Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Connection With Local Reciprocity

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

So far, we've used abstract class field theory to construct reciprocity isomorphisms

$$r'_{L/K} : C_K / \operatorname{Norm}_{L/K} C_L \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$$

and to establish the adelic form of the existence theorem. We also know that if L/K is a small cyclotomic extension, then this map induces the usual Artin map.

This time, we'll verify that this map coincides with the product of the local reciprocity maps. As noted earlier, this is enough to recover the classical Artin reciprocity law and existence theorem.

I've also included some material I won't have time to cover in class: a sketch of Milne's approach to the reciprocity isomorphism, using H^2 and an explicit computation in local class field theory. The sketchy part is (among other things) that this explicit computation requires a little of the Lubin-Tate construction, which we didn't discuss (but see Tathagata's final paper).

The relationship with local reciprocity.

Caveat. This still does not follow Milne or Neukirch.

For any extension L/K of number fields, we currently have the map $r_{L/K} : I_K \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$ formed as the product of the local reciprocity maps, and the abstract reciprocity map $r'_{L/K} : I_K \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$, which actually factors through C_K and even through $C_K / \operatorname{Norm}_{L/K} C_L$. We want to show that these agree. Before doing so, let's observe some consequences of that which we'll then use in the proof that they agree.

If L/K is abelian, v is a place of K and w is a place of L above v, then we have an injection $K_v^* \to I_K$, which we then funnel through $r'_{L/K}$ to get a map into $\operatorname{Gal}(L/K)$. If we knew that $r = r'$, we would know that:

(i) the composite map $K_v^* \to \operatorname{Gal}(L/K)$ actually maps into the decomposition group of w;

(ii) the subgroup $\operatorname{Norm}_{L_w/K_v} L_w^*$ is contained in the kernel of $K_v^* \to \operatorname{Gal}(L/K)$.

In fact, we can check these independently. (In (ii), we would also know that "contained in" can be replaced by "equal to", but we won't try to check that independently.) For (i), let M be the fixed field of the decomposition group of w; then we have the compatibility

$$\begin{tikzcd}
\operatorname{Gal}(L/K) \arrow[r] \arrow[d] & C_K / \operatorname{Norm}_{L/K} C_L \arrow[d] \\
\operatorname{Gal}(M/K) \arrow[r] & C_K / \operatorname{Norm}_{M/K} C_M
\end{tikzcd}$$

and the image of $K_v^* \to I_K$ lands in $\operatorname{Norm}_{M/K} I_M$ because v splits completely in M. So this image lies in the kernel of $\operatorname{Gal}(L/K) \to \operatorname{Gal}(M/K)$, which is to say $\operatorname{Gal}(L/M)$, the decomposition group of w.

For (ii), we need only check that $\operatorname{Norm}_{L_w/K_v} L_w^*$ is contained in the kernel of $K_v^* \to C_K/\operatorname{Norm}_{L/K} C_L$. But $\operatorname{Norm}_{L_w/K_v} L_w^*$ is already in the kernel of $K_v^* \to I_K/\operatorname{Norm}_{L/K} I_L$, so we're all set.

Our plan now is to attempt to "recover" the local reciprocity map from the maps $r'_{L/K}$. To do this, we need some auxiliary global extensions, provided by the Existence Theorem.

Lemma 1. *Let K be a number field, v a place of K and M a finite abelian extension of K_v. Then there exists a finite abelian extension L of K such that for any place w of L above v, L_w contains M.*

Proof. This is easy if v is infinite: if v is complex there is nothing to prove, and if v is real then we may take $L = K(\sqrt{-1})$. So assume hereafter that v is finite.

By the Existence Theorem and by (ii), it suffices to produce an open subgroup U of C_K of finite index such that the preimage of U under $K_v^* \to C_K$ is contained in $N = \operatorname{Norm}_{M/K_v} M^*$. Let S be the set of infinite places and $T = S \cup \{v\}$, and let $G = K_T \cap N$. Then one can choose an additional place u (finite and distinct from v) and an open subgroup V of $\mathfrak{o}_{K_u}^*$ such that $V \cap K_T \subseteq G$. Now put

$$W = N \times V \times \prod_{w \in S} K_w^* \times \prod_{w \notin S \cup \{u,v\}} \mathfrak{o}_K^*$$

and $U = WK^*/K^*$. If $\alpha_v \in K_v^*$ maps into U, then there exists $\beta \in K^*$ such that $\alpha_v \beta \in W$. That means first of all that $\beta \in K_T$ and then that $\beta \in V$, so that $\beta \in G$ and so also $\beta \in N$. It also means that $\alpha_v \beta \in N$. Thus $\alpha_v \in N$, as desired. $\square$

For each place v of K and each abelian extension M of K_v, we can now write down a map a map $r'_{K,v} : K_v^* \to \operatorname{Gal}(M/K_v)$ by choosing an abelian extension L such that $M \subseteq L_w$ for any place w of L above v, letting N be the fixed field of the decomposition group of w, and setting $r'_{K,v}$ equal to the composition

$$K_v^* \stackrel{r'_{L/K}}{\to} \operatorname{Gal}(L/N) = \operatorname{Gal}(L_w/K_v) \to \operatorname{Gal}(M/K_v).$$

By the same compatibility as above, this doesn't change if we enlarge L. Thus it doesn't depend on the choice of L at all! (Any two choices of L sit inside an abelian extension of K; compare both with that bigger field.)

Again by the usual compatibilities, these maps fit together to give a single map $r'_{K,v} : K_v^* \to \operatorname{Gal}(K_v^{\mathrm{ab}}/K_v)$. This map has the following properties:

(a) The induced map $K_v^* \to \operatorname{Gal}(M/K_v^*)$, for M unramified, kills units and maps a uniformizer of K_v to the Frobenius automorphism. (Since that extension is generated by roots of unity, we can check this using a suitable small cyclotomic extension of K, on which r' is essentially the Artin map. We leave this to the reader.)

(b) For any finite extension M/K_v^*, $r'_{K,v}$ induces an isomorphism $K_v^*/\operatorname{Norm}_{M/K_v} M^* \to \operatorname{Gal}(M/K_v^*)$. Note: we only know *a priori* that this map is injective. But by local class field theory, the two groups have the same order, so it's actually an isomorphism. (Note: for this and other reasons, we are not getting an independent proof of local class field theory by this process.)

But these properties *uniquely* characterize the local reciprocity map! We conclude that $r'_{K,v}$ is the local reciprocity map for K_v, and so $r_{L/K} = r'_{L/K}$ and at long last Artin reciprocity (and the classical existence theorem, and the whole lot) follows. Hooray!

It's worth repeating that we now know that the product $r_{L/K}$ of the local reciprocity maps kills principal ideles. That fact, which relates local behavior for different primes in a highly "global" fashion, is the basis of various "reciprocity laws". See Milne, Chapter VIII for details.

An explicit computation in local CFT.

We sketch an alternate approach for comparing the "abstract" reciprocity map $r'_{L/K}$ with the product $r_{L/K}$ of the local reciprocity maps, following Milne (and Neukirch V.2).

We first verify that $r = r'$ for cyclotomic extensions of $\mathbb{Q}$, using an explicit computation in local class field theory. Namely, we compute that if we identify $\operatorname{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q})$ with $(\mathbb{Z}/p^m\mathbb{Z})^*$, then the local reciprocity maps are given by

$$r_{\mathbb{Q}_\ell(\zeta_{p^m})/\mathbb{Q}_\ell}(a) = \begin{cases} \operatorname{sign}(a) & \ell = \infty \\ \ell^{v_\ell}(a) & \ell \neq \infty, p \\ u^{-1} & \ell = p. \end{cases}$$

This is straightforward for $\ell = \infty$. For $\ell \neq \infty, p$, we have an unramified extension of local fields, where we know the local reciprocity map takes a uniformizer to a Frobenius. In this case the latter is simply ℓ.

The hard work is in the case $\ell = p$. For that computation one uses what amounts to a very special case of the Lubin-Tate construction of explicit class field theory for local fields, using formal groups. Put $K = \mathbb{Q}_p$, $\zeta = \zeta_{p^m}$ and $L = \mathbb{Q}_p(\zeta)$.

Suppose without loss of generality that $u \in \mathbb{N}$, and let $\sigma \in \operatorname{Gal}(L/K)$ be the automorphism corresponding to u^{-1}. Since L/K is totally ramified at p, we have $\operatorname{Gal}(L/K) \cong \operatorname{Gal}(L^{\mathrm{unr}}/K^{\mathrm{unr}})$, and we can view σ as an element of $\operatorname{Gal}(L^{\mathrm{unr}}/K)$. Let $\phi_L \in \operatorname{Gal}(L^{\mathrm{unr}}/L)$ denote the Frobenius, and put $\tau = \sigma\phi_L$. Then τ restricts to the Frobenius in $\operatorname{Gal}(K^{\mathrm{unr}}/K)$ and to σ in $\operatorname{Gal}(L/K)$. By Neukirch's definition of the reciprocity map, we may compute $r_{L/K}^{-1}(\sigma)$ as $\operatorname{Norm}_{M/K} \pi_M$, where M is the fixed field of τ and π_M is a uniformizer. We want that norm to be u times a norm from L to K, i.e.,

$$r_{L/K}^{-1}(\sigma) \in u \operatorname{Norm}_{L/K} L^*.$$

Define the polynomial

$$e(x) = x^p + upx$$

and put

$$P(x) = e^{(n-1)}(x)^{p-1} + pu,$$

where $e^{(k+1)}(x) = e(e^{(k)}(u))$. Then $P(x)$ satisfies Eisenstein's criterion, so its splitting field over $\mathbb{Q}_p$ is totally ramified, any root of P is a uniformizer, and the norm of said uniformizer is $(-1)^{[L:K]}pu \in \mathrm{Norm}_{L/K} L^*$, since $\mathrm{Norm}_{L/K}(\zeta - 1) = (-1)^{[L:K]}(p)$.

The punch line is that the splitting field of $P(x)$ is precisely M! Here is where the Lubin-Tate construction comes to the rescue... and where I will stop this sketch. See Neukirch V.2 and V.4, and/or Milne I.3, and/or Tathagata's final paper.

A bit about Brauer groups.

For background about Brauer groups, see Milne IV and/or Ulrich's final paper. We'll be following Milne VII.8 for now, and omitting many details.

Proposition 2. *Put $L = K(\zeta_n)$. Then $r_{L/K} : I_K \to \mathrm{Gal}(L/K)$ maps all principal ideles to the identity.*

Proof. For $K = \mathbb{Q}$, this follows from the previous section (factor n into prime powers and apply the previous argument to each factor). In general, we have a compatibility

$$\begin{tikzcd} I_L \arrow[r] \arrow[d, "\mathrm{Norm}_{L_w/\mathbb{Q}_p}"] & \mathrm{Gal}(L_w(\zeta_n)/L_w) \\ I_{\mathbb{Q}} \arrow[r] & \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \end{tikzcd}$$

and we know the bottom row kills principal ideles and the right column is injective. Thus the top row kills principal ideles too. □

To make more progress, we need to bring in H^2, as we did in local reciprocity. (Unfortunately, trying to compute H^2 of the idele class group is a headache, so we can't imitate the argument perfectly.) Recall there that we saw that every element of $H^2(L/K)$ could be "brought in" from a suitable unramified extension of K. We have a similar situation here with "unramified" replaced by "cyclotomic".

Proposition 3. *Let L/K be any finite Galois extension of number fields. Then for any element x of $H^2(\mathrm{Gal}(L/K), L^*)$, there exists a cyclic, cyclotomic extension M of K and an element y of $H^2(\mathrm{Gal}(M/K), M^*)$ such that x and y map to the same element of $H^2(\mathrm{Gal}(ML/K), ML^*)$.*

Proof. Omitted. See above references. □

Hereafter L/K is abelian. From the exact sequence

$$0 \to L^* \to I_L \to C_L \to 0$$

we get a fragment

$$1 = H^1(\mathrm{Gal}(L/K), C_L) \to H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L)$$

so the map $H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L) = \oplus H^2(\mathrm{Gal}(L/K), I_L)$ is injective. Each factor in the direct sum is canonically a subgroup of $\mathbb{Q}/\mathbb{Z}$, so we get a sum map $H^2(\mathrm{Gal}(L/K), I_L) \to \mathbb{Q}/\mathbb{Z}$.

It turns out (see Milne, Lemma VII.8.5) that for any map $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$, there is a commuting diagram

$$\begin{tikzcd}
K^* \arrow[r] \arrow[d] & I_K \arrow[r, "r_{L/K}"] \arrow[d] & \mathrm{Gal}(L/K) \arrow[d] \\
H^2(L^*) \arrow[r] & H^2(I_L) \arrow[r] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

If L/K is cyclic, we may choose the map $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ to be injective, and then the first vertical arrow will be surjective. (In fact, it's $K^* \to K^*/\operatorname{Norm}_{L/K} L^* = H^0_T(L^*)$ plus the periodicity isomorphism $H^0_T(L^*) \to H^2_T(L^*)$.) Then the fact that $r_{L/K}$ kills principal ideles implies that the composite $H^2(L^*) \to \mathbb{Q}/\mathbb{Z}$ is the zero map.

Now if we know $H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$ vanishes for all cyclic extensions, we know it in particular for cyclic cyclotomic extensions. But then the previous proposition tells us that it also vanishes for any finite Galois extension! Now we can use the diagram in reverse: it tells us that for $a \in K^*$, $r_{L/K}(a)$ is killed by any homomorphism $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$. Since $\mathrm{Gal}(L/K)$ is an abelian group, that implies $r_{L/K}(a)$ is trivial.

To conclude, we now have that $r_{L/K}$ kills principal ideles in general. By construction, it also kills norms (since it does so locally), so it induces a surjection $C_K/\operatorname{Norm}_{L/K} C_L \to \mathrm{Gal}(L/K)$. (Remember, the fact that it's surjective follows from the First Inequality.) But the order of the first group is less than or equal to the order of the second by the Second Inequality. So it's an isomorphism, and the reciprocity law is established. Hooray again!