UNIQUE FACTORIZATION OF IDEALS IN A DEDEKIND DOMAIN

XINYU LIU

Abstract. In abstract algebra, a Dedekind domain is a Noetherian, integrally closed integral domain of Krull dimension 1. Parallel to the unique factorization of integers in $\mathbb{Z}$, the ideals in a Dedekind domain can also be written uniquely as the product of prime ideals. Starting from the definitions of groups and rings, we introduce some basic theory in commutative algebra and present a proof for this theorem via Discrete Valuation Ring. First, we prove some intermediate results about the localization of a ring at its maximal ideals. Next, by the fact that the localization of a Dedekind domain at its maximal ideal is a Discrete Valuation Ring, we provide a simple proof for our main theorem.

Contents

1. Basic Definitions of Rings

We start with some basic definitions of a ring, which is one of the most important structures in algebra.

Definition 1.1. A *ring* R is a set along with two operations $+$ and $\cdot$ (namely addition and multiplication) such that the following three properties are satisfied:

(1) $(R, +)$ is an abelian group.
(2) $(R, \cdot)$ is a monoid.
(3) The distributive law: for all $a, b, c \in R$, we have $(a+b) \cdot c = a \cdot c + b \cdot c$, and $a \cdot (b + c) = a \cdot b + a \cdot c$.

Specifically, we use 0 to denote the identity element of the abelian group $(R, +)$ and 1 to denote the identity element of the monoid $(R, \cdot)$. In particular, R is called a *commutative ring* if we have $a \cdot b = b \cdot a$ for all $a, b \in R$.

Note that in this paper, we consider commutative rings mostly. Given a commutative ring R, below we give the definitions of a module and an ideal of R.

Definition 1.2. Let R be a commutative ring. M is called a *module* over R, or a *R-module*, if M consists of an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that for all $r, s \in R$ and $x, y \in M$, the following four properties hold:

(1) $r \cdot (x + y) = r \cdot x + r \cdot y$
(2) $(r + s) \cdot x = r \cdot x + s \cdot x$
(3) $(rs) \cdot x = r \cdot (s \cdot x)$.
(4) $1 \cdot x = x$

Example 1.3. Given a commutative ring R and its addition and multiplication operations, it is easy to see that R itself is a R-module under the same two operations. According to the properties of a ring structure, all of the four conditions above are satisfied.

Now we introduce the following definitions to simplify the notations.

Definition 1.4. Let S and T be subsets of a commutative ring R. The sum of S and T is defined by $S + T = \{s + t : s \in S, t \in T\}$, and the product of S and T is defined by $ST = \{\sum_{i=1}^{n} s_i t_i : s_1, s_2, \cdots, s_n \in S, t_1, t_2, \cdots, t_n \in T, n \in \mathbb{N}\}$. Similarly, we can also define the sum of an element and a set by $s + T = \{s + t : t \in T\}$, where $s \in S$.

Definition 1.5. Let R be a ring and M be a R-module. If there exists a finite number of elements $c_1, c_2, \cdots, c_n \in M$ such that for all elements $m \in M$, it can be written as $m = a_1c_1 + a_2c_2 + \cdots + a_nc_n$ for some $a_1, a_2, \cdots, a_n \in R$, then M is called *finitely generated*, and $c_1, c_2, \cdots, c_n$ are called the *generators* of M.

Using the concept of modules, we can further define the ideal of a ring and the quotient ring.

Definition 1.6. Let R be a commutative ring, then I is called an *ideal* if I is a R-submodule of R. (i.e. $(I, +)$ is a group and $IR \subset I$) In addition, I is called *proper* if I is an ideal such that $I \neq R$.

Definition 1.7. Let R be a ring and I be an ideal of R. Then the *quotient ring* R/I is defined as:

$$R/I = \{r + I : r \in R\}$$

The addition operation $+ : R/I \times R/I \to R/I$ maps $(r+I, s+I)$ to $(r+s+I)$, and the multiplication operation $\times : R/I \times R/I \to R/I$ maps $(r + I, s + I)$ to $(rs + I)$. For simplicity, we use $[r]$ to denote the set $r + I$.

It is easy to check that the two operations in Definition 1.7 are well-defined and that the set R/I forms a ring under these two operations.

Definition 1.8. Let R be a commutative ring and I be a proper ideal of R. I is called a *prime ideal* if for any two elements $a, b \in R$ such that $a \times b \in I$, we have $a \in I$ or $b \in I$.

Definition 1.9. Let R be a commutative ring and I be a proper ideal of R. I is called a *maximal ideal* if the only ideals P such that $I \subset P$ are I itself and R.

The proposition below guarantees the existence of a maximal ideal of any ring R.

Proposition 1.10. *For any commutative ring R, there exists a maximal ideal $I \subset R$ of R.*

Proof. Zorn's Lemma states that, given a partially ordered set such that every chain has an upper bound, there exists at least one maximal element. Let $\mathcal{I}$ be the set of proper ideals in R and define the partial order $\prec$ on two ideals $I_1, I_2 \in \mathcal{I}$ as:

$$I_1 \prec I_2 \Leftrightarrow I_1 \subset I_2$$

By Zorn's Lemma, it suffices to show that, given any sequence of ideals $I_1 \prec I_2 \prec \cdots$, an upper bound of the sequence $U = I_1 \cup I_2 \cup \cdots$ is a proper ideal. Since $1 \notin U$, we know that $U \neq R$, so we only need to prove that U is an ideal.

First, it is easy to check that $(U, +)$ is a group. In fact, for any $x, y \in U$, there exists a sufficiently large natural number N such that $x, y \in I_N$. Due to the fact that I_N is a group and thus additively closed, we have $x + y \in I_N$, so $x + y \in U$.

Second, we need to prove that $UR \subset U$. For any $u \in U$ and $r \in R$, there exists a sufficiently large natural number N such that $u \in I_N$. Since I_N is an ideal, we have $I_N R \subset I_N$, so $u \times r \in I_N$, and hence $u \times r \in U$. This suggests that $UR \subset U$. Therefore, the maximal ideal always exists. □

Last, we give three equivalent definitions of a Noetherian ring and eventually the definition of Krull dimension of a commutative ring.

Definition 1.11. Suppose R is a commutative ring. R is called a *Noetherian ring* if there is no infinite ascending sequence of ideals in R.

Theorem 1.12. *The following three statements are equivalent:*

(1) A ring R is Noetherian.
(2) For every chain of ideals $I_1 \subset I_2 \subset \cdots$ in R, there exists a maximal element I_N ($N \in \mathbb{N}$). (i.e. for all natural number $n > N$, we have $I_n = I_N$)
(3) Every ideal of R is finitely generated.

Proof. First, it is easy to see that (1) implies (2). In fact, suppose that R is a Noetherian ring. By definition, there does not exist an infinite ascending sequence of ideals. Let $U = I_1 \subset I_2 \subset \cdots$ and assume that U does not have a maximal element. Then for any element of the sequence I_{n_1}, we can find a natural number $n_2 > n_1$ such that $I_{n_1} \subset I_{n_2}$. Repeating this process, we are able to construct an infinite sequence of ideals $I_{n_1} \subset I_{n_2} \subset \cdots$, where $n_1 < n_2 < \cdots$. This is a contradiction.

Second, (2) also implies (3). Suppose we have an ideal I that is not finitely generated, and we label the elements in I as $a_1, a_2, \cdots$. Consider the set of ideals such that I_1 is generated by a_1, I_2 is generated by a_1 and a_2, $\cdots\cdots$, I_n is generated by $a_1, a_2, \cdots, a_n$. Then we have $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$. However, since the ideal I is not finitely generated, the sequence does not contain a maximal element, which is a contradiction.

Last, we prove that (3) implies (1). Suppose that all ideals are finitely generated, and consider a set of ideals $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ and their union $U = I_1 \cup I_2 \cup \cdots \cup I_n \cup \cdots$. We have shown previously in Proposition 1.10 that U is a proper ideal, and is thus finitely generated by a set of elements $a_1, a_2, \cdots, a_n$. Notice that $I_1 \subset I_2 \subset \cdots$, so there exists a natural number N such that I_N is generated by $a_1, a_2, \cdots, a_n$. Hence $I_N = U$ because they are generated by the same set of elements. It follows that R is Noetherian since there is no infinite ascending sequence of ideals in R. □

Definition 1.13. Let R be a commutative ring. The *Krull dimension* of R is the largest non-negative integer n such that there exists a chain of prime ideals of R $I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n$. If for any $n \in \mathbb{N}$, there exists a chain of $n+1$ prime ideals of R under inclusion, then R has infinite dimension.

2. Localization

Localization is a concept in commutative algebra that introduces the denominators to rings and modules. Before defining localization, we first introduce an equivalence relation, which is denoted by $\sim$:

Definition 2.1. Given a ring R, let D be a subset of R that is multiplicatively closed (i.e. for any $a, b \in D$ we have $ab \in D$). Given $a, a' \in R$ and $s, s' \in D$, an equivalence relation $\sim$ on $R \times D$ is defined by:

$$(a, s) \sim (a', s') \Leftrightarrow s_1(as' - a's) = 0 \text{ for some } s_1 \in D$$

Note that $\sim$ is a well-defined equivalence relation since we are able to check that it is reflective, symmetric and transitive.

Definition 2.2. Let R be a ring and let $D \subset R$ be a multiplicatively closed set. The *equivalence class* containing the pair (a, s) $(a \in R, s \in D)$ is the set of all pairs (a', s') $(a' \in R, s' \in D)$ such that $(a, s) \sim (a', s')$, which is denoted by $[a, s]$ or $\frac{a}{s}$. We define addition and multiplication on the equivalence classes by the following two formulas:

$$[a, s] + [a', s'] = [as' + a's, ss']$$
$$[a, s] \cdot [a', s'] = [aa', ss']$$

Definition 2.3. Let R be a ring and let $D \subset R$ be a multiplicatively closed set. Then the *ring of fractions*, denoted by $D^{-1}R$, is defined on the set $D^{-1}R = \{[a, s] : a \in R, s \in D\}$ with the addition and multiplication operations defined in Definition 3.3.

The following two examples of localization are important in commutative algebra.

Example 2.4. Let R be a ring and f be an element of R such that for any positive integer n, $f^n \neq 0$. Consider $D = \{1, f, f^2, f^3, \cdots\}$, which is a subset of R. It is easy to see that D is multiplicatively closed, so the localization of the ring R at the element f can be written as $D^{-1}R = \frac{R[t]}{ft-1}$, which is also denoted as $R[f^{-1}]$, or R_f.

Example 2.5. Let R be a commutative ring, P be a prime ideal of R and let $D = R - P$. We first show that D is a multiplicatively closed set. In fact, suppose by contradiction that there exists $a, b \in D$ such that $ab \notin D$. Then by the definition of set substraction, we have $ab \in P$ and $a, b \notin P$. However, this is impossible since P is a prime ideal. Hence D is multiplicatively closed, and we can then define the ring of fractions $D^{-1}R$ (which is also denoted R_P) based on R and D. For example, if $R = \mathbb{Z}$ and $P = (p)$, then

$$D^{-1}R = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$$

The ring of fractions R_P is called the localization of R at P.

Finally, given the concept of localization, we can define a local ring.

Definition 2.6. Let R be a commutative ring. R is called a *local ring* if it has a unique maximal ideal.

Below we give two examples of a local ring.

Example 2.7. A *field* F is a commutative ring such that:

(1) $1 \neq 0$.
(2) $F - \{0\}$ is a group under multiplication.

In fact, for any field F, the maximal ideal is $\{0\}$, so F is a local ring.

Before giving another example of a local ring, we first introduce a theorem that considers a map from R to R_P for a ring R and its prime ideal P.

Theorem 2.8. *Let R be a commutative ring and let P be a prime ideal of R. Let $\pi : R \to R_P$ be the map that sends $r \in R$ into $\frac{r}{1} \in R_P$. Let I be an ideal in R, and then $\pi(I)R_P$ (the extension of I to R_P) is an ideal in R_P. In addition, let J be an ideal in R_P, and then $\pi^{-1}(J)$ (the contraction of J to R) is an ideal in R. Given these definitions, we also have $\pi(\pi^{-1}(J))R_P = J$.*

Proof. First, given an ideal $I \subset R$, we have $\pi(I) \subset R_P$. By Definition 1.4, we can write $\pi(I)R_P = \{x \cdot [r, s] : x \in \pi(I), r \in R, s \in P\}$. By Definition 2.2, given two elements $x_1 \cdot [r_1, s_1], x_2 \cdot [r_2, s_2] \in \pi(I)R_P$, their sum is equal to $[x_1r_1s_2 + x_2r_2s_1, s_1s_2]$, which is another element in $\pi(I)R_P$. Hence, $\pi(I)R_P$ is additively closed. Additionally, given elements $[m, n] \in R_P$ and $x \cdot [r, s] \in \pi(I)R_P$, their product is equal to $mx \cdot [r, ns]$, which is also an element in $\pi(I)R_P$. It follows that $R_P\pi(I)R_P \subset \pi(I)R_P$. Based on these two facts, $\pi(I)R_P$ is an ideal. Likewise, let J be an ideal in R_P, we can also prove that $\pi^{-1}(J)$ is an ideal of R.

To prove that $\pi(\pi^{-1}(J))R_P = J$, we first notice $\pi(\pi^{-1}(J))R_P \subset J$, so it suffices to show that the reverse inclusion also holds. In fact, for any element $[a, b] \in J$, we have $[b, 1] \cdot [a, b] \in J$, so $[a, 1] \in J$ and hence $a \in \pi^{-1}(J)$. This implies that $[a, 1] \in \pi(\pi^{-1}(J))R_P$ by the definition of our mapping. Since $[1, b] \in R_P$, we have $[a, 1] \cdot [1, b] \in \pi(\pi^{-1}(J))R_P$, so $[a, b] \in \pi(\pi^{-1}(J))R_P$. It follows that $J \subset \pi(\pi^{-1}(J))R_P$, and hence $\pi(\pi^{-1}(J))R_P = J$. □

Example 2.9. Let R be a ring and P be a prime ideal of R. Then R_P is a local ring, and PR_P is the maximal ideal of R_P.

Proof. By Theorem 2.8, for every ideal J of R_P, its pre-image in R generates J. Let J be an ideal in R_P besides PR_P and R_P, and let I be its pre-image in R. We consider the following two cases:

(1) $I \subset P$, then it is easy to see that $J = IR_P \subset PR_P$, so IR_P is not a maximal ideal.
(2) $I \not\subset P$, then by definition there exists an element $x \in I - P$, and it follows that $x \in R - P$. As a result, we have $x \cdot [1, 1] \in IR_P$. Since $[1, x] \in R_P$, we also have $x \cdot [1, x] \in IR_P$, and thus $1 \in IR_P$. Note that the only ideal that contains 1 is the whole ring, so $J = R_P$, which is a contradiction.

These two arguments prove that all ideals J such that $J \neq R_P$ is contained in PR_P, so by definition PR_P is the only maximal ideal. □

3. Integral Extension, Discrete Valuation Ring and Dedekind Domain

The integral extension of a ring is a well-studied concept in commutative algebra that leads to the definition of integers in finite extensions of certain fields. Given a commutative ring S and its subring R, we first define the condition for S to be an integral extension of R and the condition for R to be integrally closed.

Definition 3.1. Suppose S is a commutative ring and let R be a subring of S. Then we have the following three definitions:

(1) The element $s \in S$ is said to be *integral over* R if s is the root of a monic polynomial in $R[x]$. The ring S is an *integral extension* of R if every element $s \in S$ is integral over R.
(2) The *integral closure* of R in S is defined as the set of elements in S that are integral over R. The ring R is said to be *integrally closed* in S if R is equal to its integral closure in S.
(3) Let R be an integral domain. R is called *integrally closed* or *normal* if it is integrally closed in its field of fractions.

Example 3.2. The set of integers $\mathbb{Z}$ is integrally closed.

Proof. It suffices to show that any rational solution to a monic polynomial in $\mathbb{Z}[x]$ is an integer. In fact, suppose $\frac{p}{q}$ (p and q are coprime) is a solution to the monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, then we have $p^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0$, so p^n is divisible by q, which implies that $q = 1$. Hence, the rational solution to the monic polynomial in $\mathbb{Z}[x]$ has to be an integer. □

Based on the definitions above, we can now prove an important theorem which suggests the closeness of addition and multiplication of an integral closure.

Theorem 3.3. *Let R be a subring of the commutative ring S and let $s \in S$. The following three statements are equivalent:*

(1) s is integral over R.
(2) $R[s]$ is a finitely generated R-module.
(3) There exists a finitely generated ring T such that $R \subset T \subset S$ and $s \in T$.

Proof. First, we show that (1) implies (2). Suppose s is the root of the monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, then we have $s^n = -(a_{n-1}s^{n-1} + a_{n-2}s^{n-2} + \cdots + a_0)$. By induction, we can also see that higher powers of s can be expressed as a linear combination of $s^{n-1}, \cdots, s, 1$.

Second, it is easy to notice that (2) implies (3) with $T = R[s]$.

Third, suppose $s \in T$ for some subring T that is generated by the elements $v_1, v_2, \cdots, v_n$. Since T is a ring, we have $sv_i \in T$ for $i = 1, 2, \cdots, n$. Hence, they can be written as $sv_i = \sum_{j=1}^{n} a_{ij}v_j$. Adding up those equations, we get:

$$0 = \sum_{j=1}^{n} (\delta_{ij}s - a_{ij})v_j$$

where δ_{ij} is the Kronecker delta. Let M be the $n \times n$ matrix $(\delta_{ij}s - a_{ij})$. By Cramer's Rule, we have $(detM)v_i = 0$ for all $i = 1, 2, \cdots, n$, and hence $detM = 0$ since $1 \in T$ is a linear combination of $v_1, v_2, \cdots, v_n$. Let N be the matrix (a_{ij}) and I be the matrix (δ_{ij}), so $det(sI - N) = 0$. Note that the equation $det(xI - N) = 0$ is a monic polynomial with coefficients in R, so we proved that (3) implies (1). □

Proposition 3.4. *Let S be a commutative ring and let R be a subring of S. The integral closure of R in S is closed under addition and multiplication, and is consequently a subring of S.*

Proof. It suffices to show the following statement: for all $s, t \in S$, if s and t are integral over R, then $s+t$ and st are integral over R. In fact, since s and t are integral over R, by Theorem 3.3 we know that $R[s]$ and $R[t]$ are finitely generated R-modules. Suppose $R[s]$ is generated by $s_1, s_2, \cdots, s_n$, and $R[t]$ is generated by $t_1, t_2, \cdots, t_m$. Thus we have

$$R[s] = Rs_1 + Rs_2 + \cdots + Rs_n$$
$$R[t] = Rt_1 + Rt_2 + \cdots + Rt_m$$

Consider the following R-module:

$$R[s,t] = \sum_{i=1}^{n} \sum_{j=1}^{m} Rs_i t_j$$

Since $s+t, st \in R[s,t]$, $R[s] \subset R[s,t] \subset S$ and $R[t] \subset R[s,t] \subset S$, by Theorem 3.3, $s+t$ and st are integral over R. Since addition and multiplication are closed in the integral closure of R in S, we know that the integral closure of R in S is a subring of S. □

Discrete Valuation Ring is the easiest kind of Noetherian ring of dimension 1 and is especially important in commutative algebra. We now give the definition of a discrete valuation and a D.V.R. (Discrete Valuation Ring).

Definition 3.5. Let K be a field. A *discrete valuation* on $K^\times$ is a function f: $K^\times \to \mathbb{Z}$ such that:

(1) f is surjective.
(2) For all $x, y \in K$ we have $f(xy) = f(x) + f(y)$.
(3) For all $x, y \in K$, if $x + y \neq 0$, then $f(x+y) \geq \min\{f(x), f(y)\}$.

Definition 3.6. Let K be a field and f be a discrete valuation on K. The subring $\{x \in K : f(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of f. An integral domain R is called a *Discrete Valuation Ring* (D.V.R) if it is the valuation ring of a discrete valuation f on the field of fractions of R.

Example 3.7. Let f_p be the function on $\mathbb{Q}$ defined as follows: for an element $\frac{a}{b} \in \mathbb{Q}$, let $\frac{a_1}{b_1}$ be the fraction such that $\frac{a}{b} = p^n \frac{a_1}{b_1}$ (where both a_1 and b_1 are relatively prime to p), then $f(\frac{a}{b}) = n$. We can further check that the localization of $\mathbb{Z}$ at a prime ideal (p) is a D.V.R.

Finally, using the definition of integral closedness, we are able to define a Dedekind domain.

Definition 3.8. A *Dedekind Domain* is a Noetherian and integrally closed integral domain of Krull dimension 1.

4. Unique Factorization of Ideals in a Dedekind Domain

One of the most interesting results with regard to the Dedekind domain is that any ideal in a Dedekind domain can be written uniquely as the product of prime ideals. Below we provide a detailed proof for this theorem, using the concept of Discrete Valuation Ring.

Theorem 4.1. *Let R be a Dedekind domain and $I \subset R$ be a nonzero ideal. I can be written uniquely as the product $I = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$, where $P_1, P_2, \cdots, P_n$ are prime ideals, and $e_1, e_2, \cdots, e_n$ are positive integers.*

To prove this theorem, we first consider the following lemma.

Lemma 4.2. *Let R be a commutative ring and M be a R-module. Then we have*

(1) $M = 0$ if and only if $M_m = 0$ for all maximal ideal $m \subset R$.
(2) Suppose that $N \subset M$ is a R-submodule. If $N_m = M_m$ for all maximal ideal $m \subset R$, then $N = M$.

Proof. We first prove (1). Consider the set $\mathrm{Ann}(x) = \{r \in R : rx = 0\}$ for $x \in M$. We show that it is a proper ideal when x is nonzero. First, the set is closed under addition. Suppose $s, t \in \mathrm{Ann}(x)$, then $sx = 0$ and $tx = 0$, so $(s + t)x = 0$, which implies that $s + t \in \mathrm{Ann}(x)$. Second, suppose $r \in R$ and $s \in \mathrm{Ann}(x)$, then we have $sx = 0$ and hence $(sr)x = 0$, which implies that $sr \in \mathrm{Ann}(x)$. In addition, when $x \neq 0$, we know that $1 \notin \mathrm{Ann}(x)$, so $\mathrm{Ann}(x)$ is a proper ideal when $x \neq 0$ and is thus contained in some maximal ideal m.

In fact, suppose by contradiction that M is nonzero and suppose that $x \neq 0$ is one of its element. By the definition of localization, the localization of M at the maximal ideal m should contain the nonzero element $\frac{x}{1}$. However, this is impossible because there does not exist a nonzero element $s \in m$ such that $sx = 0$ because $\mathrm{Ann}(x)$ has included all of such s, which gives (1).

To prove (2), we consider the quotient module M/N. Since $M = N$ if and only if $M/N = 0$, by part (1) it suffices to show that $(M/N)_m = 0$ for all maximal ideal $m \subset R$. Suppose that f is an element in $R - m$, and consider the map $F : (M/N)_m \to M_m/N_m$ that sends the element $\frac{[x]}{f}$ to $[\frac{x}{f}]$.

We first show that the map F is well-defined. In fact, suppose that the two elements $\frac{[x]}{f}, \frac{[y]}{f} \in (M/N)_m$ $(x, y \in M)$ are equal, then there exists an element $a \in R - m$ such that $a(f[x] - f[y]) = 0$. Hence, we get $[afx] = [afy]$, so there exists $b \in N$ such that $af(x - y) = b$. This implies that $[\frac{x}{f}] = [\frac{y}{f}]$, so F is well-defined. Next, consider another map $G : M_m/N_m \to (M/N)_m$ that sends the element $[\frac{x}{f}]$ to $\frac{[x]}{f}$, and we can use similar methods to prove that G is also well-defined. Due to the fact that for all $n \in (M/N)_m$, we have $G(F(n)) = n$, so both F and G are bijective. This completes the proof for (2) since $(M/N)_m = M_m/N_m = 0$. □

The three theorems below are necessary for proving Theorem 4.1.

Theorem 4.3. *Let R be a Dedekind domain and let $I \subset R$ be a nonzero ideal. Then there are only finitely many maximal ideals p of R such that $I \subset p$.*

Proof. We prove the theorem by first showing the following lemma.

Lemma 4.4. *Let R be a commutative Noetherian ring. Let $I \subset R$ be an ideal, and let $p(I)$ be the set of all prime ideals containing I (ordered by inclusion), then there are only finitely many minimal elements in $p(I)$.*

Proof for Lemma 4.4. Suppose by contradiction that there exists an ideal I such that there are infinitely many minimal elements in $p(I)$. Let Σ be the collection of all such ideals. Since R is a Noetherian ring, every chain of prime ideals under inclusion has a maximal element. Hence, by Zorn's Lemma, under the partial order of inclusion, Σ contains a maximal element I_0. Now we consider the following three cases:

(1) I_0 is a prime ideal. Then I_0 itself is the only minimal element of $p(I_0)$, which contradicts with the fact that $p(I_0)$ contains infinitely many minimal elements.
(2) $I_0 = R$. Then $p(I_0)$ does not contain any elements, which is also a contradiction.
(3) I_0 is not a prime ideal. By definition, there exist two elements $a, b \in R$ such that $ab \in I_0$ but $a \notin I_0$ and $b \notin I_0$. Hence, any prime ideal I' containing I_0 must contain either a or b. (Otherwise we have $ab \in I'$, $a \notin I'$ and $b \notin I'$, yet I' is prime) This implies that I' must contain either $I_0 + (a)$ or $I_0 + (b)$, and in other words, $p(I_0) = p(I_0 + (a)) \cup p(I_0 + (b))$. However, since $I_0 \subset I_0 + (a)$ and $I_0 \subset I_0 + (b)$, by the maximality of I_0 in the set Σ, we know that both $p(I_0 + (a))$ and $p(I_0 + (b))$ contain finitely many minimal elements. However, $p(I_0)$ contains infinitely many minimal elements by our assumption, so it is impossible that $p(I_0) = p(I_0 + (a)) \cup p(I_0 + (b))$.

□

Back to the proof for Theorem 4.3. Applying Lemma 4.4 with the ideal I, we know that $p(I)$ contains finitely many minimal elements. Since a Dedekind domain has dimension 1, these minimal elements are also maximal, which completes the proof for the theorem. □

Theorem 4.5. *Let R be a Dedekind domain and let P be a nonzero prime ideal of R. Then the localization of R at P is a Discrete Valuation Ring.*

Proof. The detailed proof is written in David S. Dummit and Richard M. Foote's book *Abstract Algebra* (third edition), page 758. □

Theorem 4.6. *Let R be a Discrete Valuation Ring such that R is an integrally closed local ring with unique maximal ideal $M = \{r \in R : v(r) > 0\}$, then any nonzero ideal in R has the form M^n for some non-negative integer n.*

Proof. The detailed proof is written in David S. Dummit and Richard M. Foote's book *Abstract Algebra* (third edition), page 757. □

Finally, we are able to give a proof for Theorem 4.1.

Proof for Theorem 4.1. Suppose R is a Dedekind domain and $I \subset R$ is a nonzero ideal. By Theorem 4.3, there are only finitely many maximal ideals p of R such that $I \subset p$. Let $p_1, p_2, \cdots, p_n$ be those maximal ideals. By Theorem 4.5 and Theorem 4.6, for any $i = 1, 2, \cdots, n$, since IR_{p_i} (the extension of I to R_{p_i}) is a Discrete Valuation Ring, we have $IR_{p_i} = p_i^{e_i} R_{p_i}$, where e_i is a positive integer. For any other maximal ideal p' of R besides $p_1, p_2, \cdots, p_n$, using the same argument in Example 2.9, we get $IR_{p_i} = R_{p_i}$. Hence, consider the specific ideal $I' = p_1^{e_1} \cdots p_n^{e_n}$, and then it suffices to show that $IR_p = I'R_p$ for all maximal ideals p.

In fact, for $p \notin \{p_1, p_2, \cdots, p_n\}$, we have $I'R_p = R_p$ and $IR_p = R_p$ (as we proved in Example 2.9), so it is clear that $I'R_p = IR_p$. For $p \in \{p_1, p_2, \cdots, p_n\}$, without loss of generality we can assume that $p = p_1$. Hence, $I'R_P = p_1^{e_1}(p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}) R_{p_1} = p_1^{e_1} R_{p_1} = IR_P$ (Note that the proof in Example 2.9 suggests that $(p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}) R_{p_1} = R_{p_1}$).

Thus, it follows that for any maximal ideal $p \in R$, we get $IR_p = I'R_p$, and hence $I_p = I'_p$ by Theorem 2.8. This implies that $I = I'$ by Lemma 4.2, which completes our proof. □

Finally, we provide an example of the unique factorization of ideals in the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$.

Example 4.7. The ring $\mathbb{Z}[\sqrt{-5}]$ is the ring of numbers with the form $a + b\sqrt{-5}$, where a and b are integers. Now we show that it is a Dedekind domain, and hence all ideals have a unique factorization into prime ideals. In fact, to prove that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, it suffices to show that it is Noetherian, integrally closed and has dimension 1.

First, since $\mathbb{Z}$ is a Noetherian ring, it follows from Hilbert's Basis Theorem (see Serge Lang's book *Algebra* (revised third edition), page 186) that $\mathbb{Z}[x]$ is Noetherian. Due to the fact that the map from $\mathbb{Z}[x]$ to $\mathbb{Z}[\sqrt{-5}]$ is surjective, we know that $\mathbb{Z}[\sqrt{-5}]$ is also Noetherian.

Next, to prove that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed, it suffices to prove the following fact: if $a + b\sqrt{-5}$ $(a, b \in \mathbb{Q})$ is a solution to a monic polynomial with coefficients in $\mathbb{Z}$, then $a, b \in \mathbb{Z}$. Now we introduce the following definitions and lemma regarding polynomials.

Definition 4.8. A polynomial is called *monic* if its leading coefficient is 1.

Definition 4.9. The minimal polynomial of a number α in a field K is the polynomial $m_{\alpha,K}(x)$ with the least degree such that α is a solution to $m_{\alpha,K}(x)$ and the coefficients of $m_{\alpha,K}(x)$ are in K.

Lemma 4.10. *Let m be a number such that it is the solution to a monic polynomial with coefficients in $\mathbb{Z}$. Then its minimal polynomial in $\mathbb{Q}$ also has integer coefficients.*

Proof for Lemma 4.10. Let $f(x)$ be the minimal polynomial of m in $\mathbb{Z}$. We consider the following two cases:

(1) $f(x)$ is reducible in $\mathbb{Q}$. By Gauss' Lemma, there exists $g(x)$ and $h(x)$ of integer coefficients such that $f(x) = g(x)h(x)$. This is a contradiction since m would be either the solution to $g(x)$ or the solution to $h(x)$, yet both $g(x)$ and $h(x)$ have a lower degree than $f(x)$.
(2) $f(x)$ is irreducible in $\mathbb{Q}$, then $f(x)$ is the minimal polynomial of m in $\mathbb{Q}$ and it has integer coefficients.

This gives the proof for the lemma. □

Given Lemma 4.10, we can now prove that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed. Let $\alpha = a + b\sqrt{-5}$ $(a, b \in \mathbb{Q})$, then we know that its minimal polynomial in $\mathbb{Q}$ would be $f(x) = x^2 - 2ax + a^2 + 5b^2$. By Lemma 4.10, we have $2a \in \mathbb{Z}$ and $a^2 + 5b^2 \in \mathbb{Z}$. Hence, $20b^2 = 4(a^2 + 5b^2) - (2a)^2$ is an integer. This implies that $20b^2 \in \mathbb{Z}$, so $2b \in \mathbb{Z}$. Let $2a = a'$ and $2b = b'$, then $a^2 + 5b^2 = \frac{a'^2+5b'^2}{4}$ is an integer. This could only happen when both a' and b' are even, so a and b are integers and hence $\mathbb{Z}[\sqrt{-5}]$ is integrally closed.

Finally, to prove that $\mathbb{Z}[\sqrt{-5}]$ has Krull dimension 1, it suffices to show that it has the same dimension as $\mathbb{Z}$, so we only need to prove the following lemma.

Lemma 4.11. *Let $R \subset S$ be two commutative rings such that S is integral over R, then dim S = dim R.*

The proof for the lemma requires the following theorem:

Theorem 4.12. *Suppose that $R \subset S$ are two commutative rings such that S is integral over R. Then we have the following three facts:*

(1) Assume that S is an integral domain. Then R is a field if and only if S is a field.
(2) For every prime ideal P of R, there exists a prime ideal Q of S such that $P = Q \cap R$. In addition, P is a maximal ideal if and only if Q is a maximal ideal.
(3) Let $P_1 \subset P_2 \subset \cdots \subset P_n$ be a chain of prime ideals of R and suppose we have $Q_1 \subset Q_2 \subset \cdots \subset Q_m$ of S such that $P_i = Q_i \cap R$ ($1 \leq i \leq m$ and $m < n$). Then there exists prime ideals $Q_{m+1} \subset \cdots \subset Q_n$ of S such that $P_j = Q_j \cap R$ for all $m + 1 \leq j \leq n$.

Proof. The detailed proof is written in David S. Dummit and Richard M. Foote's book *Abstract Algebra* (third edition), page 694. □

Now we are able to give a proof for Lemma 4.11.

Proof for Lemma 4.11. It suffices to show that dim $R \geq$ dim S and dim $S \geq$ dim R. First, let $q \subset S$ be a prime ideal of S, we show that $q \cap R$ is a prime ideal of R. In fact, $q \cap R$ is an ideal of R because it is additively and multiplicatively closed, and for all $x \in q \cap R$ and $r \in R$, we have $xr \in q$ and $xr \in R$, so $xr \in q \cap R$. It is also prime because otherwise there exist $a, b \in R$ such that $a, b \notin q$ and $a, b \in q \cap R$, which contradicts with the fact that q is a prime ideal of S.

Next, let $q_0 \subset q_1$ be two prime ideals in S, and let $p_0 = q_0 \cap R$ and $p_1 = q_1 \cap R$. We want to show that if $p_0 = p_1$, then $q_0 = q_1$. Let $\overline{R} = R/p_0$, $\overline{S} = S/q_0$ and $\overline{q} = q_1/q_0$. Hence we have $\overline{R} \subset \overline{S}$ are both integral domains, and $\overline{q} \cap R = (0)$. Notice that $\overline{S}$ is still integral over $\overline{R}$: given an element $s \in S$, suppose it satisfies a monic polynomial F with coefficients in R, then $s + q_0$ satisfies the same equation F with coefficients mod p_0. In addition, let $D = \overline{R} - \{0\}$, then $D^{-1}\overline{S}$ is also integral over $D^{-1}\overline{R}$: suppose $\frac{s}{d} \in D^{-1}\overline{S}$, and suppose s satisfies a monic polynomial $F = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where $a_{n-1}, \cdots, a_0 \in R$, then $\frac{s}{d}$ satisfies the monic polynomial $F' = x^n + \frac{a_{n-1}}{d}x^{n-1} + \cdots + \frac{a_1}{d^{n-1}}x + \frac{a_0}{d^n}$. (Note that all coefficients of F' are in $D^{-1}\overline{R}$) Since $D^{-1}\overline{R}$ is a field and $\overline{R}$ and $\overline{S}$ are both integral domains, by Theorem 4.12(1), $D^{-1}\overline{S}$ is also a field. By assumption, $D \cap \overline{q} = \emptyset$, so $\overline{q}D^{-1}\overline{S}$ is a prime in $D^{-1}\overline{S}$, and hence must be the zero ideal. Finally, since the map from $\overline{S}$ to $D^{-1}\overline{S}$ is injective, we know that $\overline{q}$ must be zero, which implies that $q_0 = q_1$.

The two facts above suggest that any chain of prime ideals $q_0 \subsetneq \cdots \subsetneq q_n$ in S gives a chain of prime ideals $q_0 \cap R \subsetneq \cdots \subsetneq q_n \cap R$ in R, so dim $R \geq$ dim S. On the other hand, by Theorem 4.12(3), any chain of prime ideals $p_0 \subsetneq \cdots \subsetneq p_n$ in R also gives a chain of prime ideals $q_0 \subsetneq \cdots \subsetneq q_n$ in S, so dim $R \leq$ dim S. This indicates that dim $R =$ dim S. □

Now we are able to complete the proof for the fact that $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain. Note that (p) (p is a prime number) are the only prime ideals in $\mathbb{Z}$, and for any two prime numbers (p) and (q) we have $(p) \not\subset (q)$ and $(q) \not\subset (p)$, so the set of integers $\mathbb{Z}$ has Krull dimension 1. By Lemma 4.11, $\mathbb{Z}[\sqrt{-5}]$ also has dimension 1, so it is a Noetherian and integrally closed integral domain of Krull dimension 1.

In fact, since $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, all ideals can be uniquely factorized into the product of prime ideals. For example, the three ideals (2), (5) and (11) can be factorized as follows:

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$$
$$(5) = (\sqrt{-5})^2$$
$$(11) = (11)$$

where $(2, 1 + \sqrt{-5}), (2, 1 - \sqrt{-5}), (\sqrt{-5})$ and (11) are all prime ideals in $\mathbb{Z}[\sqrt{-5}]$.

Acknowledgements

I would like to thank my mentor, Griffin Wang, for his instruction and support on this paper. It is also a pleasure to thank Professor Peter May for organizing this program.

References

[1] David S. Dummit and Richard M. Foote. Abstract Algebra, third edition. John Wiley & Sons, Inc.
[2] Serge Lang. Algebra, revised third edition, volume 1. Springer Science+Business Media.