Math 568 Tom Tucker
NOTES FROM CLASS 11/24

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 $\mathrm{N}_{L/\mathbb{Q}}$.

Recall from earlier:

Proposition 30.1.

$$\mathrm{Vol}(X_t) = \frac{2^{r-s}\pi^s t^n}{n!}.$$

Proof. The proof of this is in the book on p. 66. The last step in the calculation is integration by parts, which the book neglects to mention. □

Lemma 30.2. *Let U be any bounded region of V and let $\mathcal{L}$ be a full lattice in V. Then $\mathcal{L} \cap U$ is finite.*

Proof. Let $w_1, \ldots, w_n$ be a basis for $\mathcal{L}$ and let $x_1, \ldots, x_n$ be the basis for V that gives the volume form. If M is the matrix given by $Mx_i = w_i$, then for any integers m_i we have

$$|\sum_{i=1}^n m_i w_i|^2 = |M(\sum_{i=1}^n m_i x_i)|^2 \geq \sum_{i=1}^n m_i^2 \|M\|_{\mathrm{inf}}^2$$

where $\|M\|_{\mathrm{inf}}$ is the minimum value of $|M(y)|$ for y on the unit sphere centered at the origin (which is nonzero). For any constant C there are finitely many integers m_i such that

$$\sum_{i=1}^n m_i^2 \|M\|_{\mathrm{inf}}^2 \leq C^2$$

so there are finitely many elements of λ in the sphere of radius C centered at the origin. Any bounded region is contained in such a sphere, so we are done. □

Now we can prove the famous Minkowski bound.

Theorem 30.3. *Let I be a nonzero fractional ideal of $\mathcal{O}_L$. Then there exists $a \neq 0$ such that*

$$|\,\mathrm{N}_{L/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}_{L/\mathbb{Q}}(I).$$

Proof. We want to choose X_t to which we can apply Minkowski's theorem and produce an element of $X_t \cap h(I)$. Recall that

$$\mathrm{Vol}(h(I)) = \frac{1}{2^s}\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I),$$

so we need t with

$$\frac{2^{r-s}\pi^s t^n}{n!} > 2^n \frac{1}{2^s}\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I),$$

which is equivalent to

$$t > \sqrt[n]{n!\frac{1}{\pi^s}2^{n-s-r+s}\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I)} = \sqrt[n]{n!\left(\frac{4}{\pi}\right)^s\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I)},$$

so let

$$C := \sqrt[n]{n!\left(\frac{4}{\pi}\right)^s\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I)}.$$

Then $\mathrm{Vol}(X_{C+\epsilon}) > \mathrm{Vol}(h(I))$ for any $\epsilon > 0$. It follows that $X_{C+\epsilon} \cap h(I) \neq 0$ by Minkowski's theorem. If

$$X_{C+\epsilon} \cap h(I) = X_C \cap h(I),$$

then $X_C \cap h(I) \neq 0$. Otherwise, let $\epsilon' > 0$ be the smallest number such that

$$X_{C+\epsilon} \cap h(I) \neq X_C \cap h(I).$$

Such a number exists since $X_{C+\epsilon} \cap h(I)$ is finite and any finite nonempty set has a minimal element. Taking $0 < \delta < \epsilon'$, we see that

$$X_C \cap h(I) = X_{C+\delta} \cap h(I) \neq 0,$$

so there is a nonzero element $a \in X_C \cap h(I)$. From earlier work, we see that

$$N(a) \leq (C/n)^n = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\mathrm{N}(I).$$

□

Let's do an easy lemma.

Lemma 30.4. *Let I be a fractional ideal of a Dedekind domain A and let $a \neq 0$ be in I. Then $aI^{-1} \subseteq A$.*

Proof. Since $Aa \subseteq I$, we have

$$I^{-1}Aa \subseteq II^{-1} = A.$$

□

Theorem 30.5. *Let $I \subset \mathcal{O}_L$ be any fractional ideal of $\mathcal{O}_L$. Then there exists an ideal $J \subset \mathcal{O}_L$ in the same ideal class as I such that*

$$|\,\mathrm{N}_{L/\mathbb{Q}}(J))| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}.$$

Proof. Applying the previous theorem to I^{-1}, we find that there is an element $a \in I^{-1}$ such that

$$|\operatorname{N}_{L/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\operatorname{N}(I)^{-1}.$$

Let $J = aI$. Since $a \in I^{-1}$, we see that

$$aI = a(I^{-1})^{-1} \subset \mathcal{O}_L.$$

We also have

$$\operatorname{N}(aI) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})}\,\operatorname{N}(I)^{-1}N(I) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{\Delta(\mathcal{O}_L/\mathbb{Z})},$$

so we are done. □

Example 30.6. $|\operatorname{Cl}(\mathbb{Z}[\frac{\sqrt{-43}+1}{2}])| = 1$. Plugging into the Minkowski bound, we get

$$(1/2)(4/\pi)\sqrt{43} \leq (1/2)(4/3)7 < 5,$$

so we only need to look at 2 and 3. The minimal polynomial for

$$\omega = \frac{\sqrt{-43}+1}{2}$$

is $x^2 - x + 11$. Over 2, we get:

$$x^2 - x + 11 \equiv x^2 - x + 1 \pmod 2$$

which is irreducible, so $2\mathbb{Z}[\omega]$ is prime. Over 3, we get

$$x^2 - x + 11 \equiv x^2 - x + 2 \pmod 3$$

which has no roots (try 0,1,2) in $\mathbb{Z}/3\mathbb{Z}$, so is irreducible. Thus, $3\mathbb{Z}[\omega]$ is prime and principal. Now, we're done.

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 later).