KTH Royal Institute of Technology

Department of Mathematics

Bachelor Thesis, SA104X

On Integers, Primes and Unique Factorization in Quadratic Fields

Author:
Alice Hedenlund

Supervisor:
Dan Laksov

May 18, 2013

Abstract. This thesis will deal with quadratic fields. The problem is to study such fields and their properties including, but not limited to, determining integers, finding primes and deciding which quadratic fields have unique factorization. The goal is to get familiar with these concepts and to provide a starting point for students with an interest in algebra to explore field extensions and integral closures in relation to elementary number theory. The reader will be assumed to have a basic knowledge in algebra and familiar with concepts such as groups, rings and fields. The necessary background material is covered in for example *A First Course In Abstract Algebra* by John B. Fraleigh. Some familiarity with basic number theory may be helpful, but not necessary for the scope of this thesis. The questions posed in this thesis was answered by means of literature and discussions with fellow students and my supervisor.

The first four sections will deal with basic concepts in algebra such as algebraic numbers, algebraic integers and prime numbers. This knowledge will then be applied to the subject of quadratic fields. The thesis is concluded with two sections about important cases of quadratic fields, Gaussian and Eisenstein.

Contents

1. Algebraic Numbers

In this first section we will explore some basic theory about algebraic numbers and algebraic field extensions. The section will not go into much detail, but focus on concepts that will help us in the upcomming sections. The reader looking for a more detailed study might want to refer the chapter "Algebraic Extensions" in *Algebra* by Serge Lang [5].

1.1. Algebraic Elements.

The concept of algebraic elements is something that the reader should be familiar with, but as it is of such importance we will begin by a quick repetition of the definition.

Definition 1.1. Let F be a subfield of E. An element $\alpha \in E$ is said to be **algebraic** over F if it is a solution for some non-zero polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} \cdots + a_1 x + a_0 = 0$$

for some $a_i \in F$ and where n is a positive integer. If α is not algebraic over F, we call it **transcendental** over F.

Definition 1.2. An element $\alpha \in \mathbb{C}$ is called an **algebraic number** if it is algebraic over $\mathbb{Q}$. Similary, if α is transcendental over $\mathbb{Q}$ it is called an **transcendental number**.

We continue with a couple of examples to illustate the difference between algebraic and transcendental numbers.

Example 1.3. The number $\sqrt{2}$ is an algebraic number since it is a zero of $x^2 - 2$. In the same way, i is a root of $x^2 + 1$, and is thus an algebraic number.

Example 1.4. The real numbers π and e are examples of transcendental numbers. However, the proof is not easy and beyond the scope of this thesis. For the full proof please refer to *Introduction of the Theory of Numbers* by G. Hardy and E. Wright [3].

We complement our terminology with a few qualities connected with algebraicity.

Definition 1.5. Let E be a field extension of F and let $\alpha \in E$ be algebraic over F. The polynomial with the smallest degree $f(X) \in F[X]$ such that $f(\alpha) = 0$ is called the **irreducible polynomial** of α over F and is denoted $\mathrm{Irr}(\alpha, F)$.

Observe that since F is a field we can easily normalize $f(X)$ so that it has a leading coefficient equal to 1. We will later see that the degree of the irreducible polynomial is closely connected to the dimension of the vectorspace of E over F, which we denote $[E : F]$.

Definition 1.6. The **degree** of α over F, denoted $\deg(\alpha, F)$ is defined as the degree of $\mathrm{Irr}(\alpha, F)$.

Example 1.7. The element $\rho = \frac{1}{2}(-1+\sqrt{3})$ has the irreducible polynomial $X^2 + X + 1$ and is thus of degree 2.

Example 1.8. The polynomial $X^4 - 2X^2 + 2$, which is irreducible by the Eisenstein critierion [2, p. 215] with $p = 2$, has the root $\sqrt{2+\sqrt{2}}$ which is therefore an algebraic number of degree 4.

Definition 1.9. Let E be a finite field extension of F. Let $\alpha \in E$ and consider the F-linear function $T_\alpha(\beta) = \alpha\beta$. We define the **field norm** as $N_{E/F}(\alpha) = \det T_\alpha$

1.2. **Algebraic Extensions.** We continue our study of algebraicity by looking into algebraic extensions. Algebraicity is an important property when it comes to field extensions, and algebraic extensions share a number of important qualities. We begin with a couple of definitions.

Definition 1.10. Let F be a subfield of E. If every element of E is algebraic over F, we simply say that E is **algebraic**.

Definition 1.11. We call K a **number field** if it is a finite extension of $\mathbb{Q}$.

We will continue with deriving a few propositions that will help us in the upcomming sections.

Proposition 1.12. *Let α be algebraic over F. Then the dimension $[F(\alpha) : F]$ is equal to $\deg(\alpha, F)$.*

Proof. Let $\deg(\alpha, F) = n$. We need to show that the powers $1, \alpha, \ldots \alpha^{n-1}$ are linearly independent over F. Assume the contrary. Then

$$a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some combination of $a_i \in F$, not all zero. Let

$$f(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

Since $f(\alpha) = 0$ it must be true that $\mathrm{Irr}(\alpha, F)|f(X)$ which is a contradiction. Hence, the elements $1, \alpha, \ldots, \alpha^{n-1}$ form a base of $F(\alpha)$ over F and $[F(\alpha) : F] = n$. □

Proposition 1.13. *If E is finite as a vector space over F, then E is algebraic over F.*

Proof. Let $[E : F] = n$ and take an arbitrary element $x \in E$. We know that any set of $n + 1$ elements in E are F-linearly dependent. Therefore the elements $1, x, x^2, \ldots, x^n$ are linearly dependant and we can find elements $a_i \in F$, not all zero, such that

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

which shows that x is algebraic over F. Since x was arbitrary we can conclude that E is algebraic over F. □

It is not true that all algebraic extensions are finite. An example is the set of algebraic numbers, which is an infinite extension of the rational numbers. Because of this, the set of algebraic numbers does not constitute a number field.

Proposition 1.14. *Let E be an extension field of F. The element $\alpha \in E$ is algebraic over F if and only if $F[\alpha] = F(\alpha)$.*

Proof. Let $f(X) \in F[X]$ be the smallest polynomial such that $f(\alpha) = 0$ and let $g(X) \in F[X]$ be such that $g(\alpha) \neq 0$. Then $f(X) \nmid g(X)$ and by the Euclidean algorithm [1, p. 307] there are $p(X)$ and $q(X)$ such that

$$f(X)p(X) + g(X)q(X) = 1$$

This means that $g(\alpha)q(\alpha) = 1$, from which can conclude that $g(\alpha)$ is invertible.
Conversely, assume that $F[\alpha] = F(\alpha)$. This means that $\alpha^{-1} \in F[\alpha]$, i.e.

$$\alpha^{-1} = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

for some $a_i \in F$. If we multiply with α we get

$$1 = a_0\alpha + a_1\alpha^2 + \cdots + a_n\alpha^{n+1}$$

substracting -1 from both sides shows us that α is algebraic. □

Specifically, this show us that inverses of algebraic numbers are algebraic numbers themselves. Finally, we will conclude this chapter with showing that algebraic numbers are closed under addition and multiplication.

Proposition 1.15. *If x and y are algebraic numbers, then $x + y$ and xy are also algebraic numbers.*

Proof. Let x, y be algebraic numbers. Then

$$x^m = a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$
$$y^n = b_{n-1}y^{n-1} + \cdots + b_1y + b_0$$

for some combination of $a_i \in \mathbb{Q}$ and $b_j \in \mathbb{Q}$ and for some positive integers m and n. Hence, we can view x^m as a linear combination of $x^{m-1}, \ldots, x, 1$. Consider a power of x greater than m, say x^{m+p}. We want to show that this power also can be written as a linear combination of $x^{m-1}, \ldots, x, 1$ for all positive integers p. We do this by induction on p. The case $p = 0$ is trivial. Assume that it is true for x^{m+p}, then it suffices to show that it is also true for x^{m+p+1}. Say

$$x^{x+p} = a'_{m-1}x^{m-1} + \cdots + a'_1x + a'_0$$

Then for x^{m+p+1}

$$x^{m+p+1} = xx^{m+p} = x(a'_{m-1}x^{m-1} + \cdots + a'_1x + a'_0) =$$
$$a'_{m-1}x^m + \cdots + a'_1x^2 + a'_0x =$$

$$a'_{m-1} \cdot (a_{m-1}x^{m-1} + \cdots + a_1x + a_0) + \cdots + a'_1x^2 + a'_0x =$$

$$(a'_{m-1}a_{m-1})x^{m-1} + \cdots + (a'_{m-1}a_1 + a_0)x + a'_{m-1}a_0$$

Hence, x^{m+p+1} can also be written as a linear combination of $x^{m-1}, \ldots, x, 1$, and we can conclude that all powers of x greater or equal to m can be written as a linear combination of $x^{m-1}, \ldots, x, 1$. With the same argument all, powers of y higher than n can be written as a linear combination of $y^{n-1}, \ldots, y, 1$. Let

$$A = \text{span}\{1, x, x^2, \ldots, x^{m-1}\}$$

and

$$B = \text{span}\{1, y, y^2, \ldots, y^{n-1}\}$$

Consider now the space

$$C = \text{span}\{1, (x+y), (x+y)^2, \ldots\}$$

Expanding the different powers of $(x+y)$ yield terms on the form x^iy^j. We replace all powers of x to m or greater,and y to n or greater, with the appropiate linear combination. This means that

$$C \subseteq \text{span}\{1, x, y, x^2, xy, y^2, \ldots, x^{m-1}y^{n-1}\}$$

Hence it suffices with mn vectors to span C, and it follows that the vectors in the set $\{1, (x+y), (x+y)^2, \ldots\}$ are lineary dependant. Hence

$$c_p(x+y)^p + \cdots + c_1(x+y) + c_0 = 0$$

for some $c_k \in \mathbb{Q}$ and integer p, which is the same as saying that $x+y$ is algebraic.
To prove that xy is algebraic, consider instead the space spanned by $\{1, (xy), (xy)^2, \ldots\}$. By repeating the argument above and replacing powers of x and y with appropiate linear combination it is easy to see that the vectors of this set are linearly dependant which implies that xy is algebraic. □

Theorem 1.16. *The set of algebraic numbers form a field.*

Proof. Proposition 1.15 gives us that the set of algebraic numbers are closed under addition and multiplication, while Proposition 1.14 shows us that inverses are algebraic. □

2. Algebraic Integers

In the previous chapter we considered algebraic field extensions. Now we will study ring extensions, in the hope of expanding the concept of integers. We will try to find a way to define integers in an arbitrary number field. Observe that all rings are assumed to be commutative in this section.

Definition 2.1. Let A be a subring of B. An element $\alpha \in B$ is called **integral** over A if it is a solution to some non-zero polynomial equation

$$x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0 = 0$$

where $a_i \in A$ and n is a positive integer.

Definition 2.2. The number $\alpha \in \mathbb{C}$ is called an **algebraic integer** if it is a solution for some polynomial equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $a_i \in \mathbb{Z}$ and n is a positive integer.

From the definition it is clear that α is integral over $\mathbb{Z}$ if and only if α is an algebraic integer. Our goal is to show that the algebraic integers are closed under addition and multiplication. At first glance one might think that the proof is the same as for the algebraic numbers. However, the problem lies in the vectorspace-assumption. Unfortunately, polynomials over $\mathbb{Z}$ do not form a vectorspace since $\mathbb{Z}$ is not a field. Hence, we will have to introduce some new concepts that will help us avoid the vectorspace assumption.

Definition 2.3. Let A be a ring. An **A-algebra** is a ring B together with a ring homomorphism $\varphi : A \to B$. When it is clear from the context which homomorphism we are refering to, we simply say that B is an A-algebra.

Example 2.4. Every unital ring A is a $\mathbb{Z}$-algebra under the homomorphism that that maps $n \in \mathbb{Z}$ to $n1$, that is the sum of the unit $1 \in A$ with itself n times.

Example 2.5. $A[\alpha_1, \ldots, \alpha_n]$ is an A-algebra under the homomorphism that simply maps $a \in A$ to $a \in A[\alpha_1, \ldots, \alpha_n]$.

Definition 2.6. Let B be an A-algebra. We call B a **finitely generated A-module** if

$$B = Ab_1 + \cdots + Ab_m$$

for some $b_i \in B$.

Theorem 2.7. *The number α is integral over A if and only if $\alpha \in B$ where B is an finitely generated A-module.*

Proof. Assume that α is integral over A. Then α is the root of some monic polynomial $f(x) \in A[X]$ of a finite degree n. Consider $A[\alpha]$ which is an A-algebra which contains α. We need to prove that $A[\alpha]$ is finitely generated. Every element of $A[\alpha]$ is on the form $g(\alpha)$ for some polynomial $g(x) \in A[X]$. Using the division algorithm for polynomials gives

$$g(x) = f(x)q(x) + r(x)$$

where degree of $r < n$. Since $f(\alpha) = 0$ this means that

$$g(\alpha) = r(\alpha)$$

This gives that every element of $A[\alpha]$ can be written as a A-linear combination of powers of α smaller than n, i.e as a A-linear combination of $\alpha^{n-1}, \ldots, \alpha, 1$. Hence $A[\alpha]$ is a finitely generated A-algebra. Conversely, assume that B is a finitely generated A-module. Take an element $z \in B$. Then it is true that

$$z = a_1 b_1 + \cdots + a_n b_n$$

for some elements $a_i \in A$ and $b_j \in B$. Consider the elements

$$\begin{aligned} zb_1 &= a_{11}b_1 + \cdots + a_{1n}b_n \\ zb_2 &= a_{21}b_1 + \cdots + a_{2n}b_n \\ &\vdots \\ zb_n &= a_{n1}b_1 + \ldots a_{nn}b_n \end{aligned}$$

Substacting from the right hand side gives

$$\begin{aligned} (z - a_{11})b_1 - a_{12}b_2 - \cdots - a_{1n}b_n &= 0 \\ -a_{21}b_1 + (z - a_{22})b_2 - \cdots - a_{2n}b_n &= 0 \\ &\vdots \\ -a_{n1}b_1 - a_{n2}b_2 - \cdots + (z - a_{nn})b_n &= 0 \end{aligned}$$

which can be written in matrix form as

$$\begin{pmatrix} z - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & z - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & z - a_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Using Cramer's Rule [5, p. 513] to calculate the solution

$$b_i \begin{vmatrix} z - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & z - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & z - a_{nn} \end{vmatrix} = 0$$

We are looking for a non-trivial solution. Let us call the deteminant above d. Since $1 \in B$ we have that $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_i \in A$. Therfore, $d = d \cdot 1 = \sum_{i=1}^{n} a_i d b_i = 0$. Expanding the determinant gives an expression on the form

$$z^n + c_{n-1}z^{n-1} + \cdots + c_1 z + c_0 = 0$$

where $c_i \in A$, which is the same as saying that z is integral over A. □

We directly use the result to show that algebraic integers are closed under addition and multiplication.

Theorem 2.8. *If x and y are algebraic integers, then $x + y$ and xy are also algebraic integers.*

Proof. Let x and y be algebraic over $\mathbb{Z}$. It follows from Proposition 2.7 that $x, y \in B$ where B is a finitely generated $\mathbb{Z}$-algebra. We will show that we can take $B = \mathbb{Z}[x, y]$. The set B is closed under addition and multiplication and hence $x + y \in B$ and $xy \in B$. This is equivalent to saying that $x + y$ and xy are integral over $\mathbb{Z}$. □

Now it makes sense to define integral closures, that is the set of integers, as follows.

Definition 2.9. Let $A \subseteq B$. The set of elements in B that are integral over A are called the **integral closure of A in B**.

Example 2.10. The ring $\mathbb{Z}[\sqrt{3}]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{3}]$, but the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{5}]$. In section 5 we will study these kind of integral closures in detail.

3. Prime Numbers

After defining integers it makes sense to divide them into primes and composite numbers. In this section we will make sense of these concepts in an abstract setting.

Definition 3.1. An element $\epsilon \in A$ is called a **unit** if ϵ is invertible in A, that is $\epsilon\delta = 1$ for some $\delta \in A$.

Example 3.2. The units of $\mathbb{Z}$ are ± 1.

Example 3.3. The units of the ring $\mathbb{Z}_{12}$ are 1, 5, 7, 11, since

$$1 \cdot 1 = 5 \cdot 5 = 7 \cdot 7 = 11 \cdot 11 = 1$$

Definition 3.4. The two elements $\alpha, \beta \in A$ are called **associates** in A if $\alpha = \beta\epsilon$ where ϵ is a unit in A.

Example 3.5. The elements 2 and 10 are associates in $\mathbb{Z}_{12}$ since $2 \cdot 5 = 10$ where 5 is a unit by Example 3.3.

We continue by defining irreducible elements and primes.

Definition 3.6. Let D be an integral domain. An element $p \in D$ is called an **irreducible** if $p = ab$ where $a, b \in A$ implies that a or b is a unit.

Definition 3.7. Let D be an integral domain. An element $p \in D$ is called a **prime** if $p|ab$ implies that $p|a$ or $p|b$.

Example 3.8. When deciding if an element is prime one must take into consideration in which ring we are looking at. For example, 2 is a prime in $\mathbb{Z}$. However, 2 is not a prime in $\mathbb{Z}[i]$ since $2 = (1 + i)(1 - i)$.

Proposition 3.9. *Let D be an integral domain and let $p \in D$ be prime. Then p is irreducible.*

Proof. Let p be prime and let $p = ab$. Then $p|ab$ which implies $p|a$ or $p|b$. Without loss of generality we can assume that $p|a$. This means that $a = cp$ for some $c \in D$. Hence, we have that $p = cpb$ which implies $1 = bc$ meaning that b and c are units. This gives that p is irreducible. □

4. Factorization

When having dealt with prime numbers a natural continuation is to explore the subject of factorization. In this section we will study the theory behind the concept of unique factorization and division algorithms.

4.1. **UFDs and PIDs.** An important property of the integers is that every element can be written as a product of primes in a unique way. Since this is such a fundamental quality it is something that can easily be taken for granted. However, to able to apply unique factorization on other domains it is important that we take our time to understant what unique factorization is really about.

Definition 4.1. A domain is called a **unique factorization domain (UFD)** if every non-zero element can be written as a product of prime elements in a unique way up to permutations of the primes and ambiguity relating to associates and units.

Definition 4.2. A **principal ideal domain (PID)** is a domain in which every ideal is principal, i.e. generated by a single element.

The goal of this section is to prove that every PID is a UFD. We do this with the help of a couple of lemmas.

Lemma 4.3. *Let A be a commutative ring and let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals. Then the union $I = \bigcup_i I_i$ is itself an ideal of A.*

Proof. Let $a \in I$ and let $b \in A$. We want to show that $ab \in I$. Since $a \in I$ and $I = \bigcup_i I_i$ there must be I_n such that $a \in I_n$. Since I_n is an ideal in A we know that $ab \in I_n$, which implies that $ab \in I$. □

Lemma 4.4. *Let D be a PID. If $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is an ascending chain of ideals, then there exists an integer n such that $I_n = I_m$ for all $m \geq n$. That is, all such chains are of finite length.*

Proof. We know that $I = \bigcup_i I_i$ is an ideal in D. Since D is a PID we know there is an element $a \in D$ such that $I = (a)$. Since I a union of ideals, there must be a set I_n such that $a \in I_n$. Now, for $m \geq n$ we have

$$(a) \subseteq I_n \subseteq I_m \subseteq I = (a)$$

which means that $I_n = I_m$ for all $m \geq n$. □

For the moment we forget about uniqueness and prove that a factorization into primes is possible in a PID.

Proposition 4.5. *Let D be a PID. Every non-zero and non-unit element can be written as a product of primes.*

Proof. Let $a_0 \in D$ be an element that is non-zero and not a unit. If a_0 is a prime, we are done. If not then a_0 can be written as $a_0 = b_1 a_1$ where neither a_1 or b_1 are units. Considering the ideals generated by a_0 and a_1 we see that

$$(a_0) \subset (a_1)$$

Continuing this procedure gives us a chain of ideals

$$(a_0) \subset (a_1) \subset (a_2) \subset \dots$$

which we kow is of finite length by Lemma 4.4. Say it ends with $I_n = (a_n)$. Since a_n is a prime we rename it p_1. Hence, we know that $a_0 = b_1 p_1$ for some $b_1 \in D$. If b_1 is not a prime we can write $b_1 = b_2 p_2$ for some non-unit $b_2 \in D$ and prime p_2. Repeating this process to create an ascending chain of ideals

$$(a_0) \subset (b_1) \subset (b_2) \subset \dots$$

which we know is of finite length, and thus ends with $b_m = p_m$. Thus

$$a_0 = p_1 p_2 \dots p_m$$

□

Finally, we prove that factorization in a PID is unique.

Theorem 4.6. *Every PID is a UFD.*

Proof. We have already shown that every element of a PID can be written as a product of primes in Proposition 4.5. What is left to prove is that this factorization is unique up to permutation of the factors and ambiguity regarding associates and units. Let D be a PID and let $a \in D$. Consider two different factorizations into primes

$$a = p_1 p_2 \dots p_m$$

and

$$a = q_1 q_2 \dots q_n$$

We must have that $p_1 | q_1 q_2 \dots q_n$ which implies that $p_1 | q_i$ for some $i = 1, \dots, n$. Without loss of generality we can rearrange the factors q_i and assume that $p_1 | q_1$. Since both p_1 and q_1 are both primes, they are associates, that is $q_1 = p_1 u_1$ for some unit $u_1 \in D$. Thus

$$p_1 p_2 \dots p_m = p_1 u_1 q_2 \dots q_n$$

and using the cancellation law in D

$$p_2 \dots p_m = u_1 q_2 \dots q_n$$

Continuing this process with p_2, and so on, will give us

$$1 = u_1 u_2 \dots u_m q_{m+1} \dots q_n$$

Since no q_i is a unit this means that $m = n$. Thus p_i and q_i are associates, and factorization is unique. □

4.2. **Euclidean Domains.** An important property that makes the treatment of factorization much easier is the existence of a division algorithm. Unfortunatly, not every UFD has such an algorithm. In this section we will explore domains with division algorithms, that is Euclidean domains.

Definition 4.7. Let D be an integral domain. An **Euclidean function** on D is a function $d : D \setminus \{0\} \to \mathbb{N}$ that satisfies the following properties

(i) if $a, b \in D$ then $d(a) \leq d(ab)$
(ii) if $a, b \in D$ and $b \neq 0$ then there are $q, r \in D$ such that $a = qb + r$ where $d(r) < d(b)$

If we can define at least one such function we call D an **Euclidean domain**.

Example 4.8. The set of integers $\mathbb{Z}$ is a Euclidean domain, and we can use the Euclidean function $d(n) = |n|$.

Example 4.9. If F is a field, then $F[X]$ is a Euclidean domain with the Euclidean function $d(f(X)) = \deg(f(X))$.

We continue by proving that every Euclidean is a PID.

Proposition 4.10. *Every Euclidean domain is a PID.*

Proof. Let D be a Euclidean Domain and let I be a non-zero ideal of D. We need to prove that I is generated by a single element. Let $b \in I$ be the smallest element in the ideal, i.e. let $d(b) < d(x)$ for any $x \in I$. Take an arbitrary element $a \in I$. Then we can find q and r in I such that

$$a = qb + r$$

where $d(r) < d(b)$. However, we said earlier that b was the smallest element of I which implies that $r = 0$. This means that b divides every element of I. Hence $I = (b)$. □

Theorem 4.11. *Every Euclidean domain is a UFD.*

Proof. By Proposition 4.10 every Euclidean domain is a PID, and by Theorem 4.6 every PID is a UFD. □

5. Quadratic Fields

We will now restrict ourselves and study quadratic fields, that is extensions $\mathbb{Q}(\xi)$ such that $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$. Such extensions are thus the simplest form of number fields, if disregarding the trivial number field $\mathbb{Q}$. We will use the knowledge from previous sections and examine integers, primes and factorization in these fields.

5.1. **Quadratic Integers.** We begin our study of quadratic fields by investigating integers in these.

Proposition 5.1. *Every quadratic extension is on the form $\mathbb{Q}(\sqrt{m})$ where m is a square free integer.*

Proof. Quadratic equations are on the form $\mathbb{Q}(\xi)$ where ξ is a root to the equation

$$\xi^2 + p\xi + q = 0$$

where $p, q \in \mathbb{Q}$. The solutions can be written as

$$\xi = \frac{a + b\sqrt{m}}{c}$$

where $a, b, c, m \in \mathbb{Z}$.We have $\mathbb{Q}(\xi) = \mathbb{Q}(\frac{a+b\sqrt{m}}{c}) = \mathbb{Q}(a + b\sqrt{m}) = \mathbb{Q}(b\sqrt{m}) = \mathbb{Q}(\sqrt{m})$. □

Now we try to determine the integral closure of quadratic fields for different m.

Take an element $\frac{a}{b} + \frac{c}{d}\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ where $gcd(a, b) = gcd(c, d) = 1$. This element certainly satisfies the equation

$$\big(X - (\frac{a}{b} + \frac{c}{d}\sqrt{m})\big)\big(X - (\frac{a}{b} - \frac{c}{d}\sqrt{m})\big) = X^2 - \frac{2a}{b}X + \frac{a^2}{b^2} - \frac{c^2}{d^2}m$$

The element is integral if and only if

$$\frac{2a}{b} \in \mathbb{Z} \tag{1}$$

$$\frac{a^2}{b^2} - \frac{c^2}{d^2}m \in \mathbb{Z} \tag{2}$$

Equation (1) gives that $b = 1$ or $b = 2$. We consider the two cases.
Consider the case where $b = 1$. Together with (2) this gives

$$a^2 - \frac{c^2}{d^2}m \in \mathbb{Z}$$

Since m is square free we need $d^2|m$ which implies that $d = 1$. Hence our element is in $\mathbb{Z}[\sqrt{m}]$.
Consider the case when $b = 2$. Then we have

$$\frac{a^2}{4} - \frac{c^2}{d^2}m = \frac{a^2d^2 - 4mc^2}{4d^2} \in \mathbb{Z}$$

This means that we need $4|a^2d^2$. This together with the fact that a is odd means that we need $4|d^2$, and so $d = 2k$. Thus

$$\frac{4a^2k^2 - 4mc^2}{16k^2} = \frac{a^2k^2 - mc^2}{4k^2} \in \mathbb{Z}$$

We need $4|(a^2k^2 - mc^2)$, or $a^2k^2 - mc^2 \equiv 0 \pmod 4$. Since a and c are odd we have $a^2 \equiv c^2 \equiv 1 \pmod 4$. Thus

$$a^2k^2 - mc^2 \equiv 0 \pmod 4 \Rightarrow k^2 - m \equiv 0 \pmod 4$$

Since m is not a square we need $m \equiv 1 \pmod 4$. Hence our element is in $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{m}]$.

We summarize the result in the theorem below.

Theorem 5.2. *The set of integral elements of $\mathbb{Q}[\sqrt{m}]$ can be divided into two cases*

(i) If $m \equiv 1 \pmod 4$ then the set of integral elements is $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{m}]$.
(ii) If $m \equiv 2 \pmod 4$ or $m \equiv 3 \pmod 4$ the set of integral elements is $\mathbb{Z}[\sqrt{m}]$.

5.2. **Unities and Primes.** Having determined the quadratic integers and obvious next step is to study primes. Of course, primes vary much between different quadratic fields. In this section we will thus focus on creating tools that will help us finding primes in the specific case. We begin with some basic concepts.

Definition 5.3. Let $\xi = a + b\sqrt{m}$. The number $\overline{\xi} = a - b\sqrt{m}$ is called the **conjugate** of ξ.

Definition 5.4. The **norm** of $\xi = a + b\sqrt{m}$ is defined as $N(\xi) = \xi\overline{\xi} = a^2 - mb^2$.

Example 5.5. We can see that this norm coincides with our definition of the field norm from section 1. To construct T_ξ we consider how the base $\{1, \sqrt{m}\}$ works on an arbitrary element $\xi = a + b\sqrt{m}$. We have

$$1 \cdot \xi = a + b\sqrt{m}$$
$$\sqrt{m} \cdot \xi = mb + a\sqrt{m}$$

Hence, the matrix representation of T_ξ is

$$T_\xi = \begin{pmatrix} a & mb \\ b & a \end{pmatrix}$$

and the field norm is hence given by $N(\xi) = \det T_\xi = a^2 - mb^2$. This norm is in a few cases also a Euclidean function.

Lemma 5.6. *The norm is multiplicative, that is*

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

Proof. Let α and β be elements of the quadratic extension $\mathbb{Q}[\sqrt{m}]$. Then

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

□

Proposition 5.7. *An element is a unit if and only if its norm is* ± 1.

Proof. Assume that ϵ is a unit. By definition this means that there is a δ such that $\epsilon\delta = 1$. Thus $N(\epsilon)N(\delta) = 1$ which implies that $N(\epsilon) = \pm 1$. Conversely, assume that $N(\xi) = \pm 1$. This is the same as saying that $\xi\overline{\xi} = \pm 1$. This implies that $\xi | 1$, which is the same as saying that ξ is a unit. □

Proposition 5.8. *The element* $\pi \in \mathbb{Z}[\sqrt{m}]$ *is a prime if* $N(\xi)$ *is a rational prime* p. *Futhermore,* p *is not a prime in* $\mathbb{Z}[\sqrt{m}]$.

Proof. Assume that $N(\alpha) = p$ where p is a rational prime. Consider a factorization $\alpha = \beta\gamma$. We have that $N(\alpha) = N(\beta)N(\gamma) = p$. This means that either $N(\beta)$ or $N(\gamma)$ must be equal to ± 1, which implies by Proposition 4.6 that either β or γ must be a unit. Hence, α is a prime.
Consider that $N(\pi) = p$ means that $p = \pi\overline{\pi}$. Hence, p is not prime in $\mathbb{Z}[\sqrt{m}]$. □

Example 5.9. The element $(1 + i) \in \mathbb{Z}[i]$ is a prime since $N(1 + i) = 1^2 + 1^2 = 2$ which is a rational prime. In the same way $3 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a prime since $N(3 + \sqrt{2}) = 3^2 - 2 \cdot 1^2 = 7$ which is a rational prime.

Example 5.10. Observe that the converse of Proposition 5.8 is not necessarily true. For example, consider $3 \in \mathbb{Z}[i]$. We have that $N(3) = 9$, which is obviously not a rational prime. However, assume that 3 is not a prime, then $3 = (a + bi)(c + di)$ for some non-units $(a + bi)$ and $(c + di)$ in $\mathbb{Z}[i]$. Consider that $N(3) = 9 = (a^2 + b^2)(c^2 + d^2)$. But this means that $a^2 + b^2 = c^2 + d^2 = 3$ which is impossible. Hence, 3 is a prime in $\mathbb{Z}[i]$.

5.3. **Unique Factorization in Quadratic Fields.** When having determined a way to find primes we might wonder whether all quadratic fields are UFDs. We can easily show that this is not the case. Take for example the element $6 \in \mathbb{Z}[\sqrt{-5}]$. We have that

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

We check if the numbers $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are prime. Assume that $1 + \sqrt{-5}$ is not a prime. Then

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$$

Checking the norm we have

$$6 = (a^2 + 5b^2)(c^2 + 5d^2)$$

This must mean that either 2 or 3 is on the form $a^2 + 5b^2$ which is not true. Hence, $1 + \sqrt{-5}$ is a prime. The other numbers can be shown to be prime with the same proceedure.

It is not hard to find examples of non-UFD quadratic fields. The problem arises when we are to list all quadratic fields that are UFDs. The fact is that this is a problem yet to be solved. The list is complete for imaginary quadratic fields, that is quadratic fields with negative m, and it can be shown that they are exactly those where

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

However, the list is uncomplete for real quadratic fields, that is fields with positive m, and it is not know if such a list is finite or not. We will now state a proposition about UFD quadratic fields that will help us to find primes in these.

Proposition 5.11. *The prime π in a UFD quadratic field divides exactly one positive rational prime.*

Proof. Let π be a prime of $\mathbb{Q}(\sqrt{m})$. Since $N(\pi) = \pi\overline{\pi}$ we have that $\pi | N(\pi)$, and thus $\pi || N(\pi)|$. Thus, π divides at least one positive integer. Let a be the smallest integer such that $\pi | a$. Assume that $a = a_1 a_2$. If $\mathbb{Q}(\sqrt{m})$ is a UFD this means that

$$\pi | a \Rightarrow \pi | a_1 a_2 \Rightarrow \pi | a_1 \text{ or } \pi | a_2$$

which is a contradiction, since a was the smallest real multiple of π. Hence a must be a rational prime. Thus, π divides at least one positive rational prime. What is left to prove is that this prime is unique. Assume that π divides the two positive rational primes p and q. Since $gcd(p, q) = 1$ it is possible to find x and y such that

$$px + qy = 1$$

This means that

$$\pi | p \text{ and } \pi | q \Rightarrow \pi | 1$$

which is a contradiction. □

6. Gaussian Integers

6.1. **Basic Terminology.** The integers of $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ are commonly referred to as the Gaussian Integers. The Gaussian Integers are probably the most commonly used example of a quadratic extension and we will here try to explore their properties. Many of these have already been dealt with in the previous section, but we will repeat a bit of basic terminology

Proposition 6.1. *The Gaussian Integers are the numbers $\mathbb{Z}[i]$.*

Proof. This is a special case of Theorem 5.2, where $-1 \equiv 3 \pmod 4$. □

Definition 6.2. The **norm** of a Gaussian integer $\zeta = a + bi$ is given by $N(\zeta) = a^2 + b^2$.

This is obviously a special case of Definition 5.4. Observe that that the norm of a Gaussian Integer always is positive. Therefore, by Proposition 5.7, the units are those elements with norm 1.

Proposition 6.3. *The units in* $\mathbb{Z}[i]$ *are* ± 1 *and* $\pm i$.

Proof. By Proposition 5.7, $\epsilon = a + bi$ in $\mathbb{Z}[i]$ is a unit if and only if $N(\epsilon) = a^2 + b^2 = 1$, which is true only for $(a, b) = (1, 0), (-1, 0), (0, 1)$ or $(0, -1)$. These correspond to the numbers ± 1 and $\pm i$. □

It follows that the associates of a Gaussian integer ζ are the four elements $\zeta, -\zeta, i\zeta - i\zeta$.

6.2. **Gaussian Primes.** We continue our investigation of the Gaussian Integers by exploring Gaussian primes, that is the primes of $\mathbb{Z}[i]$. Using Proposition 5.11 we do this by considering the factorization of the rational primes. We study three categories of rational primes: the number 2, primes on the form $4n + 3$ and those on the form $4n + 1$.

(i) The rational prime 2 can be written as

$$2 = 1^2 + 1^2 = (1 + i)(1 - i)$$

and so corresponds to the Gaussian primes $1 + i, 1 - i, -1 + i$ and $-1 - i$.

(ii) In the case of rational primes that can be written as $4n + 3$ we have that

$$4n + 3 = a^2 + b^2$$

lacks solutions, since a square is either 1 or 0 modulo 4. Hence, rational primes on this form are also Gaussian primes.

(iii) Rational primes on the form $4n + 1$ can be factored as

$$4n + 1 = (2n + i)(2n - i)$$

and are consequently not Gaussian primes.

We summarize our findings in the theorem below

Theorem 6.4. *The Gaussian primes can be categorized into the three cases below*

(i) The element $1 + i$ *and its associates.*
(ii) Rational primes on the form $4n + 3$ *and their associates.*
(iii) Factors of rational primes on the form $4n + 1$.

6.3. **Gaussian Integers as a Euclidean Domain.** We conclude the section on Gaussian integers by proving that they form a Euclidean domain.

Proposition 6.5. *Let α and β be two Gaussian integer and $\beta \neq 0$. Then there is γ and δ such that*

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

where $N(\delta) < N(\beta)$.

Proof. Since $\beta \neq 0$ we can write

$$\frac{\alpha}{\beta} = p + qi$$

where $p, q \in \mathbb{Q}$. It is possible to find rational integers x and y such that

$$|x - p| \leq \frac{1}{2}$$

and

$$|y - q| \leq \frac{1}{2}$$

Now, this means that

$$|(x + yi) - (p + qi)|^2 = |(x - p) + i(y - q)|^2 = (x - p)^2 + (y - q)^2 \leq \frac{1}{2}$$

If we where to take $\gamma = x + yi$

$$N(\delta) = N(\alpha - \gamma\beta) = |\alpha - \gamma\beta|^2 \leq \frac{N(\beta)}{2} \leq N(\beta)$$

□

Proposition 6.6. *The Gaussian Integers form a Euclidean domain with $N(a + bi) = a^2 + b^2$ as Euclidean function.*

Proof. The need to check that the two criteria of Definition 4.7 are satisfied.

(i) Let $\alpha = a + bi$ and $\beta = c + di$ two non-zero Gaussian integers. Then

$$N(\alpha\beta) = N(\alpha)N(\beta) = (a^2 + b^2)(c^2 + d^2) \geq a^2 + b^2 = N(\alpha)$$

(ii) The second criterion was proved in Proposition 6.5.

□

7. Eisenstein Integers

7.1. **Basic Terminology.** Eisenstein integers are complex numbers on the form $\zeta = a + b\rho$ where the number $\rho = \frac{1}{2}(-1 + i\sqrt{3})$. In particular the Eisenstein integers are the integers of $\mathbb{Q}(\sqrt{-3})$, and is thus an example of the second case of Theorem 5.2. As in the case of the Gaussian integers, we begin by repeating some facts that follow directly from the definitions in Section 5.

Definition 7.1. The norm of an Eisenstein integer $\zeta = a + b\rho$ is given by $N(z) = a^2 - ab + b^2$.

We observe that $a^2 - ab + b^2$ can be re-written as $(a - \frac{b}{2})^2 + \frac{3b^2}{4}$, so the norm of an Eisenstein integer is always positive.

Proposition 7.2. *The units of the Eisenstein integers are* ± 1, $\pm\rho$ *and* $\pm\rho^2$.

Proof. An element $\epsilon = a + b\rho$ is a unit if and only if its norm is equal to 1. We want to find solutions to the equation

$$(a - \frac{b}{2})^2 + \frac{3b^2}{4} = 1$$

The solutions are given by $(a, b) = (1, 0), (-1, 0), (0, 1), (0, -1), (1, 1)$ and $(-1, -1)$. These correspond to the elements $\pm 1, \pm\rho$ and $\pm(1+\rho) = \mp\rho^2$. □

Hence, every Eisenstein integer ζ has the six associates $\zeta, -\zeta, \rho\zeta, -\rho\zeta, \rho^2\zeta$ and $-\rho^2\zeta$.

7.2. **Eisenstein Primes.** As in Section 6.2, the Eisenstein primes can be determined by studying the factorization of rational primes. As before we divide the rational primes into three categories: the prime number 3, rational primes on the form $3n + 2$ and those on the form $3n + 1$.

(i) The rational prime 3 can be written as

$$3 = (1 - \rho)(1 - \rho^2)$$

and so corresponds to the Eisenstein prime $1-\rho$ and its associates.

(ii) In the case of rational primes that can be written as $3n + 2$ we have that

$$4(3n + 2) = (2a - b)^2 + 3b^2 \Rightarrow 2 \equiv (2a - b)^2 \pmod 3$$

which is impossible since a square is either 0 or 1 modulo 3. Hence, rational primes on this form are also Eisenstein primes.

(iii) Rational primes on the form $3n+1$. All such primes can be written as $x^2 + 3y^2$. Thus

$$3n + 1 = x^2 + 3y^2 = (a - \frac{b}{2})^2 + 3b^2$$

A solution is given by $a = x + y$ and $b = 2y$. Thus any prime on the form $3n + 1$ can be written as

$$3n + 1 = x^2 + 3y^2 = ((x + y) + 2y\rho)((x + y) + 2y\rho^2)$$

and is thus not an Eisenstein prime.

We summarize below

Theorem 7.3. *The Eisenstein primes can be categorized into the three cases below*

(i) The element $1-\rho$ and its associates.
(ii) Rational primes on the form $3n+2$ and their associates.
(iii) Factors of rational primes on the form $3n+1$.

7.3. **Eisenstein Integers as a Euclidean Domain.** We conclude this section with proving that the Eisenstein integers form a Euclidean domain.

Proposition 7.4. *Let α and β be two Eisenstein integers and $\beta \neq 0$. Then there is γ and δ such that*

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

where $N(\delta) < N(\beta)$.

Proof. Since $\beta \neq 0$ we can write

$$\frac{\alpha}{\beta} = p + q\rho$$

where $p, q \in \mathbb{Q}$. It is possible to find rational integers x and y such that

$$|x - p| \leq \frac{1}{2}$$

and

$$|y - q| \leq \frac{1}{2}$$

Now, this means that

$$|(x+y\rho)-(p+q\rho)|^2 = |(x-p)+i(y-q)|^2 = (x-p)^2-(x-p)(y-q)+(y-q)^2 \leq \frac{3}{4}$$

If we where to take $\gamma = x + y\rho$

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

□

Theorem 7.5. *The Eisenstein integers form a Euclidean domain with $N(a + b\rho) = a^2 - ab + b^2$ as Euclidean function.*

Proof. We check that the norm satisfies the two criteria for it being a Euclidean function.

(i) Let $\alpha = a+b\rho$ and $\beta = c+d\rho$ be two non-zero Eisenstein integers. Then

$$N(\alpha\beta) = N(\alpha)N(\beta) = (a^2-ab+b^2)(c^2-cd+d^2) \geq (a^2-ab+b^2) = N(\alpha)$$

Which proves the first criterion.
(ii) The second criterion is proved in Proposition 7.4.

□

References

[1] Norman L. Biggs. *Discrete Mathematics*. Oxford University Press, second edition, 2002.
[2] John B. Fraleigh. *A First Course In Abstract Algebra*. Addison Wesley, seventh edition, 2003.
[3] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, sixth edition, 1954.
[4] I.N. Herstein. *Topics in Algebra*. Wiley, second edition, 1975.
[5] Serge Lang. *Algebra*. Springer-Verlag, revised third edition, 2002.
[6] Hans Riesel. *En bok om primtal*. Studentlitteratur, 1968.
[7] Kenneth H. Rosen. *Elementary Number Theory and Its Applications*. Addison Wesley, fifth edition, 2005.