Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Local Class Field Theory, via Tate's Theorem

For L/K a finite extension of local fields, we have now computed that $H^1(L/K) = 0$ and $H^2(L/K)$ is cyclic of order $[L : K]$. From this we want to deduce the existence of the local reciprocity map $\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ and the local existence theorem (every open subgroup of K^* of finite index is a group of norms). Recall that we're going to get this from a canonical isomorphism $K^*/\mathrm{Norm}_{L/K}(L^*) = H^0_T(L/K) \to \mathrm{Gal}(L/K)^{\mathrm{ab}} = H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z})$. This will follow from the following theorem.

Theorem 1 (Tate). *Let G be a finite (solvable) group and let M be a G-module. Suppose that for all subgroups H of G (including G itself), $H^1(H, M) = 0$ and $H^2(H, M)$ is cyclic of order $\#H$. Then there are isomorphisms $H^i_T(G, \mathbb{Z}) \to H^{i+2}_T(G, M)$ which are canonical up to a choice of generator of $H^2(G, M)$.*

Proof. Let γ be a generator of $H^2(G, M)$. Since $\mathrm{Cor} \circ \mathrm{Res} = [G : H]$, $\mathrm{Res}(\gamma)$ generates $H^2(H, M)$ for any H. We start out by "artificially" making a G-module containing M in which γ becomes a coboundary.

Choose a 2-cocycle $\phi : G^3 \to M$ representing γ; by the definition of a cocycle,

$$\phi(g_0 g, g_1 g, g_2 g) = \phi(g_0, g_1, g_2)^g, \qquad \phi(g_1, g_2, g_3) - \phi(g_0, g_2, g_3) + \phi(g_0, g_1, g_3) - \phi(g_0, g_1, g_2) = 0.$$

And ϕ is a coboundary if and only if it's of the form $d(\rho)$, that is, $\phi(g_0, g_1, g_2) = \rho(g_1, g_2) - \rho(g_0, g_2) + \rho(g_0, g_1)$. This ρ must itself be G-invariant: $\rho(g_0, g_1)^g = \rho(g_0 g, g_1 g)$. Thus ϕ is a coboundary if $\phi(e, g, hg) = \rho(e, h)^g - \rho(e, hg) + \rho(e, g)$.

Let $M[\phi]$ be the direct sum of M with the free abelian group with one generator x_g for each element g of $G - \{e\}$, with the G-action

$$x_h^g = x_{hg} - x_g + \phi(e, g, hg).$$

(The symbol x_e should be interpreted as $\phi(e, e, e)$.) One may verify that this is indeed a G-action; by construction, the cocycle ϕ becomes zero in $H^2(G, M[\phi])$ by setting $\rho(e, g) = x_g$. (Milne calls $M[\phi]$ the *splitting module* of ϕ.)

The map $\alpha : M[\phi] \to \mathbb{Z}[G]$ sending M to zero and x_g to $[g] - 1$ is a homomorphism of G-modules. Actually it maps into the augmentation ideal I_G, and the sequence

$$0 \to M \to M[\phi] \to I_G \to 0$$

is exact. For any subgroup H of G, we can restrict to H-modules, then take the long exact sequence:

$$0 = H^1(H, M) \to H^1(H, M[\phi]) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M[\phi]).$$

To make headway with this, view $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ as an exact sequence of H-modules. Since $\mathbb{Z}[G]$ is induced, its Tate groups all vanish. So we get a dimension shift:

$$H^1(H, I_G) \cong H^0_T(H, \mathbb{Z}) = \mathbb{Z}/\#H\mathbb{Z}.$$

Also, the map $H^2(H,M) \to H^2(H,M[\phi])$ is zero because we constructed this map so as to kill off the generator ϕ. Thus $H^1(H,I_G) \to H^2(H,M)$ is surjective. But these groups are both finite of the same order! So the map is also injective, and $H^1(H,M[\phi])$ is also zero.

Now apply the lemma below to conclude that $H^i_T(G,M) = 0$ for all H. This allows us to use the four-term exact sequence

$$0 \to M \to M[\phi] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

(as in the proof of periodicity for the Tate groups when G is cyclic) to conclude $H^i_T(G,\mathbb{Z}) \cong H^{i+2}_T(G,M)$. □

Note: we only need the results of this section for G solvable, because in our desired application G is the Galois group of a finite extension of local fields. But one can remove this restriction: see the note after this lemma.

Lemma 2. *Let G be a finite (solvable) group and M a G-module. Suppose that $H^i(H,M) = 0$ for $i = 1,2$ and H any subgroup of G (including G itself). Then $H^i_T(G,M) = 0$ for all $i \in \mathbb{Z}$.*

Caveat: there's a bug in Milne's proof of this (Theorem II.2.17); see below.

Proof. For G cyclic, this follows by periodicity. We prove the general result by induction on $\#G$. Since G is solvable, it has a subgroup H so that G/H is cyclic. By the induction hypothesis, $H^i_T(H,M) = 0$ for all i. Thus by the inflation-restriction exact sequence (see previous handout),

$$0 \to H^i(G/H, M^H) \to H^i(G,M) \to H^i(H,M)$$

is exact for all $i > 0$. The term on the end being zero, we have $H^i(G/H,M^H) \cong H^i(G,M) = 0$ for $i = 1,2$. By periodicity, $H^i_T(G/H,M^H) = 0$ for all i, so $H^i(G/H,M^H) = 0$ for all $i > 0$, and $H^i(G,M) = 0$ for $i > 0$. As for $H^0_T(G,M)$, we have that $H^0_T(G/H,M^H) = 0$, so for any $x \in M^G$, there exists $y \in M^H$ such that $\mathrm{Norm}_{G/H}(y) = x$. Since $H^0_T(H,M) = 0$, there exists $z \in M$ such that $\mathrm{Norm}_H(z) = x$. Now $\mathrm{Norm}_G(z) = \mathrm{Norm}_{G/H} \circ \mathrm{Norm}_H(z) = x$. Thus $H^0_T(G,M) = 0$, as desired.

So far so good, but we want to kill off the Tate groups with negative indices too, so we do dimension shifting. (This is where the bug in Milne is. He uses the wrong exact sequence, so his dimension shift goes in the wrong direction.) Make the exact sequence

$$0 \to N \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \to 0,$$

in which $m \otimes g$ maps to m^g. The term in the middle is acyclic, so $H^{i+1}_T(H',N) \cong H^i_T(H',M)$ for any subgroup H' of G. In particular, $H^1(H',N) = H^2(H',N) = 0$, so the above argument gives $H^i_T(G,N) = 0$ for $i \geq 0$. Now from $H^0_T(G,N) = 0$ we get $H^{-1}_T(G,M) = 0$; since the same argument applies to N, we also get $H^{-2}_T(G,M) = 0$ and so on. □

To go from the solvable case to the general case, you show that the p-primary component of $H^i(G, M)$ injects into $H^i(G_p, M)$, where G_p is the p-Sylow subgroup. (Apply $\mathrm{Cor} \circ \mathrm{Res}$ from G to G_p; the result is multiplication by $[G : H]$ which is prime to p.)

Making things explicit.

The case we want is the isomorphism $H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^0(L/K)$. If we have an explicit cocycle ϕ generating $H^2(L/K)$, we can trace through this argument and get the local reciprocity map! The result is kind of messy, though, so I won't torture with all of the details. The point is simply to observe that everything we've done can be used for explicit computations. (I think this observation is due to Dwork.) If you find this intractable, wait until we hit abstract class field theory: that point of view will give a different (though of course related) mechanism for computing the reciprocity map.

Put $G = \mathrm{Gal}(L/K)$. First recall that $G^{\mathrm{ab}} = H_T^{-2}(G, \mathbb{Z})$ is isomorphic to $H_T^{-1}(G, I_G) = I_G/I_G^2$, with $g \mapsto [g] - 1$. Next, use the exact sequence

$$0 \to M \to M[\phi] \to I_G \to 0$$

and apply the "snaking" construction: pull $[g] - 1$ back to $x_g \in M[\phi]$, take the norm to get $\prod_h x_g^h = \prod_h (x_{gh} x_h^{-1} \phi(e, h, gh))$ (switching to multiplicative notation). The x_{gh} and x_h term cancel out when you take the product, so we get $\prod_h \phi(e, h, gh) \in L^*$ as the inverse image of $g \in \mathrm{Gal}(L/K)$.

As noted above, one needs ϕ to make this truly explicit; one can get ϕ using explicit generators of L/K if you have them. For $K = \mathbb{Q}_p$, one can use roots of unity; for K general, one can use the Lubin-Tate construction. In general, one can at least do the following, imitating our proof that $H^2(L/K)$ is cyclic of order n. Let M/K be unramified of degree n; then $H^2(M/K) \to H^2(ML/K)$ is injective, and its image lies in the image of $H^2(L/K) \to H^2(ML/K)$.

Now $H^2(M/K)$ is isomorphic to $H_T^0(M/K) = K^*/\operatorname{Norm}_{M/K}(M^*)$ which is generated by a uniformizer $\pi \in K$. To "explicate" that isomorphism, we recall generally how to construct the isomorphism $H_T^0(G, M) \to H_T^2(G, M)$ for G cyclic with a distinguished generator g. Recall the exact sequence we used to produce the isomorphism:

$$0 \to M \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \to 0.$$

(Remember, G acts on both factors in $M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. The first map is $m \mapsto \sum_{h \in G} m \otimes [h]$, the second is $m \otimes [h] \mapsto m \otimes ([gh] - [h])$, and the third is $[h] \mapsto 1$.) Let $A = M \otimes_{\mathbb{Z}} I_G$ be the kernel of the third arrow, so $0 \to M \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A \to 0$ and $0 \to A \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \to 0$ are exact.

Given $x \in H_T^0(M/K) = M^G/\operatorname{Norm}_G(M)$, lift it to $x \otimes [1]$. Now view this as a 0-cochain $\phi_0 : G \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by $\phi_0(h) = x \otimes [h]$. Apply d to get a 1-cocycle:

$$\phi_1(h_0, h_1) = \phi_0(h_1) - \phi_0(h_0) = x \otimes ([h_1] - \otimes[h_0])$$

which actually takes values in A. Now snake again: pull this back to a 1-cochain $\psi_1 : G^2 \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by

$$\psi_1(g^i, g^{i+j}) = x \otimes ([g^i] + [g^{i+1}] + \cdots + [g^{j-1}])$$

for $i, j = 0, \ldots, \#G - 1$. Apply d again: now we have a 2-cocycle $\psi_2 : G^3 \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ given by (again for $i, j = 0, \ldots, \#G - 1$)

$$\begin{aligned}\psi_2(e, g^i, g^{i+j}) &= \psi_1(g^i, g^{i+j}) - \psi_1(e, g^{i+j}) + \psi_1(e, g^i) \\ &= x \otimes ([e] + \cdots + [g^{i-1}] + [g^i] + \cdots + [g^{i+j-1}] - [e] - \cdots - [g^{i+j-1}]) \\ &= \begin{cases} 0 & i + j < \#G \\ -x \otimes ([e] + \cdots + [g^{\#G-1}]) & i + j \geq \#G. \end{cases}\end{aligned}$$

This pulls back to a 2-cocycle $\phi_2 : G^3 \to M$ given by

$$\phi_2(e, g^i, g^{i+j}) = \begin{cases} 0 & i + j < \#G \\ -x & i + j \geq \#G. \end{cases}$$

If you prefer, you can shift by a coboundary to get x if $i + j < \#G$ and 0 if $i + j \geq \#G$.

Back to the desired computation. Applying this to $\mathrm{Gal}(M/K)$ acting on M^*, with the canonical generator g equal to the Frobenius, we get that $H^2(M/K)$ is generated by a cocycle ϕ with $\phi(e, g^i, g^{i+j}) = \pi$ if $i + j < \#G$ and 1 otherwise. Now push this into $H^2(ML/K)$; the general theory says the image comes from $H^2(L/K)$. That is, for $h \in \mathrm{Gal}(ML/K)$, let $f(h)$ be the integer i such that h restricted to $\mathrm{Gal}(M/K)$ equals g^i. Then there exists a 1-cochain $\rho : \mathrm{Gal}(ML/K)^2 \to (ML)^*$ such that $\phi(e, h_1, h_2h_1)/(\rho(h_1, h_2h_1)\rho(e, h_2h_1)^{-1}\rho(e, h_1))$ belongs to L^* and depends only on the images of h_1, h_2 in $\mathrm{Gal}(M/K)$. Putting $\sigma(h) = \rho(e, h)$, we thus have

$$\frac{\phi(e, h_1, h_2h_1)\sigma(h_2h_1)}{\sigma(h_2)^{h_1}\sigma(h_1)}$$

depends only on h_1, h_2 modulo $\mathrm{Gal}(ML/L)$.

The upshot: once you compute such a σ (which I won't describe how to do, since it requires an explicit description of L/K), to find the inverse image of $g \in \mathrm{Gal}(L/K)$ under the Artin map, choose a lift g_1 of g into $\mathrm{Gal}(ML/K)$, then compute

$$\prod_h \frac{\phi(e, h, gh)\sigma(gh)}{\sigma(g)^h\sigma(h)}$$

for h running over a set of lifts of the elements of $\mathrm{Gal}(L/K)$ into $\mathrm{Gal}(ML/K)$.