Math 361 lecture for Friday, Week 11

The class group II

Let K be a number field of degree n with real embeddings $\sigma_1, \dots, \sigma_s$, and complex embeddings $\sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t}$. Recall our $\mathbb{Q}$-algebra embedding:

$$\begin{aligned}\sigma_K = \sigma \colon K &\to \mathbb{L}^{s,t} := \mathbb{R}^s \times \mathbb{C}^t \\ \alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)),\end{aligned}$$

and our identification

$$\begin{aligned}\mathbb{R}^s \times \mathbb{C}^t &\simeq \mathbb{R}^n \\ (x_1, \dots, x_s, z_1, \dots, z_t) &\mapsto (x_1, \dots, x_s, u_1, v_1, \dots, u_t, v_t)\end{aligned}$$

Define the *norm* of $q = (x_1, \dots, x_s, z_1, \dots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t$ to be

$$N(q) = x_1 \cdots x_s z_1 \overline{z_1} \cdots z_t \overline{z_t} = x_1 \cdots x_s |z_1|^2 \cdots |z_t|^2$$

and note that it is consistent with our earlier definition: for $\alpha \in K$,

$$N(\alpha) = \sigma_1(\alpha) \cdots \sigma_s(\alpha) \sigma_{s+1}(\alpha) \overline{\sigma}_{s+1}(\alpha) \cdots \sigma_{s+1}(\alpha) \overline{\sigma}_{s+t}(\alpha) = N(\sigma(\alpha)).$$

We proved a theorem giving the volume of a fundamental domain of the image of a lattice under σ and derived the following:

Corollary. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$. Identifying $\mathbb{L}^{s,t}$ with $\mathbb{R}^n$, regard $\sigma(\mathfrak{a}) \subset \mathbb{R}^n$. Then $\sigma(\mathfrak{a})$ is a lattice with fundamental domain of volume

$$2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Our goal now it two prove two theorems, one of which was used in the last lecture to show that the class group is finite.

Theorem 1. If $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{O}_K$, then there exists $0 \neq \alpha \in \mathfrak{O}_K$ such that

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Proof. Fix a real number $\varepsilon > 0$, and select positive real numbers $c_1, \dots, c_{s+t}$ such that

$$c_1 \cdots c_n = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|}.$$

Define $X_\varepsilon \in \mathbb{R}^n$ to be those $x = (x_1, \dots, x_s, x_{s+1}, y_{s+1}, \dots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \ldots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise). We have

$$\begin{aligned}
\operatorname{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})] \\
&= 2^s \pi^t (c_1 \cdots c_{s+t}) \\
&= 2^s \pi^t \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+t} N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+2t} \cdot 2^{-t} N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^n \operatorname{vol}(F)
\end{aligned}$$

where F is a fundamental domain for $\sigma(\mathfrak{a})$.

By Minkowski's theorem, X_ε contains a nonzero point in the lattice $\sigma(\mathfrak{a})$, i.e., there exists $0 \neq \beta \in \mathfrak{a}$ such that $\sigma(\beta) \in X_\varepsilon$. For each $\varepsilon > 0$, define

$$A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\}.$$

For each $\beta \in A_\varepsilon$, we have

$$|N(\beta)| < (c_1 + \varepsilon)c_2 \cdots c_{s+t}.$$

We have seen that each A_ε is nonempty. Further, since $\sigma(\mathfrak{a})$ is a lattice, each A_ε is finite. We have

$$A_1 \supseteq A_{1/2} \supseteq A_{1/3} \supseteq \cdots \supseteq A_{1/k} \supseteq \cdots.$$

Hence, $\bigcap_{k\geq 1} A_{1/k} \neq \emptyset$. Let $\alpha \in A$, then since $\alpha \in A_{1/k}$ for all $k \geq 1$, we have

$$|N(\alpha)| < (c_1 + 1/k)c_2 \cdots c_{s+t}.$$

It follows that

$$|N(\alpha)| \leq c_1 \cdots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

□

Theorem 2. Every element of the class group $\mathcal{H}$ is represented by an ideal with norm at most

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

Proof. Consider an arbitrary equivalence class $[\mathfrak{c}] \in \mathcal{H}$ where $\mathfrak{c}$ is an ordinary ideal. (We know that every element of $\mathcal{H}$ has this form.) Then $[\mathfrak{c}^{-1}] \in \mathcal{H}$, so there exists an ordinary ideal $\mathfrak{b}$ representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with

$$|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}.$$

Since $N(\beta) \in \mathfrak{b}$, it follows that $(\beta) \subseteq \mathfrak{b}$. Multiply this inclusion through by $\mathfrak{b}^{-1}$ to define

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

Hence, $\mathfrak{a}$ is an ideal. Further,

$$[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}],$$

since $\mathfrak{a}$ differs from $\mathfrak{b}^{-1}$ by a factor of a principal ideal. Finally,

$$N(\mathfrak{a}) = N((\beta))N(\mathfrak{b}^{-1}) = \frac{|N(\beta)|}{N(\mathfrak{b})} \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

□

Example 3. Let $K = \mathbb{Q}(\sqrt{-13})$. Every ideal class in $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)\sqrt{4 \cdot 13} < 4.6.$$

So we must consider ideals with norms $1, 2, 3, 4$. If an ideal $\mathfrak{a}$ contains a rational integer a, then $(a) \subseteq \mathfrak{a}$ implies that $\mathfrak{a}$ divides (a). So to find the ideals with norms a, we look for divisors of the ideal (a). In our case, where $a \in \{1, 2, 3, 4\}$, we factor the minimal polynomial $x^2 + 13$ modulo p for $p = 2, 3$ to find

$$(2) = (2, \sqrt{-13})^2, \quad (3) = (3).$$

An ideal with norm 4 divides

$$(4) = (2)^2 = (2, \sqrt{-13})^4.$$

Therefore, $h = |\mathcal{H}| = 1$ or 2, depending on whether $(2, \sqrt{-13})$ is principal.
If $(2, \sqrt{-13}) = (a + b\sqrt{-13})$ for some $a, b \in \mathbb{Z}$, taking norms, we find

$$2 = a^2 + 13b^2,$$

for which there are no solutions. Therefore, $\mathcal{H}$ is a group with two elements: $[(1)]$ and $[(2, \sqrt{-13})]$.