Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Hilbert Class Field

Reference. Milne, Introduction; Neukirch, VI.6.

Recall that the field $\mathbb{Q}$ has no extensions which are everywhere unramified (Minkowski's theorem from last semester, which we used in proving the Kronecker-Weber theorem). This is quite definitely not true of other number fields; we begin with an example illustrating this.

In the number field $K = \mathbb{Q}(\sqrt{-5})$, the ring of integers is $\mathbb{Z}[\sqrt{-5}]$ and the ideal (2) factors as $\mathfrak{p}^2$, where the ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$ is not principal.

Now let's see what happens when we adjoin a square root of -1, obtaining $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. The extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ only ramifies over 2, so $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})/K$ can only be ramified over $\mathfrak{p}$. Moreover, in $K_\mathfrak{p}$, $-1 \equiv (2+\sqrt{-5})^2 \pmod 8$, so -1 is a square in $K_\mathfrak{p}$. Thus L/K is also unramified over $\mathfrak{p}$!

We've now seen that $\mathbb{Q}(\sqrt{-5})$ admits both a nonprincipal ideal and an unramified abelian extension. It turns out these are not unrelated events. Caution: until further notice, the phrase "L/K is unramified" will mean that L/K is unramified over all finite places in the usual sense, *and* that every real embedding of K extends to a real embedding of L. (Get used to this. The real and complex embeddings of a number field will be treated like primes throughout the course.)

Theorem 1. *Let L be the maximal unramified abelian extension of a number field K. Then L/K is finite, and its Galois group is isomorphic to the ideal class group of K.*

In fact, there is a canonical isomorphism, given by the Artin reciprocity law. We'll see this a bit later. The field L is called the *Hilbert class field* of K.

Warning: there can be infinite unramified *nonabelian* extensions. In fact, Golod and Shafarevich used unramified abelian extensions to construct these! Namely, starting from a number field $K = K_0$, let K_1 be the Hilbert class field of K_0, let K_2 be the Hilbert class field of K_1, and so on. Then K_i is a unramified but not necessarily abelian extension of K_0, and for a suitable choice of K_0, $[K_i : K_0]$ can be unbounded.

Exercises.

1. Let K be an imaginary quadratic extension of $\mathbb{Q}$ in which t finite primes ramify. Prove that $\#(\mathrm{Cl}(K)/2\,\mathrm{Cl}(K)) = 2^{t-1}$, assuming Theorem 1. (Hint: if an odd prime p ramifies in K, show that $K(\sqrt{p})/K$ is unramified; if 2 ramifies in K, show that $K(\sqrt{-1})/K$ is unramified.) This was first proved by Gauss using binary quadratic forms, as alluded to last semester.

2. Give an example, using a real quadratic field, to illustrate that

   (a) Theorem 1 fails if we don't require the extensions to be unramified above the real place;

   (b) The previous exercise fails for real quadratic fields.

(Hint: see the hint for the previous exercise.) Optional: prove that the previous exercise works if you replace the class group by the *narrow class group*, in which you only mod out by principal ideals having a totally positive generator. This gives an example of a *ray class group*; more on those next time.

3. The field $\mathbb{Q}(\sqrt{-23})$ admits an ideal of order 3 in the class group and an unramified abelian extension of degree 3. Find both; feel free to use a computer if that helps. (Hint: the extension contains a cubic field of discriminant -23.)