Math 361 lecture for Wednesday, Week 11

The class group

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
2. There exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
3. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\alpha \in K \setminus \{0\}$ such that $I = \alpha\mathfrak{a}$.
4. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $I = \frac{1}{\alpha}\mathfrak{a}$.
5. I is finitely generated as an $\mathfrak{O}_K$-module.

A *principal fractional ideal* is defined to be a fractional ideal generated as an $\mathfrak{O}_K$-module by a single element. Thus, a nonzero principal fractional ideal has the form $\alpha\mathfrak{O}_K$ for some $\alpha \in K \setminus \{0\}$.

Let $\mathcal{F}$ denote the multiplicative group of nonzero fractional ideals of $\mathfrak{O}_K$, and let $\mathcal{P}$ denote the subgroup of nonzero principal factional ideals.

Definition 1. The *class group* of $\mathfrak{O}_K$ is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The *class number* of $\mathfrak{O}_K$ is the size of this group:

$$h_K = |\mathcal{H}|.$$

Proposition 2. Every element of $\mathcal{H}$ is represented by an ordinary ideal of $\mathfrak{O}_K$.

Proof. Let $I = \alpha\mathfrak{a}$ where $\alpha \in K \setminus \{0\}$ and $\mathfrak{a}$ is an ordinary ideal. Then $\alpha\mathfrak{O}_K$ is a principal fractional ideal. Therefore,

$$I = \alpha\mathfrak{a} = (\alpha\mathfrak{O}_K)\mathfrak{a} = \mathfrak{a} \bmod \mathcal{P}.$$

□

Proposition 3. Two ordinary ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element in $\mathcal{H}$ if and only if there exist $\alpha, \beta \in \mathfrak{O}_K \setminus \{0\}$ such $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

Proof. We have $\mathfrak{a} = \mathfrak{b} \bmod \mathcal{P}$ if and only if there exists $\gamma \in K \setminus \{0\}$ such that $(\gamma\mathfrak{O}_K)\mathfrak{a} = \mathfrak{b}$. Write $\gamma = \alpha/\beta$ to get the result. □

The above proposition gives another way to define $\mathcal{H}$. Say two nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there exist nonzer $\alpha, \beta \in \mathfrak{O}_K$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. Let [] denote the equivalence class of a nonzero ideal $\mathfrak{a}$. Then $\mathcal{H}$ can be defined to be the set of equivalence class of nonzero ideals of $\mathfrak{O}_K$ with multiplication defined be $[\mathfrak{a}][\mathfrak{b}] := [\mathfrak{ab}]$.

Proposition 4. $\mathfrak{O}_K$ is a UFD if and only if $h_K = 1$, i.e., if and only if the class group is trivial.

Proof. ($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let I be a fractional ideal. We can write $I = \frac{1}{\alpha}\mathfrak{a}$ for some nonzero $\alpha \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$. We saw earlier that $\mathfrak{O}_K$ is a UFD if and only if it is a PID. Hence, $\mathfrak{a} = (\beta)$ for some nonzero $\beta \in \mathfrak{O}_K$. Therefore I is generated as an $\mathfrak{O}_K$-module by the single element β/α. So I is principal. It follows that $\mathcal{H}$ is trivial.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. We may regard $\mathfrak{a}$ as a fractional ideal, and since $\mathcal{H}$ is trivial, it follows that $\mathfrak{a}$ is a principal fractional ideal. Thus, $\mathfrak{a} = \alpha\mathfrak{O}_K$ for some nonzero element $\alpha \in K$. Since $\mathfrak{a} \subseteq \mathfrak{O}_K$, it follows that $\alpha \in \mathfrak{O}_K$, and thus, $\mathfrak{a}$ is the principal ideal $(\alpha) \subseteq \mathfrak{O}_K$. We have shown that $\mathfrak{O}_K$ is a PID, from which it follows that $\mathfrak{O}_K$ is a UFD. □

Theorem 5. Every element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}$$

where $2t$ is the number of complex embeddings of K and Δ is the discriminant of K.

Proof. We will prove this in an upcoming lecture. □

Corollary 6. The class group $\mathcal{H}$ is finite.

Proof. Recall that there are finitely many ideals with a given norm. (To recall the proof: Let $a \in \mathbb{N}$ and suppose $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$. In $\mathfrak{O}_K$ we factor the ideal (a):

$$(a) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

We know that and ideal contains the norm of each of its element. In particular, $a \in \mathfrak{a}$. This implies $(a) \subseteq \mathfrak{a}$, and hence, $\mathfrak{a}|(a)$. It follows from unique factorization of ideals that

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{\ell_i}$$

where $0 \leq \ell_i \leq e_i$ for $i = 1, \ldots, k$. There are only finitely many possibilities for the ℓ_i, and hence, only finitely many possibilities for $\mathfrak{a}$.)

By the previous theorem, each element of $\mathcal{H}$ is represented by an ideal of norm at most $(2/\pi)^t\sqrt{|\Delta|}$. There are only finitely many positive integers less than this bound. Coupled with the fact that there are only finitely many ideals with a given norm, the result follows. □

Example 7. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathfrak{O}_K = \text{Span}_{\mathbb{Z}}\{1, \sqrt{-5}\}$. The discriminant of K is

$$\Delta = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20.$$

Then K has 2 complex embeddings. So according to Theorem 5, each element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)\sqrt{|\Delta|} < 2.9.$$

So each element of $\mathcal{H}$ is represented by an ideal with norm either 1 or 2. What are the ideals with these norms? The only ideal with norm 1 is $(1) = \mathfrak{O}_K$. Next, suppose that $\mathfrak{a}$ is an ideal with norm 2. We know that $2 \in \mathfrak{a}$, and hence, $\mathfrak{a}|(2)$.

To see how (2) factors, we factor the minimal polynomial for $\sqrt{-5}$ modulo 2:

$$x^2 + 5 = x^2 + 1 = (x+1)^2 \bmod 2.$$

Hence, $(2) = (2, 1+\sqrt{-5})^2$. Taking norms, we have $N(2) = 4 = N(2, 1+\sqrt{-5})^2$. Hence, $N(2, 1+\sqrt{-5}) = 2$, and we see that $(2, 1+\sqrt{-5})$ is the only ideal with norm equal to 2.

So far, we have seen that every element of $\mathcal{H}$ is represented by (1) or $(2, 1+\sqrt{-5})$. To show these ideals are distinct in H, we must show that $(2, 1+\sqrt{5})$ is not principal. For sake of contradiction, suppose it is. Then there exist $a, b \in \mathbb{Z}$ such that $(a+b\sqrt{-5}) = (2, 1+\sqrt{-5})$. Taking norms we have

$$N(((a+b\sqrt{-5}))) = |N(a+b\sqrt{-5}))| = a^2 + 5b^2 = N((2, 1+\sqrt{-5})) = 2.$$

However, there are no solutions in $\mathbb{Z}$ to this equation.

Corollary 8. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$, and let $h = |\mathcal{H}|$ be the class number of K. Then

1. $\mathfrak{a}^h$ is principal, and
2. If $u \in \mathbb{N}$ is relatively prime to h, and $\mathfrak{a}^u$ is principal, then $\mathfrak{a}^u$ is principal.

Proof. Let $[\mathfrak{a}]$ denote the equivalence class of $\mathfrak{a}$ modulo $\mathcal{P}$. In a finite group, raising any element to the order of the group yields the identity of the group. Hence, $[\mathfrak{a}]^h = [\mathfrak{a}^h] = (1) \bmod \mathcal{P}$. So it follows that there is a principal fractional ideal $(\alpha)\mathfrak{O}_K$ such that $\mathfrak{a}^h = (1)(\alpha) = (\alpha)$. We see that α must be in $\mathfrak{O}_K$ since $\mathfrak{a}$ is in $\mathfrak{O}_K$.

If $u \in \mathbb{N}$ is relatively prime to h, then there exist $a, b \in \mathbb{Z}$ such that $au+bh = 1$. Supposing $\mathfrak{a}^u$ is principal, it follows that

$$\mathfrak{a} = \mathfrak{a}^1 = \mathfrak{a}^{au+bh} = \mathfrak{a}^{au}\mathfrak{a}^h = \mathfrak{a}^{au} = (\mathfrak{a}^u)^a = (1)^a = (1) \bmod \mathcal{P}.$$

Hence, $\mathfrak{a}$ is principal. □