Unique Factorization in Dedekind Domains

September 4, 2016

1 Definitions

We start with some definitions.

1.1 Noetherian Rings

Definition 1.1. A commutative ring R is *Noetherian* if every ideal of R is finitely generated. In other words, for every ideal I of R, there exist a finite number of elements of I, say $a_1, a_2, \ldots, a_k$ such that $I = (a_1) + (a_2) + \cdots + (a_k)$. Elements $a_1, a_2, \ldots, a_k$ are called *generators* of I.

The following property of Noetherian rings would be useful for us.

Lemma 1.2. *A commutative ring R is Noetherian iff every strictly increasing sequence of ideals, $I_1 \subset I_2 \subset I_3 \subset \cdots$, is finite.*

Proof. Suppose R is Noetherian. Suppose R has an infinite strictly increasing sequence of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$. Define $I = \bigcup_{i \geq 1} I_i$. Set I is also an ideal of R:

- If $a, b \in I$ then there exists a j such that $a, b \in I_j$. And then $a + b \in I_j \subseteq I$.
- If $a \in I$ then there exists a j such that $a \in I_j$. Then $b \cdot a \in I_j \subseteq I$ for any $b \in R$.

Sicne R is Noetherian, I is finitely generated. Let its generators be $a_1, a_2, \ldots, a_k$. Then there exists a j such that $a_1, a_2, \ldots, a_k \in I_j$. Then $I = (a_1) + (a_2) + \cdots + (a_k) \subseteq I_j$. Hence $I = I_j$, a contradiction.

Conversely, suppose every strictly increasing sequence of ideals in R is finite. Let I be an ideal of R. Pick $a_1 \in I$, $a_1 \neq 0$. Then ideal $I_1 = (a_1) \subseteq I$. If the equality holds, then I is finitely generated. Otherwise, there exists $a_2 \in I \backslash I_1$. Then ideal $I_2 = (a_1) + (a_2) \subseteq I$. Again, if equality holds, I is finitely generated. Otherwise, there exists $a_3 \in I \backslash I_2$. Continuing this way, we construct a strictly increasing sequence of ideals $I_1 \subset I_2 \subset I_3 \cdots$. This must be finite, which gives that $I = I_k$ for some k. Thus I is finitely generated. $\square$

1.2 Integral Domains and Fraction Fields

Definition 1.3. A commutative ring R is an *integral domain* if for every $a, b \in R \backslash \{0\}$, $a \cdot b \neq 0$.

An example of integral domain is the ring $\mathbb{Z}$. An integral domain naturally gives rise to a field, called its *field of fractions* or *fraction field*. Intuitively, it is the set of elements of the form $\frac{a}{b}$ for a and b in the integral domain with $b \neq 0$. For example, $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. To define it formally, we need some work though.

Let R be an integral domain. Define ring $\hat{R}$ as:

$$\hat{R} = \{(a, b) \mid a, b \in R \text{ and } b \neq 0\}.$$

The operations in $\hat{R}$ are defined as follows: $(a_1, b_1) + (a_2, b_2) = (a_1 \cdot b_2 + a_2 \cdot b_1, b_1 \cdot b_2)$, and $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$. It is easy to verify that under these two operations, $\hat{R}$ is a commutative ring when R is an integral domain. Discerning eyes would realize that the addition and multiplication operations as defined above are capturing operations on fractions $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$. The problem is that there are multiple elements that should be the same: $\frac{a}{b}$ and $\frac{ca}{cb}$ for any $c \neq 0$. We fix this by removing multiple copies. Let

$$I = \{(0, b) \mid b \in R \text{ and } b \neq 0\}.$$

Set I is an ideal of $\hat{R}$: $(0, b_1) + (0, b_2) = (0, b_1 \cdot b_2)$ and $(a, b) \cdot (0, b_1) = (0, b \cdot b_1)$. In fact,

Lemma 1.4. *I is a maximal ideal of R.*

Proof. Let J be an ideal of R containing I. If $J \neq I$, then $(a, b) \in J$ for some $(a, b) \in \hat{R}$ with $a \neq 0$. Then $(b, a) \in \hat{R}$ and so $(a, b) \cdot (b, a) = (a \cdot b, a \cdot b) \in J$. We have:

$$(a \cdot b, a \cdot b) - (1, 1) = (a \cdot b - a \cdot b, a \cdot b) = (0, a \cdot b) \in J.$$

Hence, $(1, 1) \in J$, and therefore, $J = \hat{R}$. □

Define $F = \hat{R}/I$. Since I is a maximal ideal, F is a field. An element of F is a class $(a, b) + I$ which contains precisely the elements $(a \cdot c, b \cdot c)$ for $c \neq 0$. We will write elements of F as $\frac{a}{b}$, $b \neq 0$, with elements $\frac{a \cdot c}{b \cdot c}$ treated as equal for $c \neq 0$. This corresponds nicely to the elements of $\mathbb{Q}$. F is the field of fractions of R.

1.3 Integrally Closed Rings

Let R and $\hat{R}$ be commutative rings with $R \subset \hat{R}$.

Definition 1.5. Element $e \in \hat{R}$ is *integral over R* if $e^d + a_{d-1}e^{d-1} + \cdots + a_1 e + a_0 = 0$ for some $d > 0$ and $a_0, a_1, \ldots, a_{d-1} \in R$.

Integral elements over R in the ring $\hat{R}$ are, in a sense, "close" to the elements of R as they can be defined purely in terms of R. This notion allows us to extend the definition of integers to rings bigger than $\mathbb{Z}$. For example, in the field $\mathbb{Q}[i\sqrt{3}]$, elements of the form $a + i\sqrt{3}b$ with $a, b \in \mathbb{Z}$ are integral over $\mathbb{Z}$:

$$(a + i\sqrt{3}b)^2 = a^2 - 3b^2 + 2a \cdot (a + i\sqrt{3}b) - 2a^2 = 2a \cdot (a + i\sqrt{3}b) - a^2 - 3b^2.$$

Thus, elements of the ring $\mathbb{Z}[i\sqrt{3}]$ are all integral over $\mathbb{Z}$. These can be viewed as "integers" of the field $\mathbb{Q}[i\sqrt{3}]$. In fact, even $\frac{1+i\sqrt{3}}{2}$ is integral:

$$\frac{(1+i\sqrt{3})^2}{4} = \frac{-2+2i\sqrt{3}}{4} = \frac{1+i\sqrt{3}-2}{2} = \frac{1+i\sqrt{3}}{2} - 1.$$

It can be shown that integral elements of $\mathbb{Q}[i\sqrt{3}]$ are precisely $a + b\frac{1+i\sqrt{3}}{2}$ for $a, b \in \mathbb{Z}$.

An integrally closed ring is one that cannot be extended in this way.

Definition 1.6. Ring R is *integrally closed in* $\hat{R}$ if for every $e \in \hat{R}$, if e is integral over R then $e \in R$.

For example, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$: if $(\frac{c}{\hat{c}})^d + \sum_{i=0}^{d-1} a_i (\frac{c}{\hat{c}})^i = 0$ for $a_i, c, \hat{c} \in \mathbb{Z}$ with $\gcd(c, \hat{c}) = 1$, then $c^d + \sum_{i=0}^{d-1} a_i c^i \hat{c}^{d-i} = 0$. Therefore, c^d is divisible by $\hat{c}$. Since $\gcd(c, \hat{c}) = 1$, $\hat{c} = 1$.

1.4 Dedekind Domains

We can now define our the main objects of study.

Definition 1.7. Commutative ring R is a *Dedekind domain* if:

1. R is Noetherian,
2. R is an integral domain,
3. R is integrally closed in F, its field of fractions, and
4. Every prime ideal of R is maximal.

Dedekind domains admit unique factorization of ideals, as we show in the next section.

2 Unique Factorization in Dedekind Domains

Let R be a Dedekind domain and R its field of fractions. We first show a key property of Dedekind domains.

Theorem 2.1. *Let I be an ideal of R and $a \in I$, $a \neq 0$. Then there exists an ideal J such that $I \cdot J = (a)$.*

Proof of Theorem 2.1

Proof of this theorem is a bit involved, and uses all the properties of Dedekind domains. Define J as:

$$J = \{b \mid b \in R \text{ and } bI \subseteq (a)\}.$$

Clearly, J is an ideal and $I \cdot J \subseteq (a)$. We now show that $I \cdot J = (a)$. Let us start with a lemma:

Lemma 2.2. *Every ideal of R contains a product of prime ideals.*

Proof. Suppose not. Let S be the set of all ideals of R that do not contain a product of prime ideals. Since R is Noetherian, set S has a maximal element, say I. Observe that I is not a prime ideal and $I \neq (1)$ (as (1) contains prime ideals). Hence, there exist elements $a, b \in R$ such that $a \cdot b \in I$ but $a, b \notin I$. Consider ideals $I_1 = (a) + I$ and $I_2 = (b) + I$. Both are strictly bigger than I and hence do not belong to the set S. Therefore, both contain products of prime ideals. But $I_1 \cdot I_2 \subseteq I$ and hence I also contains a product of prime ideals. Contradiction. □

Let F be the field of fractions of R. The next lemma shows an intersting properties of proper ideals of R that we will use repeatedly.

Lemma 2.3. *Let I be a proper ideal of R. Then there exists prime ideals P_1, P_2, …, P_k such that $P_1 P_2 \cdots P_k \subseteq I \subseteq P_1$.*

Proof. By Lemma 2.2, there exist prime ideals P_1, P_2, …, P_k such that $P_1 P_2 \cdots P_k \subseteq I$. Further, since I is a proper ideal, I is contained in a maximal ideal P, which is also a prime ideal. Hence, we have $P_1 P_2 \cdots P_k \subseteq P$.

We show that $P = P_i$ for some $1 \leq i \leq k$. Assume that $P_i \not\subseteq P$ for $1 \leq i \leq k$. Then there exists $a_i \in P_i \backslash P$. However, $\prod_{i=1}^{k} a_i \in P$ which contradicts the fact that P is prime. Therefore, $P_i \subseteq P$ for some $1 \leq i \leq k$. Since P_i is a prime ideal, and R is a Dedekind domain, P_i is also maximal. Hence $P = P_i$. By renumbering, we can get $P = P_1$. □

Multiplying an ideal with any element of R keeps the resulting element in the ideal. We show that multiplying a proper ideal of R by an appropriate element of $F \backslash R$ keeps the result in R.

Lemma 2.4. *Let I be an ideal of R, $I \neq (1)$. Then there exists $\alpha \in F \backslash R$ such that $\alpha I \subseteq R$.*

Proof. Let $b \in I$. By the above lemma, ideal (b) contains a product of prime ideals. Choose such a product in (b) with smallest number of prime ideals. Let it be $P_1 P_2 \cdots P_k$. Since $I \neq (1)$, by Lemma 2.3, we have $P_1 P_2 \cdots P_k \subseteq (b) \subseteq I \subseteq P_1$. By minimality of k, we have that $P' = P_2 \cdots P_k \not\subseteq (b)$. Let $c \in P' \backslash (b)$ and $\gamma = \frac{c}{b}$. We have $\gamma \in F \backslash R$, and $\gamma I \subseteq \gamma P_1 = \frac{1}{b} P_1 c \subseteq \frac{1}{b}(b) \subseteq R$. □

We now resume the proof of theorem. Let $A = \frac{1}{a}(I \cdot J)$. Since $I \cdot J \subseteq (a)$, $A \in R$, and can be easily verified to be an ideal. If $A = (1)$, then $I \cdot J = aA = (a)$, and we are done. Otherwise, A is a proper ideal of R. Therefore, there exists $\gamma \in F \backslash R$ such that $\gamma A \subseteq R$. Since $a \in I$, we get that $J \subseteq A$. Hence, $\gamma J \subseteq \gamma A \subseteq R$. Multiplying by a, we get $a\gamma J \subseteq \gamma a A = \gamma(I \cdot J) = I \cdot \gamma J \subseteq (a)$. By definition of J, therefore, $\gamma J \subseteq J$.

Since R is Noetherian, J has a finite number of generators. Let these by g_1, g_2, …, g_t. Since $\gamma J \subseteq J$, we have $\gamma g_i = \sum_{\ell=1}^{t} c_{i,\ell} g_\ell$ for $c_{i,\ell} \in R$, $1 \leq i \leq t$. In other words, letting

$$\mathbf{C} = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,t} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ c_{t,1} & c_{t,2} & \cdots & c_{t,t} \end{bmatrix},$$

and

$$\mathbf{g} = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_t \end{bmatrix},$$

we get

$$(\gamma \mathbf{I} - \mathbf{C}) \cdot \mathbf{g} = 0,$$

where $\mathbf{I}$ is the identity matrix. Therefore, $\det(\gamma \mathbf{I} - \mathbf{C}) = 0$. This gives a polynomial of degree t over R satisfied by γ. Hence, γ is integral over R, and since R is a Dedekind domain, $\gamma \in R$. This contradicts that fact that $\gamma \in F \backslash R$. Going back in the argument, we find that A cannot be a proper ideal of R, hence $A = (1)$, or equivalently, $I \cdot J = (a)$. This completes the proof of theorem.

2.1 Fractional Ideals

By Theorem 2.1, for every ideal I of R, there exists an ideal J such that $I \cdot J = (a)$. We can rewrite this as $I \cdot \frac{1}{a} J = (1)$. Thus, $\frac{1}{a} J$ is "inverse" of I. However, $\frac{1}{a} J \notin R$. To handle this, we observe that $\frac{1}{a} J \in F$, and define the notion of fractional ideals.

Definition 2.5. Set $\hat{I} \subseteq F$ is a *fractional ideal* if there exists $a \in R$ and ideal J of R such that $\hat{I} = \frac{1}{a} J$.

Fractional ideals have similar properties as ideals:

Lemma 2.6. *A fractional ideal $\hat{I}$ is a commutative group under addition and $R \cdot \hat{I} \subseteq \hat{I}$.*

Proof. Follows immediately from the fact that $\hat{I} = \frac{1}{a} J$ and J is an ideal of R. □

Note that every ideal of R is also a fractional ideal. Let

$$\mathcal{J} = \{J \mid J \text{ is a fractional ideal}\}.$$

Multiplication of ideals can be naturally extended to multiplication of fractional ideals: if $J_1 = \frac{1}{a_1} I_1$ and $J_2 = \frac{1}{a_2} I_2$ are two fractional ideals, then $J_1 \cdot J_2 = \frac{1}{a_1 a_2} I_1 \cdot I_2$.

Lemma 2.7. *$\mathcal{J}$ is a commutative group under multiplication.*

Proof. Closure, associativity, and commutativity are immediate from the definition and above discussion. Ideal (1) is the identify of multiplication as $J \cdot (1) = J$ for every fractional ideal. For inverse of fractional ideal $J = \frac{1}{b} I$, I an ideal of R, Theorem 2.1 gives an ideal $\hat{J}$ of R and element $a \in R$ such that $I \cdot \frac{1}{a} \hat{J} = (1)$. Hence,

$$J \cdot \frac{b}{a} \hat{J} = \frac{1}{b} I \cdot \frac{b}{a} \hat{J} = (1).$$

□

2.2 Unique Factorization Theorem

We are now ready to prove the unique factorization theorem.

Theorem 2.8. *Every proper ideal I of R can be uniquely written as product of prime ideals of R.*

Proof. We will first prove existence of prime factorization. By Lemma 2.2, I contains a product of prime ideals $P_1 P_2 \cdots P_k$. Since I is a proper ideal, by Lemma 2.3, $P_1 P_2 \cdots P_k \subseteq I \subseteq P_1$. Now the proof is by induction on k.

Base case is when $k = 1$. Then, $P_1 \subseteq I \subseteq P_1$, and hence $I = P_1$.

For induction step, assume that if an ideal contains a product of up to $k-1$ primes, then it equals the product. Now suppose

$$P_1 P_2 \cdots P_k \subseteq I \subseteq P_1.$$

Let $\hat{P}_1$ be the inverse of P_1 in $\mathcal{J}$. Multiplying it to the above containments, we get:

$$P_2 P_3 \cdots P_k \subseteq \hat{P}_1 \cdot I \subseteq (1).$$

Fractional ideal $\hat{P}_1 \cdot I$ is contained in R, and hence is an ideal of R that contains a product of $k-1$ prime ideals. By induction hypothesis,

$$\hat{P}_1 \cdot I = P_2 P_3 \cdots P_k.$$

Multiplying it by P_1, we get:

$$I = P_1 P_2 P_3 \cdots P_k,$$

completing the existence proof.

Now we show uniqueness. Let I be a proper ideal with $I = P_1 P_2 \cdots P_k$ for prime ideals P_i. Suppose we can also write $I = Q_1 Q_2 \cdots Q_r$ for prime ideals Q_j. The proof is by induction on k.

Base case is $k = 1$. Then $P_1 = I = Q_1 Q_2 \cdots Q_r$. As argued earlier, P_1 equals one of Q_j, say Q_1. Multiplying with inverse of P_1 on both sides, we get $Q_2 \cdots Q_r = (1)$ which is only possible if $Q_2 = \cdots = Q_r = (1)$.

For induction step, assume the uniqueness for products of up to $k-1$ ideals. For $I = P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_r$, we have, as before,

$$P_1 \supseteq I = P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_r.$$

Arguing as before, P_1 must equal one of Q_j, say Q_1. Then, multiplying with inverse of P_1, we get:

$$P_2 \cdots P_k = Q_2 \cdots Q_r.$$

By induction hypothesis, $P_2 \cdots P_k$ has unique factorization and so $r = k$ and each of Q_j equals one of P_i. Since $P_1 = Q_1$, the uniqueness follows. □

Corollary 2.9. *Every fractional ideal in $\mathcal{J}$ can be uniquely written as a product $P_1^{m_1} P_2^{m_2} \cdots P_k^{m_k}$ where P_i are prime ideals of R, $m_i \in \mathbb{Z}$, and P_i^{-1} denotes the inverse of P_i in $\mathcal{J}$.*

Proof. Let $J \in \mathcal{J}$. Then $J = \frac{1}{a}I$. In other words, $I = aJ = (a) \cdot J$. By the above theorem, both I and (a) can be written uniquely as a product of prime ideals.Therefore, J can be written uniquely as a product of prime ideals and their inverses. □