

UNIQUE FACTORIZATION IN QUADRATIC FIELDS

Etienne Mahfouz

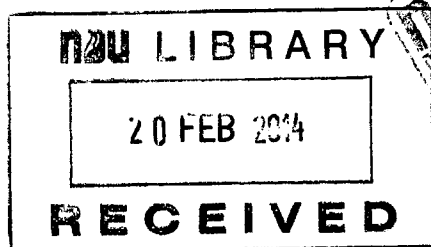
Thesis Advisor: Dr. Ajaj A. Tarabay

THESIS

**Submitted in partial fulfillment of the requirements
for the degree of Masters of Science in Mathematics
in the Department of Mathematics and Statistics in
the Faculty of Natural and Applied Sciences of
Notre Dame University-Louaize**

Lebanon

June 5, 2013



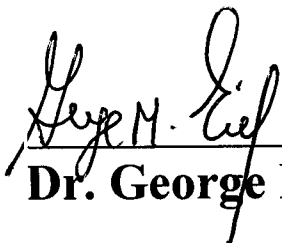
UNIQUE FACTORIZATION IN QUADRATIC FIELDS

Etienne Mahfouz

Approved by:



Dr. Ajaj A. Tarabay



Dr. George M. Eid



Dr. Bassem Ghalayini

Table of Content

Acknowledgement.....	ii
Preliminaries.....	1
Introduction.....	2
Chapter 1: Quadratic Fields.....	3
Chapter 2: Integers in Quadratic Fields.....	6
Chapter 3: Divisibility in Quadratic Fields.....	11
Chapter 4: Units in Quadratic Fields.....	13
Chapter 5: Primes in Quadratic Fields.....	17
Chapter 6: Unique Factorization Domains.....	22
Chapter 7: Euclidean Fields.....	28
Conclusion.....	43
REFERENCES.....	44

Acknowledgement

My thanks and appreciation goes to Dr. Ajaj A. Tarabay, my thesis advisor and my teacher for several graduate math courses. Without his support, this thesis would not have been possible.

Also, I want to thank Dr. George M. Eid, who was my teacher in more than one graduate course, for his encouragement and support throughout the years of my graduate studies at NDU.

I also want to thank the support of the Department of Mathematics and Statistics in the Faculty of Natural and Applied Sciences represented by the Chairperson, Dr. Bassem Ghalayini.

Preliminaries:

We need the following definitions:

- 1) An integral domain is a commutative unitary ring with no zero divisors.
- 2) A principal ideal domain (PID) is an integral domain in which every ideal can be generated by one element.
- 3) A unique factorization domain (UFD) is an integral domain in which factorization of integers into primes is unique. (more details later)
- 4) An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is a defined integer $d(a)$ such that:
 - For all $a, b \in R$, both non zero, $d(a) \leq d(ab)$.
 - For all $a, b \in R$, both non zero, there exists $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.
- 5) A subfield of \mathbb{C} is called a Euclidean field if its set of integers (to be defined later) is a Euclidean ring.
- 6) Let n be an integer. n is said to be square free if n is not divisible by the square of an integer.

Note that:

- a) Every Euclidean ring is a PID, but the converse is false.
- b) Every PID is a UFD, but the converse is false.

Introduction:

In this work Q denotes the field of rational numbers, \mathbb{Z} the set of integers, and \mathbb{C} the set of complex numbers.

A quadratic field is the set of numbers associated with a square free integer $d \notin \{0,1\}$ and given by $Q(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in Q\}$. In this study, we try to determine the complex quadratic fields in which integers have the unique factorization property. For example, the set of integers in $Q(\sqrt{-5})$ is not a UFD, whereas the set of integers in $Q(\sqrt{-1})$ is a UFD. It is well known that every Euclidean ring is a PID, but the converse is false. An example is $Q(\sqrt{-19})$ in which the set of integers is a PID, but not a Euclidean ring. It is also known that every PID is a UFD, but the converse is false. However, in complex quadratic fields every UFD is a PID. Refer to a seminar given by George T. Gilbert, Department of Mathematics, Texas Christian University, November 10, 17, and 29, 2011. We know much less about real quadratic fields than the complex ones. Still, we are able to determine all Euclidean fields and UFDs in the range $2 \leq d < 100$.

I. Quadratic Fields

Definition: Let $d \in \mathbb{Z}$. Suppose d is square free integer. We define $Q(\sqrt{d})$ to be the set $\{ a + b\sqrt{d} : a, b \in Q \}$.

$Q(\sqrt{d})$ is called a quadratic field.

Remarks: 1) If $d > 1$ then $Q(\sqrt{d})$ is called a real quadratic field.

2) If $d < 0$ then $Q(\sqrt{d})$ is called a complex quadratic field.

Example: $Q(\sqrt{2}) = \{ a + b\sqrt{2} : a, b \in Q \}$.

Note that:

- If d is a square free integer then Q is properly contained in $Q(\sqrt{d})$.
- If $\sqrt{d} \in \mathbb{Z}$ then $Q = Q(\sqrt{d})$.

The following properties are easy to prove:

- $a + b\sqrt{d} = c + e\sqrt{d}$ iff $a = c, b = e$
- $a + b\sqrt{d} = 0$ iff $a = b = 0$.
- Let $\alpha, \beta \in Q(\sqrt{d})$ then
 - $\alpha + \beta \in Q(\sqrt{d})$
 - $\alpha - \beta \in Q(\sqrt{d})$
 - $\alpha\beta \in Q(\sqrt{d})$
 - If $\beta \neq 0$ then $\frac{\alpha}{\beta} \in Q(\sqrt{d})$

Thus i), ii) and iii) imply that $Q(\sqrt{d})$ is a subfield of \mathbb{C} .

Conjugates of elements in $Q(\sqrt{d})$

Let $\alpha = a + b\sqrt{d} \in Q(\sqrt{d})$. Then, α is a root of the equation:

$$[x - (a + b\sqrt{d})][x - (a - b\sqrt{d})] = 0 \quad (1).$$

Expanding the left hand side of equation (1) we get:

$$x^2 - 2ax + a^2 - b^2d = 0 \quad (2)$$

This is a quadratic equation with rational coefficients. Multiply equation (2) by the lcm of the denominators of $2a$ and $(a^2 - b^2d)$ to obtain:

$$mx^2 + nx + p = 0 \quad (3) \text{ where } m, n, p \in \mathbb{Z}. \text{ We may assume that } m > 0.$$

Equation (3) is called the defining equation for α .

Let $\bar{\alpha} = a - b\sqrt{d}$. Then, α and $\bar{\alpha}$ are the roots of equation (3). $\bar{\alpha}$ is called the conjugate of α .

Theorem 1: Let $\alpha, \beta \in Q(\sqrt{d})$, then

- a) $\overline{\bar{\alpha}} = \alpha$
- b) $\overline{(\alpha + \beta)} = \bar{\alpha} + \bar{\beta}$
- c) $\overline{(\alpha - \beta)} = \bar{\alpha} - \bar{\beta}$
- d) $\overline{(\alpha\beta)} = \bar{\alpha}\bar{\beta}$
- e) $\overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\bar{\alpha}}{\bar{\beta}}$ where $\beta \neq 0$
- f) $\alpha = \bar{\alpha}$ iff $\alpha \in Q$

Proof: Obvious

Theorem 2: If $d \neq d_1$, then $Q(\sqrt{d}) \cap Q(\sqrt{d_1}) = Q$.

Proof: Let $\alpha \in Q(\sqrt{d}) \cap Q(\sqrt{d_1})$, then $\exists a, b, c, e \in Q$ such that

$$\alpha = a + b\sqrt{d} = c + e\sqrt{d_1}. \text{ Thus } a - c = e\sqrt{d_1} - b\sqrt{d} \text{ and hence}$$

$e\sqrt{d_1} - b\sqrt{d} \in Q$. Since d_1 and d are square free and $d_1 \neq d$, then $e = b = 0$. Therefore, $\alpha = a = c \in Q$. Hence, $Q(\sqrt{d}) \cap Q(\sqrt{d_1}) = Q$.

Definition: Let $\alpha \in Q(\sqrt{d})$. We define the norm of α by $N(\alpha) = \alpha\bar{\alpha}$.

$N(\alpha)$ has the following properties:

- 1) If $a \in Q$, then $N(a) = a^2$.
- 2) If $\alpha \in Q(\sqrt{d})$, then $N(\alpha) \in Q$.
- 3) $N(\alpha) = 0$ iff $\alpha = 0$.
- 4) If $d < 0$, then $N(\alpha) \geq 0$.
- 5) If $\alpha, \beta \in Q(\sqrt{d})$, then $N(\alpha\beta) = N(\alpha)N(\beta)$.
- 6) If $\alpha, \beta \in Q(\sqrt{d})$ and $\beta \neq 0$, then $N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}$.

II. Integers in Quadratic Fields

In this section, we specify the members of $Q(\sqrt{d})$, which we call integers.

Definition: A number $\alpha \in Q(\sqrt{d})$ is called a quadratic integer or simply an integer if either $\alpha \in \mathbb{Z}$ or $\alpha \in Q(\sqrt{d}) - \mathbb{Z}$ and the defining equation of α has leading coefficient 1.

Notation: The integers $z \in \mathbb{Z}$ are called rational integers. The term “integer” means quadratic integer.

Remarks:

- 1) Since α and $\bar{\alpha}$ have the same defining equation then α is an integer iff $\bar{\alpha}$ is an integer.
- 2) The set of integers in $Q(\sqrt{d})$ is closed under addition, subtraction, multiplication. Before proving this we need the following theorem.

Theorem 3:

- If $d \not\equiv 1 \pmod{4}$, then the integers in $Q(\sqrt{d})$ are exactly the numbers $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$.
- If $d \equiv 1 \pmod{4}$, then the integers in $Q(\sqrt{d})$ are of the form $\frac{a}{2} + \frac{b}{2}\sqrt{d}$ where a and b are rational integers both even or both odd.

Proof:

- We show that if α satisfies Theorem 3, then α is an integer.

Suppose $d \not\equiv 1 \pmod{4}$ and $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$.

Then, α satisfies the equation $x^2 - 2ax + a^2 - b^2d = 0$ (1) where $-2a$ and $a^2 - b^2d$ belong to \mathbb{Z} . Therefore, (1) is the defining equation for α . Hence, α is an integer.

Suppose $d \equiv 1 \pmod{4}$ and $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{d}$ where a and b are rational integers both even or both odd. Then, α satisfies the equation

$$x^2 - ax + \frac{a^2 - b^2d}{4} = 0 \quad (2).$$

We show that $\frac{a^2 - b^2d}{4} \in \mathbb{Z}$.

There are two cases a and b are both odd or both even . We prove only the first case . The second is trivial.

If a and b are both odd then $a^2 \equiv 1 \pmod{4}$ and $b^2 \equiv 1 \pmod{4}$.

Hence, $a^2 - b^2d \equiv 0 \pmod{4}$. Thus, $4 \mid a^2 - b^2d$. Therefore

$\frac{a^2 - b^2d}{4} \in \mathbb{Z}$. Hence (2) is the defining equation for α .

Conversely, we show that every integer in $Q(\sqrt{d}) - \mathbb{Z}$ satisfies Theorem 3. Let α be an integer in $Q(\sqrt{d}) - \mathbb{Z}$. Then, α satisfies a quadratic equation $x^2 + bx + c = 0$ where $b, c \in \mathbb{Z}$. There are two cases: b is even, b is odd.

- i) If b is even then $\exists a \in \mathbb{Z}$ such that $b = 2a$.

Then, $\alpha = \frac{-2a \pm \sqrt{4a^2 - 4c}}{2} = -a \pm \sqrt{a^2 - c}$. Let $a^2 - c = e^2 d'$ where d' is square free. Since $\alpha \notin \mathbb{Z}$, then $|d'| \notin \{0,1\}$. Then, $\alpha = -a \pm e\sqrt{d'} = \frac{-2a \pm 2e\sqrt{d'}}{2}$ where $a, e \in \mathbb{Z}$. Then, α satisfies Theorem 3.

ii) If b is odd, then $b^2 \equiv 1 \pmod{4}$. Also $b^2 - 4c \equiv 1 \pmod{4}$. We have $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$. Let $b^2 - 4c = e^2 d'$ where d' is square free. Since $\alpha \notin \mathbb{Z}$, then $|d'| \notin \{0,1\}$. Since b is odd then, $b^2 - 4c$ is odd. Then, e is odd and $e^2 \equiv 1 \pmod{4}$.

Therefore, $d' \equiv e^2 d' \equiv b^2 - 4c \equiv 1 \pmod{4}$.

If $\alpha = \frac{-b \pm e\sqrt{d'}}{2}$ where b and e are both odd rational integers then α is irrational and $\alpha \in Q(\sqrt{d}) \cap Q(\sqrt{d'})$, then $d = d'$.

Therefore, α satisfies Theorem 3.

Corollary:

If $d \equiv 1 \pmod{4}$, then a member of $Q(\sqrt{d}) - \mathbb{Z}$ is an integer iff it can be written as $a + b \frac{(1+\sqrt{d})}{2}$ where $a, b \in \mathbb{Z}$.

Proof:

Suppose that $d \equiv 1 \pmod{4}$. Let $\alpha = a + b \frac{(1+\sqrt{d})}{2} = \frac{(2a+b) + b\sqrt{d}}{2}$

where $a, b \in \mathbb{Z}$. Since $2a + b \equiv b \pmod{2}$,

then $a' = 2a + b$ and $b' = b$ are both even or both odd. Hence,

$\alpha = \frac{a' + b'\sqrt{d}}{2}$ where a' and b' are both even or both odd.

Therefore, by Theorem 3, α is an integer.

Conversely, let $\alpha = \frac{a+b\sqrt{d}}{2}$ be an integer in $Q(\sqrt{d})$ with a and b both even or both odd rational integers.

Then, $\alpha = \frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + \frac{b(1+\sqrt{d})}{2}$. Since a and b are both even or both odd, then $\frac{a-b}{2} \in \mathbb{Z}$.

Theorem 4:

If α and β are integers in $Q(\sqrt{d})$, then $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are integers in $Q(\sqrt{d})$.

Proof:

If $d \not\equiv 1 \pmod{4}$ then

$\alpha = a + b\sqrt{d}$ and $\beta = c + e\sqrt{d}$ where a, b, c and $e \in \mathbb{Z}$. Thus

$\alpha + \beta = (a + c) + (b + e)\sqrt{d}$, $\alpha - \beta = (a - c) + (b - e)\sqrt{d}$, and

$\alpha\beta = ac + bed + (ae + bc)\sqrt{d}$. Therefore, $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are integers in $Q(\sqrt{d})$. If $d \equiv 1 \pmod{4}$, then

$\alpha = a + b\frac{(1+\sqrt{d})}{2}$, $\beta = c + e\frac{(1+\sqrt{d})}{2}$ where $a, b, c, e \in \mathbb{Z}$. Then,

$\alpha + \beta = (a + c) + (b + e)\frac{(1+\sqrt{d})}{2}$ and

$\alpha - \beta = (a - c) + (b - e)\frac{(1+\sqrt{d})}{2}$

Therefore, $\alpha + \beta$ and $\alpha - \beta$ are integers in $Q(\sqrt{d})$. Now

$$\alpha\beta = ac + be\left(\frac{d-1}{4}\right) + (ae + bc + be)\left(\frac{1+\sqrt{d}}{2}\right).$$

Since $d \equiv 1 \pmod{4}$, then $\frac{d-1}{4} \in \mathbb{Z}$. Let $a' = ac + be\left(\frac{d-1}{4}\right)$.

Then, $a' \in \mathbb{Z}$. Let $b' = ae + bc + be$. Then, $b' \in \mathbb{Z}$.

Thus, $\alpha\beta = a' + b'\frac{(1+\sqrt{d})}{2}$ is an integer in $Q(\sqrt{d})$.

Theorem 5:

If α is an integer in $Q(\sqrt{d})$, then $N(\alpha)$ is a rational integer.

Proof:

$N(\alpha) = \alpha\bar{\alpha}$. Since α is an integer, then $\bar{\alpha}$ is an integer.

α and $\bar{\alpha}$ are the roots of an equation $x^2 + bx + c = 0$ with integral coefficients such that $N(\alpha) = \alpha\bar{\alpha} = c \in \mathbb{Z}$.

III. Divisibility in Quadratic Fields

In this section, we extend the theory of divisibility in \mathbb{Z} to the set of integers in $Q(\sqrt{d})$.

Definition: Let α, β be integers in $Q(\sqrt{d})$ with $\alpha \neq 0$. We say that α divides β and write $\alpha | \beta$ if there exists an integer γ in $Q(\sqrt{d})$ such that $\beta = \alpha\gamma$.

Notation: From now on, when we write $\alpha | \beta$ we mean that α and β are integers in $Q(\sqrt{d})$ with $\alpha \neq 0$ and $\frac{\beta}{\alpha}$ an integer in $Q(\sqrt{d})$.

Theorem 6:

- a) $\alpha | \beta$ iff $\bar{\alpha} | \bar{\beta}$.
- b) If $\alpha | \beta$ and $\alpha | \gamma$, then for any integers δ and ε in $Q(\sqrt{d})$,
 $\alpha | (\delta\beta + \varepsilon\gamma)$.
- c) If $\alpha | \beta$ and $\beta | \gamma$, then $\alpha | \gamma$.

Proof:

- a) Suppose $\alpha | \beta$. We show that $\bar{\alpha} | \bar{\beta}$. There exist integers α_1 such that $\beta = \alpha\alpha_1$. Then, $\bar{\beta} = \bar{\alpha}\bar{\alpha}_1$. Since α is an integer, so is $\bar{\alpha}$. Hence, $\bar{\alpha} | \bar{\beta}$.
- b) Suppose $\alpha | \beta$ and $\alpha | \gamma$. We show that $\alpha | (\delta\beta + \varepsilon\gamma)$.

There exist integers α_1 and α_2 such that $\beta = \alpha\alpha_1$ and $\gamma = \alpha\alpha_2$.

Let δ and ε be integers in $Q(\sqrt{d})$. We have: $\delta\beta = \delta\alpha\alpha_1$ and

$\varepsilon\gamma = \varepsilon\alpha\alpha_2$. Then, $\delta\beta + \varepsilon\gamma = \alpha(\alpha_1\delta + \alpha_2\varepsilon)$ where $\alpha_1\delta + \alpha_2\varepsilon$ is an integer. Therefore, $\alpha | (\delta\beta + \varepsilon\gamma)$.

c) Suppose $\alpha | \beta$ and $\beta | \gamma$. We show that $\alpha | \gamma$. There exist

integers α_1 and α_2 such that $\beta = \alpha\alpha_1$ and $\gamma = \beta\alpha_2$. Then,

$\gamma = (\alpha\alpha_1)\alpha_2 = \alpha(\alpha_1\alpha_2)$ where $\alpha_1\alpha_2$ is an integer. Therefore $\alpha | \gamma$.

Remark: Divisibility in $Q(\sqrt{d})$ generalizes divisibility in \mathbb{Z} and has the same basic properties.

Remarks:

- 1) It is well known that if n is a rational positive integer then any two factorizations of n into a product of positive rational primes are identical.
- 2) It is also well known that if n is a nonzero rational integer, then any two factorizations of n into primes are identical except possibly for the order of the primes, or the replacement of some primes by their negatives. In \mathbb{Z} , a number and its additive inverse are called associates.

e.g. $12 = (2)(2)(3) = (-2)(2)(-3) = (3)(2)(2)$

IV. Units in Quadratic Fields

To define factorization in $Q(\sqrt{d})$, we need to define units and associates in $Q(\sqrt{d})$.

Definition: An integer ε in $Q(\sqrt{d})$ is said to be a unit if $\varepsilon|1$. In particular, 1 and -1 are units in $Q(\sqrt{d})$.

Here are some useful facts about units.

Theorem 7:

- a) If ε_1 and ε_2 are units in $Q(\sqrt{d})$, then $\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$ and $\frac{\varepsilon_1}{\varepsilon_2}$ are units in $Q(\sqrt{d})$.
- b) Let ε be an integer in $Q(\sqrt{d})$. Then, ε is a unit iff $N(\varepsilon) = \pm 1$.

Proof:

- a) Suppose ε_1 and ε_2 are units in $Q(\sqrt{d})$. We show that

$\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$ and $\frac{\varepsilon_1}{\varepsilon_2}$ are units in $Q(\sqrt{d})$. Since $\varepsilon_1|1$ then $\overline{\varepsilon_1}|\overline{1} = 1$.

Therefore $\overline{\varepsilon_1}$ is a unit. Suppose there exist integers α_1 and α_2 such that

$1 = \alpha_1\varepsilon_1$ and $1 = \alpha_2\varepsilon_2$. Then $1 = (\alpha_1\varepsilon_1)(\alpha_2\varepsilon_2) = (\alpha_1\alpha_2)(\varepsilon_1\varepsilon_2)$ where $\alpha_1\alpha_2$ is an integer. Hence, $\varepsilon_1\varepsilon_2|1$. Therefore $\varepsilon_1\varepsilon_2$ is a unit.

Now suppose $\varepsilon_2 \neq 0$. Then $\frac{\varepsilon_1}{\varepsilon_2} = \frac{\varepsilon_1\alpha_2}{\varepsilon_2\alpha_2} = \varepsilon_1\alpha_2$. Hence $\frac{\varepsilon_1}{\varepsilon_2}$ is an integer.

Now $\left(\frac{\varepsilon_1}{\varepsilon_2}\right)\varepsilon_2\alpha_1 = 1$ then $\frac{\varepsilon_1}{\varepsilon_2}|1$. Therefore $\frac{\varepsilon_1}{\varepsilon_2}$ is a unit.

- b) Suppose ε is a unit. We show that $N(\varepsilon) = \pm 1$.

There exists an integer α such that $\varepsilon\alpha = 1$. Now

$N(1) = 1 = N(\alpha)N(\varepsilon)$. Since $N(\alpha)$ and $N(\varepsilon)$ are rational integers, then $N(\varepsilon) = \pm 1$. Conversely, suppose ε is an integer such that $N(\varepsilon) = \pm 1$.

We show that ε is a unit. Since $N(\varepsilon) = \pm 1$, then $\varepsilon\bar{\varepsilon} = \pm 1$. Since ε is an integer then $\bar{\varepsilon}$ and $-\bar{\varepsilon}$ are integers. If $\varepsilon\bar{\varepsilon} = 1$ then $\varepsilon|1$. Therefore ε is a unit.

If $\varepsilon\bar{\varepsilon} = -1$. Then, $\varepsilon(-\bar{\varepsilon}) = 1$. Hence $\varepsilon|1$. Therefore, ε is a unit.

Theorem 8:

- a) If $d < 0$ and $d \notin \{-1, -3\}$, then $Q(\sqrt{d})$ has exactly two units: ± 1 .
- b) $Q(\sqrt{-1})$ has exactly 4 units: ± 1 and $\pm\sqrt{-1}$.
- c) $Q(\sqrt{-3})$ has exactly 6 units: $\pm 1, \pm \frac{(-1+\sqrt{-3})}{2}$ and $\pm \frac{(-1-\sqrt{-3})}{2}$.
- d) If $d > 0$, then $Q(\sqrt{d})$ has infinitely many units.

Proof:

- a) i) Suppose $d \leq -2$ and $d \not\equiv 1 \pmod{4}$.

Let α be a unit in $Q(\sqrt{d})$. Then, $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$ and

$N(\alpha) = a^2 - b^2d = 1$. We show that $\alpha = \pm 1$.

Since $-d \geq 2$, we have: $N(\alpha) \geq a^2 + 2b^2$.

If $b \neq 0$, then $b^2 \geq 1$, and $N(\alpha) \geq a^2 + 2 \geq 2$. This is a contradiction.

Hence, $b = 0$. Therefore, $\alpha = a$ and $N(\alpha) = a^2 = 1$. Thus, $\alpha = \pm 1$.

- ii) Suppose $d < -3$ and $d \equiv 1 \pmod{4}$. Then. $d \leq -7$.

Let α be a unit in $Q(\sqrt{d})$. Then, $\alpha = a + b \frac{(1+\sqrt{d})}{2}$ where $a, b \in \mathbb{Z}$ and $N(\alpha) = \left(a + \frac{b}{2}\right)^2 - \frac{b^2 d}{4}$. Since $-d > 7$, we have $N(\alpha) > \left(a + \frac{b}{2}\right)^2 + \frac{7b^2}{4}$.

If $b \neq 0$, then $b^2 \geq 1$. Then, $N(\alpha) > 1$. This is a contradiction.

Hence, $b = 0$. Therefore, $\alpha = a = \pm 1$.

b) Suppose $d = -1$. Since $-1 \not\equiv 1 \pmod{4}$, then $\alpha = a + b\sqrt{-1}$ where $a, b \in \mathbb{Z}$.

Therefore, $N(\alpha) = a^2 - b^2(-1) = a^2 + b^2$. Thus, $a^2 + b^2 = 1$. The only possible choices for a and b are $a^2 = 1$ or $b^2 = 1$. Therefore, either $a = 0$ and $b = \pm 1$ or $a = \pm 1$ and $b = 0$.

Hence, $\alpha = \pm 1$ or $\alpha = \pm\sqrt{-1}$. Therefore, the only units of

$Q(\sqrt{-1})$ are ± 1 and $\pm\sqrt{-1} = \pm i$.

c) Suppose $d = -3$.

Let α be a unit. Then, $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-3}$ where a and b are both even or both odd rational integers. Then, $N(\alpha) = \frac{a^2 + 3b^2}{4} = 1$. Then,

$a^2 + 3b^2 = 4$. If $|b| \geq 2$, then $a^2 + 3b^2 \geq a^2 + 12 \geq 12$. This is a contradiction. Hence, $b = \pm 1$ or $b = 0$.

If $b = 0$, then $a = \pm 2$. Then, $\alpha = \pm 1$.

If $b = 1$, then $a^2 + 3 = 4$. Hence, $a^2 = 1$ and $a = \pm 1$.

Then, $\alpha = \frac{\pm 1 + \sqrt{-3}}{2}$.

If $b = -1$, then $a = \pm 1$. Hence, $\alpha = \frac{\pm 1 - \sqrt{-3}}{2}$.

Therefore, the units of $Q(\sqrt{-3})$ are: $\pm 1, \frac{\pm 1 + \sqrt{-3}}{2}$ and $\frac{\pm 1 - \sqrt{-3}}{2}$.

d) Next, suppose $d > 0$.

We show that there are infinitely many units of the form

$\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$.

Suppose α is a unit of the form $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$ and

$N(\alpha) = 1$. Then, $a^2 - db^2 = 1$. This is the Pell equation

where $\sqrt{d} \notin \mathbb{Q}$. It has infinitely many integral solutions[2].

Therefore $Q(\sqrt{d})$ has infinitely many units.

V. Primes in Quadratic Fields

Definition:

- 1) An integer π in $Q(\sqrt{d})$, which is neither 0 nor a unit, is prime if for every decomposition of π into a product of two integers $\pi = \alpha\beta$, either α or β is a unit.
- 2) An integer α in $Q(\sqrt{d})$ is said to be composite if $\alpha \neq 0$, α is a nonunit, and α is not a prime.

Remarks:

- 1) The primes in \mathbb{Z} are referred to as rational primes.
- 2) An integer $\alpha \neq 0$ is a nonunit iff $|N(\alpha)| \geq 2$.
- 3) A rational prime is not necessarily a prime in $Q(\sqrt{d})$.

Example 1:

In $Q(\sqrt{6})$ the rational prime 5 is no longer a prime because $5 = (1 + \sqrt{6})(-1 + \sqrt{6})$ and $(1 + \sqrt{6}), (-1 + \sqrt{6})$ are both nonzero, nonunits in $Q(\sqrt{6})$.

Theorem 9:

If α is an integer in $Q(\sqrt{d})$ and $N(\alpha)$ is a rational prime, then α is prime.

Proof:

Let α be an integer such that $N(\alpha)$ is a rational prime. Let γ and β be integers such that $\alpha = \gamma\beta$. Since α, β and γ are integers, then $N(\alpha), N(\beta)$ and $N(\gamma)$ are rational integers and $N(\alpha) = N(\beta)N(\gamma)$. Since

$N(\alpha)$ is a rational prime, then $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$. Hence, γ is a unit or β is a unit. Therefore, α is prime.

Example 2:

- 1) If $\alpha = \frac{3}{2} + \frac{1}{2}\sqrt{-163}$, then α is an integer in $Q(\sqrt{-163})$. Now $N(\alpha) = 43$ is a rational prime. Therefore, α is prime in $Q(\sqrt{-163})$.
- 2) If $\alpha = \frac{11}{5} + \frac{2}{5}\sqrt{-1}$, then $N(\alpha) = 5$ is a prime in \mathbb{Z} , but α is not a prime in $Q(\sqrt{-1})$ because α is not an integer.

Remark:

There are cases where α is prime in $Q(\sqrt{d})$, but $N(\alpha)$ is not a rational prime.

Example 3:

7 is prime in $Q(\sqrt{6})$, yet $N(7) = 49$ is not a rational prime.

To prove this, suppose $7 = \alpha\beta$ where α and β are nonunits, nonzero integers in $Q(\sqrt{6})$. Then $N(7) = N(\alpha)N(\beta) = 49$. Since $N(\alpha)$ and $N(\beta)$ are

rational integers of absolute value greater or equal to 2, then

$$|N(\alpha)| = |N(\beta)| = 7.$$

We show that there is no integer in $Q(\sqrt{6})$ whose norm is ± 7 .

Suppose that $\alpha = a + b\sqrt{6}$ with $a, b \in \mathbb{Z}$ is an integer in $Q(\sqrt{6})$ such that $N(\alpha) = a^2 - 6b^2 = \pm 7$. In modulo 7, the equation becomes:

$$a^2 + b^2 \equiv a^2 - 6b^2 \equiv \pm 7 \equiv 0 \pmod{7}.$$

Since 7 is a rational prime such that $7 \equiv 3 \pmod{4}$, then the equation $a^2 + b^2 \equiv 0 \pmod{7}$ has the unique solution $a \equiv b \equiv 0 \pmod{7}$ [1].

Hence, $7|a$ and $7|b$. Therefore $49|a^2$ and $49|b^2$.

Then, $49|(a^2 - 6b^2)$. Therefore, $49|\pm 7$.

This is a contradiction. Therefore, 7 is prime in $Q(\sqrt{6})$.

Definition: If α and β are nonzero integers in $Q(\sqrt{d})$ such that $\alpha = \beta\varepsilon$ where ε is a unit, then α is said to be an associate of β .

For example, 2 and $2i$ are associates in $Q(\sqrt{-1})$.

Theorem 10: Let α and β be integers in $Q(\sqrt{d})$.

- a) α is an associate of β iff β is an associate of α . (α and β are called associates.)
- b) α and β are associates iff $\alpha|\beta$ and $\beta|\alpha$.
- c) If α and β are associates and δ is an integer such that $\alpha|\delta$ then $\beta|\delta$.
- d) α is prime iff every associate of α is prime.

Proof:

- a) Suppose α is an associate of β . Then, there exists a unit ε such that $\alpha = \beta\varepsilon$. Since ε is a unit, then there exists an integer δ such that $\varepsilon\delta = 1$. Then, $\delta\alpha = \delta\beta\varepsilon$. Hence $\beta = \delta\alpha$ where δ is a unit. Therefore, β is an associate of α . It can be shown similarly that α is an associate of β .

b) Suppose α and β are associates. Then, there exist units ε_1 and ε_2 such that $\alpha = \varepsilon_1\beta$ and $\beta = \varepsilon_2\alpha$. Then $\alpha|\beta$ and $\beta|\alpha$. Conversely, Suppose that $\alpha|\beta$ and $\beta|\alpha$. Then, there exist integers δ_1 and δ_2 such that $\alpha = \beta\delta_1$

and $\beta = \alpha\delta_2$. Then, $\beta = \beta\delta_1\delta_2$. Then $\delta_1\delta_2 = 1$. Consequently δ_1 and δ_2 are units. Therefore, α and β are associates.

c) Suppose α and β are associates and δ is integer such that $\alpha|\delta$. We show that $\beta|\delta$. Since $\alpha|\delta$, then there exists an integer δ_1 such that $\delta = \delta_1\alpha$. Since α is an associate of β , then there exists a unit ε_1 such that $\alpha = \varepsilon_1\beta$. Therefore, $\delta = \delta_1\varepsilon_1\beta$. Hence, $\beta|\delta$.

d) Let α be a prime and β an associate of α . We show that β is prime. There exists a unit ε_1 such that $\alpha = \varepsilon_1\beta$. If β is not prime, then there exist two nonzero, nonunit integers β_1 and β_2 in $Q(\sqrt{d})$ such that $\beta = \beta_1\beta_2$. Then, $\varepsilon_1\beta = (\varepsilon_1\beta_1)\beta_2$. Then, $\alpha = (\varepsilon_1\beta_1)\beta_2$. Since $\varepsilon_1\beta_1$ and β_2 are nonzero and nonunits, then α is not prime. This is a contradiction. Therefore, β is prime. Conversely, suppose δ is a composite integer and an associate of α . We show that α is composite. There exists a unit ε such that $\alpha = \varepsilon\delta$. Since δ is composite, then there exist two nonzero, nonunit integers β_1 and β_2 such that $\delta = \beta_1\beta_2$. Thus, $\alpha = \varepsilon\beta_1\beta_2$. We also have $|N(\alpha)| = |N(\delta)| \geq 2$. Therefore, α is not zero, not a unit, and not a prime. Hence, α is composite.

Theorem 11:

If α is not a unit, then α can be written as a product of a finite number of primes in $Q(\sqrt{d})$.

Proof:

Suppose α is a nonzero, nonunit integer in $Q(\sqrt{d})$. We show by induction on $|N(\alpha)|$ that α can be written as a product of finitely many primes.

If $|N(\alpha)| = 2$, then α is a prime and we are done. Suppose theorem 11 holds for all integers α such that $|N(\alpha)| < k$. We show that theorem 11 holds for an integer α such that $|N(\alpha)| = k$.

If α is prime, then we are done. If α is composite, then $\alpha = \alpha_1\beta_1$ where the integers α_1 and β_1 are not units and are such that $|N(\alpha_1)| < |N(\alpha)|$ and $|N(\beta_1)| < |N(\alpha)|$. Since α_1 and β_1 can be written as products of primes, then so can α .

Remark: This theorem shows that every nonzero, nonunit integer in $Q(\sqrt{d})$ can be written as a finite product of primes.

VI. Unique Factorization Domains

Definition: Suppose $Q(\sqrt{d})$ is such that if α is a nonzero, nonunit integer in $Q(\sqrt{d})$ and there are two factorizations of α , say

$\alpha = \varepsilon\pi_1\pi_2 \dots \pi_r$ and $\alpha = \varepsilon'\pi'_1\pi'_2 \dots \pi'_s$ where ε and ε' are units and $\pi_1, \pi_2, \dots, \pi_r, \pi'_1, \pi'_2, \dots, \pi'_s$ are primes not necessarily distinct, then

1) $r = s$

2) The primes $\pi'_1, \pi'_2, \dots, \pi'_s$ can be rearranged in such a way that π_j and π'_j are associates for each $j \in \{1, \dots, r\}$.

Then, we say that the set of integers in $Q(\sqrt{d})$ is a unique factorization domain (UFD).

The following statements are equivalent:

- 1) The set of integers in $Q(\sqrt{d})$ is a UFD .
- 2) $Q(\sqrt{d})$ has the unique factorization property.

The next theorem gives a necessary and sufficient condition for $Q(\sqrt{d})$ to have the unique factorization property.

Theorem 12: The set of integers in $Q(\sqrt{d})$ is a UFD iff $Q(\sqrt{d})$ is such that if $\pi|\alpha\beta$ where π is prime and α, β are integers then, $\pi|\alpha$ or $\pi|\beta$.

Proof:

Necessary Condition:

Suppose the integers in $Q(\sqrt{d})$ form a UFD and suppose

$\pi|\alpha\beta$ where π is prime and α, β are integers. We show that $\pi|\alpha$ or $\pi|\beta$. Since $\pi|\alpha\beta$, there exists an integer δ such that $\alpha\beta = \delta\pi$.

Note that $\alpha\beta$ is not a unit. Otherwise, π would be a unit. Therefore, α and β cannot both be units.

By writing a prime factorization of δ, α and β , we get:

$\delta = \varepsilon\pi_1\pi_2 \dots \pi_n, \alpha = \varepsilon_1\pi'_1 \dots \pi'_r$ and $\beta = \varepsilon_2\pi_1'' \pi_2'' \dots \pi_s''$ where:

- 1) $\varepsilon, \varepsilon_1$ and ε_2 are units.
- 2) $\pi_1, \pi_2, \dots, \pi_n, \pi'_1, \pi'_2, \dots, \pi'_r, \pi_1'', \pi_2'', \dots, \pi_s''$ are primes.
- 3) $n, r,$ and s are natural numbers which might be zero in case δ, α or β is a unit.

If δ is a unit, then $n = 0$ and $\delta = \varepsilon$. Then, $\alpha\beta|\varepsilon\pi$ and hence, $\alpha\beta|\pi$. Since π is prime, then either α or β is a unit.

If α is a unit, then β is not a unit and $\pi = \varepsilon_1\beta$. Therefore π and β are associates. Thus, $\pi|\beta$. Similarly, if β is a unit, $\pi|\alpha$.

If δ is not a unit, then $n \geq 1$. Let $\varepsilon = 1$. We have:

$\alpha\beta = \pi\pi_1\pi_2 \dots \pi_n = \varepsilon_1\varepsilon_2\pi'_1\pi'_2 \dots \pi'_r\pi_1'' \pi_2'' \dots \pi_s''$. Since α and β are not both units, then one of the primes on the right hand side of

the equation say π_i divides π . Hence π and π_i are associates and $\pi|\pi_i$.

If π_i is a factor of α , then $\pi|\alpha$.

If π_i is a factor of β , then $\pi|\beta$.

Sufficient condition:

Suppose $Q(\sqrt{d})$ is such that if $\pi|\alpha\beta$ where π is prime and α, β are integers, then $\pi|\alpha$ or $\pi|\beta$. Suppose α is a nonunit integer in $Q(\sqrt{d})$ such that $\alpha = \varepsilon\pi_1\pi_2 \dots \pi_r = \varepsilon' \pi'_1 \dots \pi'_s$. (1)

We show that $r = s$ and for any $i \in \{1, 2, \dots, r\}$, π_i and π'_i are associates. Either $r \leq s$ or $s \leq r$. We may assume that $r \leq s$. Since π_1 divides α and consequently all associates of α , then $\pi_1 | (\pi'_1 \dots \pi'_{s-1})\pi'_s$. Thus $\pi_1 | \pi'_1 \dots \pi'_{s-1}$ or $\pi_1 | \pi'_s$. If $\pi_1 | \pi'_s$, then π_1 and π'_s are associates. Otherwise $\pi_1 | (\pi'_1 \dots \pi'_{s-2})\pi'_{s-1}$. Similarly, if π_1 and π'_{s-1} are not associates then $\pi_1 | (\pi'_1 \dots \pi'_{s-3})\pi'_{s-2}$. We continue in the same way. Hence, π_1 is an associate of one of the primes $\pi'_1, \pi'_2 \dots \pi'_s$. By renumbering the π'_j s, we prove that π_1 and π'_1 are associates. Thus, $\pi'_1 = \varepsilon_1\pi_1$ where ε_1 is a unit. Hence (1) becomes

$\varepsilon\pi_2 \dots \pi_r = (\varepsilon' \varepsilon_1)\pi'_2 \dots \pi'_s$, where $\varepsilon' \varepsilon_1$ is a unit. We now repeat the process with π_2 and show that π_2 and π'_2 are associates. We repeat the process for all $\pi_i, i \in \{1, 2, \dots, r-1\}$ and we get that π_i and π'_i are associates. Then, (1) becomes $\varepsilon\pi_r = (\varepsilon' \varepsilon_1 \dots \varepsilon_{r-1})\pi'_r \dots \pi'_s$ where $\varepsilon' \varepsilon_1 \dots \varepsilon_{r-1}$ is a unit. If $r < s$, then $\pi'_r \dots \pi'_s$ is a composite number. Hence π_r is a composite number. This is a contradiction. Therefore $r = s$ and $\varepsilon\pi_r = \varepsilon''\pi'_r$ where ε'' is a unit. This completes the proof.

Recall that if a and b are relatively prime positive rational integers such that $ab = c^n$ where c is a positive rational integer, then there exist positive rational integers d and e such that $a = d^n$ and $b = e^n$.

We generalize this theorem to $Q(\sqrt{d})$.

Theorem 13:

Suppose the set of integers in $Q(\sqrt{d})$ is a UFD.

Suppose also that α, β and γ are integers and ε is a unit in $Q(\sqrt{d})$ such that α and β have no common factors other than units.

If $\alpha\beta = \varepsilon\gamma^n$, then there exist units ε' and ε'' and integers δ and ζ in $Q(\sqrt{d})$ such that $\alpha = \varepsilon'\delta^n$ and $\beta = \varepsilon''\zeta^n$.

Proof:

- If γ is a unit, then $\alpha\beta$ is a unit. Thus, α and β are units. In this case the theorem is trivial: We put $\varepsilon' = \alpha, \varepsilon'' = \beta$ and $\delta = \zeta = 1$.
- If $\gamma = 0$, then $\alpha = 0$ or $\beta = 0$. Since every integer in $Q(\sqrt{d})$ divides 0, the only way a unit divide α is that β is a unit and vice versa. The theorem is trivial in this case with one of δ and ζ equal to zero and the other equal to one.
- Thus, we may assume γ is not zero and not a unit. Hence, we may write $\gamma = \pi_1\pi_2 \dots \pi_r$ where $\pi_1, \pi_2, \dots, \pi_r$ are primes some of which may be associates. We show that α is a unit multiplied by an n th power. The proof for β is identical. If α is a unit then set $\varepsilon' = \alpha$ and $\delta = 1$. Thus, we may assume α is not a unit. Since $\gamma \neq 0$ then $\alpha \neq 0$. Hence, we factor α into a product of primes say $\alpha = \pi'_1\pi'_2 \dots \pi'_s$. We get $\pi'_1\pi'_2 \dots \pi'_s\beta = \varepsilon\pi_1^n\pi_2^n \dots \pi_r^n$. By the unique factorization property, π'_1 is an associate of one of the π_j 's and the π_j 's can be renumbered so that π'_1 is an associate of π_1 . Now, if any associate of π_1 divides β , then so do π_1 and π'_1 . Thus, π'_1 divides α and β . This is impossible. Thus, π_1 or its associates must show up n times among the primes $\pi'_1, \pi'_2, \dots, \pi'_s$. By renumbering, if necessary, we

may assume $\pi'_1, \pi'_2, \dots, \pi'_n$ are associates of π_1 . This also means that $s \geq n$.

Hence, there are units $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ such that

$$\pi'_1 = \varepsilon_1 \pi_1, \pi'_2 = \varepsilon_2 \pi_1, \dots, \pi'_n = \varepsilon_n \pi_1 \text{ and thus}$$

$$\pi'_1 \pi'_2 \dots \pi'_n = (\varepsilon_1 \varepsilon_2 \dots \varepsilon_n) \pi_1^n \quad (1).$$

If $s = n$, then we are done since the left hand side of (1) is α . If $s > n$, we divide both sides of (1) by π_1^n and get

$$(\varepsilon_1 \varepsilon_2 \dots \varepsilon_n) \pi'_{n+1} \pi'_{n+2} \dots \pi'_s \beta = \varepsilon \pi_2^n \pi_3^n \dots \pi_r^n \quad (2).$$

We now repeat the above process. By the unique factorization property one of the π_j is an associate of π'_{n+1} . By renumbering, if necessary, we may assume π_2 is an associate of π'_{n+1} . No associate of π_2 divides β , then

π'_{n+1} divides β as well as α . Thus, π_2 or its associates must show up n times among the primes $\pi'_{n+1}, \pi'_{n+2}, \dots, \pi'_s$ and these may be renumbered so that $\pi'_{n+1}, \pi'_{n+2}, \dots, \pi'_{2n}$ are associates of π_2 . It follows from this that

$s \geq 2n$. It also follows that there are units $\varepsilon_{n+1}, \varepsilon_{n+2}, \dots, \varepsilon_{2n}$ such that

$$\pi'_{n+1} = \varepsilon_{n+1} \pi_2, \pi'_{n+2} = \varepsilon_{n+2} \pi_2, \dots, \pi'_{2n} = \varepsilon_{2n} \pi_2 \text{ and thus}$$

$$\pi'_{n+1} \pi'_{n+2} \dots \pi'_{2n} = (\varepsilon_{n+1} \varepsilon_{n+2} \dots \varepsilon_{2n}) \pi_2^n \quad (1). \text{ If } s = 2n, \text{ then}$$

$(\varepsilon_1 \varepsilon_2 \dots \varepsilon_n) (\pi_1 \pi_2)^n$ and we are done. If $s > 2n$, then we divide both sides of (2) by π_2^n and repeat the process a third time. Since there is a finite number of primes in the factorization of α , the repetitions of this process must eventually come to an end. When we have gone through this process k times, we will have found $s = kn$ and we will have reached the π'_s and the π_s and found the units $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{kn}$ such that

$$\alpha = \pi'_1 \pi'_2 \dots \pi'_{kn} = (\varepsilon_1 \varepsilon_2 \dots \varepsilon_{kn}) (\pi_1 \pi_2 \dots \pi_k)^n.$$

This completes the proof.

Theorem 14:

Let a and b be rational integers not both zero such that $\gcd(a, b) = k$.

If α is an integer in $Q(\sqrt{d})$ such that $\alpha|a$ and $\alpha|b$ then $\alpha|k$.

Proof:

If $\gcd(a, b) = k$, then $\exists e, f \in \mathbb{Z}$ such that $k = ea + fb$. Since e and f are rational integers, then they are integers in $Q(\sqrt{d})$. Since $\alpha|a$ and $\alpha|b$, then $\alpha|ea + fb$. Therefore, $\alpha|k$.

Example 4:

We show that the set of integers in $Q(\sqrt{-5})$ is not a UFD.

We have: $21 = (3)(7) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

a) We show that 3 is prime in $Q(\sqrt{-5})$. Suppose $3 = \alpha\beta$ where

$N(\alpha) > 1$ and $N(\beta) > 1$. Since $9 = N(\alpha)N(\beta)$, then

$N(\alpha) = N(\beta) = 3$. If $\alpha = a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$, then

$$N(\alpha) = a^2 + 5b^2 = 3.$$

If $b \neq 0$, then $a^2 + 5b^2 > 3$. This is impossible.

If $b = 0$, then $a^2 = 3$. This is impossible for $a \in \mathbb{Z}$. Hence, 3 is prime in $Q(\sqrt{-5})$.

b) We show that 7 is prime in $Q(\sqrt{d})$. Suppose $7 = \alpha\beta$ where $N(\alpha) > 1$

and $N(\beta) > 1$. If $\alpha = a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$, then

$N(\alpha) = a^2 + 5b^2 = 7$. If $a > 1$ and $b \neq 0$ then $N(\alpha) > 7$. Thus,

$a = 1$ or $b = 0$. If $a = 1$, then $b^2 = \frac{6}{5}$. This is impossible for $b \in \mathbb{Z}$.

If $b = 0$, then $a^2 = 7$. This is impossible for $a \in \mathbb{Z}$. Thus, 7 is prime in $Q(\sqrt{-5})$.

c) We show that $1 \pm 2\sqrt{-5}$ are primes in $Q(\sqrt{-5})$. Suppose

$1 \pm 2\sqrt{-5} = \alpha\beta$ where $N(\alpha) > 1$ and $N(\beta) > 1$. Since

$N(1 \pm 2\sqrt{-5}) = 21 = N(\alpha)N(\beta)$, then $N(\alpha) = 3$ or $N(\beta) = 3$.

This is impossible. Thus, $1 \pm 2\sqrt{-5}$ are primes in $Q(\sqrt{-5})$.

Therefore, the set of integers in $Q(\sqrt{-5})$ is not a UFD.

VII. Euclidean Fields

Definition:

A quadratic field is said to be a Euclidean field if it has the following property:

Given integers α and β in $Q(\sqrt{d})$ with $\beta \neq 0$, there exist integers γ and δ such that $\alpha = \gamma\beta + \delta$ with $|N(\delta)| < |N(\beta)|$ or $\delta = 0$.

Theorem 15:

Let $Q(\sqrt{d})$ be a Euclidean Field. If α and β are integers not both zero then there is an integer δ in $Q(\sqrt{d})$ such that;

- a) $\delta|\alpha$ and $\delta|\beta$.
- b) If γ is an integer such that $\gamma|\alpha$ and $\gamma|\beta$, then $\gamma|\delta$.
- c) An integer δ' has the above two properties iff δ' is an associate of δ .
- d) If δ has properties (a) and (b), then there are two integers ζ and η such that $\delta = \alpha\zeta + \beta\eta$.
 δ is called the greatest common divisor of α and β , and we write $\delta = \gcd(\alpha, \beta)$.

Proof:

Since α and β are not both zero, we may assume $\beta \neq 0$. Since $Q(\sqrt{d})$ is a Euclidean field, then \exists integers δ_1 and β_1 such that $\alpha = \delta_1\beta + \beta_1$ with $|N(\beta_1)| < |N(\beta)|$. If $\beta_1 = 0$, take $\delta = \beta$ and we are done. Otherwise, there are integers δ_2 and β_2 such that

$\beta = \delta_2\beta_1 + \beta_2$ with $|N(\beta_1)| > |N(\beta_2)|$. If $\beta_2 = 0$, take $\delta = \beta_1$ and we are done. Otherwise, there are integers δ_3 and β_3 such that $\beta_1 = \delta_3\beta_2 + \beta_3$ with $|N(\beta_2)| > |N(\beta_3)|$.

Now continuing in this way, we obtain a sequence $\beta_1, \beta_2, \beta_3 \dots$ of integers such that $|N(\beta)| > |N(\beta_1)| > |N(\beta_2)| \dots$

Then, $\{|N(\beta_n)|\}$ is a strictly decreasing sequence of positive rational integers.

Thus, this sequence is finite and has a last term say $|N(\beta_n)|$.

If $\beta_n \neq 0$, then $\exists \beta_{n+1}$ such that $|N(\beta_n)| > |N(\beta_{n+1})|$. This is impossible. Hence, $\beta_n = 0$.

Thus, we get the following n equations:

$$\alpha = \delta_1\beta + \beta_1 \quad (1)$$

$$\beta = \delta_2\beta_1 + \beta_2 \quad (2)$$

$$\beta_1 = \delta_3\beta_2 + \beta_3 \quad (3)$$

.

.

.

$$\beta_{n-4} = \delta_{n-2}\beta_{n-3} + \beta_{n-2} \text{ ---}(n-2)$$

$$\beta_{n-3} = \delta_{n-1}\beta_{n-2} + \beta_{n-1} \text{ ---}(n-1)$$

$$\beta_{n-2} = \delta_n\beta_{n-1} \text{ ---}(n)$$

Let $\delta = \beta_{n-1}$.

Equation (n) implies $\beta_{n-1} | \beta_{n-2}$.

Equation (n - 1) implies $\beta_{n-1} | \beta_{n-3}$.

Equation (n - 2) implies $\beta_{n-1} | \beta_{n-4}$.

By going up from Equation (n) to (1), we get $\delta | \alpha$ and $\delta | \beta$.

Next, we show that δ is a linear combination of α and β .

Equation (n - 1) implies $\beta_{n-1} = \beta_{n-3} - \delta_{n-1}\beta_{n-2}$.

Equation (n - 2) implies $\beta_{n-2} = \beta_{n-4} - \delta_{n-2}\beta_{n-3}$. Replacing β_{n-2} in the first equation, we get

$$\beta_{n-1} = \beta_{n-3} - \delta_{n-1}(\beta_{n-4} - \delta_{n-2}\beta_{n-3})$$

$= -\delta_{n-1}\beta_{n-4} + (1 + \delta_{n-2})\beta_{n-3}$. Therefore, β_{n-1} is a linear combination of β_{n-4} and β_{n-3} . By using equations (n - 2) to (1) in succession, we see that $\delta = \beta_{n-1}$ is a linear combination of α and β . Therefore, there are integers ζ and η such that $\delta = \alpha\zeta + \beta\eta$. Clearly, any divisor of α and β divides δ . Thus, $\delta = \gcd(\alpha, \beta)$.

We still need to prove Property (c):

Note that any associate of δ has Properties (a) and (b).

Conversely, suppose δ' has Properties (a) and (b).

We show that:

δ' is an associate of δ .

We have: $\delta|\alpha$, $\delta|\beta$, $\delta'|\alpha$ and $\delta'|\beta$. By using Property (b) we get $\delta|\delta'$ and $\delta'|\delta$. Hence, δ and δ' are associates. This proves Property (c). Next, we show that δ' is a linear combination of α and β . Since δ and δ' are associates, then there exist a unit ε such that $\delta' = \varepsilon\delta$. Let $\delta = \alpha\zeta + \beta\eta$. Then $\delta' = \alpha(\zeta\varepsilon) + \beta(\eta\varepsilon)$. Hence, δ' can be written as a linear combination of α and β . This completes the proof.

Theorem 16:

A Euclidean quadratic field has the unique factorization property.

Proof:

Let R be the set of integers in the Euclidean field $Q(\sqrt{d})$.

Since R is a Euclidian ring, then R is a PID . Therefore, R is a UFD .

Remark: There are quadratic fields with the unique factorization property which are not Euclidean, for example, the set

$R = \left\{ a + b \frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z} \right\}$ is a PID that is not Euclidean. This will be proved later in Theorems 19 and 22.

Theorem 17:

If $d \in \{-11, -7, -3, -2, -1, 2, 3, 5\}$, then $Q(\sqrt{d})$ is Euclidean.

Proof:

1) Suppose $d \in \{-2, -1, 2, 3\}$. Then, $d \not\equiv 1 \pmod{4}$.

Let α and β be integers in $Q(\sqrt{d})$ with $\beta \neq 0$. Then, $\frac{\alpha}{\beta} = x + y\sqrt{d}$ where $x, y \in Q$.

There exist integers $r, s \in \mathbb{Z}$ such that $|x - r| \leq \frac{1}{2}$ and $|y - s| \leq \frac{1}{2}$.

Let $\gamma = r + s\sqrt{d}$ and $\delta = \beta[(x - r) + (y - s)\sqrt{d}] = \beta\left(\frac{\alpha}{\beta} - \gamma\right) = \alpha - \beta\gamma$. Then $\alpha = \beta\gamma + \delta$. Since $r, s \in \mathbb{Z}$, then γ is an integer in $Q(\sqrt{d})$. Since $\delta = \alpha - \beta\gamma$, then δ is also an integer in $Q(\sqrt{d})$.

$$\begin{aligned} \text{Now } |N(\delta)| &= |N(\beta)| |N[(x - r) + (y - s)\sqrt{d}]| \\ &= |N(\beta)| |(x - r)^2 - d(y - s)^2|. \end{aligned}$$

$$\begin{aligned} \text{But } |(x - r)^2 - d(y - s)^2| &\leq |x - r|^2 + |-d||y - s|^2 \\ &\leq \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1. \end{aligned}$$

The above inequality becomes an equality iff

$$d = 3 \text{ and } |x - r| = |y - s| = \frac{1}{2}.$$

In this case, $|(x - r)^2 - d(y - s)^2| = \left|\frac{1}{4} - 3\left(\frac{1}{4}\right)\right| = \frac{1}{2} < 1$. Thus, for all values of d we have $|(x - r)^2 - d(y - s)^2| < 1$.

Hence, $|N(\delta)| < |N(\beta)|$, proving that $Q(\sqrt{d})$ is Euclidean.

2) Suppose $d \in \{-11, -7, -3, 5\}$, then $d \equiv 1 \pmod{4}$.

Let α and β be integers in $Q(\sqrt{d})$ with $\beta \neq 0$. Then, $\frac{\alpha}{\beta} = x + y\sqrt{d}$ where $x, y \in Q$. There exist $r, s \in \mathbb{Z}$

$$\text{such that } |2y - s| \leq \frac{1}{2} \text{ and } \left|x - \frac{s}{2} - r\right| \leq \frac{1}{2}.$$

Let $\gamma = r + s\frac{(1+\sqrt{d})}{2}$. This is an integer in $Q(\sqrt{d})$ since $d \equiv 1 \pmod{4}$.

Let $\delta = \beta \left[\left(x - r - \frac{s}{2} \right) + \left(y - \frac{s}{2} \right) \sqrt{d} \right] = \beta \left(\frac{\alpha}{\beta} - \gamma \right) = \alpha - \gamma\beta$,

then $\alpha = \gamma\beta + \delta$. Since γ is an integer, then $\delta = \alpha - \gamma\beta$ is also an

integer. Now $|N(\delta)| = |N(\beta)| \left| \left(x - r - \frac{s}{2} \right)^2 - d \left(y - \frac{s}{2} \right)^2 \right|$

$$\leq |N(\beta)| \left(\frac{1}{4} + 11 \left(\frac{1}{16} \right) \right)$$

$$= |N(\beta)| \left(\frac{15}{16} \right) < |N(\beta)|.$$

Hence, $Q(\sqrt{d})$ is Euclidean. Therefore, $Q(\sqrt{d})$ has the unique factorization property.

Theorem 18:

Suppose $d < 0$ then $Q(\sqrt{d})$ is Euclidean iff $d \in \{-11, -7, -3, -2, -1\}$.

Proof:

If $d \in \{-11, -7, -3, -2, -1\}$, then $Q(\sqrt{d})$ is Euclidean by Theorem 17.

We show that if $d < 0$ and $d \notin \{-11, -7, -3, -2, -1\}$, then $Q(\sqrt{d})$ is not Euclidean.

Suppose $d \leq -5$ and $d \not\equiv 1 \pmod{4}$. Let $\alpha = 1 + \sqrt{d}$ and $\beta = 2$ be integers in $Q(\sqrt{d})$. If $Q(\sqrt{d})$ is Euclidean, then there exist integers $\gamma = a + b\sqrt{d}$ and $\eta = c + e\sqrt{d}$ in $Q(\sqrt{d})$ with a, b, c and e rational integers and $N(\eta) < 4$. Now, we have $5 \leq c^2 + 5e^2 < c^2 - de^2 < 4$. This is a contradiction. Therefore, $Q(\sqrt{d})$ is not Euclidean.

Suppose $d \leq -15$ and $d \equiv 1 \pmod{4}$. Let $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{d}$ and $\beta = 2$ be two integers in $Q(\sqrt{d})$. If $Q(\sqrt{d})$ is Euclidean, then there exist integers $\gamma = \frac{a}{2} + \frac{b}{2}\sqrt{d}$ and $\eta = \frac{c}{2} + \frac{e}{2}\sqrt{d}$ in $Q(\sqrt{d})$ with a, b, c and e rational

integers both even or both odd and $N(\eta) < 4$. Now, we have $4 = \frac{1}{4} + \frac{15}{4} \leq \frac{c^2}{4} + \frac{15e^2}{4} \leq \frac{c^2}{4} - \frac{de^2}{4} < 4$. This is a contradiction. Therefore, $Q(\sqrt{d})$ is not Euclidean.

Lemma 1: (Criterion of Dedekind and Hasse)

Let R be an integral domain and f a function from $R - \{0\}$ to \mathbb{Z} satisfying $f(\alpha) > 0$ for $\alpha \neq 0$. Suppose that f satisfies the condition:

If $\alpha, \beta \in R - \{0\}$ such that $f(\beta) \leq f(\alpha)$ then β divides α in R or there exist $s, t \in R$ such that $0 < f(s\alpha - t\beta) < f(\beta)$. Then R is a PID.

Proof:

Let I be a non zero ideal in R . Since $\emptyset \subsetneq f(I) \subset \mathbb{N}$, then by the well ordering principle $f(I)$ has a least element. Thus, we can choose $0 \neq \beta \in I$ such that $f(\beta)$ is minimal. Then, for every $\alpha \in R - \{0\}$, $f(\beta) \leq f(\alpha)$.

If β does not divide α , then there exist $s, t \in R$ such that

$0 < f(s\alpha - t\beta) < f(\beta)$, this is a contradiction. Thus, β divides α . Thus $I = R \cdot \beta$.

This completes the proof.

Theorem 19:

If $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$, then the set of integers in $Q(\sqrt{d})$ is a UFD.

Proof:

If $d \in \{-1, -2, -3, -7, -11\}$, then by theorem 18 $Q(\sqrt{d})$ is Euclidean and thus a UFD.

For $d \in \{-19, -43, -67, -163\}$, we show that $Q(\sqrt{-19})$ is a PID and hence a UFD. For $d \in \{-43, -67, -163\}$, the proof that $Q(\sqrt{d})$ is a PID is much more complicated.

The set of integers of $Q(\sqrt{-19})$ is $R = \left\{a + b \frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\right\}$. We

show that the norm function N from R to \mathbb{Z} satisfies the function f stated in the criterion of Dedekind and Hasse. First, for every

$\alpha \in R - \{0\}$, $N(\alpha) \neq 0$. Second suppose α and β are non zero elements in R such that β does not divide α in R . Hence,

$\frac{\alpha}{\beta} \in Q(\sqrt{-19}) - R$. Since N is multiplicative, the condition

$0 < N(s\alpha - t\beta) < N(\beta)$ is equivalent to $0 < N\left(\frac{\alpha}{\beta}s - t\right) < 1$ (1). To

show that R is a PID it is enough to prove (1) for α and β and for some $s, t \in R$. Since β does not divide α in R , we write

$$\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c} \in Q(\sqrt{-19})$$

with $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b, c) = 1$ and $c > 1$. Then, there exist $x, y, z \in \mathbb{Z}$ such that $ax + by + cz = 1$. We have 4 cases to examine:

Case1: For $c \geq 5$

By the Euclidean division of integers, there exist $q, r \in \mathbb{Z}$ such that $ay - 19bx = cq + r$ and $|r| < \frac{c}{2}$. Let $s = y + x\sqrt{-19}$ and

$$t = q - z\sqrt{-19}, \text{ then } N\left(\frac{\alpha}{\beta}s - t\right) = \left(\frac{r}{c}\right)^2 + 19\left(\frac{1}{c}\right)^2.$$

If $c = 5$, then $r \leq 2$. Hence, $N\left(\frac{\alpha}{\beta}s - t\right) \leq \left(\frac{2}{5}\right)^2 + 19\left(\frac{1}{5}\right)^2 = \frac{23}{25} < 1$.

If $c > 5$, then $N\left(\frac{\alpha}{\beta}s - t\right) \leq \left(\frac{1}{2}\right)^2 + 19\left(\frac{1}{6}\right)^2 < 1$.

In both case $N\left(\frac{\alpha}{\beta}s - t\right) > 0$ since $\frac{\alpha}{\beta}s - t \neq 0$. Thus (1) holds for $c \geq 5$.

Case 2: For $c = 2$

Since $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{-19}}{2} \notin R$, then a and b are of opposite parity. Let $s = 1$ and $t = \frac{a-1+b\sqrt{-19}}{2} = \frac{a-b-1}{2} + b\frac{1+\sqrt{-19}}{2}$.

Since a and b are of opposite parity, then 2 divides $a - b - 1$. Hence, $s, t \in R$ and then $N\left(\frac{\alpha}{\beta}s - t\right) = N\left(\frac{1}{2}\right) = \frac{1}{4} < 1$.

Case 3: for $c = 3$

First, we notice that for all $x \in \mathbb{Z}$, $x^2 \equiv 0 \pmod{3}$ or $x^2 \equiv 1 \pmod{3}$. Then, $a^2 + b^2 \equiv 0 \pmod{3}$ iff $a^2 \equiv 0 \pmod{3}$ and $b^2 \equiv 0 \pmod{3}$ iff $a \equiv 0 \pmod{3}$ and $b \equiv 0 \pmod{3}$. Then $3 | \gcd(a, b, c)$. This is impossible since $\gcd(a, b, c) = 1$. Therefore, $a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod{3}$. Then, there exist $q, r \in \mathbb{Z}$ such that $a^2 + 19b^2 = 3q + r$ such that $r \in \{1, 2\}$. Let $s = a - b\sqrt{-19}$ and $t = 9$, then $N\left(\frac{\alpha}{\beta}s - t\right) = N\left(\frac{r}{3}\right) = \frac{r^2}{9} \in \left\{\frac{1}{9}, \frac{4}{9}\right\}$. Thus, $N\left(\frac{\alpha}{\beta}s - t\right) < 1$.

Case 4: for $c = 4$

Since $\gcd(a, b, c) = 1$, then a and b are not both even. We have two cases:

i) If a is even and b is odd, then

$a^2 + 19b^2 \equiv a^2 - b^2 \not\equiv 0 \pmod{4}$. Then, there exist $q, r \in \mathbb{Z}$ such that $a^2 + 19b^2 = 4q + r$ and $0 < r < 4$. Let $s = a - b\sqrt{-19}$ and $t = q$. Then, $N\left(\frac{\alpha}{\beta}s - t\right) = N\left(\frac{r}{4}\right) = \frac{r^2}{16}$. Therefore (1) holds since $0 < r < 4$. A similar proof is done in the case a is odd and b is even.

ii) If a and b are both odd then $a \equiv \pm 1$ or $\pm 3 \pmod{8}$. Hence $a^2 \equiv 1 \pmod{8}$. Similarly, $b^2 \equiv 1 \pmod{8}$. Thus, $a^2 + 19b^2 \equiv a^2 + 3b^2 \pmod{8} \equiv 4 \pmod{8}$. Then, there exists $q \in \mathbb{Z}$ such that $a^2 + 19b^2 = 8q + 4$. Let $s = \frac{a - b\sqrt{-19}}{2}$ and $t = q$, then $N\left(\frac{\alpha}{\beta}s - t\right) = N\left(\frac{1}{2}\right) = \frac{1}{4}$. This completes the proof.

This proves that N satisfies Lemma 1 and hence R is a PID.

Consequently R is a UFD. Therefore, $Q(\sqrt{-19})$ has the unique factorization property.

Theorem 20:

Suppose $d < 0$ then the set of integers in $Q(\sqrt{d})$ is a UFD iff

$$d \in \{-1, -2, -3, -7, -19, -43, -67, -163\}.$$

The Sufficient condition is proved in theorem 20. The proof of the necessary condition is so lengthy that Stark omitted it from his book "An Introduction to Number Theory" Chapter 8 page 295. We show later that if $d \not\equiv 1 \pmod{4}$ and $d < 0$, then the set of integers in $Q(\sqrt{d})$ is a UFD iff $d \in \{-1, -2\}$. But first, we need the following definition.

Definition:

Let $\mathbb{Z}[\sqrt{d}]$ denote the set of all numbers in $Q(\sqrt{d})$ of the form

$$a + b\sqrt{d} \text{ where } a, b \in \mathbb{Z}.$$

$$\text{i.e. } \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \in Q(\sqrt{d}) : a, b \in \mathbb{Z}\}$$

We note the following assertions whose proof is trivial.

- 1) If $d \not\equiv 1 \pmod{4}$, then $\mathbb{Z}[\sqrt{d}]$ is simply the set of integers in $Q(\sqrt{d})$.
- 2) If $d \equiv 1 \pmod{4}$, then $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is simply the set of integers in $Q(\sqrt{d})$.
- 3) If $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, then $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\sqrt{d}]$.
- 4) Let $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ and $\alpha \neq 0$. We say that α divides β in $\mathbb{Z}[\sqrt{d}]$ if there exist $\delta \in \mathbb{Z}[\sqrt{d}]$ such that $\beta = \delta\alpha$. Equivalently, $\frac{\beta}{\alpha} \in \mathbb{Z}[\sqrt{d}]$.
For example, $2|(1 + \sqrt{5})$ in $Q(\sqrt{5})$ but 2 does not divide $(1 + \sqrt{5})$ in $\mathbb{Z}[\sqrt{5}]$.
- 5) A unit in $\mathbb{Z}[\sqrt{d}]$ is a number that divides 1. Thus, ε is a unit in $\mathbb{Z}[\sqrt{d}]$ iff $N(\varepsilon) = \pm 1$.
- 6) The definition of primes and associates are similar to those in $Q(\sqrt{d})$.
- 7) If $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, then $N(\alpha) = \alpha\bar{\alpha} = a^2 - db^2 \in \mathbb{Z}$.
- 8) If $d > 0$, then $\mathbb{Z}[\sqrt{d}]$ has infinitely many units.
- 9) A nonzero nonunit element of $\mathbb{Z}[\sqrt{d}]$ can be factored into a finite product of primes.
- 10) $\mathbb{Z}[\sqrt{d}]$ is a UFD if factorization into primes is unique up to the order and associates.
- 11) Theorem 14 is valid in $\mathbb{Z}[\sqrt{d}]$. Thus, $\mathbb{Z}[\sqrt{d}]$ is a UFD iff $\mathbb{Z}[\sqrt{d}]$ has the following property:
If $\pi|\alpha\beta$ where π is prime and $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, then $\pi|\alpha$ or $\pi|\beta$.

Theorem 21:

If $\mathbb{Z}[\sqrt{d}]$ is a UFD, then 2 is not prime in $\mathbb{Z}[\sqrt{d}]$.

Proof:

Either d or $(d - 1)$ is even. Then, $2|d(d - 1)$. Now

$$(d + \sqrt{d})(d - \sqrt{d}) = d^2 - d = d(d - 1). \text{ Thus, } 2|(d + \sqrt{d})(d - \sqrt{d})$$

but 2 does not divide neither $(d + \sqrt{d})$ nor $(d - \sqrt{d})$.

Since $\mathbb{Z}[\sqrt{d}]$ is a UFD, then 2 is not prime in $\mathbb{Z}[\sqrt{d}]$.

Theorem 22:

If $d < 0$, then $\mathbb{Z}[\sqrt{d}]$ is a UFD iff $d = -1$ or $d = -2$.

Proof:

We will show that if $d \leq -3$ or $d \equiv 1 \pmod{4}$, then 2 is prime in

$\mathbb{Z}[\sqrt{d}]$. Note that we already know that $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ are UFD's.

Suppose $\mathbb{Z}[\sqrt{d}]$ is a UFD. Then, 2 is not prime in $\mathbb{Z}[\sqrt{d}]$. Then,

there exist $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ such that $2 = \alpha\beta$ and $|N(\alpha)| > 1$

and $|N(\beta)| > 1$.

$N(2) = 4 = N(\alpha).N(\beta)$. Since $N(\alpha)$ and $N(\beta)$ are rational integers of absolute value greater than 1, then $|N(\alpha)| = 2$ $|N(\beta)| = 2$.

Thus, if 2 is not prime in $\mathbb{Z}[\sqrt{d}]$, then there exists

$$\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \text{ such that } N(\alpha) = a^2 - db^2 = \pm 2.$$

Case 1: Suppose $d \leq -3$.

If $b \neq 0$, then $a^2 - db^2 = a^2 + (-d)b^2 \geq 0 + 3(1) = 3 > \pm 2$. This is a contradiction.

If $b = 0$, then $a^2 - db^2 = a^2 = \pm 2$. This is a contradiction since $a \in \mathbb{Z}$.

Case 2: Suppose $d \equiv 1 \pmod{4}$. Thus, $N(\alpha) = a^2 - db^2 = \pm 2$. Thus,

$a^2 - db^2 \equiv a^2 - b^2 \equiv \pm 2 \equiv 2 \pmod{4}$. The square of a number

modulo 4 is either 0 or 1. Then, $a^2 - b^2 \equiv 0, 1 \text{ or } -1 \pmod{4}$. Thus, the equation $N(\alpha) = \pm 2$ has no solution.

Therefore, 2 is prime and $\mathbb{Z}[\sqrt{d}]$ is not a UFD.

Lemma 2:

Let $R = \left\{ a + b \frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z} \right\}$. Then, 2 and 3 are primes in R .

Proof:

a) We show that 2 is prime. Suppose there exist elements α and β in R such that $2 = \alpha\beta$ and $N(\alpha) > 1$ and $N(\beta) > 1$. We have

$4 = N(\alpha)N(\beta)$. Since $N(\alpha)$ and $N(\beta)$ are rational integers greater than 1, then $N(\alpha) = N(\beta) = 2$. There exist $a, b \in \mathbb{Z}$ such that

$\alpha = a + b \frac{1+\sqrt{-19}}{2}$. Then, $N(\alpha) = \left(a + \frac{b}{2} \right)^2 + \frac{19b^2}{4}$. If $b \neq 0$, then

$N(\alpha) > \frac{19}{4}$. This is a contradiction. If $b = 0$, then $N(\alpha) = a^2 = 2$.

This is impossible for $a \in \mathbb{Z}$. Therefore 2 is prime.

b) We show that 3 is prime. Suppose there exist elements α and β in R such that $3 = \alpha\beta$ and $N(\alpha) > 1$ and $N(\beta) > 1$. We have

$9 = N(\alpha)N(\beta)$. Since $N(\alpha)$ and $N(\beta)$ are rational integers greater than 1, then $N(\alpha) = N(\beta) = 3$. There exist $a, b \in \mathbb{Z}$ such that

$\alpha = a + b \frac{1+\sqrt{-19}}{2}$. Then, $N(\alpha) = \left(a + \frac{b}{2}\right)^2 + \frac{19b^2}{4}$. If $b \neq 0$ then

$N(\alpha) > \frac{19}{4}$. This is a contradiction. If $b = 0$, then $N(\alpha) = a^2 = 3$.

This is impossible for $a \in \mathbb{Z}$. Therefore, 3 is prime.

Theorem 23:

The set of integers R in $Q(\sqrt{-19})$ is not a Euclidean Domain.

Proof:

Note that :

1) The set of integers of $Q(\sqrt{-19})$ is $R = \left\{a + b \frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\right\}$

2) The only units in R are ± 1 .

3) 2 and 3 are primes in R .

Suppose there exists a Euclidean function d on R . Choose $m \in R$ such that $d(m)$ is as small as possible and such that m is not a unit and not zero. First, we divide 2 by m and get a quotient $q \in R$ and a remainder $r \in R$:

$2 = mq + r$ with $d(r) < d(m)$ or $r = 0$. Then, $r \in \{0, 1, -1\}$. If $r = 0$, then m divides 2 and hence $m = \pm 2$. Similarly, if $r = -1$, then $m = \pm 3$.

If $r = 1$, then m is a unit and this cannot be. Let $\theta = \frac{1}{2}(1 + \sqrt{-19})$.

Next, we divide θ by m and we get: $\theta = mq' + r'$ with $d(r') < d(m)$ or $r' = 0$. Then, $r' \in \{0, 1, -1\}$. Thus, either $\theta, \theta + 1$ or $\theta - 1$ is divisible by m . This is a contradiction since $m \in \{-2, 2, -3, 3\}$.

For real quadratic fields, we state the following theorem without proof.

Theorem 24:[1]

Let $2 \leq d < 100$. Then,

- a) If $d \in \{14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97\}$, then the set of integers in $Q(\sqrt{d})$ is a UFD but not Euclidean.
- b) $Q(\sqrt{d})$ is Euclidean iff $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

Conclusion:

As a result of this study, we are able to classify the quadratic fields as follows:

- 1) The complex quadratic fields which are Euclidean are the ones that correspond to $d \in \{-11, -7, -3, -2, -1\}$.
- 2) The complex quadratic fields which are PIDs but not Euclidean are the ones that correspond to $d \in \{-19, -43, -67, -163\}$.
- 3) The real quadratic fields which are Euclidean with $2 \leq d < 100$ are the ones that correspond to $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 22, 27, 41, 57, 73\}$.
- 4) The real quadratic fields which are UFDs but not Euclidean with $2 \leq d < 100$ are the ones that correspond to $d \in \{14, 21, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93, 94, 97\}$.

The problem of finding all real quadratic fields which are UFDs is still wide open.

References:

- [1] “An Introduction to Number Theory” by Harold M. Stark. Published by Markham publishing company, Chicago, 1970.
- [2] “An Introduction to the Theory of Numbers” 5th edition by Ivan Niven, H.S. Zuckerman, and H.L. Montgomery. Published by John Wiley and sons, 1991.
- [3] “An Introduction to the Theory of Numbers” 5th edition by G.H. Hardy and E.M. Wright. Published by Oxford University press, 1985.
- [4] George T. Gilbert, Seminar on Unique Factorization and Class Groups, Texas Christian University, November 2011.