Math 361 lecture for Wednesday, Week 7

Dedekind domains

Field of fractions of a domain. The rational numbers $\mathbb{Q}$ form a field that is just big enough to contain the inverses of all nonzero integers. Here we review and generalize the construction of the rationals from the integers. Let R be a domain. Define an equivalence relation on $R \times R \setminus \{0\}$ by $(a, b) \sim (c, d)$ if $ad = bc$, and then let fraction a/b denote the equivalence class of (a, b). Thus,

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc.$$

Define addition and multiplication as usual:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

The collection of these fractions along with these two operations give the *field of fractions* of R, denoted $Q(R)$. The field of fractions is also called the *quotient field* of R. (Exercise: check that $Q(R)$ is actually a field). We identify $r \in R$ with $r/1 \in Q(R)$.

Proposition 1. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Proof. We have seen (in homework) that if $\alpha \in K$ then there exists a nonzero integer $c \in \mathbb{Z}$ such that $c\alpha = \beta \in \mathfrak{O}_K$. Thus, $\alpha = \beta/c$ with $\beta, c \in \mathfrak{O}_K$. Thus, every element of K is in the field of fractions of $\mathfrak{O}_K$. Conversely, since K is a field and contains $\mathfrak{O}_K$, it contains the field of fractions of $\mathfrak{O}_K$. □

Dedekind domains. We define a Dedekind domain below. The definition captures some of the most consequential properties of a number ring. There are several equivalent formulations of the definition, some of which we will get to later. (For instance: our definition is equivalent to the property that every nonzero prime ideal in a domain factors into prime ideals!)

Recall that an element $\alpha \in Q(R)$ is *integral over* R is there exists a monic polynomial $f \in R[x]$ such that $f(\alpha) = 0$.

Definition 2. A domain R is *integrally closed* if the only elements of its field of fractions $Q(R)$ that are integral over R are the elements of R, itself.

Recall that we denote the ring of all complex numbers that are integral over $\mathbb{Z}$ by $\mathfrak{O}$, and the ring of integers in a number field K by $\mathfrak{O}_K := K \cap \mathfrak{O}$. One of our goals today is to show that $\mathfrak{O}_K$ is integrally closed.

Example 3. The quotient field of $\mathbb{Z}$ is $\mathbb{Q}$, and we has seen that $\mathbb{Z}$ is integrally closed: the elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ are exactly the elements of $\mathbb{Z}$.

Definition 4. A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem 5. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

We give some preliminary results that will be used in proving the theorem.

From now on, we take K to be a number field with ring of integers $\mathfrak{O}_K$.

Theorem 6. (Structure theorem for finitely-generated $\mathbb{Z}$-modules.) Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

It is possible to take the n_i so that $n_i | n_{i+1}$ for all i, in which case, the above representation of M as a product of cyclic groups is unique.

Proof. We will give a constructive proof later in the course. (Probably.) □

Proposition 7. Let R be a finite domain. Then R is a field.

Proof. Homework. □

On last preliminary result:

Proposition 8. A prime ideal in a number ring contains the norm of each of its elements: if $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{p}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{p}$.

Proof. We have already seen that $N(\alpha) \in \mathbb{Z}$ since the norm is a coefficient of the field polynomial for α, which in turn is a power of the minimal polynomial for α.

If $\alpha = 0$, the result is obvious. So assume that $\alpha \neq 0$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K with $\sigma_1 = \mathrm{id}$, as usual. Then, define β by

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

Since $N(\alpha) \in \mathbb{Z} \subset K$ and $0 \neq \alpha \in K$, it follows that $\beta = N(\alpha)/\alpha \in K$. Let $\mathfrak{O}$ denote the set of all algebraic integers (in $\mathbb{C}$). We have seen that each $\sigma_i(\alpha)$ is an algebraic integer (apply σ_i to the minimal polynomial for α). Since $\mathfrak{O}$ is a ring, and each $\sigma_i \in \mathfrak{O}$, it follows that $\beta \in \mathfrak{O}$. So we have $\beta \in K \cap \mathfrak{O} =: \mathfrak{O}_K$. Therefore, $N(\alpha) = \alpha\beta$ with $\alpha \in \mathfrak{p}$ and $\beta \in \mathfrak{O}_K$. It follows that $N(\alpha) \in \mathfrak{p}$. □

We now prove our main theorem:

Proof of Theorem 5. We have seen that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module since it is a finitely generated $\mathbb{Z}$-module and $\mathbb{Z}$ is Noetherian. If $\mathfrak{a} \subseteq \mathfrak{O}_K$ is an ideal, it follows that $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module. Any set of generators over $\mathbb{Z}$ will generate $\mathfrak{a}$ as an ideal. Thus, $\mathfrak{O}_K$ is a Noetherian ring (i.e., $\mathfrak{O}_K$ is Noetherian as an $\mathfrak{O}_K$-module.) Alternatively, we could use the Hilbert basis theorem: since $\mathfrak{O}_K$ is finitely generated as a $\mathbb{Z}$-module, it is certainly finitely generated as a ring over $\mathbb{Z}$. Then, since $\mathbb{Z}$ is a Noetherian domain, so is $\mathfrak{O}_K$.

Next, we would like to show that every nonzero prime ideal of $\mathfrak{O}_K$ is maximal. Let $0 \neq \mathfrak{p}$ ve a prime ideal. Take any nonzero $\alpha \in \mathfrak{p}$. Let N denote the integer $N(\alpha) \in \mathbb{Z}$. We have seen that $N \in \mathfrak{p}$. Consider the (surjective) quotient mapping

$$\begin{aligned} \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta}. \end{aligned}$$

Since $N \in \mathfrak{p}$, it is in the kernel of the quotient mapping. Therefore, we get a well-defined surjective mapping

$$\begin{aligned} \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta}. \end{aligned} \tag{1}$$

where (N) is the principal ideal generated by N in $\mathfrak{O}_K$. Now, $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module (indeed, even $\mathfrak{O}_K$, itself, is a finitely generated $\mathbb{Z}$-module). Thus, we have an isomorphism of $\mathbb{Z}$-modules:

$$\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k.$$

for some $r, n_1, \ldots, n_k$. If $r \neq 0$, then $\mathfrak{O}_K/(N)$ would have elements of infinite order. However, for each $\gamma \in \mathfrak{O}_K$, we have

$$\underbrace{\gamma + \cdots + \gamma}_{N \text{ times}} = N\gamma = 0 \in \mathfrak{O}_K/(N).$$

So

$$\mathfrak{O}_K/(N) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k.$$

for some list of integers n_i with $n_i > 1$. This means that $\mathfrak{O}_K/(N)$ is finite. The surjection (1), then implies that $\mathfrak{O}_K/\mathfrak{p}$ is finite.

Since $\mathfrak{p}$ is prime, $\mathfrak{O}_K/\mathfrak{p}$ is a domain. Since a finite domain is a field (from a proposition, above), it follows that $\mathfrak{O}_K/\mathfrak{p}$ is a field. Hence, $\mathfrak{p}$ is maximal, as we wanted to show.

It remains to show that $\mathfrak{O}_K$ is integrally closed. Take $\alpha \in K$ and suppose that α is integral over $\mathfrak{O}_K$. We must show that α is integral over $\mathbb{Z}$, i.e., that $\alpha \in \mathfrak{O}$. We then have that $\alpha \in K \cap \mathfrak{O} = \mathfrak{O}_K$. We do so by showing there exists a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (This was one of the equivalent conditions established for integrality. You may remember that it involved multiplying each element of a generating set by α and then evaluating a certain determinant.)

Since α is integral over $\mathfrak{O}_K$, there exists a monic polynomial $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say

$$f(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$$

with $b_i \in \mathfrak{O}_K$ for all i. Let B be the subring of $\mathfrak{O}_K$ generated b_i over $\mathbb{Z}$:

$$B = \mathbb{Z}[b_0, \ldots, b_k] := \{g(b_0, \ldots, b_k) : g \in \mathbb{Z}[x_0, \ldots, x_k]\}.$$

The ring B is a $\mathbb{Z}$-submodule of $\mathfrak{O}_K$. Since $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module, it follows that B is finitely generated as a $\mathbb{Z}$-module. Since $\mathbb{Z}$ is Noetherian, it follows that B is a Noetherian $\mathbb{Z}$-module. Next consider the ring

$$B[\alpha] := \{g(\alpha) : g \in B[x]\}$$

Since

$$0 = f(\alpha) = \alpha^k + b_{k-1}\alpha^{k-2} + \cdots + b_1\alpha + b_0,$$

it follows that $B[\alpha]$ is finitely generated as a B-module by $\{1, \alpha, \ldots, \alpha^k\}$.

We have $\mathbb{Z} \subseteq B \subseteq B[\alpha]$ with B finitely generated as a $\mathbb{Z}$-module and $B[\alpha]$ finitely generated as a B-module. We have seen that this implies $B[\alpha]$ is finitely generated as a $\mathbb{Z}$-module (by the set of products of generators of B over $\mathbb{Z}$ with generators of $B[\alpha]$ over B).

So $B[\alpha]$ is a finitely generated $\mathbb{Z}$-module, and it is clear that $\alpha B[\alpha] \subseteq B[\alpha]$. Therefore, α is integral over $\mathbb{Z}$, completing the proof. $\square$