Math 430 Tom Tucker
NOTES FROM CLASS 11/03

Recall from last time... From now on, we'll stick to L a finite field extension of $\mathbb{Q}$ of degree n with ring of integers $\mathfrak{o}_L$. Some of what we do applies to other orders in L, too.

Let's order the embeddings $\sigma_1, \ldots, \sigma_n$ ($n = [L : \mathbb{Q}]$) in the following way. We let $\sigma_1, \ldots, \sigma_s$ be real embeddings. The remaining embeddings come in pairs as explained above, so for $i = r+1, r+3, \ldots,$ we let σ_i be a complex embedding and let $\sigma_{i+1} = \overline{\sigma_i}$. We let s be the number of complex embeddings. We have $r + 2s = n$.

Now, we can embed $\mathfrak{o}_L$ into $\mathbb{R}^n$ by letting

$$\begin{aligned} h(y) &= (\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \Re(\sigma_{r+1}(y)), \Im(\sigma_{r+1}(y)), \ldots, \Re(\sigma_{r+2(s-1)}(y)), \Im(\sigma_{r+2(s-1)}(y))) \\ &= \big(\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \frac{\sigma_{r+1}(y) + \sigma_{r+2}(y)}{2}, \frac{\sigma_{r+1}(y) - \sigma_{r+2}(y)}{2i}, \ldots, \\ &\quad \frac{\sigma_{r+2(s-1)}(y) + \sigma_{r+2(s-1)}(y)}{2}, \frac{\sigma_{r+2(s-1)}(y) - \sigma_{r+2(s-1)+1}(y)}{2i}\big). \end{aligned} \tag{1}$$

Let us also denote as h_i the map $h : \mathfrak{o}_L \longrightarrow \mathbb{R}$ given by composing h with projection p_i onto the i-th coordinate of $\mathbb{R}^n$.

We will continue to use h and h_i as defined above. We will also continue to let s and r be as above and to let $n = r + 2s$ be the degree $[L : \mathbb{Q}]$.

Proposition 18.1. *Let B be an integral extension of $\mathbb{Z}$ with field of fractions L. Let $w_1, \ldots, w_n$ be a basis for a B over $\mathbb{Z}$. Then*

$$(\det[h_i(w_j)])^2 = \frac{1}{(2i)^{2s}} |\Delta(B/\mathbb{Z})|.$$

Proof. From the HW just assigned (problem #2), we know that

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

We also know from (1) that h_i differs from σ_i (when the σ's are ordered as in that equation) only for σ_i complex and we can obtain h_i for even $i > r$ by adding up two σ_i and dividing by 2. We can then get the odd i-th rows by subtracting the $i-1$ row from the i-th row and diving by $2i$. I will put this on the board. □

Corollary 18.2. *The image $h(\mathfrak{o}_L)$ in $\mathbb{R}^n$ is a full lattice.*

Proof. Since $\Delta(\mathfrak{o}_L/\mathbb{Z}) \neq 0$, the determinant $\det[h_i(w_j)] \neq 0$, so the $h_i(w_j)$ are linearly independent over $\mathbb{R}$. Hence they generate $\mathbb{R}^n$ as an $\mathbb{R}$-vector space and $\mathfrak{o}_L$ is a full lattice. □

In the book the following characterization of a lattice is proven. We will not use it, so I will not give the proof in class.

Theorem 18.3. *(Thm. 12.2) An additive subgroup $\mathcal{L} \subset \mathbb{R}^n$ is a lattice if and only if every sphere in $\mathbb{R}^n$ contains only finitely many elements of $\mathcal{L}$.*

We will not need this characterization.

****** Fundamental parallelepipeds. Let $\mathcal{L}$ be a full lattice in $\mathbb{R}^n$ and let $w_1, \dots, w_n$ be a basis for $\mathcal{L}$ over $\mathbb{Z}$. We call the set

$$\mathcal{T} = \{r_1 w_1 + \cdots + r_n w_n \mid 0 \le r_i < 1, \ r_i \in \mathbb{R}\}$$

the *fundamental parallelepiped* for the basis $w_1, \dots, w_n$.

Lemma 18.4. *Let $\mathcal{L}$ be a full lattice in $\mathbb{R}^n$ and let $w_1, \dots, w_n$ be a basis for $\mathcal{L}$ over $\mathbb{Z}$ with fundamental parallelepipeds $\mathcal{T}$. Then every element $v \in \mathbb{R}^n$ can be written as $t + \lambda$ for a unique $t \in \mathcal{T}$ and $\lambda \in \mathcal{L}$. In particular, the sets $\lambda + \mathcal{T}$ are disjoint and cover all of $\mathbb{R}^n$.*

Proof. Let $v \in V$. Write $v = \sum_{i=1}^{m} s_i w_i$ (uniquely). Then each s_i can be written uniquely as an integer plus a real number less than 1, that is as

$$s_i = [s_i] + r_i$$

where the brackets are the greatest integer function and $r_i < 1$. □

Now, we want to work with volumes. A volume on $\mathbb{R}^n$ comes from a choice of orthonormal basis $x_1, \dots, x_n$. Let V be the vector space $\mathbb{R}^n$ equipped with the orthonormal basis $x_1, \dots, x_n$. For a lattice $\mathcal{L}$ with basis $w_1, \dots, w_n$, we can write

$$w_i = \sum_{j=1}^{n} s_{ij} x_j.$$

It follows from multivariable calculus that the volume of the parallelepipeds $\mathcal{T}$ for the w_i is

$$\int \cdots \int_{\mathcal{T}} dx_1 \dots dx_n = \int \cdots \int_{0 \le x_i < 1} |\det[s_{ij}]| dx_1 \dots dx_n = |\det[s_{ij}]|.$$

We call the quantity $|\det[s_{ij}]|$ the volume of $\mathcal{L}$. It does not depend on our choice of basis since any two choice of bases differ by a change of basis matrix with determinant ± 1.

Note that there is a choice of basis implicit in our map $h : \mathfrak{o}_L \longrightarrow \mathbb{R}^n$. This basis comes from the coordinates with which we have described our map. Draw picture on board. We will call this basis x_i and call $\mathbb{R}^n$ equipped with this volume form V.

Theorem 18.5. *The volume of $h(\mathfrak{o}_L)$ in V is*

$$\frac{1}{2^s}\sqrt{|\Delta(\mathfrak{o}_L/\mathbb{Z})|}.$$

Proof. This follows immediately from Proposition 18.1, since the matrix we have written is with respect to the basis x_i above. □

Now, let I be a fractional ideal in $\mathcal{L}$. The ideal I is torsion-free as $\mathbb{Z}$-module. We can calculate the volume of $h(I)$ in terms of the degree of L, the discriminant $|\Delta(\mathfrak{o}_L/\mathbb{Z})|$, and $|\mathrm{N}_{L/K}(I)|$.

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 18.6. Let I be an fractional ideal of $\mathfrak{o}_L$. 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 18.7. Let p be a prime in $\mathbb{Z}$. Let $S = \mathbb{Z}\setminus p\mathbb{Z}$. Let J be a fractional ideal of $S^{-1}\mathfrak{o}_L$. 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 18.8. *Let I be a fractional ideal of $\mathfrak{o}_L$. 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 $\mathbb{Z}_{(p)}$. □

Theorem 18.9. *We have $\mathbb{Z}\Delta(I/\mathbb{Z}) = \mathrm{N}_{L/K}(I)^2\Delta(\mathfrak{o}_L/\mathbb{Z})$.*

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

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

Since $S^{-1}\mathfrak{o}_L$ is a principal ideal domain, we can write $S^{-1}I = S^{-1}\mathfrak{o}_L y$ for some $y \in L$. Now, if $w_1,\ldots,w_n$ is a basis for $S^{-1}\mathfrak{o}_L$ 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,

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

□

Corollary 18.10. *Let $I \subset \mathfrak{o}_L$ be an fractional ideal. Then $h(I)$ is a lattice with volume*

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

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

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

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

Theorem 18.12. *Assume Theorem 18.11 above. For any fractional ideal I of $\mathfrak{o}_L$, there is an ideal $J \subset \mathfrak{o}_L$ in the same ideal class as I such that*

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

Proof. By Theorem 18.11 above, there exists $a \in I^{-1}$ such that

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

Then $J = Ia \subseteq \mathfrak{o}_L$ and

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

□