AN ABSTRACT OF THE THESIS OF

Sue Elaine Hardy Waldman for the M.S. in Mathematics
(Name) (Degree) (Major)

Date thesis is presented July 18, 1966

Title THE QUADRATIC INTEGRAL DOMAINS $Ra[\sqrt{3}]$ AND $Ra[\sqrt{-15}]$

Abstract approved Redacted for Privacy
(Major professor)

This paper is the record of an exploration of two quadratic number fields. The first section is devoted to the field with elements of the form $a+b\sqrt{3}$ where a and b are rational numbers. This field contains an integral domain in which unique factorization holds. The second section is concerned with a field having an integral domain in which the unique factorization theorem does not hold; therefore ideals are introduced to restore this property. The elements of this field are of the form $a+b\sqrt{-15}$ where a and b are rational numbers.

THE QUADRATIC INTEGRAL DOMAINS $Ra[\sqrt{3}]$ AND $Ra[\sqrt{-15}]$

by

SUE ELAINE HARDY WALDMAN

A THESIS

submitted to

OREGON STATE UNIVERSITY

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1967

APPROVED:

Redacted for Privacy

Professor of Mathematics

In Charge of Major

Redacted for Privacy

Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented July [illegible], [illegible]

Typed by Carol Baker

TABLE OF CONTENTS

THE QUADRATIC INTEGRAL DOMAINS $Ra[\sqrt{3}]$ and $Ra[\sqrt{-15}]$

I. THE QUADRATIC INTEGRAL DOMAIN $Ra[\sqrt{3}]$

Let $px^2+qx+r = 0$, $p \neq 0$ with rational coefficients be a quadratic equation irreducible over the rational field. Since the roots remain unchanged if both sides of an equation are multiplied by the common denominator of the coefficients, we may assume, without loss of generality, that p, q, and r are integers of the rational field which will be called rational integers $p \neq 0$. Let us consider this case: $q^2-4pr = 3k$ where $k = t^2$ and t is a rational integer not zero.

ρ is one of the roots of the equation. Since the equation is irreducible, ρ is not a rational number. Denote by $Ra(\rho)$ the set of numbers $a+b\rho$ where a and b range over the rational numbers.

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

Taking the particular case noted above, where

$$q^2-4pr = 3k, \quad k = t^2 \neq 0$$

then the roots are $\rho_1 = \dfrac{-q+\sqrt{3k}}{2p}$, $\rho_2 = \dfrac{-q-\sqrt{3k}}{2p}$.

Let $\rho = \dfrac{-q+\sqrt{3k}}{2p}$, then $\sqrt{3k} = 2p\rho+q$.

The first equation shows that every number of the form $a+b\rho$ can be written in the form $c+d\sqrt{3k}$ and the second equation shows all numbers of the form $a+b\sqrt{3k}$ are of the form $c+d\rho$. Then $Ra(\rho) = Ra(\sqrt{3k})$.

Now set $3k = 3t^2$, then $a+b\sqrt{3k} = a+bt\sqrt{3}$. So

$$Ra(\rho) = Ra(\sqrt{3k}) = Ra(\sqrt{3}) \quad \text{and} \quad m = 3.$$

A similar argument would hold if we let $\rho = \dfrac{-q-\sqrt{3k}}{2p}$.

Example: Consider the quadratic equation $3x^2+6x+2 = 0$. ρ is one of its roots so

$$\rho = \frac{-6+\sqrt{12}}{6} = \frac{-6+\sqrt{3\cdot 4}}{6} = -1+\frac{1}{3}\sqrt{3}$$

then

$$a+b\rho = a+b(-1+\frac{1}{3}\sqrt{3}) = (a-b)+(\frac{b}{3})\sqrt{3} = c+d\sqrt{3}$$

and since

$$\rho = -1+\frac{1}{3}\sqrt{3}, \quad \sqrt{3} = 3\rho+3 \;;$$

so

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

where a, b, c, d in both cases are rational.

Hence, numbers of the form $a+b\rho$ may be expressed as $c+d\sqrt{3}$ and conversely. Or, in general, $Ra(\rho) = Ra(\sqrt{3})$.

Theorem 1.2: The set $Ra(\sqrt{3})$ is a field.

Since the set $Ra(\sqrt{3})$ is contained in the complex field the associative, commutative and distributive laws hold for addition and multiplication. It is to be shown that the set is closed for the two operations, the identity elements for each operation are contained in the set, each element has an additive inverse in the set, and every element except the identity in $Ra(\sqrt{3})$ has its reciprocal in $Ra(\sqrt{3})$.

i) closure:

$$(a_1+b_1\sqrt{3}) + (a_2+b_2\sqrt{3}) = (a_1+a_2) + (b_1+b_2)\sqrt{3}$$

hence addition is closed.

$$(a_1+b_1\sqrt{3})(a_2+b_2\sqrt{3}) = (a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3}$$

hence multiplication is closed.

ii) identities:

$$(c+d\sqrt{3}) + (0+0\sqrt{3}) = c+d\sqrt{3}$$

Therefore $0+0\sqrt{3} = 0$ is the additive identity.

$(c+d\sqrt{3})(1+0\sqrt{3}) = c+d\sqrt{3}$

Therefore $1+0\sqrt{3} = 1$ is the multiplicative identity.

iii) inverses:

$(c+d\sqrt{3}) + (-c-d\sqrt{3}) = 0+0\sqrt{3}$

and every element of $Ra(\sqrt{3})$ has an additive inverse in $Ra(\sqrt{3})$.

$(c+d\sqrt{3})y = 1$ $c \neq d \neq 0$ since the additive identity is excluded.

$$y = \frac{1}{c+d\sqrt{3}} = \frac{c-d\sqrt{3}}{c^2-3d^2} = \left(\frac{c}{c^2-3d^2}\right) + \left(\frac{-d}{c^2-3d^2}\right)\sqrt{3}$$

an element of $Ra(\sqrt{3})$,

c and d are rational and $c^2-3d^2 \neq 0$. If $c^2-3d^2 = 0$ then $c^2 = 3d^2$ or $3 = \frac{c^2}{d^2}$, $d \neq 0$ since this would imply in the previous step that c also be 0 and it was given that $c \neq d \neq 0$. So $\sqrt{3} = \frac{c}{d}$, a rational number, which is a contradiction, hence $c^2 - 3d^2 \neq 0$.

Theorem 1.3: Every number of $Ra(\sqrt{3})$ satisfies a quadratic equation with rational coefficients.

If $\alpha = a+b\sqrt{3}$ is any number of $Ra(\sqrt{3})$, then its conjugate is $\bar{\alpha} = a-b\sqrt{3}$ and α satisfies the equation $(x-a)^2-3b^2 = x^2-2ax+a^2-3b^2 = 0$. This equation is called the principal equation of $\alpha = a+b\sqrt{3}$. Its constant term $N(a+b\sqrt{3}) = a^2-3b^2$ is called the norm of $a+b\sqrt{3}$ and $N(\alpha) = \alpha\bar{\alpha}$. The negative of the coefficient of x, $T(a+b\sqrt{3}) = 2a$, is called the trace of $a+b\sqrt{3}$. Since a and b are rational, a^2-3b^2 and $2a$ are rational.

Integers of $Ra(\sqrt{3})$

The integers of $Ra(\sqrt{3})$ are the numbers of $Ra(\sqrt{3})$ which will satisfy equations of the form $x^2+px+q = 0$ where p and q are rational integers. These numbers constitute the integral domain $Ra[\sqrt{3}]$ of $Ra(\sqrt{3})$.

Theorem 1.4: Every rational integer is in $Ra[\sqrt{3}]$. Every number of $Ra[\sqrt{3}]$ which is rational is a rational integer.

If a is a rational integer then its principal equation is $x^2-2ax+a^2 = 0$ and is therefore in $Ra[\sqrt{3}]$.

If conversely, $a+b\sqrt{3}$ is rational then $b = 0$ and since $a+b\sqrt{3}$ satisfies the equation $x^2-2ax+a^2$ where $2a$ and a^2 are rational integers a must also be a rational integer.

Theorem 1.5: The conjugate of a number of $Ra[\sqrt{3}]$ is in $Ra[\sqrt{3}]$: for $a+b\sqrt{3}$ and $a-b\sqrt{3}$ have the same principal equation.

Hereafter the word integer will refer to integers of $Ra[\sqrt{3}]$. The integers of the rational field will always be called rational integers.

Theorem 1.6: The numbers of $Ra[\sqrt{3}]$ are given by $a+b\sqrt{3}$ where a and b range over all rational integers.

Every number $\alpha = a+b\sqrt{3}$ of $Ra(\sqrt{3})$ satisfies the principal equation $x^2-2ax+a^2-3b^2 = 0$. The integers of $Ra(\sqrt{3})$ will satisfy equations of the form $x^2+px+q = 0$, where p and q are rational integers. Therefore $2a = p$ and $a^2-3b^2 = q$ are rational integers. If $a+b\sqrt{3}$ is a number of $Ra(\sqrt{3})$ then a and b are rational or $\frac{a_1}{c_1} = a$, $\frac{b_1}{c_1} = b$ where a_1, b_1, c_1 are relatively prime rational integers. Then $\frac{2a_1}{c_1} = p$ (1), $\frac{a_1^2-3b_1^2}{c_1^2} = q$ (2), so $c_1 = 2$ or 1 since if $c_1 \neq 2$ or 1 then by (1) c_1 and a_1 would have a common factor of b_1 by (2) contrary to our hypothesis that a_1, b_1 and c_1 are relatively prime. If $c_1 = 2$ then by (2) a_1^2 and b_1^2 would be divisible by 2^2 or $a_1^2 - 3b_1^2 = 4q$. If a_1 is odd and b_1 is even or a_1 is even and b_1 is odd the contradiction is obvious. If a_1 is odd and b_1 is odd, then

$$(2n+1)^2-3(2m+1)^2 = 4q$$

$$4n^2+4n+1-24m^2-12m-3 = 4q$$

$$4n^2+4n-24m^2-12m-2 = 4q$$

$$n^2+n-6m^2-3m-\frac{1}{2} = q \quad .$$

But this is contrary to the fact that q is an integer. Hence a_1 and b_1 must both be even. Therefore a_1, b_1, c_1 would have a common factor contrary to our hypothesis. So $c_1 = 1$ and thus $a_1 = a$ and $b_1 = b$ are rational integers.

The numbers 1 and $\sqrt{3}$ form a basis for $Ra[\sqrt{3}]$. In other words every number of the domain $Ra[\sqrt{3}]$ is given without repetition in the form $a(1) + b(\sqrt{3})$ where a and b range independently over all rational integers and conversely every such number is in the domain.

Theorem 1.7: If θ_1 and θ_2 be a basis of $Ra[\sqrt{3}]$ every basis of $Ra[\sqrt{3}]$ is given by $\theta'_1 = a_{11}\theta_1 + a_{12}\theta_2$,

$$\theta'_2 = a_{21}\theta_1 + a_{22}\theta_2 \qquad (1)$$

where

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

Assume θ'_1 and θ'_2 is a basis for $Ra[\sqrt{3}]$. Then

$$\theta_1 = b_{11}\theta'_1 + b_{12}\theta'_2 \quad \text{and} \quad \theta_2 = b_{21}\theta'_1 + b_{22}\theta'_2 .$$

So

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

and

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

or

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

and

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

Therefore $a_{11}b_{11} + a_{21}b_{12} = 1$, $a_{12}b_{11} + a_{22}b_{12} = 0$, $a_{11}b_{21} + a_{21}b_{22} = 0$, $a_{12}b_{21} + a_{22}b_{22} = 1$ or

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

hence it is necessary for the determinant of the coefficients to be ± 1.

Any number in the domain $Ra[\sqrt{3}]$ can be written in terms of the basis. From (1) we know $\theta_1 = \pm(a_{22}\theta'_1 - a_{12}\theta'_2)$ and $\theta_2 = \pm(a_{21}\theta'_1 - a_{11}\theta'_2)$. If $\omega = c_1\theta_1 + c_2\theta_2$ is any number of the domain then

$$\omega = c_1[\pm(a_{22}\theta'_1 - a_{12}\theta'_2)] + c_2[\pm(a_{21}\theta'_1 - a_{11}\theta'_2)]$$

or

$$\omega = \pm(c_1a_{22} + c_2a_{21})\theta'_1 \mp (c_1a_{12} + c_2a_{11})\theta'_2 \quad .$$

Hence θ_1', θ_2' is a basis for $Ra[\sqrt{3}]$ since every number of $Ra[\sqrt{3}]$ may be written as a linear combination of θ_1' and θ_2' and every such combination is in the domain.

Since 1 and $\sqrt{3}$ is one basis θ_1, θ_2, for $Ra[\sqrt{3}]$ then all θ_1', θ_2' may be written as: $\theta_1' = a_{11} + a_{12}\sqrt{3}$, $\theta_2' = a_{21} + a_{22}\sqrt{3}$ where

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

<u>Theorem 1.8:</u> The norm of a product is the product of the norms.

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

<u>Proof.</u> $\alpha = a+b\sqrt{3}$ $\quad \beta = c+d\sqrt{3}$ $\quad \alpha\beta = (ac+3bd)+(ad+bc)\sqrt{3}$

$$N(\alpha) = a^2-3b^2 \quad N(\beta) = c^2-3d^2 \quad N(\alpha\beta) = (ac+3bd)^2-3(ad+bc)^2$$

$$N(\alpha\beta) = a^2c^2 + 9b^2d^2 - 3a^2d^2 - 3b^2c^2$$

$$= a^2c^2-3b^2c^2-3a^2d^2+9b^2d^2$$

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

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

<u>Theorem 1.9:</u> The norm of a quotient is the quotient of the norms.

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)} \quad \beta \neq 0$$

Let α, β, and $N(\alpha)$, $N(\beta)$ be as in Theorem 1.8

$$\frac{\alpha}{\beta} = \frac{(a+b\sqrt{3})(c-d\sqrt{3})}{(c+d\sqrt{3})(c-d\sqrt{3})} = \frac{ac-3bd}{c^2-3d^2} + \frac{(bc-ad)\sqrt{3}}{c^2-3d^2}$$

Then

$$N(\frac{\alpha}{\beta}) = (\frac{ac-3bd}{c^2-3d^2})^2 - 3(\frac{bc-ad}{c^2-3d^2})^2$$

$$= \frac{a^2c^2+9b^2d^2-3b^2c^2-3a^2d^2}{(c^2-3d^2)^2} = \frac{a^2(c^2-3d^2)-3b^2(c^2-3d^2)}{(c^2-3d^2)^2}$$

$$= \frac{a^2-3b^2}{c^2-3d^2} = \frac{N(\alpha)}{N(\beta)} .$$

If $\alpha \cdot \beta = \gamma$ in $Ra[\sqrt{3}]$ we say that α and β are divisors of γ. Further α divides γ in $Ra[\sqrt{3}]$ if and only if there is a β in $Ra[\sqrt{3}]$ such that $\alpha\beta = \gamma$.

A number of $Ra[\sqrt{3}]$ is called a unit if it divides 1.

<u>Theorem 1.10:</u> A number ϵ of $Ra[\sqrt{3}]$ is a unit if and only if $N(\epsilon) = \pm 1$. So $N(a+b\sqrt{3}) = a^2-3b^2 = \pm 1$ if $a+b\sqrt{3}$ is a unit. Conversely if $N(a+b\sqrt{3}) = \pm 1$, then $a+b\sqrt{3}$ is a unit.

If α is a unit then there exists a β such that $\alpha\beta = 1$.

$$N(\alpha\beta) = N(\alpha)N(\beta) \qquad \text{by Theorem 1.8}$$

$$N(1) = N(\alpha)N(\beta)$$

$$1 = N(\alpha)N(\beta)$$

So $N(\alpha) = \pm 1$ and $N(\beta) = \pm 1$. Conversely if $N(\alpha) = \pm 1$, then

$$\alpha\bar{\alpha} = \pm 1.$$

Therefore α divides 1 and α is a unit.

Theorem 1.11: All units of $Ra[\sqrt{3}]$ are of the form $\pm(2+\sqrt{3})^n$, where n is a positive or negative rational integer or 0 and all numbers of this form are units of $Ra[\sqrt{3}]$.

If $\epsilon = 2+\sqrt{3}$, then every positive power n of ϵ is a unit since $N(\epsilon^n) = [N(\epsilon)]^n = [\pm 1]^n = \pm 1$; hence ϵ^n is a unit. Furthermore ϵ^0 is a unit for $\epsilon^0 = 1$. Since $\epsilon^n\epsilon^{-n} = 1$, ϵ^{-n} is a unit also, or all negative powers of ϵ are units.

Different powers of ϵ give different units. $2+\sqrt{3}$ is greater than 1 so the positive powers will all be greater than 1 and will continually increase; hence no two positive powers are equal. Also $\epsilon^{-n} = \frac{1}{\epsilon^n}$ so ϵ^{-1} is less than 1 and ϵ^{-n} will continually decrease as n increases; therefore no two negative powers will be the same nor will they equal any positive power. Hence every power of ϵ is a unit of $Ra[\sqrt{3}]$ and two different powers always give different units.

We must further show that the powers of ϵ multiplied by ± 1 are all the units of $Ra[\sqrt{3}]$; that is, if η be any unit of $Ra[\sqrt{3}]$ then $\eta = \pm\epsilon^n$ where n is positive, negative or zero.

If $a+b\sqrt{3}$ is any unit of $Ra[\sqrt{3}]$, then $a-b\sqrt{3}$, $-a+b\sqrt{3}$ and $-a-b\sqrt{3}$ are also units of $Ra[\sqrt{3}]$. In other words the number, its conjugate and their associates, associates being numbers which are the same except for a unit factor, are each units of $Ra[\sqrt{3}]$ if any are.

Denote that one of these four units which has both terms positive by η_1 (b may be 0), the remaining three will be $-\eta_1$, η_1', and $-\eta_1'$.

Since $\eta_1 \geq 1$, it follows that

$$\eta_1 = \epsilon^n \qquad \text{or} \qquad \epsilon^n < \eta_1 < \epsilon^{n+1} \qquad (1)$$

where n is a positive integer or zero. Dividing (1), the latter expression, by ϵ^n we have

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

where $\dfrac{\eta_1}{\epsilon^n}$ is a unit for the quotient of two units is a unit. So let

$$\frac{\eta_1}{\epsilon^n} = x + y\sqrt{3} \; .$$

Then

$$(x+y\sqrt{3})(x-y\sqrt{3}) = \pm 1$$

and since according to (2) $x+y\sqrt{3} > 1$ then $|x-y\sqrt{3}| < 1$ or

$-1 < x-y\sqrt{3} < 1$. This, combined with

$$1 < x+y\sqrt{3} < 2+\sqrt{3} \qquad (3)$$

gives $0 < 2x < 3+\sqrt{3}$ and since x is a rational integer $x = 1$ or $x = 2$.

But if $x = 1$ (3) becomes

$$1 < 1+y\sqrt{3} < 2+\sqrt{3}$$

which implies that $y = 1$. So $\frac{\eta_1}{\epsilon^n} = 1+\sqrt{3}$ but $1+\sqrt{3}$ is <u>not</u> a unit since $N(1+\sqrt{3}) \neq \pm 1$. Furthermore for $x = 2$ we have

$$1 < 2+y\sqrt{3} < 2+\sqrt{3} .$$

There are no integral values of y which will satisfy this inequality. Positive values make $2+y\sqrt{3} \geq 2+\sqrt{3}$, negative values make $2+y\sqrt{3} < 1$, and if $y = 0$ then $\frac{\eta_1}{\epsilon^n} = 2$, but 2 is not a unit since $N(2) \neq \pm 1$. Hence (1) is impossible and we have $\eta_1 = \epsilon^n$, which implies that $-\eta_1 = -\epsilon^n$; and since $\eta_1\eta_1' = \pm 1$, $\eta_1' = \pm\frac{1}{\epsilon^n} = \pm\epsilon^{-n}$ and $-\eta_1' = \mp\epsilon^{-n}$. Therefore, if η be any one of the four units η_1, $-\eta_1$, η_1', $-\eta_1'$, that is any unit of $Ra[\sqrt{3}]$, we have $\eta = \pm\epsilon^n$ where n is positive, negative or zero.

Prime Numbers of Ra$[\sqrt{3}]$

Nonzero numbers of Ra$\sqrt{3}$ which are not units but are divisible only by units are called prime numbers. To determine whether an integer is prime or composite we may use methods similar to that of the following example.

Assume

$$5+\sqrt{3} = (a+b\sqrt{3})(c+d\sqrt{3})$$

Then

$$N(5+\sqrt{3}) = N(a+b\sqrt{3})N(c+d\sqrt{3})$$

or

$$22 = (a^2-3b^2)(c^2-3d^2)\ .$$

There are three cases to consider:

i) $a^2-3b^2 = \pm 1$ $\qquad c^2-3d^2 = \pm 22$

ii) $a^2-3b^2 = -11$ $\qquad c^2-3d^2 = -2$

iii) $a^2-3b^2 = +11$ $\qquad c^2-3d^2 = +2$

Case i) has $a+b\sqrt{3}$ a unit and need not be considered. Case ii) has solution $a = \mp 8$, $b = \pm 5$, $c = \pm 5$, $d = \pm 3$ or

$$5+\sqrt{3} = (-8+5\sqrt{3})(5+3\sqrt{3}) = (8-5\sqrt{3})(-5-3\sqrt{3}).$$

Since neither of the integers $-8+5\sqrt{3}$ or $5+3\sqrt{3}$ is a unit, $5+\sqrt{3}$ is a composite number. Other solutions of case ii) include

$a = \pm 17$, $b = \pm 10$, $c = \mp 5$, $d = \pm 3$ or

$$5+\sqrt{3} = (17+10\sqrt{3})(-5+3\sqrt{3}) = (-17-10\sqrt{3})(5-3\sqrt{3}).$$

Case iii) has solution $a = \mp 1$, $b = \pm 2$, $c = \pm 1$, $d = \pm 1$ or

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

We see however, that each of these factorizations can be derived from any particular one by multiplying the factors by suitable units, and hence are not different, except for unit factors; that is

$$-8+5\sqrt{3} = \epsilon^{-1}(-1+2\sqrt{3}) \qquad 5+3\sqrt{3} = \epsilon^{1}(1+\sqrt{3})$$

$$17+10\sqrt{3} = \epsilon^{2}(-1+2\sqrt{3}) \qquad -5+3\sqrt{3} = \epsilon^{-2}(1+\sqrt{3})$$

where $\epsilon = 2+\sqrt{3}$ and we have in general

$$5+\sqrt{3} = [\pm\epsilon^{n}(-1+2\sqrt{3})][\pm\epsilon^{-n}(1+\sqrt{3})] .$$

<u>Theorem 1.12</u>: If α is any integer of $Ra[\sqrt{3}]$ and β is any integer of $Ra[\sqrt{3}]$ different from zero, there exists an integer γ of $Ra[\sqrt{3}]$ such that

$$|N(\alpha-\gamma\beta)| < |N(\beta)|. \qquad (1)$$

Let $\frac{\alpha}{\beta} = a+b\sqrt{3}$ where $a = r+r_1$, $b = s+s_1$, r and s being the rational integers nearest to a and b respectively, and hence $|r_1| \leq \frac{1}{2}$, $|s_1| \leq \frac{1}{2}$. We then show that $\gamma = r+s\sqrt{3}$ will fulfill the required conditions.

Since $\frac{\alpha}{\beta} - \gamma = r_1+s_1\sqrt{3}$

$$|N(\frac{\alpha}{\beta}-\gamma)| = |r_1^2-3s_1^2| \leq \frac{3}{4}$$

whence

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

or multiplying by $|N(\beta)|$,

$$|N(\alpha-\gamma\beta)| < |N(\beta)| .$$

Example: Consider the integers of $Ra[\sqrt{3}]$ $\alpha = 2+3\sqrt{3}$ and $\beta = 3+\sqrt{3}$

$$\frac{\alpha}{\beta} = \frac{2+3\sqrt{3}}{3+\sqrt{3}} = \frac{(2+3\sqrt{3})(3-\sqrt{3})}{6} = \frac{-3+7\sqrt{3}}{6} = -\frac{1}{2}+\frac{7}{6}\sqrt{3} = a+b\sqrt{3}$$

where $a = r+r_1 = -1+\frac{1}{2}$, $b = s+s_1 = 1+\frac{1}{6}$. Then

$$\gamma = r+s\sqrt{3} = -1+\sqrt{3} .$$

Then

$$|N(\alpha-\gamma\beta) = |N[(2+3\sqrt{3})-(-1+\sqrt{3})(3+\sqrt{3})]| = |N(2+\sqrt{3})| = 1$$

and

$$|N(\beta)| = |N(3+\sqrt{3})| = 6 .$$

So

$$|N(\alpha-\gamma\beta)| = 1 < 6 = |N(\beta)| .$$

Hence there exists an integer γ in $Ra[\sqrt{3}]$ such that the inequality (1) is true.

Theorem 1.13: If α and β are any two integers of $Ra[\sqrt{3}]$ prime to each other, there exist two integers, σ and η of $Ra[\sqrt{3}]$ such that

$$\alpha\sigma + \beta\eta = 1 \quad .$$

If either α or β is a unit then the existence of the required integers σ and η is evident. If neither α or β is a unit, the determination of σ and η can be made to depend upon the determination of a corresponding pair of integers σ_1 and η_1 for a pair of integers α_1 and β_1, prime to each other and such that the absolute value of the norm of one of them is less than both $|N(\alpha)|$ and $|N(\beta)|$.

Assume $|N(\beta)| \leq |N(\alpha)|$, which does not limit the generality of the proof.

By Theorem 1.12 there exists an integer γ such that

$$|N(\alpha-\gamma\beta)| < |N(\beta)| \ .$$

Then β and $\alpha-\gamma\beta$ are a pair of integers α_1, β_1, prime to each other and such that the absolute value of the norm of one of them is less than both $|N(\alpha)|$ and $|N(\beta)|$.

If now, two integers σ_1, η_1, exist such that $\alpha_1\sigma_1 + \beta_1\eta_1 = 1$; that is

$$\beta\sigma_1 + (\alpha-\gamma\beta)\eta_1 = 1\,,$$

so

$$\alpha\eta_1 + \beta(\sigma_1 - \gamma\eta_1) = 1$$

and hence $\sigma = \eta_1$ and $\eta = \sigma_1 - \gamma\eta_1$.

If neither α_1 nor β_1 is a unit the determination of σ_1 and η_1 for α_1 and β_1 may be made to depend similarly upon that of σ_2 and η_2 for a pair of integers α_2 and β_2 prime to each other and such that the absolute value of the norm of one of them is less than both $|N(\alpha_1)|$ and $|N(\beta_1)|$.

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

Since the existence of σ_n and η_n is evident, the existence of σ and η is proved.

Example: Consider $\alpha = 2+3\sqrt{3}$ and $\beta = 3+\sqrt{3}$. α and β are relatively prime since $\alpha = 2+3\sqrt{3}$ is a prime number of $Ra[\sqrt{3}]$ and α is not a factor of β. If β were divisible by α then a γ would exist such that $\alpha\gamma = \beta$. But, if $\alpha\gamma = \beta$ then $N(\alpha)N(\gamma) = N(\beta)$ or $(-23)(N(\gamma)) = 6$ or $N(\gamma) = \frac{-6}{23}$. There is no

γ in $Ra[\sqrt{3}]$ such that $N(\gamma) = \frac{-6}{23}$. So α and β are relatively prime and

$$|N(\beta)| = 6 < 23 = |N(\alpha)|.$$

Is there a σ and η in $Ra[\sqrt{3}]$ such that $\alpha\sigma + \beta\eta = 1$? By Theorem 1.12 there exists γ such that

$$|N(\alpha-\gamma\beta)| < |N(\beta)| \quad \text{i.e.} \quad \gamma = -1+\sqrt{3}.$$

So

$$\alpha-\gamma\beta = 2+\sqrt{3} = \beta_1$$

$$\beta = 3+\sqrt{3} = \alpha_1 .$$

Then

$$\alpha_1\sigma_1 + \beta_1\eta_1 = 1$$

or

$$\beta\sigma_1 + (\alpha-\gamma\beta)\eta_1 = 1 . \qquad (1)$$

But $\alpha-\gamma\beta$ is a unit; therefore let η_1 be its conjugate or associate of its conjugate and σ_1 be zero. So (1) becomes

$$(3+\sqrt{3})(0) + (2+\sqrt{3})(2-\sqrt{3}) = 1 .$$

From (1) $\sigma = \eta_1$ and $\eta = \sigma_1 - \gamma\eta_1$. So $\sigma = 2-\sqrt{3}$ and $\eta = 0-(-1+\sqrt{3})(2-\sqrt{3}) = 5-3\sqrt{3}$ and

$$\alpha\sigma + \beta\eta = (2+3\sqrt{3})(2-\sqrt{3})+(3+\sqrt{3})(5-3\sqrt{3}) = -5+4\sqrt{3}+6-4\sqrt{3} = 1 .$$

Hence there is a σ and an η in $Ra[\sqrt{3}]$ to satisfy the required condition.

Corollary 1.13: If α and β are any two integers of $Ra[\sqrt{3}]$, there exists a common divisor, δ, of α and β such that every common divisor of α and β divides δ, and there exists two integers, σ and η, of $Ra[\sqrt{3}]$ such that $\alpha\sigma + \beta\eta = \delta$.

If α and β are relatively prime then by Theorem 1.13 $\alpha\sigma + \beta\eta = 1$ (1) and $1 = \delta$.

If α and β are not prime to each other then $\alpha = \alpha_1\delta$ and $\beta = \beta_1\delta$ where α_1 and β_1 are relatively prime. Then if $\alpha = \alpha_1$ and $\beta = \beta_1$ in (1) and we multiply by δ we have

$$\alpha_1\delta\sigma + \beta_1\delta\eta = \delta$$

or

$$\alpha\sigma + \beta\eta = \delta .$$

Every common divisor of α and β divides δ and δ is the divisor sought. The divisor δ is called the greatest common divisor of α and β.

Theorem 1.14: If the product of two integers α and β of $Ra[\sqrt{3}]$ is divisible by a prime number θ at least one of the integers is divisible by θ.

Let $\alpha\beta = \theta\gamma$ where γ is an integer of $Ra[\sqrt{3}]$ and assume α not to be divisible by θ. Then α and θ are relatively prime and from Theorem 1.13 there exist two integers σ and η of $Ra[\sqrt{3}]$ such that $\alpha\sigma + \theta\eta = 1$.

Multiplying by β the equation becomes:

$$\beta\alpha\sigma + \beta\theta\eta = \beta \quad . \qquad (1)$$

But $\alpha\beta = \theta\gamma$ so (1) is $\theta\gamma\sigma + \beta\theta\eta = \beta$ or $\theta(\gamma\sigma + \beta\eta) = \beta$ where $(\gamma\sigma + \beta\eta)$ is an integer of $Ra[\sqrt{3}]$, hence β is divisible by θ.

Corollary 1.14: If the product of any number of integers of $Ra[\sqrt{3}]$ is divisible by a prime number, θ, at least one of the integers is divisible by θ.

If $\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \cdots \alpha_n = \theta\beta$ (1) where $\alpha_1, \cdots, \alpha_n, \theta, \beta,$ in $Ra[\sqrt{3}]$ and $\gamma = \alpha_2 \cdot \alpha_3 \cdots \alpha_n$ then (1) may be written as $\alpha_1\gamma = \theta\beta$.

By Theorem 1.14, θ divides α_1 or γ. If α_1 is divisible by θ the corollary is proved. If instead γ is divisible by θ then since $\gamma = \alpha_2\gamma_1$, θ divides α_2 or γ_1. Continuing in the same manner as before the number of factors in question is reduced one at a time until only two are left. Then by Theorem 1.14 one of the other must be divisible by θ.

Theorem 1.15: (Unique Factorization Theorem) Every integer of $Ra[\sqrt{3}]$ can be represented in one and only one way as the product of prime numbers.

Let α be an integer of $Ra[\sqrt{3}]$. If α is not a prime number, then $\alpha = \beta\gamma$ where β and γ are integers of $Ra[\sqrt{3}]$ neither of which is a unit. It follows then that $N(\alpha) = N(\beta)N(\gamma)$. Since $N(\beta) \neq \pm 1$ and $N(\gamma) \neq \pm 1$, we have $|N(\beta)| < |N(\alpha)|$ and $|N(\gamma)| < |N(\alpha)|$.

If β is not a prime number we have as before $\beta = \beta_1\gamma_1$ where β_1 and γ_1 are integers neither of which is a unit, hence $|N(\beta_1)| < |N(\beta)|$ and $|N(\gamma_1)| < |N(\beta)|$. If β_1 is not a prime number, we proceed in the same manner and, since $|N(\beta)|$, $|N(\beta_1)|$, $|N(\beta_2)| \cdots$ form a decreasing series of positive rational integers, we must, after a finite number of such factorizations, reach in the series $\beta, \beta_1, \beta_2, \beta_3 \cdots$ a prime number θ_1. Thus α has the prime factor θ_1 and we have $\alpha = \theta_1\alpha_1$.

Proceeding similarly with α_1, in case it is not a prime number, we obtain $\alpha_1 = \theta_2\alpha_2$ where θ_2 is a prime number, and hence $\alpha = \theta_1\theta_2\alpha_2$.

Continuing this process we must reach in the series $\alpha, \alpha_1, \alpha_2, \cdots$ a prime number θ_n since $|N(\alpha)|$, $|N(\alpha_1)|$, $|N(\alpha_2)| \cdots$ form a decreasing series of positive rational integers. We have thus $\alpha = \theta_1\theta_2\theta_3 \cdots \theta_n$ where the θ's are all prime numbers; that is α can be represented as a product of a finite number of factors all of which are prime numbers.

We now need to show that this representation is unique.

Suppose that $\alpha = \phi_1\phi_2\phi_3 \cdots \phi_m$; then it follows that $\theta_1\theta_2\theta_3 \cdots \theta_n = \phi_1\phi_2\phi_3 \cdots \phi_m$. From Corollary 1. 14 we can conclude that if $\theta_1\theta_2\theta_3 \cdots \theta_n = \phi_1\phi_2\phi_3 \cdots \phi_m$ then at least one of the ϕ's say ϕ_1 is divisible by θ_1 and hence associated with θ_1 that is $\phi_1 = \epsilon_1\theta_1$, where ϵ_1 is a unit. Dividing by θ_1 we have $\theta_2\theta_3 \cdots \theta_n = \epsilon_1\phi_2\phi_3 \cdots \phi_m$. From this it follows that at least one of the remaining ϕ's say ϕ_2 is divisible by θ_2 and hence associated with it. Thus $\phi_2 = \epsilon_2\theta_2$ where ϵ_2 is a unit, and hence

$$\theta_3\theta_4 \cdots \theta_n = \epsilon_1\epsilon_2\phi_3\phi_4 \cdots \phi_m .$$

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

In exactly the same manner we can prove that with each ϕ there is associated at least one θ, and, if two or more ϕ's be associated with one another, at least as many θ's are associated with these ϕ's and hence with one another.

Hence since we always consider two associated factors as the same, the two representations are identical. For if in our representation there occur e factors associated with a certain prime, there will be exactly e factors in the other representation associated with the same prime.

We can write every integer, α, of $Ra[\sqrt{3}]$ in the form $\alpha = \epsilon\theta_1^{e_1}\theta_2^{e_2}\cdots\theta_n^{e_n}$ where $\theta_1, \theta_2\cdots\theta_n$ are the unassociated prime factors of α and ϵ a suitable unit. This representation is unique.

II. THE QUADRATIC INTEGRAL DOMAIN $Ra[\sqrt{-15}]$

Consider a quadratic equation $px^2+qx+r = 0$, $p \neq 0$ irreducible over the rational field; again we may assume without loss of generality that $p, q,$ and r are rational integers. Now consider the case where $q^2-4pr = -15k$ where $k = t^2$ and t is a nonzero rational integer.

ρ is one of the roots of the equation. Since the equation is irreducible, ρ is not a rational number. Denote by $Ra(\rho)$ the set of numbers $a+b\rho$ where a and b range over the rational numbers.

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

For the case referred to above $m = -15$. Since the proof is similar to that for $m = 3$, we omit the proof and consider the following example:

Example: Consider the equation $2x^2-x+17 = 0$, ρ is one of its roots so

$$\rho = \frac{1+\sqrt{-135}}{4} = \frac{1}{4}+\frac{3}{4}\sqrt{-15}.$$

Then

$$a+b\rho = a+b(\frac{1}{4}+\frac{3}{4}\sqrt{-15}) = (a+\frac{1}{4}b)+\frac{3b}{4}\sqrt{-15} = c+d\sqrt{-15}$$

and since

$$\rho = \frac{1}{4} + \frac{3}{4}\sqrt{-15}, \qquad \sqrt{-15} = \frac{4\rho-1}{3}$$

and

$$a+b\sqrt{-15} = a+b(\frac{4}{3}\rho - \frac{1}{3}) = (a - \frac{1}{3}b) + (\frac{4}{3}b)\rho = c+d\rho$$

where a, b, c, d in both cases are rational. Hence numbers of the form $a+b\rho$ may be expressed as $c+d\sqrt{-15}$ and conversely. Therefore $Ra(\rho) = Ra(\sqrt{-15})$.

<u>Theorem 2. 2:</u> The set $Ra(\sqrt{-15})$ is a field.

Since the complex numbers form a field and $Ra(\sqrt{-15})$ is a subset of the complex field the associative, commutative and distributive laws hold for addition and multiplication. It remains to be shown that the set is closed under the two operations, the identity element for each operation is contained in the set and every element except the additive identity in $Ra(\sqrt{-15})$ has its reciprocal in $Ra(\sqrt{-15})$.

i) closure:

$$(a_1+b_1\sqrt{-15}) + (a_2+b_2\sqrt{-15}) = (a_1+a_2)+(b_1+b_2)\sqrt{-15}$$

hence addition is closed.

$$(a_1+b_1\sqrt{-15})(a_2+b_2\sqrt{-15}) = (a_1a_2-15b_1b_2)+(a_1b_2+a_2b_1)\sqrt{-15}$$

hence multiplication is closed.

ii) identities:

$(c+d\sqrt{-15}) + (0+0\sqrt{-15}) = c+d\sqrt{-15}$

Therefore $0+0\sqrt{-15} = 0$ is the additive identity.

$(c+d\sqrt{-15})(1+0\sqrt{-15}) = c+d\sqrt{-15}$

Therefore $1+0\sqrt{-15} = 1$ is the multiplicative identity.

iii) inverses:

$(c+d\sqrt{-15}) + (-c-d\sqrt{-15}) = 0+0\sqrt{-15} = 0$

and every element of $Ra(\sqrt{-15})$ has an additive inverse in $Ra(\sqrt{-15})$.

$$(c+d\sqrt{-15})\left(\frac{1}{c+d\sqrt{-15}}\right) = 1 \qquad c \neq d \neq 0$$

since additive identity excluded.

$\frac{1}{c+d\sqrt{-15}}$ is an element of $Ra(\sqrt{-15})$ since

$$\frac{1}{c+d\sqrt{-15}} = \frac{c-d\sqrt{-15}}{c^2+15d^2} = \frac{c}{c^2+15d^2} - \frac{d}{c^2+15d^2}\sqrt{-15}$$

where c, d are rational and $c^2+15d^2 \neq 0$.

If $c^2+15d^2 = 0$ then $c^2 = -15d^2$ or $\frac{c^2}{d^2} = -15$,

$d \neq 0$ for the previous step would imply if $d = 0$ that $c = 0$ contrary to the given statement $c \neq d \neq 0$. So $\frac{c}{d} = \sqrt{-15}$ but $\frac{c}{d}$ is rational which is a contradiction and $c^2+15d^2 \neq 0$.

The proofs to many of the theorems of $Ra(\sqrt{-15})$ are similar to the proofs of the same theorems of $Ra(\sqrt{3})$. When this is the case the theorem will be stated without proof.

Theorem 2.3: Every number of $Ra(\sqrt{-15})$ satisfies a quadratic equation with rational coefficients.

If $\alpha = a+b\sqrt{-15}$ is any number of $Ra(\sqrt{-15})$, then its conjugate is $\bar{\alpha} = a-b\sqrt{-15}$ and α satisfies the equation

$$(x-a)^2 + 15b^2 = x^2 - 2ax+a^2 + 15b^2 = 0.$$

This equation is called the principal equation of $\alpha = a+b\sqrt{-15}$. The constant term $N(a+b\sqrt{-15}) = a^2+15b^2$ is called the norm of $a+b\sqrt{-15}$ and $N(\alpha) = \alpha\bar{\alpha}$. The negative of the coefficient of x, $T(a+b\sqrt{-15}) = 2a$ is called the trace of $a+b\sqrt{-15}$. Since a and b are rational, a^2+15b^2 and $2a$ are also rational.

The integers of $Ra(\sqrt{-15})$ are the numbers of the field $Ra(\sqrt{-15})$ which will satisfy equations of the form $x^2+px+q = 0$

where p and q are rational integers. These numbers constitute the integral domain $Ra[\sqrt{-15}]$ of $Ra(\sqrt{-15})$.

Theorem 2.4: Every rational integer is in $Ra[\sqrt{-15}]$. Every number of $Ra[\sqrt{-15}]$ which is rational is a rational integer.

Theorem 2.5: The conjugate of a number of $Ra[\sqrt{-15}]$ is in $Ra[\sqrt{-15}]$.

Theorem 2.6: The numbers of $Ra[\sqrt{-15}]$ are given by $a+b\sqrt{-15}$ where a and b are either rational integers or are both halves of odd integers.

Every number $\alpha = a+b\sqrt{-15}$ of $Ra(\sqrt{-15})$ satisfies the principal equation $x^2-2ax+a^2+15b^2 = 0$. The integers of $Ra(\sqrt{-15})$ will satisfy equations of the form $x^2+px+q=0$ where p and q are rational integers. Therefore $2a = p$ $a^2+15b^2 = q$ are rational integers.

If $a+b\sqrt{-15}$ is a number of $Ra(\sqrt{-15})$ then a and b are rational or $\frac{a_1}{c_1} = a$, $\frac{b_1}{c_1} = b$ where a_1, b_1, c_1 are relatively prime rational integers. Then

$$\frac{2a_1}{c_1} = p \quad (1) \quad \text{and} \quad \frac{a_1^2+15b^2}{c_1^2} = q \quad (2) .$$

So $c_1 = 2$ or $c_1 = 1$ for unless $c_1 = 2$ or $c_1 = 1$ by (1) c_1 and a_1 would have a common factor which would also be a factor of b_1 by (2) contrary to our hypothesis that a_1, b_1 and c_1 are relatively prime. If $c_1 = 2$ then by (2) $c_1^2 = 4$ is a factor of $a_1^2 + 15b_1^2$. If a_1 is odd and b_1 is odd then

$$a_1^2+15b_1^2 = (2n+1)^2+15(2m+1) \text{ where } m \text{ and } n \text{ are rational integers}$$

$$= 4n^2+4n+1+60m^2+60m+15$$

$$= 4(n^2+n+15m^2+15m+4) .$$

Therefore if $c_1 =2$ and a_1 and b_1 are odd then $a = \frac{a_1}{2}$ and $b = \frac{b_1}{2}$. If a_1 and b_1 are both even they have a common factor or with c_1 contrary to our hypothesis. If a_1 is odd and b_1 even $a_1^2 + 15b_1^2$ is odd and not divisible by 4. Similarly if a_1 is even and b_1 is odd. If $c_1 = 1$ then $a_1 = a$ and $b_1 = b$ or a and b are rational integers.

The numbers 1 and $\frac{1}{2} + \frac{1}{2}\sqrt{-15}$ form a basis for $Ra[\sqrt{-15}]$. In other words every number of the domain $Ra[\sqrt{-15}]$ is given without repetition in the form $a(1) + b(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ where a and b range independently over all rational integers and conversely every such number is in the domain.

Theorem 2.7 : If 1 and $\frac{1}{2}+\frac{1}{2}\sqrt{-15}$ is a basis of $Ra[\sqrt{-15}]$, every basis of $Ra[\sqrt{-15}]$ is given by $\theta'_1 = a_{11}+a_{12}(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$, $\theta'_2 = a_{21}+a_{22}(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ where

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

Example: Solving the equations given in the general theorem, Theorem 1.7, for θ_1 and θ_2

$$\theta_1 = \pm(a_{22}\theta'_1 - a_{12}\theta'_2)$$

and

$$\theta_2 = \pm(a_{21}\theta'_1 - a_{11}\theta'_2) \ .$$

Therefore if $\theta'_1 = \frac{21}{2}+\frac{5}{2}\sqrt{-15}$, $\theta'_2 = 4+\sqrt{-15}$ is a basis then $\theta_1 = 1$ and $\theta_2 = \frac{1}{2}+\frac{1}{2}\sqrt{-15}$ can be written in terms of it.

i.e. $$1 = [\,2(\frac{21}{2}+\frac{5}{2}\sqrt{-15})-5(4+\sqrt{-15})]$$

$$= [\,21+5\sqrt{-15}-20-5\sqrt{-15}]$$

$$= 1$$

and

$$\begin{aligned}\frac{1}{2}+\frac{1}{2}\sqrt{-15} &= -[3(\frac{21}{2}+\frac{5}{2}\sqrt{-15})-8(4+\sqrt{-15})] \\ &= -[\frac{63}{2}+\frac{15}{2}\sqrt{-15}-32-8\sqrt{-15}] \\ &= -[-\frac{1}{2}-\frac{1}{2}\sqrt{-15}] \\ &= \frac{1}{2}+\frac{1}{2}\sqrt{-15}\ .\end{aligned}$$

So $\theta_1 = 2\theta'_1-5\theta'_2$ and $\theta_2 = -(3\theta'_1-8\theta'_2)$.

<u>Theorem 2.8:</u> The norm of a product is the product of the norms.

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

<u>Theorem 2.9:</u> The norm of a quotient is the quotient of the norms.

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

<u>Theorem 2.10:</u> A number ϵ of $Ra[\sqrt{-15}]$ is a unit if and only if $N(\epsilon) = \pm 1$.

<u>Theorem 2.11:</u> The units of $Ra[\sqrt{-15}]$ are ± 1.

If $\epsilon = a+b\sqrt{-15}$, then $N(\epsilon) = N(a+b\sqrt{-15}) = a^2+15b^2 = +1$ since the norm of $a+b\sqrt{-15}$ is always positive. So this gives the solution $a = \pm 1$, $b = 0$ hence ± 1 are the only units of $Ra[\sqrt{-15}]$.

The definitions concerning prime numbers of $Ra[\sqrt{-15}]$ are identical to those of $Ra[\sqrt{3}]$. Consider the following examples:

Example 1: To determine if $7 + 3\sqrt{-15}$ is prime or composite let

$$7+3\sqrt{-15} = (a+b\sqrt{-15})(c+d\sqrt{-15}) .$$

So

$$N(7+3\sqrt{-15}) = N(a+b\sqrt{-15})N(c+d\sqrt{-15})$$

then

$$94 = (a^2+15b^2)(c^2+15d^2) .$$

$$\text{case i): } \quad a^2+15b^2 = 2 \quad \text{or} \quad \text{case ii) } \quad a^2+15b^2 = 1$$

$$c^2+15d^2 = 47 \qquad\qquad c^2+15d^2 = 94$$

Case i) is impossible since a and b must be rational integers or halves of odd integers. From ii) it follows that $a+b\sqrt{-15}$ is a unit. Hence $7+3\sqrt{-15}$ is a prime in $Ra[\sqrt{-15}]$.

Example 2: To determine whether 15 is prime or composite in $Ra[\sqrt{-15}]$ let $15 = (a+b\sqrt{-15})(c+d\sqrt{-15})$.

Then

$$225 = (a^2+15b^2)(c^2+15d^2) .$$

case i) $a^2+15b^2 = 1$

$c^2+15d^2 = 225$

case ii) $a^2+15b^2 = 3$

$c^2+15d^2 = 75$

case iii) $a^2+15b^2 = 5$

$c^2+15d^2 = 45$

case iv) $a^2+15b^2 = 9$

$c^2+15d^2 = 25$

case v) $a^2+15b^2 = 15$

$c^2+15d^2 = 15$

Case ii) and iii) are impossible since a and b must be rational integers or halves of odd integers. Case i) indicates that $a+b\sqrt{-15}$ is a unit. Case iv) yields a solution $a = \pm 3$, $b = 0$, $c = \pm 5$, $d = 0$ and case v) gives the solution $a = 0$, $b = \pm 1$, $c = 0$, $d = \pm 1$. Hence 15 is composite in $Ra[\sqrt{-15}]$ and $15 = (3)(5) = (\sqrt{-15})(-\sqrt{-15})$. It must now be determined if these factors are prime.

If $3 = (a+b\sqrt{-15})(c+d\sqrt{-15})$ then $9 = (a^2+15b^2)(c^2+15d^2)$

case i) $a^2+15b^2 = 1$

$c^2+15d^2 = 9$

case ii) $a^2+15b^2 = 3$

$c^2+15d^2 = 3$

If $5 = (a+b\sqrt{-15})(c+d\sqrt{-15})$ then $25 = (a^2+15b^2)(c^2+15d^2)$

case i) $a^2+15b^2 = 1$ case ii) $a^2+15b^2 = 5$

$c^2+15d^2 = 25$ $c^2+15d^2 = 5$

If $-\sqrt{-15} = (a+b\sqrt{-15})(c+d\sqrt{-15})$ then $15 = (a^2+15b^2)(c^2+15d^2)$

case i) $a^2+15b^2 = 1$ case ii) $a^2+15b^2 = 3$

$c^2+15d^2 = 15$ $c^2+15d^2 = 5$

For each of these numbers case i) indicates $a+b\sqrt{-15}$ is a unit and case ii) is impossible since a and b must be rational integers or halves of odd integers. Therefore 3, 5 and $-\sqrt{-15}$ are prime in $Ra[\sqrt{-15}]$.

If $\sqrt{-15} = (a+b\sqrt{-15})(c+d\sqrt{-15})$ then $-15=(a^2+15b^2)(c^2+15d^2)$

which is impossible since the norm of $a+b\sqrt{-15}$ and of $c+d\sqrt{-15}$ is always positive and $\sqrt{-15}$ is also prime in $Ra]\sqrt{-15}]$.

Therefore there are two ways to factor 15 into prime factors in $Ra[\sqrt{-15}]$ which illustrates that the property of unique factorization into primes does not exist in this domain.

In order to restore this property of unique factorization to $Ra[\sqrt{-15}]$, we introduce the concept of ideal numbers.

If every pair of numbers of $Ra[\sqrt{-15}]$ not both zero had a g.c.d. expressible linearly in terms of the numbers we could prove unique factorization (see Theorems 1.12, 1.13, 1.14 and 1.15) It is the lack of a g.c.d. which is the fundamental difficulty. An example illustrates.

Consider the set S of positive integers which are $\equiv 1$ modulo 3. This set is closed under multiplication. A number of S may be called prime if it cannot be written as a product of two numbers of S. Factorization into primes is not unique:

$$220 = 55 \cdot 4 = 22 \cdot 10$$

where 55, 4, 22, and 10 are all primes.

The difficulty is due to the absence from S of the other integers. We therefore introduce these missing numbers by using a notation involving only the numbers of S. Let (a, b) denote the g.c.d. of a and b so

$$2 = (4, 22) = (4, 10) \qquad 11 = (55, 22) \quad 5 = (55, 10)$$

Thus $220 = (4, 22)(4, 10)(55, 22)(55, 10)$ is uniquely factored into ideal numbers.

The set of numbers $\alpha\sigma + \beta\eta = \delta$ of $Ra[\sqrt{3}]$ consists exactly of the multiples of δ where δ is the g.c.d. of α and β or in symbols $\delta = (\alpha, \beta)$, α, β, σ and η are integers of $Ra[\sqrt{3}]$. Set up the correspondence $\alpha\sigma + \beta\eta \leftrightarrow (\alpha, \beta)$. The problem is so to define multiplication of sets that this correspondence shall be an isomorphism. In $Ra[\sqrt{-15}]$, two numbers α and β do not necessarily have a g.c.d. The sets $\alpha\sigma+\beta\eta$ where σ and η range independently over $Ra[\sqrt{-15}]$ do exist, however, and are the ideals of $Ra[\sqrt{-15}]$.

An ideal of $Ra[\sqrt{-15}]$ is a set of integral numbers of $Ra[\sqrt{-15}]$ not all 0 which is a group relative to addition, and which is closed under multiplication by all the numbers of $Ra[\sqrt{-15}]$.

Theorem 2.12: In every ideal there exist 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.

These numbers form a minimal basis for the ideal.

Let 1 and $\frac{1}{2}+\frac{1}{2}\sqrt{-15}$ be a basis for $Ra[\sqrt{-15}]$. 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 $\delta = \ell_1+\ell_2(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ in A having $\ell_2 \neq 0$, choose as ω_2 one such in which ℓ_2 is positive and minimal. Let $\alpha = a_1+a_2(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ be any number of A. Write

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

Then

$$\alpha-k_2\omega_2 = (a_1-k_2\ell_1)+r_2(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$$

is in A, and if r_2 were not zero, the definition of ω_2 would be violated. Thus $\alpha - k_2\omega_2 = a_1 - k_2\ell_1 = b$. 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.

Theorem 2.13: If ω_1, ω_2 is a minimal basis for an ideal A in $Ra[\sqrt{-15}]$, every minimal basis is given by

$$\omega_1' = a_{11}\omega_1 + a_{12}\omega_2 \qquad \omega_2' = a_{21}\omega_1 + a_{22}\omega 2 ,$$

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 follows as in Theorem 1.7.

Theorem 2.14: Every ideal A has a minimal basis $k, \ell + r\theta$, 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 $\omega_1 = k$, $\omega_2 = m+r(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ where k was the smallest positive integer in A.

Set

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

The transformation $\omega_1' = \omega_1 = k$, $\omega_2' = \omega_2 - q\omega_1 = \ell+r(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ is of determinant 1, so the result follows from Theorem 2.13.

Theorem 2.15: Every ideal A has a minimal basis of the form $\omega_1 = ra$, $\omega_2 = r(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ where r and a are positive integers, and $0 \leq b < a$. Moreover

$$b^2+b+\frac{1}{4}[1-(-15)] \equiv 0 \quad \text{mod } a$$

$$b^2+b+4 \equiv 0 \quad \text{mod } a \ .$$

Such a basis is called a canonical basis.

Using the notation for Theorem 2.14, since k is in A, $k(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ is in A. Set

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

Then

$$k(\frac{1}{2}+\frac{1}{2}\sqrt{-15}) - a\omega_2 = -a\ell + t(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$$

is in A. This is impossible unless $t = 0$, in which case r divides k. Hence $\omega_1 = ra$, $\omega_2 = \ell + r(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$.

Since $\ell + r(\frac{1}{2}+\frac{1}{2}\sqrt{-15})$ is in A, so is

$$\ell(\frac{1}{2}+\frac{1}{2}\sqrt{-15}) + r(\frac{1}{2}+\frac{1}{2}\sqrt{-15})^2 = \ell(\frac{1}{2}+\frac{1}{2}\sqrt{-15}) + r[(\frac{1}{2}+\frac{1}{2}\sqrt{-15})-4].$$

Set

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

Then

$$r[(\frac{1}{2}+\frac{1}{2}\sqrt{-15})-4]+\ell(\frac{1}{2}+\frac{1}{2}\sqrt{-15}) -(b+1)\omega_2 = -4r+t_1(\frac{1}{2}+\frac{1}{2}\sqrt{-15})-(b+1)\ell$$

is in A so $t_1 = 0$ and r divides ℓ. Hence there is a basis

$$\omega_1 = ra, \quad \omega_2 = r(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15})$$

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

Since $\omega_2(\frac{1}{2}+\frac{1}{2}\sqrt{-15}) - (b+1)\omega_2 = -rb^2-rb-4$ is a rational integer in A, it is divisible by ra by Corollary 2.12. That is

$$b^2+b+4 \equiv 0 \mod a .$$

Example: Consider the ideal $C = (5, \frac{5}{2}+\frac{1}{2}\sqrt{-15})$ with minimal basis $\omega_1 = 5$ and $\omega_2 = \frac{5}{2}+\frac{1}{2}\sqrt{-15}$. Then

$$\omega_1 = 5 = ra$$

and

$$\omega_2 = r(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) = \frac{5}{2}+\frac{1}{2}\sqrt{-15}$$

$$= r(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) = (2+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) .$$

So $r = 1$, $b = 2$ and $a = 5$ and $0 \leq 2 < 5$ and $b^2+b+4 = 10 \equiv 0 \mod 5$. Therefore ω_1, ω_2 is a canonical basis.

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 subtracting these numbers until no new ones are obtained. This set of numbers satisfies the definition of ideal.

For example: 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 $Ra[\sqrt{-15}]$.

If all the numbers of an ideal A are multiples by numbers of $Ra[\sqrt{-15}]$ of one number α, the ideal A is called principal and is written (α).

If every number of an ideal A is replaced by its conjugate, the resulting set is an ideal $\overline{A}$ called the conjugate of A.

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

If

$$A = (\omega_1, \omega_2) \quad \text{and} \quad B = (\chi_1, \chi_2),$$

then

$$\overline{AB} = (\overline{\omega_1\chi_1}, \ \overline{\omega_1\chi_2}, \ \overline{\omega_2\chi_1}, \ \overline{\omega_2\chi_2}),$$

$$\overline{A}\,\overline{B} = (\overline{\omega_1}\,\overline{\chi_1}, \ \overline{\omega_1}\,\overline{\chi_2}, \ \overline{\omega_2}\,\overline{\chi_1}, \ \overline{\omega_2}\,\overline{\chi_2}).$$

Theorem 2.17: If $A = (ra, r(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}))$ then $A\overline{A} = (r^2a)$. The number r^2a is called the norm of A, written N(A).

Proof. The product $A\overline{A}$ consists of all numbers

$$kr^2a^2 + \lambda r^2a(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) + \mu r^2a(b+\frac{1}{2}-\frac{1}{2}\sqrt{-15}) + \nu r^2(b^2+b+4) \tag{1}$$

where k, λ, μ and ν range over all numbers of $Ra[\sqrt{-15}]$. By Theorem 2.15 $c = \frac{b^2+b+4}{a}$ 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

$$k_1 r^2 a^2 + \lambda_1 r^2 a(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) + \nu_1 r^2 a(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) + \lambda_1 r^2 a(b+\frac{1}{2}-\frac{1}{2}\sqrt{-15}) + \mu_1 r^2 (b^2+b+4)$$

$$= k_1 r^2 a^2 + \lambda_1 r^2 a(2b+1) + \mu_1 r^2 ac + \nu_1 r^2 a(b+\frac{1}{2}+\frac{1}{2}\sqrt{-15}) \ . \tag{2}$$

Hence every number of (2) is in (1). The converse is true, since $k_1 = k$, $\lambda_1 = \mu$, $\mu_1 = \nu$, $\nu_1 = \lambda - \mu$.

Let $g = (2b+1, a, c)$. Since $g|a$ and $g|c$, $g^2|ac$ or $b^2+b+4 = ac \equiv 0 \mod g^2$. Since $g|2b+1$, $g^2|4b^2+4b+1$ or $4b^2+4b+1 \equiv 0 \mod g^2$. So

$$b^2+b+4 \equiv 4b^2+4b+16 \equiv (4b^2+4b+1) + 15 \equiv 0 \mod g^2 \ .$$

Therefore $15 \equiv 0 \mod g^2$. Since 15 has no square factor > 1, $g = 1$.

We can then see that the set of numbers

$$k_1 r^2 a^2 + \lambda_1 r^2 a(2b+1) + \mu_1 r^2 ac \tag{3}$$

is the same as the set $\rho r^2 a$. Obviously every number of (3) is in $\rho r^2 a$. Since a, $2b+1$ and c are relatively prime, there exist rational integers p, q, t such that

$$1 = pa + q(2b+1) + tc \ .$$

Multiply through by r^2a. Then

$$r^2a = pr^2a^2 + qr^2a\,(2b+1) + tr^2ac$$

so that every number of ρr^2a is in (3).

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

$$\rho r^2a + \nu_1 r^2a\,(b + \frac{1}{2} + \frac{1}{2}\sqrt{-15}) .$$

But obviously every number of this set is a multiple of r^2a, and conversely, every multiple of r^2a is in the set, with $\nu_1 = 0$. Thus $A\bar{A} = (r^2a)$.

Theorem 2.18: 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 $Ra[\sqrt{-15}]$. Let $s = N(S)$. The numbers of (s) are given by λs. Thus the numbers of $(s)A$ consist of the numbers

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

where η_1, η_2 range over $Ra[\sqrt{-15}]$. Thus every number of

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

If $SA = SB$, then $\bar{S}SA = \bar{S}SB$, and by Theorem 2.17

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

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

$$s\alpha = s\beta, \quad \alpha = \beta,$$

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

If three ideals A, B, C of $Ra[\sqrt{-15}]$ are in the relation $AB=C$, we say that A divides C and B divides C. A and B are called factors of C.

Theorem 2.19: A divides C if and only if every number of C is in A.

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

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

where k, λ, μ, η vary over $Ra[\sqrt{-15}]$. But this can be written in either of two ways.

$$(k\chi_1+\lambda\chi_2)\omega_1+(\mu\chi_1+\eta\chi_2)\omega_2, \qquad (k\omega_1+\mu\omega_2)\chi_1+(\lambda\omega_1+\eta\omega_2)\chi_2$$

so every number of C is in A and also in 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 varies over a certain set B of numbers of the domain. It must now be proven that B is an ideal.

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 $Ra[\sqrt{-15}]$. 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 $\bar{A}C = (a)B = \bar{A}AB$ that

$$C = AB.$$

Theorem 2.20: A positive integer t occurs in but a finite number of ideals.

Let the ideal A containing t have a canonical basis $(ra, rb+r(\frac{1}{2}+\frac{1}{2}\sqrt{-15}))$, 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 2.21: An ideal C is divisible by only a finite number of ideals.

By Theorem 2.17 $C\overline{C} = (c)$, where c is a positive integer. By Theorem 2.19, c is in C and also in every ideal which divides C. By Theorem 2.20, there is but a finite number of such divisors.

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.

An ideal G is called a greatest common divisor of A and B if G divides A and G divides B and if every common divisor of A and B divides G.

Theorem 2.22: 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 $G = K_1G_1$, $G_1 = KG$, so that

$$(1)\, G = K_1KG \quad .$$

Hence

$$K_1K = (1).$$

Since $N(K_1)\cdot N(K) = 1$

$$K_1 = K = (1) .$$

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

<u>Corollary to Theorem 2.22:</u> If A and B are relatively prime, there exists an α in A and a β in B such that $\alpha + \beta = 1$.

<u>Theorem 2.23:</u> If A divides BC and is prime to B, then A divides C.

If A is prime to B then by the corollary to Theorem 2.22

$$\alpha + \beta = 1, \quad \gamma\alpha + \gamma\beta = \gamma$$

for every γ in C. Since A divides BC the number $\gamma\beta$ of BC is in A. So is $\gamma\alpha$, and so therefore is γ. Then A divides C by Theorem 2.19.

Theorem 2.24: Every composite ideal can be factored into prime ideals in one and, except for order of the factors, in only one way.

By Theroem 2.21 every ideal can be factored into a finite number of prime ideals.

Let C be a composite such that

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

where the A's are prime ideals.

Suppose that

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

is a second such representation. Then

$$A_1 A_2 A_3 \cdots A_n = B_1 B_2 B_3 \cdots B_m .$$

Since A_1 is a prime ideal dividing $B_1 B_2 B_3 \cdots B_m$, then by Theorem 2.23 it divides some B_i. Since B_i is also a prime ideal, $A_1 = B_1$. By a rearrangement of the order of the B's if necessary we may assume $A_1 = B_1$. Then since $A_1 \neq 0$

$$A_2A_3 \cdots A_n = B_2B_3 \cdots B_m .$$

As before, A_2 divides one of the remaining B's say B_2, and hence equals it. We proceed in this manner until all the A's or all the B's are exhausted. It is now evident that $n = m$, for otherwise we should have a product of primes equal to 1.

It follows therefore that every ideal C can be written uniquely as a product of prime ideals

$$C = A_1A_2A_3 \cdots A_n .$$

Example: Factor (15) into prime ideals.

$$(15) = (3)(5) = (\sqrt{-15})(-\sqrt{-15})$$

But these are not prime ideals for

$$(3, \sqrt{-15})(3, \sqrt{-15}) = (9, 3\sqrt{-15}, 3\sqrt{-15}, -15), = (3)$$

and

$$(5, \sqrt{-15})(5, \sqrt{-15}) = (25, 5\sqrt{-15}, 5\sqrt{-15}, -15) = (5)$$

$$(3\sqrt{-15})(5, \sqrt{-15}) = (15, 5\sqrt{-15}, 3\sqrt{-15}, -15) = (\sqrt{-15}) = (-\sqrt{-15}) .$$

So

$$(15) = (3, \sqrt{-15})(3, \sqrt{-15})(5, \sqrt{-15})(5, \sqrt{-15}) = (3, \sqrt{-15})^2(5, \sqrt{-15})^2.$$

$(3, \sqrt{-15})$ is a prime ideal, for if this is not the case then two ideals, A and B, neither of which is (1), must exist such that

$$(3, \sqrt{-15}) = AB .$$

Let $A = (\alpha_1, \alpha_2, \cdots, \alpha_m)$, $B = (\beta_1, \beta_2, \cdots, \beta_n)$. Then

$$(3, \sqrt{-15}) = (\alpha_1, \alpha_2, \cdots, \alpha_m)(\beta_1, \beta_2, \cdots, \beta_n).$$

By Theorem 2.19, 3 and $\sqrt{-15}$ are numbers of each of the ideals of A and B and hence

$$(3, \sqrt{-15}) = (\alpha_1, \cdots, \alpha_m, 3, \sqrt{-15})(\beta_1, \cdots, \beta_n, 3, \sqrt{-15}) .$$

Let $\alpha_i = a + b\sqrt{-15}$, be any one of the integers $\alpha_1, \alpha_2, \cdots, \alpha_m$, where a and b are integers or halves of odd integers. If a is a rational integer then a is of the form $3c$, $3c+1$, or $3c-1$ where c is a rational integer. Similarly if a is half of an odd integer it is of the from $3c$, $3c+1$, or $3c-1$ where c is half of an odd integer. We have therefore

1) $\alpha_i = b\sqrt{-15} + 3c$

2) $\alpha_i = b\sqrt{-15} + 3c+1$

3) $\alpha_i = b\sqrt{-15} + 3c-1$.

If 1) is the case α_i may be omitted from the symbol A. If 2) is the case, we have $\alpha_i - b\sqrt{-15} - 3c = 1$ and 1 may be introduced into the symbol of A. All other numbers could then be omitted and we would have $A = (1)$. If 3) is the case, we have $b\sqrt{-15} + 3c - \alpha_i = 1$ and again $A = (1)$.

Proceeding in this manner with each of the numbers $\alpha_1, \alpha_2, \cdots \alpha_m$ we find that either all of the numbers $\alpha_1, \alpha_2, \cdots, \alpha_m$ are linear combinations of 3 and $\sqrt{-15}$ and hence may be omitted from the symbol of A, in which case we have $A = (3, \sqrt{-15})$ or some number of A is not a linear combination of 3 and $\sqrt{-15}$, in which case 1 may be introduced into the symbol of A and $A = (1)$. The same is evidently true for B. We have therefore as the only possible factorization of $(3, \sqrt{-15})$

$$(3, \sqrt{-15}) = (1)(1) = (1) \qquad 4)$$

or

$$= (3, \sqrt{-15})(3, \sqrt{-15}) \qquad 5)$$

or

$$= (1)(3, \sqrt{-15})$$

or

$$= (3, \sqrt{-15})(1) .$$

If 4) is the case then 1 must be a number of the ideal or

$$1 = 3(x+y\sqrt{-15})+\sqrt{-15}(u+v\sqrt{-15}).$$

Thus $1 = 3x-15v$ and $0 = 3y\sqrt{-15}+u\sqrt{-15}$. But if x and v are rational integers or halves of odd integers, $1 = 3x-15v$ is impossible since the second number only is divisible by 3. Hence 1 is not a number of the ideal $(3, \sqrt{-15})$ and $(3, \sqrt{-15}) \neq (1)$ so 4) is impossible.

5) is also impossible for we have previously shown

$$(3, \sqrt{-15})^2 = (9, 3\sqrt{-15}, 3\sqrt{-15}, -15) = (3)$$

but $\sqrt{-15}$ is not a multiple of 3 so $(3, \sqrt{-15}) \neq (3)$.

The only divisors of $(3, \sqrt{-15})$ are therefore the ideal itself and (1). Hence $(3, \sqrt{-15})$ is a prime ideal.

It may be shown similarly that $(5, \sqrt{-15})$ is a prime ideal.

As before if $(5, \sqrt{-15})$ is not a prime ideal then two ideals, A and B, neither of which is (1), must exist such that

$$(5, \sqrt{-15}) = AB.$$

Let $A = (\alpha_1, \alpha_2, \cdots, \alpha_m)$, $B = (\beta_1, \beta_2, \cdots, \beta_n)$.

Then $(5, \sqrt{-15}) = (\alpha_1, \alpha_2, \cdots, \alpha_m)(\beta_1, \beta_2, \cdots, \beta_n)$. By Theorem 2.19 5 and $\sqrt{-15}$ are numbers of each of the ideals A and B and hence

$$(5, \sqrt{-15}) = (\alpha_1, \cdots, \alpha_m, 5, \sqrt{-15})(\beta_1, \cdots, \beta_n, 5, \sqrt{-15}).$$

Let $\alpha_i = a+b\sqrt{-15}$, be any one of the integers $\alpha_1, \alpha_2, \cdots, \alpha_m$, where a and b are integers or halves of odd integers. If a is a rational integer then a is of the form $5c$, $5c+1$, $5c-1$, $5c+2$, or $5c-2$ where c is a rational integer. Similarly if a is half of an odd integer it is of the same form where c is half of an odd integer. We have therefore

1) $\alpha_i = b\sqrt{-15} + 5c$

2) $\alpha_i = b\sqrt{-15} + 5c+1$

3) $\alpha_i = b\sqrt{-15} + 5c-1$

4) $\alpha_i = b\sqrt{-15} + 5c+2$

5) $\alpha_i = b\sqrt{-15} + 5c-2$.

If 1) is the case we find that α_i is a linear combination of 5 and $\sqrt{-15}$ so $A = (5, \sqrt{-15})$. If 2) or 3) is the case 1 may be introduced into the symbol of A and all other numbers omitted and we would have $A = (1)$. If 4) is the case then $\alpha_i - b\sqrt{-15} - 5c = 2$ or $A = (2)$. If 5) is the case $b\sqrt{-15} + 5c - \alpha_i = 2$ so again $A = (2)$. The same is evidently true for B. We have therefore as the only possible factorizations of $(5, \sqrt{-15})$

$(5, \sqrt{-15}) = (1)(1) = (1)$ 6)

$= (2)(2) = (4)$ 7)

$= (1)(2) = (2)$ 8)

$= (2)(1) = (2)$ 9)

$= (2)(5, \sqrt{-15}) = (10, 2\sqrt{-15}) = (2)$ 10)

$= (5, \sqrt{-15})(2) = (10, 2\sqrt{-15}) = (2)$ 11)

$= (5, \sqrt{-15})(5, \sqrt{-15}) = (5)$ 12)

$= (1)(5, \sqrt{-15})$

$= (5, \sqrt{-15})\ (1)$

If 6) is the case then 1 must be a number of the ideal or $1 = 5(x+y\sqrt{-15}) + \sqrt{-15}(u+v(\sqrt{-15})$. Thus $1 = 5x-15v$ and $0 = 5y\sqrt{-15} + u\sqrt{-15}$. But if x and v are rational integers or halves of odd integers, $1 = 5x-15v$ is impossible since the second number only is divisible by 5. Hence 1 is not a number of the ideal and therefore $(5, \sqrt{-15}) \neq 1$. If 7) is the case, then 4 must be a number of the ideal or $4 = 5(x+y\sqrt{-15})+\sqrt{-15}(u+v\sqrt{-15})$. Thus $4 = 5x-15v$ and $0 = 5y\sqrt{-15} + u\sqrt{-15}$. But if x and v are rational integers or halves of odd integers $4 = 5x-15v$ is impossible since the second number only is divisible by 5. So 4 is not a number of the ideal and $(5, \sqrt{-15}) \neq (4)$. Likewise if 8), 9), 10), or 11) is the case, then 2 is a member of the ideal so in the same manner as before $2 = 5x - 15v$ which is impossible since only the second number is divisible by 5. So 2 is not a number of the ideal and $(5, \sqrt{-15}) \neq (2)$. 12) is also impossible for $\sqrt{-15}$ is not a multiple of 5 so $(5, \sqrt{-15}) \neq (5)$.

The only divisors of $(5, \sqrt{-15})$ are therefore the ideal itself and (1). Hence $(5, \sqrt{-15})$ is a prime ideal.

BIBLIOGRAPHY

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

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