IDEAL CLASS GROUPS - AN INTRODUCTION

ROLAND A.

Abstract. In this expository paper, we introduce Ideal Class Groups, the context in which they arise, and the light they shed on number theory questions. We will see that the order of the finite group of ideal classes is the class number of a ring of integers, a concept that we have seen in class through the lens of quadratic forms. The key powerful idea captured by the class number is that it measures how far from being a unique factorization domain (UFD) a ring of integers is. A trivial ideal class group of order 1 corresponds to a UFD, whereas higher class numbers correspond to rings in which unique factorization of integers into primes (up to units) breaks down. A key step forward in number theory occurred in the late 19^{th} century when Kummer and Dedekind introduced the concept of ideals. In non-UFD rings where unique factorization is not satisfied for ring elements, it can be restored but at the level of new objects called ideals.

1. Introduction and Motivation

Unique factorization is a key premise that enables the familiar construction of a multiplicative theory of numbers, i.e., how numbers are constructed from primes and units. This is most commonly exhibited by the Fundamental Theorem of Arithmetic for integers in $\mathbb{Z}$.

However, answering questions about representation of integers by algebraic expressions, such as which prime integer $p \in \mathbb{N}$ can be represented as $p = x^2 + 5y^2$, with x, $y \in \mathbb{Z}$, leads us to work in rings or fields that are extensions of the integers, e.g., in $\mathbb{Z}[\sqrt{-5}]$ in this example. This is the smallest ring containing the integers and $\sqrt{-5}$.

Working in this ring, unexpected multiplicative behaviors arise, with respect to our familiarity with arithmetic in $\mathbb{Z}$. These are due to the fact that prime factorization is not unique. Indeed, it is easy to see that in $\mathbb{Z}[\sqrt{-5}]$, we have:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}). \tag{1.1}$$

While there are similar occurrences in $\mathbb{Z}$, such as with:

$$12 = 3 \cdot 4 = 2 \cdot 6, \tag{1.2}$$

things become unambiguous when we restrict ourselves to factorizations into prime integers up to units, i.e., when we only consider factorizations of the form:

$$12 = 2^2 \cdot 3, \tag{1.3}$$

and

$$-12 = (-1) \cdot 2^2 \cdot 3. \tag{1.4}$$

It turns out that, after we have defined primes and units in $\mathbb{Z}[\sqrt{-5}]$, the elements 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are all primes. Therefore, factorization into primes and units is still not unique in that ring, and that is really the crucial difference with rings that are unique factorization domains such as $\mathbb{Z}$.

This hurdle has led to the development of a concept of ideal numbers, now commonly called ideals, which are abstract algebraic structures within rings that can restore unique factorization into primes, except that the primes in question are not prime elements of the ring but prime ideals.

The theory of ideals, and especially ideal class groups which we will introduce in this paper, provides insights into how far from being a unique factorization domain a given ring is. This will be quantified with a specific number called the class number, and it corresponds to the order of a multiplicative group that can be defined on equivalence classes of ideals within the ring.

In section 2 of this paper, we recall basic notions relative to rings and fields, and we introduce the concept of ideals. Section 3 focuses on operations and arithmetic on ideals. We then get to the core of our subject in section 4 where an equivalence relation and equivalence classes are defined on ideals of rings of integers, from which a group structure and its order will emerge: the ideal class group and the class number. Section 5 wraps up the paper with examples where we highlight the difference between unique factorization domains, whose class number is 1, and rings where unique factorization breaks down for ring elements, but can be restored for ideals of such non-UFD rings.

We note the following trade-off that we have chosen to make in this paper: some results from algebraic number theory are accepted as fact, and referenced as arguments in some proofs of propositions in the paper. A longer version of this paper would have dedicated a section to cover these elements of algebraic number theory, and this would have made the paper much more self-contained and with explicit proofs of all results. However, this would have come at the cost of nearly doubling the length of the paper, and with the risk of introducing too many concepts and proofs that could distract from the focus remaining on ideal class groups and class numbers.

2. Rings, Integral Domains, Ideals, and Fields

In this section, we cover several concepts of abstract algebra that will be assumed in the later sections of this paper. For each subsection below, readers already familiar with the concepts under the subsection title can skip the corresponding section. We assume readers are already familiar with necessary background in group theory.

Definition 2.1 (*Ring*)**.** A ring $(R, +, \cdot)$ is a non-empty set with two binary operations, which we refer to as addition and multiplication, respectively, satisfying the following properties:

- $(R, +)$ is an Abelian group with the addition operation. Its identity is designated as 0.
- The multiplication operation is associative.
- The multiplication operation is distributive over the addition, i.e., for all x, y, $z \in R$, we have $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

Notation. We typically elide the $\cdot$ multiplication symbol when writing multiplicative expressions on elements of a ring.

Definition 2.2 (*Commutative Ring*)**.** A ring is said to be commutative if the multiplication operation is also commutative.

Definition 2.3 (*Unitary Ring*)**.** A ring R is said to be unitary or also a ring with one ("ring with 1"), if the multiplication operation has an identity element, which will be designated by 1_R or just 1 when the context is clear.

Going forward, we only consider rings that are commutative and unitary, as this will keep us focused on the scope relevant to our number theory area of interest.

Definition 2.4 (*Integral Domain*)**.** A ring is an *integral domain* if it has no non-zero divisors, i.e., if it satisfies the property

$$a, b \in R \text{ and } ab = 0 \implies a = 0 \text{ or } b = 0. \tag{2.1}$$

Definition 2.5 (*Ring Units*)**.** An element x of a commutative and unitary ring R is said to be a unit if it has a multiplicative inverse in the ring, i.e., if there exists an element y in R such that $xy = yx = 1$.

Example. We illustrate the definitions above with a few familiar examples of rings.

- The integers with usual addition and multiplication form a ring $(\mathbb{Z}, +, \cdot)$, with the usual 0 and 1. The set of units in $(\mathbb{Z}, +, \cdot)$ is $\{1, -1\}$. This ring is an integral domain.
- The integers modulo an integer n, $\mathbb{Z}/n\mathbb{Z}$, also form a ring with the modular addition and multiplication operations.
- If n is composite, then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain. As an example, we have $2 \cdot 3 \equiv 0 \pmod 6$, despite having both $2 \not\equiv 0 \pmod 6$ and $3 \not\equiv 0 \pmod 6$.
- If $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. All non-zero elements in this ring are units.
- An example of non-commutative ring is $\mathcal{M}_n(\mathbb{Z})$, the set of $n \times n$ matrices with integer entries.

Proposition 2.6 (*Group of Ring Units*)**.** *The set of units of a ring R is a group under the multiplication operation. We designate this group of units by $R^\times$.*

Proof. The proof is pretty straightforward as the set is non-empty and contains a multiplicative identity which is the element 1_R from the unitary ring R. Associativity, and commutativity in our area of focus, are inherited from the ring's operations. Closure under inverses is evident from the definition of a unit having a multplicative inverse in the ring.

We just show closure under multiplication: for u_1, u_2 in the set of units, there exist v_1, v_2 such that $u_1v_1 = v_1u_11$ and $u_2v_2 = v_2u_2 = 1$, and we have $(u_1u_2)(v_2v_1) = u_1(u_2v_2)v_1 = u_1v_1 = 1$, which shows that the product u_1u_2 also has a multiplicative inverse in the ring. $\square$

Definition 2.7 (*Subring*)**.** A non-empty subset of a ring R is a *subring* of R that is a ring under the same operations as R and has the same additive and multiplicative identity elements as R.

To mirror the quotient structure of a group by a normal subgroup, we introduce the concept of ideal in a ring, and it will play a similar role to that of a normal subgroup in a group. As we have chosen to only focus on commutative rings, this allows us to restrict our interest to the exclusion of left ideals and right ideals which would otherwise arise.

Definition 2.8 (*Ideal*)**.** Let R be a ring. A non-empty subset $\mathfrak{I} \subseteq R$ is an *ideal* of R if:

- $\mathfrak{I}$ is a subgroup of R under the $+$ operation.
- For any $r \in R$ and $x \in \mathfrak{I}$, $r \cdot x = x \cdot r \in \mathfrak{I}$.

A common notation for an ideal $\mathfrak{I}$ of a ring R is

$$\mathfrak{I} \trianglelefteq R.$$

Remark 2.9. We see that the second condition in the definition of an ideal is significantly stronger than simply being closed under multiplication as with a subring. There are various, colorful ways of describing this absorptive property of multiplication with ideals, such as "ideals swallow by multiplication" or "ideals are contagious for multiplication".

Definition 2.10 (*Field*)**.** A field is an integral domain with unit, in which every non-zero element has a multiplicative inverse in the field.

Example. The set of integers modulo a prime p, $\mathbb{Z}/p\mathbb{Z}$, is a field. The fact that each non-zero element has a multiplicative inverse derives from the following:

$$\forall n \in \{1, 2, \ldots, p-1\}, \gcd(n, p) = 1 \implies \exists a, b \in \mathbb{Z} \mid an + bp = 1 \implies an \equiv 1 \pmod{p}.$$

Proposition 2.11 (*Ideals in Field*)**.** *Let K be a field. The only ideals in K are (0) and K itself.*

Proof. It is clear that (0) and K are ideals. Otherwise, let $\mathfrak{I}$ be a proper and non-trivial ideal, i.e., an ideal distinct from (0) and from K. Let a be a non-zero element in $\mathfrak{I}$. Then a^{-1} exists in K, and by the absorptive multiplication property of $\mathfrak{I}$, we have $a^{-1} \cdot a \in \mathfrak{I}$, so $1_K \in \mathfrak{I}$. But then for any other $k \in K$, since $1 \in \mathfrak{I}$, we have $k \cdot 1_K \in \mathfrak{I}$, so $K \subseteq \mathfrak{I}$. □

Definition 2.12 (*Principal Ideal*)**.** An ideal $\mathfrak{I}$ of a ring R is *principal* if it is generated by a single element $a \in R$, i.e., if

$$\mathfrak{I} = \{x \in R : \exists y \in R \text{ such that } x = ay\}.$$

We denote such a principal ideal as (aR) or (Ra), or just (a) when the ring in question is clear from context.

Example. In the ring of integers $\mathbb{Z}$, the set of integer multiples of a given integer m, $(m\mathbb{Z})$, is an ideal. It is clearly an abelian group under addition, and multiplying any integer by a multiple of m results in a multiple of m. This ideal an example of a principal ideal.

Remark 2.13. One way to grasp an intuition for an ideal generated by an element a is that it is the set of all polynomials with coefficients in the ring R evaluated on the element a generating the ideal.

Proposition 2.14 (Ideal with Unit)**.** *An ideal containing a unit of its ring generates the entire ring.*

Proof. Let $u \in \mathfrak{I} \trianglelefteq R$ be a unit of the ring R with $\mathfrak{I}$ an ideal of R. Then there exists an inverse unit $v = u^{-1} \in R$ such that $vu = 1$ in the ring. Since $u \in \mathfrak{I}$ and $v \in R$, we have $1 = vu \in \mathfrak{I}$. And with $1 \in \mathfrak{I}$, for any $x \in R$, we must have $x \cdot 1 = x \in \mathfrak{I}$, so $\mathfrak{I} = R$. □

Definition 2.15 (*Proper Ideal*)**.** An ideal which is not the entire ring is said to be *proper*. If $\mathfrak{I}$ is a proper ideal of a ring R, we can denote this by

$$\mathfrak{I} \triangleleft R.$$

Definition 2.16 (*Maximal Ideal*)**.** A proper ideal is said to be *maximal* if it is maximal with respect to set inclusion among proper ideals. Said otherwise, no other proper ideal is nested between a maximal ideal and the ring of which it is a proper ideal.

Definition 2.17 (*Principal Ideal Domain*)**.** A commutative ring in which all ideals are principal is a *principal ideal domain*, also referred to as a PID. In such a ring, all ideals are generated by a single element.

Proposition 2.18 ($\mathbb{Z}$ is a PID)**.** *The ring of integers $\mathbb{Z}$ is a PID.*

Proof. We first note that if $\mathfrak{I}$ has no non-zero elements, then $\mathfrak{I} = (0) = \{0\}$, which is the trivial ideal, and it is clearly generated by a single element 0. Let $\mathfrak{I} \trianglelefteq \mathbb{Z}$ be a non-trivial ideal, so it must have at least a non-zero element, therefore at least a positive element (if $x \in \mathfrak{I}$, then $-x = (-1)x \in \mathfrak{I}$). We can order the positive elements of $\mathfrak{I}$ in increasing order, and we let a be the least positive element in $\mathfrak{I}$. This element a exists, by the least ordering principle over the natural numbers. We will show that $\mathfrak{I} = (a)$.

As mentioned above, for any $x \in \mathfrak{I}$, if $x \leq 0$, then $x = (-1)(-x)$ with $-x$ in the set of positive elements of $\mathfrak{I}$, or $x \geq 0$ in the first place, so we can focus on the non-negative elements of $\mathfrak{I}$. We use the Euclidean division algorithm, and we have:

$$x = aq + r, \text{ with } 0 \leq r < a.$$

Since $x \in \mathfrak{I}$ and $a \in \mathfrak{I} \implies aq \in \mathfrak{I}$, we must have $r = x - aq \in \mathfrak{I}$ because $\mathfrak{I}$ is a group under addition. We have just found an element $r \in \mathfrak{I}$ with $0 \leq r < a$. The only way to not contradict the minimality of a among the positive elements of $\mathfrak{I}$ is to have $r = 0$, so $x = aq$.

We have just shown that any element of the ideal $\mathfrak{I} \trianglelefteq R$ is a multiple of a single element a, where a is the least positive element of I, so $\mathfrak{I} \subseteq (a)$. Since it is clear that $a \in \mathfrak{I} \implies (a) \in \mathfrak{I}$, we have $\mathfrak{I} = (a)$, i.e., every ideal of $\mathbb{Z}$ is principal, and $\mathbb{Z}$ is a PID. □

Definition 2.19 (*Noetherian Ring*)**.** A commutative ring is a *noetherian ring* if all ideals are finitely generated, i.e., no ideal in that ring requires an infinite set to generate it.

Example (*Polynomials with Even Constant Coefficient*)*.* In the ring of polynomials with integer coefficients $\mathbb{Z}[X]$, the set of polynomials with even constant coefficient is an ideal. This ideal is not principal, however. It is generated by the set of polynomials $\{2, X\}$ and every polynomial in this ideal is of the form $2P(X) + XQ(X)$ for some $P(X)$, $Q(X) \in \mathbb{Z}[X]$. The ring $\mathbb{Z}[X]$ is therefore not a PID. This ring is in fact noetherian, though the example of a single ideal being finitely generated isn't sufficient to prove it. The Hilbert Basis Theorem proves that if a ring R is noetherian, then so is the associated polynomial ring $R[X]$ with coefficients in R.

Proposition 2.20 (Ascending Ideals in Noetherian Rings)**.** *A ring R is noetherian if and only if every infinite ascending sequence of ideals $\mathfrak{I}_1 \subseteq \mathfrak{I}_2 \subseteq \ldots \subseteq \mathfrak{I}_k \subseteq \mathfrak{I}_{k+1} \subseteq \ldots$ eventually stabilizes, i.e., there exists $n \in \mathbb{N}$ such that $\mathfrak{I}_{n+N} = \mathfrak{I}_n$ for all $N \in \mathbb{N}$.*

Proof. If the ring R is noetherian, then every ideal of R is finitely generated. We consider

$$\mathfrak{I} = \bigcup_{i=1}^{\infty} \mathfrak{I}_k.$$

We claim that $\mathfrak{I}$ is an ideal. We first show that it is an abelian group under addition:

- Identity: each of the $\mathfrak{I}_k$ contains 0 and so does their union I.
- Inverses: each element $x \in \mathfrak{I}$ is the element of some $\mathfrak{I}_k$, and so is its inverse $x^{-1} \in \mathfrak{I}_k \subseteq \mathfrak{I}$, so $\mathfrak{I}$ is closed under taking inverses.
- Closure: for any two elements $x, y \in \mathfrak{I}$, there is some k_1 and some k_2 such that $x \in \mathfrak{I}_{k_1}$ and $y \in \mathfrak{I}_{k_2}$, so $x, y \in \mathfrak{I}_{max(k_1, k_2)}$ due to the ascending sequence of the $\mathfrak{I}_k$s. Since $\mathfrak{I}_{max(k_1, k_2)}$ is an abelian subgroup, it is also closed under addition so $x + y \in \mathfrak{I}_{max(k_1, k_2)} \subseteq \mathfrak{I}$.

We now show that $\mathfrak{I}$ satisfies the multiplicative property of ideals. We let $r \in R$ and $x \in \mathfrak{I}$. Then $x \in \mathfrak{I}_k$ for some k, and since $\mathfrak{I}_k$ is an ideal, we have $rx \in \mathfrak{I}_k \subseteq \mathfrak{I}$, so $\mathfrak{I}$ has the "absorptive property of multiplication by elements of R".

Since $\mathfrak{I}$ is an ideal, it must be finitely generated, so there is a finite set $\{x_1, \ldots, x_m\} \subseteq R$ that generates $\mathfrak{I}$, i.e., we have $\mathfrak{I} = (x_1, \ldots, x_m)$. For each $i \in \{1, \ldots, m\}$, there is some ideal $\mathfrak{I}_{k_i}$ such that $x_i \in \mathfrak{I}_{k_i}$. We note that $x_i \in \mathfrak{I}_{k_i} \implies (x_i) \subseteq \mathfrak{I}_{k_i}$. We now define $n = \max(k_1, \ldots, k_m)$. By the ascending nature of the sequence of ideals, we have:

$$(x_i) \subseteq \mathfrak{I}_{k_i} \subseteq \mathfrak{I}_n \text{ for all } i \in \{1, \ldots, m\}. \tag{2.2}$$

With the equation above, we now show that the ideal $(x_1, \ldots, x_m)$ generated by the set of x_i is also a subset of $\mathfrak{I}_n$. Indeed, an element of $(x_1, \ldots, x_m)$ is a polynomial with coefficients in R in the variables $x_1, \ldots, x_m$. Each monomial in that sum is a product of x_is, each of which is in $\mathfrak{I}_n$ so the product making up the monomial is in $\mathfrak{I}_n$ because ideals are closed under multiplication. And with $\mathfrak{I}_n$ being closed under addition, the entire polynomial is in $\mathfrak{I}_n$. We have therefore shown that:

$$\mathfrak{I} = (x_1, \ldots, x_m) \subseteq \mathfrak{I}_n. \tag{2.3}$$

And we of course also have $\mathfrak{I}_n \subseteq \bigcup_{i=1}^{\infty} \mathfrak{I}_i = \mathfrak{I}$, so we have

$$\mathfrak{I} = \mathfrak{I}_n \implies \mathfrak{I}_{n+N} \subseteq \mathfrak{I} \subseteq \mathfrak{I}_n \implies \mathfrak{I}_{n+N} = \mathfrak{I}_n \text{ for all } N \in \mathbb{N}. \tag{2.4}$$

For the reverse direction, we consider an ideal $\mathfrak{I} \trianglelefteq R$ and we want to show that it is finitely generated. If $\mathfrak{I}$ is not finitely generated, let us choose $a_1 \in \mathfrak{I}$ and define a first ideal $\mathfrak{I}_1 = (a_1)$. We have $\mathfrak{I}_1 \subsetneq \mathfrak{I}$ or else $\mathfrak{I}$ would have been finitely generated. So we can pick an element $a_2 \in \mathfrak{I} \setminus (a_1)$, and form the ideal $\mathfrak{I}_2 = (a_1, a_2)$, with $\mathfrak{I}_1 \subseteq \mathfrak{I}_2$. Again since $\mathfrak{I}$ is not finitely generated, we must have $(a_1, a_2) \subsetneq \mathfrak{I}$, so we can pick an element $a_3 \in \mathfrak{I} \setminus (a_1, a_2)$, and define $\mathfrak{I}_3 = (a_1, a_2, a_3)$.

We can iterate this process indefinitely, relying on the fact that $\mathfrak{I}$ is not finitely generated, allowing us to always pick the next $a_k \in \mathfrak{I} \setminus \mathfrak{I}_{k-1}$ and form the next $\mathfrak{I}_k = (a_1, \ldots, a_k)$ in an infinite ascending sequence of ideals, where the inclusion is *strict* because each $\mathfrak{I}_k$

contains an element $a_k \in \mathfrak{I} \setminus \mathfrak{I}_{k-1}$, i.e., $a_k \notin \mathfrak{I}_{k-1}$. This contradicts the assumption that every infinite increasing sequence of ideals must stall at some point and beyond. □

We now introduce two important concepts related to rings and ideals, that extend those that we have seen for groups and normal subgroups. The first will be the concept of quotient rings obtained by defining equivalence classes on ring elements. The second will be the concept of homomorphisms of rings that extend the structure preservation to the two operations of a ring.

Proposition 2.21 (*Quotient Ring*)**.** *Let R be a commutative ring with unit, and let $\mathfrak{I}$ be an ideal of R. We define the relation on R*

$$x\mathcal{R}y \text{ if and only if } x - y \in \mathfrak{I}, \text{ for } x, y \in R. \tag{2.5}$$

This defines an equivalence relation on R. We then define addition and multiplication on these equivalence classes, and we show that this endows the equivalence classes with a ring structure. This is the quotient ring of R by $\mathfrak{I}$, denoted $R/\mathfrak{I}$.

Proof. Since the ideal $\mathfrak{I}$ is an abelian subgroup of R for addition, it is clear that $x\mathcal{R}x$ because $0 \in \mathfrak{I}$, so we have reflexivity. It is also clear that if $x\mathcal{R}y$, i.e., if $x - y \in \mathfrak{I}$, then $-(x - y) = y - x \in \mathfrak{I}$ because $\mathfrak{I}$ is closed under additive inverses, so $y\mathcal{R}x$. And if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x - y \in \mathfrak{I}$ and $y - z \in \mathfrak{I}$, so that $x - z = (x - y) + (y - z) \in \mathfrak{I}$ because $\mathfrak{I}$ is closed under addition, so $x\mathcal{R}z$ and we have transitivity. We have therefore shown that we have an equivalence relation, and that the equivalence classes partition the ring R. We will denote equivalence of two ring elements x and y by $x \sim y$.

We now define addition and multiplication on the equivalence classes $\mathfrak{I}$ as follows:

- $(x + \mathfrak{I}) + (y + \mathfrak{I}) = (x + y) + \mathfrak{I}$.
- $(x + \mathfrak{I}) \cdot (y + \mathfrak{I}) = xy + \mathfrak{I}$.

These operations are well-defined, i.e., they do not depend on the choice of representative of an equivalence class. Indeed, let $x' \in x + \mathfrak{I}$, i.e., $x - x' = i_1 \in \mathfrak{I}$ and let $y' \in y + \mathfrak{I}$, i.e., $y - y' = i_2 \in \mathfrak{I}$. Then $x' + y' = x - i_1 + y - i_2 = (x + y) - (i_1 + i_2)$, with $-(i_1 + i_2) \in \mathfrak{I}$ due to the additive group property of $\mathfrak{I}$. We have therefore shown that $(x' + y') - (x + y) \in \mathfrak{I}$, i.e., $(x' + y') \sim (x + y)$, and that addition of equivalence classes is indifferent to the choice of class representatives.

Similarly for multiplication, we have: $x'y' - xy = (x - i_1)(y - i_2) - xy = i_1i_2 - xi_2 - yi_1 \in \mathfrak{I}$, with $i_1i2 - xi_2 - yi_1 \in \mathfrak{I}$ due to the absorptive multiplication property of $\mathfrak{I}$ and its closure under addition. We have therefore shown that $x'y' \sim xy$, and that multiplication is indifferent to the choice of class representative.

From the definition of the addition and multiplication operations, it is clear that the set of equivalence classes is closed under these operations, so we have closure under the two binary operations. It is also clear that we have commutativity for both addition and multiplication, as these are inherited from those in the parent ring R.

There is an additive identity element which is $0_R + \mathfrak{I} = \mathfrak{I}$, and it is easily seen that

$x + \mathfrak{I} + \mathfrak{I} = x + \mathfrak{I}$ for all $x \in R$, so the class corresponding to the ideal $\mathfrak{I}$ itself is the additive identity element.

There is also a multiplicative identity element which is $1_R + \mathfrak{I}$, as we can verify: for $x \in \mathfrak{I}$, we have $(x + \mathfrak{I})(1_R + \mathfrak{I}) = (1_R \cdot x) + \mathfrak{I} = x + \mathfrak{I}$.

Lastly, we have additive inverses with $-(x+\mathfrak{I})$ being $(-x)+\mathfrak{I}$, as their sum is $(x+(-x))+\mathfrak{I} = 0 + \mathfrak{I} = \mathfrak{I}$.

We therefore have a ring structure on the classes modulo the ideal $\mathfrak{I}$, which we designate as the quotient ring of R by $\mathfrak{I}$: $R/\mathfrak{I}$. We also note that if the ring R has units, then the corresponding classes modulo $\mathfrak{I}$ are also units in the quotient ring $R/\mathfrak{I}$ as can be easily seen from the definition of multiplication of classes. □

Definition 2.22 (*Ring Homomorphism*)**.** We extend the concept of group homomorphisms to structure preservation with two operations, via the concept of ring homomorphisms. Specifically, we let R and R' be two rings, with additive identities 0_R and $0_{R'}$ and multiplicative identities 1_R and $1_{R'}$, respectively, and with multiplication operations $*$ and $\cdot$, respectively. A function $\phi : R \to R'$ is a ring homomorphism if it satisfies:

- $\phi(x + y) = \phi(x) + \phi(y)$ for all x, $y \in R$
- $\phi(x * y) = \phi(x) \cdot \phi(y)$ for all x, $y \in R$
- $\phi(0_R) = 0_{R'}$
- $\phi(1_R) = 1_{R'}$

Proposition 2.23 (*Subring, Ideal, and Ring Homomorphism*)**.** *Let $\phi : A \to B$ be a homomorphism from the ring A to the ring B. Then:*

- *The image by ϕ of A, $\phi(A)$, is a subring of B.*
- *If $\mathfrak{I}$ is an ideal of A, then $\phi(\mathfrak{I})$ is an ideal of $\phi(A)$. It is not necessarily an ideal of B, especially if ϕ is not surjective in B.*
- *The kernel of ϕ, i.e., the set of elements of A whose image by ϕ is 0_B is an ideal of A.*
- *If $\mathfrak{J}$ is an ideal of B, then the pre-image of $\mathfrak{J}$ by ϕ, i.e., $\phi^{-1}(\mathfrak{J})$ is an ideal of A.*

Proof. We go through each point in the proposition.

- The proof of the first point carries easily from the properties of a ring homomorphism, so we skip detailing it.
- Let $b \in \phi(\mathfrak{I})$ and let $y \in \phi(A)$. We want to show that $yb \in \phi(\mathfrak{I})$. We know that $b = \phi(a)$ for some $a \in \mathfrak{I}$, and $y = \phi(x)$ for some $x \in A$. Then $yb = \phi(x)\phi(a) = \phi(xa)$, and $xa \in \mathfrak{I}$ because $\mathfrak{I}$ is an ideal in A. Therefore $yb = \phi(xa) \in \phi(\mathfrak{I})$, which shows that $\phi(\mathfrak{I})$ is an ideal of the subring $\phi(A)$ of B. We give an example of $\phi(\mathfrak{I})$ failing to be an ideal of the entire ring B: if $A = \mathbb{Z}$ and $B = \mathbb{Q}$, with ϕ being the (trivial) inclusion embedding that sends an element of $\mathbb{Z}$ to itself as an element of $\mathbb{Q}$. We recall from *Proposition* 2.11 that the only ideals in a field are the (0) ideal and the field itself, so this is true of $\mathbb{Q}$. Yet, if we take an ideal of $\mathbb{Z}$, such as $n\mathbb{Z}$ for some $n \neq 0$, its image by the inclusion homomorphism is itself, which is neither (0) nor $\mathbb{Q}$.
- We already know that the kernel of a group homomorphism is a (normal) subgroup. We now let $r \in \ker(\phi)$ and $x \in A$. We then have $\phi(x \cdot r) = \phi(x) \cdot \phi(r) = \phi(x) \cdot 0_B = 0_B$, which shows that $x \cdot r \in \ker(\phi)$. So $\ker(\phi)$ is an ideal of A.

- Similarly, we already know that the pre-image by a group homomorphism of a subgroup of B is a subgroup of A. We now let $r \in \phi^{-1}(\mathfrak{J})$ and $x \in A$, and we want to show that $x \cdot r \in \phi^{-1}(\mathfrak{J})$. We have $\phi(x \cdot r) = \phi(x) \cdot \phi(r)$ with $\phi(x) \in B$ and $\phi(r) \in \mathfrak{J}$, so $\phi(x) \cdot \phi(r) \in \mathfrak{J}$ because $\mathfrak{J}$ is an ideal of B. This shows that $x \cdot r \in \phi^{-1}(\mathfrak{J})$, and thus $\phi^{-1}(\mathfrak{J})$ has the absorptive property of multiplication which makes it an ideal of A.

□

Theorem 2.24 (*Ring Isomorphism Theorem*)**.** *Let $\phi : A \to B$ be a homomorphism of rings. We then have*

$$A/\ker(\phi) \cong \mathrm{im}(\phi). \tag{2.6}$$

Proof. We show the isomorphism between the quotient ring and the image by defining it. We let:

$$\Psi : A/\ker(\phi) \to \mathrm{im}(\phi)$$
$$a + \ker(\phi) \mapsto \phi(a)$$

We show that Ψ is well-defined, injective, surjective, and a ring homomorphism. We already know from group theory that Ψ is well-defined, injective, surjective, and a group homomorphism. So what is left to prove is that it also preserves multiplication of the quotient ring when mapping it to the image.

Let $a + \ker(\phi)$ and $b + \ker(\phi)$ be two elements of the quotient ring. We have:

$$\Psi[(a + \ker(\phi)) \cdot (b + \ker(\phi))] = \Psi(a \cdot b + \ker(\phi)) = a \cdot b = \Psi(a + \ker(\phi)) \cdot \Psi(b + \ker(\phi)).$$

We have therefore shown preservation of the multiplicative structure as well, thus completing the proof that Ψ is an isomorphism of rings from $A/\ker(\phi)$ to $\mathrm{im}(\phi)$. □

3. Arithmetic on Ideals

In this section, we will first define a few significant types of ideals as well as operations on ideals with number theoretic significance.

Definition 3.1 (*Prime Ideal*)**.** An ideal $\mathfrak{I}$ of a ring R is said to be prime if it is proper and if whenever a, $b \in R$ are such that $ab \in \mathfrak{I}$, then either $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$.

Remark 3.2. We can see that the prime ideal definition extends to rings the concept of Euclid's Lemma, which states that in the integers, an integer p is a prime numbers if whenever $p \mid ab$ for some a, $b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Example. In the integers, a prime ideal is the set of all multiples of a prime number p, including 0. For instance, the ideals $(2\mathbb{Z})$ and $(7\mathbb{Z})$ are prime ideals in the ring of integers. The proof of this is simply a restatement of the definition of a prime number: $p \mid ab \implies p \mid a$ or $p \mid b$ is equivalent to stating that if ab is a multiple of p, then a is a multiple of p or b is a multiple of p, which is equivalent to saying that if $ab \in (p\mathbb{Z})$, then $a \in (p\mathbb{Z})$ or $b \in \mathbb{Z})$.

Example. We have already seen the example of the ideal of polynomials with integer coefficients and with even constant coefficient, when we discussed this ideal being not principal and being generated by the set of two ring elements $\{2, X\}$. This ideal is in fact a prime ideal. Indeed, if the product of two polynomials with integer coefficients has an even constant

coefficient, then at least one of the polynomials in the product must have an even constant coefficient (or else the constant coefficient of the product would be odd as the product of two odd constant coefficients).

Definition 3.3 (*Spectrum*)**.** Let R be a commutative ring with unit. We define the *spectrum* of R to be the set of its prime ideals.

$$\mathrm{Spec}(R) = \{\mathfrak{I} : \mathfrak{I} \triangleleft R, \mathfrak{I} \text{ prime}\}. \tag{3.1}$$

Proposition 3.4 (*Quotient by Prime Ideal*)**.** *Let R be a ring and $\mathfrak{I}$ an ideal of R. The ideal $\mathfrak{I}$ is prime if and only if the quotient ring $R/\mathfrak{I}$ is an integral domain.*

Proof. If $\mathfrak{I}$ is a prime ideal of R, then we consider two elements of $R/\mathfrak{I}$, say $a+\mathfrak{I}$ and $b+\mathfrak{I}$, such that their product $(a+\mathfrak{I})(b+\mathfrak{I}) = (ab+\mathfrak{I})$ is equal to the zero element of the quotient ring, i.e., $ab+\mathfrak{I} = \mathfrak{I}$. This implies that $ab \in \mathfrak{I}$. And since $\mathfrak{I}$ is prime, by definition, we must have $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, or equivalently, $a+\mathfrak{I} = \mathfrak{I}$ or $b+\mathfrak{I} = \mathfrak{I}$, which shows that $R/\mathfrak{I}$ is an integral domain.

Conversely, if $R/\mathfrak{I}$ is an integral domain, and we consider two elements $a, b \in R$ such that $ab \in \mathfrak{I}$. This implies that $ab+\mathfrak{I} = \mathfrak{I}$, and equivalently $(a+\mathfrak{I})(b+\mathfrak{I}) = \mathfrak{I}$. By the fact that $R/\mathfrak{I}$ is an integral domain, a product of two elements is the zero element implies that one of the elements is the zero element. So either $a+\mathfrak{I} = \mathfrak{I}$ or $b+\mathfrak{I} = \mathfrak{I}$. Equivalently, $a \in \mathfrak{I}$ or $b \in \mathfrak{I}$, and we have thus shown that the ideal $\mathfrak{I}$ is prime. □

Proposition 3.5 (*Pre-Image of Prime Ideal*)**.** *Let $\phi : A \to B$ be a ring homomorphism. Let $\mathfrak{J}$ be a prime ideal of B. Then $\phi^{-1}(\mathfrak{J})$, the pre-image of $\mathfrak{J}$ by ϕ, is a prime ideal of A.*

Proof. We have already shown in *Proposition* 2.23 that the pre-image of an ideal by a ring homomorphism is an ideal. We now show that if J is prime, then its pre-image is also prime.

We let $a, b \in A$ and suppose $ab \in \phi^{-1}(\mathfrak{J})$. Then $\phi(ab) = \phi(a)\phi(b) \in \mathfrak{J}$. Since $\mathfrak{J}$ is prime, we must have $\phi(a) \in \mathfrak{J}$ or $\phi(b) \in \mathfrak{J}$. This implies that $a \in \phi^{-1}(\mathfrak{J})$ or $b \in \phi^{-1}(\mathfrak{J})$. We have shown that $\phi^{-1}(\mathfrak{J})$ is a prime ideal in A. □

3.1. **Operations on Ideals and Principal Ideals.**

Proposition 3.6 (*Intersection of Principal Ideals*)**.** *Let $\mathfrak{I} = (a)$ and $\mathfrak{J} = (b)$ be principal ideals in a ring R. Then $\mathfrak{I} \cap \mathfrak{J}$ is a principal ideal generated by* $\mathrm{lcm}(a, b)$.

Proof. Let $r \in (a) \cap (b)$, then $a \mid r$ and $b \mid r$, which implies that $\mathrm{lcm}(a, b) \mid r$ as the least common multiple of two integers divides any common multiple of these integers, in this case r.

In the reverse direction, it is clear that $\mathrm{lcm}(a, b)$ is a multiple of a, therefore it is an element of (a), as well as a multiple of b, therefore it is an element of (b), and thus an element of $(a) \cap (b)$. □

Definition 3.7 (*Product of Ideals*)**.** Let $\mathfrak{I}$ and $\mathfrak{J}$ be ideals of a ring R. We define the product ideal as the ideal generated by products of elements from $\mathfrak{I}$ and from $\mathfrak{J}$. Equivalently, it is

the set of finite sums of products

$$\mathfrak{I}\mathfrak{J} = \{\sum_{i=1}^{n} x_i y_i : x_i \in \mathfrak{I},\, y_i \in \mathfrak{J},\, n \in \mathbb{N}\}. \tag{3.2}$$

Proposition 3.8 (*Product of Principal Ideals*)**.** *Let $\mathfrak{I} = (a)$ and $\mathfrak{J} = (b)$ be principal ideals in a ring R. Then the product ideal of $\mathfrak{I}$ and $\mathfrak{J}$ is $\mathfrak{I}\mathfrak{J} = (a)(b) = (ab)$, i.e., it is the principal ideal generated by the product of a and b.*

Proof. Let $r \in \mathfrak{I}\mathfrak{J} = (a)(b)$. Then, by definition of the product of ideals, $r = \sum_{i=1}^{n} x_i y_i$ with $x_i \in (a)$ and $y_i \in (b)$, i.e., $r = \sum_{i=1}^{n} r_i a r_i' b = (\sum_{i=1}^{n} r_i r_i')ab$ for some set of r_i, $r_i' \in R$, which shows that $r \in (ab)$. So $(a)(b) \subseteq (ab)$.

The reverse direction is simple as $r \in (ab) \implies r = r'ab$ for some $r' \in R$. With $r = r'a \cdot b$, we have expressed r as the product of an element of (a) (which is $r'a$) and an element of (b) (which is b itself). So $(ab) \subseteq (a)(b)$. □

Definition 3.9 (*Sum of Ideals*)**.** Let $\mathfrak{I}$ and $\mathfrak{J}$ be two ideals of a ring R. We define the sum ideal of $\mathfrak{I}$ and $\mathfrak{J}$ as the ideal generated by sums of elements from $\mathfrak{I}$ and from $\mathfrak{J}$. Since each ideal is an abelian subgroup for addition, any element of the sum ideal is itself just the sum of an element of $\mathfrak{I}$ with an element of $\mathfrak{J}$.

$$\mathfrak{I} + \mathfrak{J} = (\{x + y : x \in \mathfrak{I},\, y \in \mathfrak{J}\}) = \{x + y : x \in \mathfrak{I},\, y \in \mathfrak{J}\}. \tag{3.3}$$

Proposition 3.10. *The sum of ideals is a well-defined ideal.*

Proof. The set $\mathfrak{I} + \mathfrak{J}$ inherits the properties of addition and multiplication of its parent ring R, so we focus on showing that it is a subgroup under addition and that it has the absorptive multiplication property.

It is clear that $\mathfrak{I} + \mathfrak{J}$ is non-empty and has the additive identity element as $0 = 0 + 0$. Let $r = x + y \in \mathfrak{I} + \mathfrak{J}$, with $x \in \mathfrak{I}$ and $y \in \mathfrak{J}$ and $r' = x' + y' \in \mathfrak{I} + \mathfrak{J}$ with $x' \in \mathfrak{I}$ and $y' \in \mathfrak{J}$. Then $r - r' = (x - x') + (y - y')$ with $x - x' \in \mathfrak{I}$ and $y - y' \in \mathfrak{J}$ as $\mathfrak{I}$ and $\mathfrak{J}$ are additive (abelian) subgroups. So $r - r' \in \mathfrak{I} + \mathfrak{J}$. This proves that $\mathfrak{I} + \mathfrak{J}$ is a subgroup of R under addition.

We now let $r \in R$ and $a = x + y \in \mathfrak{I} + \mathfrak{J}$, with $x \in \mathfrak{I}$ and $y \in \mathfrak{J}$. Then $ra = r(x + y) = rx + ry$ with $rx \in \mathfrak{I}$ and $ry \in \mathfrak{J}$ thanks to the absorptive multiplication property of $\mathfrak{I}$ and of $\mathfrak{J}$. So $ra \in \mathfrak{I} + J$, and we have shown that $\mathfrak{I} + \mathfrak{J}$ is an ideal. □

Proposition 3.11 (*Sum of Principal Ideals*)**.** *Let $\mathfrak{I} = (a)$ and $\mathfrak{J} = (b)$ be principal ideals in a Euclidean or norm-Euclidean ring R. Then*

$$(a) + (b) = (d), \text{ where } d = \gcd(a, b). \tag{3.4}$$

Proof. Let $r = x + y$ with $x \in (a)$ and $y \in (b)$, then $x = x'a$ and $y = y'b$ for some a, $a' \in R$, so that $r = x'a + y'b$. If r is an integer linear equation in a and b, then r must be a multiple of $\gcd(a, b)$, so $r \in (gcd(a, b))$. We note that we needed the Euclidean property to have a well-defined gcd.

In the reverse direction, let $r \in (d)$ where $d = \gcd(a, b)$. We therefore have $r = zd$ for some $z \in R$. By Bézout's Lemma, or the extended Euclidean Algorithm, there are x, $y \in R$

such that $d = xa + yb$, with $xa \in (a)$ and $yb \in (b)$ by the absorptive multiplicative property of ideals. So we have shown that $d \in (a) + (b)$ and consequently $(d) \subseteq (a) + (b)$ because all multiples of d such as $r = zd$ are in the ideal $(a) + (b)$ if d is in it. □

3.2. **Field of Fractions and Fractional Ideals.** As one of the last required algebraic structures needed before introducing ideal class groups, we need to introduce fractional ideals. These ideals are generally defined with respect to a structure called the field of fractions of our integral domain of interest. We will see that such fractional ideals can sometimes be contained within our ring of interest, but not always. The field of fractions of an integral domain generalizes the relationship that $\mathbb{Q}$ plays with respect to $\mathbb{Z}$.

Definition 3.12 (*Field of Fractions*)**.** Given an integral domain that is also unitary R and with $R^*=\backslash\{0\}$, we define an equivalence relation on $R \times R^*$ by setting

$$(n,\, d) \sim (n',\, d') \text{ if and only if } nd' = n'd. \tag{3.5}$$

It is trivial to see that the relation is reflexive and symmetric, so we just show that it is transitive. We let $(n,\, d)$, $(n',\, d')$, $(n'',\, d'')$ be in $R \times R^*$, with $(n,\, d) \sim (n',\, d')$ and $(n',\, d') \sim (n'',\, d'')$. We then have:

$$nd' = n'd \implies n''nd' = n''n'd,$$

and

$$n'd'' = n''d' \implies nn'd'' = nn''d',$$

so that, with $n''nd' = nn''d'$ by commutativity, we have:

$$n''n'd = nn'd'', \text{ i.e., } n'(n''d - nd'') = 0.$$

If $n' = 0$, then we must also have $n = n'' = 0$ because $nd' = n'd$ and$n'd'' = n''d'$ and we clearly have $nd'' = n''d = 0$. Otherwise, and since we are in an integral domain, $n' \neq 0$ implies that the other factor $n''d - nd'' = 0$, and we have proven transitivity.

With the equivalence relation in place, we denote an equivalence class by $\frac{n}{d}$. We then define addition and multiplication on the equivalence classes with

$$\frac{n}{d} + \frac{n'}{d'} = \frac{nd' + n'd}{dd'}, \tag{3.6}$$

and

$$\frac{n}{d} \cdot \frac{n'}{d'} = \frac{nn'}{dd'}. \tag{3.7}$$

It can be verified but we will skip it for the sake of brevity that this is a field structure on the equivalence classes which are the fractions. The class with 0 as numerator is the additive identity, and the class of $\frac{1}{1}$ is the multiplicative identity, and the additive inverse of $\frac{n}{d}$ is $\frac{-n}{d}$ and the multiplicative inverse of a non-zero element $\frac{n}{d}$ is $\frac{d}{n}$. We note that commutativity of multiplication is derived from the integral domain R being commutative by definition.

We also note that the unitary integral domain R can be naturally embedded into its field of fractions via the injection that maps $r \in R$ to the class $\frac{r}{1}$ in the field of fractions. In fact,

even if the integral domain R did not have a unit, we could still embed R into its field of fractions by mapping $r \in R$ to $\frac{rx}{x}$ with $x \neq 0$, and the embedding is insensitive to the choice of $x \neq 0$ because such fractions $\frac{x}{x}$ are all one equivalence class.

We now proceed with the definition of fractional ideals in the context of the field of fractions. First, we recall that a module generalizes the notion of vector space over a field, by relaxing the condition of field to a less restrictive condition of ring.

Definition 3.13 (*Module over a Ring*)**.** A set M is a *module over a ring* R or an *R-module* if $(M, +)$ is a commutative ring, and there is a so-called scalar multiplication operation between elements of R (the scalars) and elements of the module with results in the module, with the following properties. For all r, $s \in R$ and m_1, $m_2 \in M$, we have:

- $r \cdot m_1 \in M$
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$
- $(r + s)m_1 = r \cdot m_1 + s \cdot m_1$
- $(rs) \cdot m_1 = r \cdot (s \cdot m_1)$
- $1 \cdot m_1 = m_1$

The last condition above can be dropped if the ring R is not unitary. When R is not commutative, there are distinct definitions of left-modules and right-modules, but we will confine our interest in two-sided modules with the assumption of working with R being integral and unitary too.

Definition 3.14 (*Sub-Module*)**.** A subset M' of a module M over a ring R is a *sub-module* if it is an abelian subgroup of $(M, +)$ and is also closed under the scalar multiplication operation.

Remark 3.15. In our context, we will restrict ourselves to modules or sub-modules that are *finitely generated* also known as *of finite dimension*. This definition is identical to the definition for vector spaces, i.e., it refers to modules that have a *finite basis* of n elements, and such that every element of the module can be expressed as a linear combination of the n module elements, with coefficients of the linear combination being elements of the ring over which our module is defined.

We now get to the definition of a fractional ideal which will be at the core of our ideal class group discussion.

Definition 3.16 (*Fractional Ideal*)**.** Let R be a ring and K its field of fractions. A subset $\mathfrak{I}$ of the field of fractions K is a *fractional ideal of* R if $\mathfrak{I}$ an R-submodule of the field of fractions K such that there exists $r \in R^*$ satisfying $r\mathfrak{I} \subseteq \mathfrak{I}$.

We can think of the elements of $\mathfrak{I}$ as having a common denominator r, and of multiplication of elements of $\mathfrak{I}$ by r as clearing their denominator.

Even though we have already defined ideals of a ring R as just ideals when they are subsets of R, these ideals are sometimes referred to as *integral ideals* for contrast, when the context also includes *fractional ideals*. So we formalize the definition in the following.

Definition 3.17 (*Integral Ideal*)**.** When a fractional ideal $\mathfrak{I}$ is contained within the ring R, we refer to it as an *integral ideal*.

Definition 3.18 (*Principal Fractional Ideal*)**.** A fractional ideal $\mathfrak{I}$ of a ring R with field of fractions K is a *principal fractional ideal* if it is generated by a single, non-zero element of K.

3.3. **Dedekind Domains.** We end this section with a brief introduction of Dedekind domains before getting into ideal class groups, the core subject of this paper in the next section. As we have seen in *Equation* 1.1 at the start of the paper, some rings do not exhibit unique factorization into primes up to units. Historically speaking, the concept of ideals came about as an attempt to remedy what could not be done with ring elements (such as unique prime factorization) by doing it with so-called "ideal numbers", which we now call ideals. Dedekind domains are algebraic structures that exhibit unique factorization into primes, but at the level of ideals rather than at the level of ring elements.

Definition 3.19 (*Dedekind Domain*)**.** We let R be a commutative ring with unit as well as an integral domain. R is said to be a *Dedekind domain* if every non-zero proper ideal of R factors into a product of prime ideals, with factoring in the sense of the ideal multiplication as defined in *Definition* 3.7.

We end with a few properties of Dedekind domains.

Proposition 3.20 (*Fractional Ideals in Dedekind Domains*)**.** *In a Dedekind domain, every non-zero fractional ideal is multiplicatively invertible.*

Proposition 3.21 (*Ideal Inclusion and Divisibility*)**.** *Let R be a Dedekind domain, and $\mathfrak{I}_1$ and $\mathfrak{I}_2$ two ideals in R. Then, $\mathfrak{I}_1 \subseteq \mathfrak{I}_2$ if and only if $\mathfrak{I}_2$ divides $\mathfrak{I}_1$ as ideals, i.e., if and only if there exists an ideal $\mathfrak{a}$ such that $\mathfrak{I}_1 = \mathfrak{I}_2\mathfrak{a}$.*

Proposition 3.22 (*PIDs are Dedekind Domains*)**.** *A Principal Ideal Domain is a Dedekind domain.*

Proposition 3.23. *A Dedekind domain is a PID if and only if it is a Unique Factorization Domain.*

4. Ideal Classes and Ideal Class Group

We briefly introduce algebraic numbers, algebraic integers, and the ring of integers of an algebraic field.

Definition 4.1 (*Algebraic Number*)**.** An *algebraic number* is a complex number that is a root of a polynomial with coefficients in $\mathbb{Q}$.

Definition 4.2 (*Algebraic Integer*)**.** An *algebraic integer* is a complex number that is a root of a *monic* polynomial with coefficients in $\mathbb{Z}$.

Definition 4.3 (*Algebraic Number Field*)**.** A subfield K of $\mathbb{C}$ is called an algebraic number field if $[K : \mathbb{Q}]$ is finite.

Definition 4.4 (*Ring of Algebraic Integers*)**.** With $K \subseteq \mathbb{C}$ an algebraic number field, the subset of K consisting of algebraic integers forms a ring $\mathcal{O}_K$, called the ring of algebraic integers in K, or the ring of integers in K.

We now introduce an equivalence relation on ideals of the ring of integers $\mathcal{O}_K$, from which the equivalence classes will be the main object of our remaining study.

Definition 4.5. Let $\mathfrak{I}_1$ and $\mathfrak{I}_2$ be ideals fo $\mathcal{O}_K$. We define the relation $\mathcal{R}$ on ideals of $\mathcal{O}_K$ as:

$$\mathfrak{I}_1 \mathcal{R} \mathfrak{I}_2 \iff \exists \alpha, \beta \in \mathcal{O}_K,\ \alpha, \beta \neq 0, \text{ such that } (\alpha)\mathfrak{I}_1 = (\beta)\mathfrak{I}_2. \tag{4.1}$$

Proposition 4.6 (*Ideal Equivalence*)**.** *The relation on ideals as defined above is an equivalence relation.*

Proof. We prove that the relation is reflexive, symmetric, and transitive.

- Reflexive: for any $\alpha \neq 0$ in $\mathcal{O}_K$ and any $\mathfrak{I} \trianglelefteq \mathcal{O}_K$, we have $(\alpha)\mathfrak{I} = (\alpha)\mathfrak{I}$.
- Symmetric: obviously true by switching the positions of α and $\mathfrak{I}_1$ with those of β and $\mathfrak{I}_2$, respectively.
- Transitive: we suppose $(\alpha)\mathfrak{I}_1 = (\beta)\mathfrak{I}_2$ and $(\beta')\mathfrak{I}_2 = (\gamma)\mathfrak{I}_3$, then

  $$(\alpha)(\beta')\mathfrak{I}_1 = (\beta)(\beta')\mathfrak{I}_2 = (\beta)(\gamma)\mathfrak{I}_3 \implies (\alpha\beta')\mathfrak{I}_1 = (\beta\gamma)\mathfrak{I}_3,$$

  and $\alpha\beta' \neq 0$, $\alpha\beta' \in \mathcal{O}_K$ and $\beta\gamma \neq 0$, $\beta\gamma \in \mathcal{O}_K$ because $\mathcal{O}_K$ is a ring, thus closed under multiplication and is an integral domain, thus a product of non-zero elements cannot be zero.

We have therefore shown that we have an equivalence relation on non-zero ideals of $\mathcal{O}_K$. □

Definition 4.7 (*Ideal Classes*)**.** The equivalence relation above partitions the non-zero ideals of $\mathcal{O}_K$ into equivalence classes, which we call *ideal classes* of $\mathcal{O}_K$.

Although we haven't proven it at this point, it turns out that the number of ideal classes of an algebraic number field K is always finite, so it is relevant to make mention of this number.

Definition 4.8 (*Class Number*)**.** The number of ideal classes is called the *class number* of the field K, and is denoted h_K.

Proposition 4.9 (*Class Number of a PID*)**.** *The class number h_K is equal to 1 if and only if the ring of integers of K , $\mathcal{O}_K$, is a Principal Ideal Domain, i.e., if and only if every ideal $\mathfrak{I} \trianglelefteq \mathcal{O}_K$ is a principal ideal, of the form (α) for some $\alpha \in \mathcal{O}_K$.*

Proof. If $\mathcal{O}_K$ is a PID, then every ideal is of the form (α) with $\alpha \in \mathcal{O}_K$. As a result, any two ideals (α) and (β) are in the same equivalence class because we have:

$$(\beta)(\alpha) = (\alpha)(\beta) = (\alpha\beta) \implies (\alpha) \sim (\beta).$$

We therefore have a single equivalence class, and $h_K = 1$.

In the reverse direction, we suppose that $h_K = 1$, i.e., all ideals are equivalent. We recall that $\mathcal{O}_K$ itself is an ideal, as is always the case with a ring. So for any ideal $\mathfrak{I} \trianglelefteq \mathcal{O}_K$, we have

$$\mathfrak{I} \sim \mathcal{O}_K \implies \exists \alpha,\, \beta \in \mathcal{O}_K \mid (\alpha)\mathfrak{I} = (\beta)\mathcal{O}_K = (\beta).$$

Since $(\alpha)\mathfrak{I} \subseteq (\alpha)$, we have $(\beta) \subseteq (\alpha)$, i.e., α divides β. Therefore, we have that $\frac{\beta}{\alpha} \in \mathcal{O}_K$, so there is some $\gamma \in \mathcal{O}_K$ such that $\beta = \alpha\gamma$.

We now have $(\alpha)\mathfrak{I} = (\alpha\gamma) = (\alpha)(\gamma)$. Here too, we rely on an algebraic number theory result that lets us conclude that $\mathfrak{I} = (\gamma)$, with $\gamma \in \mathcal{O}_K$, so $\mathfrak{I}$ is a principal ideal in $\mathcal{O}_K$. This completes the proof that $\mathcal{O}_K$ is a Principal Ideal Domain. □

Remark 4.10. We recall that in a Dedekind domain, being a PID is equivalent to being a UFD. Thus, when the class number of a field K is equal to 1, the corresponding ring of integers $\mathcal{O}_K$ is a PID and therefore a UFD.

Remark 4.11. In the interest of brevity, we will skip detailing the proof that h_K is always finite. The key idea in the proof is to study an n-dimensional lattice and to use a pigeonhole principle to show that any fractional ideal is in the same coset of $\mathcal{O}_K/\mathfrak{I}$ as an integral ideal, and to use an algebraic number theory result that there are finitely many cosets in that quotient ring.

The key consequence of the fact that all fractional ideals reside within the same classes as the integral ideals, is to allow manipulations on ideals where an integral ideal can be (multiplicatively) inverted and we get a fractional ideal, which can be multiplied by the ideal generated by some ring element to clear its denominator and get an integral ideal again, invert that one again, etc., all the while remaining in the same ideal class.

We now prove an important proposition that will enable us to define a group structure on ideal classes.

Proposition 4.12 (*Powers of Ideal Become Principal*)**.** *For any ideal $\mathfrak{I} \trianglelefteq \mathcal{O}_K$, there is some integer m, with $1 \leq m \leq h_K$, such that $\mathfrak{I}^m$ is principal.*

Proof. We consider the set of ideals $\{\mathfrak{I}^i : 1 \leq i \leq h_K + 1\}$. Since there is a total of h_K ideal classes, at least two of these ideals must fall within the same class. We suppose $\mathfrak{I}^i \sim \mathfrak{I}^j$, with $i < j$. By definition of being in the same class, there exist $\alpha,\, \beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{I}^i = (\beta)\mathfrak{I}^j$. We set $m = j - i$, and we have:

$$(\alpha)\mathfrak{I}^i = (\beta)\mathfrak{I}^m\mathfrak{I}^i. \tag{4.2}$$

As reasoned above in the proof of *Proposition* 4.9, we have $\frac{\alpha}{\beta}\mathfrak{I}^i \subseteq \mathfrak{I}^i$, and $\frac{\alpha}{\beta} \in \mathcal{O}_K$, i.e., β divides α. If we set $\gamma = \frac{\alpha}{\beta}$, we now have

$$(\gamma)\mathfrak{I}^i = \mathfrak{I}^m\mathfrak{I}^i.$$

We apply the same result that we referenced in the reverse direction proof of *Proposition* 4.9 and we conclude that $\mathfrak{I}^m = (\gamma)$, i.e., $\mathfrak{I}^m$ is principal. □

We now show that the set of ideal classes can be endowed with a group structure by defining a multiplication operation on the ideal classes derived from the multiplication on the ideals. The identity element is the class of principal ideals, and each ideal class has an inverse class.

Proposition 4.13 (*Ideal Class Group*)**.** *We consider the set of classes of ideals in $\mathcal{O}_K$, and we designate the class of the ideal $\mathfrak{I}$ by $[\mathfrak{I}]$. We define the multiplication operation on ideal classes as $[\mathfrak{I}][\mathfrak{J}] = [\mathfrak{I}\mathfrak{J}]$. This endows the set of ideal classes in $\mathcal{O}_K$ with a group structure.*

Proof. We first show that the operation is well-defined, i.e., that it does not depend on the choice of representative of the class.

Let $[\mathfrak{I}_1] = [\mathfrak{I}_2]$ and $[\mathfrak{J}_1] = [\mathfrak{J}_2]$. Then, there are α_1, β_1, α_2, $\beta_2 \in \mathcal{O}_K$ such that

$$(\alpha_1)\mathfrak{I}_1 = (\alpha_2)\mathfrak{I}_2,$$

and

$$(\beta_1)\mathfrak{J}_1 = (\beta_2)\mathfrak{J}_2,$$

so that

$$(\alpha_1)(\beta_1)\mathfrak{I}_1\mathfrak{J}_1 = (\alpha_2)(\beta_2)\mathfrak{I}_2\mathfrak{J}_2,$$

i.e.,

$$(\alpha_1\beta_1)\mathfrak{I}_1\mathfrak{J}_1 = (\alpha_2\beta_2)\mathfrak{I}_2\mathfrak{J}_2,$$

which shows that

$$[\mathfrak{I}_1\mathfrak{J}_1] = [\mathfrak{I}_2\mathfrak{J}_2].$$

Associativity (and commutativity, for that matter) is inherited from associativity of the operation on ideals.

The identity element is the class of $\mathcal{O}_K$, which is the class of all the principal ideals.

Lastly, in *Proposition* 4.12 we have shown that $\mathfrak{I}^m$ is principal for some m, $1 \leq m \leq h_K$. This means that $[\mathfrak{I}^m]$ is equal to the identity element $[\mathcal{O}_K]$. So the inverse of $[\mathfrak{I}]$ is $[\mathfrak{I}^{m-1}]$.

We therefore have a multiplicative group structure on the classes of ideals of $\mathcal{O}_K$, and the order of the group is h_K. □

We now prove two propositions that allow us to prove the theorem that any ideal in $\mathcal{O}_K$ can be uniquely factored into prime ideals.

Proposition 4.14 (*Cross Division*)**.** *Let $\mathfrak{I}_1$, $\mathfrak{I}_2$, and $\mathfrak{I}_3$ be ideals in $\mathcal{O}_K$. If $\mathfrak{I}_1\mathfrak{I}_2 = \mathfrak{I}_1\mathfrak{I}_3$, then $\mathfrak{I}_2 = \mathfrak{I}_3$.*

Proof. By *Proposition* 4.12, there is an integer m,$1 \leq m \leq h_K$ and an algebraic integer $\alpha \in \mathcal{O}_K$ such that $\mathfrak{I}_1^m = (\alpha)$.

We have

$$\mathfrak{I}_1\mathfrak{I}_2 = \mathfrak{I}_1\mathfrak{I}_3 \implies \mathfrak{I}_1^{m-1}\mathfrak{I}_1\mathfrak{I}_2 = \mathfrak{I}_1^{m-1}\mathfrak{I}_1\mathfrak{I}_3 \implies (\alpha)\mathfrak{I}_2 = (\alpha)\mathfrak{I}_3.$$

An element of $(\alpha)\mathfrak{I}_2$ is of the form $\sum_i \alpha x_i \cdot y_i$, with $x_i \in \mathcal{O}_K$ and $y_i \in \mathfrak{I}_2$. This is equal to $\alpha \sum_i x_i y_i$, and $\sum_i x_i y_i$ is just the form of any element of $\mathfrak{I}_2$. So any element of $(\alpha)\mathfrak{I}_2$ is of the form αx with $x \in \mathfrak{I}_2$. Similarly, every element of $(\alpha)\mathfrak{I}_3$ is of the form αy, with $y \in \mathfrak{I}_3$.

But by equality of $(\alpha)\mathfrak{I}_2 = (\alpha)\mathfrak{I}_3$, any element αx with $x \in \mathfrak{I}_2$ is equal to αy for some $y \in \mathfrak{I}_3$. We pick a non-zero element αx in $(\alpha)\mathfrak{I}_2$, and we have:

$$\alpha x = \alpha y \iff \alpha(x - y) = 0 \implies x = y,$$

where the last implication above is because $\mathcal{O}_K$ is an integral domain. This shows that $\alpha x \in \mathfrak{I}_3$, and consequently $\mathfrak{I}_2 \subseteq \mathfrak{I}_3$.

The argument is completely symmetric in the two ideals, so we conclude that $\mathfrak{I}_2 = \mathfrak{I}_3$. □

Proposition 4.15 (*Containing is Dividing*)**.** *If $\mathfrak{I}$ and $\mathfrak{J}$ are in $\mathcal{O}_K$, and $\mathfrak{I} \subseteq \mathfrak{J}$. Then there is an ideal $\mathfrak{H}$ such that $\mathfrak{J}\mathfrak{H} = \mathfrak{I}$.*

Proof. Let $\mathfrak{J}^m = (\alpha)$. Then we have:

$$\mathfrak{I}\mathfrak{J}^{m-1} \subseteq \mathfrak{J}\mathfrak{J}^{m-1} = (\alpha).$$

The ideal inclusion $\mathfrak{I}\mathfrak{J}^{m-1} \subseteq (\alpha)$ shows that α divides every element in the ideal $\mathfrak{I}\mathfrak{J}^{m-1}$. We set $\mathfrak{H} = \left(\frac{1}{\alpha}\right)\mathfrak{J}^{m-1}\mathfrak{I}$, which is an ideal in $\mathcal{O}_K$, and we have:

$$\mathfrak{J}\mathfrak{H} = \mathfrak{J}\mathfrak{J}^{m-1}\left(\frac{1}{\alpha}\right)\mathfrak{I} = (\alpha)\left(\frac{1}{\alpha}\right)\mathfrak{I} = \mathfrak{I}.$$

□

Proposition 4.16 (*Factorization into Prime Ideals*)**.** *Every non-zero ideal in $\mathcal{O}_K$ can be written as a product of prime ideals.*

Proof. The ideal $\mathcal{O}_K$ is trivially prime, so we focus on proper ideals. Let $\mathfrak{I}$ be a proper ideal in $\mathcal{O}_K$. We accept an algebraic number theory result that $\mathcal{O}_K/\mathfrak{I}$ is finite. Then, there is some maximal $\mathfrak{P}_1$ such that $\mathfrak{I} \subseteq \mathfrak{P}_1$. By *Proposition* 4.15, there is some ideal $\mathfrak{Q}_1$ such that $\mathfrak{I} = \mathfrak{P}_1\mathfrak{Q}_1$. If $\mathfrak{Q}_1 \subsetneq \mathcal{O}_K$, then it is contained in some maximal ideal $\mathfrak{P}_2$, and then $\mathfrak{I} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{Q}_2$. If $\mathfrak{Q}_2 \subsetneq \mathcal{O}_K$, we continue the process, while building a strictly ascending chain of proper ideals

$$\mathfrak{I} \subset \mathfrak{Q}_1 \subset \mathfrak{Q}_2 \subset \dots$$

But accept as fact an algebraic number theory result that $\mathcal{O}_K$ is noetherian. So the ascending chain must stabilize after some finite number of steps, i.e., $\mathfrak{Q}_r = \mathcal{O}_K$ for some $r \in \mathbb{N}$. This implies

$$\mathfrak{I} = \mathfrak{P}_1 \dots \mathfrak{P}_r \text{ for some finite } r \in \mathbb{N}, \tag{4.3}$$

with all $\mathfrak{P}_i$ in the product being prime ideals. □

Proposition 4.17 (*Powers of Prime Ideal*)**.** *Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. The chain of ideals $\mathfrak{P} \supset \mathfrak{P}^2 \supset \mathfrak{P}^3 \supset \dots$ is a strictly descending chain of ideals.*

Proof. If $\mathfrak{P}^m = \mathfrak{P}^{m+1}$ for some m, then by a lemma that requires viewing an ideal as a finitely generated module over the ring (and which we omit proving), we would have $\mathfrak{P} = \mathcal{O}_K$. This is a contradiction because a prime ideal is proper, by definition. □

Definition 4.18 (*Order of a Prime Ideal in an Ideal*)**.** Let $\mathfrak{I}$ be an ideal in $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. We define the order of $\mathfrak{P}$ in $\mathfrak{I}$, and denote it by $\operatorname{ord}_{\mathfrak{P}} \mathfrak{I}$, to be the unique non-negative integer m such that $\mathfrak{P}^m \supseteq \mathfrak{I}$ and $\mathfrak{P}^{m+1} \not\supseteq \mathfrak{I}$.

Proposition 4.19 (*Properties of Order of Prime in Ideal*)**.** *Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. Then*

(1) $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P} = 1$.
(2) If $\mathfrak{P}' \neq \mathfrak{P}$ is a prime ideal in $\mathcal{O}_K$, then $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P}' = 0$.
(3) If $\mathfrak{I}$ and $\mathfrak{J}$ are two ideals in $\mathcal{O}_K$, then $\operatorname{ord}_{\mathfrak{P}} \mathfrak{I}\mathfrak{J} = \operatorname{ord}_{\mathfrak{P}} \mathfrak{I} + \operatorname{ord}_{\mathfrak{P}} \mathfrak{I}$.

Proof. We prove each of the claims in the proposition.

(1) We clearly have $\mathfrak{P} \supseteq \mathfrak{P}$ so $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P} \geq 1$. If $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P} \geq 2$, then $\mathfrak{P}^2 \supseteq \mathfrak{P}$, which implies $\mathfrak{P}^2 = \mathfrak{P}$. This implies $\mathfrak{P} = \mathcal{O}_K$ by the same lemma that we have referred to in *Proposition* 4.17. But a prime ideal is proper, so we have a contradiction, and $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P} = 1$.
(2) If $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P}' \geq 1$, then $\mathfrak{P} \supseteq \mathfrak{P}'$. We accept as fact that every prime ideal of $\mathcal{O}_K$ is maximal, so we must have $\mathfrak{P} \supseteq \mathfrak{P}'$, in contradiction of the assumption. So $\operatorname{ord}_{\mathfrak{P}} \mathfrak{P}' = 0$.
(3) Let $i = \operatorname{ord}_{\mathfrak{P}} \mathfrak{I}$ and $j = \operatorname{ord}_{\mathfrak{P}} \mathfrak{J}$. Then, by *Proposition* 4.15, there are ideals $\mathfrak{I}'$ and $\mathfrak{J}'$ such that

$$\mathfrak{I} = \mathfrak{P}^i \mathfrak{I}' \text{ and } \mathfrak{J} = \mathfrak{P}^j \mathfrak{J}',$$

and by definition of the order of the prime ideal in another ideal, we also have

$$\mathfrak{P} \not\supseteq \mathfrak{I}' \text{ and } \mathfrak{P} \not\supseteq \mathfrak{J}'. \tag{4.4}$$

We now consider the ideal $\mathfrak{I}\mathfrak{J} = \mathfrak{I}'\mathfrak{J}'\mathfrak{P}^{i+j}$. If $\mathfrak{P}^{i+j+1} \supseteq \mathfrak{I}\mathfrak{J}$, then by *Proposition* 4.15, we have

$$\mathfrak{P}^{i+j+1}\mathfrak{H} = \mathfrak{I}\mathfrak{J} \text{ for some ideal } \mathfrak{H}.$$

And by *Proposition* 4.14, we must have

$$\mathfrak{P}\mathfrak{H} = \mathfrak{I}'\mathfrak{J}',$$

therefore

$$\mathfrak{P} \supseteq \mathfrak{I}'\mathfrak{J}'.$$

Since $\mathfrak{P}$ is prime, this implies

$$\mathfrak{P} \supseteq \mathfrak{I}' \text{ or } \mathfrak{P} \supseteq \mathfrak{J}',$$

and this contradicts *Equation* 4.4. So $\operatorname{ord}_{\mathfrak{P}} \mathfrak{I}\mathfrak{J} = i + j$.

We therefore have

$$\operatorname{ord}_{\mathfrak{P}} \mathfrak{I}\mathfrak{J} = \operatorname{ord}_{\mathfrak{P}} \mathfrak{I} + \operatorname{ord}_{\mathfrak{P}} \mathfrak{J}.$$

□

We are now equipped to state the theorem of *unique* factorization of ideals in $\mathcal{O}_K$ into prime ideals of $\mathcal{O}_K$.

Theorem 4.20 (*Unique Factorization of Ideals into Prime Ideals*)**.** *Let $\mathfrak{I}$ be an ideal of $\mathcal{O}_K$. We recall that the spectrum of the ring $\mathcal{O}_K$ is its set of prime ideals, and is denoted by* $\mathrm{Spec}(\mathcal{O}_K)$*. Then,*

$$\mathfrak{I} = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)} \mathfrak{P}^{\mathrm{ord}_{\mathfrak{P}} \mathfrak{I}}, \tag{4.5}$$

and we note that all but finitely many of the exponents $\mathrm{ord}_{\mathfrak{P}} \mathfrak{I}$ *are zero.*

Proof. We already know from *Proposition* 4.17 that such a decomposition into a product of prime ideals exists. So we really need to show the value of each exponent being uniquely determined.

We pick a particular prime ideal $\mathfrak{P}_0$, and we start from an initial prime decomposition with unknown exponents $\mathfrak{I} = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)} \mathfrak{P}^{e(\mathfrak{P})}$, and we apply $\mathrm{ord}_{\mathfrak{P}_0}$ to the equality with unknown exponents, and we have:

$$\mathrm{ord}_{\mathfrak{P}_0} \mathfrak{I} = \sum_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)} e(\mathfrak{P}) \, \mathrm{ord}_{\mathfrak{P}_0} \mathfrak{P} = e(\mathfrak{P}_0), \tag{4.6}$$

which shows that the exponent $e(\mathfrak{P}_0)$ of the ideal $\mathfrak{P}_0$ in the product of $\mathfrak{I}$ into powers of prime factors is equal to $\mathrm{ord}_{\mathfrak{P}_0} \mathfrak{I}$, i.e., it is the order of the prime ideal $\mathfrak{P}_0$ in the ideal $\mathfrak{I}$. □

Lemma 4.21. *Let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. We take it as fact that $\mathfrak{P} \cap \mathbb{Z}$ is not zero, as this is a result from algebraic number theory. But $\mathfrak{P} \cap \mathbb{Z}$ is also a prime ideal of $\mathbb{Z}$, so it is generated by a prime number p.*

Definition 4.22 (*Ramification*)**.** We consider a prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$, and the natural prime number p as obtained in *Lemma* 4.21. We let (p) be the principal ideal generated by p in the ring of integers $\mathbb{O}_K$. We define the *ramification index* of $\mathfrak{P}$ to be

$$e = \mathrm{ord}_{\mathfrak{P}}(p).$$

If $e = \mathrm{ord}_{\mathfrak{P}}(p) \geq 2$, we say that the prime p *ramifies* in the ring of integers $\mathcal{O}_K$.

Definition 4.23 (*Degree*)**.** We state without proving that the quotient ring $\mathcal{O}_K/\mathfrak{P}$ is a finite field containing $\mathbb{Z}/p\mathbb{Z}$. By a well-known result of finite fields, the number of elements in the field is a power of p, say p^f, for some $f \geq 1$. Then f is called the degree of the prime ideal $\mathfrak{P}$.

We end with the mention of an important algebraic number theory result that we state without proof.

Proposition 4.24 (*Equation in Ramification, Degree, and Field Dimension*)**.** *Let $p \in \mathbb{N}$ be a prime number and let $\mathfrak{P}_1$, $\mathfrak{P}_2$, …, $\mathfrak{P}_r$ be the prime ideals in $\mathcal{O}_K$ containing the principal ideal (p) of $\mathcal{O}_K$. We recall that $[K : \mathbb{Q}] = n$. Let e_i and f_i be the ramification index and degree of each prime ideal $\mathfrak{P}_i$, for $1 \leq i \leq r$.*

By Theorem 4.20*, we have* $(p) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$*. Then,*

$$\sum_{i=1}^{r} e_i f_i = n. \tag{4.7}$$

5. Examples

In this section, we illustrate via concrete examples the concepts of unique factorization when it exists at the level of ring elements, or at the level of ideals when it fails at the level of ring elements.

5.1. **Ring of Gaussian Integers $\mathbb{Z}[i]$.** We start with the ring of Gaussian integers $\mathbb{Z}[i]$ in which unique factorization exists for non-zero ring elements. Indeed, $\mathbb{Z}[i]$ is a norm-Euclidean domain with the norm being $N(a + bi) = a^2 + b^2$. This implies that it is a Principal Ideal Domain (PID), which in turn implies that it is a Unique Factorization Domain (UFD).

The units in this ring are ± 1, $\pm i$. In this ring, some rational primes remain prime, as is the case with odd primes p with $p \equiv 3 \pmod 4$ such as 3, 7, 11, etc.

Other odd rational primes split into distinct prime factors that are conjugate of one another, as is the case with $5 = (2 + i)(2 - i) = (1 - 2i)(1 + 2i)$, and these factorizations are unique up to units, e.g., $1 + 2i = i(2 - i)$ and $1 - 2i = (-i)(2 + i)$.

Lastly and interestingly, the rational prime 2 factors as $2 = (1 + i)(1 - i)$, but we note that $1 - i = i(1 + i)$, so that the factorization of 2 is in fact $2 = i(1 + i)^2$, with $1 + i$ a prime in $\mathbb{Z}[i]$ and i a unit. This is an example of *ramification* as seen in the context of ideals above. The rational integer 2 *ramifies* in $\mathbb{Z}[i]$.

In this simple case of a PID and UFD, all ideals are principal by definition of a PID, and all ideals $\mathfrak{I}$ and $\mathfrak{J}$ are related to each other by a relation of the type $(\alpha)\mathfrak{I} = (\beta)\mathfrak{J}$ for some α, $\beta \in \mathbb{Z}[i]$. Indeed, since $\mathbb{Z}[i]$ is a PID, $\mathfrak{I} = (a)$ for some $a \in \mathbb{Z}[i]$ and $\mathfrak{J} = (b)$ for some $b \in \mathbb{Z}[i]$, so we can pick $\alpha = b$ and $\beta = a$, and we have our desired ideal equality by having $(a)(b) = (a)(b)$.

We therefore have a single equivalence class among ideals, and the corresponding ideal class group is the trivial group. This ideal class group being the trivial group is characteristic of being in a PID, therefore in a UFD.

5.2. **Quadratic Imaginary Ring $\mathbb{Z}[\sqrt{-5}]$.** We have started the paper with an illustrative example in *Equation* 1.1 of how unique factorization into primes up to units breaks down in this ring. We want to show that the theory of ideals that we have developed in this paper restores unique factorization into primes, except that this will be a factorization of ideals into prime ideals.

We start by mentioning a technicality that allows us to use the results of the previous section. We have developed the previous section on ideal classes and ideal class groups in the context of a ring of integers $\mathcal{O}_K$ of an algebraic field K which is a finite extension of $\mathbb{Q}$.

It is a fact that if the algebraic field K is $\mathbb{Q}[\sqrt{-5}]$, then its ring of integers $\mathcal{O}_{\mathbb{Q}[\sqrt{-5}]}$ is $\mathbb{Z}[\sqrt{-5}]$. This allows us to use the theory developed in the previous section for our ring $\mathbb{Z}[\sqrt{-5}]$ of interest. We note that it is not always the case that the ring of integers of an algebraic field takes this "nice" form where the ring of integers is simply $\mathbb{Z}$ to which we adjoin the same element $\sqrt{-5}$ that defined the field $K = \mathbb{Q}[\sqrt{-5}]$ as an extension of $\mathbb{Q}$.

Going back to *Equation* 1.1, we have:

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

Noting that the norm of $a + b\sqrt{-5} = a^2 + 5b^2$, with a, $b \in \mathbb{Z}$, we see that the equality above has the equality among norms:

$$36 = N(6) = N(2) \cdot N(3) = 4 \cdot 9 = N(1 + \sqrt{-5}) \cdot N(1 - \sqrt{-5}) = 6 \cdot 6.$$

Even though 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$, we can see that the norms 4, 9, 6, and 6 are not prime. From a purely intuitive standpoint, the product of norms above is "begging for" the existence of "more primitive objects", let's call them p_1, p_2, p_3, p_4, such that we might have

$$2 = p_1 \cdot p_2, \qquad 3 = p_3 \cdot p_4, \qquad 1 + \sqrt{-5} = p_1 \cdot p_3, \qquad 1 - \sqrt{-5} = p_2 \cdot p_4.$$

Of course, by the fact that our ring elements 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ are irreducible, there are no such objects in the ring itself, especially as the only units of $\mathbb{Z}[\sqrt{-5}]$ are ± 1. However, this is where the theory of ideals and ideal classes comes in.

We consider the following ideals:

$$\mathfrak{P}_1 = (2,\, 1 + \sqrt{-5}),$$
$$\mathfrak{P}_2 = (2,\, 1 - \sqrt{-5}),$$
$$\mathfrak{P}_3 = (3,\, 1 + \sqrt{-5}),$$
$$\mathfrak{P}_4 = (3,\, 1 - \sqrt{-5}),$$

which are generated by pairs of ring elements of $\mathbb{Z}[\sqrt{-5}]$.

We make the remark that if we had been in a PID, then each of these ideals generated by two elements would have been a principal ideal generated by the gcd of these two elements. So we can think of these ideals that seem to appear out of thin air as "stand-ins" for what would have been a principal ideal generated by a gcd.

We now note that $\mathfrak{P}_1 = \mathfrak{P}_2$. Indeed, it is sufficient to show that $1 + \sqrt{-5} \in \mathfrak{P}_2$ and that $1 - \sqrt{-5} \in \mathfrak{P}_1$. We have:

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

so it is a linear combination of 2 and $1 - \sqrt{5}$ with coefficients in $\mathbb{Z}$, therefore it is an element of the ideal generated by 2 and $1 - \sqrt{-5}$, i.e., it is an element of $\mathfrak{P}_2 = (2,\, 1 - \sqrt{-5})$. Since we trivially have $2 \in (2,\, 1 - \sqrt{-5})$, we have shown that

$$\mathfrak{P}_1 \subseteq \mathfrak{P}_2.$$

We also have:

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

which shows that $1 - \sqrt{-5} \in \mathfrak{P}_1 = (2,\, 1 + \sqrt{-5})$, and subsequently

$$\mathfrak{P}_2 \subseteq \mathfrak{P}_1.$$

This completes the proof that

$$\mathfrak{P}_1 = \mathfrak{P}_2.$$

We can now verify that we have the following ideal equalities:

$$\mathfrak{P}_1\mathfrak{P}_2 = (2),$$

$$\mathfrak{P}_3\mathfrak{P}_4 = (3),$$

$$\mathfrak{P}_1\mathfrak{P}_3 = (1 + \sqrt{-5}),$$

$$\mathfrak{P}_2\mathfrak{P}_4 = (1 - \sqrt{-5}).$$

We only show one of these equalities, leaving the others for the reader to verify. Let us show that $\mathfrak{P}_3\mathfrak{P}_4 = (3)$. We recall from the arithmetic on ideals that an element of a product of two ideals is a sum of products of elements of each, i.e.,

$$x \in \mathfrak{P}_3\mathfrak{P}_4 \implies x = \sum_i a_i b_i, \text{ with } a_i \in \mathfrak{P}_3,\, bi \in \mathfrak{P}_4,$$

and

$$a_i \in \mathfrak{P}_3 \implies a_i = a_i'(3) + a_i''(1 + \sqrt{-5}), \text{ with } a_i',\, a_i'' \in \mathbb{Z},$$

and

$$b_i \in \mathfrak{P}_4 \implies b_i = b_i'(3) + b_i''(1 - \sqrt{-5}), \text{ with } b_i',\, b_i'' \in \mathbb{Z},$$

so that:

$$\begin{aligned}
x &= \sum_i a_i b_i \\
&= \sum_i \left(a_i'(3) + a_i''(1+\sqrt{-5})\right)\left(b_i'(3) + b_i''(1-\sqrt{-5})\right) \\
&= \sum_i 9a_i'b_i' + 3a_i'b_i''(1-\sqrt{-5}) + 3a_i''b'i(1+\sqrt{-5}) + 6a_i''b_i'' \\
&= 3\left[(3a_i'b_i' + a_i'b_i'' + a_i''b_i' + 2a_i''b_i'') + (a_i''b'i - a_i'b_i'')\sqrt{-5}\right] \\
&= 3(\alpha + \beta\sqrt{-5}) \text{ with } \alpha,\, \beta \in \mathbb{Z} \\
&\in (3), \text{ where } (3) \text{ is the ideal generated by 3 in } \mathbb{Z}[\sqrt{-5}].
\end{aligned}$$

We have therefore shown that

$$\mathfrak{P}_3\mathfrak{P}_4 \subseteq (3).$$

We now note that:

$$3 = 3 \cdot 3 - (1+\sqrt{-5})(1-\sqrt{-5}) = 9 - 6 = a_1b_1 - a_2b_2,$$

with

$$a_1 = 3 \in \mathfrak{P}_3,\, a_2 = 3 \in \mathfrak{P}_4,\, b_1 = 1+\sqrt{-5} \in \mathfrak{P}_3,\, b_2 = 1-\sqrt{-5} \in \mathfrak{P}_4.$$

This shows that:

$$3 \in \mathfrak{P}_3\mathfrak{P}_4, \text{ i.e., } (3) \subseteq \mathfrak{P}_3\mathfrak{P}_4.$$

We have therefore shown that

$$(3) = \mathfrak{P}_3\mathfrak{P}_4.$$

Having shown how to obtain unique factorization of ideals into prime ideals through the example above, we gather a few relevant results in $\mathbb{Z}[\sqrt{-5}]$ before concluding the section with a few directions of further interest in other rings.

We do not show it here but the class number of the field $\mathbb{Q}[\sqrt{-5}]$ is 2. The proofs of this result rely on defining norms of ideals, showing that all ideal classes are represented by some finite set of integral ideals of bounded norm, and on using a pigeonhole principle to argue that all ideals, whether integral or fractional, are represented in this finite set of classes (in our case 2).

In our example of the ring $\mathbb{Z}[\sqrt{-5}]$, the ideal class group has order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and there is simply one class of principal ideals, and another class of non-principal ideals. According to the only possible multiplication table for a group of order 2, the product of a principal ideal and a non-principal ideal is non-principal, and the product of two non-principal ideals is principal.

Some examples of representatives of the two classes are as follows.
The principal class:

$$\mathcal{C}_1 \supseteq \left\{(1) = \mathbb{Z}[\sqrt{-5}],\, (\sqrt{-5}),\, (2) = \mathfrak{P}_2^2,\, \mathfrak{P}_2\mathfrak{P}_3 = (1+\sqrt{-5}),\, \mathfrak{P}_2\mathfrak{P}_4 = (1-\sqrt{-5})\right\}$$

The non-principal class:

$$\mathcal{C}_2 \supseteq \left\{(2,\, 1+\sqrt{-5}) = \mathfrak{P}_2,\, (3,\, 1+\sqrt{-5}) = \mathfrak{P}_3,\, (3,\, 1-\sqrt{-5}) = \mathfrak{P}_4\right\}$$

One can check that the group multiplication table for the two classes is the only one possible for a group that is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, i.e.:

Ideal Class	$\mathcal{C}_1$	$\mathcal{C}_2$
$\mathcal{C}_1$	$\mathcal{C}_1$	$\mathcal{C}_2$
$\mathcal{C}_2$	$\mathcal{C}_2$	$\mathcal{C}_1$

We end this sub-section by listing a few results relative to the ideals generated by integral primes in the ring $\mathbb{Z}[\sqrt{-5}]$. We have the following:

- The ideal (2) ramifies because $(2) = \mathfrak{P}_1^2 = \mathfrak{P}_2^2$.
- The ideal (5) ramifies because $(5) = \left(\sqrt{-5}\right)^2$.
- For $p \equiv 11, 13, 17, 19 \pmod{20}$, the ideal (p) remains *inert*, i.e., it is prime in $\mathbb{Z}[\sqrt{-5}]$.
- For $p \equiv 1, 3, 7, 9 \pmod{20}$, the ideal (p) *splits*, i.e., it is the product of distinct ideals.

5.3. **More General Rings.** There are other rings where the group order is higher than 2 and the group multiplication table more elaborate. In such rings where the order of elements varies, we might have some some non-principal ideal classes whose product is a principal ideal, and others where the product is still non-principal, as there are several non-principal classes in the ideal class group.

Rings such as $\mathbb{Z}[\sqrt{-23}]$ or $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ present such more elaborate structure between ideal classes, due to having ideal class groups of higher order than 2, thus more complex group multiplication tables. Furthermore, one can look at non-imaginary quadratic rings for other directions of exploration.

In the course of researching this topic, one may come across concepts of algebraic number theory that shed new light on quadratic form concepts that we have covered in class. In particular, norms and discriminants are obtained in the context of operators on finitely generated modules and determinants or traces of their associated matrices in given bases of the modules.

6. Acknowledgements

I would like to thank Andrei Mandelshtam for his help in making this paper more focused, in addition to his support throughout the class. Sincere thanks go to Simon Rubinstein-Salzedo for his never-ending efforts to inspire students to pursue and research challenging mathematical questions. His love of math and the energy and passion he puts into teaching it are truly humbling. Lastly, I would like to acknowledge and thank my peers in the Euler Circle for their stimulating questions and interactions throughout the class.

References

[1] "A Classic Introduction to Modern Number Theory", Kenneth Ireland, Michael Rosen, 2nd Edition, Springer (1990).
[2] "An unorthodox introduction to algebraic number theory" (YouTube video playlist), Billy Woods, *https://www.youtube.com/playlist?list=PLSibAQEfLnTwq2-zCB-t9v2WvnnVKd0wn*.