Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Cohomology of the Ideles 1: The "First Inequality"

Reference. Milne VII.2-VII.4; Neukirch VI.3; but see below about Neukirch.

By analogy with local class field theory, we want to prove that for K, L number fields and C_K, C_L their idele class groups,

$$H^1(\mathrm{Gal}(L/K), C_L) = 1, \qquad H^2(\mathrm{Gal}(L/K), C_L) = \mathbb{Z}/[L:K]\mathbb{Z}.$$

In this section, we'll look at the special case L/K cyclic, and prove that

$$\# H^0_T(\mathrm{Gal}(L/K), C_L)/\# H^1_T(\mathrm{Gal}(L/K), C_L) = [L:K].$$

That is, the Herbrand quotient of C_L is $[L:K]$. As we'll see, this will end up reducing to looking at units in a real vector space, much as we did last term to prove Dirichlet's units theorem.

This will imply the "First Inequality": for L/K cyclic,

$$\# H^0_T(\mathrm{Gal}(L/K), C_L) \geq [L:K].$$

The "Second Inequality" will be the reverse, which will be a bit more subtle.

Some basic observations. But first, some general observations. Put $G = \mathrm{Gal}(L/K)$.

Proposition 1. *For each $i > 0$, $H^i(G, I_L) = \sum_v H^i(G_v, L_v^*)$. For each i, $H^i_T(G, I_L) = \sum_v H^i_T(G_v, L_v^*)$.*

Proof. For any finite set S of places of K containing all infinite places and all ramified primes, let $I_{L,S}$ be the set of ideles with a unit at each component other than at the places dividing any places S. Note that $I_{L,S}$ is stable under G (because we defined it in terms of places of K, not L). By definition, I_L is the direct limit of the $I_{L,S}$ over all S, so $H^i(G, I_L)$ is the direct limit of the $H^i(G, I_{L,S})$. The latter is the product of $H^i(G, \prod_{w|v} L_w^*)$ over all $v \in S$ and $H^i(G, \prod_{w|v} \mathfrak{o}_{L_w}^*)$ over all $v \notin S$, but the latter is trivial because $v \notin S$ cannot ramify. By Shapiro's lemma, $H^i(G, \prod_{w|v} L_w^*) = H^i(G_v, L_w^*)$, so we have what we want. The argument for Tate groups is analogous. ☐

Notice what this says for $i = 0$ on the Tate groups: an idele is a norm if and only if each component is a norm. Obvious, perhaps, but useful.

In particular,

$$H^1(G, I_L) = 0, \qquad H^2(G, I_L) = \oplus_v \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

One other thing I should have mentioned earlier: if S contains all infinite places and all ramified places, then

$$\mathrm{Norm}_{L/K} I_{L,S} = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathfrak{o}_{K_v}^*$$

where U_v is open in K_v^*. The group on the right is open in I_K, so $\mathrm{Norm}_{L/K} I_K$ is open.

By quotienting down to C_K, we see that $\mathrm{Norm}_{L/K} C_K$ is open. In fact, the snake lemma on the diagram

$$\begin{tikzcd}
0 \arrow[r] & L^* \arrow[r] \arrow[d, "\mathrm{Norm}_{L/K}"] & I_L \arrow[r] \arrow[d, "\mathrm{Norm}_{L/K}"] & C_L \arrow[r] \arrow[d, "\mathrm{Norm}_{L/K}"] & 0 \\
0 \arrow[r] & K^* \arrow[r] & I_K \arrow[r] & C_K \arrow[r] & 0
\end{tikzcd}$$

implies that the quotient $I_K/(K^* \times \mathrm{Norm}_{L/K} I_L)$ is isomorphic to C_K.

Cohomology of the units.

Remember, we're going to be assuming $G = \mathrm{Gal}(L/K)$ until further notice, so that we may use periodicity of the Tate groups, and the Herbrand quotient.

First of all, working with I_L all at once is a bit unwieldy; we'd rather work with $I_{L,S}$ for some finite set S. In fact, we can choose S to make our lives easier: we choose S containing all infinite places, and all ramified primes, and perhaps some extra primes so that

$$I_L = I_{L,S} L^*.$$

The reason I can do this is the same as my "cheating" proof that C_L^0 is compact: it's enough to make sure S contains a set of primes that generate the ideal class group of L, so then I can move a generator of any other prime to some stuff in S times units.

Put $L_S = L^* \cap I_{L,S}$; that is, L_S is the group of S-units in L. From the exact sequence

$$1 \to L_S \to I_{L,S} \to I_{L,S}/L_S = C_L \to 1$$

we have, in case L/K is cyclic, an equality of Herbrand quotients

$$h(C_L) = h(I_{L,S})/h(L_S).$$

From the computation we did of $H^i(G, I_{L,S})$, it's easy to read off its Herbrand quotient:

$$h(I_{L,S}) = \prod_{v \in S} \# H_T^0(G_v, L_w^*) = \prod_{v \in S} [L_w : K_v].$$

So to get $h(C_L) = [L : K]$, we need

$$h(L_S) = \frac{1}{[L : K]} \prod_{v \in S} [L_w : K_v].$$

This will in fact be true even if we only assume S contains all infinite places, as we now check.

Let T be the set of places of L dividing the places of S. Let V be the real vector space consisting of one copy of $\mathbb{R}$ for each place in T. Define the map $L_S \to V$ by sending

$$\alpha \to \prod_w \log |\alpha|_w,$$

with the caveat that the norm at a complex place is the *square* of the usual absolute value; the kernel of this map consists solely of roots of unity. Let M be the quotient of L_S by the group of roots of unity; since the latter is finite, $h(M) = h(L_S)$. Let $H \subset V$ be the hyperplane of vectors with sum of coordinates 0; by the product formula, M maps into H. As noted earlier, in fact M is a discrete subgroup of H of rank equal to the dimension of H; that is, M is a lattice in H. Moreover, we have an action of G on V compatible with the embedding of M; namely, G acts on the places in T, so acts on V by permuting the coordinates.

Caveat. There seems to be an error in Neukirch's derivation at this point. Namely, his Lemma VI.3.4 is only proved assuming that G acts transitively on the coordinates of V; but in the above situation, this is not the case: G permutes the places above any given place v of K but those are separate orbits. So we'll follow Milne instead.

We can write down two natural lattices in V. One of them is the lattice generated by M together with the all-ones vector, on which G acts trivially. As a G-module, the Herbrand quotient of that lattice is $h(M)h(\mathbb{Z}) = [L : K]h(M)$. The other is the lattice M' in which, in the given coordinate system, each element has integral coordinates. To compute its Herbrand quotient, notice that the projection of this lattice onto the coordinates corresponding to the places w above some v form a copy of $\operatorname{Ind}_{G_v}^G \mathbb{Z}$. Thus

$$h(G, M') = \prod_v h(G, \operatorname{Ind}_{G_v}^G \mathbb{Z}) = \prod_v h(G_v, \mathbb{Z}) = \prod_v \#G_v = \prod_v [L_w : K_v].$$

So all that remains is to prove the following.

Lemma 2. *Let V be a real vector space on which a finite group G acts linearly, and let L_1 and L_2 be G-stable lattices in V for which $h(L_1)$ and $h(L_2)$ are both defined. Then $h(L_1) = h(L_2)$.*

In fact, one can show that if one of the Herbrand quotients is defined, so is the other.

Proof. We first show that $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as $\mathbb{Q}[G]$-modules. We are given that $L_1 \otimes_{\mathbb{Z}} \mathbb{R}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{R}$ are isomorphic as $\mathbb{R}[G]$-modules. That is, the real vector space $W = \operatorname{Hom}(L_1 \otimes_{\mathbb{Z}} \mathbb{R}, L_2 \otimes_{\mathbb{Z}} \mathbb{R})$, on which G acts, contains an invariant vector which, as a linear transformation, is invertible. Now W can also be written as

$$\operatorname{Hom}(L_1, L_2) \otimes_{\mathbb{Z}} \mathbb{R};$$

that is, $\operatorname{Hom}(L_1, L_2)$ sits inside as a sublattice. The fact that W has an invariant vector says that a certain set of linear equations has a nonzero solution over $\mathbb{R}$, namely the equations that express the fact that the action of G leaves the vector invariant. But those equations have coefficients in $\mathbb{Q}$, so there must already be invariant vectors over $\mathbb{Q}$. Moreover, if we fix an isomorphism (not G-equivariant) between $L_2 \otimes_{\mathbb{Z}} \mathbb{R}$ and $L_1 \otimes_{\mathbb{Z}} \mathbb{R}$, we can compose this with any element of W to get a map from L_1 to itself, which has a determinant; and by hypothesis, there is some invariant vector of W whose "determinant" is nonzero. Thus the determinant doesn't vanish identically on the set of invariant vectors in W, so it also doesn't vanish identically on the set of invariant vectors in $\operatorname{Hom}(L_1, L_2) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Thus there is a G-equivariant isomorphism between $L_1 \otimes_{\mathbb{Z}} \mathbb{Q}$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{Q}$; that is, L_1 is isomorphic to a sublattice of L_2. Since a lattice has the same Herbrand quotient as any sublattice (the quotient is finite, so its Herbrand quotient is 1), that means $h(L_1) = h(L_2)$. $\square$

Aside. The calculation we've made is enough to prove that in any nontrivial extension L/K of number fields, infinitely many primes must fail to split completely. In fact, it suffices to do this for L/K cyclic; in that case, if all but finitely many primes split completely, we can put the remaining primes into S and deduce that $C_K = \mathrm{Norm}_{L/K} C_L$, whereas the above calculation forces $H^0_T(\mathrm{Gal}(L/K), C_L) \geq [L : K]$, contradiction. See Neukirch, Corollary VI.3.8 for more details.