Math 531 Tom Tucker
NOTES FROM CLASS 11/08

We'll want to define the discriminant of fractional ideal I first. We haven't yet defined the norm of a fractional ideal. Since a fractional ideal I of a Dedekind domain factors as

$$\mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_m^{e_m}$$

we can simply define the norm of I to be

$$\mathrm{N}_{L/\mathbb{Q}}(I) = \mathrm{N}_{L/\mathbb{Q}}(\mathcal{Q}_1^{e_1}) \cdots \mathrm{N}_{L/\mathbb{Q}}(\mathcal{Q}_m^{e_m}).$$

Definition 28.1. Let I be an fractional ideal of $\mathcal{O}_L$. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of $L \longrightarrow \mathbb{C}$ and let $w_1, \ldots, w_n$ generate I over $\mathbb{Z}$. We define the discriminant of $\Delta(I/\mathbb{Z})$ to be

$$\Delta(I/\mathbb{Z}) := \det[\sigma_i(w_j)]^2.$$

This definition does not depend on our choice of the basis, since two different bases differ by a linear transformation with determinant ± 1.

Definition 28.2. Let p be a prime in $\mathbb{Z}$. Let $S = \mathbb{Z} \setminus p\mathbb{Z}$. Let J be a fractional ideal of $S^{-1}\mathcal{O}_L$. We define

$$\Delta(J/\mathbb{Z}_{(p)}) = Z_{(p)} \det[\sigma_i(w_j)]^2,$$

where $w_1, \ldots, w_n$ is a basis for J over $\mathbb{Z}_{(p)}$

Lemma 28.3. *Let I be a fractional ideal of $\mathcal{O}_L$. Then*

$$\mathbb{Z}_{(p)}\Delta(I/\mathbb{Z}) = \Delta(S^{-1}I/\mathbb{Z}).$$

Proof. This follows immediately from the fact that any basis for I over $\mathbb{Z}$ is a basis for $S^{-1}I$ over $\mathbb{Z}_{(p)}$. $\square$

Theorem 28.4. *We have $\mathbb{Z}\Delta(I/\mathbb{Z}) = \mathrm{N}_{L/K}(I)^2\Delta(\mathcal{O}_L/\mathbb{Z})$.*

Proof. Both the norm and the discriminant can be calculated locally, so it suffices to prove that for p a prime of $\mathbb{Z}$ and $S = \mathbb{Z} \setminus p\mathbb{Z}$ we have

$$\Delta(S^{-1}\mathcal{O}_L I/\mathbb{Z}_{(p)}) = \mathrm{N}_{L/K}(S^{-1}\mathcal{O}_L I)\Delta(\mathcal{O}_L/\mathbb{Z}_{(p)}).$$

Since $S^{-1}\mathcal{O}_L$ is a principal ideal domain, we can write $S^{-1}I = S^{-1}\mathcal{O}_L y$ for some $y \in L$. Now, if $w_1, \ldots, w_n$ is a basis for $S^{-1}\mathcal{O}_L$ over $\mathbb{Z}_{(p)}$, then $yw_1, \ldots, yw_n$ is basis for $S^{-1}I$ over $\mathbb{Z}_{(p)}$. The matrix $[\sigma_i(yw_j)]$ is equal to the matrix $[\sigma_i(y)\sigma_i(w_j)]$ which is equal to $[\det \sigma_i(w_j)]$ times the matrix

$$\begin{pmatrix} \sigma_1(y) & 0 & \cdots & 0 \\ 0 & \sigma_2(y) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \sigma_n(y) \end{pmatrix}$$

which has determinant equal to $\mathrm{N}_{L/\mathbb{Q}}(y)$. Thus,

$$\Delta(S^{-1}\mathcal{O}_L I/\mathbb{Z}_{(p)}) = \left(\mathrm{N}_{L/K}(y)\det[\sigma_i(w_j)]\right)^2 = \mathrm{N}_{L/K}(y)^2\Delta(S^{-1}\mathcal{O}_L/\mathbb{Z}_{(p)}).$$

□

Corollary 28.5. *Let $I \subset \mathcal{O}_L$ be an fractional ideal. Then $h(I)$ is a lattice with volume*

$$(1/2)^s|\,\mathrm{N}_{L/\mathbb{Q}}(I)|\sqrt{|\Delta(\mathcal{O}_L/\mathbb{Z})|}.$$

Proof. Since h is a $\mathbb{Z}$-homomorphism, the same matrix that represents the generators for I in terms of a basis for $\mathcal{O}_L$ represents generators for $h(I)$ in terms of a basis for $h(\mathcal{O}_L)$. □

We want to show that there is an element of small norm in I. To make the proof of the finiteness of the class number as clear as possible, we'll first give simple versions of it and then prove more quantitative versions later.

Theorem 28.6. *(Imprecise small element of fractional ideal) There exists a constant $C(L)$ depending only on L such that for any fractional ideal I of $\mathcal{O}_L$ there is an element $y \in I$*

$$\mathrm{N}_{L/K}(y) \leq C(L)\,\mathrm{N}_{L/K}(I).$$

Theorem 28.7. *Assume Theorem 28.6 above. For any fractional ideal I of $\mathcal{O}_L$, there is an ideal $J \subset \mathcal{O}_L$ in the same ideal class as I such that*

$$|\,\mathrm{N}_{L/\mathbb{Q}}(J)| \leq C(L).$$

Proof. By Theorem 28.6 above, there exists $a \in I^{-1}$ such that

$$|\,\mathrm{N}_{L/\mathbb{Q}}(a)| \leq |\,\mathrm{N}_{L/\mathbb{Q}}(I^{-1})|C(L).$$

Then $J = Ia \subseteq \mathcal{O}_L$ and

$$|\,\mathrm{N}_{L/\mathbb{Q}}(J)| \leq C(L).$$

□