Math 568 Tom Tucker
NOTES FROM CLASS 12/1

Unit groups of rings of integers. As usual, L is a finite extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_L$ and norm $\mathrm{N} = \mathrm{N}_{L/\mathbb{Q}}$. We want to find out what the group of unit $\mathcal{O}_L^*$ looks like. First a simple proposition on units.

Proposition 32.1. *Let $y \in \mathcal{O}_L$. Then y is a unit if $\Leftrightarrow$ if* $\mathrm{N}(y) = 1$.

Proof. ($\Rightarrow$) If y is a unit then $xy = 1$ for some $x \in \mathcal{O}_L$. Then $\mathrm{N}(x)\,\mathrm{N}(y) = 1$. Since $\mathrm{N}(x)$ and $\mathrm{N}(y)$ are both integers, this means that $\mathrm{N}(y) = \pm 1$.
($\Leftarrow$) It will suffice to show that $\frac{\mathrm{N}(y)}{y}$ is in $\mathcal{O}_L$. Since $\frac{\mathrm{N}(y)}{y}$ is a product of conjugates of y, it must be integral over $\mathbb{Z}$. Moroever, since $\mathrm{N}(y)$ and y are in L, their quotient $\frac{\mathrm{N}(y)}{y}$ must be as well. Thus $\frac{\mathrm{N}(y)}{y} \in \mathcal{O}_L$. □

Let's look at the case of quadratic field first. If L is an imaginary quadratic field, then $\mathcal{O}_L$ can be thought of as a subfield of $\mathbb{C}$ and $\mathrm{N}(x) = x\bar{x} = a^2 + b^2$, where $x = a + ib$. If $a^2 + b^2 = 1$, then $a + bi$ lies on the unit circle. We can go a bit further and write $\mathcal{O}_L \subseteq \mathbb{Z}\omega$ where $\omega = \frac{1+\sqrt{-d}}{2}$ for some positive squarefree d. Then any norm can be written as $\frac{a^2+db^2}{4}$. In order to have

$$\frac{a^2 + db^2}{4} = 1, \tag{1}$$

we must have $d \leq 4$ or $b = 0$. When $b = 0$, we must have $a^2 = 4$, so $a = \pm 2$, which gives us the obvious units ± 1. When $d = 2$, we cannot solve (1) except with $b = 0$ and $a = \pm 1$. When $d = 3$, we have 4 additional solutions

$$\frac{\pm 1 \pm \sqrt{-3}}{2}.$$

It is easy to check that that all of these are powers of ξ_6, a primitive 6-th root of unity. We've shown then that in an imaginary quadratic the only units are the roots of unity.

What about real quadratics? In this case a unit $x + \sqrt{d}y$ (d positive and squarefree) with $x, y \in \mathbb{Z}$ is solution to Pell's equation

$$x^2 - dy^2 = 1.$$

It was known in the 19th century that this has a solution other than $y = 0$ and $x = \pm 1$ and that there is a fundamental solution $u = x + y\sqrt{d}$ such that any other nontrivial (not ± 1) solution v is a power of u. Furthermore, we know that u is not a root of unity since the only roots of unity in $\mathbb{R}$ are ±1. For real quadratics, then the free rank of $\mathcal{O}_L*$ is 1.

In general, here is what we'll do:
As usual, let n be the degree of L over $\mathbb{Q}$ and let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of L into $\mathbb{C}$ with $\sigma_{r+1}, \sigma_{r+2}, \sigma_{n-1}, \sigma_n$ the complex embeddings. Let's reorder the complex embeddings so that $\sigma_{r+i+s} = \overline{\sigma_{r+i}}$ for odd $r < i \leq s$. For $b \in \mathcal{O}_L$, we define

$$\ell(b) = (\log|\sigma_1(b)|, \ldots, \log|\sigma_r(b)|, \log|\sigma_{r+1}(b)|^2, \log|\sigma_{r+2}(b)|^2,$$
$$\ldots, |\sigma_{r+s}(b)|^2)$$
$$= (\log|\sigma_1(b)|, \ldots, \log|\sigma_1(b)|, 2\log|\sigma_{r+1}(b)|, 2\log|\sigma_{r+2}(b)|, \ldots, 2|\sigma_{r+s}(b)|)$$

Since

$$\begin{aligned}\log|\,\mathrm{N}(b)| =& \log|\sigma_1(b)| + \cdots + \log|\sigma_1(b)| \\ &+ 2\log|\sigma_{r+1}(b)| + 2\log|\sigma_{r+2}(b)| + \cdots + 2|\sigma_{r+s}(b)|\end{aligned}$$

and $\log|\,\mathrm{N}(b)| = 0$ if and only if b is a unit, we see that ℓ sends $\mathcal{O}_L$ into the hyperplane in $\mathbb{R}^{s+r}$ consisting of elements with coordinates $(x_1, \ldots, x_{r+1})$ for which

$$x_1 + \cdots + x_n = 0.$$

We might ask what the kernel of ℓ is. First, a Lemma.

Lemma 32.2. *For any constant C, there are finitely many $b \in \mathcal{O}_L$ such that $|\sigma_i(b)| \leq C$ for each σ_i.*

Proof. To see this, we use the map we used in the finiteness of the class group $h : L \longrightarrow \mathbb{R}^n$ (with the old numbering of the embeddings σ) defined by

$$h(b) = (\sigma_1(b), \ldots, \sigma_r(b), \Re(\sigma_{r+1}(b)), \Im(\sigma_{r+1}(b)),$$
$$\ldots, \Re(\sigma_{r+2(s-1)}(b)), \Im(\sigma_{r+2(s-1)}(b))).$$

Note that h is injective, since each σ_i is injective. It is clear that if $|\sigma_i(b)| \leq C$, for all i, then the coordinates of $h(b)$ must all be less than or equal to 1. Hence all $h(b)$ with $|\sigma_i(b)| \leq C$ for each embedding σ_i are contained in a bounded region of $\mathbb{R}^n$. Since $h(\mathcal{O}_L)$ intersects a bounded region in finitely many points. Hence there are finitely many b such that $|\sigma_i(b)| \leq C$ for each embedding σ_i. □

Proposition 32.3. *The kernel of ℓ is finite and is equal to the roots of unity of L.*

Proof. Suppose that $\ell(b) = (0, \ldots, 0)$. Then $|\sigma_i(b)| = 1$ for each embedding σ_i. From the Lemma above are finitely many such b. Now, if $|\sigma_i(b)| = 1$ for each embedding σ_i, then $|\sigma_i(b^n)| = 1$ for each embedding

σ_i. Thus, the group generated by any such b much be finite. Hence, b must be a root of unity. Finally, it is easy to see that any root of unity is integral (we saw this earlier when we studied cyclotomic fields), so all the roots of unity in L are in $\mathcal{O}_L$. □

Next, we will show that $\ell(\mathcal{O}_L^*)$ is a sublattice in $\mathbb{R}^{r+s}$. We define a sublattice is a subgroup of $\mathbb{R}^m$ that has $\mathbb{Z}$-rank equal to the $\mathbb{R}$-dimension of the vector space it generates.

Proposition 32.4. *Let $\mathcal{L}$ be a finitely generated subgroup of $\mathbb{R}^m$. Then $\mathcal{L}$ is a sublattice if and only if every bounded region in $\mathbb{R}^m$ contains at most finitely many elements of $\mathcal{L}$.*

Proof. Note, we already proved the "only if" part last week during our proof of the finiteness of the class group.

We will prove the "if" part by induction on m. If $m = 1$ and $\mathcal{L} \neq 0$ (0 is trivially a sublattice), then $\mathbb{R}^m = \mathbb{R}$, and we choose u to be the smallest positive number in $\mathcal{L}$. Then, for any $v \in \mathcal{L}$, we can write $v = tu + z$ where t is an integer and $0 \leq z < u$. But, since $z = v - tu$, we must have $z \in \mathcal{L}$, which means that $z = 0$ by the minimality of u. Thus, u must generate $\mathcal{L}$ as a $\mathbb{Z}$-module, so the rank of $\mathcal{L}$ as a group is equal to 1.

Now, we do the inductive step. Note that we may assume $\mathcal{L}$ generates $\mathbb{R}^m$ as a vector space, since otherwise it is contained in a vector space of dimension $\mathbb{R}^{m-1}$ and we are done by the inductive hypothesis. Thus, we can choose $\mathbb{R}$-linearly independent elements $v_1, \ldots, v_m$ of $\mathcal{L}$. By the inductive hypothesis, if V_0 is the $\mathbb{R}$-vector space generated by $v_1, \ldots, v_{m-1}$, then $\mathcal{L}_0 := V_0 \cap \mathcal{L}$ is a sublattice, and is a full lattice in V_0. Let $w_1, \ldots w_{m-1}$ be a basis for $\mathcal{L}_0$ (as a $\mathbb{Z}$-module). Then, $w_1, \ldots, w_{m-1}, v_m$ is a basis for $\mathbb{R}^m$, so any element of $\lambda \in \mathcal{L}$ can be written as

$$\lambda = \sum_{i=1}^{m-1} r_i w_i + r_m v_m$$

for real numbers r_i. Note that if $r_m = 0$, then $\lambda \in \mathcal{L}_0$, and we can choose all of the r_i to be integers. Note also that by subtracting off an appropriate element of $\mathcal{L}_0$, we obtain such a λ with all $0 \leq r_i < 1$ for $i \leq (m-1)$. There are only finitely many such λ with r_m also smaller than a certain bound (since any bounded region in $\mathbb{R}^m$ intersects $\mathcal{L}$ in finitely many points). Thus, there is a nonzero element λ' with $0 \leq r_i < 1$, for $i = 1, \ldots, m-1$ and $r_m > 0$ minimal (if $r_m = 0$, then the other r_i must be integers, we recall). I claim that $w_1, \ldots, w_{m-1}, \lambda'$ must be a $\mathbb{Z}$-basis for $\mathcal{L}$. Indeed, if we pick any element $\eta \in \mathcal{L}$ and write

$$\eta = \sum_{i=1}^{m-1} a_i w_i + a_m v_m$$

with $a_i \in \mathbb{R}$. Then by writing

$$a_m = t r_m + z$$

with $t \in \mathbb{Z}$ and $0 \leq z < r_m$ and subtracting

$$\sum_{i=1}^{m-1} ([a_i - r_i t]) w_i + t\lambda'$$

from η we obtain an element of $\mathcal{L}$ written as

$$\sum_{i=1}^{m-1} ((a_i - r_i t) - [a_i - r_i t]) w_i + z v_m$$

with $0 \leq z < a_m$. Thus, we must have $z = 0$ and

$$\eta - t\lambda' \in \mathcal{L}_O$$

and we are done. □

Let's define some notation now. For a finitely generated abelian group G we define $\mathrm{rk}(G)$ to be the free rank of G. Let's also define H to be the hyperplane $x_1 + \ldots x_{s+r} = 0$ in $\mathbb{R}^{s+r}$.

Proposition 32.5. *$\ell(\mathcal{O}_L^*)$ is a sublattice in H.*

Proof. Any bounded region in $\mathbb{R}^{s+r}$ is contained in a set Y_C consisting of all $(x_1, \ldots, x_{r+s})$ with $|x_i| \leq C$ for $C \geq 0$. For $b \in \mathcal{O}_L^*$, the absolute value of the i-th coordinate of $\ell(b)$ is less than or equal to C only if $|\sigma_i(b)| \leq e^C$ for all i. There are only finitely many such b by a Lemma from last time. □

Corollary 32.6.

$$\mathrm{rk}(\mathcal{O}_L^*) \leq (r + s - 1)$$

Proof. Since the kernel of ℓ is finite,

$$\mathrm{rk}(\mathcal{O}_L^*) = \mathrm{rk}(\ell(\mathcal{O}_L^*)).$$

From the previous Proposition we know that $\ell(\mathcal{O}_L^*)$ is sublattice in a vector space of dimension $s + r - 1$, so it must have $\mathbb{Z}$-rank at most $s + r - 1$. □

We're going to want use another embedding of $\mathcal{O}_L$ into an $\mathbb{R}$-vector space. This embedding, which we denote as h^* is almost exactly like the embedding h that we used earlier. It is

$$h^*(b) = (\sigma_1(b), \ldots, \sigma_r(b), \sigma_{r+1}(b), \ldots, \sigma_{r+s}(b)).$$

Note that is very similar to the embedding h used earlier. In fact, we can choose the $\mathbb{R}$-basis $x_1, \ldots, x_r$, $y_1, z_1, \ldots, y_s, z_1, \ldots, z_s$, where x_j is the element with j-th coordinate equal to 1 and all other coordinates equal to 0, y_j to be the the element with $(r+j)$-th element equal to 1 and all other coordinates equal to 0, and z_j to be the the element with $(r+j)$-th element equal to i and all other coordinates equal to 0. Then h is exactly the same with respect to its usual basis for V as h^* is with respect to the basis

$$x_1, \ldots, x_r, y_1, \ldots, y_s, z_1, \ldots, z_s.$$

If we give $\mathbb{R}^r \times \mathbb{C}^s$ the volume form associated to this basis, then

$$\mathrm{Vol}(h^*(\mathcal{O}_L)) = \mathrm{Vol}(h(\mathcal{O}_L)) = 2^{-s}\sqrt{\Delta(L/K)}.$$

In particular, $h^*(\mathcal{O}_L)$ is a full lattice in $\mathbb{R}^r \times \mathbb{C}^s$ (if it had $\mathbb{R}$-rank less than n, the volume would be 0).

The advantage of working with h^* is that ℓ is that if we denote as p_j projection onto the j-th coordinate (for $\mathbb{R}^r \times \mathbb{C}^s$). then

$$p_j(\ell(b)) = \log|p_j(h^*(b))|$$

for $1 \leq j \leq r$ and

$$p_j(\ell(b)) = 2\log|p_j(h^*(b))|$$

for $r+1 \leq j \leq r+s$.

We have already established that $h^*(\mathcal{O}_L)$ is a lattice so we should be able to find elements in it with certain properties. The idea roughly is this: we want to find a family of units u_i in $h^*(\mathcal{O}_L)$ for which we can control the ± sign of $\log|p_j(h^*(b))|$ for various j. We might hope that these units are linearly independent.

We will work with a region somewhat similar to the region we worked on when we were doing the finiteness of the class group. We define the region as follows. Let (t) be an $(r+s)$-tuple of positive numbers indexed as $(t)_i$. We define

$$\begin{aligned} Z_{(t)} :=& \{(x_1, \ldots, x_{s+r}) \in \mathbb{R}^r \times \mathbb{C}^s \mid |x_i| \leq (t)_i, 1 \leq i \leq r \\ & \text{and } |x_i|^2 \leq (t)_i \text{ for } r+1 \leq i \leq r+s\} \end{aligned}$$

The region $Z_{(t)}$ is just a cross product of regions in $\mathbb{R}$ and $\mathbb{C}$, specifically it is

$$[-(t)_1,(t)_1]\times\cdots\times[-(t)_r,(t)_r]$$
$$\times\{(x,y)\ \mid x^2+y^2\leq(t)_{r+1}^2\}\times\cdots\times\{(x,y)\ \mid x^2+y^2\leq(t)_{r+s}\}.$$

Thus,

$$\mathrm{Vol}(Z_{(t)})=2^r\pi^s t_1\cdots t_{r+s}$$