and η such that

$$\mu a + \eta\beta = 1 .$$

Proof: By definition 2. 12 and theorem 2. 20 there exist integers μ_1 and η_1 such that

$$\mu_1 a + \eta_1 \beta = \epsilon ,$$

ϵ a unit. Then

$$\frac{1}{\epsilon} \mu_1 a + \frac{1}{\epsilon} \eta_1 \beta = \frac{1}{\epsilon} \epsilon$$

and the units being closed under division and the integers closed under multiplication it follows that

$$\mu a + \eta\beta = 1 .$$

Theorem 2. 21. If a prime π of $Ra[\sqrt{5}]$ divides a product $a\beta$ of two integers of the domain, then π divides at least one of the integers.

Proof: Suppose π does not divide a. Then by corollary 2. 20 there exist integers μ and η such that

$$a\mu + \pi\eta = 1 .$$

Multiplying by β we have

$$\beta \alpha\mu + \beta \pi \eta = \beta$$

or since $\pi \mid \alpha\beta$ $\qquad \pi(\lambda \mu + \beta \eta) = \beta$

and $\pi \mid \beta$.

Corollary 2.21. If a prime π divides a product of several integers $\alpha_1\alpha_2 \cdots \alpha_n$, it divides some one of them.

Proof: By theorem 2.21, if $\pi \mid \alpha_1\alpha_2$, then $\pi \mid \alpha_1$ or $\pi \mid \alpha_2$. So the corollary is true for the case $n = 2$. Suppose it is true for $n = k$. Then if π divides the product of $k + 1$ integers we may write without loss of generality

$$\pi \mid (\alpha_1\alpha_2 \cdots \alpha_k)\, \alpha_{k+1}$$

and either $\pi \mid (\alpha_1\alpha_2 \cdots \alpha_k)$ or $\pi \mid \alpha_{k+1}$ or both. If π does not divide α_{k+1}, then by the induction hypothesis it divides some one of the integers $\alpha_1, \alpha_2, \cdots, \alpha_k$. Thus the theorem is true for the product of any n integers, $n \geq 2$.

Theorem 2.22. Every composite number of $Ra[\sqrt{5}]$ can be factored into a finite number of primes, and this factorization is unique up to associates.

Lemma 1. Every composite number of $Ra[\sqrt{5}]$ can be factored into a finite number of primes.

Proof: Let $P(n)$ be the proposition that every integer $\alpha \neq 0$ of $Ra[\sqrt{5}]$ where $|N(\alpha)| = n$ (a natural number) is either a unit or a prime or can be factored into a finite number of primes.

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

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

If α is composite, then $\alpha = \beta\gamma$ where neither β nor γ is a unit nor an associate of α. So $|N(\beta)| \neq 1$, $|N(\gamma)| \neq 1$ and both $|N(\beta)|$ and $|N(\gamma)|$ are less than $|N(\alpha)|$ since $|N(\alpha)| = |N(\beta)|\,|N(\gamma)|$ and the norms are rational integers.

Now suppose that every composite integer κ with $|N(\kappa)| < |N(\alpha)| = n$ has a finite prime decomposition. β and γ would then be

$$\beta = \beta_1\beta_2\cdots\beta_r, \qquad \gamma = \gamma_1\gamma_2\cdots\gamma_s,$$

products of finite numbers of primes and

$$\alpha = \beta_1\beta_2\cdots\beta_r\gamma_1\gamma_2\cdots\gamma_s$$

a product of a finite number of primes. Thus by the second principle of mathematical induction, $P(n)$ is true for all $n \geq 1$.

Lemma 2. The decomposition of a composite integer into primes is unique.

Proof: Suppose there are two prime decompositions of α, say

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

So
$$\pi_1 (\pi_2 \cdots \pi_r) = \lambda_1 \lambda_2 \cdots \lambda_s$$

and by corollary 2.21, π_1 divides some λ_i, say λ_1. Then $\lambda_1 = \epsilon_1 \pi_1$ where ϵ_1 is a unit and

$$\pi_2 \pi_3 \cdots \pi_r = \epsilon_1 \lambda_2 \lambda_3 \cdots \lambda_s .$$

Then π_2 divides some λ_i, say λ_2, and

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

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

$$1 = \epsilon_1 \epsilon_2 \cdots \epsilon_r \lambda_{s-r} \cdots \lambda_s .$$

This implies

$$1 = N(\lambda_{s-r}) \cdots N(\lambda_s)$$

and this is impossible as each λ_i is a prime and hence $N(\lambda_i)$ is a rational integer not equal to ± 1. Similarly the case $r > s$ is impossible. Then $r = s$ and

$$1 = \epsilon_1 \epsilon_2 \cdots \epsilon_s$$

and the prime factorization of a composite integer of $Ra[\sqrt{5}]$ is unique up to associates.

III. THE NUMBERS $Ra(\sqrt{-13})$

Theorem 3.1. The set $Ra(\sqrt{-13}) = a + b\sqrt{-13}$ where a and b range independently over the field of rational numbers is a field.[1]

Theorem 3.2. The numbers α and $\bar{\alpha}$ of $Ra(\sqrt{-13})$ satisfy a unique monic quadratic equation with rational coefficients.

Proof: $\alpha = a + b\sqrt{-13}$ satisfies

$$(x-a)^2 + 13b^2 = x^2 - 2ax + a^2 + 13b^2 = 0$$

as does $\bar{\alpha}$.

Definition 3.1. $N(\alpha) = \alpha\,\bar{\alpha}$.

Theorem 3.3. For every number $\alpha \neq 0$ of $Ra(\sqrt{-13})$, $N(\alpha)$ is a positive rational number.

Proof: Let $\alpha = a + b\sqrt{-13}$ where a and b are rational numbers. Then

$$N(\alpha) = \alpha\,\bar{\alpha} = a^2 + 13b^2$$

---

[1] 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 $Ra(\sqrt{5})$ and will be omitted for sake of brevity. For the same reason, only major theorems and definitions will be restated in this chapter.

which is a rational number since a and b are, and positive since a^2 and b^2 are squares of real numbers not both zero.

Theorem 3.4. $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$ for α, β numbers of $Ra(\sqrt{-13})$.

Theorem 3.5. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Definition 3.2. α is an integer of $Ra(\sqrt{-13})$ if its principal equation has rational integral coefficients. The set of integers will be denoted $Ra[\sqrt{-13}]$.

Theorem 3.6. Every rational integer is in $Ra[\sqrt{-13}]$. Every number of $Ra[\sqrt{-13}]$ which is rational is a rational integer.

Theorem 3.7. If α is in $Ra[\sqrt{-13}]$, so is $\overline{\alpha}$.

Theorem 3.8. A number of $Ra(\sqrt{-13})$ is in $Ra[\sqrt{-13}]$ if and only if it is of the form $a + b\sqrt{-13}$ where a and b are rational integers.

Proof: Let $\alpha = \dfrac{a_1 + b_1\sqrt{-13}}{c_1}$ be a number of $Ra(\sqrt{-13})$ with a_1, b_1 and c_1 relatively prime rational integers and $b_1 \neq 0$. Then the principal equation of α is

$$x^2 - \frac{2a_1}{c_1} x + \frac{a_1^2 + 13b_1^2}{c_1^2} = 0$$

and if α is in $Ra[\sqrt{-13}]$

$$(1) \qquad \frac{2a_1}{c_1},$$

$$(2) \qquad \frac{a_1^2 + 13b_1^2}{c_1^2}$$

are rational integers. One of the following cases must hold.

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

Case (i) may be eliminated by exactly the reasoning which disposed of the similar case of theorem 2.7.

If case (ii) should hold, then $c_1^2 = 4$ and from (2) $a_1^2 + 13b_1^2 \equiv 0 \bmod 4$. Then $a_1^2 \equiv -13b_1^2 \bmod 4$. If $b_1 \equiv 0 \bmod 2$

$$b_1^2 \equiv 0 \bmod 4,$$

$$a_1^2 \equiv 0 \bmod 4,$$

$$a_1 \equiv 0 \bmod 2$$

and we have a_1, b_1 and c_1 all with factor 2 contrary to hypothesis. If $b_1 \equiv 1 \bmod 2$

$$b_1^2 \equiv 1 \bmod 4,$$

$$a_1^2 \equiv 3 \bmod 4$$

which is impossible by principle 1.6e.

Therefore case (iii), $c_1 = 1$ holds and a and b are rational integers.

Conversely, if $\alpha = a + b\sqrt{-13}$, and a and b are rational integers, then $2a$ and $a^2 + 13b^2$ are rational integers and the principal equation of α has rational coefficients.

Theorem 3.9. The numbers 1 and $\sqrt{-13}$ form a basis for $Ra[\sqrt{-13}]$.

This theorem is an immediate consequence of theorem 3.8.

Clearly $Ra[\sqrt{-13}]$ is closed under addition, subtraction and multiplication and this, with theorems 3.1 and 3.6, and the fact that multiplication is complex number multiplication and allows no proper divisors of zero, show that $Ra[\sqrt{-13}]$ is an integral domain.

Theorem 3.10. If θ_1 and θ_2 form a basis of $Ra[\sqrt{-13}]$, the necessary and sufficient condition that

$$\theta_1^* = a_{11}\theta_1 + a_{12}\theta_2$$

$$\theta_2^* = a_{21}\theta_1 + a_{22}\theta_2$$

where the a_{ij}'s are rational integers, is also a basis is

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

Theorem 3.11. The discriminant of a pair of integers θ_1 and θ_2 which form a basis of $Ra[\sqrt{-13}]$

$$\Delta(\theta_1, \theta_2) = \begin{vmatrix} \theta_1 & \theta_2 \\ \overline{\theta}_1 & \overline{\theta}_2 \end{vmatrix}^2$$

is invariant under change of basis.

Theorem 3.12. $\Delta[\sqrt{-13}] = -52$.

Proof: By theorems 3.9 and 3.11,

$$\Delta[\sqrt{-13}] = \Delta(1, \sqrt{-13}) = \begin{vmatrix} 1 & \sqrt{-13} \\ 1 & -\sqrt{-13} \end{vmatrix}^2 = -52$$

Theorem 3.13. A necessary and sufficient condition that θ_1, θ_2 form a basis for $Ra[\sqrt{-13}]$ is that $\Delta(\theta_1, \theta_2) = -52$.

Theorem 3.14. If α and β are members of $Ra[\sqrt{-13}]$ and $\alpha | \beta$ then $N(\alpha) | N(\beta)$.

Definition 3.3. A number of $Ra[\sqrt{-13}]$ is a unit if and only if it divides 1.

Theorem 3.15. α is a unit if and only if $N(\alpha) = 1$.

Theorem 3.16. The product and quotient of two units are units.

Theorem 3. 17. The only units of $Ra[\sqrt{-13}]$ are $+1$ and -1.

Proof: Let $\epsilon = x + y\sqrt{-13}$ be a unit. Then

$$N(\epsilon) = x^2 + 13y^2 = 1$$

and x and y are rational integers so $x = \pm 1$, $y = 0$.

It was at this point in the development of $Ra[\sqrt{5}]$ that theorems leading to the proof of unique factorization were introduced. It can be shown that the analogous theorems are not true in $Ra[\sqrt{-13}]$, but it will suffice to show that there is at least one composite integer in $Ra[\sqrt{-13}]$ which does not have a unique prime factorization.

First let us observe that 2, an integer of the domain, is prime. For if not we would have

$$2 = (x + y\sqrt{-13})\,(u + v\sqrt{-13})$$

with x, y, u and v rational integers, and since $N(\alpha\beta) = N(\alpha)N(\beta)$,

$$4 = (x^2 + 13y^2)\,(u^2 + 13v^2)$$

and either

$$\begin{matrix} x^2 + 13y^2 = 4 & & x^2 + 13y^2 = 2 \\ & \text{or} & \\ u^2 + 13v^2 = 1 & & u^2 + 13v^2 = 2 \end{matrix}$$

But the case on the right is impossible and that on the left has rational integer solutions only if $x = \pm 2$, $y = 0$, $u = \pm 1$, $v = 0$. So 2 is prime.

In the same manner it can be shown that 7, $1+\sqrt{-13}$, and $1-\sqrt{-13}$ are prime.

Now consider

$$14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13}).$$

By theorem 3.17 it is clear that neither factor in the first pair is an associate of a number in the second pair. Thus 14 has two distinct prime factorizations.

IV. THE IDEALS OF Ra[$\sqrt{-13}$]

In Chapter III, it was shown that the unique factorization law does not apply to the composite integers of Ra[$\sqrt{-13}$]. In this chapter the concept of ideal numbers will be introduced, and it will be shown that unique factorization of an ideal into prime ideals exists.

Definition 4.1. An ideal of Ra[$\sqrt{-13}$] is an additive subgroup of integers, which is closed under multiplication by all the integers of the domain.

If $\alpha_1, \alpha_2, \cdots, \alpha_n$ is a set of n integers of Ra[$\sqrt{-13}$], then the set of integers $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n$, where $\lambda_1, \lambda_2, \cdots, \lambda_n$ range independently over the integers of Ra[$\sqrt{-13}$], is clearly an ideal. We denote such an ideal $A = (\alpha_1, \alpha_2, \cdots, \alpha_n)$. An ideal which consists of all multiplicities of a single integer α by integers of the domain is called a principal ideal and denoted (α).

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.

It follows 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 integers of Ra[$\sqrt{-13}$] as coefficients in both cases.

Example: $(2, 3-\sqrt{-13}) = (2, 3-\sqrt{-13}, 1-\sqrt{-13})$. Obviously both numbers in the left hand ideal are expressible as linear combinations of the integers in the ideal on the right. And since $1-\sqrt{-13} = 2 \times -1 + 3-\sqrt{-13}$, it is equally clear that all three integers in the right ideal are linear combinations of those defining the left hand ideal.

Theorem 4.1. If $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is an ideal, any one of the α's may be eliminated from the symbol of the ideal provided it is a linear combination of the remaining integers in the symbol. Likewise an integer may be placed in the symbol for the ideal if it is any number of the ideal.

Proof: Let $\alpha_1 = \mu_2\alpha_2 + \mu_3\alpha_3 + \cdots + \mu_n\alpha_n$, $\mu_2, \mu_3, \cdots, \mu_n$ of $Ra[\sqrt{-13}]$, and α be any number of the ideal. Then

$$\alpha = \lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n$$

where $\lambda_1, \lambda_2, \cdots, \lambda_n$ are integers of $Ra[\sqrt{-13}]$. Then

$$\begin{aligned} \alpha &= \lambda_1(\mu_2\alpha_2 + \cdots + \mu_n\alpha_n) + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n, \\ &= \lambda_1\mu_2\alpha_2 + \cdots + \lambda_1\mu_n\alpha_n + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n, \\ &= (\lambda_1\mu_2 + \lambda_2)\alpha_2 + \cdots + (\lambda_1\mu_n + \lambda_n)\alpha_n . \end{aligned}$$

Since the integers of $Ra[\sqrt{-13}]$ are closed under addition and multiplication, it follows that

$$(\alpha_1, \alpha_2, \cdots, \alpha_n) = (\alpha_2, \cdots, \alpha_n)$$

Similarly, any number of the ideal is a linear combination of the integers in the symbol for the ideal and including it among them will not change the ideal.

Theorem 4.2. In every ideal there exist two integers ω_1, ω_2 such that the numbers of the ideal are given by $k_1\omega_1 + k_2\omega_2$ where k_1 and k_2 are rational integers.

Proof: Every number of an ideal A of $Ra[\sqrt{-13}]$ is of the form $c_1 + c_2\sqrt{-13}$ with c_1 and c_2 rational integers. If α is in A, $-\alpha$ is in A. Let ω_2 be a number of A with $c_2 \neq 0$ in which c_2 is positive and minimal. Then for any number $\alpha = a_1 + a_2\sqrt{-13}$ of A we can write

$$a_2 = k_2c_2 + r_2 \qquad 0 \leq r_2 < c_2 .$$

Then

$$\alpha - k_2\omega_2 = a_1 + a_2\sqrt{-13} - k_2(c_1 + c_2\sqrt{-13}),$$

$$= a_1 + (k_2c_2 + r_2)\sqrt{-13} - k_2(c_1 + c_2\sqrt{-13}),$$

$$= a_1 - k_2c_1 + r_2\sqrt{-13}$$

is in A and $r_2 = 0$ otherwise the definition of ω_2 would be violated. So $\alpha - k_2\omega_2 = b$ is a rational integer.

Since for any α in A, $\alpha\bar{\alpha}$ is in A, A contains positive rational integers. Let ω_1 be one of these which is least. Then

$$b = \omega_1 k_1 + r_1, \qquad 0 \leq r_1 < \omega_1 .$$

So $\alpha - k_2\omega_2 - k_1\omega_1 = b - k_1\omega_1 = r_1$

is in A and $r_1 = 0$ or else ω_1 is not the least positive rational integer in A. Hence

$$\alpha = k_1\omega_1 + k_2\omega_2 .$$

Definition 4.3. A pair of numbers ω_1, ω_2 derived as in theorem 4.2 form a minimal basis for the ideal.

Example 1: To show that $2, 1 + \sqrt{-13}$ is a basis for $(7 - \sqrt{-13}, -10 + 2\sqrt{-13})$ one observes that any number of the ideal is of the form

$$\lambda_1(7 - \sqrt{-13}) + \lambda_2(-10 + 2\sqrt{-13})$$

where λ_1, λ_2 are integers of $Ra[\sqrt{-13}]$, and if $2, 1+\sqrt{-13}$ is to be a basis for the ideal it must be possible to find rational integers k_1 and k_2 which satisfy the equation

$$k_1(2) + k_2(1 + \sqrt{-13}) = (a + b\sqrt{-13})(2) + (c + d\sqrt{-13})(-10 + 2\sqrt{-13})$$

for all rational integral values of a, b, c, and d. Expanding and equating coefficients of powers of $\sqrt{-13}$ one obtains the system

$$\begin{aligned} 2k_1 + k_2 &= 7a + 13b - 10c - 26d \\ k_2 &= -a + 7b + 2c - 10d \end{aligned}$$

and this is equivalent to the system

$$\begin{aligned} k_1 &= 4a + 3b - 6c - 8d \\ k_2 &= -a + 7b + 2c - 10d \end{aligned}$$

which satisfies the requirments.

Example 2: $3, 1+\sqrt{-13}$ is not a basis for $(3, 1+\sqrt{-13})$. If it was there would be a rational integral value for k_1 and k_2 for every rational integer a, b, c, and d in

$$3k_1 + (1+\sqrt{-13})k_2 = (a+b\sqrt{-13})(3) + (c+d\sqrt{-13})(1+\sqrt{-13}).$$

Then
$$\begin{aligned} 3k_1 + k_2 &= 3a + c - 13d \\ k_2 &= 3b + c + d \end{aligned}$$

which is equivalent to

$$\begin{aligned} 3k_1 &= 3a - 3b - 14d \\ k_2 &= 3b + c + d \end{aligned}$$

and it is impossible to find a k_1 which is a rational integer for every rational integral value of $a, b, c,$ and d.

<u>Corollary 4. 2a.</u> Every rational integer of ideal A is divisible by ω_1.

If not there is a rational integer a in A such that

$$a = \omega_1 k + r \qquad 0 < r < \omega_1$$

with k and r rational integers. But then $a - \omega_1 k = r$ would be in A and this contradicts the hypothesis that ω_1 is the smallest positive rational integer in A.

<u>Corollary 4. 2. b.</u> If ω_1, ω_2 is a minimal basis for A, then

$$\lambda_1 \omega_1 + \lambda_2 \omega_2$$

gives a number of A for λ_1 and λ_2 any integers of $Ra[\sqrt{-13}]$.

Let $A' = \{\lambda_1 \omega_1 + \lambda_2 \omega_2, \quad \lambda_1, \lambda_2$ integers of $Ra[\sqrt{-13}]\}$,

$A = \{k_1 \omega_1 + k_2 \omega_2, \quad k_1, k_2$ rational integers$\}$

Then $A \subseteq A'$ since any rational integer is an integer of $Ra[\sqrt{-13}]$ and ω_1 and ω_2 are integers of A, so $\lambda_1 \omega_1$, $\lambda_2 \omega_2$, and $\lambda_1 \omega_1 + \lambda_2 \omega_2$ are integers of A for all λ_1, λ_2 from $Ra[\sqrt{-13}]$. So $A' \subseteq A$. Then $A = A'$.

In exactly the same way as was done for theorem 2. 10, one can prove

Theorem 4.3. A necessary and sufficient condition that any two numbers of A

$$\omega_1^* = a_{11}\omega_1 + a_{12}\omega_2$$

$$\omega_2^* = a_{21}\omega_1 + a_{22}\omega_2$$

with the a_{ij}'s rational integers and ω_1, ω_2 a basis of ideal A, be also a basis of A is

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

Theorem 4.4. Every ideal A has a minimal basis of the form

$$k, p + r\sqrt{-13}$$

where k is the smallest positive rational integer in A and $0 \leq p < k$.

Proof: Let $\omega_1 = k$, $\omega_2 = m + r\sqrt{-13}$ be a basis as determined by theorem 4.2. Then

$$m = qk + p , \qquad 0 \leq p < k ,$$

and $\omega_1^* = \omega_1 = k$, $\omega_2^* = \omega_2 - q\omega_1 = p + r\sqrt{-13}$

are numbers of A and

$$\begin{vmatrix} 1 & 0 \\ -q & 1 \end{vmatrix} = 1 .$$

So by theorem 4. 3, ω_1^*, ω_2^* is a basis of A

Theorem 4. 5. Every ideal A of Ra[$\sqrt{-13}$] has a minimal basis of the form

$$\omega_1^* = ra , \quad \omega_2^* = r(b + \sqrt{-13}) , \qquad 0 \le b < a, \quad b^2 + 13 \equiv 0 \bmod a,$$

where r and a are positive rational integers.

Proof: By theorem 4. 4, A has a basis $k = \omega_1$, $p + r\sqrt{-13} = \omega_2$ with k the smallest positive rational integer in A, and $0 \le p < k$. Set

$$k = ar + t , \qquad 0 \le t < r .$$

Then
$$\begin{aligned} k\sqrt{-13} - a\omega_2 &= k\sqrt{-13} - ap - ar\sqrt{-13}, \\ &= -ap + (k - ar)\sqrt{-13} , \\ &= -ap + t\sqrt{-13} \end{aligned}$$

is in A, which by theorem 4. 2 is impossible unless $t = 0$, in which case $r | k$. Then

$$\omega_1 = ra \qquad \omega_2 = p + r\sqrt{-13}$$

and since $p + r\sqrt{-13}$ is in A, so is $p\sqrt{-13} - 13r$.

Set

$$p = br + t_1, \qquad 0 \leq t_1 < r,$$

b and t_1 rational integers. Then

$$\begin{aligned} -13r + p\sqrt{-13} - b\omega_2 &= -13r + p\sqrt{-13} - bp - br\sqrt{-13}, \\ &= -13r - bp + (p - br)\sqrt{-13}, \\ &= (-13r - pb) + t_1\sqrt{-13} \end{aligned}$$

is in A and $t_1 = 0$ for the same reason $t = 0$ above. Then $r \mid p$ and

$$\omega_1^* = \omega_1 = ra, \quad \omega_2^* = \omega_2 = r(b + \sqrt{-13})$$

is a basis for A. Since r and ω_1 are positive by theorem 4. 2, a is positive and of course a rational integer. Since by theorem 4. 4 $0 \leq p < k$, $0 \leq rb < ra$ and $0 \leq b < a$.

Since $\omega_2\sqrt{-13} - b\omega_2 = r(b + \sqrt{-13})(-b + \sqrt{-13}) = rb^2 - 13r$ is a rational integer in A, it is divisible by $\omega_1 = ra$, according to corollary 4. 2a. So

$$b^2 + 13 \equiv 0 \bmod a.$$

Definition 4. 4. The basis defined in theorem 4. 5 is called a canonical basis.

Example: $2, 1+\sqrt{-13}$ is clearly a canonical basis for the ideal $A = (2, 1 + \sqrt{-13})$ since the coefficient of $\sqrt{-13}$ is one and so surely is the least positive coefficient of $\sqrt{-13}$ in any number $a + b\sqrt{-13}$

of A, and 2 is the least positive rational integer of A. For if not then 1 is in A and so

$$1 = 2(x+y\sqrt{-13}) + (1+\sqrt{-13})(u+v\sqrt{-13})$$

where x, y, u and v are rational integers. So

$$1 = 2x + u - 13v$$

$$0 = 2y + u + \quad v.$$

When the second equation is subtracted from the first

$$1 = 2x - 2y - 14v$$

is obtained, a relation which has no integral solutions since the left number is odd and the right is even.

<u>Definition 4.5.</u> If A and B are ideals, the <u>product</u> 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 integers of $Ra[\sqrt{-13}]$.

If $A = (\omega_1, \omega_2)$, $B = (\psi_1, \psi_2)$, then AB is the set of all numbers given by

$$k_1\omega_1\psi_1 + k_2\omega_1\psi_2 + k_3\omega_2\psi_1 + k_4\omega_2\psi_2$$

where, by corollary 4.2b, k_1, k_2, k_3 and k_4 may be either rational integers or integers of $Ra[\sqrt{-13}]$.

It is evident that the product of ideals is an ideal of the same domain, and that ideal multiplication is both commutative and associative.

Example: $(1+\sqrt{-13},\ 2-\sqrt{-13})\ (2, 3-\sqrt{-13},\ 1-\sqrt{-13}) = (2+2\sqrt{-13},$ $16+2\sqrt{-13},\ 14, 4-2\sqrt{-13},\ -7,\ -5\sqrt{-13},\ -11-3\sqrt{-13})$.

Theorem 4.6. If every number of an ideal A of $Ra[\sqrt{-13}]$ is replaced by its conjugate, the resulting set is an ideal of $Ra[\sqrt{-13}]$.

Proof: If $(a_1, a_2, \cdots, a_n)$ is an ideal, then any number a of the ideal is given by

$$a = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$$

with the λ_j's integers of $Ra[\sqrt{-13}]$ and

$$\overline{a} = \overline{\lambda}_1 \overline{a}_1 + \overline{\lambda}_2 \overline{a}_2 + \cdots + \overline{\lambda}_n \overline{a}_n$$

and since the λ_j's range over $Ra[\sqrt{-13}]$ so do the $\overline{\lambda}_j$'s and

$$(\overline{a}_1, \overline{a}_2, \cdots, \overline{a}_n)$$

is an ideal of $Ra[\sqrt{-13}]$.

Definition 4.6. The ideal defined by theorem 4.6 is called the conjugate ideal. The conjugate of A is denoted $\overline{A}$.

<u>Corollary 4. 6.</u> If ω_1, ω_2 is a basis for A, then $\overline{\omega}_1, \overline{\omega}_2$ is a basis for $\overline{A}$.

Let $\overline{\alpha}$ be any number of $\overline{A}$. Then α is in A and since $A = (\omega_1, \omega_2)$

$$\alpha = k_1\omega_1 + k_2\omega_2$$

for k_1 and k_2 some rational integers. Then

$$\overline{\alpha} = k_1\overline{\omega}_1 + k_2\overline{\omega}_2$$

and $\overline{A} = (\overline{\omega}_1, \overline{\omega}_2)$.

<u>Theorem 4. 7.</u> If A and B are ideals of $Ra[\sqrt{-13}]$, $\overline{AB} = \overline{A} \cdot \overline{B}$.

<u>Proof:</u> Let $A = (\omega_1, \omega_2)$, $B = (\psi_1, \psi_2)$. Then

$$AB = (\omega_1\psi_1, \omega_1\psi_2, \omega_2\psi_1, \omega_2\omega_2)$$

and

$$\overline{AB} = (\overline{\omega_1\psi_1}, \overline{\omega_1\psi_2}, \overline{\omega_2\psi_1}, \overline{\omega_2\psi_2})$$

$$= (\overline{\omega}_1\overline{\psi}_1, \overline{\omega}_1\overline{\psi}_2, \overline{\omega}_2\overline{\psi}_1, \overline{\omega}_2\overline{\psi}_2)$$

$$= (\overline{\omega}_1\overline{\omega}_2)(\overline{\psi}_1\overline{\psi}_2)$$

$$= \overline{A} \cdot \overline{B}.$$

Theorem 4.8. If $A = (ar, r(b + \sqrt{-13}))$ is an ideal of $Ra[\sqrt{-13}]$, then

$$A\bar{A} = (r^2 a) .$$

Proof: Any number of $A\bar{A}$ is given by

$$\kappa a^2 r^2 + \lambda a r^2 (b + \sqrt{-13}) + \mu a r^2 (b - \sqrt{-13}) + \nu r^2 (b^2 + 13)$$

where κ, λ, μ and ν range over $Ra[\sqrt{-13}]$. By theorem 4.5, $b^2 + 13 \equiv 0 \bmod a$. Set $b^2 + 13 = ac$, c a rational integer, and let

$$\kappa = \kappa_1, \quad \lambda = \lambda_1 + \nu_1, \quad \mu = \lambda_1, \quad \nu = \mu_1 .$$

Then the set of numbers $A\bar{A}$ is given by

$$\kappa_1 a^2 r^2 + \lambda_1 a r^2 (b + \sqrt{-13}) + \nu_1 a r^2 (b + \sqrt{-13}) + \lambda_1 a r^2 (b - \sqrt{-13}) + \mu_1 r^2 ac$$

$$= \kappa_1 a^2 r^2 + 2\lambda_1 abr^2 + \mu_1 ar^2 c + \nu_1 ar^2 (b + \sqrt{-13}).$$

Conversely every number in this second set is a number of $A\bar{A}$.

Now $\qquad b^2 \equiv 0$ or $1 \bmod 4$ and $13 \equiv 1 \bmod 4$

so $\qquad b^2 + 13 \equiv 1$ or $2 \bmod 4$

but $\qquad b^2 + 13 = ac$

so it is impossible for both a and c to be even. Let d be the g.c.d. of a, 2b, and c. Then d is odd since a and c are not both even, and $d|b$.

Then $$b^2 + 13 \equiv ac \equiv 0 \mod d^2 .$$

So $$-13 \equiv 0 \mod d^2$$

and $d = 1$, since 13 has no square factors other than 1. Then any number of the set $\kappa_1 r^2 a^2 + \lambda_1 (2r^2 ab) + \mu_1 r^2 ac$ is a multiple of $r^2 a$ by some integer of $Ra[\sqrt{-13}]$.

Since a, 2b and c are relatively prime rational integers, there exist rational integers x, y and z such that

$$xa + 2yb + zc = 1 .$$

Then $$xr^2 a^2 + 2ybr^2 a + zcr^2 a = r^2 a.$$

So every number which is a multiple of $r^2 a$ by an integer of $Ra[\sqrt{-13}]$ is a number in the set $\kappa_1 r^2 a^2 + \lambda_1 2r^2 ab + \mu_1 r^2 ac$ and we have

$$(r^2 a^2, 2r^2 ab, r^2 ac, r^2 a(b + \sqrt{-13})) = (r^2 a, r^2 a (b + \sqrt{-13})) .$$

But every number of the ideal on the right is clearly a number of $(r^2 a)$ and conversely. So $A\bar{A} = (r^2 a)$.

<u>Definition 4.7.</u> The number $r^2 a$ of theorem 4.8 is called the norm of A and written N(A).

Theorem 4.9. The norm of the product of two ideals is equal to the product of their norms.

Proof: $(N(AB)) = AB \cdot \overline{AB} = A\overline{A} \cdot B\overline{B} = (N(A))(N(B))$

Then by definition 4.5 any number of $(N(A))(N(B))$ is a multiple of $N(A)N(B)$. The numbers of $(N(AB))$ are multiples of $N(AB)$. Then it must be that $N(AB)$ and $N(A)N(B)$ divide each other, but since the norms in $Ra[\sqrt{-13}]$ are rational integers it follows that $N(AB) = N(A)N(B)$.

Theorem 4.10. If A, B and S are ideals of $Ra[\sqrt{-13}]$ and

$$SA = SB,$$

then

$$A = B.$$

Proof: Let ω_1, ω_2 be a basis for A. Then any number of A is given by

$$\lambda_1\omega_1 + \lambda_2\omega_2$$

where λ_1, λ_2 are integers of $Ra[\sqrt{-13}]$. Let $N(S) = s$ then the numbers of (s) are given by μs, where μ ranges over $Ra[\sqrt{-13}]$. Any number of $(s)A$ is given by

$$\mu s\lambda_1\omega_1 + \mu s\lambda_2\omega_2 = \eta_1 s\omega_1 + \eta_2 s\omega_2$$

where η_1, η_2 are in $Ra[\sqrt{-13}]$. So every number of $(s)A$ is of the form $s\alpha$ where α is in A. If

$$SA = SB\ ,$$

then
$$\bar{S}SA = \bar{S}SB\ ,$$
$$(s)A = (s)B$$

and for every number α in A there is a number β in B such that

$$s\alpha = s\beta$$

and
$$\alpha = \beta$$

and conversely. Thus every α is in B and every β is in A, so A = B.

Definition 4.8. If A, B, and C are ideals of $Ra[\sqrt{-13}]$ and A = BC, we say that B divides A and C divides A, denoted $B|A$ and $C|A$. C and B are called factors of A.

Theorem 4.11. If A and C are ideals of $Ra[\sqrt{-13}]$, $A|C$ if and only if every number of C is in A.

Proof: If $A|C$, then there exists an ideal B of $Ra[\sqrt{-13}]$ such that

$$AB = C\ .$$

Let $A = (\omega_1, \omega_2)$, $B = (\psi_1, \psi_2)$. Then any number of C is given by

$$\lambda_1\omega_1\psi_1 + \lambda_2\omega_1\psi_2 + \lambda_3\omega_2\psi_1 + \lambda_4\omega_2\psi_2$$

where the λ_j's are in $Ra[\sqrt{-13}]$. But this can be written

$$(\lambda_1\psi_1 + \lambda_2\psi_2)\omega_1 + (\lambda_3\psi_1 + \lambda_4\psi_2)\omega_2$$

or $$(\lambda_1\omega_1 + \lambda_3\omega_2)\psi_1 + (\lambda_2\omega_1 + \lambda_4\omega_2)\psi_2$$

so in the first arrangement every number of C is in A, and in the second arrangement every number of C is also in B.

Now suppose every number of C is in A. Then every number of $C\bar{A}$ is in $A\bar{A} = (a)$ where a is some positive rational integer. Then all numbers of $C\bar{A}$ are given by βa, where β ranges over $Ra[\sqrt{-13}]$. $C\bar{A}$ is an ideal of $Ra[\sqrt{-13}]$, so for every two numbers $\beta_1 a$ and $\beta_2 a$ of $C\bar{A}$ there are numbers $\beta_3 a$, $\beta_4 a$ and $\beta_5 a$ of $C\bar{A}$ such that

$$\beta_1 a + \beta_2 a = \beta_3 a, \quad \beta_1 a - \beta_2 a = \beta_4 a, \quad \lambda\beta_1 a = \beta_5 a$$

for every λ in $Ra[\sqrt{-13}]$. So

$$\beta_1 + \beta_2 = \beta_3, \quad \beta_1 - \beta_2 = \beta_4, \quad \lambda\beta_1 = \beta_5$$

and so the set B of all the β's is an ideal. Then

$$\bar{A}C = (a)B = \bar{A}AB$$

and by theorem 4.10 $$C = AB .$$

Theorem 4.12. A positive rational integer t occurs in only a finite number of ideals of $Ra[\sqrt{-13}]$.

Proof: Let A be an ideal of $Ra[\sqrt{-13}]$ which contains t and let ra, $r(b + \sqrt{-13})$ be a canonical basis of A. Then by corollary 4.2a, $ra|t$ and by theorem 4.5, r and a are positive rational integers and b is positive or zero but less than a. So there are no more than t possibilities for each of a, b and r, thus no more than t^3 ideals which can contain t.

Theorem 4.13. An ideal A of $Ra[\sqrt{-13}]$ is divisible by only a finite number of ideals of $Ra[\sqrt{-13}]$.

Proof: $A\bar{A} = (a)$ where a is a positive number, by theorem 4.8. By theorem 4.11, a is in A and in every ideal which divides A. But by theorem 4.12, there are but a finite number of ideals which contain a. Hence the theorem.

Definition 4.9. An ideal which divides every ideal of the domain is called a unit ideal.

Theorem 4.14. The only unit ideal in $Ra[\sqrt{-13}]$ is (1).

Proof: The ideal (1) is the set of all mutliples of 1 by numbers of $Ra[\sqrt{-13}]$ and thus is the set $Ra[\sqrt{-13}]$. Since any ideal of $Ra[\sqrt{-13}]$ consists of numbers from $Ra[\sqrt{-13}]$ only, every ideal is divisible by (1).

Let A be any ideal of $Ra[\sqrt{-13}]$ which divides all the ideals of the domain. Then $A | (1)$. But then, by theorem 4.11, every number of (1) is in A and $A = (1)$.

Definition 4.10. An ideal, different from the unit ideal, and divisible only by itself and the unit ideal is called a prime ideal. Every ideal not prime is said to be composite.

Example: $(2, 1+\sqrt{-13})$ is a prime ideal. If not there would be ideals $A = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $B = (\beta_1, \beta_2, \cdots, \beta_m)$ such that

$$(2,\ 1+\sqrt{-13}) = AB .$$

But then A and B both divide $(2,\ 1+\sqrt{-13})$ so we may write

$$A = (\alpha_1, \alpha_2, \cdots, \alpha_n,\ 2,\ 1+\sqrt{-13}),$$

$$B = (\beta_1, \beta_2, \cdots, \beta_m,\ 2,\ 1+\sqrt{-13}).$$

Let $\alpha_i = a + b\sqrt{-13}$ be any integers $\alpha_1, \alpha_2, \cdots, \alpha_n$. Then

$$\alpha_i = b(1+\sqrt{-13}) + a - b$$

and $a - b$ is a rational integer so

$$\alpha_i = b(1+\sqrt{-13}) + 2c$$

or $$\alpha_i = b(1+\sqrt{-13}) + 2c + 1 ;$$

in the first case α_i is a linear combination of $2,\ 1+\sqrt{-13}$ and so may be dropped from the symbol for A. In the second case we have

$$\alpha_i - b(1 + \sqrt{-13}) - 2c = 1$$

and 1 may be inserted in the symbol for A, in which case A = (1). Since α_i was arbitrary we find that either $A = (2, 1+\sqrt{-13})$ or A = (1). Similarly for B. So either

$$(2, 1+\sqrt{-13}) = (1)(1) = (1)$$

or
$$= (2, 1 + \sqrt{-13})^2$$

or
$$= (2, 1 + \sqrt{-13})(1)$$

or
$$= (1)(2, 1 + \sqrt{-13}).$$

But $(2, 1 + \sqrt{-13}) \neq (1)$ for it was shown in the example following definition 4. 4, that the integer 1 is not in $(2, 1 + \sqrt{-13})$. Also $(2, 1 + \sqrt{-13}) \neq (2, 1 + \sqrt{-13})^2$ since

$$(2, 1 + \sqrt{-13})^2 = (4, 2 + 2\sqrt{-13}) - 12 + 2\sqrt{-13}) = (2)$$

and $(2, 1 + \sqrt{-13}) \neq (2)$ since $1 + \sqrt{-13}$ is prime. So only the last two equations can be true and $(2, 1 + \sqrt{-13})$ is a prime ideal.

An ideal G is the <u>greatest common divisor</u> of the ideals A and B if $G|A$ and $G|B$ and if every common divisor of A and B divides G.

<u>Theorem 4. 15.</u> Every pair of ideals A and B of $Ra[\sqrt{-13}]$ have a unique greatest common divisor. It is composed of all numbers $\alpha + \beta$ where α ranges over A and β ranges over B

<u>Proof</u>: Consider any two numbers γ_1 and γ_2 of the

set G of numbers of the form $\alpha + \beta$ with α in A and β in B. Let $\gamma_1 = \alpha_1 + \beta_1$ and $\gamma_2 = \alpha_2 + \beta_2$.

Then $\gamma_1 \pm \gamma_2 = (\alpha_1 \pm \alpha_2) + (\beta_1 \pm \beta_2)$. So G is closed under addition and subtraction, and of course 0 is in G. Also for any λ of $Ra[\sqrt{-13}]$ and $\alpha + \beta$ of G

$$\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$$

is in G. So G is an ideal of $Ra[\sqrt{-13}]$.

Every number of A is in G and every number of B is in G, so G is a common divisor of A and B.

Let C be any common divisor of A and B. Then C contains all the numbers α of A and all the numbers β of B. C is closed under addition and so contains all the $(\alpha + \beta)$'s of G. Thus $C|G$ and G is a g.c.d. of A and B.

Suppose G and G' are two g.c.d's of A and B. Then $G = K'G'$ and $G' = KG$ where K and K' are ideals of the domain. So $G = K'KG$. By theorem 4.14, $G = (1)G$ so $(1)G = K'KG$ and, by theorem 4.10, $(1) = K'K$. But then K'(1) and K(1), so $K = K' = (1)$ and $G = G'$.

<u>Definition 4.12.</u> Two ideals are <u>relatively prime</u> if their greatest common divisor is (1).

<u>Example 1:</u> G the g.c.d of $(2, 1 - \sqrt{-13})$ and $(4, 3 + \sqrt{-13})$ is

the set

$$\lambda_1(2) + \lambda_2(1 - \sqrt{-13}) + \lambda_3(4) + \lambda_4(3 + \sqrt{-13})$$

where the λ's range over $Ra[\sqrt{-13}]$. So

$$\begin{aligned} G &= (2, 1-\sqrt{-13}, 4, 3+\sqrt{-13}), \\ &= (2, 1-\sqrt{-13}, 3+\sqrt{-13}), \\ &= (2, 3+\sqrt{-13}) \end{aligned}$$

since $1 - \sqrt{-13} = 2(2) - (3 + \sqrt{-13})$.

Example 2: $(2, 1+\sqrt{-13})$ and $(3, 4+\sqrt{-13})$ are relatively prime since

$$\begin{aligned} G &= (2, 1+\sqrt{-13}, 3, 4+\sqrt{-13}), \\ &= (2, 1+\sqrt{-13}, 3, 4+\sqrt{-13}, 1), \\ &= (1). \end{aligned}$$

Corollary 4.15. If A and B are two ideals of $Ra[\sqrt{-13}]$ which are relatively prime, there is an α in A and a β in B such that

$$\alpha + \beta = 1$$

By theorem 4.15, A and B have a g.c.d composed of all numbers $\alpha + \beta$ where α is in A and β is in B. By definition 4.12 this g.c.d is (1), so 1 is a number of the g.c.d.

Theorem 4.16. If $A \mid BC$, then A divides at least one of B or C.

Proof: Suppose A is prime to B. Then $\alpha + \beta = 1$ for some α in A and some β in B. So for every γ in C

$$\gamma\alpha + \gamma\beta = \gamma .$$

Since $A \mid BC$, the numbers $\gamma\beta$ of BC are in A and of course $\gamma\alpha$ is in A so $\gamma\alpha + \gamma\beta$ is in A. Then γ is in A and $A \mid C$.

Corollary 4.16. If a prime ideal divides a product of ideals, then it divides at least one of the ideals making up the product.

The proof is similar to that of corollary 2.21.

Theorem 4.17. Every composite ideal of $Ra[\sqrt{-13}]$ can be factored into a finite number of prime ideals, and the factorization is unique except for the arrangement of the factors.

Proof: If C is any composite ideal of $Ra[\sqrt{-13}]$, there are ideals A and B of the domain, neither equal to (1), such that

$$C = AB .$$

Either A is prime or it can be decomposed into factors A_1 and A_2. Then each of these is prime or it can be decomposed. The process is finite by theorem 4.13. The factor B can be treated similarly. Thus the ideal C has a finite prime factorization.

The proof that there is a unique factorization into primes rests on corollary 4.16, and is similar to that of theorem 2.22.

Example: In Chapter III it was shown that, in $Ra[\sqrt{-13}]$, the integer 14 factors into two sets of prime integers, $2 \cdot 7$ and $(1+\sqrt{-13})(1-\sqrt{-13})$.

Now consider $(14) = (2)(7) = (1+\sqrt{-13})(1-\sqrt{-13})$. The ideal (2) is not prime for

$$(2) = (2,\ 1+\sqrt{-13})^2.$$

Similarly

$$(7) = (7,\ 1+\sqrt{-13})(7,\ 1-\sqrt{-13}),$$

$$(1+\sqrt{-13}) = (7,\ 1+\sqrt{-13})(2,\ 1+\sqrt{-13}),$$

$$(1-\sqrt{-13}) = (7,\ 1-\sqrt{-13})(2,\ 1+\sqrt{-13}).$$

It was shown in the example after definition 4.10 that $(2, 1+\sqrt{-13})$ is a prime ideal. In the same manner $(7,\ 1+\sqrt{-13})$ and $(7,\ 1-\sqrt{-13})$ can be shown to be primes. So

$$(2)(7) = (2,\ 1+\sqrt{-13})^2\ (7,\ 1+\sqrt{-13})(7,\ 1-\sqrt{-13})$$

and

$$(1+\sqrt{-13})(1-\sqrt{-13}) = (7,\ 1+\sqrt{-13})(2, 1+\sqrt{-13})(7, 1-\sqrt{-13})(2, 1+\sqrt{-13}).$$

Thus (14) has this decomposition into prime ideal factors which by Theorem 4.17 is unique.

V. A NECESSARY AND SUFFICIENT CONDITION FOR UNIQUE FACTORIZATION

It has been shown that the introduction of ideal numbers into the domain $Ra[\sqrt{-13}]$ restored the property of unique prime factorization of the integers of the domain. [1]

In much the same way, the ideals of the domain $Ra[\sqrt{5}]$ may be discussed and theorems analagous to theorems 4.1 through 4.17 derived. In addition we have

Theorem 5.1. Any ideal A of $Ra[\sqrt{5}]$ is principal.

Proof: Let (ω_1, ω_2) be a basis for any ideal of $Ra[\sqrt{5}]$. Then ω_1 and ω_2 are integers of $Ra[\sqrt{5}]$ and, by theorem 2.20, ω_1 and ω_2 have a g.c.d δ and there are integers μ and η of $Ra[\sqrt{5}]$ such that

$$\mu\omega_1 + \eta\omega_2 = \delta.$$

Then

$$(\omega_1, \omega_2) = (\omega_1, \omega_2, \delta) = (\delta)$$

by theorem 4.1. Thus every ideal of $Ra[\sqrt{5}]$ is principal.

That a similar theorem does not hold in $Ra[\sqrt{-13}]$ can be shown by considering the ideal $(2, 1 + \sqrt{-13})$. If this ideal is

---

[1] Actually, it is the principal ideal generated by the integer which has this property.

principal, there must be an integer α of $Ra[\sqrt{-13}]$ such that, for any λ_1, λ_2 of $Ra[\sqrt{-13}]$, there is a ρ of the domain such that

$$\lambda_1(2) + \lambda_2(1 + \sqrt{-13}) = \rho\alpha$$

and in particular a ρ_1 and ρ_2 such that

$$2 = \rho_1\alpha, \qquad 1 + \sqrt{-13} = \rho_2\alpha .$$

Then α divides both 2 and $1 + \sqrt{-13}$. But each of these is prime so their g.c.d δ can only be ± 1 and it must be that $(2, 1 + \sqrt{-13}) = (1)$. This contradicts the fact that it has already been shown in a previous example the ideal $(2, 1 + \sqrt{-13})$ does not contain the integer 1.

The foregoing theorem and example suggest a possible connection between the existence of a unique factorization law and the form of the ideals of an integral domain. It can be shown, in fact, that any quadratic domain $Ra[\sqrt{m}]$ has a unique prime factorization law if and only if every ideal of the domain is principal.

Lemma 1. A necessary and sufficient condition that two numbers α and β of $Ra[\sqrt{m}]$ have a greatest common divisor δ such that

$$\delta = \lambda\alpha + \mu\beta$$

λ, μ in $Ra[\sqrt{m}]$ is that the ideal (α, β) be principal.

Proof: If α and β have a g.c.d. δ, it follows as in theorem 5.1, that $(\alpha, \beta) = (\delta)$ is principal.

Conversely, if $(\alpha, \beta) = (\delta)$, then for any given λ, μ of $Ra[\sqrt{m}]$ there exists a ρ of the domain; and for any ρ of the domain there is a λ and a μ of the domain such that

$$\lambda\alpha + \mu\beta = \rho\delta .$$

Then in particular there exist ρ_1 and ρ_2 such that

$$\alpha = \rho_1\delta, \qquad \beta = \rho_2\delta.$$

So $\delta | \alpha$ and $\delta | \beta$.

Also there is a λ_1 and a μ_1 so that

$$\lambda_1\alpha + \mu_1\beta = \delta.$$

Therefore δ is a g.c.d of α and β.

It can be shown in a manner similar to that used for lemma 1 theorem 2.22 that any integer of any quadratic integral domain has a finite decomposition into prime factors.

Lemma 2. Prime factorization in $Ra[\sqrt{m}]$ is unique, up to associates, if and only if for π, β, γ in $Ra[\sqrt{m}]$, π a prime, $\pi | \beta\gamma$ implies $\pi | \beta$ or $\pi | \gamma$.

Proof: If $\pi | \beta\gamma$ implies $\pi | \beta$ or $\pi | \gamma$ then uniqueness of prime factorization follows as in Chapter II as demonstrated by corollary 2. 21 and theorem 2. 22.

If factorization into primes is unique and $\pi \mid \beta\gamma$, then

$$\beta\gamma = \beta_1\beta_2 \cdots \beta_n\gamma_1\gamma_2 \cdots \gamma_m$$

where the β_j's and γ_j's are primes. Since π is a prime and prime factorization is unique, π is one of the β_j's or one of the γ_j's. So $\pi \mid \beta$ or $\pi \mid \gamma$.

Theorem 5. 2. A necessary and sufficient condition that factorization into primes of integers of $Ra[\sqrt{m}]$ be unique is that every ideal shall be principal.

Proof: Let α, β be any pair of relatively prime integers of $Ra[\sqrt{m}]$ and suppose every ideal of the domain is principal. Then by lemma 1, there exist λ and μ in $Ra[\sqrt{m}]$ such that

$$\lambda\alpha + \mu\beta = 1 .$$

Then $$\gamma\lambda\alpha + \gamma\mu\beta = \gamma$$

for any γ in $Ra[\sqrt{m}]$. If $\alpha \mid \beta\gamma$ then $\alpha \mid \gamma$, and there is unique factorization by lemma 2.

If $Ra[\sqrt{m}]$ has unique factorization:

By lemma 2, if π is a prime and $\pi \mid \beta\gamma$, $\pi \mid \beta$ or $\pi \mid \gamma$.

If π is a prime (π) is a prime ideal, otherwise $(\pi) = AB$ where neither A nor B is (π). Then for any α in A and any β in B $\alpha\beta$ is a multiple of π which means $\pi | \alpha$ or $\pi | \beta$. But if $\pi | \alpha$ every number of A is a multiple of π so $A = (\pi)$. Similarly for B. So one of A or B is π, a contradiction.

Let P be any prime ideal of $Ra[\sqrt{m}]$. Then any number α of P may be written

$$\alpha = \pi_1^{e_1} \pi_2^{e_2} \cdots \pi_n^{e_n}$$

the π's being primes of $Ra[\sqrt{m}]$ and the e's natural numbers. Then

$$(\alpha) = (\pi_1)^{e_1} (\pi_2)^{e_2} \cdots (\pi_n)^{e_n}$$

and each (π_j) is a prime ideal. But every number of (α) is a number of P so $P | (\alpha)$. Then P is one of the (π_j)'s since for ideals there is unique factorization, and P is principal.

Also, any ideal A of $Ra\sqrt{m}$ factors

$$A = P_1 P_2 \cdots P_n$$

the P's being prime ideals and thus principal ideals. Clearly the product of principal ideals is itself a principal ideal, so A is principal.

BIBLIOGRAPHY

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

2. MacDuffee, Cyrus Colton. An introduction to abstract algebra. New York, John Wiley and Sons, 1940. 303 p.

3. Reid, Legh Wilber. The elements of the theory of algebraic numbers. New York, MacMillan, 1910. 454 p.