Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Generalized Ideal Class Groups and the Artin Reciprocity Law

Reference. Milne V.1; Neukirch VI.6.

An example (continued from last time).

Before proceeding to generalized ideal class groups, we continue a bit with the example from last time to illustrate what is about to happen. Let $K = \mathbb{Q}(\sqrt{-5})$ and let $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$; recall that L/K is unramified everywhere. (Corrected proof that L is unramified above $(2, 1+\sqrt{-5})$; write $L = K(\alpha)$ where $\alpha = (1+\sqrt{5})/2$. Modulo $(2, 1+\sqrt{-5})$, the minimal polynomial $x^2 - x - 1$ of α is irreducible. So $(2, 1+\sqrt{-5})$ does not ramify and also does not split.)

Theorem 1. *Let $\mathfrak{p}$ be a prime of $\mathfrak{o}_K$. Then $\mathfrak{p}$ splits in L if and only if $\mathfrak{p}$ is principal.*

Proof. First suppose $\mathfrak{p} = (p)$, where $p \neq 2, 5$ is a rational prime that remains inert (does not split and is not ramified) in K. This happens if and only if -5 is not a square mod p. In this case, one of -1 and 5 is a square in $\mathbb{F}_p$, so $\mathfrak{o}_K/\mathfrak{p}$ contains a square root of one of them, hence of both (since -5 already has a square root there). Thus the residue field does not grow when we pass to L, that is, $\mathfrak{p}$ is split.

Next suppose $p \neq 2, 5$ is a rational prime that splits as $\mathfrak{p}\overline{\mathfrak{p}}$. If $\mathfrak{p} = (\beta)$ is principal, then the equation $x^2 + 5y^2 = p$ has a solution in $\mathbb{Z}$ (namely, for $x + y\sqrt{-5} = \beta$), but this is only possible if $p \equiv 1 \pmod 4$. Then p splits in $\mathbb{Q}(\sqrt{-1})$ as well, so p is totally split in L, so $\mathfrak{p}$ splits in L.

Conversely, suppose $\mathfrak{p}$ is not principal. Since there are only two ideal classes in $\mathbb{Q}(\sqrt{-5})$, we have $\mathfrak{p} = \alpha(2, 1+\sqrt{-5})$ for some $\alpha \in K$. Thus $\mathrm{Norm}(\mathfrak{p}) = |\mathrm{Norm}(\alpha)|\,\mathrm{Norm}(2, 1+\sqrt{-5})$. If $\alpha = x + y\sqrt{-5}$ for $x, y \in \mathbb{Q}$, we then have $p = 2(x^2 + 5y^2)$. Considering things mod 2, we see that $2x$ and $2y$ must be odd integers, and $p \equiv 3 \pmod 4$. Thus p does not split in L, so $\mathfrak{p}$ cannot split in L.

The only cases left are $\mathfrak{p} = (2, 1+\sqrt{-5})$, which does not split (see above), and $\mathfrak{p} = (\sqrt{-5})$, which does split (since -1 has a square root mod 5). $\square$

Bonus aside: for any ideal $\mathfrak{a}$ of $\mathfrak{o}_K$, $\mathfrak{a}\mathfrak{o}_L$ is principal. (It suffices to verify that $(2, 1+\sqrt{-5})\mathfrak{o}_L = (1+\sqrt{-1})\mathfrak{o}_L$.) This is a special case of the "capitulation" theorem; we'll come back to this a bit later.

Generalized ideal class groups.

In this section, we formulate (without proof) the Artin reciprocity law for an arbitrary abelian extension L/K of number fields. This map will generalize the canonical isomorphism, in the case $K = \mathbb{Q}$, of $\mathrm{Gal}(L/\mathbb{Q})$ with a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ for some m, as well as the splitting behavior we saw in the previous example. Before proceeding, we need to define the appropriate generalization of $(\mathbb{Z}/m\mathbb{Z})^*$ to number fields.

Recall that the ideal class group of K is defined as the group of fractional ideals modulo the subgroup of principal fractional ideals. Let $\mathfrak{m}$ be a formal product of places of K; you may regard such a beast as an ordinary integral ideal together with a nonnegative coefficient for each infinite place. Let $I_K^{\mathfrak{m}}$ be the group of fractional ideals of K which are coprime to each finite place of K. Let $P_K^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$ be the group of principal fractional ideals generated by elements $\alpha \in K$ such that:

- for $\mathfrak{p}^e | \mathfrak{m}$ finite, $\alpha \equiv 1 \pmod{\mathfrak{p}^e}$;
- for every real place τ in $\mathfrak{m}$, $\tau(\alpha) > 0$.

(There is no condition for complex places.) Then the *ray class group* $\mathrm{Cl}_K^{\mathfrak{m}}$ is defined as the quotient $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$. A quotient of a ray class group is called a *generalized ideal class group.*

The Artin reciprocity law.

Now let L/K be a (finite) abelian extension of number fields. We imitate the "reciprocity law" construction we made for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, but this time with no *a priori* reason to expect it to give anything useful. For each prime $\mathfrak{p}$ of K that does not ramify in L, let $\mathfrak{q}$ be a prime of L above K, and put $\kappa = \mathfrak{o}_K/\mathfrak{p}$ and $\lambda = \mathfrak{o}_L/\mathfrak{q}$. Then the residue field extension λ/κ is an extension of finite fields, so it has a canonical generator σ, the Frobenius, which acts by raising to the q-th power. (Here $q = \mathrm{Norm}(\mathfrak{p}) = \#\kappa$ is the absolute norm of $\mathfrak{p}$.) Since $\mathfrak{p}$ does not ramify, the decomposition group $G_{\mathfrak{q}}$ is isomorphic to $\mathrm{Gal}(\lambda/\kappa)$, so we get a canonical element of $G_{\mathfrak{q}}$, called the Frobenius of $\mathfrak{q}$. In general, replacing $\mathfrak{q}$ by $\mathfrak{q}^\tau$ for some $\tau \in \mathrm{Gal}(L/K)$ conjugates both the decomposition group and the Frobenius by τ; since L/K is abelian in our case, that conjugation has no effect. Thus we may speak of "the Frobenius of $\mathfrak{p}$" without ambiguity.

Now for $\mathfrak{m}$ divisible by all primes of K which ramify in L, define a homomorphism (the Artin map)

$$I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K) \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}\,.$$

(Aside: the fact that we have to avoid the ramified primes will be a bit of a nuisance later. Eventually we'll get around this using the adelic formulation.) Then the following miracle occurs.

Theorem 2 (Artin reciprocity). *There exists a formal product $\mathfrak{m}$ of places of K, including all (finite and infinite) places over which L ramifies, such that $P_K^{\mathfrak{m}}$ belongs to the kernel of the above homomorphism.*

In particular, we get a map $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ which turns out to be surjective (see exercises). Only now, we don't have the Kronecker-Weber theorem to explain it.

Define the *conductor* of L/K to be the smallest formal product $\mathfrak{m}$ for which the conclusion of the Artin reciprocity law holds. We say L/K is the *ray class field* corresponding to the product $\mathfrak{m}$ if L/K has conductor dividing $\mathfrak{m}$ and the map $I_K/I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is an isomorphism.

Theorem 3 (Existence of ray class fields). *Every formal product $\mathfrak{m}$ has a ray class field.*

For example, the ray class field of $\mathbb{Q}$ of conductor $m\infty$ is $\mathbb{Q}(\zeta_m)$; the ray class field of $\mathbb{Q}$ of conductor m is the maximal real subfield of $\mathbb{Q}(\zeta_m)$.

Unfortunately, for number fields other than $\mathbb{Q}$, we do not have an explicit description of the ray class fields as being generated by particular algebraic numbers. (A salient exception is the imaginary quadratic fields, for which the theory of elliptic curves with complex multiplication provides such numbers. Also, if we were to work with function fields instead of number fields, the theory of Drinfeld modules would do something similar.) This gap in our knowledge, also referred to as Hilbert's 12th Problem, will make establishing class field theory somewhat more complicated than it would be otherwise.

Exercises.

1. For $\mathfrak{p}$ a prime ideal of K and L/K an abelian extension in which $\mathfrak{p}$ does not ramify, let $\mathrm{Frob}_{L/K}(\mathfrak{p}) \in \mathrm{Gal}(L/K)$ be the Frobenius of $\mathfrak{p}$. Prove that Frobenius obeys the following compatibilities:

   (a) if M/L is another extension with M/K abelian, $\mathfrak{q}$ is a prime of L over $\mathfrak{p}$, and M/L is unramified over $\mathfrak{q}$, then $\mathrm{Frob}_{M/K}(\mathfrak{p})$ restricted to L equals $\mathrm{Frob}_{L/K}(\mathfrak{p})$.

   (b) with notation as in (a), $\mathrm{Frob}_{M/L}(\mathfrak{q}) = \mathrm{Frob}_{M/K}(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}$, where f denotes the residue field degree.

2. Find a formula for the order of $\mathrm{Cl}_{\mathfrak{m}}(K)$ in terms of the order of $\mathrm{Cl}(K)$ and other relevant stuff. (Hint: it's in Milne V.1. Make sure you understand its proof!) Then use that formula to give a formula for the order of $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}(\sqrt{D}))$ for D odd and squarefree, in terms of the prime factors of $\mathfrak{m}$ and D and the class number of $\mathbb{Q}(\sqrt{D})$.

3. Show that the homomorphism $I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective. You may assume the following fact: if L/K is an extension of number fields (with $L \neq K$), there exists a prime of K which does not split completely in L.

4. Find the ray class field of $\mathbb{Q}(i)$ of conductor (3), and verify Artin reciprocity explicitly in this case.