4/12, 4/15: Dedekind domains, unique factorization of ideals, and the class group

So far, we have developed the notion of integrality, as well that of traces and norms to study integral elements. Say \( K/\mathbb{Q} \) is a finite extension and we would like to study algebraic integers in \( K \):

**Definition 5.1.** Let \( K/\mathbb{Q} \) be a finite extension. We call such \( K \) a **number field**. The subring of algebraic integers in \( K \) is the integral closure of \( \mathbb{Z} \) in \( K \). We denote the subring by \( \mathcal{O}_K \).

For example, when \( K = \mathbb{Q}(i) \) we have \( \mathcal{O}_K = \mathbb{Z}[i] \). By definition \( \mathcal{O}_K \) is integrally closed. To further work with \( \mathcal{O}_K \), we would like \( \mathcal{O}_K \) to be finitely generated over \( \mathbb{Z} \) (as a ring) and thus Noetherian. For \( \mathbb{Z}[i] \) this is obvious. How do we prove this in general? The closest thing we have is probably a basis of \( K \) as a vector space over \( \mathbb{Q} \). We want to turn those into something in \( \mathcal{O}_K \):

**Lemma 5.2.** For any \( \alpha \in K \), there exists \( c \in \mathbb{Z} - \{0\} \) such that \( c\alpha \in \mathcal{O}_K \).

**Proof.** We have \( \alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + ... + c_n = 0 \) for some \( c_1, ..., c_n \in \mathbb{Q} \). This implies that for any \( c \) we have \( (c\alpha)^n + cc_1(c\alpha)^{n-1} + c^2c_2(c\alpha)^{n-2} + ... + c^n c_n \). By choosing \( c \) to be divisible by all denominators of \( c_1, ..., c_n \) we have \( c\alpha \) integral over \( \mathbb{Z} \).

In other words, given any basis \( \alpha_1, ..., \alpha_m \in K \) as a \( \mathbb{Q} \)-module (i.e. vector space), multiplying each \( \alpha_i \) by some integer we can assume \( \alpha_i \in \mathcal{O}_K \). Can we hope, then, that \( \mathcal{O}_K \) is generated by these \( \alpha_i \) as a \( \mathbb{Z} \)-module? For example, \( 2 \) and \( 3i \) generates \( \mathbb{Q}(i) \) as a \( \mathbb{Q} \)-module, and they don’t generate \( \mathbb{Z}[i] \) as a \( \mathbb{Z} \)-module. But it’s not too far from it: \( \mathbb{Z}[i]/(2, 3i) \mathbb{Z} \) has order 6, i.e. \( (2, 3i) \mathbb{Z} \) is an index 6 subgroup in \( \mathbb{Z}[i] \), as a \( \mathbb{Z} \)-module or abelian group. Our goal in this section is to prove that this is a general phenomenon:

**Proposition 5.3.** Let \( \alpha_1, ..., \alpha_m \in \mathcal{O}_K \) be such that they generate \( K \) as a \( \mathbb{Q} \)-module. Then \( (\alpha_1, ..., \alpha_m)_\mathbb{Z} \subset \mathcal{O}_K \) has finite index.

**Corollary 5.4.** The ring \( \mathcal{O}_K \) is finite over \( \mathbb{Z} \), and is in particular Noetherian.

**Proof.** With the proposition we have \( \mathcal{O}_K/(\alpha_1, ..., \alpha_m)_\mathbb{Z} \) finite and thus has a finite of generators. Take some representatives of such generators. Together with \( \alpha_1, ..., \alpha_m \) they generate \( \mathcal{O}_K \) as a \( \mathbb{Z} \)-module. This implies that they generate \( \mathcal{O}_K \) as a ring. Since \( \mathbb{Z} \) is a PID and therefore Noetherian, \( \mathcal{O}_K \) is also Noetherian by P3(b) in Problem Set 1.

**Corollary 5.5.** Every non-zero prime ideal of \( \mathcal{O}_K \) is maximal.
Proof. Let $I \subset \mathcal{O}_K$ be a non-zero ideal. Let $a \in I$ be arbitrary. Let $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$ be a basis of $K$ over $\mathbb{Q}$; we have seen such exist. Then $a\alpha_1, \ldots, a\alpha_m \in I$ is still a basis of $K$ over $\mathbb{Q}$. For if $c_1 a\alpha_1 + \ldots + c_m a\alpha_m = 0$ then $c_1 \alpha_1 + \ldots + c_m \alpha_m = 0$. But then $(a\alpha_1, \ldots, a\alpha_m)_\mathbb{Z} \subset I$ and by Proposition 5.3 we have $\mathcal{O}_K/(a\alpha_1, \ldots, a\alpha_m)_\mathbb{Z}$ finite. Hence $\mathcal{O}_K/I$ is finite.

Now when $I$ is a prime ideal, $\mathcal{O}_K/I$ is a finite domain. A finite domain is always a field, which implies that $I$ is in fact maximal. We remark that this also gives another proof that $\mathcal{O}_K$ is Noetherian; if $\mathcal{O}/I$ is already finite, $I$ can’t increasing infinitely many times. 

**Definition 5.6.** A Dedekind domain is a domain $D$ which is Noetherian, integrally closed, and such that every non-zero prime ideal in $D$ is maximal.

This is the kind of “best domain” we would like to work with. For example, we have seen that a PID is a Dedekind domain. Indeed, we have seen that a PID is Noetherian and integrally closed (UFD are integrally closed). Every non-zero prime ideal of a PID is generated by an irreducible element, which then generates a maximal ideal. Now the following is a combination of Corollary 5.4 and 5.5:

**Corollary 5.7.** For every number field $K$, the ring of integers $\mathcal{O}_K$ in it is a Dedekind domain. Moreover, $\mathcal{O}_K$ is a free abelian group generated by $[K : \mathbb{Q}]$ generators.

Proof. It suffices to prove the last statement. We note that $\mathcal{O}_K$ is a finitely generated abelian group. In group theory we learn that any finitely generated abelian group, in particular $\mathcal{O}_K$, is isomorphic to $\mathbb{Z}^r \times C$ where $C$ is some finite abelian group. We claim that $C$ is trivial. If not, then for some non-trivial $c \in C$ we have $|C|c = 0$, which never happen in $\mathcal{O}_K \subset K$, a field of characteristic zero. So $\mathcal{O}_K$ is a free abelian group generated by some $r$ elements. By Lemma 5.2 these $r$ elements also generates $K$ as a vector space over $\mathbb{Q}$. Moreover, it is a basis because if $c_1 \alpha_1 + \ldots + c_r \alpha_r = 0$ for some $c_i \in \mathbb{Q}$, then we can always clear the denominator so that all $c_i \in \mathbb{Z}$. This proves $r = [K : \mathbb{Q}]$. 

Now we get back to Dedekind domains. The big theorem is

**Theorem 5.8.** Let $D$ be a Dedekind domain and $I \subset D$ any non-zero proper ideal. Then $I$ can be uniquely written as $I = p_1 \ldots p_k$ a product of non-zero prime ideals.

Let us recall a bit about product of ideals. For any ideals $I_1, I_2 \in R$ in a ring $R$, we define $I_1 I_2$ to be the ideal $(xy \mid x \in I_1, y \in I_2)$. The first step for Theorem 5.8 is

**Lemma 5.9.** Let $R$ be a Noetherian ring, then every non-zero proper ideal $I$ of $R$ contains a product of non-zero prime ideals.
Proof. If \( I \) is a prime ideal then we are done. Otherwise, \( I \) is not prime and there exists \( x, y \notin I \) such that \( xy \in I \). This implies that \( I \supseteq (I + (x)) \cdot (I + (y)) \). Note that neither \( I + (x) \) nor \( I + (y) \) can be the whole ring \( R \), for if \( I + (x) = R \) we have \( I \supseteq I + (y) \supseteq y \), a contradiction. By axiom of dependent choice, if either \( I + (x) \) or \( I + (y) \) is not a prime ideal we can keep factoring it until we get \( I \supseteq p_1 p_2 \ldots p_k \), or this never stops and we have an ascending chain (strictly increasing sequence) of ideals, which contradicts with that \( R \) is Noetherian.

Now use now generalize the notion of ideals and their products a bit.

**Definition 5.10.** Let \( D \) be a Dedekind domain. A fractional ideal of \( D \) is a non-zero finitely generated sub-\( D \)-module \( I \) of \( \text{Frac}(D) \) (when it’s a submodule of \( D \), it will be an ideal). For any two fractional ideals \( I_1, I_2 \) we again define \( I_1 I_2 := (xy \mid x \in I_1, y \in I_2)_D \) to be the submodule of \( \text{Frac}(D) \) generated by such \( xy \).

We note that the product of two fractional ideals is indeed still finitely generated, for if \( I_1 = (x_1, \ldots, x_s)_D \) and \( I_2 = (y_1, \ldots, y_t)_D \) we have \( I_1 I_2 = (x_1 y_1, \ldots, x_s y_t) \) for \( 1 \leq i \leq s, 1 \leq j \leq t \).

**Proposition 5.11.** Let \( D \) be a Dedekind domain and \( p \subset D \) be a non-zero prime ideal (i.e. maximal). Then 

\[
p^{-1} := \{ x \in \text{Frac}(D) \mid xy \in D, \forall y \in p \}
\]

is a fractional ideal, and \( pp^{-1} = D \).

**Proof.** Pick any non-zero \( a \in p \) so that \( p \supseteq (a) \). It is easy to check that \( p^{-1} \) is a \( D \)-module, and we have that \( p^{-1} \subset (a^{-1}) \), for \( x \in p^{-1} \implies xa \in D \implies x \in (a^{-1}) \). As a module, \( p^{-1} \) is isomorphic to \( (a)p^{-1} \subset D \). Since \( D \) is Noetherian, \( (a)p^{-1} \) is finitely generated and so is \( p^{-1} \). Hence \( p^{-1} \) is a fractional ideal.

By Lemma 5.9 we may write \( (a) \supseteq p_1 p_2 \ldots p_k \) for some non-zero prime ideals \( p_1, \ldots, p_k \), and we may assume that they are chosen so that \( k \) is minimal. We claim that \( p \) is equal to one of the \( p_i \)'s. Indeed if otherwise we can pick \( x_i \in p_i - p \) (as \( p_i \) are maximal) which gives \( \prod x_i \in p_1 p_2 \ldots p_k \) but \( \prod x_i \notin p \), a contradiction. Without loss of generality we may assume \( p = p_1 \).

In the spirit of Theorem 5.8 we expect \( (a) = pp_2 \ldots p_k \implies p^{-1} = (a^{-1})p_2 \ldots p_k \). Note that by the minimality of \( k \) we have \( (a) \not\supset p_2 \ldots p_k \). Pick \( b \in p_2 \ldots p_k \) with \( b \notin (a) \). We have that \( b/a \in p^{-1} \); indeed for any \( y \in p \) we have \( by \in pp_2 \ldots p_k \subset (a) \implies by/a \in D \). On the other hand \( b \notin (a) \implies b/a \notin D \). So we have at least proved that \( p^{-1} \supsetneq D \) (by definition \( p^{-1} \supseteq D \)).

Also from definition we have \( p \subset pp^{-1} \subset D \). Suppose on the contrary that \( pp^{-1} \neq D \). As \( p \) is maximal, we have \( p = pp^{-1} \). So we have some \( x \in p^{-1} \) (as \( b/a \) above) such that \( xy \in p \) for all \( y \in p \), yet \( x \notin D \). We will derive a contradiction by showing that \( x \) is integral over \( D \).
that the other side must also be canceled out, so doing this and eventually one side is completely canceled out (to be up to permutation.

In other words, \( x \) satisfies a monic polynomial with coefficients in \( D \); \( x \in D \). This gives us the desired contradiction and thus \( pp^{-1} = D \). \qed

Let us record the trick:

**Lemma 5.12.** If \( x \in \text{Frac}(D) \) is such that there exists a fractional ideal \( I \) such that \( xI \subset I \). Then \( x \in D \).

**Proof of Theorem 5.8.** We first prove that a factorization exists. Let \( I \subset D \) be a non-zero proper ideal. Take some \( p_1 \supset I \) that is maximal. Then \( I = p_1 p_1^{-1} I \). Since \( p_1 \supset I \), one checks by definition that \( I_1 := p_1^{-1} I \subset D \) is still an ideal, and we have \( I = p_1 I_1 \). We claim that \( I \nsubseteq I_1 \). If otherwise \( I = I_1 \), multiplying by \( p_1^{-1} \) gives \( p_1^{-1} I = I \). We have seen that there exists \( x \in p_1^{-1} \) that is not in \( D \), and \( p_1^{-1} I = I \implies xI = I \). But Lemma 5.12 says \( x \in D \), a contradiction! Hence \( I \nsubseteq I_1 \). If \( I_1 = D \), then \( I = p_1 D = p_1 \) and we are done. Otherwise we can continue to write \( I_1 = p_2 I_2, \ldots \). Since \( D \) is Noetherian, this process must stop and some \( I_k = D \). But this means \( I = p_1 p_2 \ldots p_k \). This proves the existence.

Now suppose \( p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell \) with all \( p_i, q_j \) non-zero prime (i.e. maximal) ideals. We claim that \( p_1 \) must be equal to one of the \( q_j \). Indeed, if not, then since all \( q_j \) are maximal, we can find \( y_j \in q_j \) with \( y_j \notin p_1 \). But then \( y_1 \ldots y_\ell \in p_1 p_2 \ldots p_k \subset p_1 \), a contradiction! Hence we may assume \( p_1 = q_1 \). Multiplying both side by \( p_1^{-1} \) we get \( p_2 \ldots p_k = q_2 \ldots q_\ell \). We keep doing this and eventually one side is completely canceled out (to be \( D \)), which will imply that the other side must also be canceled out, so \( k = \ell \) and the prime ideals are the same up to permutation. \qed

**Corollary 5.13.** The set of non-zero fractional ideals form an abelian group (under ideal multiplication).

**Proof.** We have a multiplication which is obviously commutative and associative. It remains to prove that every fractional ideal has an inverse. Let \( I = (b_1/a_1, b_2/a_2, \ldots, b_s/a_s)_D \) be a non-zero fractional ideal. Let \( a = a_1 a_2 \ldots a_s \). Then \( a I = (b_1 a_2 \ldots a_s, \ldots)_D \) is an ideal. By Theorem 5.8 we write \( a I = p_1 \ldots p_k \), or \( I = a^{-1} p_1 \ldots p_k \). We then have \( I^{-1} = a p^{-1} \ldots p^{-k} \) is an inverse. \qed
Definition 5.14. The ideal group $\text{Div}(D)$ for a number field is the group of non-zero fractional ideals of $D$. It has a subgroup $\text{pDiv}(D)$ called the principal ideal group, generated by fractional ideals of the form $(a)_D$, $a \neq 0$. The (ideal) class group of $D$ is $\text{Cl}(D) := \text{Div}(D)/\text{pDiv}(D)$.

Definition 5.15. The (ideal) class group of a number field $K$ is $\text{Cl}(K) := \text{Cl}(\mathcal{O}_K)$.

Our next big goal is to show that the class group $\text{Cl}(K)$ is finite, and give some method to compute it.