Math 531 Tom Tucker
NOTES FROM CLASS 11/17

Throughout, L is as usual degree n over $\mathbb{Q}$, $h : L \longrightarrow V$ is the usual embedding, r is the number of real places of L and $s = (n-r)/2$. Also, N is $\mathrm{N}_{L/\mathbb{Q}}$.

Question: Are there any nontrivial extensions of $\mathbb{Q}$ that don't ramify anywhere? Since $|\Delta(L/\mathbb{Q})|$ is a positive integer and the only positive integer that isn't divisible by any primes is 1, this is the same as asking whether or not there are any extensions with $|\Delta(L/\mathbb{Q})| = 1$. Now, recall that we know that every nonzero ideal $I \subseteq \mathcal{O}_L$ has norm equal to at least 1. Looking at the Minkowski bound, we know that any ideal class contains an ideal with norm at most

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(L/\mathbb{Q})} > 1,$$

which means that

$$\sqrt{\Delta(L/\mathbb{Q})} > \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s.$$

Since $2s+r = n$ for some integer $r \geq 0$, we know that $s \leq [n/2]$ (where $[\cdot]$ is the greatest integer function). Now, we can write

$$\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s > \frac{n^{[n/2]}}{[n/2]!}(3/4)^{[n/2]} > 2^{[n/2]}(3/4)^{[n/2]} > 1,$$

for $n \geq 2$, so for $L \neq \mathbb{Q}$, we have

$$\sqrt{\Delta(L/\mathbb{Q})} > 1$$

so there is some p dividing $\sqrt{\Delta(L/\mathbb{Q})}$, so L ramifies at some prime. On the other hand, many quadratic fields do have unramified extensions. In fact, $\mathbb{Q}[\sqrt{d}]$ for square-free d has an unramified extension whenever d is composite (see homework).

****

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 $\frac{\mathrm{N}(y)}{y} \in \mathcal{O}_L$. $\square$

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

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

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

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

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. $\square$

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.

We'll do the inductive step next time. □