Math 568 Tom Tucker
NOTES FROM CLASS 11/12

Recall from last time that when R is Dedekind, all fractional ideals are invertible (and thus form a group) so we have an exact sequence

$$0 \longrightarrow \mathrm{Pri}(R) \longrightarrow \mathrm{Fr}(R) \longrightarrow \mathrm{Cl}(R) \longrightarrow 0.$$

We call the quotient $\mathrm{Cl}(R)$ above the class group of R. When R is the integral closure $\mathcal{O}_L$ of $\mathbb{Z}$ in some number field L, we often write $\mathrm{Cl}(L)$ for $\mathrm{Cl}(\mathcal{O}_L)$. We also write $\Delta(L)$ for $\Delta(\mathcal{O}_L/\mathbb{Z})$. We want to prove the following.

Theorem 18.1. *Let L be a number field. Then $\mathrm{Cl}(L)$ is finite.*

Recall the main idea... If we have a number field L of degree n over $\mathbb{Q}$, then we have n different embeddings of L into $\mathbb{C}$. They can be obtained by fixing one embedding $L \longrightarrow \mathbb{C}$ and then conjugating this embedding by elements in the cosets of H_L in $\mathrm{Gal}(M/\mathbb{Q})$ for M some Galois extension of $\mathbb{Q}$ containing L. We'll use these to make B a full lattice in $\mathbb{R}^n$. What is a full lattice? (Last time I only introduced this informally.)

Definition 18.2. A lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module whose rank as a $\mathbb{Z}$-module is the equal to the dimension of the $\mathbb{R}$-vector space generated by $\mathcal{L}$. A full lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module of rank n that generates $\mathbb{R}^n$ as a $\mathbb{R}$-vector space.

Example 18.3.
(1) $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ is *not* a full lattice of $\mathbb{R}^2$ under the embedding $1 \mapsto 1$ and $\theta \mapsto \sqrt{3}$, since it generates an $\mathbb{R}$-vector space of dimension 1.
(2) $\mathbb{Z}[i]$ is full lattice in $\mathbb{R}^2$ where $\mathbb{R}^2$ is $\mathbb{C}$ considered as an $\mathbb{R}$-vector space with basis $1, i$ over $\mathbb{R}$.

On the other hand, we can send $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ into $\mathbb{R}^2$ in such a way that it is a full lattice in the following way. Let $\phi : 1 \mapsto (1,1)$ and $\phi : \theta :\longrightarrow (\sqrt{3}, -\sqrt{3})$. In this case, we must generated $\mathbb{R}^2$ as an $\mathbb{R}^2$ vector space since $(1,1)$ and $(\sqrt{3}, -\sqrt{3})$ are linearly independent.

There are two different types of embeddings of L into $\mathbb{C}$. There are the real ones and the complex ones. An embedding $\sigma : L \longrightarrow \mathbb{C}$ is real if $\overline{\sigma(y)} = \sigma(y)$ for every $y \in L$ (the bar here denotes complex conjugation) and is complex otherwise. How can we tell which is which?

Suppose we have a number field L. We can write $L \cong \mathbb{Q}[X]/f(X)$ for some monic irreducible polynomial L with integer coefficients. Then by the Chinese remainder theorem $\mathbb{R}[X]/f(X) \cong \bigoplus_{i=1}^m \mathbb{R}[X]/f_i(X)$ where the f_i have coefficients in $\mathbb{R}$, are irreducible over $\mathbb{R}$, and $f_1 \dots f_m = g$

(note that the f_i are distinct since L is separable over $\mathbb{Q}$). We also know that each f_i is of degree 1 or 2. When f_i has degree 1, then $\mathbb{R}[X]/f_i(X)$ is isomorphic to $\mathbb{R}$ and when f_i has degree 2, then $\mathbb{R}[X]/f_i(X)$ is isomorphic to $\mathbb{C}$. Since $\mathbb{Q}$ has a natural embedding into $\mathbb{R}$, we obtain a natural embedding of

$$j : L \cong \mathbb{Q}[X]/f(X) \longrightarrow \bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X).$$

Composing j with projection onto the i-th factor of

$$\bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X)$$

then gives a map from $L \longrightarrow \mathbb{R}$ or $L \longrightarrow \mathbb{C}$. In fact, when $\deg f_i = 2$ and $\mathbb{R}[X]/f_i(X)$ is $\mathbb{C}$ we get two embeddings by composing with conjugation. The image of L is the same for these two embeddings, so we will want to link these two in some way...

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 $\sigma_{i+1} = \overline{\sigma_{i+1}}$. We let s be the number of complex embeddings. We have $r + 2s = n$.

Now, we can embed $\mathcal{O}_L$ 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 $h : \mathcal{O}_L \longrightarrow \mathbb{R}$ 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 18.4. *Let $\{w_1 \ldots, w_m\}$ be a basis for $\mathcal{O}_L$ over $\mathbb{Z}$. We have*

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

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

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

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 $-i$. I will put this on the board. □

Note that we can actually define $\Delta(\mathcal{O}_L/\mathbb{Z})$ as a number (positive or negative) not just an ideal. I will say more about this next time.

Corollary 18.5. *The image $h(\mathcal{O}_L)$ in $\mathbb{R}^n$ is a full lattice.*

Proof. Since $\Delta(\mathcal{O}_L/\mathbb{Z}) \neq 0$, 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 $\mathcal{O}_L$ 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 $\mathcal{L} \subset \mathbb{R}^n$ of $\mathbb{Z}$-rank n is a full 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 $x_1, \dots, x_n$. Let V be the vector space $\mathbb{R}^n$

equipped with the orthonormal basis $x_1, \dots, x_n$. For a full 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

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

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 $h : \mathcal{O}_L \longrightarrow \mathbb{R}^n$. This basis comes from the coordinates with which we have described our map. We will call this basis $\{x_1, \dots, x_n\}$ and call $\mathbb{R}^n$ equipped with this volume form V.

Definition 18.8. For a full lattice $\mathcal{L}$ in $\mathbb{R}^n$, we define $\mathrm{Vol}(\mathcal{L})$ to the absolute value of the determinant of the matrix obtained by lining up the bases elements for $\mathcal{L}$ as vectors. (Observe that this does not depend on our choice of basis).

Theorem 18.9. *The volume of $h(\mathcal{O}_L)$ in V is*

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

Proof. This follows immediately from Proposition 18.4, since the matrix we have written is with respect to the basis x_i above. ☐

Now, let I be anideal 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 $|\Delta(\mathcal{O}_L/\mathbb{Z})|$, and $|\mathrm{N}(I)|$.

Theorem 18.10. *We have* $\mathrm{Vol}(h(I)) = |\mathrm{N}(I)||\mathrm{Vol}(h(\mathcal{O}_L))|$.

Proof. Write $I = \mathcal{Q}_1^{e_1} \dots \mathcal{Q}_m^{e_m}$ and let f_i be the degree $[\mathcal{O}_L/\mathcal{Q}_i : \mathbb{Z}/p_i\mathbb{Z}]$ where $p_i = \mathcal{Q}_i \cap \mathbb{Z}$. Since $N(\mathcal{Q}_i) = p_i^{f_i} = |\mathcal{O}_L/\mathcal{Q}_i|$ and $\mathcal{O}_L/\mathcal{Q}_i^{e_i}$ is a e_i-dimensional vector space over $\mathcal{O}_L/\mathcal{Q}_i$, we we see by the Chinese Remainder Theorem that $N(I) = |\mathcal{O}_L/I|$. Now, we can choose a basis $\{w_1, \dots, w_n\}$ for $\mathcal{O}_L$ such that $\{a_1 w_1, \dots, a_n w_n\}$ is a basis for I for some positive integers $a_1, \dots, a_n$ (this a standard fact about free abelian groups that I will have you prove on your homework later). Clearly, we have

$$(2) \qquad |\det[\sigma_i(a_j w_j)]| = |(a_1 \cdots a_n)| \mathrm{Vol}(h(\mathcal{O}_L)) = N(I) \mathrm{Vol}(h(\mathcal{O}_L))$$

□