M3P8 LECTURE NOTES 11: DEDEKIND DOMAINS

1. Dedekind Domains

For number theorists, it is often convenient to work in a ring of the form $\mathbb{Z}[\alpha]$, where $\alpha \in \mathbb{C}$ is an algebraic integer, or more generally in some subring $\mathcal{O}$ of $\mathbb{C}$ that is integral over $\mathbb{Z}$. Unfortunately, unique factorization only rarely holds in such rings. If $\mathcal{O}$ is integrally closed, however, there is a substitute for unique factorization that is often "good enough": unique factorization of ideals. In this section we develop the ideas behind this result, in the more general context of what are called *Dedekind Domains*.

Definition 1.1. An integral domain R is called a *Dedekind Domain* if R is Noetherian and integrally closed, and every nonzero prime ideal of R is maximal.

In particular, any PID is a Dedekind domain- we have seen that every nonzero prime ideal is maximal in a PID, and PIDs are certainly Noetherian. They are integrally closed because any UFD is integrally closed. As another example, the rings $\mathcal{O}_K$, with K a quadratic extension of $\mathbb{Q}$ are integrally closed and generated over $\mathbb{Z}$ by a single element. They are thus Noetherian, and we proved on Example Sheet 2 that every nonzero prime of such a ring is maximal.

More generally, we have:

Theorem 1.2. *Let R be a PID with field of fractions K, and let K' be a finite extension of K. Let R' be the integral closure of R in K'. Then R' is a Dedekind domain.*

We will prove this later in the course, under a mild additional hypothesis on the extension K'/K.

The reason Dedekind domains are interesting to us is that the nonzero ideals in a Dedekind domain factor uniquely as products of prime ideals. The idea to study factorization of ideals into prime ideals comes from the following observation:

Lemma 1.3. *Let $\mathfrak{p}$ be a prime ideal of* any *ring R, let I and J be ideals, and suppose that $\mathfrak{p}$ contains IJ. Then either $\mathfrak{p}$ contains I or $\mathfrak{p}$ contains J.*

Proof. Suppose that $\mathfrak{p}$ does not contains I, and fix an $r \in I$ such that r is not in $\mathfrak{p}$. Then for all $s \in J$, the product rs lies in IJ and hence in $\mathfrak{p}$. Since r does not lie in $\mathfrak{p}$, and $\mathfrak{p}$ is prime, we must have $s \in \mathfrak{p}$. □

Note the resemblance of this to the property "$p|ab$ implies $p|a$ or $p|b$ for p irreducible" which holds in UFDs and implies unique factorization. We

might hope that the above result thus implies "unique factorization into primes" for arbitrary rings, but this is too much to ask for- the problem is that ideal multiplication is usually badly behaved compared to multiplication of elements in integral domains.

For example, let $R = \mathbb{Z}[\sqrt{-3}]$ (not a Dedekind domain, since it fails to be integrally closed). Then the ideal $\mathfrak{p} = \langle 2, 1+\sqrt{-3}\rangle$ is prime, and we have

$$\langle 2, 1+\sqrt{-3}\rangle^2 = \langle 4, 2+2\sqrt{-3}, -2+2\sqrt{-3}\rangle = \langle 4, 2+2\sqrt{-3}\rangle.$$

There is thus a chain of inclusions: $\mathfrak{p}^2 \subsetneq \langle 2\rangle \subsetneq \mathfrak{p}$, so the ideal $\langle 2\rangle$ is *not* a product of prime ideals!

Dedekind domains give precisely the context where this doesn't happen. In order to make this precise, we first define:

Definition 1.4. Let R be an integral domain. A *fractional ideal* of R is a finitely generated nonzero R-submodule of the field of fractions K of R. A *principal* fractional ideal is an R-submodule of K generated by a single nonzero element of K.

For instance, the subgroup of $\mathbb{Q}$ generated by $\frac{3}{5}$ is a principal fractional ideal of $\mathbb{Z}$. (Indeed, every fractional ideal of $\mathbb{Z}$, or any PID, is principal). More generally, let R be an integral domain, and let I be the R-submodule of K generated by $r_1, \ldots, r_n \in K$. Then by definition I is a fractional ideal of R. On the other hand, we can clear denominators: there exists an $r \in R$, nonzero, such that rr_i lies in R for all I. Then rI is an ideal J of R, and $I = \frac{1}{r}J$. Thus the fractional ideals of R are precisely the subsets of K of the form $\frac{1}{r}J$, where r is a nonzero element of R and J is an ideal of R.

Let I and J be fractional ideals of R. The *product* IJ is the R-submodule of K generated by all products of the form $i \in I$, $j \in J$. It is a fractional ideal of R. The multiplication $I, J \mapsto I, J$ is an associative and commutative operation. Note that R is a fractional ideal of R, and $RJ = J$ for any fractional ideal J, so R is an "identity element" for this operation.

For a nonzero ideal I of R, let I^{-1} denote the set $\{r \in K : rI \subseteq R\}$. Then I^{-1} is clearly an R-submodule of K. If $r \in I$ is nonzero, then rI^{-1}, by definition, is contained in R, so I^{-1} is contained in $\frac{1}{r} \cdot R$ and is thus a fractional ideal.

For a prime ideal $\mathfrak{p}$ of R, and n a positive integer, define $\mathfrak{p}^{-n} := (\mathfrak{p}^{-1})^n$. We then have:

Theorem 1.5. *Let R be a Dedekind domain. Then the set of fractional ideals of R form a group under multiplication. Moreover, any fractional ideal I of R factors uniquely as ${\mathfrak{p}_1}^{n_1} \ldots {\mathfrak{p}_s}^{n_s}$, where the n_i are integers and the $\mathfrak{p}_i$ are nonzero prime ideals.*

The proof of this statement will occur in several steps. We first show:

Proposition 1.6. *Let I be a nonzero ideal of a Dedekind domain R. Then there exist nonzero primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and positive integers $n_1, \ldots, n_s$ such that I contains ${\mathfrak{p}_1}^{n_1}{\mathfrak{p}_2}^{n_2} \ldots {\mathfrak{p}_s}^{n_s}$.*

Proof. Note first that if the claim holds for an ideal I then it holds for any ideal containing I, and that if the claim holds for I and J then it holds for $I \cap J$.

Suppose the claim fails for some I. Since R is Noetherian, there exists an I such that the claim fails for I but holds for any ideal containing I. Certainly I can't be prime. So there exist $a, b \in R$ with $ab \in I$ but a and b not in I. Then $I + \langle a \rangle$ and $I + \langle b \rangle$ strictly contain I, so the claim holds for both of these ideals. Then it also holds for their product, but this product is contained in I. Thus the claim holds for I as well and we have a contradiction. □

Next, we show that prime ideals have "multiplicative inverses". To do so we use the following lemma:

Lemma 1.7. *Let R be a Dedekind domain with field of fractions K, and let x be an element of K that is not in R, and let I be any nonzero ideal of R. Then xI is not contained in I.*

Proof. Suppose xI were contained in I. Let $a \in I$, and for each i let M_i be the ideal of I generated by $a, xa, x^2a, \ldots, x^ia$. This is an increasing tower of ideals of R; since R is Noetherian, it is eventually constant; i.e. $M_{i+1} = M_i$ for some i. Then $x^{i+1}a$ can be expressed as an R-linear combination of the x^ja; that is, we have:

$$x^{i+1}a = \sum_{j=0}^{i} r_j x^j a.$$

Since R is an integral domain we can cancel the a: $x^{i+1} = \sum_{j=0}^{i} r_j x^j$. Thus x is *integral* over R. Since R is integrally closed and x does not lie in R this is a contradiction. □

Proposition 1.8. *Let $\mathfrak{p}$ be a nonzero prime ideal of a Dedekind domain R. Then $\mathfrak{p}^{-1}\mathfrak{p} = R$.*

Proof. We first show that there is an element $x \in \mathfrak{p}^{-1}$ such that $x \notin R$. Let a be an element of $\mathfrak{p}$, so that we have $\langle a \rangle \subset \mathfrak{p}$. Choose a minimal set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq \langle a \rangle.$$

Then we have in particular:

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subseteq \mathfrak{p},$$

so by the lemma above we must have $\mathfrak{p} = \mathfrak{p}_i$ for some i; WLOG we can take $i = 1$. Then by our minimality assumption $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ is not contained in $\langle a \rangle$. Take b to be an element of $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ that is *not* in $\langle a \rangle$. Then $x = \frac{b}{a}$ is not in R. On the other hand for any $y \in \mathfrak{p}$, $xy = \frac{by}{a}$, and by lies in $\mathfrak{p}_1 \ldots \mathfrak{p}_r$ and hence in $\langle a \rangle$. Thus xy lies in R. By definition, this means x lies in $\mathfrak{p}^{-1}$ but not in R.

Now consider $\mathfrak{p}^{-1}\mathfrak{p}$. By definition this is contained in R; since $1 \in \mathfrak{p}^{-1}$ it contains $\mathfrak{p}$. Since $\mathfrak{p}$ is a nonzero prime ideal it is maximal, so we must have either $\mathfrak{p}\mathfrak{p}^{-1} = R$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Suppose the latter holds. Then in particular multiplication by x sends $\mathfrak{p}$ to $\mathfrak{p}$. This contradicts the lemma above. □

Proposition 1.9. *Let I be a nonzero ideal of a Dedekind domain R. Then there exists a fractional ideal J of R such that $IJ = R$.*

Proof. Suppose otherwise. Then there is a maximal nonzero ideal I of R for which no such J exists. The previous proposition shows that I is not a maximal ideal, so I is properly contained in some maximal ideal $\mathfrak{p}$ of R. Then $\mathfrak{p}^{-1}$ is contained in I^{-1}. We thus have inclusions:

$$I \subseteq I\mathfrak{p}^{-1} \subseteq II^{-1} \subseteq R.$$

Suppose that $I\mathfrak{p}^{-1} = I$. By the previous proposition there exists $x \in \mathfrak{p}^{-1}$ not in R, so we would have $xI \subset I$ contradicting the lemma above. Thus $I\mathfrak{p}^{-1}$ strictly contains I and thus has an inverse J'. But then $J'\mathfrak{p}$ is an inverse for I. □

Theorem 1.10. *Let R be a Dedekind domain. Then the fractional ideals of R form a group under multiplication.*

Proof. We must show that every fractional ideal of R is invertible. Let I be such a fractional ideal; then there is $r \in R$ such that rI is an ideal of R. The preceding proposition shows that rI has a multiplicative inverse J; then $r^{-1}J$ is a multiplicative inverse for I. □

It remains to show that every fractional ideal of R factors uniquely as a product of prime powers. The hard part is showing such factorizations exist, and we make heavy use of the fact that the fractional ideals are a group. Uniqueness is then almost an afterthought:

Proposition 1.11. *Every fractional ideal in a Dedekind domain is uniquely a product of (possibly negative) prime powers.*

Proof. We first show that every nonzero ideal I in R is a product of (non-negative) prime powers. Suppose otherwise. Then there is a largest ideal I that is not; since every maximal ideal of R is certainly such a product I cannot be a maximal ideal; thus I is properly contained in a maximal ideal $\mathfrak{p}$. Then $J = \mathfrak{p}^{-1}I$ is an ideal of R; since the fractional ideals of R form a group this ideal strictly contains I and thus factors as a product of prime powers. But then $\mathfrak{p}J = I$ is also a product of prime powers, contradicting our assumption.

Now suppose that I is a fractional ideal. Then $I = r^{-1}J$ for some nonzero ideal J of R and some nonzero element r of R. Since $\langle r \rangle$ and J factor as products of prime powers, so does I.

It remains to show that such factorizations are unique. Suppose otherwise. Then we have a finite collection of distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and two

sequences of integers $n_1, \dots, n_r, m_1, \dots, m_r$ such that

$$\mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\dots\mathfrak{p}_r^{n_r} = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\dots\mathfrak{p}_r^{m_r}$$

and we must show that $m_i = n_i$ for all i. Suppose this is not the case. We can make all prime powers involved positive by cancelling $\mathfrak{p}_i^{\min(m_i,n_i)}$ from both sides of the equation. We then get an expression of the form:

$$\mathfrak{q}_1^{a_1}\dots\mathfrak{q}_s^{a_s} = \mathfrak{t}_1^{b_1}\dots\mathfrak{t}_u^{b_u}$$

where the primes $\mathfrak{q}_i, \mathfrak{t}_j$ are all distinct and all powers a_i, b_j are positive. But since $\mathfrak{q}_1$ divides the left hand side it also divides the right hand side, and thus must be equal to one of the $\mathfrak{t}_j$'s, which is impossible. □

2. Ideal class groups

Let R be a Dedekind domain. Then the fractional ideals of R form a group, which we will denote $\mathcal{I}(R)$. The principal fractional ideals are a subset of $\mathcal{I}(R)$ that is easily seen to be closed under multiplication and inverses: if $r, s \in K^\times$, then $(rR)^{-1} = r^{-1}R$ and $(rR)(sR) = rsR$. Denote this subgroup by $\mathcal{P}(R)$. We can then form the *quotient* $\mathcal{A}(R) = \mathcal{I}(R)/\mathcal{P}(R)$; this group is called the *ideal class group* of R. It is a measure of the failure of fractional ideals of R to be principal; that is, it measures the failure of R to be a principal ideal domain.

We will show that if K is a finite extension of $\mathbb{Q}$ then the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is a Dedekind domain. A fundamental result of algebraic number theory (which we won't prove!) is:

Theorem 2.1. *The ideal class group $\mathcal{A}(\mathcal{O}_K)$ is a* finite *group.*

The order of the ideal class group of $\mathcal{O}_K$ is called the *class number* of K; the study of class groups and class numbers is a central part of modern number theory and there are many, many open questions.