

# The Ideal Class Group

Christina Jamroz

July 31, 2009

In this paper, we will analyze the ideal class group of the ring of integers of the imaginary quadratic number field,  $\mathbb{Q}[\sqrt{-5}]$ . We will conclude that this ideal class group is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ . But, before we are able to reach this astonishing result, we must first discuss some preliminary topics including integral domains, lattices, and algebraic integers.

I would like to acknowledge my use of Michael Artin's text, *Algebra* [1]. In comparing this paper to his text, one would notice similar arguments for many of the following results.

## 1 Integral Domains

It will be important for future results that we discuss the properties of some specific integral domains. We will use these properties to classify rings of integers later in our discussion.

**Definition 1.1.** An integral domain,  $R$ , is a unique factorization domain if,  $\forall x \in R$ ,  $x$  can be factored into irreducibles in exactly one way, up to units.

For this discussion, it is important to note the difference between an irreducible element and a prime element. Let  $p \in R$ . The element  $p$  is irreducible if for some  $a, b \in R$  if  $p = ab$ , then  $p \mid a$  or  $p \mid b$ . The element  $p$  is prime if for some  $a, b \in R$  if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ . In a unique factorization domain, every prime element is irreducible.

**Definition 1.2.** An integral domain,  $R$ , is a principal ideal domain if, for every ideal  $A \subset R$ ,  $A = \alpha R$  for some  $\alpha \in R$ .

We denote this  $A = (\alpha)$ . Notice that every principal ideal domain is a unique factorization domain [See Artin [1]]. But, the converse is not always

true. For example,  $\mathbb{Z}[x]$  is a unique factorization domain, but not a principal ideal domain.

**Definition 1.3.** An integral domain,  $R$ , is a Euclidean domain if  $\exists$  a "size function",  $\sigma : R - \{0\} \rightarrow \{0, 1, 2, \dots\}$ , such that  $\forall a, b \in R$  where  $a \neq 0$ ,  $\exists p, q \in R$  that satisfy  $b = aq + r$  and  $r = 0$  or  $\sigma(r) < \sigma(a)$ .

$\mathbb{Z}[i]$  is an example of a Euclidean domain. This can be shown using  $\sigma(x) = |x|^2 \forall x \in \mathbb{Z}[i]$ .

## 2 Plane Lattices

To prove some of the results of this paper, we must also introduce some basic ideas about plane lattices.

**Definition 2.1.** A subgroup  $L \subset \mathbb{R}^2$  is called discrete if  $\exists \varepsilon > 0$  such that the only vector with length  $< \varepsilon$  contained in  $L$  is the zero vector.

**Definition 2.2.** A plane lattice is a subgroup of  $\mathbb{R}^2$  generated by two linearly independent vectors,  $a$  and  $b$ . We call the generating set  $(a, b)$  a lattice basis for  $L$ .

Let  $L$  be a plane lattice generated by the vectors  $a$  and  $b$ . Then,  $L = \{ma + nd \mid m, n \in \mathbb{Z}\}$ . It also follows from the definition that  $L$  is a discrete subgroup of  $\mathbb{R}^2$ . Also, the fundamental parallelogram of  $L$  is  $P = \{ra + sb \mid 0 \leq r \leq 1, 0 \leq s \leq 1; r, s \in \mathbb{R}\}$ .

**Lemma 2.3.** *Let  $L$  be a lattice generated by two linearly independent vectors  $a, b \in \mathbb{R}^2$ . Let  $P$  be the fundamental parallelogram. Then, for any  $x \in \mathbb{R}^2$ ,  $\exists l \in L$  such that  $x - l \in P$ .*

*Proof.* Let  $x \in \mathbb{R}^2$ . Then,  $x = c_1a + c_2b$  where  $c_i \in \mathbb{R}$ . Let  $m_1 = [c_1]$ , the greatest integer less than  $c_1$ . And let  $m_2 = [c_2]$ . Then,  $c_1 = m_1 + r$  and  $c_2 = m_2 + s$  for some  $0 \leq r, s < 1$ . Let  $l \in L$  such that  $l = m_1a + m_2b$ . Then,  $x - l = ra + sb \in P$ .  $\square$

Although it is not yet applicable, this lemma will be vital in proving a result later. Now that we know a few basics about lattices, we will begin with our discussion of algebraic integers.

### 3 Algebraic Integers

**Definition 3.1.** An algebraic number that is the root of a monic polynomial with coefficients in  $\mathbb{Z}$  is called an algebraic integer.

It is well-known that the set of algebraic integers forms a subring  $R$  of  $\mathbb{C}$ , and  $\mathbb{Z} \subset R$ . In this paper, we will analyze the algebraic integers of a quadratic number field,  $\mathbb{Q}[\sqrt{d}]$ . Elements of  $\mathbb{Q}[\sqrt{d}]$  have the form  $a + b\sqrt{d}$  where  $a, b \in \mathbb{Q}$  and  $d$  is a square-free integer. Now we will identify which elements of  $\mathbb{Q}[\sqrt{d}]$  are algebraic integers.

**Corollary 3.2.** *An element  $\alpha$  of  $\mathbb{Q}[\sqrt{d}]$  is an algebraic integer iff  $2a \in \mathbb{Z}$  and  $a^2 - b^2 \in \mathbb{Z}$ .*

*Proof.* First, assume  $b \neq 0$ . This implies that  $\alpha \in \mathbb{Q}[\sqrt{d}]$ , but  $\alpha \notin \mathbb{Q}$ . Define  $\alpha' = a - b\sqrt{d}$ . So, we see that  $\alpha$  and  $\alpha'$  are roots of the polynomial,  $p(x)$ , where:

$$p(x) = (x - \alpha)(x - \alpha') = x^2 - 2ax + (a^2 - b^2d).$$

Since  $\alpha \notin \mathbb{Q}$ , we know that it is not the root of a linear polynomial in  $\mathbb{Q}[x]$ . So,  $p(x)$  is irreducible. It is the monic irreducible polynomial of  $\alpha$  over  $\mathbb{Q}$ . This means that  $\alpha$  is an algebraic integer iff  $-2a$  and  $a^2 - b^2d$  are integers. Furthermore, if  $b = 0$ , then  $a^2 - b^2d = a^2$ . And  $a^2$  is an integer iff  $a$  is an integer. So, the corollary holds for all  $b \in \mathbb{Q}$ .  $\square$

So, if we are given an element of  $\mathbb{Q}[\sqrt{d}]$ , we can use this corollary to decide if it is an algebraic integer. But, this result is actually useful in proving a much easier method to show that  $\alpha \in \mathbb{Q}[\sqrt{d}]$  is an algebraic integer.

**Proposition 3.3.** *An algebraic integer  $\alpha \in \mathbb{Q}[\sqrt{d}]$  has the form  $\alpha = a + b\sqrt{d}$ , where:*

- (1) *If  $d \equiv 2$  or  $3 \pmod{4}$ , then  $a, b \in \mathbb{Z}$ . In this case,  $R = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ .*
- (2) *If  $d \equiv 1 \pmod{4}$ , then  $a, b \in \mathbb{Z} + \frac{1}{2}$  or  $a, b \in \mathbb{Z}$ . In this case,  $R = \mathbb{Z} \oplus \mathbb{Z}\eta$ , where  $\eta = \frac{1}{2}(1 + \sqrt{d})$ .*

Note that if  $c \in \mathbb{Z} + \frac{1}{2}$ , it is called a half-integer and can be written  $c = \frac{1}{2}m$  for an odd integer  $m$ . The proof of the proposition is as follows.

*Proof.*  $\implies$ : Suppose  $\alpha \in \mathbb{Q}[\sqrt{d}]$  is an algebraic integer. Then, by 3.2,  $2a \in \mathbb{Z}$  and  $a^2 - b^2d \in \mathbb{Z}$ . There are two cases:

Case 1:  $a \in \mathbb{Z}$ . So,  $b^2d \in \mathbb{Z}$  as well. Write  $b = \frac{m}{n}$  where  $m, n \in \mathbb{Z}$  and they

are relatively prime. Also,  $n > 0$ . Then,  $b^2d = \frac{m^2d}{n^2}$ . Since  $d$  is square-free,  $n^2 \nmid d$ . So,  $n = 1$ . Therefore,  $b \in \mathbb{Z}$ .

Case 2:  $a \in \mathbb{Z} + \frac{1}{2}$ . So,  $a = \frac{m}{2}$  for some odd integer  $m$ . Then,  $4a^2 \in \mathbb{Z}$ . This implies that  $4b^2d \in \mathbb{Z}$  because  $a^2 - b^2d \in \mathbb{Z}$ . But,  $b^2d \notin \mathbb{Z}$ . We can write  $b = \frac{n}{2}$  for some odd integer  $n$ . So,  $m^2 - n^2d \equiv 0 \pmod{4}$ . Hence,

$$(m \bmod 4)^2 - (n \bmod 4)^2d \equiv 0 \pmod{4}$$

$$(\pm 1)^2 - (\pm 1)^2d \equiv 0 \pmod{4}.$$

Therefore,  $d \equiv 1 \pmod{4}$  in this case. This completes the proof of the forward implication.

$\Leftarrow$ : Assume  $a, b \in \mathbb{Z}$ . It is obvious that  $\alpha$  is an algebraic integer from 3.2. Now assume  $d \equiv 1 \pmod{4}$  and  $a, b \in \mathbb{Z} + \frac{1}{2}$ . Obviously,  $2a \in \mathbb{Z}$ . We will now show that  $a^2 - b^2d \in \mathbb{Z}$ . Let  $a = \frac{m}{2}$  and  $b = \frac{n}{2}$ . Hence,

$$m^2 - n^2d \equiv (\pm 1)^2 - (\pm 1)^2 \times 1 \equiv 0 \pmod{4}.$$

This tells us that  $4 \mid m^2 - n^2d$ . Therefore,  $\frac{1}{4}(m^2 - n^2d) \in \mathbb{Z}$ . So,  $a^2 - b^2d \in \mathbb{Z}$  as required.  $\square$

We now have the tools necessary to identify algebraic integers in any quadratic number field. As stated earlier, these integers of a quadratic number field,  $F$ , form a ring called the ring of integers. Actually, it is just  $R \cap F$ . In the next section, we will examine these rings and, in particular, determine their units.

## 4 Rings of Integers of a Number Field

Throughout the rest of this paper,  $R_d$  will denote the ring of integers of a quadratic number field,  $\mathbb{Q}[\sqrt{d}]$ , except where otherwise noted. Also, assume  $d$  is a square-free integer.

The notion of the norm of an integer is central to this discussion. So, we must now present the following definition.

**Definition 4.1.** The norm of an integer  $\alpha \in \mathbb{Q}[\sqrt{d}]$  is  $N(\alpha) = \alpha\bar{\alpha}$ , where  $\bar{\alpha} = a - b\sqrt{d}$ .

So,  $N(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d$ . Note that this was the constant term of the monic irreducible polynomial for  $\alpha$ . So, for nonzero  $\alpha$ ,  $N(\alpha)$  is a positive integer. We also have the following result:

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

where  $\alpha$  and  $\beta$  are integers in  $\mathbb{Q}[\sqrt{d}]$ . If  $\alpha = a + b\sqrt{d}$ ,  $\beta = m + n\sqrt{d}$  where  $a, b, m, n \in \mathbb{Q}$ , then  $\alpha\beta = am + bnd + (an + bm)\sqrt{d}$ . So,

$$N(\alpha\beta) = (am + bnd)^2 - (an + bm)^2d.$$

On the other hand,  $N(\alpha) = a^2 - b^2d$  and  $N(\beta) = m^2 - n^2d$ . So,  $N(\alpha)N(\beta) = a^2m^2 - a^2n^2d - b^2m^2d + b^2n^2d$ . By expanding the first equation, we see that  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

Now we will identify the units of  $R_d$  in the following propositions.

**Proposition 4.2.** *An element  $\alpha$  in  $R_d$  is a unit iff  $N(\alpha) = 1$ .*

*Proof.* To prove the forward implication, let  $\alpha$  be a unit. Then,  $\alpha^{-1} \in R_d$ . So,  $N(\alpha\alpha^{-1}) = N(1) = 1$ . Hence,  $N(\alpha)N(\alpha^{-1}) = 1$ . Conversely, assume  $N(\alpha) = 1$ . So,  $\alpha\bar{\alpha} = 1$ . This implies that  $\bar{\alpha} = \alpha^{-1}$ . Hence,  $\alpha^{-1} \in R_d$ , so  $\alpha$  is a unit.  $\square$

**Proposition 4.3.** *The units  $\alpha \in R_{-d}$ , where  $\alpha = a + b\sqrt{-d}$  and  $d \in \mathbb{N}$ , are  $\pm 1$  except when  $d = 1$  or  $3$ . If  $d = 1$ , then  $R_{-1}^x = \{\pm 1, \pm i\}$ . If  $d = 3$ ,  $R_{-3}^x = \{[\frac{1}{2}(1 + \sqrt{-3})]^j \mid j = 0, 1, \dots, 5\}$ .*

Notice, here we write  $-d$  instead of  $d$ . And, since  $d \in \mathbb{N}$ , we are restricted to the ring of integers of an imaginary quadratic number field for this proposition.

*Proof.* Let  $\alpha = a + b\sqrt{-d}$  be a unit in  $R_{-d}$  where  $d \in \mathbb{N}$  is square-free. So,  $N(\alpha) = a^2 + b^2d = 1$ . And assume  $d \neq 1$  or  $3$ . So,  $d \geq 2$ . If  $a, b \in \mathbb{Z}$ , then  $b = 0$  and  $a = \pm 1$ . So,  $\alpha = \pm 1$ . If  $a, b \in \mathbb{Z} + \frac{1}{2}$ , then  $a = \frac{m}{2}$  and  $b = \frac{n}{2}$  for odd integers  $m$  and  $n$ . Hence,  $\frac{m^2}{4} + \frac{n^2}{4}d = 1$  implies  $m^2 + n^2d = 4$ . Since  $d \equiv 1 \pmod{4}$ , then  $d \geq 5$ . So,  $m^2 \leq 4 - 5n^2$ . There are no solutions to this inequality.

Therefore, the units are  $\pm 1$  unless  $d = 1$  or  $3$ . Now assume  $d = 1$ . Then,  $a^2 + b^2 = 1$ . Also,  $a, b \in \mathbb{Z}$ , so  $a = \pm 1$  and  $b = 0$  or  $a = 0$  and  $b = \pm 1$ . So,  $R_{-1}^x = \{\pm 1, \pm i\}$ .

Next, assume  $d = 3$ . Then,  $a^2 + 3b^2 = 1$ , and there are two cases:

Case 1:  $a, b \in \mathbb{Z}$ . In this case,  $a = \pm 1$  and  $b = 0$ .

Case 2:  $a, b \in \mathbb{Z} + \frac{1}{2}$ . In this case,  $a = \frac{m}{2}$  and  $b = \frac{n}{2}$ . So,  $\frac{m^2}{4} + \frac{3n^2}{4} = 1$ . It follows that  $|m| = |n| = 1$ . So,  $\alpha = \pm \frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ . In summary, if  $d = 3$ , then  $R_{-3}^x = \{[\frac{1}{2}(1 + \sqrt{-3})]^j \mid j = 0, 1, \dots, 5\}$ .  $\square$

This is discussed in Samuel's text [3]. Since we have identified the units of this ring, we can begin to look at factorization of elements. First, we must prove the following proposition.

**Proposition 4.4.** *Factorization of elements into irreducibles exists in the ring of integers,  $R_d$ .*

*Proof.* Let  $\alpha, \beta, \gamma \in R_d$  so that  $\alpha = \beta\gamma$ . Assume this is a proper factorization of  $\alpha$ . This is to say that  $\beta$  and  $\gamma$  are not units. So,  $N(\beta) \neq 1$  and  $N(\gamma) \neq 1$ . Hence,  $N(\alpha) = N(\beta)N(\gamma)$  is a proper factorization in  $\mathbb{Z}$ . Since every element of  $\mathbb{Z}$  factors into a finite number of irreducible elements,  $N(\alpha) = N(\beta_1) \cdots N(\beta_n)$  for some finite  $n \in \mathbb{N}$  and irreducibles  $N(\beta_1), \dots, N(\beta_n) \in \mathbb{Z}$ . So,  $\alpha = \beta_1 \cdots \beta_n$  is a factorization of  $\alpha$  into a finite number of irreducible elements in  $R_d$ .  $\square$

Notice that we did not prove that these factorizations are unique. In fact, there is usually more than one way to factor an element into irreducibles in  $R_d$ . For example,  $6 \in \mathbb{Q}[\sqrt{-5}]$  can be factored as  $6 = 2 \times 3$ . But, it is also equal to  $(1 - \sqrt{-5})(1 + \sqrt{-5})$ . These elements:  $2, 3, 1 - \sqrt{-5}$ , and  $1 + \sqrt{-5}$  are all irreducible in  $\mathbb{Q}[\sqrt{-5}]$ . So, we can conclude from this example that  $\mathbb{Q}[\sqrt{-5}]$  is not a unique factorization domain. Actually, we can prove the following statement about imaginary quadratic number fields where  $d \equiv 3 \pmod{4}$ .

**Proposition 4.5.** *Assume  $d \equiv 3 \pmod{4}$  and  $d < 0$ . Then,  $R_d$  is not a unique factorization domain unless  $d = -1$ . If  $d = -1$ , then  $R_{-1}$  is a unique factorization domain.*

Before presenting the proof, we must prove the following statement: Assume  $d \equiv 3 \pmod{4}$  and  $d < 0$ , but  $d \neq -1$ . If  $\alpha \in R_d$  and is not a unit, then  $N(\alpha) \geq 4$ .

Since  $d < 0$ , then  $d = -(4n + 1)$  for some  $n \in \mathbb{N}$ . Assume  $\alpha$  is not a unit, and  $\alpha = a + b\sqrt{d}$  for some  $a, b \in \mathbb{Z}$ . Then,

$$N(\alpha) = a^2 - b^2(-4n - 1)$$

$$N(\alpha) = a^2 + 4nb^2 + b^2.$$

Let  $n = 1$ , so  $N(\alpha) = a^2 + 5b^2$ . If  $b = 0$ , then  $a \geq 2$ . And if  $a = 0$ , then  $b \geq 1$ . So, the smallest value taken by  $N(\alpha)$  is 4.

Now, we will present the proof of Proposition 4.5.

*Proof.* Assume  $d \equiv 3 \pmod{4}$  and  $d \neq -1$ . Observe that there are two factorizations of  $1 - d$  in  $R_d$ :

$$1 - d = 2 \left( \frac{1 - d}{2} \right)$$

$$1 - d = (1 + \sqrt{d})(1 - \sqrt{d}).$$

We will now show that 2 is an irreducible element. First, 2 is not a unit because  $N(2) = 2 \times \bar{2} = 4 \neq 1$ . Also, 2 can be written as a product of two elements of  $R_d$ :  $2 = ab$  for some  $a, b \in R_d$ . So, 2 is irreducible if  $a$  or  $b$  is a unit. We know:

$$4 = N(2) = N(ab) = N(a)N(b).$$

Assume neither  $a$  nor  $b$  is a unit. Then,  $N(a) \geq 4$  and  $N(b) \geq 4$  from the above discussion. Hence,  $N(a)N(b) \geq 16$ . This is a contradiction, so either  $a$  or  $b$  is a unit. Therefore, 2 is an irreducible element. So, if  $R_d$  was a unique factorization domain, 2 would divide either  $(1 + \sqrt{d})$  or  $(1 - \sqrt{d})$ . But,  $\frac{1}{2} \pm \frac{1}{2}\sqrt{d}$  is not in  $R_d$ . So,  $R_d$  is not a unique factorization domain. Furthermore, recall that  $\mathbb{Z}[i]$  is a Euclidean domain. So, when  $d = -1$ ,  $R_{-1} = \mathbb{Z}[i]$  is a unique factorization domain.  $\square$

Now that we are familiar with these rings, it is natural to wonder about the ideals of such a ring. In the next section, we will examine the ideal classes of a ring and prove that they form an abelian group.

## 5 The Ideal Class Group

Ideal classes are the equivalence classes formed by ideals of a ring of integers of  $\mathbb{Q}[\sqrt{d}]$ . But, what does it mean for two ideals to be in the same equivalence class?

**Definition 5.1.** Two nonzero ideals  $A, B \subset R_d$  are equivalent if  $\exists r, s \in R_d$  such that  $rA = sB$ .

Equivalently, we can say that  $A = \lambda B$  for some  $\lambda \in \mathbb{Q}[\sqrt{d}]$ . Since  $r, s \in R_d$ , then  $r, s \in \mathbb{Q}[\sqrt{d}]$ . So,  $r^{-1}s \in \mathbb{Q}[\sqrt{d}]$ . Let  $\lambda = r^{-1}s$ , so  $A = \lambda B$ . Notice that  $r, s \in R_d$ , but  $\lambda \in \mathbb{Q}[\sqrt{d}]$ .

We need to prove that this definition of equivalent ideals actually is an equivalence relation. For this proof, we need to show that the relation is transitive, reflexive, and symmetric. It is obviously symmetric and reflexive,

so we need only show that  $\forall A, B, C$  ideals in  $R_d$ , if  $A \sim B$  and  $B \sim C$ , then  $A \sim C$ . If  $A \sim B$  and  $B \sim C$ , then  $\exists p, q, r, s \in R_d$  such that  $pA = qB$  and  $rB = sC$ . Hence,

$$rpA = rqB = qrB = qsC.$$

Therefore,  $A \sim C$ . And we conclude that this definition of equivalent is an equivalence relation.

As previously stated, these equivalence classes are called ideal classes. We will denote the ideal class of an ideal  $A \subset R_d$  by  $[A]$ . Our goal is to prove that these classes form an abelian group. Before we can present this proof, we must first discuss some properties of ideals.

**Proposition 5.2.** *If  $\alpha, \beta \in R_d$  such that  $A = (\alpha)$  and  $B = (\beta)$ , then  $AB = (\alpha\beta)$ .*

*Proof.* So,  $AB = \{\sum_i \alpha_i \beta_i \mid \alpha_i = r_i \alpha, \beta_i = s_i \beta \text{ for some } r_i, s_i \in R_d\}$ . Hence,  $AB = \{(\sum_i r_i s_i) \alpha \beta\}$ . Since  $\sum_i r_i s_i \in R_d$ , then  $AB = (\alpha\beta)$ .  $\square$

In other words, the product of two principal ideals is a principal ideal.

**Lemma 5.3.** *Let  $J$  be a principal ideal of  $R_{-5}$ . So, for some  $\alpha \in J$ ,  $J = (\alpha)$ . Then,  $\alpha$  is the element of  $J$  with smallest absolute value.*

*Proof.* Assume  $J = (\alpha)$  where  $\alpha \in J$  is not the element of smallest absolute value. Let  $r \in R_{-5}$ . So,  $r = m + n\sqrt{-5}$  for some  $m, n \in \mathbb{Z}$ . Hence,  $|r|^2 = m^2 + 5n^2$ . This implies that  $|r| \geq 1$ . Also,  $\forall x \in J$ , we know  $x = r\alpha$ . So,  $|x| = |r||\alpha|$ . But, since  $|r| \geq 1$ , this implies that  $|x| \geq |\alpha|$ . This is a contradiction, so  $\alpha$  is the element of  $J$  with smallest absolute value.  $\square$

**Proposition 5.4.** *An ideal of  $R_d$  is prime iff it is maximal.*

*Proof.* Assume  $M$  is a maximal ideal of  $R_d$ . Then,  $R/M$  is a field. This implies that  $R/M$  is an integral domain. Therefore,  $M$  is prime. Conversely, if  $P$  is a nonzero prime ideal of  $R$ , then  $P$  has finite index in  $R$ . This is true because  $P$  contains  $\alpha R$  if  $\alpha$  is a nonzero element of  $P$ . But,  $R$  and  $\alpha$  are free abelian groups of rank 2. By Cerenzia [2], it follows that  $R/\alpha R$  is a finite group, and so  $R/P$  is a finite group. So, we have that  $P$  has finite index. Therefore,  $R/P$  is a finite integral domain. Hence,  $R/P$  is a field, and  $P$  is maximal.  $\square$

**Lemma 5.5.** *The product of a nonzero ideal  $A \subset R$  and its conjugate  $\overline{A}$  is a principal ideal:*

$$A\overline{A} = (n)$$

for some  $n \in \mathbb{Z}$ .

*Proof.* We must first generate  $A$  as a lattice. Recall that we can generate  $A$  by two elements, so let  $A$  be generated by  $\alpha$  and  $\beta$ , where  $\alpha, \beta \in A$ . So, as an ideal,  $A$  is also generated by these elements. Also,  $\overline{\alpha}$  and  $\overline{\beta}$  generate  $\overline{A}$ . Therefore,  $A\overline{A}$  is generated by  $\alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta}$ . Look at the elements  $\alpha\overline{\alpha}, \beta\overline{\beta}, \overline{\alpha}\beta + \alpha\overline{\beta} \in A\overline{A}$ . Each of these elements is a rational number because it is equal to its conjugate. So, they are elements of  $\mathbb{Z}$ . Let  $n = \gcd(\alpha\overline{\alpha}, \beta\overline{\beta}, \overline{\alpha}\beta + \alpha\overline{\beta})$ , so  $n \in \mathbb{Z}$ . Hence,

$$n = a\alpha\overline{\alpha} + b\beta\overline{\beta} + c(\overline{\alpha}\beta + \alpha\overline{\beta})$$

for some  $a, b, c \in \mathbb{Z}$ . Since  $n$  is a sum of multiples of elements of  $A\overline{A}$ , then  $n \in A\overline{A}$ . Furthermore,  $(n) \subset A\overline{A}$ .

Now we will prove that  $A\overline{A} \subset (n)$ . To do this, it is sufficient to show that  $n$  divides each of the generators of  $A\overline{A}$ . We already know  $n \mid \alpha\overline{\alpha}$  and  $n \mid \beta\overline{\beta}$  in  $\mathbb{Z}$  by our choice of  $n$ . So,  $n$  divides them in  $R_d$ . We will show that  $n \mid \overline{\alpha}\beta$  and  $n \mid \alpha\overline{\beta}$  in  $R_d$ . Both  $\frac{\overline{\alpha}\beta}{n}$  and  $\frac{\alpha\overline{\beta}}{n}$  are roots of the monic polynomial  $p(x) = x^2 - rx + s$ , where  $r = \frac{\overline{\alpha}\beta + \alpha\overline{\beta}}{n}$  and  $s = \frac{\alpha\overline{\alpha}\beta\overline{\beta}}{n}$ . So,  $r$  and  $s$  are integers. Hence,  $\frac{\overline{\alpha}\beta}{n}$  and  $\frac{\alpha\overline{\beta}}{n}$  are algebraic integers. So,  $A\overline{A} \subset (n)$ . Therefore,  $A\overline{A} = (n)$ .  $\square$

From this result and that of the next proposition, we will be able to identify the identity element and the inverse of an element of the ideal class group.

**Proposition 5.6.** *The ideal class of  $R_d$ ,  $[R_d]$ , is the class of principal ideals.*

*Proof.* Let  $A$  be an ideal of  $R_d$  such that  $A \sim R_d$ . So,  $A = aR_d$  for some  $a \in \mathbb{Q}[\sqrt{d}]$ . So,  $a \in A$  and, furthermore,  $a \in R_d$ . Therefore,  $A = (a)$ . Since  $[A] = [R_d]$ , we see that  $[R_d]$  contains only principal ideals.

But, we need to show that all the principal ideals of  $R_d$  are contained in  $[R_d]$ . Let  $B$  be a principal ideal of  $R_d$ . So,  $B = bR_d$  for some  $b \in R$ . Hence,  $B \subset R_d$ .  $\square$

We are now prepared to prove that the ideal classes form a group.

**Proposition 5.7.** *The ideal classes of  $R_d$  form an abelian group,  $C(R_d)$ . The law of composition is given by:*

$$[A][B] = [AB]$$

$\forall A, B$  ideals of  $R_d$ . Also, the identity element is the class of principal ideals and  $[\bar{A}] = [A]^{-1}$ .

*Proof.* Let  $A, A', B, B'$  be ideals of  $R_d$  such that  $A \sim A'$  and  $B \sim B'$ . So,  $\exists a, b \in \mathbb{Q}[\sqrt{d}]$  such that  $A' = aA$  and  $B' = bB$ . Hence,  $A'B' = abAB$ . So,  $A'B' \sim AB$ . Therefore,  $[A'B'] = [AB]$ , which implies that the law of composition is well-defined. Also,

$$[A][B] = [AB] = [BA] = [B][A].$$

And  $\forall A, B, C$  ideals of  $R_d$ :

$$[A]([B][C]) = [A][BC] = [A(BC)] = [(AB)C] = [AB][C] = ([A][B])[C].$$

So, the law of composition is both commutative and associative.

Also, since  $R_d = (1)$ , we say  $[R_d]$  is the identity. Therefore, the identity consists of the principal ideals of  $R_d$ . And, since  $A\bar{A} = (n)$ , then  $[A][\bar{A}] = [R_d]$ . this implies that  $[\bar{A}] = [A]^{-1}$ .  $\square$

This result is very useful to us. We can look at the elements of the group to learn about the nature of  $R_d$  itself. The following corollary is an important example of this.

**Corollary 5.8.** *The following assertions are equivalent:*

- (1)  $R_d$  is a principal ideal domain.
- (2)  $R_d$  is a unique factorization domain.
- (3)  $C(R_d)$  is the trivial group.

Before we present the proof, we need to prove the following theorem.

**Theorem 5.9.** *An integral domain,  $R$ , is a unique factorization domain iff it is a principal ideal domain.*

*Proof.* We already know that every principal ideal domain is a unique factorization domain. So, we will prove the converse. Suppose  $R$  is a unique factorization domain. Let  $P$  be a nonzero prime ideal of  $R$ . Let  $\alpha \in P$  be

a nonzero element. This element can be written as a product of irreducible elements. Let  $\alpha = \pi_1 \cdots \pi_n$  be this factorization, where  $n \in \mathbb{N}$ . Then, at least one of these elements is contained in  $P$ . Say  $\pi_i \in P$  for some  $i$  such that  $1 \leq i \leq n$ . Since  $R$  is a unique factorization domain,  $\pi_i$  is maximal. So,  $(\pi_i) \subset P$  is a prime ideal. By 5.4,  $(\pi_i)$  is maximal. This implies that  $P \subset (\pi_i)$ . Hence,  $P = (\pi_i)$  and  $P$  is principal. Since every nonzero ideal  $A \subset R$  is a product of prime ideals, then, by 5.2,  $A$  is principal. Therefore,  $R$  is a principal ideal domain.  $\square$

*Proof.* We can now prove Corollary 5.7. By the previous theorem, the first two statements are equivalent. So, we will prove that (1) and (3) are equivalent.  $C(R_d)$  is the trivial group iff every ideal  $A \subset R$  is equivalent to the unit ideal. Hence,  $A \sim R$ . But,  $A \sim R$  iff every ideal is principal. So, (1) and (3) are equivalent statements, and this completes the proof of the corollary.  $\square$

This is a very important result. We can now say that the ideal class group of a ring of integers is trivial iff it is a principal ideal domain. We already know that when  $d \equiv 3 \pmod{4}$  the only principal ideal domain is  $\mathbb{Z}[i]$ . But, now it is slightly easier for us to look at rings where  $d \equiv 1$  or  $2 \pmod{4}$ . For example,  $|C(\mathbb{Z}[\sqrt{-2}])| = 1$ . So, the ring of integers where  $d = -2$  is a principal ideal domain. On the other hand,  $\mathbb{Z}[\sqrt{-5}]$  is not a principal ideal domain, but we will use some properties of its ideal classes to make an interesting conclusion about  $C(\mathbb{Z}[\sqrt{-5}])$ .

## 6 Application to $\mathbb{Q}[\sqrt{-5}]$

The main result of this paper comes from the following theorem.

**Theorem 6.1.** *Let  $A$  be a nonzero ideal of  $\mathbb{Z}[\sqrt{-5}]$ . Let  $\alpha \in A$  such that  $\alpha \neq 0$  and  $\alpha$  has minimal absolute value,  $r$ . Let  $\delta = \sqrt{-5}$ . Then, either:*

Case 1:  *$A$  is the principal ideal  $(\alpha)$  with lattice basis  $(\alpha, \alpha\delta)$ , or*

Case 2:  *$A$  is not a principal ideal and has lattice basis  $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ .*

We are not yet able to prove this result. First, we must present the following lemma.

**Lemma 6.2.** *Let  $r$  be the minimum absolute value among nonzero elements of the lattice,  $A$ . Let  $\gamma \in A$  and  $n \in \mathbb{N}$ .  $D$  is the disc of radius  $\frac{1}{n}r$  about the point  $\frac{1}{n}\gamma$ . Then, there is no point of  $A$  in the interior of  $D$  other than its center.*

*Proof.* Let  $\alpha$  be a point in the interior of  $D$ , and  $\alpha \in A$ . We will show that  $\alpha = \frac{1}{n}\gamma$ . By the definition of the disc,  $|\alpha - \frac{1}{n}\gamma| < \frac{1}{n}r$ . So,  $|n\alpha - \gamma| < r$ . Since  $\alpha \in A$ , then  $n\alpha - \gamma \in A$ . Therefore,  $n\alpha - \gamma = 0$  because the only element whose absolute value is less than  $r$  is 0. So,  $\alpha = \frac{1}{n}\gamma$ .  $\square$

We will now use this result in the proof of the theorem.

*Proof.* By the assumptions of the theorem,  $(\alpha) \subset A$ . Let  $R_{-5} = \mathbb{Z}[\sqrt{-5}]$ . the elements of  $(\alpha)$  have the form  $(a + b\sqrt{d})\alpha$ , where  $a, b \in \mathbb{Z}$ . Hence,  $(\alpha)$  has the lattice basis  $(\alpha, \alpha\delta)$ . Now, there are two cases:

Case 1: Assume  $A = (\alpha)$ . By the above statements,  $A$  has the lattice basis  $(\alpha, \alpha\delta)$ .

Case 2: Assume  $A \neq (\alpha)$ . Since  $(\alpha) \subset A$ , this implies that  $\exists \beta \in A$  such that  $\beta \notin (\alpha)$ . The lattice basis  $(\alpha, \alpha\delta)$  specifies a rectangle with vertices  $0, \alpha, \alpha\delta$ , and  $\alpha + \alpha\delta$ . The half-lattice points of  $P$  are  $\frac{1}{2}\alpha\delta, \frac{1}{2}(\alpha + \alpha\delta)$ , and  $\alpha + \frac{1}{2}\alpha\delta$ . If we place discs of radius  $r$  about each vertex of the rectangle and discs of radius  $\frac{1}{2}r$  about each of the three half-lattice points, we cover the interior of the rectangle. By 2.3, the element  $\beta$  can be chosen so that it lies in this rectangle. Since  $\beta \notin (\alpha)$ , then it cannot be one of the vertices of the rectangle. But, by 6.2, the only points of  $A$  that lie inside any of the discs are their centers. So,  $\beta$  is one of the half-lattice points.

(1) Assume  $\beta = \frac{1}{2}\alpha\delta$ . So,  $\frac{1}{2}\alpha\delta \in A$ . Also,  $\frac{-5}{2}\alpha \in A$ . By definition of  $(\alpha)$ ,  $3\alpha \in (\alpha)$ . Hence,  $3\alpha \in A$ . So,  $3\alpha + \frac{-5}{2}\alpha = \frac{1}{2}\alpha \in A$ . But, this contradicts that  $\alpha$  is the element with minimal absolute value in  $A$ .

(2) Assume  $\beta = \alpha + \frac{1}{2}\alpha\delta$ . In this case,  $\alpha + \frac{1}{2}\alpha\delta - \alpha = \frac{1}{2}\alpha\delta \in A$ . So, this reduces to the case (1) and gives us a contradiction.

Hence,  $\beta = \frac{1}{2}(\alpha + \alpha\delta)$ . Therefore, the lattice basis for  $A$  is  $(\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ . Since  $\frac{1}{2}(\alpha + \alpha\delta) \in (\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ , but  $\frac{1}{2}(\alpha + \alpha\delta) \notin (\alpha)$ , then  $(\alpha) \neq (\alpha, \frac{1}{2}(\alpha + \alpha\delta))$ . So,  $A$  is not a principal ideal in this case.  $\square$

**Theorem 6.3.**  $C(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$ .

*Proof.* The first case of the previous theorem is the identity class of  $\mathbb{Z}[\sqrt{-5}]$ . And the second case is another ideal class. For, if  $B$  is another ideal of  $\mathbb{Z}[\sqrt{-5}]$ , then  $B = b\frac{1}{2}(1 + \delta)$ , for some  $b \in B$ . So,  $B = \frac{b}{\alpha}A$ , where  $A = \frac{1}{2}(\alpha + \alpha\delta)$  as in the proof. Therefore, the ideals in case 2 form an ideal class. Hence,  $C(\mathbb{Z}[\sqrt{-5}])$  is a group with exactly two elements. Since every group of order 2 is isomorphic to the cyclic group of order 2, we conclude that  $C(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$ .  $\square$

## References

- [1] Artin, Michael. *Algebra*, Prentice Hall, Upper Saddle River, NJ, 1991.
- [2] Cerenzia, Mark. *Paper on The Structure Theorem*.
- [3] Samuel, Pierre. *Algebraic Theory of Numbers*, Dover Publications Inc, Mineola, NY, 1970.