GENERALIZED FACTORIZATION

GRANT LARSEN

Abstract. Familiarly, in $\mathbb{Z}$, we have unique factorization. We investigate the general ring and what conditions we can impose on it to necessitate analogs of unique factorization. The trivial ideal structure of a field, the extent to which primary decomposition is unique, that a Noetherian ring necessarily has one, that a principal ideal domain is a unique factorization domain, and that a Dedekind domain has unique prime decomposition, are all covered. The relationship of quadratic reciprocity and the class group to the question of factorization is discussed, and Gauss's method of computing the class number of quadratic fields and new work generalizing this to many other fields is briefly advertised.

Contents

1. Introduction

Factoring in $\mathbb{Z}$ is something we're taught to do in elementary school and is taken for granted. If one doesn't pursue a mathematics education, one rarely realizes that the existence of unique factorization is something that needs to be proven. Fortunately, in $\mathbb{Z}$, the proof is simple number theory. When we generalize to more interesting rings than $\mathbb{Z}$, unique factorization no longer necessarily holds: the clichéd example is $\mathbb{Z}\left(\sqrt{-5}\right)$, in which $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$[†]. So what is to be done? Luckily, Kummer, Dedekind, Hilbert, and Noether have worked hard on this question and come up with the concept of ideals - sets of numbers where we can talk about factoring in all the domains that matter. The first half of this paper talks about how we can decompose ideals in which situations. The second half investigates the interesting questions of how factoring works in extensions, how

Date: AUGUST 17, 2007.

[†]It is not immediate that these numbers are distinct primes, but it is not hard to show.

quadratic reciprocity is related to the answer, how ideal factoring and numerical factoring are related, and how to compute the extent to which the latter fails.

2. Conventions

- All rings are assumed to be commutative and have $1 \neq 0$.
- The whole ring will in general be denoted R.
- The word "unique" always carries the caveat "up to ordering."

All conventions hold as far as is convenient; deviations will be explicitly noted.

3. Prelimaries

Definition 3.1. Let R be a ring. A non-empty subset $\mathfrak{a} \subseteq R$ that is closed under addition, and for which $ra \in \mathfrak{a}$ for each $r \in R$ and $a \in \mathfrak{a}$, is called an **ideal** of R. An ideal that is not equal to the ring is called a **proper ideal**. The ideal $\{0\}$ is often denoted 0.

Proposition 3.2. *Let F be a ring. Then F is a field if and only if the only proper ideal of F is 0.*

Proof. Suppose F is a field. Let $\mathfrak{a}$ be a proper ideal, and $a \in \mathfrak{a}$. Then $a \neq 0$ implies that $a^{-1}x \in F$ for every $x \in F$, so $x \in \mathfrak{a}$ for every $x \in F$, so $\mathfrak{a} = F$, contradicting the properness of $\mathfrak{a}$, so $\mathfrak{a} = 0$, since an ideal is defined to be non-empty.

Suppose now that the only proper ideal of F is 0. Let $x \in F \setminus 0$. Then xF is a non-zero ideal, since $x \in xF$. By assumption, $xF = F$. Particularly, $1 \in xF$, so there is a $y \in F$ such that $xy = 1$. Therefore F is a field. □

Definition 3.3. Let A be a set. The smallest ideal that contains A can easily be shown to be

$$\mathfrak{a} = \left\{ \sum_{i=1}^{n} a_i r_i \mid n \in \mathbb{N}, a_i \in A, r_i \in R \right\}, \tag{3.4}$$

and is called the ideal **generated by** A, and A is its **generating set** or **set of generators**. We write $\mathfrak{a} = (A)$. If $\mathfrak{a}$ is generated by a finite set, say $A = \{a_1, \ldots, a_n\}$, we write $\mathfrak{a} = (a_1, \ldots, a_n)$, and say it is **finitely generated**.

Definition. Set and ideal operations:

$$A + B = \{a + b \mid a \in A, b \in B\}, \quad A, B \subseteq R. \tag{3.5}$$

$$rA = \{ra \mid a \in A\}, \quad A \subseteq R, r \in R. \tag{3.6}$$

$$\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}, \quad \mathfrak{a}, \mathfrak{b} \text{ ideals of } R. \tag{3.7}$$

$$\mathfrak{a} : \mathfrak{b} = \{x \in R \mid xb \in \mathfrak{a} \ \forall b \in \mathfrak{b}\}, \quad \mathfrak{a}, \mathfrak{b} \text{ ideals of } R. \tag{3.8}$$

The following are direct consequences of the definitions.

Proposition 3.9. *Properties of ideal operations:*

(1) $\mathfrak{a} \cap \mathfrak{b}$ is an ideal,
(2) $\mathfrak{a} + \mathfrak{b}$ is an ideal,
(3) $\mathfrak{a} : \mathfrak{b}$ is an ideal,

(4) $\mathfrak{ab}$ *is an ideal,*
(5) $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b}$,
(6) $(\mathfrak{a} : \mathfrak{b})\, \mathfrak{b} \subseteq \mathfrak{a}$,
(7)

$$\left(\bigcap_{i \in I} \mathfrak{a}_i \right) : \mathfrak{b} = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b}),$$

(8) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{bc})$, *and*
(9) $(a)(b) = (ab)$.

Definition 3.10. Let $\mathfrak{a}$ be an ideal. Then its **radical**, $\operatorname{Rad}(\mathfrak{a})$, is given by $\{x \in R \mid \exists n \in \mathbb{N} \text{ such that } x^n \in \mathfrak{a}\}$.

Proposition 3.11. *Let* $\mathfrak{a}$ *be an ideal. Then* $\operatorname{Rad}(\mathfrak{a})$ *is an ideal.*

Proof. Given $x, y \in \operatorname{Rad}(\mathfrak{a})$, there are $m, n \in \mathbb{N}$ such that $x^m, y^n \in \mathfrak{a}$. Also, there are $\alpha_i, \mu_i, \nu_i \in \mathbb{N} \cup \{0\}$ such that

$$(x+y)^{m+n} = \sum_{i=0}^{m+n} \alpha_i x^{\mu_i} y^{\nu_i}. \tag{3.12}$$

For each i, $\mu_i + \nu_i = m+n$, so either $\mu_i \geq m$ or $\nu_i \geq n$. Therefore, $x^{\mu_i} \in \mathfrak{a}$ or $y^{\nu_i} \in \mathfrak{a}$, so $\alpha_i x^{\mu_i} y^{\nu_i} \in \mathfrak{a}$ for every i. Hence, $(x+y)^{m+n} \in \mathfrak{a}$, so $x+y \in \operatorname{Rad}(\mathfrak{a})$, i.e. $\operatorname{Rad}(\mathfrak{a})$ is closed under addition. For any $r \in R$, $(rx)^n = r^n x^n \in \mathfrak{a}$, so $rx \in \operatorname{Rad}(\mathfrak{a})$. Thus, $\operatorname{Rad}(\mathfrak{a})$ is an ideal of R. □

4. Primary Decomposition

Definition 4.1. A proper ideal $\mathfrak{p}$ is **prime** in R if for every $ab \in \mathfrak{p}$, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Proposition 4.2. *If* $\mathfrak{p}, \mathfrak{p}_i$ *are all prime ideals and*

$$\prod_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{p}, \tag{4.3}$$

then there is a $k \leq n$ *such that* $\mathfrak{p}_k \subseteq \mathfrak{p}$.

Proof. Assume that for each i, $\mathfrak{p}_i \nsubseteq \mathfrak{p}$. Then for each i, there is a $p_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, so

$$\prod_{i=1}^{n} p_i \in \prod_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{p}. \tag{4.4}$$

But $\mathfrak{p}$ is prime, so there is a $k \leq n$ such that $p_k \in \mathfrak{p}$, contradicting the method by which the p_i were selected. Therefore, there is a $k \leq n$ such that $\mathfrak{p}_k \subseteq \mathfrak{p}$. □

Definition 4.5. A **primary ideal** is an ideal $\mathfrak{q}$ such that $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$ imply there exists an $n \in \mathbb{N}$ such that $b^n \in \mathfrak{q}$.

Proposition 4.6. *Let* $\mathfrak{q}$ *be a primary ideal in* R. *Let* $\mathfrak{p} = \operatorname{Rad}(\mathfrak{q})$. *Then* $\mathfrak{p}$ *is a prime ideal, and for all prime ideals* $\mathfrak{p}' \supseteq \mathfrak{q}$, $\mathfrak{p}' \supseteq \mathfrak{p} \supseteq \mathfrak{q}$.

Proof. $\mathfrak{p}$ is an ideal by Proposition 3.11. If $xy \in \mathfrak{p}$ and $x \notin \mathfrak{p}$, then there is an $n \in \mathbb{N}$ such that $x^n y^n \in \mathfrak{q}$. Since we assume $x \notin \mathfrak{p}$, it follows that $x^n \notin \mathfrak{q}$, so there is an $m \in \mathbb{N}$ such that $y^{nm} \in \mathfrak{q}$, i.e. $y \in \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime. $\mathfrak{q} \subseteq \mathfrak{p}$ trivially. For any prime ideal $\mathfrak{p}' \supseteq \mathfrak{q}$, given $x \in \mathfrak{p}$, there must be an $n \in \mathbb{N}$ such that $x^n \in \mathfrak{q} \subseteq \mathfrak{p}'$. $\mathfrak{p}'$ is prime, so $x \in \mathfrak{p}'$, so $\mathfrak{p} \subseteq \mathfrak{p}'$. □

Definition 4.7. In the situation of the Proposition 4.6, $\mathfrak{q}$ **belongs** to $\mathfrak{p}$, and it is called $\mathfrak{p}$**-primary**.

Corollary 4.8. *Let $\mathfrak{q}$ be $\mathfrak{p}$-primary. Then:*

(1) For any $ab \in \mathfrak{q}$ such that $a \notin \mathfrak{p}$, $b \in \mathfrak{q}$,
(2) For any ideals $\mathfrak{ab} \subseteq \mathfrak{q}$ such that $\mathfrak{a} \nsubseteq \mathfrak{p}$, $\mathfrak{b} \subseteq \mathfrak{q}$, and
(3) $\mathfrak{a} \nsubseteq \mathfrak{p}$ implies $\mathfrak{q} : \mathfrak{a} = \mathfrak{q}$.

Proof. (1) is an immediate consequence of the definitions, and (2) follows immediately from (1). For (3), we know that $(\mathfrak{q} : \mathfrak{a})\,\mathfrak{a} \subseteq \mathfrak{q}$, so by (2) , $\mathfrak{q} : \mathfrak{a} \subseteq \mathfrak{q}$. We also know that $\mathfrak{q} \subseteq \mathfrak{q} : \mathfrak{a}$, so $\mathfrak{q} : \mathfrak{a} = \mathfrak{q}$. □

Definition 4.9. Let $\mathfrak{a}$ be an ideal. If

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i, \tag{4.10}$$

where each $\mathfrak{q}_i$ is primary, $\mathfrak{a}$ has a **primary decomposition**, $\mathfrak{a}$ is called **decomposable**, and the $\mathfrak{q}_i$ are called the **primary components** of the decomposition. A decomposition in which no $\mathfrak{q}_j$ contains the intersection of the remaining $\mathfrak{q}_i$ is **irredundant**. An irredundant decomposition in which all the $\mathfrak{q}_i$ are distinct is a **normal decomposition**.

Knowing these terms, we can claim a certain level of uniqueness to primary decomposition, when it exists:

Theorem 4.11. *If the ideal*

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i = \bigcap_{j=1}^{n} \mathfrak{q}'_j, \tag{4.12}$$

where both are normal decompositions, $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for every i, and $\mathfrak{q}'_j$ is $\mathfrak{p}'_j$-primary for every j, then $m = n$, and the components can be indexed such that $\mathfrak{p}_i = \mathfrak{p}'_i$ for every i.

Proof. If $\mathfrak{a} = R$, then $n = m = 1$ and $\mathfrak{q}_1 = \mathfrak{q}'_1 = R$.

Otherwise, $\mathfrak{a}$ is a proper ideal. From the finite set $\{\mathfrak{p}_i\}_{i \le m} \cup \{\mathfrak{p}'_j\}_{j \le n}$ of prime ideals, we may select one which is not strictly a subset of any other. Assume without loss of generality that this is $\mathfrak{p}_m$.

Assume that $\mathfrak{q}_m \nsubseteq \mathfrak{p}'_j$ for all j. Then by Corollary 4.8(3) , $\mathfrak{q}'_j : \mathfrak{q}_m = \mathfrak{q}'_j$, so

$$\mathfrak{a} : \mathfrak{q}_m = \bigcap_{j=1}^{n} (\mathfrak{q}'_j : \mathfrak{q}_m) = \bigcap_{j=1}^{n} \mathfrak{q}'_j = \mathfrak{a}. \tag{4.13}$$

If m were 1, $\mathfrak{a}$ would be $\mathfrak{q}_m$, so by the above, $\mathfrak{a}$ would be R, the case handled previously, so in the case at bar, m must be greater than 1. By the selection of $\mathfrak{p}_m$, $\mathfrak{p}_m \nsubseteq \mathfrak{p}_i$ for every $i < m$, since the decomposition is normal. Therefore by Proposition 4.6, $\mathfrak{q}_m \nsubseteq \mathfrak{p}_i$. This lets Corollary 4.8(3) be applied, giving $\mathfrak{q}_i : \mathfrak{q}_m = \mathfrak{q}_i$. Since $\mathfrak{q}_m : \mathfrak{q}_m = R$,

$$\mathfrak{a} : \mathfrak{q}_m = \bigcap_{i=1}^{m} (\mathfrak{q}_i : \mathfrak{q}_m) = \bigcap_{i=1}^{m-1} \mathfrak{q}_i. \tag{4.14}$$

Combining (4.13) and (4.14),

$$\mathfrak{a} = \bigcap_{i=1}^{m-1} \mathfrak{q}_i. \tag{4.15}$$

This contradicts the normality of the decomposition in (4.12), so our assumption must be false, i.e. there must exist a $j \leq m$ such that $\mathfrak{q}_m \subseteq \mathfrak{p}'_j$. By Proposition 4.6, $\mathfrak{p}_m \subseteq \mathfrak{p}'_j$, so by the selection of $\mathfrak{p}_m$, $\mathfrak{p}_m = \mathfrak{p}'_j$. Assume without loss of generality that $\mathfrak{p}_m = \mathfrak{p}'_n$. By definition, $\mathfrak{q}_m \cap \mathfrak{q}'_n$ belongs to $\mathfrak{p}_m = \mathfrak{p}'_n$. By similar arguments to those above,

$$\bigcap_{i=1}^{m-1} \mathfrak{q}_i = \mathfrak{a} : \mathfrak{q} = \bigcap_{j=1}^{n-1} \mathfrak{q}'_j. \tag{4.16}$$

Since $\mathfrak{a} : \mathfrak{q}$ is an ideal, we are in the same position we started in, now with $n-1$ and $m-1$.

Assume $m < n$. After m recursions of the above process, one would get

$$R = \bigcap_{j=1}^{n-m} \mathfrak{q}'_j, \tag{4.17}$$

but the composition was normal, so all the $\mathfrak{q}'_j$ should have been proper, contradicting (4.17), so $m \not< n$.

A perfectly analogous argument shows $n \not< m$, so $m = n$, and after $m = n$ steps of this recursive process, all $m = n$ pairs of equal prime ideals have been identified. □

Definition 4.18. The prime ideals proved to be unique in Theorem 4.11 are called **the prime ideals belonging to $\mathfrak{a}$**.

5. Noetherian Rings

In general we can't get any more unique than the above decomposition, and Theorem 4.11 rests on the condition that such a decomposition exists. We can make a step in the right direction by demanding the following property:

Definition 5.1. A ring R is **Noetherian** if, given an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ of ideals, there is an $m \in \mathbb{N}$ such that for all $n \geq m$, $\mathfrak{a}_n = \mathfrak{a}_m$.

Proposition 5.2. *Given a ring R, TFAE:*

1. *R is Noetherian;*
2. *Every non-empty set of ideals has a maximal element with respect to inclusion;*
3. *Every proper ideal is finitely generated.*

Proof. Suppose R is Noetherian. Let I be a non-empty set of ideals of R.

If I is finite, the existence of a maximal element is trivial.

Otherwise, pick $\mathfrak{a}_1 \in I$. Given $\mathfrak{a}_i \in I$, there is an $\mathfrak{a}'_i \in I$ such that $\mathfrak{a}_i \subseteq \mathfrak{a}'_i$. Let $\mathfrak{a}_{i+1} = \mathfrak{a}'_i$. The assumption that R is Noetherian implies that this chain is eventually the same ideal over and over, and this ideal is necessarily maximal. Therefore, we have (1) ⇒ (2).

Suppose now that (2) holds. Let $\mathfrak{a}$ be an ideal of R, let A be the set of finitely generated ideals contained in $\mathfrak{a}$, and let $\mathfrak{m}$ be a maximal element of A.

Assume that there is an element $x \in \mathfrak{a} \setminus \mathfrak{m}$. Then $\mathfrak{m} + xR$ is finitely generated, so $\mathfrak{m} + xR \in A$. But $\mathfrak{m} + xR \supsetneq \mathfrak{m}$, contradicting the maximality of $\mathfrak{m}$ in A. Therefore $\mathfrak{m} = \mathfrak{a}$, i.e. $\mathfrak{a}$ is finitely generated. This reveals that (2) $\Rightarrow$ (3).

Suppose now that every ideal of R is finitely generated. Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ be an ascending chain of ideals of R. Let

$$\mathfrak{A} = \bigcup_{i \in \mathbb{N}} \mathfrak{a}_i. \tag{5.3}$$

$\mathfrak{A}$ is an ideal in R, so it is generated by a finite set, say $\{a_1, \dots, a_n\}$, by assumption. Then for every $i \in \mathbb{N}$, $\mathfrak{a}_i \subseteq (a_1, \dots, a_n)$. For every $j \leq n$, there is a k_j such that $a_j \in \mathfrak{a}_{k_j}$. Let $k' = \max\{k_j\}_{j \leq n}$. Then for each $j \leq n$, $a_j \in \mathfrak{a}_{k'}$. Therefore $\mathfrak{a}_{k'} \supseteq (a_1, \dots, a_n)$, so $\mathfrak{a}_{k'} = (a_1, \dots, a_n)$. Therefore, for all $i \geq k'$, $\mathfrak{a}_i = \mathfrak{a}_{k'}$. So, we have (3) $\Rightarrow$ (1). □

In this case, the situation is slightly improved, but in order to see why, we must introduce a new concept:

Definition 5.4. An ideal $\mathfrak{a}$ is **irreducible** if whenever $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$. An ideal that is not irreducible is **reducible**.

Lemma 5.5. *If $\mathfrak{a}$ is an ideal of a Noetherian ring, it is the intersection of a finite number of irreducible ideals.*

Proof. Let I be the set of ideals which cannot be written as finite intersections of irreducible ideals. By Proposition 5.2, if I is non-empty, it has a maximal element, $\mathfrak{m}$. There exist ideals $\mathfrak{a}, \mathfrak{b}$ such that $\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}$, but $\mathfrak{m}$ cannot be irrdeucible, so $\mathfrak{m} \subsetneq \mathfrak{a}$ and $\mathfrak{m} \subsetneq \mathfrak{b}$. $\mathfrak{m}$ is maximal, so $\mathfrak{a}, \mathfrak{b} \notin I$, i.e. they're both finite intersections of irreducible ideals. Therefore, so is $\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}$, so $\mathfrak{m} \notin I$, a contradiction. Therefore I is empty. □

Lemma 5.6. *In a Noetherian ring, all irreducible ideals are primary.*

Proof. Let $\mathfrak{a}$ be an ideal of a Noetherian ring that is not primary, i.e. there are b and c such that $bc \in \mathfrak{a}$ and $b, c^n \notin \mathfrak{a}$ for any $n \in \mathbb{N}$. Thus, we find that $\mathfrak{a} \subsetneq \mathfrak{a} : (c)$. By the properties of ideal operations, $\mathfrak{a} : \left(c^k\right) \subseteq \left(\mathfrak{a} : \left(c^k\right)\right) : (c) = \mathfrak{a} : \left(c^{k+1}\right)$, so there is an ascending chain:

$$\mathfrak{a} \subsetneq \mathfrak{a} : (c) \subseteq \mathfrak{a} : \left(c^2\right) \subseteq \mathfrak{a} : \left(c^3\right) \subseteq \dots \tag{5.7}$$

Since the ring is Noetherian, there is an $m \in \mathbb{N}$ such that $\mathfrak{a} : (c^n) = \mathfrak{a} : (c^m)$ for all $n \geq m$. Let $x \in (\mathfrak{a} : (c^m)) \cap (\mathfrak{a} + (c^m))$. Since $x \in \mathfrak{a} + (c^m)$, there is an $a \in \mathfrak{a}$ and an $r \in R$ such that $x = a + rc^m$. Since $x \in \mathfrak{a} : (c^m)$, we must have $xc^m = ac^m + rc^{2m} \in \mathfrak{a}$, meaning that $rc^{2m} \in \mathfrak{a}$, i.e. $r \in \mathfrak{a} : \left(c^{2m}\right) = \mathfrak{a} : (c^m)$ by the selection of m. Therefore, $rc^m \in \mathfrak{a}$, so $x = a + rc^m \in \mathfrak{a}$. This means that $(\mathfrak{a} : (c^m)) \cap (\mathfrak{a} + (c^m)) \subseteq \mathfrak{a}$. It is clear that $\mathfrak{a} \subsetneq \mathfrak{a} + (c^m)$, and $\mathfrak{a} \subsetneq \mathfrak{a} : (c^m)$ by (5.7). Therefore $\mathfrak{a} = (\mathfrak{a} : (c^m)) \cap (\mathfrak{a} + (c^m))$, i.e. $\mathfrak{a}$ is the intersection of two ideals that srtictly contain it, so it is reducible. □

Theorem 5.8. *Every ideal of a Noetherian ring has a primary decomposition.*

Proof. This is the direct combination of Lemma 5.5 and Lemma 5.6. □

So, in Noetherian rings, we have existence of primary decomposition in which the associated primes are unique, though the decomposition itself it is not necessarily unique.

6. Principal Ideal Domains

Of course, we can get unique factorization by imposing strict conditions. We know that the rational integers have unique factorization, so if we generalize just enough that the proof needn't change, then the claims still holds.

Definition 6.1. If there is an $a \in R$ such that $\mathfrak{a} = (a)$, $\mathfrak{a}$ is a **principal ideal**.

Definition 6.2. A ring where all ideals are principal is a **principal ideal domain** (**P.I.D.**).

Unique factorization of ideals in a P.I.D. holds for exactly the same reasons as unique factorization of rational integers. To repeat that proof here would waste the time of a reader who knows it, and rob the reader that doesn't of a crucial exercise. It can also be found in [4], [6], and [8].

Theorem 6.3. *Let R be a P.I.D. Then for any proper ideal $\mathfrak{a} \subsetneq R$, there exist proper prime ideals $\mathfrak{p}_i \subsetneq R$ such that*

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{p}_i. \tag{6.4}$$

This prime decomposition is unique.

Definition 6.5. An element with a multiplicative inverse is a **unit**.

Remark 6.6. The set of ideals of a P.I.D. is isomorphic to the P.I.D. itself in the obvious way, i.e.

$$\begin{aligned} R &\to \{\mathfrak{a} \subseteq R\}, \\ a &\mapsto (a), \end{aligned} \tag{6.7}$$

where one can check that $ab \mapsto (a) \cap (b) = (ab)$. Units map to R.

Definition 6.8. An element is **irreducible** if it is a nonzero non-unit $r \in R$ such that $r = ab$ implies that a or b is a unit.

Proposition 6.9. *In an integral domain, any prime element is an irreducible element.*

Proof. Suppose p is a prime element and $p = ab$. Without loss of generality, assume $p|b$, i.e. there is a $c \in R$ such that $pc = b$. Then $apc = ab$, so $ac = 1$, i.e. a is a unit. □

Definition 6.10. A domain is a **Unique Factorization Domain**, U.F.D. for short, if any nonzero non-unit can be written uniquely as a product of irreducible elements.

Corollary 6.11. *Any P.I.D. is a U.F.D.*

Proof. This is immediate from Theorem 6.3, Remark 6.6, and Proposition 6.9. □

Also, the language of principal ideals lets us prove a conclusion about the elements of a Noetherian ring:

Proposition 6.12. *If R is a Noetherian integral domain, every nonzero non-unit can be written as the product of finitely many irreducible elements.*

Proof. Analogously to the proof of Lemma 5.5, let I be the set of principal ideals generated by elements of R that cannot be written as the product of finitely many irreducibles. If I was nonempty, there would be a maximal element $(m) \in I$, and since m could not be reducible, there would be non-units $a, b \in R$ such that $m = ab$. Therefore $(m) \subsetneq (a)$ and $(m) \subsetneq (b)$, so by the maximality of (m) in I, $(a), (b) \notin I$, so a and b would both be products of finitely many irreducibles, so $ab = m$ would be as well. Therefore I is necessarily empty. □

7. Dedekind Domains

The condition of being a principal ideal domain is very strict, so it is natural to inquire if there is a more general case in which unique factorization holds. This generalization is what is known as a Dedekind domain, the conditions of which we need to define.

Definition 7.1. An ideal is **maximal** if it is not strictly contained in any proper ideal.

Proposition 7.2. *A maximal ideal is prime.*

Proof. Let $\mathfrak{a}$ be a non-prime proper nonzero ideal, i.e. let $x, y \notin \mathfrak{a}$ such that $xy \in \mathfrak{a}$. Then $x \in (\mathfrak{a} : (y)) \setminus \mathfrak{a}$ and $1 \notin \mathfrak{a} : (y)$, so $\mathfrak{a} \subsetneq \mathfrak{a} : (y) \subsetneq R$, i.e. $\mathfrak{a}$ is not maximal. □

Proposition 7.3. *An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

Proof. The Lattice Isomorphism Theorem for rings states that the ideal structure of $R/\mathfrak{m}$ is the same as the ideal structure of R, limited to those ideals containing $\mathfrak{m}$. Therefore, this claim is a direct consequence of Proposition 3.2. □

Definition 7.4. $R \subseteq S$ is an **extension** of rings/fields if both sets are rings/fields, and the notions of addition and multiplication agree on R. In the case of fields, one writes $S|R$.

Definition 7.5. Let $R \subseteq S$ be an extension of rings. An element $s \in S$ that satisfies a monic polynomial with coefficients in R is said to be **integral over** R. If s is integral over R for all $s \in S, S$ is an **integral extension** of, or **integral over**, R. The subset of S consisting of all elements integral over R is the **integral closure** of R in S. A ring R that equals its integral closure in S is **integrally closed** in S. The integral closure of R in its field of fractions[†] is its **normalization**. A ring R that is its own normalization is **normal** or **integrally closed**.

Definition 7.6. For $a_1, \ldots, a_m \in S \supseteq R$, R **adjoin** $a_1, \ldots, a_m$ is

$$R[a_1, \ldots, a_m] = \left\{ \sum_{j=1}^{n} \sum_{i=1}^{m} r_j a_i^j \mid r_j \in R, n \in \mathbb{N} \right\} \subseteq S.$$

$R[x]$ will be used in this paper to denote the similar but distinct construct, the **polynomial ring over** R.

[†]The field of fractions takes a bit of effort to construct rigorously, but is essentially as it sounds: fractions where the numerator and denominator come fom the domain in question. $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. For more, see [4], [7], or [10].

Definition 7.7. An R-module[‡] M is **finitely generated** if there is a finite set $A \subseteq M$ such that for every $m \in M$, there are elements $r_a \in R$ such that

$$m = \sum_{a \in A} r_a a. \tag{7.8}$$

Proposition 7.9. *The elements $s_1, \ldots, s_m \in S$ are integral over R if and only if $R[s_1, \ldots, s_m] \subseteq S$ is a finitely generated R-module.*

Proof. Suppose $s \in S$ is integral over R. Let $f(x) \in R[x]$ be a monic polynomial of degree n, such that $f(s) = 0$, and $g(x)$ an arbitrary polynomial in $R[x]$. $R[x]$ is Euclidean, i.e. there are $q(x), \rho(x) \in R[x]$ such that $g(x) = q(x) f(x) + \rho(x)$ and $\deg \rho(x) < n$. Then $g(s) = \rho(s)$, a sum of finitely many products of elements of R and powers of s. Therefore, $R[s]$ is a finitely generated R-module.

Suppose now that $R[s]$ is an R-module generated by $\{\alpha_1, \ldots, \alpha_k\}$. Then for every element $t \in R[s]$, there are $r_{ij} \in R$ such that

$$t\alpha_i = \sum_{j=1}^{k} r_{ij}\alpha_j, \ \forall i. \tag{7.10}$$

We know from linear algebra that $\det(t\mathbf{1}_k - (r_{ij}))\,\alpha_i = 0$ for every i.[†] That is, for every $t \in R[s]$, there is an R-linear transformation (r_{ij}) such that t is an eigenvalue of the transformation. $\det(t\mathbf{1}_k - (r_{ij})) = 0$ is a monic polynomial for s with coefficients in R, so s is integral over R.

Observe that $R[s_1][s_2] = R[s_1, s_2]$ and induct. □

Corollary 7.11. *If $R \subseteq S \subseteq T$ are ring extensions, where T is integral over S, and S is integral over R, then T is integral over R.*

Proof. Let $t \in T$. Then there is an $n \in \mathbb{N}$ and $s_i \in S$ such that

$$t^n + \sum_{i=1}^{n} s_i t^{n-i} = 0. \tag{7.12}$$

Let $M = R[s_1, \ldots, s_n]$. By Proposition 7.9, M is finitely generated over R, and $R[t]$ is finitely genereated over R, so t is integral over R, so T is integral over R. □

Corollary 7.13. *The integral closure of a ring in another ring is integrally closed.*

Proof. This is immediate from Corollary 7.11. □

Definition 7.14. A Noetherian integral domain that is integrally closed, in which every nonzero prime ideal is maximal, is a **Dedekind domain**.

In order to get where we want, we'll need a couple of lemmas concerning prime ideals in Dedekind domains:

Lemma 7.15. *Any nonzero ideal of a Dedekind domain contains the product of finitely many prime ideals.*

[‡]A module over a ring is the generalization of a vector space over a field. For more, see [4].

[†]$\mathbf{1}_k$ denotes the $k \times k$ identity matrix, (δ_{ij}) in Kronecker delta notation.

Proof. Let I be the set of ideals which do not contain the product of finitely many prime ideals. By Proposition 5.2, there is a maximal element $\mathfrak{m} \in I$. $\mathfrak{m}$ cannot be prime, so there must be $a, b \in \mathcal{O}$ such that $ab \in \mathfrak{m}$ and $a, b \notin \mathfrak{m}$. Letting $\mathfrak{a} = \mathfrak{m} + (a)$ and $\mathfrak{b} = \mathfrak{m} + (b)$, it is clear that $\mathfrak{m} \subsetneq \mathfrak{a}$ and $\mathfrak{m} \subsetneq \mathfrak{b}$. By the maximality of $\mathfrak{m}$, $\mathfrak{a}$ and $\mathfrak{b}$ are supersets of finite products of prime ideals, but a quick check shows that $\mathfrak{ab} \subseteq \mathfrak{m}$, so $\mathfrak{m}$ is as well. Therefore I is empty. □

Definition 7.16. Let $\mathfrak{p}$ be a prime ideal in the Dedekind domain $\mathcal{O}$ with field of fractions K. Then $\mathfrak{p}^{-1} = \{k \in K \mid k\mathfrak{p} \subseteq \mathcal{O}\}$.

Definition 7.17. A **fractional ideal** of K is a nonzero finitely generated $\mathcal{O}$-submodule of K.

Definition 7.18. A **principal fractional ideal** is a fractional ideal of the form $k\mathcal{O}$ for some $k \in K$. It will be denoted (k).

Remark 7.19. $\mathfrak{p}^{-1}$ is a fractional ideal, and the same operations that apply to ideals apply to fractional ideals.

Lemma 7.20. *For a prime ideal $\mathfrak{p}$ of a Dedekind domain $\mathcal{O}$, $\mathfrak{p}^{-1} \supsetneq \mathcal{O}$.*

Proof. By Definition 7.16 and the definition of ideal, $\mathfrak{p}^{-1} \supseteq \mathcal{O}$. Let $p \in \mathfrak{p} \setminus 0$. By Lemma 7.15, there must be nonzero prime ideals $\mathfrak{p}_i$ such that

$$\prod_{i=1}^{m} \mathfrak{p}_i \subseteq (p) \subseteq \mathfrak{p}, \tag{7.21}$$

where m is as small as possible. By Proposition 4.2, there is a $k \leq m$ such that $\mathfrak{p}_k \subseteq \mathfrak{p}$. Assume without loss of generality that $k = m$. Since $\mathcal{O}$ is a Dedekind domain, $\mathfrak{p}_m$ is maximal, so $\mathfrak{p}_m = \mathfrak{p}$. By the minimality of m,

$$\prod_{i=1}^{m-1} \mathfrak{p}_i \nsubseteq (p)\,, \text{ i.e. } \exists x \in \left(\prod_{i=1}^{m-1} \mathfrak{p}_i\right) \setminus p\mathcal{O}, \text{ i.e. } p^{-1}x \in K \setminus \mathcal{O}. \tag{7.22}$$

By (7.21), $x\mathfrak{p} \subseteq (p)$, so $p^{-1}x\mathfrak{p} \subseteq \mathcal{O}$, so $p^{-1}x \in \mathfrak{p}^{-1}$, so $\mathfrak{p}^{-1} \supsetneq \mathcal{O}$ by (7.22). □

Lemma 7.23. *For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for all nonzero ideals $\mathfrak{a}$.*

Proof. By Proposition 5.2, there must exist $\alpha_1, \ldots, \alpha_n$ that generate $\mathfrak{a}$.

Assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, so for any $x \in \mathfrak{p}^{-1}$, there are $a_{ij} \in \mathcal{O}$ such that

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j. \tag{7.24}$$

Let $A = (x\mathbf{1}_n - (a_{ij}))$. Then $A\,(\alpha_1, \ldots, \alpha_n)^t = 0$. We know that $\det(A)\,\alpha_i = 0$ for every i, so $\det(A) = 0$, so x is integral over $\mathcal{O}$. Since $\mathcal{O}$ is a Dedekind domain, this implies that $x \in \mathcal{O}$, so $\mathfrak{p}^{-1} \subseteq \mathcal{O}$, contradicting the previous lemma. Therefore $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. □

Theorem 7.25. *Every nonzero, proper ideal of a Dedekind domain can be uniquely factored into nonzero prime ideals.*

Proof. Let I be the set of nonzero proper ideals of the Dedekind domain $\mathcal{O}$ that do not factor into prime ideals.

Assume I is non-empty. By Proposition 5.2, there is a maximal element $\mathfrak{m} \in I$. Applying Proposition 5.2 to the supersets of $\mathfrak{m}$, we find that it is contained in a

maximal ideal $\mathfrak{p}$.[†] By Lemma 7.20, $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$, so $\mathfrak{m}\mathfrak{p}^{-1}$ is an ideal of $\mathcal{O}$. By Lemma 7.23, $\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1}$. It's simple to show that $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal, so since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. We know $\mathfrak{p}$ is maximal, hence prime by Proposition 7.2, but $\mathfrak{m}$ cannot be prime, so $\mathfrak{m} \subsetneq \mathfrak{p}$, so $\mathfrak{m}\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$, so $\mathfrak{m}\mathfrak{p}^{-1}$ is a proper ideal containing $\mathfrak{m}$. Since $\mathfrak{m}$ is a maximal element of $I, \mathfrak{m}\mathfrak{p}^{-1}$ has a prime factorization. But $\mathfrak{m} = \mathfrak{m}\mathfrak{p}^{-1}\mathfrak{p}$, so $\mathfrak{m}$ also has a prime factorization, so I is necessarily empty. Therefore all ideals in a Dedekind domain can be factored into primes.

Let the following be two prime factorizations of the same ideal:

$$\mathfrak{a} = \prod_{i=1}^{m} \mathfrak{p}_i = \prod_{j=1}^{n} \mathfrak{p}'_j \tag{7.26}$$

Since $\mathfrak{p}_m$ is prime, there must be a j' such that $\mathfrak{p}_m \supseteq \mathfrak{p}'_{j'}$, but prime ideals are maximal in a Dedekind domain, so $\mathfrak{p}_m = \mathfrak{p}'_{j'}$. Assume without loss of generality that $j' = n$. Since $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$, by mulitplying by $\mathfrak{p}_m^{-1}$, we find that

$$\prod_{i=1}^{m-1} \mathfrak{p}_i = \prod_{j=1}^{n-1} \mathfrak{p}'_j. \tag{7.27}$$

Using this recursive process, and remembering that the ideals are prime, we find that $m = n$ and pair up all $m = n$ pairs of equal prime ideals. Thus, the factorization of ideals in a Dedekind domain into prime ideals is unique. □

8. Factoring in Extensions, Ramification, and Quadratic Reciprocity

But what about factoring in extensions of Dedekind domains?

Remark 8.1. In the situation of a field extension $L|K$, L is a K-vector space.

Definition 8.2. The **degree** of the extension $L|K$ is $[L : K] = \dim_K L$. If this is finite, L is called a **fintite extension** of K.

Definition 8.3. For a field extension $L|K$ and a set $A \subseteq L$, K **adjoin** A, denoted $K(A)$, is the inersection of all subfields of L containing K and A. If $A = \{a_1, \ldots, a_n\}$, we write $K(a_1, \ldots, a_n)$.

Definition 8.4. A polynomial is **separable** over K if all of its irreducible factors have distinct roots in the algebraic closure of K. A field extension $L|K$ is **separable** if there is a set of roots of separable polynomials over K that, when adjoined to K, give L.

Definition 8.5. The **discriminant** of a basis $\alpha_1, \ldots, \alpha_n$ of a separable extension $L|K$ is $d(\alpha_1, \ldots, \alpha_n) = \det\left(Tr_{L|K}(\alpha_i \alpha_j)\right)$.

Remark 8.6. It can be shown that if $L|K$ is separable, then the discriminant of any basis is nonzero. See [9] for details.

Henceforth, $\mathcal{O}$ denotes a Dedekind domain with field of fractions K, $L|K$ an extension of fields, and $\mathscr{O}$ the integral closure of $\mathcal{O}$ in L.

[†]Actually, in any ring, any proper ideal is contained in a maximal ideal, but the general proof of this requires Zorn's Lemma. See [4].

Lemma 8.7. *If $\mathscr{O}$ contains $\alpha_1, \ldots, \alpha_n$, a basis for $L|K$, and $d = d(\alpha_1, \ldots, \alpha_n)$, then*

$$\mathscr{O} \subseteq \sum_{i=1}^{n} \mathcal{O}\alpha_i/d. \tag{8.8}$$

Proof. If $\alpha \in \mathscr{O}$ and

$$\alpha = \sum_{i=1}^{n} a_i\alpha_i \in \mathscr{O},\ a_i \in K. \tag{8.9}$$

Then

$$Tr_{L|K}(\alpha_i\alpha) = \sum_{j=1}^{n} Tr_{L|K}(\alpha_i\alpha_j)\, a_j. \tag{8.10}$$

Since $Tr_{L|K}(\alpha_i\alpha) \in \mathcal{O},\ \det\left(Tr_{L|K}(\alpha_i\alpha_j)\right) a_j \in \mathcal{O}$. But $\det\left(Tr_{L|K}(\alpha_i\alpha_j)\right) = d$, so

$$\alpha \in \sum_{j=1}^{n} \mathcal{O}\alpha_j/d, \quad \text{i.e. } \mathscr{O} \subseteq \sum_{j=1}^{n} \mathcal{O}\alpha_j/d. \tag{8.11}$$

□

Proposition 8.12. *If the extension $L|K$ is separable,[†] then $\mathscr{O}$ is a Dedekind domain.*

Proof. The domain $\mathscr{O}$ is integrally closed by assumption.

Let $\mathfrak{P}$ be a nonzero prime ideal in $\mathscr{O}$. Then for a $y \in \mathfrak{P} \setminus 0$, there are $m \in \mathbb{N}$, $x_i \in \mathcal{O}$ such that $x_m \neq 0$ and

$$y^m + \sum_{i=1}^{m} x_i y^{m-i} = 0, \tag{8.13}$$

so $x_m \in \mathfrak{P} \cap \mathcal{O}$, i.e. $\mathfrak{P} \cap \mathcal{O} \neq 0$. $\mathfrak{P} \cap \mathcal{O}$ is clearly a prime, and therefore maximal, ideal in $\mathcal{O}$, so Proposition 7.3 shows $\frac{\mathcal{O}}{\mathfrak{P}\cap\mathcal{O}}$ to be a field. By Proposition 3.2, it has no proper nonzero ideals, so neither can $\mathscr{O}/\mathfrak{P}$, or else the intersection of such an ideal with $\frac{\mathcal{O}}{\mathfrak{P}\cap\mathcal{O}}$ would yield a proper nonzero ideal in $\frac{\mathcal{O}}{\mathfrak{P}\cap\mathcal{O}}$. By Proposition 3.2, $\mathscr{O}/\mathfrak{P}$ is a field, so by Proposition 7.3, $\mathfrak{P}$ is maximal in $\mathscr{O}$.

Since $L|K$ is separable, let $\alpha_1, \ldots, \alpha_n$ be a basis of $L|K$ contained in $\mathscr{O}$ of nonzero discriminant d. By Lemma 8.7, $\mathscr{O}$ is contained in a finitely generated $\mathcal{O}$-module, so every ideal of $\mathscr{O}$ is as well, making every ideal of $\mathscr{O}$ a finitely generated $\mathcal{O}$-module. Since $\mathcal{O} \subseteq \mathscr{O}$, an ideal of $\mathscr{O}$ is a finitely generated $\mathscr{O}$-module, i.e. $\mathscr{O}$ is Noetherian.

Since $\mathscr{O}$ is integrally closed, has every prime ideal maximal, and is Noetherian, it is a Dedekind domain. □

Proposition 8.14. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, then $\mathfrak{p}\mathscr{O}$ is a proper ideal of $\mathscr{O}$.*

Proof. The statement is trivial if $\mathfrak{p} = 0$.

Otherwise, let $p \in \mathfrak{p} \setminus \mathfrak{p}^2$, so there is some ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $\mathfrak{p}\mathfrak{a} = p\mathcal{O}$ and $\mathfrak{p} \not\supseteq \mathfrak{a}$. In this case, $\mathfrak{p} + \mathfrak{a} = \mathcal{O}$. Therefore, there exist $q \in \mathfrak{p}$ and $a \in \mathfrak{a}$ such that $q + a = 1$. Then a cannot be in $\mathfrak{p}$ and $a\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = p\mathcal{O}$.

[†]The separable condition here is actually weaker than necessary, but the proof is trickier and requires more machinery if one wants to prove this for finite extensions in general. See [1], [7], or [9] for details. Also, most extensions considered here are separable.

Assume $\mathfrak{p}\mathscr{O} = \mathscr{O}$. Then $a\mathscr{O} = a\mathfrak{p}\mathscr{O} \subseteq p\mathscr{O}$. So, there is an $x \in \mathscr{O} \cap K$ such that $px = a$, so $a \in \mathfrak{p}$, contradicting our earlier conclusion. Hence, $\mathfrak{p}\mathscr{O}$ is a proper ideal of $\mathscr{O}$. □

Corollary 8.15. *A nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ factors uniquely into prime ideals in $\mathscr{O}$, i.e. there exist unique prime ideals $\mathfrak{P}_i \subseteq \mathscr{O}$ and naturals $m, \nu_i \in \mathbb{N}$ such that*

$$\mathfrak{p}\mathscr{O} = \prod_{i=1}^{m} \mathfrak{P}_i^{\nu_i}. \tag{8.16}$$

Proof. Proposition 8.12 and Proposition 8.14 allow us to apply Theorem 7.25. □

Definition 8.17. In the above situation, ν_i is the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$. The **inertia degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$ is $f_i = \left[\frac{\mathscr{O}}{\mathfrak{P}_i} : \frac{\mathcal{O}}{\mathfrak{p}}\right]$.

Proposition 8.18. *If $L|K$ is separable, then the above quantities are related to the degree of the extension $L|K$ in the* **fundamental identity***:*

$$\sum_{i=1}^{m} \nu_i f_i = [L : K].$$

Proof. Let $\varphi : \mathcal{O}[x] \to \frac{\mathcal{O}}{\mathfrak{p}}[x]$ be the natural homomorphism. Let $\varphi(\omega_1), \ldots, \varphi(\omega_n)$ be a basis of $\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$ over $\mathcal{O}/\mathfrak{p}$.

Assume the ω_i are linearly dependent in K. Then they are linearly dependent in $\mathcal{O}$. Then there are $a_i \in \mathcal{O}$ and $k \leq n$ such that $a_k \neq 0$ and

$$\sum_{i=1}^{n} a_i \omega_i = 0. \tag{8.19}$$

This means we can generate a nonzero ideal $\mathfrak{a} = (a_1, \ldots, a_n)$ of $\mathcal{O}$. We can find an $a \in \mathfrak{a}^{-1}$ such that $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, so $a\mathfrak{a} \nsubseteq \mathfrak{p}$. This means that $\{aa_i \mid i \leq n\} \subseteq \mathcal{O}$, but $\{aa_i \mid i \leq n\} \nsubseteq \mathfrak{p}$. Therefore, since

$$\varphi\left(\sum_{i=1}^{n} aa_i\omega_i\right) = \varphi(0) = 0, \tag{8.20}$$

the $\varphi(\omega_i)$ are linearly dependent over $\mathcal{O}/\mathfrak{p}$, contradicting the fact that they form a basis. Therefore the ω_i are linearly independent in K.

Let

$$M = \sum_{i=1}^{n} \mathcal{O}\omega_i \tag{8.21}$$

and $N = \mathscr{O}/M$. Then $\mathscr{O} = M + \mathfrak{p}\mathscr{O}$, so $\mathfrak{p}N = N$. $L|K$ is separable, so $\mathscr{O}$ is a finitely generated $\mathcal{O}$-module, as shown in the proof of Proposition 8.12, so N must be as well. Therefore, we can find generators $\alpha_i, \ldots, \alpha_m$ of N. Then for every i, j there must be $\rho_{ij} \in \mathfrak{p}$ such that

$$\alpha_i = \sum_{j=1}^{m} \rho_{ij}\alpha_j. \tag{8.22}$$

Let A be the matrix $(\rho_{ij}) - \mathbf{1}_m$, let the minor B_{ij} be the determinant of the $(m-1) \times (m-1)$ matrix formed by deleting the ith row and jth column of A, and let $\operatorname{adj}(A)$ be the classical adjoint of A, meaning $\operatorname{adj}(A)_{ij} = (-1)^{i+j} B_{ji}$. Then we

have $A(\alpha_1,\ldots,\alpha_m)^t = 0$ and $\operatorname{adj}(A)A = \det(A)\mathbf{1}_m$. Therefore,
$\operatorname{adj}(A)A(\alpha_1,\ldots,\alpha_m)^t = (\det(A)\alpha_1,\ldots,\det(A)\alpha_m)^t = 0$, so
$\det(A)N = 0$, so $\det(A)\mathscr{O} \subseteq M$. Since $\rho_{ij} \in \mathfrak{p}$, we find that $\varphi(\det(A)) = (-1)^m$. Thus, we can find that

$$L = \det(A)L = \sum_{i=1}^{n} K\omega_i. \tag{8.23}$$

Thus, we find that $\omega_1,\ldots,\omega_m$ is a basis of $L|K$, so $\dim_{\mathcal{O}/\mathfrak{p}}\left(\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}\right) = [L:K]$.

Now fix $i \leq n$. Let $\mathfrak{Q}_i^\mu = \mathfrak{P}_i^\mu/\mathfrak{P}_i^{\nu_i}$ for each non-negative integer $\mu \leq \nu_i$. Then we have $\mathscr{O}/\mathfrak{P}_i^{\nu_i} = \mathfrak{Q}_i^0 \supseteq \mathfrak{Q}_i^1 \supseteq \ldots \supseteq \mathfrak{Q}_i^{\nu_i} = 0$, all of which are $\frac{\mathcal{O}}{\mathfrak{p}}$-vector spaces. We also have that $\mathfrak{Q}_i^\mu/\mathfrak{Q}_i^{\mu+1} \cong \mathfrak{P}_i^\mu/\mathfrak{P}_i^{\mu+1}$ for all $\mu < \nu_i$. Let $q \in \mathfrak{P}_i^\mu/\mathfrak{P}_i^{\mu+1}$. Let $\psi_q : \mathscr{O} \to \mathfrak{P}_i^\mu/\mathfrak{P}_i^{\mu+1}$, $\psi_q(x) = xq$. ψ_q is a homomorphism, $\ker\psi_q = \mathfrak{P}_i$, and ψ_q is surjective, because $\mathfrak{P}_i^\mu = \mathfrak{P}_i^{\mu+1} + q\mathscr{O}$. Therefore, $\mathfrak{Q}_i^\mu/\mathfrak{Q}_i^{\mu+1} \cong \mathfrak{P}_i^\mu/\mathfrak{P}_i^{\mu+1} \cong \mathscr{O}/\mathfrak{P}_i$. By the definition of inertia degree, $f_i = \dim_{\mathcal{O}/\mathfrak{p}}\left(\mathfrak{Q}_i^\mu/\mathfrak{Q}_i^{\mu+1}\right)$, so

$$\dim_{\mathcal{O}/\mathfrak{p}}(\mathscr{O}/\mathfrak{P}_i^{\nu_i}) = \sum_{\mu=0}^{\nu_i-1} \dim_{\mathcal{O}/\mathfrak{p}}\left(\mathfrak{Q}_i^\mu/\mathfrak{Q}_i^{\mu+1}\right) = \nu_i f_i. \tag{8.24}$$

The Chinese Remainder Theorem tells us that

$$\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}} \cong \bigoplus_{i=1}^{m} \mathscr{O}/\mathfrak{P}_i^{\nu_i}, \tag{8.25}$$

so

$$\dim_{\mathcal{O}/\mathfrak{p}}\left(\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}\right) = \sum_{i=1}^{m} \dim_{\mathcal{O}/\mathfrak{p}}(\mathscr{O}/\mathfrak{P}_i^{\nu_i}),\ \text{i.e. } [L:K] = \sum_{i=1}^{m} \nu_i f_i, \tag{8.26}$$

by (8.24). □

Definition 8.27. Suppose $p(x) \in \mathcal{O}[x]$, and $\theta \in L$ such that $p(\theta) = 0$ and $L = K(\theta)$. The **conductor** of the ring $\mathcal{O}[\theta]$ is the largest ideal of $\mathscr{O}$, the integral closure of $\mathcal{O}$ in L, contained in $\mathcal{O}[\theta]$, explicitly given by $\mathfrak{F} = \{\alpha \in \mathscr{O} \mid \alpha\mathscr{O} \subseteq \mathcal{O}[\theta]\}$.

Proposition 8.28. *Let $\mathfrak{p}$ a prime of $\mathcal{O}$ such that $\mathfrak{p}\mathscr{O} + \mathfrak{F} = \mathscr{O}$, and let*

$$\varphi(p(x)) = \prod_{i=1}^{m} \varphi(p_i(x))^{\nu_i} \tag{8.29}$$

be the factorization of $\varphi(p(x))$ into irreducibles such that $p_i(x)$ is monic for all i. Then one finds the prime ideals over $\mathfrak{p}$ of (8.16) by $\mathfrak{P}_i = \mathfrak{p}\mathscr{O} + p_i(\theta)\mathscr{O}$. The inertia degree of $\mathfrak{P}_i$ is the degree of $\varphi(p_i(x))$. Also,

$$\mathfrak{p}\mathscr{O} = \prod_{i=1}^{m} \mathfrak{P}_i^{\nu_i}. \tag{8.30}$$

Proof. By assumption, $\mathfrak{p}\mathscr{O}+\mathfrak{F} = \mathscr{O}$, so since $\mathfrak{F} \subseteq \mathcal{O}[\theta]$, $\mathscr{O} = \mathfrak{p}\mathscr{O}+\mathcal{O}[\theta]$, so the natural homomorphism from $\mathcal{O}[\theta]$ to $\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$ is surjective. Its kernel is $\mathfrak{p}\mathscr{O} \cap \mathcal{O}[\theta] = \mathfrak{p}\mathcal{O}[\theta]$. Since $\mathfrak{p} + \mathfrak{F} \cap \mathcal{O} = \mathcal{O}$, $\mathfrak{p}\mathscr{O} \cap \mathcal{O}[\theta] = (\mathfrak{p}+\mathfrak{F})(\mathfrak{p}\mathscr{O} \cap \mathcal{O}[\theta]) \subseteq \mathfrak{p}\mathcal{O}[\theta]$. Therefore

$\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}} \cong \frac{\mathcal{O}[\theta]}{\mathfrak{p}\mathcal{O}[\theta]}$. Let $\mathcal{R} = \varphi(\mathcal{O}[x]) / (\varphi(p(x)))$. Let $\phi : \mathcal{O}[x] \to \mathcal{R}$ be the natural homomorphism. It is surjective and $\ker\phi$ is generated by $\mathfrak{p}$ and $p(x)$. Since $\mathcal{O}[\theta] = \mathcal{O}[x] / (p(x))$, we must have $\frac{\mathcal{O}[\theta]}{\mathfrak{p}\mathcal{O}[\theta]} \cong \mathcal{R}$, so $\mathcal{R} \cong \frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$. Since

$$\varphi(p(x)) = \prod_{i=1}^{m} \varphi(p_i(x))^{\nu_i}, \tag{8.31}$$

the Chinese Remainder Theorem gives us

$$\mathcal{R} \cong \bigoplus_{i=1}^{m} \varphi(\mathcal{O}[x]) / (\varphi(p_i(x)))^{\nu_i}. \tag{8.32}$$

This shows that the prime ideals of $\mathcal{R}$ are the principal ideals $(\phi(p_i))$, that $[\mathcal{R}/(\phi(p_i)) : \mathcal{O}/\mathfrak{p}] = \deg\varphi(p_i(x))$, and that

$$0 = \phi(p) = \bigcap_{i=1}^{m} (\phi(p_i))^{\nu_i}. \tag{8.33}$$

Let $\Phi : \mathscr{O} \to \frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$ be the natural homomorphism. It is surjective, i.e. $\Phi(\mathscr{O}) = \frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$. Since $\mathcal{R} \cong \frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$, the conclusions above hold in $\frac{\mathscr{O}}{\mathfrak{p}\mathscr{O}}$. That is, the prime ideals $\Phi(\mathfrak{P}_i)$ of $\Phi(\mathscr{O})$ correspond to the prime ideals $(\phi(p_i))$ and are $(\Phi(p_i(\theta)))$, $[\Phi(\mathscr{O})/\Phi(\mathfrak{P}_i) : \mathcal{O}/\mathfrak{p}] = \deg\varphi(p_i(x))$, and

$$0 = \bigcap_{i=1}^{m} \Phi(\mathfrak{P}_i)^{\nu_i}. \tag{8.34}$$

Thus, the preimage of $\Phi(\mathfrak{P}_i)$, i.e. $\mathfrak{P}_i$, is $\mathfrak{p}\mathscr{O} = p_i(\theta)\mathscr{O}$, and by definition, $f_i = [\Phi(\mathscr{O})/\Phi(\mathfrak{P}_i) : \mathcal{O}/\mathfrak{p}] = \deg\varphi(p_i(x))$, as desired.

Since $\nu_i = |\left\{\Phi(\mathfrak{P})^k \mid k \in \mathbb{N}\right\}|$, $\mathfrak{P}_i^{\nu_i} = \Phi^{-1}(\Phi(\mathfrak{P}_i)^{\nu_i})$. Also,

$$\mathfrak{p}\mathscr{O} \supseteq \bigcap_{i=1}^{m} \mathfrak{P}_i^{\nu_i}, \ \therefore\ \mathfrak{p}\mathscr{O} \supseteq \prod_{i=1}^{m} \mathfrak{P}_i^{\nu_i}, \tag{8.35}$$

so, since the fundamental identity states that

$$\sum_{i=1}^{m} \nu_i f_i = [L : K], \quad \mathfrak{p}\mathscr{O} = \prod_{i=1}^{m} \mathfrak{P}_i^{\nu_i}. \tag{8.36}$$

□

So we want to know more about how a prime ideal factors in an extension, but we lack the vocabulary to ask about it, hence some definitions:

Definition 8.37. A prime ideal $\mathfrak{p}$ of $\mathcal{O}$ **splits completely**, or is **totally split**, in L if the unique factorization of $\mathfrak{p}\mathscr{O}$ (8.16) has $m = [L : K]$, so $\nu_i = f_i = 1$ for all i. $\mathfrak{p}$ is **nonsplit**, or **indecomposed**, if $n = 1$.

Definition 8.38. A prime ideal $\mathfrak{P}_i$ of $\mathscr{O}$ from (8.16) is **unramified** over $\mathcal{O}$ or K if $\nu_i = 1$ and $\frac{\mathscr{O}}{\mathfrak{P}_i} | \frac{\mathcal{O}}{\mathfrak{p}}$ is separable. Otherwise, it is **ramified**. It is **totally ramified** if it is ramified and $f_i = 1$. The prime ideal $\mathfrak{p}$ is **unramified** if all the $\mathfrak{P}_i$ are unramified; otherwise it is **ramified**. The extension $L|K$ is **unramified** if all prime ideals $\mathfrak{p}$ of K are unramified in L.

Now, the fun part: What's the easiest way to figure out just when this total splitting happens in, say, a quadratic number field, $\mathbb{Q}(\sqrt{a})$?

Definition 8.39. Let $a, b \in \mathbb{Z}$. Then a is a **quadratic residue** of b if there is an integer k such that $k^2 \equiv a \mod b$.

Definition 8.40. The **Legendre symbol**, $\left(\frac{a}{p}\right)$, read "a on p," is defined for any $a \in \mathbb{Z}$ and odd prime $p \in \mathbb{N}$ to be 1 if a is a quadratic residue modulo p, 0 if $p|a$, and -1 otherwise. It can be shown that this is equivalent to $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Proposition 8.41. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proof. This is an immediate consequence of the alternate definition mentioned above. □

This tool lets us apply Proposition 8.28 rather succinctly in the case of quadratic fields:

Corollary 8.42. *For square-free a and odd prime $p \nmid a$, we find that $\left(\frac{a}{p}\right) = 1$ if and only if (p) is totally split in $\mathbb{Q}(\sqrt{a})$.*

Proof. It is easily verifiable that $\mathbb{Z}$ is a Dedekind domain, so let $\mathcal{O} = \mathbb{Z}$, $K = \mathbb{Q}$, $\theta = \sqrt{a}$, $p(x) = x^2 - a$, and $L = \mathbb{Q}(\sqrt{a})$. What is less trivial, but not difficult to show, is that $\mathfrak{F} \supseteq (2)$. See [4] or [9]. Since p is odd, this means that we can apply Proposition 8.28 to (p). For square-free a, $\left(\frac{a}{p}\right) = 1$ is equivalent to the existence of some $\alpha \in \mathbb{Z}$ such that $x^2 - a \equiv (x+\alpha)(x-\alpha) \mod p$. Hence, the decomposition given by (8.29) has all linear factors, i.e. the inertial degrees are all 1, if and only if $\left(\frac{a}{p}\right) = 1$. a is square-free, so all the ramification indices are 1. Hence, by the fundamental identity, $m = [L : K]$, i. e. (p) splits completely, if and only if $\left(\frac{a}{p}\right) = 1$. □

If you're wondering how this makes life any easier, I have the pleasure of introducing you to one of the truest gems of number theory, Gauss's famous **Quadratic Reciprocity Law**:

Theorem 8.43. *For two distinct odd primes $p, q \in \mathbb{N}$, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(q-1)(p-1)}{4}}$.*

This, along with the two simple supplementary statements below that handle -1 and 2, makes computation of a Legendre symbol as easy as a few steps of modular arithmetic.

Theorem 8.44. *For an odd prime $p \in \mathbb{N}$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.*

There are literally hundreds of distinct proofs of this law, with 8 by Gauss himself. The most enlightening, i.e. the one that best answers the question, "But, why?" that I have encountered is in the section on cyclotomic fields in [9]. There are other proofs in [5], [6], [7], [8], and [9].

Corollary 8.45. *Let q and p be distinct odd primes. Then if $(p-1)(q-1)/4$ is odd, (q) splits completely in $\mathbb{Q}(\sqrt{p})$ if and only if (p) does not split completely in $\mathbb{Q}(\sqrt{q})$. If $(p-1)(q-1)/4$ is even, (q) splits completely in $\mathbb{Q}(\sqrt{p})$ if and only if (p) also splits completely in $\mathbb{Q}(\sqrt{q})$.*

Proof. This is a restatement of Theorem 8.43 in terms of Corollary 8.42. □

9. The Class Group, Gauss, and Bhargava

For Noetherian rings and P.I.D.'s, we used our understanding of ideal structure to come to conclusions about factorization of elements[†]. Dedekinds domains are a subset of the former and a superset of the latter, so is there some analogous intermediate statement that can be made?

Henceforth, unless otherwise stated, R_S is the notation for the localization of R at S.[†]

Proposition 9.1. *If $\mathfrak{a} \supseteq \mathfrak{b}$ are two ideals in a Dedekind domain $\mathcal{O}$, then there is an $a \in \mathcal{O}$ such that $\mathfrak{a} = \mathfrak{b} + (a)$.*

Proof. By Theorem 7.25, there are unique naturals $\nu_i \in \mathbb{N}$ and prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$ such that

$$\mathfrak{b} = \prod_{i=1}^{n} \mathfrak{p}_i^{\nu_i}. \tag{9.2}$$

Because $\mathfrak{a} \supseteq \mathfrak{b}$, there are integers μ_i such that $0 \leq \mu_i \leq \nu_i$ and

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{\mu_i}. \tag{9.3}$$

For each $i \in \mathbb{N}$ such that $i \leq n$, let $a_i \in \mathfrak{p}_i^{\mu_i} \setminus \mathfrak{p}_i^{\mu_i+1}$. By the Chinese Remainder Theorem, there is an $a \in \mathcal{O}$ such that $a \equiv a_i \mod \mathfrak{p}_i^{\nu_i}$ for all $i \leq n$. Because of this, every element of the fractional ideal generated by $\mathfrak{b} + (a)$ in $\mathcal{O}_{\mathfrak{p}_i}$ is congruent to an element of the fractional ideal generated by $\mathfrak{a}$ in $\mathcal{O}_{\mathfrak{p}_i}$, and vice versa, i.e. the two fractional ideals are equal, for every i. In the localization of $\mathcal{O}$ at any other prime ideal, the fractional ideals generated by both are trivially the same. Since the two ideals generate the same fractional ideals in the localization of $\mathcal{O}$ at any prime ideal of $\mathcal{O}$, $\mathfrak{b} + (a) = \mathfrak{a}$. □

Definition 9.4. Two nonzero proper ideals $\mathfrak{a}$ and $\mathfrak{b}$ are **relatively prime** if they have no primes in common in their unique factorizations as given by Theorem 7.25. This can be shown to be equivalent to $\mathfrak{a} + \mathfrak{b} = R$.

Corollary 9.5. *Given any nonzero ideals $\mathfrak{a}, \mathfrak{b}$ of a Dedekind domain $\mathcal{O}$ and $b \in \mathfrak{a}$, there exist nonzero ideals $\mathfrak{a}_{\mathfrak{b}}^*$ and $\mathfrak{a}_b^*$ of $\mathcal{O}$ such that $\mathfrak{a}\mathfrak{a}_{\mathfrak{b}}^*$ is principal, $\mathfrak{a}_{\mathfrak{b}}^*$ is relatively prime to $\mathfrak{b}$, and $\mathfrak{a}\mathfrak{a}_b^* = (b)$.*

Proof. The claim for $b \in \mathfrak{a}$ is trivial if $b = 0$.

Otherwise, $(b) \subseteq \mathfrak{a}$ is nonzero, so by Theorem 7.25, as in the previous proof, there exist unique prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$, naturals n and ν_i, and integers μ_i such that $0 \leq \mu_i \leq \nu_i$,

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{\mu_i}, \text{ and } (b) = \prod_{i=1}^{n} \mathfrak{p}_i^{\nu_i}. \tag{9.6}$$

[†]Proposition 6.12 and Corollary 6.11, respectively

[†]Good resources for learning about localization are [4], [5], [7], and [9].

Let

$$\mathfrak{a}_b^* = \prod_{i=1}^{n} \mathfrak{p}_i^{\nu_i - \mu_i}. \tag{9.7}$$

Then $\mathfrak{a}\mathfrak{a}_b^* = (b)$.

We know $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$, so by Proposition 9.1, there is an $a \in \mathcal{O}$ such that $\mathfrak{a} = \mathfrak{a}\mathfrak{b} + (a)$. Therefore, $\mathfrak{a} = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{a}_a^*$, so $\mathcal{O} = \mathfrak{b} + \mathfrak{a}_a^*$. Set $\mathfrak{a}_\mathfrak{b}^*$ to be $\mathfrak{a}_a^*$. □

Theorem 9.8. *A Dedekind domain is a U.F.D. if and only if it is a P.I.D.*

Proof. A P.I.D. is necessarily a U.F.D.

Suppose then, that $\mathcal{O}$ is a Dedekind U.F.D. Let $\mathfrak{p}$ be a prime nonzero ideal of $\mathcal{O}$. There is a nonzero element in $\mathfrak{p}$, and by Proposition 6.9, it has an irreducible factor p. By Corollary 9.5, there are elements $a, b \in \mathcal{O}$ and nonzero ideals $\mathfrak{p}_p^*,\ \mathfrak{p}_a^*,\ (\mathfrak{p}_a^*)_b^*$ of $\mathcal{O}$ such that $\mathfrak{p}\mathfrak{p}_p^* = (p)$, $\mathfrak{p}\mathfrak{p}_a^* = (a)$, $\mathfrak{p}_p^* + \mathfrak{p}_a^* = \mathcal{O}$, $\mathfrak{p}_a^* (\mathfrak{p}_a^*)_b^* = (b)$, and $(\mathfrak{p}_a^*)_b^* + \mathfrak{p} = \mathcal{O}$. We can see that $(pb) = \mathfrak{p}\mathfrak{p}_p^*\mathfrak{p}_a^* (\mathfrak{p}_a^*)_b^* = (a)\,\mathfrak{p}_p^* (\mathfrak{p}_a^*)_b^*$. Therefore $a|pb$, i.e. there exists a $c \in \mathcal{O}$ such that $ac = pb$. Because $\mathcal{O}$ is a U.F.D., $p|a$ or $p|c$.

Assume that $p|c$. Then there is a $d \in \mathcal{O}$ such that $pd = c$, so $d\mathfrak{p} = (\mathfrak{p}_a^*)_b^*$, contradicting their selection as relatively prime. Hence, $p|a$, i.e. there is an $e \in \mathcal{O}$ such that $pe = a$, so $e\mathfrak{p}_p^* = \mathfrak{p}_a^*$. This means that any ideal that was a factor of $\mathfrak{p}_p^*$ would also be a factor of $\mathfrak{p}_a^*$, which cannot be because they are relatively prime. Thus, $\mathfrak{p}_p^* = \mathcal{O}$. Since $\mathfrak{p}\mathfrak{p}_p^* = (p)$ by construction, this argument tells us that $\mathfrak{p} = (p)$. □

So our hope seems to have been naïve - in reality, to talk about unique prime factorization of elements in a Dedekind domain, we necessarily must require it to be a P.I.D. However, with a new tool, we can measure how far away we are.

Proposition 9.9. *The set of fractional ideals form an abelian group under multiplication, with* $1 = \mathcal{O}$ *and* $\mathfrak{a}^{-1} = \{k \in K \mid k\mathfrak{a} \subseteq \mathcal{O}\}$.

Proof. Associativity, commutativity, and identity are all trivial to show.

Lemma 7.23 says that for a prime ideal $\mathfrak{p}$, $\mathfrak{p}\mathfrak{p}^{-1} \supsetneq \mathfrak{p}$, and since $\mathcal{O}$ is Dedekind, this means that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Therefore, if $\mathfrak{a}$ is an ideal and

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i,\ \mathfrak{b} = \prod_{i=1}^{n} \mathfrak{p}_i^{-1} \tag{9.10}$$

will give $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. By this, $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. If $b \in \mathfrak{a}^{-1}$, $b\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, so $b \in \mathfrak{b}$, remembering that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Therefore $\mathfrak{a}^{-1} = \mathfrak{b}$. Were $\mathfrak{a}$ a fractional ideal and not an ideal, we could pick an $a \in \mathfrak{a}$ such that $a\mathfrak{a}$ is an ideal of $\mathcal{O}$, with an inverse that is easily shown to be $a^{-1}\mathfrak{a}^{-1}$, so $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Definition 9.11. The group in Proposition 9.9 is the **ideal group** of K, denoted J_K.

Corollary 9.12. *Every fractional ideal* $\mathfrak{a} \in J_K$ *has unique prime factorization*

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{\nu_i},\ \nu_i \in \mathbb{Z}. \tag{9.13}$$

Proof. After realizing that there are ideals $\mathfrak{b}, \mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ for any fractional ideal $\mathfrak{a}$, this is a direct consequence of Theorem 7.25. □

Definition 9.14. It is trivial to show that $P_K = \{k\mathcal{O} \mid k \in K\}$ is a subgroup of J_K. $\mathrm{Cl}_K = J_K/P_K$ is the **class group** of K. $|\mathrm{Cl}_K|$ is the **class number** of K.

Remark 9.15. It is elementary to show that a domain is a P.I.D. if and only if its class number is 1.

In a very hands-waving manner, let me say that the class number indicates to what extent the ideals can vary from being principal, i.e. to what extent unique prime factorization can fail for elements despite holding for ideals, in a Dedekind domain. This makes a little more sense if Theorem 9.8 and Remark 9.15 are kept in mind. The class number is in fact necessarily finite, but the proof of this is outside the scope of this paper. Different proofs can be found in [5], [7], and [9].

Calculating the class number of a domain is tricky. One way to do it is using Minkowski's Lemma.[†] That is not the subject of this paper, but more about it can be found in [7] and [9]. One of the more common settings where this is an issue is the quadratic field, as addressed in the last section. It turns out that Gauss developed an explicit isomorphism between ideal classes in quadratic rings of a given discriminant and $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary integral quadratic forms of the same discriminant D, denoted $\mathrm{Cl}\left(\left(\mathrm{Sym}^2\mathbb{Z}^2\right)^*; D\right)$. Binary quadratic forms are thoroughly understood, and number theorists have used this correspondence for centuries to compute the class numbers of quadratic rings. This method, though powerful, was lamentably limited to the special case of quadratic rings. However, a few years ago, by finding a correspondence between sets of binary quadratic forms and the space of $2\times2\times2$ cubes of integers, denoted $\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2$, Manjul Bhargava of Princeton found that Gauss's correspondence was just a special case of a more general trend, and found 13[‡] analogous laws for other spaces, such as the ideal classes of cubic rings, that is rings in degree 3 extensions of the rationals. These correspondences ease calculations of determinants, simplify the criteria for finding which orders in an algebraic number field are maximal, improve our understanding of the splitting of primes in rings of integers, and aid in determining the invertibility of ideal classes of a domain that isn't Dedekind. The correspondences can be remarkably simple. A teaser is laid out below. For a list of the correspondences and speculation as to their implications, see [2]. For the paper that fleshes out and proves the most important and accessible ones, see [3].

Let $A = (a,b,c,d,e,f,g,h) \in \mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2$. It's best to think of this as a cube, where

$M_1^A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $N_1^A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ are the front and back,

$M_2^A = \begin{pmatrix} a & c \\ e & g \end{pmatrix}$ and $N_2^A = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$ are the left and right, and

$M_3^A = \begin{pmatrix} a & e \\ b & f \end{pmatrix}$ and $N_3^A = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$ are the top and bottom halves, respectively.

A little expansion will show that $Q_i^A = -\det\left(M_i^A x - N_i^A y\right)$ will give a binary quadratic form for which $\mathrm{Disc}\left(Q_1^A\right) = \mathrm{Disc}\left(Q_2^A\right) = \mathrm{Disc}\left(Q_3^A\right)$, so we can define

[†]This is also known as Minkowski's Theorem.

[‡]There are probably more.

$\mathrm{Disc}\,(A) = \mathrm{Disc}\left(Q_1^A\right)$. This discriminant can be shown to be the only invariant under the natural action of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, which is shown to be equivalent to a more geometrically intuitive action by way of this cube correspondence in [3]. After a lot of work, one can show that, given three binary quadratic forms of the same discriminant D, after modding out by an equivalence relation, this uniquely determines the cube that would map to them, up to another equivalence relation, i.e. there is a bijection between $\mathrm{Cl}\left(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D\right)$ and $\mathrm{Cl}\left(\left(\left(\mathrm{Sym}^2 \mathbb{Z}^2\right)^*\right)^3; D\right)$. Moreover, in [3], it is shown how group laws can be formed on $\mathrm{Cl}\left(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D\right)$ and $\mathrm{Cl}\left(\left(\mathrm{Sym}^2 \mathbb{Z}^2\right)^*; D\right)$ such that the above map composed with any projection is a group homomorphism.

References

[1] J. A. Beachy. Introductory lectures on rings and modules supplement. `http://www.math.niu.edu/~beachy/rings_modules/supplement.html`, May 1999. Unpublished supplement: Chapter 5: Commutative rings.

[2] M. Bhargava. Gauss composition and generalizations. *Lecture Notes in Computer Science*, 2369:1–8, 2002.

[3] M. Bhargava. Higher composition laws i: A new view on gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159:217–250, 2004.

[4] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wile & Sons, Inc., New York, second edition, 1999.

[5] S. Lang. *Algebraic Number Theory*. Addison-Wesley Series in Mathematics. Addson-Wesley Publishing Company, Inc., Redding, Massachusetts, June 1970.

[6] G. B. Mathews. *Theory of Numbers*. Chelsea Publication Company, New York, second edition, 19—. Originally published as Theory of numbers, part I.

[7] J. Milne. Algebraic number theory. `http://www.jmilne.org/math/CourseNotes/math676.html`, 1998. Course notes.

[8] M. B. Nathanson. *Elementary Methods in Number Theory*, volume 195 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[9] J. Neukirch. *Algebraic Number Theory*, volume 322 of *A Series of Comprehensive Studies in Mathematics*. Springer-Verlag, Berlin, March 1999.

[10] D. G. Northcott. *Ideal Theory*, volume 42 of *Cambridge Texts in Mathematics and Mathematical Physics*. Cambridge at the University Press, Cambridge, 1953.