Math 430 Tom Tucker
NOTES FROM CLASS 11/04

First, a little bit about the idea of our proof. We will prove the following. All of our norms here will be relative to $\mathbb{Q}$ (i.e. over K they are $N_{K/\mathbb{Q}}$.

Theorem 18.1. *Let K be a number field. Then there is a constant $C(K)$ such that for any nonzero fractional ideal I in $\mathfrak{o}_K$, there is an element $a \in I$ such that $|N(a)| \leq |N(I)|C(K)$.*

This means that a "almost generates" I. In particular it give the following (which easily shows that the class group of K is finite).

Corollary 18.2. *Let K be a number field. Then there is a constant $C(K)$ such that for any nonzero ideal fractional I in $\mathfrak{o}_K$, there is an integral idea $J \subseteq \mathfrak{o}_K$ such that $J = Ia$ for some $a \in K$ and $|N(J)| \leq C(K)$.*

Proof. Apply the previous theorem to I^{-1}. Then there is an $a \in I^{-1}$ such that $|N(a)| \leq |N(I^{-1}|C(K)$. Let $J = Ia$. □

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 18.3. *Let B be an integral extension of $\mathbb{Z}$ with field of fractions L. Let $w_1, \dots, w_n$ 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. □

Recall our definitions of lattices.

Definition 18.4. A subgroup $\mathcal{L}$ of $\mathbb{R}^n$ is said to be a lattice if $\mathcal{L}$ is isomorphic to $\mathbb{Z}^r$ as a group and the $\mathbb{R}$-vector space generated by $\mathcal{L}$ has dimension r. When this holds for $\mathcal{L}$ with $r = n$, we say that $\mathcal{L}$ is a full lattice in $\mathbb{R}^n$.

Corollary 18.5. *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 18.6. *(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

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

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

Lemma 18.7. *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 $x_1, \ldots, x_n$. Let V be the vector space $\mathbb{R}^n$ equipped with the orthonormal basis $x_1, \ldots, x_n$. For a lattice $\mathcal{L}$ with basis $w_1, \ldots, w_n$, 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

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

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 18.8. *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 18.3, since the matrix we have written is with respect to the basis x_i above. □