AN ABSTRACT OF THE THESIS OF

WILLIAM EUGENE MILLER for the MASTER OF SCIENCE
(Name) (Degree)

in MATHEMATICS presented on August 2, 1968
(Major) (Date)

Title: THE QUADRATIC INTEGRAL DOMAINS $Ra[\sqrt{-11}]$ AND $Ra[\sqrt{10}]$

Abstract approved: Redacted for Privacy
William H. Simons

This paper records a study of two quadratic number fields. In the first field, denoted by $Ra[\sqrt{-11}]$, the unique factorization theorem holds. In the second field, denoted by $Ra[\sqrt{10}]$, it is demonstrated that the unique factorization theorem does not hold and therefore ideals are introduced to restore this property.

The Quadratic Integral Domains $Ra[\sqrt{-11}]$ and $Ra[\sqrt{10}]$

by

William Eugene Miller

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

June 1969

APPROVED:

Redacted for Privacy

Professor of Mathematics

in charge of major

Redacted for Privacy

Acting Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented August 2, 1968

Typed by Clover Redfern for William Eugene Miller

TABLE OF CONTENTS

THE QUADRATIC INTEGRAL DOMAINS $Ra[\sqrt{-11}]$ AND $Ra[\sqrt{10}]$

I. THE QUADRATIC INTEGRAL DOMAIN $Ra[\sqrt{-11}]$

Consider a quadratic equation, irreducible over the rational field, of the form $ax^2 + bx + c = 0$, where the coefficients are rational and $a \neq 0$. We can assume that a, b, c are rational integers since this does not alter the roots of the equation. We will consider the case: $b^2 - 4ac = -11d^2$ where d is a rational integer not zero.

Let ρ be one of the irrational roots of the above quadratic equation. Denote by $Ra(\rho)$ the set of numbers $r + s\rho$ where r and s range over the rational field Ra.

Theorem 1.1: There exists a rational integer m without a repeated factor such that $Ra(\rho) = Ra(\sqrt{m})$.

From the above, $b^2 - 4ac = -11d^2$, $d \neq 0$. The roots are $\rho_1 = \frac{-b+\sqrt{-11d^2}}{2a}$, $\rho_2 = \frac{-b-\sqrt{-11d^2}}{2a}$. We will let 1) $\rho = \frac{-b+\sqrt{-11d^2}}{2a}$ as the argument is similar for the other root. Then 2) $\sqrt{-11d^2} = b + 2a\rho$. Equation 1) shows that every number of the form $p + q\rho$ is of the form $k + \ell\sqrt{-11d^2}$. Equation 2) shows that every number of the form $p + q\sqrt{-11d^2}$ is of the form $k + \ell\rho$. Hence $Ra(\rho) = Ra(\sqrt{-11d^2})$. Now $p + q\sqrt{-11d^2} = p + qd\sqrt{-11}$, so $Ra(\rho) = Ra(\sqrt{-11d^2}) = Ra(\sqrt{-11})$, and $m = -11$.

Theorem 1. 2: The set $Ra(\sqrt{-11})$ is a field.

Since $Ra(\sqrt{-11})$ is a subset of the complex number field, both the associative and commutative properties for the operations of addition and multiplication carry over to the elements of $Ra(\sqrt{-11})$. Also the distributive property carries over to the elements of $Ra(\sqrt{-11})$. We observe that: i) the operations of addition and multiplication are closed in $Ra(\sqrt{-11})$ since the sum of two rational numbers is rational and the product of two rational numbers is rational; ii) the additive identity is $0 + 0\sqrt{-11} = 0$, while the multiplicative identity is $1 + 0\sqrt{-11} = 1$; iii) the additive inverse of $p + q\sqrt{-11}$ is $-(p+q\sqrt{-11}) = -p + (-q)\sqrt{-11}$ and the multiplicative inverse of $p + q\sqrt{-11}$, for p and q not both zero, is $(\frac{p}{p^2+11q^2}) + (\frac{-q}{p^2+11q^2}\cdot\sqrt{-11})$, an element of $Ra(\sqrt{-11})$ since the reciprocal of a non zero rational number is rational.

Theorem 1. 3: Every number of $Ra(\sqrt{-11})$ satisfies a quadratic equation with rational coefficients.

Let $\alpha = p + q\sqrt{-11}$ be any number of $Ra(\sqrt{-11})$. Then α satisfies the equation 1) $(x-p)^2 - q^2(-11) = x^2 - 2px + p^2 + 11q^2 = 0$. i. e., substituting α for x we have $(p+q\sqrt{-11}-p)^2 - q^2(-11)$ $= q^2(-11) - q^2(-11) = 0$. Equation 1) is called the principal equation of $\alpha = p + q\sqrt{-11}$. Its constant term $N(p+q(\sqrt{-11})) = p^2 + 11q^2$ is

called the norm of $p + q\sqrt{-11}$ and the negative of the coefficient of x, $T(p+q\sqrt{-11}) = 2p$, is called the trace of $p + q\sqrt{-11}$. The norm and trace of $\alpha = p + q\sqrt{-11}$ are both rational since p and q are rational. Also, it is seen that $N(\alpha) = \alpha\bar{\alpha}$ where $\bar{\alpha}$ is the complex conjugate of α

Integers of $Ra(\sqrt{-11})$: The set of all numbers of $Ra(\sqrt{-11})$ that satisfy equations of the form $x^2 + bx + c = 0$ where b and c are rational integers constitute the integral domain, $Ra[\sqrt{-11}]$, of $Ra(\sqrt{-11})$. Numbers of $Ra[\sqrt{-11}]$ will be called integral numbers of $Ra(\sqrt{-11})$. We need to find such numbers.

Theorem 1.4: Every rational integer is in $Ra[\sqrt{-11}]$. Every number of $Ra[\sqrt{-11}]$ which is rational is a rational integer.

If b is a rational integer, its principal equation is $x^2 - 2bx + b^2 = 0$. Therefore, from the definition, b is a member of $Ra[\sqrt{-11}]$.

If, conversely, $a + b\sqrt{-11}$ is rational, then $b = 0$. The principal equation becomes $x^2 - 2ax + a^2 = 0$. Let $2a = M$, then $a^2 = M^2/4$. Since 2a and a^2 are both rational integers, M must have 2 as a factor, hence $a = M/2$ is a rational integer.

Theorem 1.5: The conjugate of a number of $Ra[\sqrt{-11}]$ is in $Ra[\sqrt{-11}]$.

Let $\alpha = a + b\sqrt{-11}$ be in $Ra[\sqrt{-11}]$. Then the principal equation for α is $x^2 - 2ax + a^2 + 11b^2 = 0$. But the principal equation for $\bar{\alpha} = a - b\sqrt{-11}$ is also $x^2 - 2ax + a^2 + 11b^2 = 0$. Hence $\bar{\alpha} \in Ra[\sqrt{-11}]$.

Theorem 1.6: The numbers of $Ra[\sqrt{-11}]$ are given by $a + b\sqrt{-11}$, where a and b are both integers or both halves of odd integers.

The principal equation for a number $\alpha = a + b\sqrt{-11}$ is $x^2 - 2ax + a^2 + 11b^2 = 0$. If α is in $Ra[\sqrt{-11}]$ then α satisfies an equation of the form $x^2 + px + q = 0$, where p and q are rational integers. Hence $2a = p$ and $a^2 + 11b^2 = q$ are rational integers. There are two cases to consider: either $a = p/2$ is a rational integer or half an odd rational integer.

i) Suppose $a = p/2$ is a rational integer. If b is not a rational integer, then since $11b^2 = q - a^2$ is a rational integer and b is rational, we have the square of the denominator of b divides 11 which is impossible. Therefore, we conclude that b is a rational integer.

ii) Suppose $a = p/2$ is half an odd rational integer. Then $a = (n+1)/2$, where n is a rational integer. We have

$$11b^2 = q - a^2 = q - (4n^2+4n+1)/4$$

$$= (4q-4n^2-4n-1)/4,$$

so

$$4 \cdot 11b^2 = 4q - 4n^2 - 4n - 1.$$

Since the right hand member of this equation is an odd rational integer, it is necessary that b be half an odd rational integer.

Theorem 1.7: The numbers 1 and $\theta = \frac{1}{2} + \frac{1}{2}\sqrt{-11}$ form a basis for $Ra[\sqrt{-11}]$.

Let $(a_1+b_1\sqrt{-11}) \in Ra[\sqrt{-11}]$. We need to show that this number can be put in the form $a_2\ 1 + b_2\theta = a_2 + \frac{b_2}{2} + \frac{b_2}{2}\sqrt{-11}$, where a_2 and b_2 are rational integers. We put $a_1 = a_2 + \frac{b_2}{2}$ so $2a_1 = 2a_2 + b_2$, and $b_1 = \frac{b_2}{2}$ so $2b_1 = b_2$, then $a_2 = a_1 - b_1$. If a_1 and b_1 are rational integers, so are a_2 and b_2. If a_1 and b_1 are halves of odd integers, a_2 and b_2 are integers. Also, if $a_2\ 1 + b_2\ \theta$ is such that a_2 and b_2 are rational integers, $a_2\ 1 + b_2\ \theta$ is in $Ra[\sqrt{-11}]$. Because, if a_2 and b_2 are rational integers and b_2 is even, then a_1 and b_1 are rational integers; if b_2 is odd, a_1 and b_1 are both halves of odd rational integers.

That the numbers are given without repetition follows from the

fact that 1 and $(\frac{1}{2}+\frac{1}{2}\sqrt{-11})$ are linearly independent.

Theorem 1.8: If θ_1, θ_2 is a basis for $Ra[\sqrt{-11}]$, every basis of $Ra[\sqrt{-11}]$ is given by

$$\theta_1' = a_{11}\theta_1 + a_{12}\theta_2$$

$$\theta_2' = a_{21}\theta_1 + a_{22}\theta_2$$

where the a's are rational integers and

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

Conversely, every such pair θ_1', θ_2' constitutes a basis for $Ra[\sqrt{-11}]$.

Let θ_1' and θ_2' be a basis for $Ra[\sqrt{-11}]$. Since θ_1' and θ_2' are in $Ra[\sqrt{-11}]$ and θ_1, θ_2 form a basis,

1) $\theta_1' = a_{11}\theta_1 + a_{12}\theta_2$, $\theta_2' + a_{21}\theta_1 + a_{22}\theta_2$ where the a's are rational integers. Also, since θ_1 and θ_2 are in $Ra[\sqrt{-11}]$ and θ_1', θ_2' form a basis,

2) $\theta_1 = b_{11}\theta_1' + b_{12}\theta_2'$, $\theta_2 = b_{21}\theta_1' + b_{22}\theta_2'$ where the b's are rational integers. Substituting the values of θ_1', θ_2' in 2) we have

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

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

Since θ_1 and θ_2 form a basis they are linearly independent and we can equate coefficients as follows:

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

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

or

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

Hence each determinant of the coefficients is $+1$ or -1.

Now, if θ_1, θ_2 is a basis for $Ra[\sqrt{-11}]$ then define $\theta_1' = a_{11}\theta_1 + a_{12}\theta_2$, $\theta_2' = a_{21}\theta_1 + a_{22}\theta_2$. Clearly every linear combination of θ_1', θ_2' with rational coefficients is in $Ra[\sqrt{-11}]$. Solving these two equations for θ_1 and θ_2 we have

$$\theta_1 = (a_{22}\theta_1' - a_{12}\theta_2') \frac{1}{a_{12}a_{21} - a_{22}a_{11}}$$

$$\theta_2 = (a_{21}\theta_1' - a_{11}\theta_2') \frac{1}{a_{12}a_{21} - a_{22}a_{11}},$$

but by hypothesis

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

Therefore we have shown the existence of rational integral b's such that

$$\theta_1 = b_{11}\theta_1' + b_{12}\theta_2'$$

$$\theta_2 = b_{21}\theta_1' + b_{22}\theta_2'.$$

Thus, since every number of $Ra[\sqrt{-11}]$ can be written as a linear combination of θ_1 and θ_2, it is seen that every number of $Ra[\sqrt{-11}]$ can also be written as a linear combination of θ_1', θ_2' with rational integral coefficients. Hence θ_1', θ_2' constitute a basis for $Ra[\sqrt{-11}]$.

Example: Since $1, \frac{1}{2} + \frac{1}{2}\sqrt{-11}$ form a basis for $Ra[\sqrt{-11}]$ we have $\theta_1' = 3 \cdot 1 + 2\ (\frac{1}{2}+\frac{1}{2}\sqrt{-11}) = 4 + \sqrt{-11}$,
$\theta_2' = 7 \cdot 1 + 5\ (\frac{1}{2}+\frac{1}{2}\sqrt{-11}) = \frac{19}{2} + \frac{5}{2}\sqrt{-11}$ form a basis for $Ra[\sqrt{-11}]$.
Note that

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} 3 & 2 \\ 7 & 5 \end{vmatrix} = 1.$$

In general, all θ_1', θ_2' may be written as

$$\theta_1' = a_{11} + a_{12}(\frac{1}{2}+\frac{1}{2}\sqrt{-11})$$

$$\theta_2' = a_{21} + a_{22}(\frac{1}{2}+\frac{1}{2}\sqrt{-11})$$

where

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

Theorem 1.9: The norm of the product of two numbers in $Ra[\sqrt{-11}]$ is equal to the product of the norms. $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$.

Let $\alpha = p + q\sqrt{-11}$ and $\beta = r + s\sqrt{-11}$ be in $Ra[\sqrt{-11}]$.

$$\begin{aligned} N(\alpha\beta) &= [(p+q\sqrt{-11})(r+s\sqrt{-11})] \\ &= N[(pr-11qs) + (ps+qr)\sqrt{-11}] \\ &= p^2r^2 + 11q^2r^2 + 11p^2s^2 + 121q^2s^2 \\ &= (p^2+11q^2)r^2 + 11s^2(p^2+11q^2) \\ &= (p^2+11q^2)(r^2+11s^2) \\ &= N(\alpha) \cdot N(\beta) \end{aligned}$$

Theorem 1.10: The norm of a quotient is equal to the quotient of the norms. $N(\frac{\alpha}{\beta}) = \frac{N(\alpha)}{N(\beta)}$, $\beta \neq 0$.

Let α, β be as in Theorem 1.9. Then

$$N(\frac{\alpha}{\beta}) = N(\frac{p+q\sqrt{-11}}{r+s\sqrt{-11}})$$

$$= N[\frac{(p+q\sqrt{-11})(r-s\sqrt{-11})}{r^2+11s^2}]$$

$$= N(\frac{pr+11qs}{r^2+11s^2}+\frac{qr-ps}{r^2+11s^2}\cdot\sqrt{-11})$$

$$= \frac{p^2r^2+22pqrs+121q^2s^2+11(q^2r^2-2pqrs+p^2s^2)}{(r^2+11s^2)^2}$$

$$= \frac{p^2r^2+11q^2r^2+11p^2s^2+121q^2s^2}{(r^2+11s^2)^2}$$

$$= \frac{(p^2+11q^2)r^2+11s^2(p^2+11q^2)}{(r^2+11s^2)^2}$$

$$= \frac{(p^2+11q^2)(r^2+11s^2)}{(r^2+11s^2)^2}$$

$$= \frac{p^2+11q^2}{r^2+11s^2}$$

$$= \frac{N(\alpha)}{N(\beta)}$$

Units of $Ra[\sqrt{-11}]$: If α and β are in $Ra[\sqrt{-11}]$ and $\alpha\cdot\beta=\gamma$, then α and β are divisors of γ. α divides γ in $Ra[\sqrt{-11}]$ iff. there exists a β in $Ra[\sqrt{-11}]$ such that $\alpha\cdot\beta=\gamma$.

A number of $Ra[\sqrt{-11}]$ is called a unit of $Ra[\sqrt{-11}]$ if it divides 1.

Theorem 1.11: A number, ϵ, of $Ra[\sqrt{-11}]$ is a unit iff. $N(\epsilon) = 1$. The units of $Ra[\sqrt{-11}]$ are $1, -1$.

If ϵ_1 is a unit, there exists an ϵ_2 such that $\epsilon_1\epsilon_2 = 1$. By Theorem 1.9 we have $N(\epsilon_1\epsilon_2) = N(\epsilon_1)N(\epsilon_2) = 1$. Since $N(\alpha)$ is a positive rational integer for all $\alpha \epsilon Ra[\sqrt{-11}]$, $N(\epsilon_1) = N(\epsilon_2) = 1$.

If $N(\epsilon) = 1$ then we have $N(\epsilon) = a^2 + 11b^2 = 1$, where $\epsilon = a + b\sqrt{-11}$. The only solutions to this equation are $a = \pm 1$, $b = 0$. Hence $\epsilon = \pm 1$.

Prime Numbers of $Ra[\sqrt{-11}]$: A number π is a prime if it is neither 0 nor a unit, and is divisible only by a unit and itself. (i.e., if $\pi = \alpha\beta$ implies that α or β is a unit.) A number that is non-zero, not a unit, and not a prime, is composite.

Example: It can be seen that the number $1 + \sqrt{-11}$ is composite because

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

and neither of the factors, 2, $\frac{1}{2} + \frac{1}{2}\sqrt{-11}$, is a unit.

Example: Assume

$$2 + 3\sqrt{-11} = \alpha\beta$$

where

$$\alpha = p + q\sqrt{-11}, \quad \beta = r + s\sqrt{-11}.$$

Then

$$N(2+3\sqrt{-11}) = N(p+q\sqrt{-11}) \cdot N(r+s\sqrt{-11})$$

$$103 = (p^2+11q^2)(r^2+11s^2).$$

Now, if p, q, r, s are all rational integers then one of α, β is a unit. Otherwise we have the two cases:

i) p, q are rational integers and r, s are both halves of odd rational integers. Let $r = (2m+1)/2$, $s = (2n+1)/2$, m and n are rational integers. Then

$$4 \cdot 103 = (p^2+11q^2)[(2m+1)^2+11(2n+1)^2].$$

Now, we have the following possibilities:

a) $p^2 + 11q^2 = 2 \quad (2m+1)^2 + 11(2n+1)^2 = 206$

b) $p^2 + 11q^2 = 4 \quad (2m+1)^2 + 11(2n+1)^2 = 103$

c) $p^2 + 11q^2 = 103 \quad (2m+1)^2 + 11(2n+1)^2 = 4$

d) $p^2 + 11q^2 = 206 \quad (2m+1)^2 + 11(2n+1)^2 = 2$

a) has no solution because no rational integers exist such that $p^2 + 11q^2 = 2$. b) has no solution because the left hand member of the equation $(2m+1)^2 + 11(2n+1)^2 = 103$ is always an even rational integer. c) and d) have no solutions because $(2m+1)^2 + 11(2n+1)^2 > 11$ for m, n rational integers.

ii) p, q, r, s are all halves of odd rational integers. Let

$$p = \frac{(2m+1)}{2}, \quad q = \frac{(2n+1)}{2}, \quad r = \frac{(2k+1)}{2}, \quad s = \frac{(2j+1)}{2},$$

where m, n, k, j are all rational integers. Then

$$[(2n+1)^2+11(2m+1)^2][(2k+1)^2+11(2j+1)^2] = 103 \cdot 16$$

and we consider the following possibilities:

a) $[(2n+1)^2+11(2m+1)^2] = 103 \quad [(2k+1)^2+11(2j+1)^2] = 16$

b) $[(2n+1)^2+11(2m+1)^2] = 206 \quad [(2k+1)^2+11(2j+1)^2] = 8$

c) $[(2n+1)^2+11(2m+1)^2] = 412 \quad [(2k+1)^2+11(2j+1)^2] = 4$

d) $[(2n+1)^2+11(2m+1)^2] = 824 \quad [(2k+1)^2+11(2j+1)^2] = 2$

e) $[(2n+1)^2+11(2m+1)^2] = 1648 \quad [(2k+1)^2+11(2j+1)^2] = 1$

a) has no solution because the left side of the first equation is always even for n, m rational integers. The other cases have no solutions because in each set of equations, $[(2k+1)^2+11(2j+1)^2] > 11$ for k, j rational integers.

Hence it is concluded that $2 + 3\sqrt{-11}$ can only be written as the product of a unit and itself, therefore $2 + 3\sqrt{-11}$ is prime.

Furthermore it can be proved in a manner similar to the above example, that if $\alpha \in Ra[\sqrt{-11}]$ and $N(\alpha)$ is a prime rational

integer, then α is prime in $Ra[\sqrt{-11}]$. But it can be seen, from the following example, that a prime rational integer is not necessarily a prime of $Ra[\sqrt{-11}]$.

Let $\alpha = 11$, then $\alpha = (\sqrt{-11})(-\sqrt{-11})$ and since neither of these factors is a unit of $Ra[\sqrt{-11}]$ but both factors are in $Ra[\sqrt{-11}]$, therefore 11 is not a prime of $Ra[\sqrt{-11}]$.

Theorem 1.12: If α is any integer of $Ra[\sqrt{-11}]$ and β is any non-zero integer of $Ra[\sqrt{-11}]$, there exists an integer γ, of $Ra[\sqrt{-11}]$ such that $N(\alpha-\gamma\beta) < N(\beta)$.

By Theorem 1.8, $1, -\frac{1}{2}+\frac{1}{2}\sqrt{-11}$ form a basis for $Ra[\sqrt{-11}]$. Let

$$\frac{\alpha}{\beta} = p + q(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{-11})$$

where $p = r + r_1$ and $q = s + s_1$, r and s being the rational integers nearest p and q respectively. Therefore

$$|r_1| \leq \tfrac{1}{2}, \quad |s_1| \leq \tfrac{1}{2}.$$

If

$$\mu = r + s(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{-11})$$

then

$$\frac{\alpha}{\beta} - \mu = r_1 + s_1(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{-11})$$

and

$$N(\frac{\alpha}{\beta}-\mu) = r_1^2 - r_1 s_1 + 3s_1^2.$$

Now if

$$|r_1| < \frac{1}{\sqrt{5}} \quad \text{and} \quad |s_1| < \frac{1}{\sqrt{5}},$$

we have

1) $$r_1^2 - r_1 s_1 + 3s_1^2 < 1.$$

Also, if either $|r_1|$ or $|s_1|$ or both equal $1/2$, then we can choose the signs of r_1 and s_1 so that they are alike and hence

$$r_1^2 - r_1 s_1 + 3s_1^2 < 1.$$

If

$$\frac{1}{\sqrt{5}} < |r_1| < \frac{1}{2}, \quad \frac{1}{\sqrt{5}} < |s_1| < \frac{1}{2}$$

and r_1, s_1 have the same sign equation 1) holds. If r_1 and s_1 have opposite signs, for r_1 we put $r_2 = r_1 + 1$ or $r_2 = r_1 - 1$, depending whether r_1 is negative or positive. Then

$$|r_2| \leq \frac{\sqrt{5}-1}{\sqrt{5}}$$

and r_2 is of the same sign as s_1, in which case

$$r_2^2 - r_2 s_1 + 3s_1^2 < 1.$$

Hence

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

so

$$N(\alpha - \mu\beta) < N(\beta)$$

and

$$\gamma = \mu.$$

Example: Let $\alpha = \frac{3}{2} + \frac{7}{2}\sqrt{-11}$, $\beta = -\frac{5}{2} + \frac{1}{2}\sqrt{-11}$, then

$$\frac{\alpha}{\beta} = \frac{2}{3} - \frac{19}{9}(-\frac{1}{2} + \frac{1}{2}\sqrt{-11})$$

so $r = 1$, $s = -2$ and

$$\mu = 1 - 2(-\frac{1}{2} + \frac{1}{2}\sqrt{-11}) = 2 - \sqrt{-11}.$$

$$N(\alpha - \mu\beta) = N[(\frac{3}{2} + \frac{7}{2}\sqrt{-11}) - (2 - \sqrt{-11})(-\frac{5}{2} + \frac{1}{2}\sqrt{-11})]$$

$$= N(1) = 1 < N(\beta) = 9.$$

Theorem 1.13: If α and β be any two integers of $Ra[\sqrt{-11}]$ prime to each other, there exists two integers, ξ and η, of $Ra[\sqrt{-11}]$ such that $\alpha\xi + \beta\eta = 1$.

If either α or β is a unit, then the existence of the required integers, ξ, η, is evident. i. e. If α is a unit then so is $1/\alpha$ and $\xi = 1/\alpha$, $\eta = 0$.

In case neither α nor β be a unit, assume $N(\beta) \leq N(\alpha)$

which does not limit the generality of the proof.

By Theorem 1.12 there exists an integer μ such that $N(\alpha-\mu\beta) < N(\beta)$. Thus β and $\alpha-\mu\beta$ are a pair of integers, α_1, β_1, prime to each other and $N(\alpha-\mu\beta)$ is less than both $N(\alpha)$ and $N(\beta)$.

If, now, two integers ξ_1, η_1, exist such that

$$\alpha_1\xi_1 = \beta_1\eta_1 = 1$$

that is $\beta\xi_1 + (\alpha-\mu\beta)\eta_1 = 1$, then we have

$$\xi = \eta_1, \quad \eta = \xi_1 - \mu\eta_1$$

The determination of ξ_1, η_1 for α_1, β_1 may, if neither α_1 nor β_1 is a unit, be made to depend similarly upon that of ξ_2, η_2 for a pair of integers α_2, β_2 prime to each other and such that the norm of one of them is less than both $N(\alpha_1)$ and $N(\beta_1)$.

By continuing this process, we are always able to make the determination of ξ and η depend eventually upon that of ξ_n, η_n for a pair of integers α_n, β_n, one of which is a unit.

Since the existence of ξ_n and η_n is evident, the existence of ξ and η is proved.

The following example will serve as a method by which ξ and η may be found.

Example: Let $\alpha = 6 + \sqrt{-11}$, $\beta = \frac{1}{2} + \frac{3}{2}\sqrt{-11}$. α is a prime number of $Ra[\sqrt{-11}]$. Suppose β is divisible by α Then a γ would exist such that $\alpha\gamma = \beta$. This means that $N(\alpha)N(\gamma) = N(\beta)$ or $N(\gamma) = \frac{N(\beta)}{N(\alpha)} = \frac{25}{47}$. But the norm of each number of $Ra[\sqrt{-11}]$ is a rational integer. Therefore β is not divisible by α, so α and β are relatively prime.

$$N(\beta) = 25 < N(\alpha) = 47.$$

By Theorem 1.12 there exists μ such that $N(\alpha - \mu\beta) < N(\beta)$. Using the method previously exampled we find a $\mu = \frac{1}{2} - \frac{1}{2}\sqrt{-11}$. So $\alpha - \mu\beta = -\frac{5}{2} + \frac{1}{2}\sqrt{-11} = \beta_1$, $\beta = \frac{1}{2} + \frac{3}{2}\sqrt{-11} = \alpha_1$. Now neither α_1 nor β_1 be a unit so we use the method of Theorem 1.12 again to find a μ_1 such that $N(\alpha_1 - \mu_1\beta_1) < N(\beta_1) < N(\alpha_1)$. We find a $\mu_1 = \frac{1}{2} - \frac{1}{2}\sqrt{-11} = \mu$. Then $\alpha_1 - \mu_1\beta_1 = -1 = \beta_2$, which is a unit, and $\alpha_2 = \beta_1$.

So

$$0 \cdot \alpha_2 + (-1)\beta_2 = 1$$

$$(-1)(\alpha_1 - \mu_1\beta_1) = 1$$

$$(-1)[\beta - (\mu)(\alpha - \mu\beta)] = 1$$

$$\mu\alpha + (-1 - \mu^2)\beta = 1.$$

Then

$$\xi = \mu = \frac{1}{2} - \frac{1}{2}\sqrt{-11}$$

$$\eta = (-1-\mu^2) = \frac{3}{2} + \frac{1}{2}\sqrt{-11}.$$

Corollary 1.13: If α and β are any two integers of $Ra[\sqrt{-11}]$, there exists a common divisor, δ, of α and β such that every common divisor of α and β divides δ, and there exist two integers, ξ and η, of $Ra[\sqrt{-11}]$ such that $\alpha\xi + \beta\eta = \delta$.

If α and β are relatively prime then $\delta = 1$ because by Theorem 1.13 there exist ξ and η such that $\alpha\xi + \beta\eta = 1$.

If α and β are not relatively prime then let $\alpha = \alpha_1\gamma$ and $\beta = \beta_1\gamma$ where α_1 and β_1 are relatively prime. Then by Theorem 1.13 there exist integers ξ and η such that $\alpha_1\xi + \beta_1\eta = 1$. We multiply both sides of this equation by γ to obtain $\alpha_1\gamma\xi + \beta_1\gamma\eta = \gamma$ or $\alpha\xi + \beta\eta = \gamma$. Every common divisor of α and β divides γ and hence $\delta = \gamma$. The number δ is called the greatest common divisor of α and β.

Theorem 1.14: If the product of two integers, α and β, of $Ra[\sqrt{-11}]$ is divisible by a prime number, π, at least one of the integers is divisible by π.

Let $\alpha\beta = \gamma\pi$, where γ is a number of $Ra[\sqrt{-11}]$, and

assume α is not divisible by π. Then α and π are prime to each other and by Theorem 1.13 there exist two integers, ξ and η, such that $\alpha\xi + \pi\eta = 1$. Multiplying this equation by β, we have

$$\beta\alpha\xi + \beta\pi\eta = \beta,$$

and therefore

$$\pi(\gamma\xi + \beta\eta) = \beta.$$

Since $(\gamma\xi + \beta\eta)$ is in $Ra[\sqrt{-11}]$ we have β is divisible by π.

Corollary 1.14: If the product of any number of integers of $Ra[\sqrt{-11}]$ is divisible by a prime number, π, at least one of the integers is divisible by π.

Suppose the numbers $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n, \pi, \beta$ are in $Ra[\sqrt{-11}]$ and such that $\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \ldots \alpha_n = \pi\beta$. Let $\gamma_1 = \alpha_2 \cdot \alpha_3 \ldots \alpha_n$, then $\alpha_1\gamma_1 = \pi\beta$ and by Theorem 1.14 π divides either α_1 and γ_1. If π divides α_1 the corollary is proved. If π divides γ_1 then let $\gamma_2 = \alpha_3 \cdot \alpha_4 \ldots \alpha_n$ so $\alpha_2 \cdot \gamma_2 = \pi\beta_1$ for some β_1 in $Ra[\sqrt{-11}]$. Hence π divides either α_2 or γ_2. Continuing in this manner if π divides α_k, $k = 1, 2, \ldots, n-2$ the corollary is proved. Otherwise π divides $\gamma_j = \alpha_{j+1}\ \alpha_{j+2} \ldots \alpha_n$, $j = 1, 2, \ldots, n-2$ and the number of factors of γ_j is reduced one at a time until there are only two left. Then by Theorem 1.14 one of these two is divisible by π.

Theorem 1.15: (Unique Factorization Theorem). Every number of $Ra[\sqrt{-11}]$ can be represented in one and only one way as the product of prime numbers.

Let α be in $Ra[\sqrt{-11}]$. If α is not prime, we have $\alpha = \beta\gamma$, where neither of γ, β is a unit. Then $N(\alpha) = N(\beta)N(\gamma)$, and since $N(\beta) \neq 1$, $N(\gamma) \neq 1$, we have $N(\beta) < N(\alpha)$ and $N(\gamma) < N(\alpha)$.

If β is not a prime number then $\beta = \beta_1\gamma_1$, where neither of β_1, γ_1 is a unit and as before $N(\beta_1) < N(\beta)$ and $N(\gamma_1) < N(\beta)$. If β_1 is not a prime, we proceed in the same manner, and, since $N(\beta)$, $N(\beta_1)$, $N(\beta_2)\ldots$ form a decreasing series of positive rational integers, we must after a finite number of such factorizations reach in the series $\beta, \beta_1, \beta_2, \ldots$ a prime π_1. Thus α has a prime factor π_1, and we have $\alpha = \pi_1\alpha_1$.

If α_1 is not a prime number we proceed similarly to obtain $\alpha_1 = \pi_2\alpha_2$, where π_2 is a prime, and hence

$$\alpha = \pi_1\pi_2\alpha_2.$$

Since the series $N(\alpha)$, $N(\alpha_1)$, $N(\alpha_2), \ldots$ form a decreasing series of positive rational integers, if we continue this process we must reach in the series $\alpha, \alpha_1, \alpha_2, \ldots$ a prime number π_n. Thus we have $\alpha = \pi_1\ \pi_2\ \pi_3 \ldots \pi_n$, where the π's are all prime. Hence α can be represented as a product of a finite number of

factors all of which are prime.

Now suppose $\alpha = \rho_1\ \rho_2\ \rho_3 \cdots \rho_m$ is another representation of α as a product of prime factors, then

1) $$\pi_1\ \pi_2\ \pi_3 \cdots \pi_n = \rho_1\ \rho_2\ \rho_3 \cdots \rho_m.$$

By Corollary 1.14, then, at least one of the ρ's, say ρ_1, is divisible by π_1; that is $\rho_1 = \pm 1\ \pi_1$ since ρ_1 is a prime. Dividing 1) by π_1, we have $\pi_2\ \pi_3 \cdots \pi_n = (\pm 1)\rho_2\ \rho_3 \cdots \rho_m$. Again, by Corollary 1.14 at least one of the remaining ρ's, say ρ_2, is divisible by π_2. Thus $\rho_2 = \pm 1\ \pi_2$ and

$$\pi_3\ \pi_4 \cdots \pi_n = (\pm 1)(\pm 1)\rho_3\ \rho_4 \cdots \rho_m = \pm\ \rho_3\ \rho_4 \cdots \rho_m.$$

Proceeding in this manner, we see that with each π there is associated at least one ρ, and, if two or more π's are associated with each other, at least as many ρ's are associated with these π's, and hence with one another.

In the same manner we can show that with each ρ there is associated at least one π, and, if two or more ρ's are associated with one another, at least as many π's are associated with these ρ's, and hence with one another.

Since in all questions of divisiblity we consider two associated factors as the same, (i.e., $a + b\sqrt{-11}$ is considered the same as $-a - b\sqrt{-11}$), the two representations are the same. Hence the representation of a number of $Ra[\sqrt{-11}]$ in prime factors is unique.

II. THE QUADRATIC INTEGRAL DOMAIN $Ra[\sqrt{10}]$

Consider a quadratic equation with rational coefficients, irreducible over the rational field, of the form $ax^2 + bx + c = 0$, $a \neq 0$. We can assume that a, b, c are rational integers since this assumption does not alter the roots of the equation. We will consider the case $b^2 - 4ac = 10d^2$, where d is a rational integer not zero.

Let ρ be one of the roots of the above quadratic. ρ is not a rational number since the equation is irreducible. Denote by $Ra(\rho)$ the set of numbers $r + s\rho$ where r and s range over the rational field Ra.

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

For the above considered case $m = 10$. Since the proof of this theorem is similar to that for $m = -11$, we omit the proof.

When the proof of a theorem of $Ra(\sqrt{10})$ is similar to the proof of the corresponding theorem of $Ra(\sqrt{-11})$, the theorem will be stated without proof.

Example: Let $2x^2 + 8x + 3 = 0$, then $b^2 - 4ac = 10 \cdot 4$ and

$$\rho = \frac{-8+\sqrt{40}}{4} = \frac{-8+2\sqrt{10}}{4} = \frac{-4+\sqrt{10}}{2}.$$

So

$$p + q\rho = p + q(\frac{-4+\sqrt{10}}{2}) = (p-2q)+ \frac{q}{2}\sqrt{10} = r + s\sqrt{10}.$$

Also, since $\rho = -2 + \frac{1}{2}\sqrt{10}$, we have $\sqrt{10} = 2\rho + 4$ and $p + q\sqrt{10} = p + q(2\rho+4) = (p+4) + 2q\rho = r + s\rho$. And it can be seen that numbers of the form $p + q\sqrt{10}$ are of the form $r + s\rho$ and conversely. Hence $Ra(\rho) = Ra(\sqrt{10})$.

Theorem 2. 2: The set $Ra(\sqrt{10})$ is a field.

The proof of this theorem is similar to that of Theorem 1. 2. We will show that each non-zero number of $Ra(\sqrt{10})$ has its reciprocal in $Ra(\sqrt{10})$. Let $(p+q\sqrt{10}) \in Ra(\sqrt{10})$, where not both p, q are zero.

$$\frac{1}{p+q\sqrt{10}} = \frac{p-q\sqrt{10}}{p^2-10q^2} = \frac{p}{p^2-10q^2} + \frac{-q}{p^2-10q^2}\sqrt{10}$$

This is in $Ra(\sqrt{10})$ provided that $p^2 - 10q^2 \neq 0$.

Suppose $p^2 - 10q^2 = 0$. Since $p, q \neq 0$ then $\frac{p^2}{q^2} = 10$ so $\frac{p}{q} = \sqrt{10}$. But both p, q are rational numbers and so is $\frac{p}{q}$, and this implies that $\sqrt{10}$ is rational, a contradiction, therefore the reciprocal of a non-zero number of $Ra(\sqrt{10})$ is in $Ra(\sqrt{10})$.

Theorem 2. 3: Every number of $Ra(\sqrt{10})$ satisfies a quadratic equation with rational coefficients.

Let $\alpha = p + q\sqrt{10}$ be in $Ra(\sqrt{10})$, then α satisfies the equation

$$x^2 - 2px + p^2 - 10q^2.$$

This equation is called the principal equation of α. The constant term $N(p+q\sqrt{10}) = p^2 - 10q^2$ is called the norm of α and it can be seen that $N(\alpha) = \alpha\,\bar{\alpha}$, where $\bar{\alpha} = p - q\sqrt{10}$. The negative of the coefficient of x, $T(p+q\sqrt{10}) = 2a$ is called the trace of $p + q\sqrt{10}$. Since p, q are rational, $N(p+q\sqrt{10})$ and $T(p+q\sqrt{10})$ are also rational.

Integers of $Ra(\sqrt{10})$: The set of all numbers of $Ra(\sqrt{10})$ that satisfy equations of the form $x^2 + bx + c = 0$ where b and c are rational integers constitute the integral domain $Ra[\sqrt{10}]$ of $Ra(\sqrt{10})$.

Theorem 2.4: Every rational integer is in $Ra[\sqrt{10}]$. Every number of $Ra[\sqrt{10}]$ which is rational is a rational integer.

Theorem 2.5: The conjugate of a number of $Ra[\sqrt{10}]$ is in $Ra[\sqrt{10}]$.

Theorem 2.6: The numbers of $Ra[\sqrt{10}]$ are given by $a + b\sqrt{10}$, where a, b range over all rational integers.

The principal equation for a number $\alpha = a + b\sqrt{10}$ is

$$x^2 - 2ax + a^2 - 10b^2 = 0.$$

If $\alpha \in Ra[\sqrt{10}]$ then α satisfies an equation of the form $x^2 + px + q = 0$ where p, q are rational integers. Hence $2a = p$ and $a^2 - 10b^2 = q$ are rational integers. There are two cases to consider: either $a = p/2$ is a rational integer or half an odd rational integer.

Suppose $a = p/2$ is half an odd rational integer. So $a = (2n+1)/2$ where n is a rational integer. From $a^2 - 10b^2 = q$ we have

1) $$4 \cdot 10b^2 = a^2 - q = 4(n^2+n-q) + 1$$

Now, if $2b$ were not a rational integer then the square of its denominator would divide 10 which is impossible. Then the left side of 1) is an even rational integer while the right side of 1) is an odd rational integer, a contradiction. Thus $a = p/2$ must be a rational integer.

We have shown that $a = p/2$ must be a rational integer. From $a^2 - 10b^2 = q$ we have $10b^2 = a^2 - q$ a rational integer. If b were not a rational integer, the square of its denominator would divide 10 which is impossible. Therefore b must be a rational integer.

Moreover it can be seen from the principal equation that if a, b are rational integers then $(a+b\sqrt{10}) \in Ra[\sqrt{10}]$.

Basis for $Ra[\sqrt{10}]$: Every number of $Ra[\sqrt{10}]$ is given without repetition in the form $a \cdot 1 + b\sqrt{10}$ where a and b range independently over all rational integers and every such number is in $Ra[\sqrt{10}]$. We call two such numbers, $1, \sqrt{10}$, a basis for $Ra[\sqrt{10}]$.

Theorem 2.7: If 1 and $\sqrt{10}$ is a basis for $Ra[\sqrt{10}]$, every basis of $Ra[\sqrt{10}]$ is given by $\theta_1' = a_{11} + a_{12}\sqrt{10}$, $\theta_2' = a_{21} + a_{22}\sqrt{10}$ where

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

Theorem 2.8: The norm of a product of two numbers in $Ra[\sqrt{10}]$ is equal to the product of the norms.

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

Theorem 2.9: The norm of a quotient is the quotient of the norms.

$$N(\frac{\alpha}{\beta}) = \frac{N(\alpha)}{N(\beta)} , \quad \beta \neq 0.$$

It was shown in Theorem 2.2 that if $\beta \neq 0$ then $N(\beta) \neq 0$. The rest of the proof of this theorem is similar to the proof of Theorem 1.10.

Units of $Ra[\sqrt{10}]$: If α and β are in $Ra[\sqrt{10}]$ and $\alpha \cdot \beta = \gamma$, then α and β are divisors of γ. α divides γ in $Ra[\sqrt{10}]$ iff. there exists a β in $Ra[\sqrt{10}]$ such that $\alpha \cdot \beta = \gamma$.

A number of $Ra[\sqrt{10}]$ is called a unit of $Ra[\sqrt{10}]$ if it divides 1.

Theorem 2.10: A number ϵ of $Ra[\sqrt{10}]$ is a unit iff. $N(\epsilon) = \pm 1$.

Theorem 2.11: All units of $Ra[\sqrt{10}]$ have the form $\pm (3+\sqrt{10})^n$, where n is a positive or negative rational integer or zero, and all numbers of this form are units of $Ra[\sqrt{10}]$.

Let $\epsilon = 3 + \sqrt{10}$. So $N(\epsilon^n) = [N(\epsilon)]^n = (-1)^n = \pm 1$. Hence ϵ^n is a unit.

Also, since $\epsilon^n \epsilon^{-n} = 1$, ϵ^{-n} is a unit.

Moreover, since $\epsilon = (3+\sqrt{10}) > 1$, the positive powers of ϵ are all greater than 1 and continually increase. Hence no two are equal.

Since $\epsilon^{-n} = \frac{1}{\epsilon^n}$, it is clear that $\epsilon^{-1} < 1$ and hence that the negative powers of ϵ are all less than 1 and continually decrease. Therefore no two negative powers are equal, and no negative power is equal to any positive power. So every power of ϵ is a unit of $Ra[\sqrt{10}]$, and two different powers give different units.

Now we need to show that the powers of ϵ multiplied by ± 1 are all the units of $Ra[\sqrt{10}]$.

Let $a + b\sqrt{10}$ be a unit of $Ra[\sqrt{10}]$. Then $a - b\sqrt{10}$, $-a + b\sqrt{10}$, $-a - b\sqrt{10}$ are also units of $Ra[\sqrt{10}]$. Denote that one of these four units which has $a > 0$ and $b \geq 0$ by η_1, so the remaining three will be $-\eta_1, \eta_1'$ and $-\eta_1'$.

Since $\eta_1 \geq 1$ it follows that either $\eta_1 = \epsilon^n$ or

1) $$\epsilon^n < \eta_1 < \epsilon^{n+1}$$

where n is a positive rational integer or zero. Dividing 1) by ϵ^n, we have

2) $$1 < \frac{\eta_1}{\epsilon^n} < \epsilon ,$$

where η_1/ϵ^n is a unit, since the quotient of two units is a unit.

Let

$$\frac{\eta_1}{\epsilon^n} = x + y\sqrt{10} .$$

Then

$$(x+y\sqrt{10})(x-y\sqrt{10}) = \pm 1,$$

and hence, since $x + y\sqrt{10} > 1$, it follows that

$$|x-y\sqrt{10}| < 1$$

or

$$-1 < x - y\sqrt{10} < 1$$

This combined with 2), gives

$$0 < x < 2 + \frac{1}{2}\sqrt{10}\ ,$$

and since x must be a rational integer,

$$x = 1, 2, \text{ or } 3.$$

If $x = 1$, by 2) $y = 1$, but $1+\sqrt{10}$ is not a unit of $Ra[\sqrt{10}]$. If $x = 2$, then $y = 0$ or 1, but neither $2 + 0\sqrt{10}$ nor $2 + \sqrt{10}$ is a unit. And if $x = 3$, $y = 0$, but $3 + 0\sqrt{10}$ is not a unit.

Hence 1) is impossible, and we have

$$\eta_1 = \epsilon^n$$

and therefore

$$-\eta_1 = -\epsilon^n, \quad \text{and since} \quad \eta_1\eta_1' = \pm 1,$$

$$\eta_1' = \pm\frac{1}{\epsilon^n} = \pm\epsilon^{-n}, \quad \text{and} \quad -\eta_1' = \mp\epsilon^{-n}.$$

Therefore, if η is any one of the four units $\eta_1, -\eta_1, \eta_1', -\eta_1'$, we have $\eta = \pm\epsilon^n$ where n is a rational integer.

Prime numbers of $Ra[\sqrt{10}]$: A number π of $Ra[\sqrt{10}]$ is prime if it is neither 0 nor a unit, and is divisible only by a unit and itself.

Example 1: To determine whether $5 - 2\sqrt{10}$ is prime or composite. Put

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

then

$$-15 = (a^2-10b^2)(c^2-10d^2)$$

There are only four distinct cases to be considered:

i) $a^2 - 10b^2 = 3$, $c^2 - 10d^2 = -5$ ii) $a^2 - 10b^2 = -3$, $a^2 - 10b^2 = 5$ iii) and iv) $a^2 - 10b^2 = \pm 1$, $c^2 - 10d^2 = \mp 15$.

Both iii) and iv) have $a + b\sqrt{10}$ a unit and therfore need not be considered. From i) we have

$$b^2 = \frac{a^2-3}{10}$$

and this makes it necessary that $a^2 \equiv 3 \mod 10$. But no such rational integer exists. Hence i) has no solutions.

From ii) we have

$$b^2 = \frac{a^2+3}{10}$$

and it is necessary that $a^2 \equiv 7 \mod 10$. But no such rational integer exists. Hence ii) has no solutions. Therefore $5 - 2\sqrt{10}$ is prime.

Example 2: It can be seen that the number 26 is not prime since $26 = 13 \cdot 2$. Also $26 = (6+\sqrt{10})(6-\sqrt{10})$ and neither of these factors is a unit. It remains to be seen whether they are prime factors.

Assume $(6+\sqrt{10}) = (a+b\sqrt{10})(c+d\sqrt{10})$, where neither factor is a unit, then $26 = (a^2-10b^2)(c^2-10d^2)$.

There are two cases to consider:

$$\text{i)} \quad \begin{aligned} a^2 - 10b^2 &= 13 \\ c^2 - 10d^2 &= 2 \end{aligned} \qquad \text{ii)} \quad \begin{aligned} a^2 - 10b^2 &= -13 \\ c^2 - 10d^2 &= -2 \end{aligned}$$

Since $b^2 = \frac{a^2 \pm 13}{10}$ requires that $a^2 \equiv 3$ or $7 \mod 10$ and no such rational integer, a, exists, we conclude that $(6+\sqrt{10})$ and $(6-\sqrt{10})$ are prime factors.

Therefore it is clear that

$$26 = 13 \cdot 2 = (6+\sqrt{10})(6-\sqrt{10})$$

cannot be factored uniquely into prime factors.

The introduction of so-called ideal numbers restore this property of unique factorization in terms of these ideal numbers.

If every pair of numbers of $Ra[\sqrt{10}]$, not both zero, had a greatest common divisor (g. c. d.) expressed linearly in terms of the numbers we could prove unique factorization. (See Theorems 1. 12 through 1. 15.)

Example: Consider the positive rational integers congruent to 1 modulo 4. This set is closed under multiplication. A number of this set is considered prime if it cannot be written as the product of two numbers $\equiv$ 1 mod. 4, where neither of the two numbers be a unit. Then

$$2541 = 33 \cdot 77 = 121 \cdot 21$$

where 33, 77, 121, 21 are all primes.

The cause of the failure of the unique factorization law is because of the absence of the remaining positive integers. Let (a, b) denote the g. c. d. of a and b so

$$11 = (33, 121) = (77, 121), \quad 7 = (77, 21), \quad 3 = (33, 21).$$

Then $2541 = (33, 121)(77, 121)(77, 21)(33, 21)$ is uniquely factored into prime "ideal" numbers.

Ideals of $Ra[\sqrt{10}]$: If $a_1, a_2, \ldots, a_n$ are any numbers of $Ra[\sqrt{10}]$ not all zero, then the set

$$\{\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n \mid \lambda_1, \lambda_2, \ldots, \lambda_n \text{ range over } Ra[\sqrt{10}]\}$$

constitutes an ideal A of $Ra[\sqrt{10}]$. We will denote A by $A = (a_1, a_2, \ldots, a_n)$.

Theorem 2.12: In every ideal there exists two numbers 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, k_2 range over the rational integers.

Two such numbers are called a minimal basis for the ideal.

Let $1, \sqrt{10}$ be a basis for $Ra[\sqrt{10}]$. If $\alpha \neq 0$ is a number of the ideal A, then A contains $\pm\alpha\bar{\alpha} = \pm N(\alpha)$, and so A contains positive integers. Let ω_1 be the smallest positive integer in A. Of all numbers $\ell_1 + \ell_2\sqrt{10}$ in A having $\ell_1 \neq 0$, choose as ω_2 one such in which ℓ_2 is positive and minimal. Let $\alpha = a_1 + a_2\sqrt{10}$ be any number of A. Write

$$a_2 = \ell_2 k_2 + r_2 \qquad 0 \leq r_2 < \ell_2.$$

Then

$$\alpha - k_2\omega_2 = (a_1 - k_2\ell_1) + r_2\sqrt{10}$$

is in A, and if r_2 were not zero, the definition of ω_2 would be violated. Thus $\alpha - k_2\omega_2 = a_1 - k_2\ell_2 = b$. Now write

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

so that $\alpha - k_2\omega_2 - k_1\omega_1 = r_1$. Since ω_1 was minimal, $r_1 = 0$, and

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

Corollary 2.12: Every rational integer in A is divisible by ω_1.

Because if α is a rational integer then we can let $k_2 = 0$, so $\alpha = k_1\omega_1$.

Theorem 2.13: If ω_1, ω_2 is a minimal basis for an ideal A in $Ra[\sqrt{10}]$, every minimal basis is given by

$$\omega_1' = a_{11}\omega_1 + a_{12}\omega_2, \quad \omega_2' = a_{21}\omega_1 + a_{22}\omega_2,$$

where the a's are rational integers such that

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

and every such pair ω_1', ω_2' is a minimal basis.

The proof is similar to that of Theorem 1.8.

Theorem 2.14: Every ideal A has a minimal basis $k, \ell + r\sqrt{10}$, where k is the smallest positive integer in A and $0 \leq \ell < k$.

In the proof of Theorem 2.12 we saw that we could choose a basis $\omega_1 = k$, $\omega_2 = m + r\sqrt{10}$, where k was the smallest positive integer in A. Set

$$m = qk + \ell, \quad 0 \leq \ell < k .$$

In the transformation $\omega_1' = \omega_1 = k$, $\omega_2' = \omega_2 - q\omega_1 = \ell + r\sqrt{10}$ we have the determinant of coefficients

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

so the result follows from Theorem 2.13.

Theorem 2.15: Every ideal A has a minimal basis of the form

$$\omega_1 = ra, \quad \omega_2 = r(b+\sqrt{10}),$$

where r and a are positive integers, and $0 \leq b < a$. Moreover,

$$b^2 - 10 \equiv 0 \text{ modulo } a.$$

Such a basis is called a canonical basis.

Using the notation of Theorem 2.14, since k is in A, $k\sqrt{10}$ is in A. Set

$$k = ar + t, \quad 0 \leq t < r.$$

Then $k\sqrt{10} - a\omega_2' = -a\ell + t\sqrt{10}$ is in A. This is impossible unless $t = 0$, in which case r divides k. Hence

$$\omega_1 = ra, \quad \omega_2 = \ell + r\sqrt{10}\ .$$

Since $\ell + r\sqrt{10}$ is in A, so is $\ell\sqrt{10} + 10r$. Set

$$\ell = br + t_1 \qquad 0 \leq t_1 < r.$$

Then $10r + \ell\sqrt{10} - b\omega_2 = 10r - b\ell + t_1\sqrt{10}$ is in A, so $t_1 = 0$ and r divides ℓ. Hence there is a basis

$$\omega_1 = ra, \quad \omega_2 = r(b+\sqrt{10}),$$

where r and a are positive. Since, by Theorem 2.14, $0 \leq rb < ra$, we have $0 \leq b < a$.

Since $\omega_2\sqrt{10} - b\omega_2 = 10r - rb^2$ is a rational integer in A, it is divisible by ra by Corollary 2.12.

$$\text{i.e.} \quad b^2 - 10 \equiv 0 \text{ modulo } a.$$

The product AB of two ideals A and B is defined to be the set of all numbers obtained by multiplying every number of A by every number of B, and then adding and subracting these numbers until no new numbers are obtained. This set of numbers satisfies the definition of ideal.

If $A = (\omega_1, \omega_2)$, and $B = (\chi_1, \chi_2)$, then AB consists of the

numbers

$$k_1\omega_1\chi_1 + k_2\omega_1\chi_2 + k_3\omega_2\chi_1 + k_4\omega_2\chi_2 ,$$

where k_1, k_2, k_3, k_4 range over all numbers of $Ra[\sqrt{10}]$.

It is evident that ideal multiplication is associative and commutative.

If all the numbers of an ideal A are multiples by numbers of $Ra[\sqrt{10}]$ of one number a, the ideal A is called principal and is written (a).

The conjugate of A, denoted by $\overline{A}$, is an ideal formed by replacing every number of A by its conjugate.

Theorem 2.16: $\overline{AB} = \overline{A}\,\overline{B}$.

Let $A = (\omega_1, \omega_2)$, $B = (\chi_1, \chi_2)$, then

$$\begin{aligned} AB &= (\overline{\omega_1\chi_1}, \overline{\omega_1\chi_2}, \overline{\omega_2\chi_1}, \overline{\omega_2\chi_2}) \\ &= (\overline{\omega}_1\overline{\chi}_1, \overline{\omega}_1\overline{\chi}_2, \overline{\omega}_2\overline{\chi}_1, \overline{\omega}_2\overline{\chi}_2) \\ &= \overline{A}\,\overline{B} \end{aligned}$$

Theorem 2.17: If $A = (ra, r(b+\sqrt{10}))$, then $A\overline{A} = (r^2a)$.

The number r^2a is called the norm of A, written $N(A)$.

$$\overline{A} = (ra, r(b-\sqrt{10}))$$

so

$$A\,\bar{A} = (r^2a^2,\ r^2a(b-\sqrt{10}),\ r^2a(b+\sqrt{10}),\ r^2(b^2-10)).$$

Then $A\,\bar{A}$ consists of all numbers

1) $$kr^2a^2 + \lambda r^2a(b+\sqrt{10}) + \mu r^2a(b-\sqrt{10}) + \nu r^2(b^2-10)),$$

where k, λ, μ, ν range over all numbers of $Ra[\sqrt{10}]$. By Theorem 2.15

$$c = \frac{b^2-10}{a}$$

is an integer. The transformation

$$k = k_1, \quad \lambda = \lambda_1 + \nu_1, \quad \mu = \lambda_1, \quad \nu = \mu_1$$

takes the set of numbers 1) into the set

2) $$k_1r^2a^2 + \lambda_1 2r^2ab + \mu_1 r^2ac + \nu_1 r^2a(b+\sqrt{10}) .$$

Hence every number of 1) is in 2). The converse is true, since

$$k_1 = k, \quad \lambda_1 = \mu, \quad \mu_1 = \nu, \quad \nu_1 = \lambda - \mu.$$

Suppose that a and c were both even. Then $b^2 - 10 = ac \equiv 0 \bmod 4$. But $b^2 \equiv 0$ or $1 \bmod 4$ according as b is even or odd, and neither of these agrees with the fact that

$10 \equiv 2 \bmod 4$. Hence a and c are not both even.

Let $g = (a, 2b, c)$. Since a and c are not both even, g is odd and so g divides b. Then

$$b^2 - 10 = ac \equiv 0 \bmod g^2$$

implies $10 \equiv 0 \bmod g^2$. Since 10 has no square factor > 1, $g = 1$.

We can now see that the set of numbers

3) $$\{k_1 r^2 a^2 + \lambda_1 2r^2 ab + \mu_1 r^2 ac\}$$

is the same as the set $\{\rho r^2 a \mid \rho$ ranges over $Ra[\sqrt{10}]\}$. Clearly, every number of 3) is in $\{\rho r^2 a\}$. Since a, 2b, c are relatively prime, there exist rational integers p, q, t such that

$$1 = pa + 2qb + tc.$$

Multiply through by $r^2 a$. Then

$$r^2 a = pr^2 a^2 + 2qr^2 ab + tr^2 ac$$

so that every number of $\{\rho r^2 a\}$ is in 3).

The set 2) is now seen to be equal to the set

4) $$\{\rho r^2 a + \nu_1 r^2 a(b+\sqrt{10})\}$$

Obviously every number of 4) is a multiple of r^2a, and, conversely, every multiple of r^2a is in the set; i. e. $\nu_1 = 0$. Thus $A\,\overline{A} = (r^2a)$.

Theorem 2. 18: $N(AB) = N(A)N(B)$, where A and B are ideals.

By Theorem 2. 16 $N(AB) = AB\ \overline{AB}$

$= AB\ \overline{A}\ \overline{B}$

$= A\,\overline{A}\ B\,\overline{B}$

$= N(A)\ N(B)$

Theorem 2. 19: If $SA = SB$, where S, A, and B are ideals, then $A = B$.

The numbers of A are given by

$$k_1\omega_1 + k_2\omega_2,$$

where ω_1, ω_2 form a basis for A, and k_1, k_2 are in $Ra[\sqrt{10}]$. Let $s = N(S)$. The numbers of (s) are given by λs, where $\lambda \in Ra[\sqrt{10}]$. Thus the numbers of (s)A consist of the numbers

$$\lambda k_1 s\omega_1 + \lambda k_2 s\omega_2 = \eta_1 s\omega_1 + \eta_2 s\omega_2 = s(\eta_1\omega_1 + \eta_2\omega_2)$$

where η_1, η_2 range over $Ra[\sqrt{10}]$. Thus every number of (s)A

is of the form $s\alpha$ where α is in A.

If $SA = SB$, then $\bar{S}SA = \bar{S}SB$, or

$$(s)A = (s)B,$$

where s is a rational integer. That is, for every number α in A there is a number β in B such that

$$s\alpha = s\beta, \qquad \alpha = \beta,$$

and conversely. Hence every α is in B and every β is in A, so that $A = B$.

Divisors of Ideals: If three ideals of $Ra[\sqrt{10}]$ are such that $AB = C$, we say that A divides C and B divides C. A and B are called factors of C.

Theorem 2.20: A divides C if an only if every number of C is in A.

Let $A = (\omega_1, \omega_2)$, $B = (\chi_1, \chi_2)$, then $AB = C$ consists of all numbers

$$k\omega_1\chi_1 + \lambda\omega_1\chi_2 + \mu\omega_2\chi_1 + \nu\omega_2\chi_2$$

where k, λ, μ, ν range over $Ra[\sqrt{10}]$. Putting this form in the following two ways,

$$(k\omega_1+\mu\omega_2)\chi_1 + (\lambda\omega_1+\nu\omega_2)\chi_2, \quad (k\chi_1+\lambda\chi_2)\omega_1 + (\mu\chi_1+\nu\chi_2)\omega_2$$

it can be seen that every number of C is in both A and B.

Conversely, suppose that every number of C is in A. Then every number of $C\bar{A}$ is in $A\bar{A} = (a)$, where a is a positive integer. That is, all numbers of $C\bar{A}$ are given by βa, where β ranges over a certain set B of numbers of $Ra[\sqrt{10}]$.

Since $C\bar{A}$ is an ideal, 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

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

for every k in $Ra[\sqrt{10}]$. Hence

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

so that B is an ideal.

It follows from Theorem 2.19 and

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

that $C = AB$.

Theorem 2.21: A positive integer t occurs in but a finite number of ideals.

Let the ideal A containing t have a canonical basis $(ra, rb+r\sqrt{10})$, where $r > 0$, $a > 0$, $0 \leq b < a$. By Corollary 2.12, ra divides t. For a given t, there are not more than t choices for each of the positive integers r, a, and b, and therefore not more than t^3 such ideals A.

Theorem 2.22: An ideal C is divisible by only a finite number of ideals.

We have $C\overline{C} = (c)$ where c is a positive integer. By Theorem 2.20, c is in C and also in every ideal which divides C. By Theorem 2.21 there is but a finite number of such ideals.

Prime Ideals: If an ideal P, different from the unit ideal, (1), is divisible by no ideal other than itself and (1), it is called a prime ideal. All other ideals, except (1), are composite.

Greatest Common Divisor: An ideal G is called a greatest common divisor of A and B if G divides both A and B, and if every common divisor of A and B divides G.

Theorem 2.23: Every pair of ideals, A and B, possesses a unique g.c.d., G. It is composed of all numbers $\alpha + \beta$ where α ranges over A and β over B.

The set G of all numbers $\alpha + \beta$ satisfies the definition of

ideal. Since every number of A is in G and every number of B is in G, G is a common divisor of A and B.

Let E be any common ideal divisor of A and B; that is, any ideal containing all the numbers of A and all the numbers of B. Since it is closed under addition, it contains all numbers $\alpha + \beta$ of G and hence divides G.

Suppose that G and G_1 are two g. c. d. 's of A and B. Then $G = K_1 G_1$, $G_1 = KG$, so that

$$(1)G = K_1 KG.$$

Hence, by Theorem 2.19 $K_1 K = (1)$. Since

$$N(K_1 K) = N(K_1)N(K) = N(1) = 1, \quad K = K_1 = (1).$$

So

$$G = G_1$$

Two ideals are called relatively prime if their g. c. d. is (1).

Theorem 2.24: If A and B are relatively prime, there exists an α in A and a β in B such that $\alpha + \beta = 1$.

Since A and B are relatively prime their g. c. d. is (1); that is $G = (\omega_1, \omega_2, \chi_1, \chi_2) = (1)$ where $A = (\omega_1, \omega_2)$, $B = (\chi_1, \chi_2)$.

But since 1 is a number of G, it must be a linear combination of $\omega_1, \omega_2, \chi_1, \chi_2$;

that is,

$$k_1\omega_1 + k_2\omega_2 + \ell_1\chi_1 + \ell_2\chi_2 = 1,$$

where k_1, k_2, ℓ_1, ℓ_2 are in $Ra[\sqrt{10}]$.

But $k_1\omega_1 + k_2\omega_2$ is in A and $\ell_1\chi_1 + \ell_2\chi_2$ is in B, and we have

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

Theorem 2. 25: If A divides BC and is prime to B, then A divides C.

If A is prime to B, then by Theorem 2. 24 there exists an α in A and a β in B such that

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

Multiplying through by γ we have

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

For every γ in C. Since A divides BC, the number $\gamma\beta$ of BC is in A. So is $\alpha\gamma$, and so therefore is γ. Then, by Theorem 2. 20, A divides C.

Theorem 2. 26: (Unique factorization of composite ideals). Every composite ideal can be factored into prime ideals in one and, except

for order of the factors, in only one way.

That every ideal can be factored into a finite number of prime ideals follows from Theorem 2. 22.

If C is a composite ideal then

$$C = A_1 A_2 A_3 \cdots A_m$$

where the A's are prime ideals.

Suppose that

$$C = B_1 B_2 B_3 \cdots B_n$$

is another representation of C, where the B's are prime ideals. Then

$$A_1 A_2 A_3 \cdots A_m = B_1 B_2 B_3 \cdots B_n.$$

Since A_1 is a prime ideal dividing $B_1 B_2 B_3 \cdots B_n$ then by Theorem 2. 25, A_1 divides some B_k. (As in the proof of Theorem 1. 15.) Also, since B_k is prime we must have $A_1 = B_k$. Since we can rearrange the order of the B's, we may assume $A_1 = B_1$. Now, since $A_1 \neq (0)$

$$A_2 A_3 \cdots A_m = B_2 \; B_3 \cdots B_n.$$

As before A_2 divides one of the remaining B's, say B_2, and since A_2 and B_2 are both prime, $A_2 = B_2$. We continue in this

manner until all the A's or all the B's are exhausted. Evidently $m = n$, or otherwise we should have a product of primes equal to (1).

Hence every ideal can be written uniquely as a product of prime ideals.

Example: To factor (26) into prime ideals.

$$(26) = (2)(13) = (6+\sqrt{10})(6-\sqrt{10})$$

but $$(2) = (2, \sqrt{10})(2, \sqrt{10}) = (4, 2\sqrt{10}, 2\sqrt{10}, 10)$$

and $$(13) = (13, 6+\sqrt{10})(13, 6-\sqrt{10})$$

Now, suppose $(2, \sqrt{10})$ is not a prime ideal. Then

$$(2, \sqrt{10}) = AB,$$

where neither A nor B = (1). Let

$$A = (a_1, a_2, a_3, \ldots, a_m), \quad B = (b_1, b_2, b_3, \ldots, b_n)$$

then

$$(2, \sqrt{10}) = (a_1, a_2, a_3, \ldots, a_m)(b_1, b_2, b_3, \ldots, b_n).$$

By Theorem 2. 20, 2 and $\sqrt{10}$ are numbers of both A and B. So

$$(2, \sqrt{10}) = (a_1, a_2, \ldots, a_m, 2, \sqrt{10})(b_1, b_2, \ldots, b_n, 2, \sqrt{10}).$$

Let $a_k = p+q\sqrt{10}$ be any one of the a's. Then p is of the form 2r, 2r + 1, or 2r-1. We have

1) $$a_i = q\sqrt{10} + 2r$$

2) $$a_i = q\sqrt{10} + 2r + 1$$

3) $$a_i = q\sqrt{10} + 2r - 1.$$

If 1) is the case we may omit a_i from the symbol A. If 2) is the case, we have

$$a_i - q\sqrt{10} - 2r = 1$$

and 1 may be introduced in the symbol A, so A = (1). If 3) is the case, we have

$$q\sqrt{10} + 2r - a_i = 1$$

and again A = (1).

Continuing in this manner we find that either all numbers $a_1, a_2, \ldots, a_m$ are linear combinations of $2, \sqrt{10}$, in which case $A = (2, \sqrt{10})$, or 1 may be introduced in the symbol A and so A = (1). Similar conclusions hold for B. Therefore the only possible factorizations for $(2, \sqrt{10})$ are as follows:

4) $$(2, \sqrt{10}) = (1)(1) = (1)$$

5) $$(2, \sqrt{10}) = (2, \sqrt{10})(2, \sqrt{10}) = (2)$$

6) $$(2, \sqrt{10}) = (2, \sqrt{10})(1)$$
$$= (1)(2, \sqrt{10}).$$

If 4) be the case then 1 must be in $(2, \sqrt{10})$, that is

$$2(x+y\sqrt{10}) + \sqrt{10}(u+v\sqrt{10}) = 1,$$

or

$$2x + 10v = 1, \quad 2y + u = 0.$$

Since no two rational integers satisfy the equation

$2x + 10v = 2(x+5v) = 1$, 4) is impossible.

5) is impossible because $\sqrt{10}$ is not a multiple of 2.

Hence we have shown the ideal, $(2, \sqrt{10})$, to be a prime ideal.

Suppose $(13, 6+\sqrt{10})$ is composite. Then, as before,

$$(13, 6+\sqrt{10}) = AB = (a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_n),$$

and by Theorem 2.20 13 and $6 + \sqrt{10}$ are numbers of both A and B. Since, by Theorem 2.7, 1 and $6 + \sqrt{10}$ form a basis for the numbers of $Ra[\sqrt{10}]$, we can express any one of the numbers $a_1, a_2, \ldots, a_m$ in the form $a_i = p + q(6+\sqrt{10})$. Since p is a rational integer, p is of the form $13r \pm n$, $n = 0, 1, 2, 3, 4, 5, 6$, and r, a rational integer. Then we have,

$$a_i - [q(6+\sqrt{10}) + 13r] = \pm n.$$

If $n = 0$ we may omit a_i from the symbol A. If n is any other of its permissible values then we may introduce that number in the symbol A and since 13 is also in A, we will have two rational integers in A which are relatively prime. Therefore, rational integers, α, β, exist such that $n\alpha + 13\beta = 1$. So 1 may

be introduced in the symbol A, hence A = (1).

Continuing in this manner we find that either all numbers $a_1, \ldots, a_m$ are linear combination of 13, $6+\sqrt{10}$, in which case $A = (13, 6+\sqrt{10})$, or 1 may be introduced in the symbol A, so A = (1). Similar conclusions hold for B. Therefore the only possible factorizations for $(13, 6+\sqrt{10})$ are as follows:

7) $$(13, 6+\sqrt{10}) = (1)(1) = (1)$$

8) $$(13, 6+\sqrt{10}) = (13, 6+\sqrt{10})(13, 6+\sqrt{10})$$

9) $$(13, 6+\sqrt{10}) = (13, 6+\sqrt{10})(1)$$
$$= (1)(13, 6+\sqrt{10})$$

Since 1 is not a member of $(13, 6+\sqrt{10})$, 7) is impossible. 8) is impossible, for if not, then Theorem 2. 19 would imply that $(13, 6+\sqrt{10}) = (1)$ but 1 is not in $(13, 6+\sqrt{10})$.

Hence we have shown the ideal $(13, 6+\sqrt{10})$ to be a prime ideal.

Since $1, 6-\sqrt{10}$ also form a basis for $Ra[\sqrt{10}]$ a similar argument shows $(13, 6-\sqrt{10})$ to be a prime ideal.

Therefore

$$(26) = (2, \sqrt{10})(2, \sqrt{10})(13, 6+\sqrt{10})(13, 6-\sqrt{10})$$

and by Theorem 2. 26, this representation of (26) as a product of prime ideals is unique.

BIBLIOGRAPHY

1. MacDuffee, Cyrus Colton. An introduction to abstract algebra. New York, Wiley, 1940. 303 p.

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