Math 430 Tom Tucker
NOTES FROM CLASS 11/15

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).

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 $b \in \mathcal{O}_L \setminus 0$, we define

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

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

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

The kernel of ℓ turns out to be roots of unity.

It turns out that $\ell(\mathcal{O}_L^*)$ is a sublattice in $\mathbb{R}^{r+s}$ that is a full lattice in the subspace H of $\mathbb{R}^{r+s}$ consisting of all $(x_1, \ldots, x_{r+s})$ such that $x_1 + \cdots + x_{r+s} = 0$. This gives the Dirichlet unit theorem.

Theorem 21.1 (Dirichlet Unit Theorem)**.** *Let μ_L be the roots of unity in L. There exist elements $v_1, \ldots, v_{r+s-1} \in \mathcal{O}_L^*$ such that every unit $u \in \mathcal{O}_L^*$ can be written uniquely as*

$$u = v v_1^{m_1} \cdots v_{r+s-1}^{m_{r+s-1}}$$

for $v \in \mu_L$ and $m_i \in \mathbb{Z}$.

Here's a link to a nice discussion of Hensel's Lemma. Note that this is only done over $\mathbb{Q}_p$ not over general closed fields with respect to ultrametrics. Also note that $\mathbb{Z}_p$ means the set of all z in $\mathbb{Q}_p$ such that $|z|_p \leq 1$. Alternatively it can be thought of as the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

`https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`