Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Cohomology of the Ideles 2: The "Second Inequality"

Reference. Milne VII.5; Neukirch VI.4.

We proved last time that for L/K a cyclic extension of number fields, the Herbrand quotient $h(C_L)$ of the idele class group of L is equal to $[L : K]$. This time we'll prove the following.

Theorem 1. *Let L/K be a Galois extension of number fields, with Galois group G. Then*

(a) the group $I_K/(K^* \operatorname{Norm}_{L/K} I_L)$ is finite of order at most $[L : K]$;

(b) the group $H^1(G, C_L)$ is trivial;

(c) the group $H^2(G, C_L)$ is finite of order at most $[L : K]$.

By the first inequality, for L/K cyclic, these three are equivalent and all imply that $H^2(G, C_L)$ has order exactly $[L : K]$. That would suffice to prove the "class field axiom" in Neukirch's setup.

There are two basic ways to prove this result: an analytic proof and an algebraic proof. Although the analytic proof is somewhat afield of what we have been doing (it requires some properties of zeta functions that we haven't worked out), it's somewhat simpler overall than the algebraic proof. So we'll sketch it first before proceeding to the algebraic proof.

The analytic proof.

For the analytic proof, we need to recast the Second Inequality back into classical, ideal-theoretic language. Let L/K be a finite Galois extension and $\mathfrak{m}$ a formal product of places of K. Back when we defined generalized ideal class groups, we defined the group $I_\mathfrak{m}$ of fractional ideals of K coprime to $\mathfrak{m}$ and $P_\mathfrak{m}$ the group of principal ideals admitting a generator α such that $\alpha \equiv 1 \pmod{\mathfrak{p}^e}$ if the prime power $\mathfrak{p}^e$ occurs in $\mathfrak{m}$ for a finite prime $\mathfrak{p}$, and $\tau(\alpha) > 0$ if τ is the real embedding corresponding to a real place in $\mathfrak{m}$. Also, let $J_\mathfrak{m}$ be the group of fractional ideals of L coprime to $\mathfrak{m}$. Then the Second Inequality states that

$$\# I_\mathfrak{m}/P_\mathfrak{m} \operatorname{Norm}_{L/K} J_\mathfrak{m} \leq [L : K].$$

Note that we don't have to assume $\mathfrak{m}$ is divisible by the ramified primes of L/K.

We'll need the following special case of the Chebotarev density theorem, which fortunately we can prove without already having all of class field theory.

Proposition 2. *Let L be a finite extension of K and let M/K be its Galois closure. Then the set S of prime ideals of K that split completely in L has Dirichlet density $1/[M : K]$.*

Proof. A prime of K splits completely in L if and only if it splits completely in M, so we may assume $L = M$ is Galois. Recall that the set T of unramfied primes $\mathfrak{q}$ of L of absolute degree 1 has Dirichlet density 1; each such prime lies over an unramified prime $\mathfrak{p}$ of K of absolute degree 1 which splits completely in L.

Now recall how the Dirichlet density works: the set T having Dirichlet density 1 means that

$$\sum_{\mathfrak{q}\in T} \frac{1}{\mathrm{Norm}(\mathfrak{q})^s} \sim \frac{1}{s-1} \qquad s \searrow 1$$

(s approaching 1 from above, that is). If we group the primes in T by which prime of S they lie over, then we get

$$[L:K] \sum_{\mathfrak{p}\in T} \frac{1}{\mathrm{Norm}(\mathfrak{p})^s} \sim \frac{1}{s-1}.$$

That is, the Dirichlet density of S is $1/[L:K]$. $\square$

Now for the inequality. For $\chi : I_{\mathfrak{m}}/P_{\mathfrak{m}} \to \mathbb{C}^*$ a character, we defined the L-function

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\,\mathrm{Norm}(\mathfrak{p})^{-s}}.$$

We'll use some properties of this function that were on a previous homework. For starters,

$$\log L(s,1) \sim \log \zeta_K(s) \sim \log \frac{1}{s-1} \qquad s \searrow 1,$$

while if χ is not the trivial character, $L(s,\chi)$ is holomorphic at $s=1$. If $L(s,\chi) = (s-1)^{m(\chi)}g(s)$ where g is holomorphic and nonvanishing at $s=1$, then $m(\chi)\geq 0$, and

$$\log L(s,\chi) \sim m(\chi)\log(s-1) = -m(\chi)\log\frac{1}{s-1}.$$

Let H be a subgroup of $I_{\mathfrak{m}}$ containing $P_{\mathfrak{m}}$. By finite Fourier analysis, or orthogonality of characters,

$$\sum_{\chi: I_{\mathfrak{m}}/H\to\mathbb{C}^*} \log L(s,\chi) \sim \#(I_{\mathfrak{m}}/H) \sum_{\mathfrak{p}\in H} \frac{1}{\mathrm{Norm}(\mathfrak{p})^{-s}}.$$

We conclude that the set of primes in H has Dirichlet density

$$\frac{1-\sum_{\chi\neq 1} m(\chi)}{\#(I_{\mathfrak{m}}/H)};$$

this is $1/\#(I_{\mathfrak{m}}/H)$ if the $m(\chi)$ are all zero, and 0 otherwise.

We apply this with $H = P_{\mathfrak{m}}\,\mathrm{Norm}_{L/K} J_{\mathfrak{m}}$. This in particular includes every prime of K that splits completely, since such a prime is the norm of any prime of L lying over it. Thus the set of primes in H has Dirichlet density, on one hand, is at least $1/[L:K]$. On the other hand, this set has density either zero or $1/\#(I_{\mathfrak{m}}/H)$. We conclude $\#I_{\mathfrak{m}}/H \leq [L:K]$, as desired.

The algebraic proof.

We now proceed to the algebraic proof of the Second Inequality. To prove the theorem in general, we can very quickly reduce to the case of L/K not just cyclic, but cyclic of prime order. The reductions are similar to those we used to compute $H^2(L^*)$ in the local case. First of all, if we have the theorem for all solvable groups, then if G is general and H is a Sylow p-subgroup of G, then for any G-module M,

$$\mathrm{Res} : H^r_T(G, M) \to H^r_T(H, M)$$

is injective on p-primary components (because $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $[G : H]$), so we can deduce the desired result. Thus it suffices to consider L/K solvable. In that case, starting from the cyclic of prime order case we can induct using the inflation-restriction exact sequence: if K'/K is a subextension and $H = \mathrm{Gal}(L/K')$, then

$$0 \to H^i(G/H, C_{K'}) \to H^i(G, C_L) \to H^i(H, C_L)$$

Upshot: we need only consider L/K cyclic of prime order p.

One more reduction to make things simpler: we reduce to the case where K contains a p-th root of unity. Let $K' = K(\zeta_p)$ and $L' = L(\zeta_p)$; then K' and L are linearly disjoint over K (since their degrees are coprime), so $[L' : K'] = [L : K] = p$ and the Galois groups of L/K and L'/K' are canonically isomorphic. It suffices to check that the homomorphism

$$H^0_T(\mathrm{Gal}(L/K), C_L) \to H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$$

induced by the inclusion $C_L \to C_{L'}$ is injective. These groups are both killed by multiplication by p, since for $x \in C_K$, $\mathrm{Norm}_{L/K} x = x^p$. Thus multiplication by $d = [K' : K]$, which divides $p - 1$, is an isomorphism on these groups. If $x \in C_K$ maps to the identity in $H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$, we can choose a representative of the same class as x in $H^0_T(\mathrm{Gal}(L/K), C_L)$ of the form y^d; then y also maps to the identity in $H^0_T(\mathrm{Gal}(L'/K'), C_{L'})$. That is, $y = \mathrm{Norm}_{L'/K'}(z')$ for some $z' \in C_{L'}$, and

$$y^d = \mathrm{Norm}_{K'/K}(y) = \mathrm{Norm}_{L'/K}(z') \in \mathrm{Norm}_{L/K} C_L.$$

Thus $x \in \mathrm{Norm}_{L/K} C_L$, so the homomorphism is injective.

The key case.

To sum up: it suffices to prove the theorem for K containing a p-th root of unity ζ_p and L/K cyclic of order p. We now address this case.

As in the proof of the First Inequality, we will use a set S of places of K containing the infinite places, the primes that ramify in L, and enough additional primes so that $I_K = I_{K,S}K^*$. Again, we put $K_S = I_{K,S} \cap K^*$. Also we write $s = \#S$.

The plan is to explicitly produce a subgroup of C_K of index $[L : K]$ consisting of norms from C_L. We do this by using an auxiliary set of places T disjoint from S. For such T, we define

$$J = \prod_{v \in S} (K_v^*)^n \times \prod_{v \in T} K_v^* \times \prod_{v \notin S \cup T} \mathfrak{o}_{K_v}^*.$$

Let $\Delta = (L^*)^p \cap K_S$. We will show that:

(a) $L = K(\Delta^{1/p})$.

(b) We can choose a set T of $s-1$ primes such that Δ is the kernel of the map $K_S \to \prod_{v \in T} K_v^*/(K_v^*)^n$.

(c) For such a set T, if we put $C_{K,S,T} = JK^*/K^*$, then

$$\# C_K / C_{K,S,T} = [L:K] = p.$$

(d) With the same notation, $C_{K,S,T} \subseteq \operatorname{Norm}_{L/K} C_L$.

That will imply $\# C_K / \operatorname{Norm}_{L/K} C_L \leq p$, as desired.

We first concentrate on (a). By Kummer theory, since K contains a primitive p-th root of unity, we can write $L = K(D^{1/p})$ for $D = (L^*)^p \cap K^*$. Thus $K(\Delta^{1/p}) \subseteq L$ and since there is no room between K and L for an extension ($[L:K]$ being prime), all that we have to check is that $\Delta \neq (K_S)^p$. Choose a single $x \in D$ such that $L = K(x^{1/p})$. For each $v \notin S$, the extension $K_v(x^{1/p})/K_v$ is unramified, so we can write x as a unit times a p-th power, say $x = u_v y_v^p$. If we put $y_v = 1$ for $v \in S$, we can assemble the y_v into an idele y, which by $I_K = K^* I_{K,S}$ we can rewrite as zw for $z \in K^*$ and $w \in I_{K,S}$. Now for $v \notin S$, $(x/z^p)_v = u_v / w_v^p \in \mathfrak{o}_{K_v}^*$. Thus $x/z^p \in (L^*)^p \cap K_S \in \Delta$ but $x \notin (K^*)^p$. We conclude $L = K(\Delta^{1/p})$.

Now we move to (b). Put $N = K(K_S^{1/p})$. By Kummer theory,

$$\operatorname{Gal}(N/K) \cong \operatorname{Hom}(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z}).$$

By the generalization of Dirichlet's units theorem to S-units, K_S modulo torsion is a free abelian group of rank $s-1$, and the torsion subgroup consists of roots of unity, so is cyclic of order divisible by p. Thus $K_S/K_S^p \cong (\mathbb{Z}/p\mathbb{Z})^s$. Choose generators $g_1, \dots, g_{s-1}$ of $\operatorname{Gal}(N/L)$; these correspond in $\operatorname{Hom}(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z})$ to a set of homomorphisms whose common kernel is precisely Δ/K_S^p.

So to establish (b), we need to find for each g_i a place v_i such that the kernel of g_i is the same as the kernel of $K_S \to K_v^*/(K_v^*)^p$. Let N_i be the fixed field of g_i; as noted last time, it follows from the First Inequality that there are infinitely many primes of N_i that do not split in N. So we can choose a place w_i of each N_i such that their restrictions v_i to K are distinct, not contained in S, and don't divide p.

We claim N_i is the maximal subextension of N/K in which v_i splits completely (a/k/a the "decomposition field" of v_i). On one hand, v_i does not split completely in N, so the decomposition field is no larger than N_i. On the other hand, the decomposition field is the fixed field of the decomposition group, which has exponent p and is cyclic (since v_i does not ramify in N). Thus it must have index p in N, so must be N_i itself.

Thus $L = \cap N_i$ is the maximal subextension of N in which all of the v_i split completely. We conclude that for $x \in K_S$, x belongs to Δ iff $K_{v_i}(x^{1/p}) = K_{v_i}$ for all i, which occurs iff $x \in K_{v_i}^p$. That is, Δ is precisely the kernel of the map $K_S \to \prod_i K_{v_i}^*/(K_{v_i}^*)^p$. In fact, under this map, K_S actually maps to the units in $K_{v_i}^*$ for each i.

Next, we verify (c), using the following lemma.

Lemma 3. $J \cap K^* = (K_{S\cup T})^p$.

Proof. Clearly $K_{S\cup T}^p \subseteq J \cap K^*$; we have to work to show the other inclusion. Take $y \in J \cap K^*$ and $M = K(y^{1/p})$. We'll show that $\operatorname{Norm}_{M/K} C_M = C_K$; by the First Inequality, this will imply $M = K$, so $y \in (K^*)^p \cap J = (K_{S\cup T})^p$.

Since $I_K = I_{K,S}K^*$, it is enough to choose $\alpha \in I_{K,S}$ and show that $\alpha/x \in \operatorname{Norm}_{L/K} I_M$ for some $x \in K^*$. As noted above, the map

$$K_S \to \prod_{v\in T} \mathfrak{o}_{K_v}^*/(\mathfrak{o}_{K_v}^*)^p$$

is surjective, and $\#K_S/\Delta = p^{s-1}$. That's also the order of the product, so the map is actually an isomorphism. Thus we can find $x \in K_S$ so that α/x has component the p-th power of a unit of K_v at each $v \in T$. In particular, such a component is the norm of its p-th root, so α/x is a norm at each $v \in T$. For $v \in S$, we don't have anything to check: because y is a p-th power at v, $M_w = K_v$. Finally, for $v \notin S \cup T$, M_w/K_v is unramified, so any unit is a norm. Thus α/x is indeed a norm. We conclude $\operatorname{Norm}_{M/K} C_M = C_K$, so $M = K$ and $y \in K_{S\cup T}^p$, as desired. $\square$

Given the lemma, we now have an exact sequence

$$1 \to I_{K,S\cup T} \cap K^*/J \cap K^* \to I_{K,S\cup T}/J \to I_{K,S\cup T}K^*/JK^* \to 1.$$

We can rewrite $I_{K,S\cup T}K^*$ as simply I_K. So the group on the right is precisely $C_K/C_{K,S,T}$. By the lemma, the group on the left is $K_{S\cup T}^*/(K_{S\cup T}^*)^n$, which has order p^{2s-1} because $K_{S\cup T}$ is free of rank $2s-2$ plus a cyclic group of order a multiple of p. And the group in the middle is the product of $K_v^*/(K_v^*)^p$ over all $v \in S$, and each of those has order p^2 (generated by ζ_p and a uniformizer of K_v). Adding it all up, we get $\#C_K/C_{K,S,T} = p$.

Finally, to check (d), it suffices to check that $J \subseteq \operatorname{Norm}_{L/K} I_L$, which we may check component by component. It's automatic for the places $v \notin S \cup T$, since those places are unramified, so every unit is a norm. For places $v \in S$, any element of $(K_v^*)^p$ is a norm from $K_v(K_v^{1/p})$ (see the proof of the local existence theorem), so also from L_w. Finally, for places $v \in T$, from the construction of T, we see that $\Delta \subseteq (K_v^*)^p$, so $L_w = K_v$, and so all of K_v^* are norms.

Aside. We get from this calculation that $H_T^{-1}(G, C_L) = 1$, so $H_T^0(G, L^*) \to H_T^0(G, C_L)$ is injective. That is,

$$K^*/\operatorname{Norm}_{L/K} L^* \to \oplus_v K_v^*/\operatorname{Norm}_{L_w/K_v} L_w^*$$

is injective. In other words, we have an interesting "local-to-global" statement, namely Hasse's Norm Theorem: if L/K is cyclic, $x \in K^*$ is a norm if and only if it is locally a norm.