Math 361 lecture for Friday, Week 7

Fractional ideals

In the following, let K be a number field with ring of integers $\mathfrak{O}_K$.

We have seen that addition and multiplication of ideals have nice properties: commutativity, distributivity, there is an additive identity, (0), and a multiplicative identity, (1). However, nonzero ideals do not necessarily have multiplicative inverses. To fix that in the case of number rings, we introduce fractional ideals.

Definition 1. An $\mathfrak{O}_K$-submodule $I \subseteq K$ is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Remark 2.

1. Let I be a fractional ideal of $\mathfrak{O}_K$, and say $\alpha \in \mathfrak{O}_K \setminus \{0\}$ is such that $\mathfrak{a} := \alpha I \subseteq \mathfrak{O}_K$. Then $\mathfrak{a}$ is an ideal of $\mathfrak{O}_K$ (reason: I an $\mathfrak{O}_K$-submodule implies αI an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$, i.e., an ideal).
2. The fractional ideals are exactly the $\mathfrak{O}_K$-submodules of K of the form $\alpha^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ and nonzero $\alpha \in \mathfrak{O}_K$.
3. If I is an $\mathfrak{O}_K$-submodule, then I is a fractional ideal if and only if there exists some $c \in K \setminus \{0\}$ such that $cI \subseteq \mathfrak{O}_K$. (In the definition, c is required to be in $\mathfrak{O}_K$.) Suppose such a c exists. Then since K is the quotient field of $\mathfrak{O}_K$, there exists $\alpha, \beta \in \mathfrak{O}_K$ such that $c = \alpha/\beta$. Then
$$\alpha I = (c\beta)I \subseteq cI \subseteq \mathfrak{O}_K.$$

Example 3. In the rational integers $\mathbb{Z}$, the fractional ideals have the form

$$r\mathbb{Z} = \{ra : a \in \mathbb{Z}\}.$$

For instance, the set of all integer multiples of $2/3$ is a fractional ideal of $\mathbb{Z}$. In general, if $\mathfrak{O}_K$ is a PID, then every fractional ideal has the form $c\mathfrak{O}_K$ for some $c \in K$.

Proposition 4. Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of K.

Proof. First, suppose that I is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then αI is an ideal of the Noetherian ring $\mathfrak{O}_K$. Hence, αI is finitely generated as an $\mathfrak{O}_K$-module. We have an isomorphism of $\mathfrak{O}_K$-modules:

$$I \to \alpha I$$
$$x \mapsto \alpha x.$$

Hence, I is a finitely generated as an $\mathfrak{O}_K$-module (just multiply the generators of αI by α^{-1} to get generators for I).

Conversely, suppose that $I = \mathrm{Span}_{\mathfrak{O}_K}\{x_1, \ldots, x_m\}$ is a finitely-generated $\mathfrak{O}_K$-submodule of K. Since K is the quotient field of $\mathfrak{O}_K$, we can write $x_i = \alpha_i/\beta_i$ with $\beta_i \neq 0$ for all i. Define $\alpha = \prod_{i=1}^m \beta_i$. Then $\alpha I \subseteq \mathfrak{O}_K$. So I^{-1} is finitely generated. □

Proposition 5. The set of nonzero fractional ideals in a number field K forms an abelian group under multiplication. If I is a nonzero fractional ideal of $\mathfrak{O}_K$, then its inverse is

$$I^{-1} = \{x \in K : xI \subseteq \mathfrak{O}_K\}.$$

Proof. Let I and J be fractional ideals. Say $I = c\mathfrak{a}$ and $J = d\mathfrak{b}$ for some ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathfrak{O}_K$ and some nonzero elements $c, d \in \mathfrak{O}_K$. Then

$$IJ = (c\mathfrak{a})(d\mathfrak{b}) = (cd)\mathfrak{a}\mathfrak{b}$$

is fractional ideal since $cd \in \mathfrak{O}_K \setminus \{0\}$ and $\mathfrak{a}\mathfrak{b}$ is an ideal of $\mathfrak{O}_K$. Hence, the set of fractional ideals is closed under multiplication. Multiplication is clearly associative, and there is an identity element, the principal ideal (1). We prove that nonzero fractional ideals have inverses as stated as part of the next theorem. □

Definition 6. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if there exists an ideal H such that $J = IH$.

Proposition 7. (*To contain is to divide.*) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$. Then $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Proof. ($\Rightarrow$) Suppose that $\mathfrak{a}|\mathfrak{b}$, and take $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. The result follows since $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$.

($\Leftarrow$) Now suppose that $\mathfrak{b} \subseteq \mathfrak{a}$. If $\mathfrak{a} = 0$, the result is trivial. So suppose $\mathfrak{a} \neq 0$. We then have

$$\mathfrak{b} \subseteq \mathfrak{a} \quad \Rightarrow \quad \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{O}_K.$$

Define $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$. Then $\mathfrak{c}$ is a fractional ideal contained in $\mathfrak{O}_K$, so $\mathfrak{c}$ is an ideal. Further, $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$, as required. □

Theorem 8. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Proof. We follow our text, breaking down the proof to several steps.

Step 1. Claim: Let $\mathfrak{a} \neq 0$ be an ideal of $\mathfrak{O}_K$. Then there there exists nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Proof of claim. Let $\mathcal{A}$ be the set of all nonzero ideals that do not have the desired property. We would like to show that $\mathcal{A}$ is empty. For the sake of contradiction, suppose it is not.

Then since $\mathfrak{O}_K$ is Noetherian, $\mathcal{A}$ has a maximal element $\mathfrak{a}$. Since $\mathfrak{a}$ does not have the desired property, it cannot be prime. So there exist $\beta, \gamma \in \mathfrak{O}_K$ such that $\beta\gamma \in \mathfrak{a}$, yet $\beta \notin \mathfrak{a}$ and $\gamma \notin \mathfrak{a}$. We have

$$\mathfrak{a} \subsetneq \mathfrak{a} + (\beta) \quad \text{and} \quad \mathfrak{a} \subsetneq \mathfrak{a} + (\gamma).$$

By maximality of $\mathfrak{a}$, the ideals $\mathfrak{a} + (\beta)$ and $\mathfrak{a} + (\gamma)$ are not in $\mathcal{A}$. Hence, there exist prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ such that

$$\prod_{i=1}^{k} \mathfrak{p}_i \subseteq \mathfrak{a} + (\beta) \quad \text{and} \quad \prod_{i=j}^{\ell} \mathfrak{q}_i \subseteq \mathfrak{a} + (\gamma).$$

It follows that

$$\left(\prod_{i=1}^{k} \mathfrak{p}_i\right)\left(\prod_{i=j}^{\ell} \mathfrak{q}_i\right) \subseteq (\mathfrak{a} + (\beta))\,(\mathfrak{a} + (\gamma)) \subseteq \mathfrak{a} + (\beta\gamma) \subseteq \mathfrak{a},$$

which yields that contradiction that $\mathfrak{a} \notin \mathcal{A}$.

Step 2. Given a nonzero fractional ideal I, define

$$I^{-1} := \{x \in K : xI \subseteq \mathfrak{O}_K\}.$$

Since I is a fractional ideal, there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Hence, $\alpha \in I^{-1}$. So $I^{-1} \neq \emptyset$ (and $I^{-1} \neq 0$). It is straightforward to check that I^{-1} is an $\mathfrak{O}_K$-submodule. Letting $y \in I \neq 0$, we have $y \in K \setminus \{0\}$ and $yI^{-1} \subseteq \mathfrak{O}_K$ (recall that it suffices to find such an element in K, not necessarily in $\mathfrak{O}_K$). Hence, I^{-1} is a fractional ideal.

Claim: I^{-1} is the multiplicative inverse of I, i.e., $II^{-1} = (1) = \mathfrak{O}_K$. We now prove this in several steps.

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof of claim. Since $\mathfrak{a}$ is an ideal, it is clear from the definition of $\mathfrak{a}^{-1}$ that $\mathfrak{O}_K \subseteq \mathfrak{a}^{-1}$. Let $\mathcal{A}$ now be the set of proper ideals of $\mathfrak{O}_K$. Since $\mathfrak{O}_K$ is a Noetherian ring and $\mathcal{A} \neq \emptyset$, it follows that $\mathcal{A}$ has a maximal element $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, it is prime.

Since $\mathfrak{a} \subseteq \mathfrak{p}$, it follows that $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$. So it suffices to show that $\mathfrak{p}^{-1} \neq \mathfrak{O}_K$. In other words, we must show that $\mathfrak{p}^{-1}$ contains an element that is not integral over $\mathbb{Z}$. Pick $0 \neq \alpha \in \mathfrak{p}$. Using Step 1, we may pick a minimal r such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}$$

for some nonzero prime ideals $\mathfrak{p}_i$. Since $\mathfrak{p}$ is prime $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i (this follows from a homework problem). Without loss of generality, say $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Since $\mathfrak{O}_K$ is Dedekind, nonzero primes are maximal. Hence, $\mathfrak{p}_1 = \mathfrak{p}$. By minimality of r, $\mathfrak{p}_2 \cdots \mathfrak{p}_r$ is not contained in (α). Take $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \{(\alpha)\}$. Our goal is to show that $\alpha^{-1}\beta \in \mathfrak{p}^{-1}$ but $\alpha^{-1}\beta \notin \mathfrak{O}_K$. We have

$$\beta\mathfrak{p} = \beta\mathfrak{p}_1 \subseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (\alpha).$$

So $\alpha^{-1}\beta\mathfrak{p} \subseteq \alpha^{-1}(\alpha) = (1) = \mathfrak{O}_K$, and thus $\alpha^{-1}\beta \in \mathfrak{p}^{-1}$. However, $\beta \notin (\alpha) = \alpha\mathfrak{O}_K$. So $\alpha^{-1}\beta \notin \mathfrak{O}_K$.

Step 2.2. Claim: if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Proof of claim. Let $\theta \in S$. To show $\theta \in \mathfrak{O}_K$, we must show that θ is integral over $\mathbb{Z}$. For that, it suffices to find a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\theta M \subseteq M$ (recall the determinant trick). We know that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module (since is finitely generated as a module over the Noetherian ring $\mathbb{Z}$). The ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is thus not only finitely generated as an ideal (i.e., as an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$), it is finitely generated as a $\mathbb{Z}$-module. So we can let $M = \mathfrak{a}$.

Step 2.3 Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$. Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof of claim. From the definition of $\mathfrak{p}^{-1}$, it immediately follows that $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$. Since $\mathfrak{p}\mathfrak{p}^{-1}$ is a product of fractional ideals, it is a fractional ideal. Hence $\mathfrak{p}\mathfrak{p}^{-1}$ is an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$, i.e., an ideal. Since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1}$ is either $\mathfrak{p}$ or $\mathfrak{O}_K$. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, then Step 2.2 implies that $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, in contradiction to Step 2.1. Hence, $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}_K$, as claimed.

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof of claim. If not, since $\mathfrak{O}_K$ is a Noetherian ring, we can choose an ideal $\mathfrak{a}$ that is maximal with respect to the property that $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{O}_K$. We can then choose a maximal ideal $\mathfrak{p}$ such that $\mathfrak{a} \subset \mathfrak{p} \subsetneq \mathfrak{O}_K$. Hence, $\mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$. Multiplying this string of subset inclusions through by $\mathfrak{a}$,

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K.$$

Since $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, it is an ideal. It cannot be that $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ since, otherwise, $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$ by Step 2.2, contradicting Step 2.1. Therefore $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. By maximality of $\mathfrak{a}$, we have

$$(\mathfrak{a}\mathfrak{p}^{-1})(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}_K.$$

It then follows from the definition of $\mathfrak{a}^{-1}$ that

$$\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1},$$

but then

$$\mathfrak{O}_K = \mathfrak{a}\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K.$$

This forces $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}_K$, contradicting our choice of $\mathfrak{a}$.

Step 2.5. If I is a nonzero fractional ideal, then $II^{-1} = \mathfrak{O}_K$.

Proof of claim. Suppose I is a nonzero fractional ideal. Pick $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. By Step 2.4, we have $(\alpha I)(\alpha I)^{-1} = \mathfrak{O}_K$. We have

$$(\alpha I)^{-1} = \{x \in K : x(\alpha I) \subseteq \mathfrak{O}_K\}.$$

So $x \in (\alpha I)^{-1}$ if and only if $\alpha x \in I^{-1}$. Therefore, $(\alpha I)^{-1} = (1/\alpha)I^{-1}$. We have

$$\mathfrak{O}_K = (\alpha I)(\alpha I)^{-1} = (\alpha I)\left(\frac{1}{\alpha}I^{-1}\right) = II^{-1}.$$

Step 3. Claim: Every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is a product of prime ideals.

Proof of claim. If not, since $\mathfrak{O}_K$ is Noetherian, we can take an ideal $\mathfrak{a}$ maximal with respect to the property of not having a prime factorization. In particular, $\mathfrak{a}$ is not prime. It is also the case that $\mathfrak{a} \neq \mathfrak{O}_K = (1)$. That's because $\mathfrak{O}_K$ does have a prime factorization—the empty factorization. (This is just like the case of ordinary prime factorization in $\mathbb{Z}$: every nonzero integer has a prime factorization, including ± 1.) Pick a maximal ideal $\mathfrak{p}$ containing $\mathfrak{a}$. In Step 2.4, we showed that

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}.$$

By maximality of $\mathfrak{a}$, the ideal $\mathfrak{a}\mathfrak{p}^{-1}$ has a prime factorization. So

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

for some primes $\mathfrak{p}_i$. Multiplying through by $\mathfrak{p}$, we get

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

That contradicts the fact that $\mathfrak{a}$ does not factor into primes. The result follows.

Step 4. Claim: prime factorization of ideals in $\mathfrak{O}_K$ is unique.

Proof of claim. Suppose that there are nonzero prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Since $\mathfrak{p}_1$ divides $\mathfrak{q}_1 \cdots \mathfrak{q}_s$ and $\mathfrak{p}_1$ is prime, it follows that divides some $\mathfrak{q}_i$. Without loss of generality, say $\mathfrak{p}_1 | \mathfrak{q}_1$. Therefore, $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since $\mathfrak{q}_1$ is a nonzero prime ideal in $\mathfrak{O}_K$, it is maximal. Therefore $\mathfrak{p}_1 = \mathfrak{q}_1$. By induction, $r = s$ and the set of $\mathfrak{p}_i$s equals the set of $\mathfrak{q}_j$s. □