DEDEKIND DOMAINS

KEWEN BU

Abstract. As is known to all, Fermat's Last Theorem has long been one of the most challenging problems. Many mathematicians have tried to prove it. Due to their efforts, many new methods have been developed. Many new branches. Algebraic number theory is the summary of mathematicians' attempsts. When we discuss the solutions of polynomial equations, the unique factorization property of elements is very important. But unfortunately, not all rings are unique factorization domain. We need to generalize the idea of unique factorization domain. This is the reason why we study the unique factorization of ideals. The domain where ideals can be factored uniquely is called Dedekind domian. This paper will discuss some properties about Dedekind domains.

Contents

1. Why do we want to study Dedekind domains?

Dedekind domain is a very important object in algebraic number theory. First of all, I want to talk about something about algebraic number theory. To be honest, algebraic number theory is a "failed theory". Why do I say that algebraic number theory is a "failed theory"? Actually, algebraic number theory is originated from Fermat's Last Theorem. Mathematicians like Dedekind, Krull worked on it because they want to prove Fermat's Last Theorem. In this view, algebraic number theory is similar to Galois theory. Both of them are studied to solve a kind of problems. The difference is that Galois theory succeeded but algebraic number theory failed to prove Fermat's Last Theorem. What's Fermat's Last Theorem? Fermat claimed that when $n > 2$ the equation $x^n + y^n = z^n$ has no integer solutions. Fermat's Last Theorem has long obsessed mathematicians. Mathematicians' first attempt is to use the knowledge of Unique Factorization. Suppose ξ is one of the nth primitive roots of -1. Then the equation $x^n + y^n = z^n$ can be written as $\prod_{i=0}^{n-1}(x - \xi^i y) = z^n$. If the ring $\mathbb{Z}[\xi]$ is a unique factorization domain then we can use the property of unique factorization to get a lot of useful things. However, it's not true that every $\mathbb{Z}[\xi]$ is a unique factorization domain. Due to this, we may not be able to use the property of unique factorization. What Dedekind did was to generalize the idea of unique factorization. For any single element, the prime element factorization of this element might not be unique, but when we consider the prime ideal factorization

Date: DEADLINE APRIl 27, 2020.

of ideals, it might be unique. Many objects in algebraic number theory unique factorization property of ideals. That's where Dedekind domain comes from. In the next section, I will introduce some results in Dedekind domain.

2. What's Dedekind domain?

In this section, we will introduce Dedekind domains and you will see that in Dedekind domains we have the unique factorization of prime ideals. There is a concept, which is connected very closely to Dedekind domain.

Definition 2.1. Discrete valuation ring is a principal ideal domain which has only one nonzero prime ideal.

There are many equivalent definition of discrete valuation ring like: Discrete valuation ring is a principal ideal domain which has only one prime element up to associates. Discrete valuation ring is a principal ideal domain which is local but not a field. An example of discrete valuation ring is $\mathbb{Z}_{(p)} = \{\frac{m}{n} | m, n \in \mathbb{Z}, p \nmid n\}$(This is actually the localization of $\mathbb{Z}$ at (p)). It's easy to see these definitions are equivalent.

Next, we will introduce an important result about discrete valuation ring.

Theorem 2.2. *An integral domain A is a discrete valuation ring iff it's Noetherian, integrally closed and has only one nonzero prime ideal.*

Proof. First of all, from the definition of discrete valuation ring we know that discrete valuation ring is Noetherian, integrally closed and has only one nonzero prime ideal. What we need to show now is that if an integral domain A is Noetherian, integrally closed and has only one nonzero prime ideal then it's a discrete valuation ring. From the definition we know that we only need to show that A is a PID(principal ideal domain). First of all, choose a nonzero element $c \in A$. Denote $A/(c)$ by M. We can choose an $m \in M$ such that $Ann(m)$ is maximal among all ideals like this kind.(This is possible because $Ann(m)$ is an ideal in A and A is Noetherian) Denote m by $b + (c)$, $Ann(m) = Ann(b + (c))$ by $\mathfrak{p}$. We first show that $\mathfrak{p}$ is a prime ideal. For contradiction, suppose there is x and y such that $x, y \in \mathfrak{p}$ but neither x nor y is in $\mathfrak{p}$. Then consider $Ann(xb + (c))$. We know that $\mathfrak{p} \subset Ann(xb + (c))$ and $y \in Ann(xb + (c))$. Then it contradicts the maximality of $Ann(b + (c))$, hence we know that $\mathfrak{p}$ is a prime ideal.

Second, we need to show that $\frac{b}{c} \notin A$ but $\frac{c}{b} \in A$. $\frac{b}{c} \notin A$ is because $b = c\frac{b}{c} \in (c)$ which is a contradiction. Then $\frac{b}{c} \notin A$. Now we will show that $\frac{c}{b} \in A$. We know that $\mathfrak{p}b \subset (c)$, so we have $\mathfrak{p}\frac{b}{c} \subset A$. Since A has only one prime ideal so either $\mathfrak{p}\frac{b}{c} \subset \mathfrak{p}$ or $\mathfrak{p}\frac{b}{c} = A$.(since $\mathfrak{p}\frac{b}{c}$ is an ideal) If $\mathfrak{p}\frac{b}{c} \subset \mathfrak{p}$ then $\frac{b}{c} \in \mathfrak{p}$ from the fact that A is integrally closed. So $\mathfrak{p} = (\frac{b}{c})$. Then we know that the only prime ideal in A is a principal ideal.

Finally, we need to shown that any ideal is principal ideal. Denote $\frac{b}{c}$ by β, then for any given ideal $\mathfrak{a}$ consider the sequence $\mathfrak{a} \subset \mathfrak{a}\beta^{-1} \subset \mathfrak{a}\beta^{-2} \subset ....$ First, this sequence is strictly increasing because if $\mathfrak{a}\beta^{-i} = \mathfrak{a}\beta^{-i-1}$ then β^{-1} is integral over A so contained in A, a contradiction. Then there is a maximal i such that $\mathfrak{a}\beta^{-i} \subset A$ and $\mathfrak{a}\beta^{-i}$ have to be equal to A otherwise it will be contained in $\mathfrak{p}$ but $\mathfrak{p}\beta^{-1} \subset A$, which is a contradiction to the maximality of i, so $\mathfrak{a} = (\beta^i)$.

□

The reason why we introduce discrete valuation domain is because it has strong connections with Dedekind domain.

Definition 2.3. A **Dedekind domain** is an integral domain A which is Noetherian, integrally closed, and every nonzero prime ideal is maximal.

The connection between Dedekind domain and discrete valuation domain is the next result we will introduce:

Proposition 2.4. *A Noetherian integral domain A is a Dedekind domain iff its localization $A_\mathfrak{p}$ is a discrete valuation ring for any nonzero prime ideal $\mathfrak{p} \in A$.*

Proof. $\Rightarrow$ We know that A is Noetherian, so is its localization $A_\mathfrak{p}$. And when we localize A the only prime ideal in $A_\mathfrak{p}$ is $\mathfrak{p}A_\mathfrak{p}$. Next we need to show that $A_\mathfrak{p}$ is integrally closed. To show this, we only need to show that if A is integrally closed, then $S^{-1}A$ is integrally closed. If α integral over $S^{-1}A$, then we have $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for $a_i \in S^{-1}A$ and $i = 1, 2, \cdots, n-1$. We know that there is a $\beta \in S$ such that $\beta a_i \in A$. So consider $\beta^n(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) = 0$, then we have $\overline{\alpha}^n + a'_{n-1}\overline{\alpha}^{n-1} + \cdots + a'_1\overline{\alpha} + a'_0 = 0$ for $\overline{\alpha} = \alpha\beta$ and $a'_i = a_i\beta^{n-i}$. Now we know that $a'_i \in A$ so $\overline{\alpha} \in A$ since A is integrally closed, then we can say that $\alpha \in S^{-1}A$.

$\Leftarrow$ First of all, The localization of A, which is $A_\mathfrak{p}$ is a discrete valuation ring. This means that $\mathfrak{p}$ is a maximal ideal. So we only need to show that A is integrally closed here. For x in the field of fraction of A, if x is integral over A, then it's also integral over $A_\mathfrak{p}$ for any prime ideal $\mathfrak{p}$. Then $x \in A_\mathfrak{p}$ since $A_\mathfrak{p}$ is integrally closed. Now consider $\mathfrak{a}$, which is the set of a such that $ax \in A$. It's easy to see that $\mathfrak{a}$ is an ideal. Next we claim that $\mathfrak{a}$ is not contained in any maximal ideal $\mathfrak{p}$. Since for any $\mathfrak{p}$, $x \in A_\mathfrak{p}$, then there is a $c \in A\backslash\mathfrak{p}$ such that $cx \in A$. So we know that $\mathfrak{a} = A$ so $x \in A$. Now we prove the fact that A is integrally closed.

□

What this proposition can tell us is that if we want to determine whether a Noetherian integral domain is a Dedekind domain, we can try to localize it and determine whether the localization is a discrete valuation ring. What's more, some property can be passed from an integral domain to its localization. That is to say sometimes we can consider the local ring to see whether we get a simplified problem. Sometimes, instead of considering Dedekind domain, we can try to consider discrete valuation ring. It may help us solve our problems.

The next thing I want to introduce is the most important result in the theory of Dedekind domain, the unique factorization of ideals. The result is :

Theorem 2.5. *Let A be a Dedekind domain. Every proper nonzero ideal $\mathfrak{a}$ of A can be written in the form $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ with the ideals $\mathfrak{p}_i$ distinct prime ideals and $r_i > 0$; the $\mathfrak{p}_i$ and r_i are uniquely determined.*

If we want to prove this theorem, we need to prove first the existence of factorization and next the uniqueness of this factorization. To prove the existence of factorization, we need a lemma.

Lemma 2.6. *Let A be a Noetherian ring; then every ideal $\mathfrak{a}$ in A contains a product of nonzero prime ideals.*

Proof. We will prove by contradiction. Suppose not, then consider the set of ideals Σ which don't satisfy the condition. Since A is Noetherian, we know that there is a maximal one in Σ, denote by $\mathfrak{a}$. First of all, $\mathfrak{a}$ itself can't be prime. Then there is $x, y \in A$, such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$. Then we know that $\mathfrak{a} \subset \mathfrak{a} + (x)$

and $\mathfrak{a} \subset \mathfrak{a} + (y)$ but $(\mathfrak{a} + (x))(\mathfrak{a} + (y)) \subseteq \mathfrak{a}$. From the maximality of $\mathfrak{a}$ we know that $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contains a product of nonzero prime ideals which is a contradiction since their product is contained in $\mathfrak{a}$.

□

The proof of the above lemma is very similar to the proof of the Fundamental Theorem of Arithmetic. The above lemma just told us that any ideal in A contains a product of prime ideals but we don't know whether they are equal. Next, we will show that they are equal and the uniqueness of the factorization. We will use the property about localization and the connection between Dedekind domain and discrete valuation ring. First we need some lemmas.

Lemma 2.7. *Let A be a ring, and $\mathfrak{a}, \mathfrak{b}$ two relatively prime ideals in A; then $\mathfrak{a}^m, \mathfrak{b}^n$ are also two relatively prime ideals for all $m, n \in \mathbb{Z}$*

Proof. Since $\mathfrak{a}, \mathfrak{b}$ relatively prime, then we know that there $x \in \mathfrak{a}$, $y \in \mathfrak{b}$ such that $x + y = 1$. Then we know that $(x + y)^{m+n} = 1$. We know that $(x + y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}$. If $i \geq m$ then $x^i \in \mathfrak{a}^m$, otherwise $y^{m+n-i} \in \mathfrak{b}^n$. So we know that every term of $\sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}$ either in $\mathfrak{a}^m$ or in $\mathfrak{b}^n$. Then we know that $(x + y)^{m+n} = 1$ is in $\mathfrak{a}^m + \mathfrak{b}^n$ so $\mathfrak{a}^m, \mathfrak{b}^n$ also two relatively prime ideals. □

Next lemma is very important because it tells us the corresponding of ideals between the integral domain A and its localization $A_\mathfrak{p}$.

Lemma 2.8. *Let $\mathfrak{p}$ be a maximal ideal of an integral domain A, and let $\mathfrak{q}$ be the ideal it generates in $A_\mathfrak{p}$, $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$. The map*

$$a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m : A/\mathfrak{p}^m \to A/\mathfrak{q}^m$$

is an isomorphism for all $m \in \mathbb{N}$.

Proof. We know that the map above is a homomorphism first. So what we need to show is that the map is a bijection.

First we show that this map is injective. To show this map is injective, we just need to show that the kernel of this map is zero. Which is to say, $\mathfrak{q}^m \cap A$ is $\mathfrak{p}^m$. Then choose $x \in \mathfrak{q}^m \cap A$. We know that $\mathfrak{q}^m = S^{-1}\mathfrak{p}^m$ where $S = A - \mathfrak{p}$, so $x \in S^{-1}\mathfrak{p}^m \cap A$. We can write x as $\frac{a}{s}$, where $a \in \mathfrak{p}^m$ and $s \in S$. We know that $sx \in \mathfrak{p}^m$ so 0 in $A/\mathfrak{p}^m$. We know that the only maximal ideal which contains $\mathfrak{p}^m$ in A is $\mathfrak{p}$. This is because if a maximal ideal $\mathfrak{m}$ contains $\mathfrak{p}^m$ then for any $y^m \in \mathfrak{p}^m (y \in \mathfrak{p})$, we have $y^m \in \mathfrak{m}$. From the fact that $\mathfrak{m}$ is a maximal ideal, we know that it's a prime ideal. Then we know that $y \in \mathfrak{m}$, so we know that $\mathfrak{p} \subseteq \mathfrak{m}$, which contradicts the fact that $\mathfrak{p}$ is a nonzero maximal ideal. Since $\mathfrak{p}$ is the only maximal ideal which contains $\mathfrak{p}^m$, we know that $\mathfrak{p}/\mathfrak{p}^m$ is the only nonzero maximal ideal in $A/\mathfrak{p}^m$. So we know that $A/\mathfrak{p}^m$ is a local ring. Since $s \notin \mathfrak{p}$ it's not in $\mathfrak{p}/\mathfrak{p}^m$. From this fact, we can say that s is a unit in $A/\mathfrak{p}^m$. Since $sx = 0$ in $A/\mathfrak{p}^m$ and s is unit in $A/\mathfrak{p}^m$ we know that x is 0 in $A/\mathfrak{p}^m$. So x is in $\mathfrak{p}^m$. Then $S^{-1}\mathfrak{p}^m \cap A \subseteq \mathfrak{p}^m$. What's more, we know that $\mathfrak{p}^m \subseteq S^{-1}\mathfrak{p}^m \cap A$. So we get $\mathfrak{p}^m = S^{-1}\mathfrak{p}^m \cap A$.

Next, we will prove that this map is surjective. To prove this, we need the lemma 2.7. Choose an element $\frac{a}{s} \in A_\mathfrak{p}$, then $s \notin \mathfrak{p}$. Since $\mathfrak{p}$ is a maximal ideal, and $s \notin \mathfrak{p}$, we know that $(s) + \mathfrak{p} = A$. So $(s), \mathfrak{p}$ are relatively prime. From lemma 2.7 we know that $(s), \mathfrak{p}^m$ are also relatively prime. So we know that there is an element $b \in A$ such that $bs + x = 1$ for $x \in \mathfrak{p}^m$. Then b is mapped to $\frac{1}{s}$, and ba is mapped to $\frac{a}{s}$. Then we can say that this map is surjective. □

Now we finished our preparation of proving our main result. Next is the proof of theorem 2.5.

Proof. First of all, we know that the ideal $\mathfrak{a}$ contains a product of prime ideals denote this product by $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$. From Chinese Remainder Theorem we know that $A/\mathfrak{b} \simeq A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_n^{r_n}$. From lemma 2.8 we know that $A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_n^{r_n} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_n}/\mathfrak{q}_n^{r_n}$, where $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ for $i = 1, 2, \cdots, n$. From this isomorphism, we know that $\mathfrak{a}/\mathfrak{b}$ is isomorphic to $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \mathfrak{q}_n^{s_n}/\mathfrak{q}_n^{r_n}$ for $s_i \leq r_i$. We know that image of the ideal $\mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n}$ under this isomorphism is also $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \mathfrak{q}_n^{s_n}/\mathfrak{q}_n^{r_n}$, so we know that $\mathfrak{a} = \mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n}$. The above content is the existence of the factorization. We also need to show that this factorization is unique. If $\mathfrak{a}$ has two different factorization say $\mathfrak{a} = \mathfrak{p}_1^{s_1} \times \cdots \times \mathfrak{p}_n^{s_n} = \mathfrak{p}_1^{t_1} \times \cdots \times \mathfrak{p}_n^{t_n}$(Some s_i, t_i can be zero such that their form is the same). And we have $\mathfrak{p}_i^{s_i} = \mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{t_i}$ so $s_i = t_i$. Then factorization is unique.

□

Now we finished our main results about Dedekind domain. It's easy to see that principal ideal domain is Dedekind domain. But unique factorization doesn't need to be Dedeking domain and Dedekind domain doesn't need to be unique factorization domain. The example that is unique factorization domain but not Dedekind domain-$\mathbb{C}[x_1, x_2, \cdots]$(infinitely many indeterminates). The example that is Dedekind domain but not unique factorization domain is $\mathbb{Z}[\sqrt{-5}]$.

References

[1] James Milne. Algebraic Number Theory. Course Note. 2017.