We'll be meeting Monday and Wednesday, 11:30-12:45.

Let's see. Before break, we defined the following. For G a group, and a G-module A[1] we defined cohomology of groups,

$$\begin{aligned} H^\bullet(G,A) &= \operatorname{Ext}^\bullet_{\mathbb{Z}[G]}(\mathbb{Z},A) \\ H_\bullet(G,A) &= \operatorname{Tor}_\bullet^{\mathbb{Z}[G]}(\mathbb{Z},A) \end{aligned}$$

We had explicit resolution via standard complexes; there were homogeneous and inhomogeneous versions, canonically isomorphic to each other. In topology, this is the bar resolution.

En passant, geometrically we can think of this as, umm, take the category of one object with lots of isomorphisms, and all the morphisms are invertible. And once you have such, there's a standard way of making a simplicial complex out of it. And that's exactly what we wrote down. If you don't get it, don't worry.

We also defined, for $H \subseteq G$ a subgroup, restriction maps. And if H is normal in G, we get an inflation map. Restriction is via $H^\bullet(G,A) \to H^\bullet(H,A)$, and inflation is $H^\bullet(G/H,A^H) \to H^\bullet(G,A)$. And similarly for homology.

We also had Shapiro's lemma. Given a subgroup H, we can take the induced module (H,A), and define $\operatorname{Ind}_H^G(A)$. Shapiro's lemma says that $H^\bullet(H,A) \cong H^\bullet(G,\operatorname{Ind}_H^G A)$ canonically.

There's something called the inflation-restriction sequence. We've got $H \trianglelefteq G$, and A a G-module. There's a sequence

$$0 \longrightarrow H^1(G/H,A^H) \xrightarrow{\text{Inf}} H^1(G,A) \xrightarrow{\text{Res}} H^1(H,A)$$

which is actually exact.

Proof of this is left as an exercise. Well, last time we gave explicit definitions of these resolutions, and in particular what H^1 means. It's the collection of elements $\{a_s\}_{s\in G}$ satisfying certain conditions, namely, the cocycle condition; that differentiating gives you zero. But the derivative is a 2-chain; $\partial a(s,t) = sa_t - a(st) + a_s$. So the condition is that this thing is zero; $sa_t - a_{st} + a_s = 0$ for all s and t. And you divide out that set by the coboundaries of zero co-chains. This, in turn is $(\partial b)_s = sb - b$; these form a group. Anyways, that quotient is $H^1(G,A)$.

[1]That is, a $\mathbb{Z}[G]$-module.

The content of this exercise is just to use this definition to grind it through.

So, wonderful. We can prove it. Why might one suspect it would be true in the first place? Here's a good way to think about it. It turns out to be a small part of the Hoschild-Serre spectral sequence.

$$E_2^{p,q} = H^p(G/H, H^q(H,A)).$$

In our case,

$$\begin{aligned} E_2^{0,1} &= H^0(G/H, H^1(H,A)) \\ &= H^1(H,A)^G \end{aligned}$$

And one winds up with

$$0 \to E_2^{1,0} \to H^1(G,A) \to \ker d_2^{0,1} \to 0$$

So where does this thing come from, anyway? Our cohomology comes from the functor $A \rightsquigarrow A^G$, the fixed part. But this is a composition of two functors; $A \rightsquigarrow A^H$, a G/H-module. And then use $A^H \rightsquigarrow (A^H)^{G/H}$. And the composition is all elements fixed under G. And this composition functor gives you the Hoschild-Serre spectral sequence.

Suppose we have $H \subseteq G$ a subgroup of finite index, not necessarily normal. There's a natural map $H^\bullet(G,A) \to H^\bullet(H,A)$ for A a G-module, and the map here is restriction. This has nothing to do with the finiteness assumption; it's a subgroup thing. Under the assumption that this subgroup has finite index, we'll get an arrow in the other direction. In topology, this is usually referred to as transfer, though perhaps it's more modern to call it corestriction.

What about homology? There's a natural map $H_\bullet(H,A) \to H_\bullet(G,A)$. And you can get an arrow in the reverse direction here, too. But in the context of homology, we'll call the natural arrow corestriction; and the unnatural arrow will be restriction. This may not be completely standard, but there you are.

Let's talk about cohomological corestriction $\operatorname{cor}_{G,H}$. At the very least we should know how to define these before taking derivations; we should understand what it says for $\bullet = 0$. For H^0, what's the corestriction? Well, $H^0(H,A) = A^H$, etc. To get an invariant, we'll just average over coset representatives.

$$\begin{array}{ccc} H^0(G,A) & \longleftarrow & H^0(H,A) \\ A^G & & A^H \\ \sum_{s\in G/H} sa & \xleftarrow[N_{G/H}]{} & a \end{array}$$

We don't divide, since we don't necessarily know how to. We just fiat that this is what we do.

How do we define this map in general? Just dimension shift. As long as you're allowed to use different coefficient modules, there's no such thing as, say, an intrinsinic dimension three thing; you can just as easily put it in dimension four or two, just by changing the coefficients.

$$0 \longrightarrow A \longrightarrow I \longrightarrow I/A \longrightarrow 0$$

Embed A in an injective I. Then

$$H^i(G,A) \cong H^{i-1}(G,I/A)$$

via the long exact sequence. Hmm. This is certainly true for $i \geq 2$. Should go slowly when $i = 1$.

Well, when $i = 1$, we have

$$0 \longrightarrow A^G \longrightarrow I^G \longrightarrow (I/A)^G \longrightarrow H^1(G,A) \longrightarrow 0$$

The point now is that, if I is injective as a G-module, it's still injective as an H-module. Gotta show that $\mathrm{Hom}_H(?,I)$ is exact. Compute:

$$\mathrm{Hom}_H(?,I) \quad = \quad \mathrm{Hom}_G(\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}?,I)$$

So that's fine. Still working with $i = 1$. We still have

$$
\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r] & I^G \arrow[r] & (I/A)^G \arrow[r] & H^1(G,A) \arrow[r] & 0 \\
0 \arrow[r] & A^H \arrow[r] \arrow[u, "\mathrm{cor}_{G/H}"] & I^H \arrow[r] \arrow[u, "\mathrm{cor}_{G/H}"] & (I/A)^H \arrow[r] \arrow[u, "\mathrm{cor}_{G/H}"] & H^1(H,A) \arrow[r] \arrow[u, dashed, "\mathrm{cor}_{G/H}"] & 0
\end{tikzcd}
$$

The dashed arrow comes from the induced map on the quotient. And it's even easier for $i \geq 2$;

$$
\begin{tikzcd}
H^i(G,A) & H^{i-1}(G,I/A) \arrow[l, "\cong"'] \\
H^i(H,A) \arrow[u] & H^{i-1}(H,I/A) \arrow[l, "\cong"'] \arrow[u]
\end{tikzcd}
$$

Well, we now know that it exists, but computing it's a bear; for you have to chase the diagram all the way back to zero. Fortunately, one can give an explicit formula.

Use the standard resolution of, say, the inhomogeneous complex, for G. Call the resolution C. Observe that this is also a free resolution of $\mathbb{Z}$ by free $\mathbb{Z}[H]$-modules; $C_\bullet \to \mathbb{Z}$. We can use this complex to compute the cohomology of the group H.

$$H^\bullet(\mathrm{Hom}_H(C_\bullet, A)) = H^\bullet(H, A).$$

So if we can define a map $\mathrm{Hom}_H(C_\bullet, A) \to \mathrm{Hom}_G(C_\bullet, A)$ then we're in business. Use $f \mapsto (c \mapsto \sum_{s \in G/H} sf(s^{-1}c))$. For that's exactly how G operates on Hom_H This gives a map on the level of cochains, which induces everything.

Last time we talked about corestriction. Now we want to discuss homologies. Let $H \subseteq G$ be of finite index, with A a G-module. Then there's a natural map $H_i(H, A) \to H_i(G, A)$. How so? There's the classifying space of H, B_H running around; an the universal cover E_H. And we can think of A as a sheaf of coefficients.[2]

$$\begin{tikzcd}
E_H \arrow[dr, dash] & E_G \arrow[dr, dash] & \\
 & B_H \arrow[r] & B_G
\end{tikzcd}$$

And the E_H and E_G are contractible; topologically equivalent to a point.

After some prompting, we're going to work out an example. Take a cyclic group $G = \mathbb{Z}/n\mathbb{Z} = \langle s \rangle$. Want its homology; we'll try to give an explicit resolution of it, substituting for the standard one.

So, G is generated by s. Let $D = s - 1$; $N = N_G = \sum_{i=0}^{n-1} s^i$.

$$\mathbb{Z}[G] \xrightarrow[N]{} \mathbb{Z}[G] \xrightarrow[D]{} \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

It's an exercise to show that this is exact. Can think of this as an infinite dimensional chain complex attached to a simplicial complex, and at each level there are n elements. And that complex is what we denoted by E_G.

F'rinstance, take $n = 2$. Then $B_G = \mathbb{P}^\infty_{\mathbb{R}}$. $E_G = S^\infty$; and $S^\infty \rightharpoonup \mathbb{P}^\infty_{\mathbb{R}}$.

So much for the examples. The map $H_i(H, A) \to H_i(G, A)$ is $\mathrm{cor}_{G/H}$. And there's a map $H_i(G, A) \to H_i(H, A)$. But in a sense this really isn't the natural map. We'll call it the restriction map $\mathrm{res}_{G/H}$.

We'll define it first on H_0, and then get to H_i with dimension shifting.

$$\begin{array}{rcl}
\mathrm{res} : H_0(G, A) & \to & H_0(H, A) \\
A_G & \to & A_H \\
\overline{a} & \mapsto & \displaystyle\sum_{s \in H \backslash G} \overline{sa}
\end{array}$$

[2]Refs: Siegel, $<$ 10 pages, *IHES*. Given a group you get a category with one object, lots of arrows, and run with that. Otherwise, could look at Eilenberg-Maclane. Probably in Hussemoller's book.

Let $\sigma \in G$, $b \in A$. Make sure the stuff you modded out by in A_G dies in A_H. So look at $(\sigma - 1)b \mapsto \sum_{s \in H\backslash G} s(\sigma - 1)b$. Exercise to verify this.

For the other i's, use a dimensionshift. Given $0 \to A' \to P \to A$. Then $H_i(\begin{smallmatrix} G \\ H \end{smallmatrix}, A) \xrightarrow{\partial} H_{i-1}(\begin{smallmatrix} G \\ H \end{smallmatrix}, A')$.

Proposition $H^i(G, A) \leftrightarrow^{\mathrm{res}}_{\mathrm{cor}} H_i(H, A)$. Then $\mathrm{cor}_{G/H} \circ \mathrm{res}_{G/H} = [G : H]$ on $H^i(G, A)$.

Proof It suffices to prove this for $i = 0$; but this is obvious.

Exercise: do the same statement for homology; $\mathrm{res} \circ \mathrm{cor}$.

Keep applying functors, and when the music stops see if your arrows point in the same way.

As a special case, suppose $H \subseteq G$ of finite index. We've said that $H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Z})$.

$$\mathrm{Ver} : H_1(G, \mathbb{Z}) \longrightarrow H_1(H, \mathbb{Z})$$

$$G^{\mathrm{ab}} = \frac{G}{G'} \qquad H^{\mathrm{ab}} = \frac{H}{H'}$$

Here, Ver is essentially German for transfer. Let's compute this puppy explicitly; just group theory and using nothing else. Well, according to the definition we need a free resolution.

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

Recall that I_G is the elements of the group ring whose coefficients add up to zero. Take the long exact sequence of this guy.

$$0 \longrightarrow H_1(G, \mathbb{Z}) \xrightarrow{\partial} H_0(G, I_G) = I_G / I_G^2 \longrightarrow 0$$

Remember that $H_1(G, \mathbb{Z}[G]) = 0$, since it's a free abelian thing. And similarly for H. But maybe we should use $\mathbb{Z}[G]$ to resolve H. And of course we have

$$\begin{tikzcd}
0 \arrow[r] & I_G \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \arrow[r] \arrow[d, phantom, "="] & 0 \\
0 \arrow[r] & I_H \arrow[r] \arrow[u] & \mathbb{Z}[H] \arrow[r] \arrow[u] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

So maybe what we want is

$$\begin{tikzcd}
 & H_0(H, I_G) \\
H_1(H, \mathbb{Z}) \arrow[ur] \arrow[r, "\cong", "\partial"'] & H_0(H, I_H) \arrow[u, hook]
\end{tikzcd}$$

Well, dammit, we define things so that everything commutes:

$$\begin{tikzcd}
H_1(G, \mathbb{Z}) \arrow[r, "\partial", "\cong"'] \arrow[dd] & H_0(G, I_G) \arrow[d, "N_{G/H}"'] & = & I_G/I_G^2 \arrow[d] \\
 & H_0(H, I_G) & = & I/G/I_H I_G \arrow[d] \\
H_1(H, \mathbb{Z}) \arrow[r, "\partial", "\cong"'] \arrow[ur, "\partial"] & H_i(H, I_H) \arrow[u, hook] & = & I_H/I_H^2
\end{tikzcd}$$

Moving on, somewhat.

$$
\begin{tikzcd}
H_1(G,\mathbb{Z}) \arrow[r, "\cong"] \arrow[dd, "\mathrm{Ver}"] & I_G/I_G^2 \arrow[dr, hook] & \\
& & I_G/I_H I_G \\
H_1(H,\mathbb{Z}) \arrow[r, "\cong"] & I_H/I_H^2 \arrow[ur, hook] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
G \ni s \arrow[r, mapsto] \arrow[dd, "\mathrm{Ver}"] & s-1 H_1(G,\mathbb{Z}) \arrow[r, "\cong"] \arrow[dr, hook] & I_G/I_G^2 \\
& & I_G/I_H I_G \\
H_1(H,\mathbb{Z}) \arrow[r, "\cong"] & I_H/I_H^2 \arrow[ur, hook] &
\end{tikzcd}
$$

Let $H\backslash G = \{t_i\}$; consider $\sum_{t_i} t(s-1)$, I think. Well, $t_i s = h_i t_{j(i)}$, $h_i \in H$. So

$$
\begin{aligned}
\sum_{t \in H\backslash G} t(s-1) &= \sum_i h_i t_{j(i)} - t_{j(i)} \\
&= \sum_i (h_i - 1) t_{j(i)} \\
&= \sum_i (h_i - 1)(t_{j(i)} - 1) + \sum_i (h_i - 1) \\
\sum_i (h_i - 1)(t_{j(i)} - 1) &\in I_H I_G \\
\sum_i (h_i - 1) &\in I_H
\end{aligned}
$$

We summarize the conclusions of this computation.

Proposition The map $\mathrm{Ver}: G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is given by the following recipe. For $s \in G$, choose a set of representatives $\{t_i\}$ of $H\backslash G$. Then $t_i s = h_i t_{j(i)}$; then $\mathrm{Ver}(\overline{s}) = \overline{\prod_i h_i}$.

What would have happened if we'd used G/H instead? Well, $s^{-1}t_i^{-1} = t_{j(i)}^{-1}h_i^{-1}$. Then $\overline{s^{-1}} \mapsto \overline{\prod_i h_i^{-1}}$. So using either side gives you the *same* transfer map.

Exercise. Using only the definition of the group, show directly that the choice is independent of the choice of coset representatives for $H\backslash G$.

Galois theoretic reinterpretation[?] We've got $H\backslash G$, $s \in G$. Want to look at the subgroup generated by s, $\langle s\rangle$; and then look at $H\backslash G/\langle s\rangle$. Let $\{w_j\}$ be a set of representatives, certainly finite. This is the set of orbits of $\langle s\rangle$ acting on the set $H\backslash G$. And clearly each orbit is finite. Let f_j be the cardinality of the orbit of Hw_j under $\langle s\rangle$. Then

$$w_j s^{f_j} = h_j w_j$$

A perfectly reasonable set of representatives for $H\backslash G$ would be $\{w_1, w_1 s, w_1 s^2, \cdots, w_1 s^{f_1 - 1}, w_2, \cdots, w_j s^{f_j - 1}\}$. Then $\mathrm{Ver}(\overline{s}) = \overline{\prod_j h_j}$.

Let L/K be a finite Galois extension of global field. Want to interpret what we just did as a formula for the transfer map. We'll use Frobenii to describe elements of the abelianization. Let $G = \mathrm{Gal}(L, K)$, and $L \supset M \supset K$; $H = \mathrm{Gal}(L, M)$. Then there's a map $\mathrm{Ver}_{L/M}$: $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. Let's try to describe it as explicitly as possible. For a prime $\mathfrak{p}$ of K we get an element – up to conjugation – of G, namely the Frobenius $\mathfrak{p} \rightsquigarrow (\mathfrak{p}, L/K)$.[3] Anyways, $\mathfrak{p} \rightsquigarrow (\mathfrak{p}, L/K) \in G^{\mathrm{ab}}$. Since all reps are conjugate, this is well-defined. We apply $\mathrm{Ver}_{L,M}$ to it. What do we get?

Try and use the stuff we did just above. It's not difficult to see that we already have something. If you think about this $w_j s^{f_j} = h_j w_j$, well, what does it mean? H is exactly those elements of the Galois group which fix M. And the f_j turn out to be the degree of residue field extensions. If $\mathfrak{q}_j \in M$ lie above it, then these guys correspond to such things. Anyways, the map winds up to be $(\mathfrak{p}, L/K) \mapsto (\mathfrak{p}, L/M)$. For $\mathfrak{p} = \prod_j \mathfrak{q}_j$, etc.

[3] In general, L/K, $\mathfrak{p} \subseteq \mathcal{O}_K$ unramified. Then $\mathfrak{p}$ decomposes into $\mathfrak{P}_i$'s. We've got the decomposition group $G_{\mathfrak{P}_i/\mathfrak{p}}$; and it maps to $\mathrm{Gal}(\lambda_{\mathfrak{P}_i}, \kappa)$. And this is an isomorphism. There's a Frobenius element in the galois group of finite fields, and we identify it with some element of $\mathrm{Gal}(L, K)$.

We've got $L \supset M \supset K$, with $G = \mathrm{Gal}(L, K)$, $H = \mathrm{Gal}(L, M)$. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ unramified. We want to show that $\mathrm{Ver}(\mathfrak{a}, L/K) = (\mathfrak{a}\mathcal{O}_M, L/M)$ in H^{ab}. We may assume $\mathfrak{a} = \mathfrak{p}$. Suppose it splits into $\mathfrak{q}_j$ in M, and $\mathfrak{P}_i$ in L. Let $s = \mathrm{Fr}(\mathfrak{P}, \mathfrak{p})$; fix some prime ideal upstairs. Then $\langle s \rangle = D_{\mathfrak{P},\mathfrak{p}}$ the decomposition group. Consider

$$H \backslash G / \langle s \rangle = \{w_j\}$$

where $w_j s^{f_j} = h_j w_j$. So then we know that

$$\overline{(\prod_j h_j)} = \mathrm{Ver}(s)$$

Claim that these double cosets are in 1-1 correspondence with the prime ideal $\mathfrak{q}_j$. Well, G operates on $\{\mathfrak{P}_i\}$. And $\langle s \rangle = D_{\mathfrak{P},\mathfrak{p}}$ the stabilizer of $\mathfrak{P}$. So we see that if we fix our choice, then $G/\langle s \rangle$! $\{\mathfrak{P}_i\}$. Now, last semester we proved that for each $\mathfrak{q}_j$ there's a bunch of $\mathfrak{P}_i$'s lying above it. And since L/K is Galois, we know that the Galois group operates transitively on the $\mathfrak{P}_i$ above a fixed $\mathfrak{q}_j$. So in our context, it means that the orbit of H on this set corresponds to $\mathfrak{q}_j$.

Thus, $f_j = [\mathfrak{m}_j, \kappa]$, the residue field extension degree.

Now,

$$\begin{aligned}
h_j &= w_j s^{f_j} w_j^{-1} \\
&= \mathrm{Fr}_{\mathfrak{P}_i, \mathfrak{q}_j} \\
\overline{(\prod_j h_j)} &= \prod_j \mathrm{Fr}_{\mathfrak{q}_j} \\
&= \mathrm{Ver}(\prod \mathfrak{q}_j, L/M) \\
&= \mathrm{Ver}(\mathfrak{p}\mathcal{O}_M, L/M)
\end{aligned}$$

◇

We'll now discuss cohomology of *finite* groups. So let G be a finite group. The following is basically said to be Tate's fault; Tate cohomology groups. Recall how we defined homology and cohomology. They're defined by, well, let $P_\bullet \to \mathrm{Z} \to 0$ be a standard resolution of Z. Take the dual of everything in sight, I guess.

$$0 \to \mathbb{Z} \to P_\bullet^* = \mathrm{Hom}_{\mathbb{Z}}(P_\bullet, \mathbb{Z})$$

Explicitly we have $0 \to \mathbb{Z} \to P_0^* \to P_1^* \to \cdots$. This is still a resolution of $\mathbb{Z}$. And P_0^* is a free $\mathbb{Z}[G]$-module, and thus injective. We've got

$$\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r] & P_0 \arrow[rr, dashed] \arrow[dr] & & P_0^* \arrow[r] & P_1^* \arrow[r] & \cdots \\
& & & \mathbb{Z} \arrow[ur] & & &
\end{tikzcd}$$

It's exact up to P_0, and past P_0^*. Call P_0^* P_{-1}, $P_1^* = P_{-2}$. One would also write $P_1 = P^{-1}$, $P_0 = P^0$, etc; you can put a subscript into a superscript [and vice-versa], provided you switch a sign. It's eventually possible to get this nonsenses straight.

Let's break down the middle a bit. Well, $P_0 = \mathbb{Z}[G]$. And the map there is the only one possible; $\sum n_\sigma \sigma \mapsto \sum n_\sigma$. That's ϵ; feels a little like the degree map. And $P_0^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Z})$. So we've got $\mathbb{Z} \to P_0^*$, via $1 \mapsto (\sigma \mapsto 1)$; $1 \mapsto \sum \sigma^*$.

Of course, $P_0^* = \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$. A dual basis is all σ^*, where $\sigma^*(t) = \delta_{\sigma,t}$.

$$\begin{tikzcd}
P_0 \arrow[r] & P_0^* \\
\mathbb{Z}[G] & \mathbb{Z}[G]
\end{tikzcd}$$

If $g \in G$ then

$$\begin{aligned}
(g\sigma^*)(t) &\stackrel{\text{def}}{=} \sigma^*(g^{-1}t) \\
&= \delta_{\sigma, g^{-1}t} \\
&= \begin{cases} 1 & t = g\sigma \\ 0 & \end{cases} .
\end{aligned}$$

We're trying to put a G action on P_0^*.

At the end of the day, we conclude that

$$\begin{tikzcd}
P_0 \arrow[rr, "N_G"] \arrow[dr] & & P_0^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Z}) \cong \mathbb{Z}[G] \\
& \mathbb{Z} \arrow[ur] &
\end{tikzcd}$$

The composite mp is the norm; and $\ker(N_G) = \ker(\epsilon)$, $\mathrm{im}(N_G) = \mathrm{im}(\epsilon^*)$. Therefore, the whole infinite sequence is exact.

Definition For a G-module A,

$$\widehat{H}^\bullet(G, A) \stackrel{\text{def}}{=} H^\bullet(\mathrm{Hom}_{\mathbb{Z}[G]}(Q_\bullet, A))$$

[4]

If $i \geq 1$, then $\widehat{H}^i(G, A) = H^i(G, A)$. That should be obvious.

And the same thing applies further to the right, more or less.

If $i \geq 2$, then $\widehat{H}^{-i}(G, A) = H_{i-1}(G, A)$.

What about $\widehat{H}^0(G, A)$ and $\widehat{H}^{-1}(G < A)$? Well, we've got $\mathbb{Z}[G] \stackrel{N_G}{\to} \mathbb{Z}[G]$. Take $\mathrm{Hom}(\cdot, A)$ to get $A \leftarrow A$. And actually, we've got

$$\begin{tikzcd}
\ker = A^G & A \arrow[l] & & A \arrow[ll, "N_G"'] \arrow[dl] & \mathrm{coker} = A_G \arrow[l] \\
& & A^G \arrow[ul] & &
\end{tikzcd}$$

So now we can take homology of the sequence. $\widehat{H}^0$ is the cohmology at the A on the left. That's $\frac{A^G}{N_G A}$. And $\widehat{H}^{-1}(G, A) = \frac{\ker N_G}{I_G A}$. This is a little different from the usual cohomology. It's now a subquotient of A, instead of a subthing of A.

[4]Recall that $Q_\bullet$ is the name of that infinite complex we just made. And apparently, while I was gone it was decided that P_n can be thought of as $\mathbb{Z}[G]^{\otimes n}$.

Basic Properties

- Given $0 \to A' \to A \to A''' \to 0$ an exact sequence fo G-modules, well, each of the $Q_\bullet$'s is free, so tensoring with 'em is exact. Thus,

  $$0 \to \mathrm{Hom}_G(Q_\bullet, A') \to \mathrm{Hom}_G(Q_\bullet, A) \to \mathrm{Hom}_G(Q_\bullet, A'') \to 0$$

  is an exact sequence of complexes, so we get a long exact sequence of cohomology.

  $$\to \widehat{H}^i(G, A') \to \widehat{H}^i(G, A) \to \widehat{H}^i(G, A'') \xrightarrow{\delta} \widehat{H}^{i+1}(G, A') \to \cdots$$

  This should be obvious.

- Functoriality of res and cor. This is less than obvious. At some point restriction and corestriction collide. One thing to check is that our definitions were really the right thing to do, in term s of co- versus regular stuff. Something commutes with boundary operators?

  Let's verify it. We had a formula for [co]restriction, but I think we'll just do it directly.

  Let $H \subseteq G$; remember everything is finite. Suppose we've got $0 \to A' \to A \to A'' \to 0$. Then we've got

  $$\begin{tikzcd} \widehat{H}^{-1}(G, A'') \arrow[r, "\delta"] \arrow[d, shift right, "\mathrm{res}"'] & \widehat{H}^0(G, A') \arrow[d, shift left, "\mathrm{res}"] \\ \widehat{H}^{-1}(H, A'') \arrow[r, "\delta"] \arrow[u, shift right, "\mathrm{cor}"'] & \widehat{H}^0(H, A') \arrow[u, shift left, "\mathrm{cor}"] \end{tikzcd}$$

  The assertion is that these commute.[5]

  Hold on. We need to know the following. Just stare at this and build the only map you could possibly do.

  $$\begin{array}{ccc} \widehat{H}^{-1}(G, A'') & \xrightarrow{\delta} & \widehat{H}^0(G, A') \\ \dfrac{\ker N_G}{I_G A''} & & \dfrac{A'^G}{N_G A'} \end{array}$$

[5] "This isn't going to be hard. If it's really hard, you can't do it."

Go for the proof.

$$\begin{tikzcd}
{} \arrow[r] & \mathrm{Hom}_G(Q_{-1}, A'') \arrow[r] & \mathrm{Hom}_G(Q_0, A'') \arrow[r] & \mathrm{Hom}_G(Q_1, A'') \arrow[r] & {} \\
{} \arrow[r] & \mathrm{Hom}_G(Q_{-1}, A) \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_0, A) \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_1, A) \arrow[r] \arrow[u] & {} \\
{} \arrow[r] & \mathrm{Hom}_G(Q_{-1}, A') \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_0, A') \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_1, A') \arrow[r] \arrow[u] & {}
\end{tikzcd}$$

Do the usual diagram chase to get from $\mathrm{Hom}_G(_{-1}, A'')$ to $\mathrm{Hom}_G(Q_0, A')$. But we know what some of these objects are.

$$\begin{tikzcd}
{} \arrow[r] & A'' \arrow[r] & \mathrm{Hom}_G(Q_0, A'') \arrow[r] & \mathrm{Hom}_G(Q_1, A'') \arrow[r] & {} \\
{} \arrow[r] & \mathrm{Hom}_G(Q_{-1}, A) \arrow[r, "N_G"] \arrow[u] & A \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_1, A) \arrow[r] \arrow[u] & {} \\
{} \arrow[r] & \mathrm{Hom}_G(Q_{-1}, A') \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_0, A') \arrow[r] \arrow[u] & \mathrm{Hom}_G(Q_1, A') \arrow[r] \arrow[u] & {}
\end{tikzcd}$$

So the map we were worrying about before is, essentially, given by the norm N_G; the map $\widehat{H}^{-1}(G, A'') \xrightarrow{\delta} \widehat{H}^0(G, A')$ works like this. For $a'' \in A''$ so that $N_G(a'') = 0$, choose $a \in A$ lifting a''. Then $N_G(a) = \sum_{\sigma \in G} \sigma a \in A^G$. And actually, since it dies in A'', we really know that $N_G(a) \in A^G \cap A' = A'^G$.

So it's an exercise now to show that the restriction and corestriction things give commutative diagrams.

The advantage of cohomology is that we have a cup-product.

A remark on the origins of this nonsense. Geometrically, the cup product is induced from a diagonal map, $\Delta : X \to X \times X$. The Künneth formula says, more or less, $H^\bullet(X \times X, A \otimes B) = H^\bullet(X, A) \otimes H^\bullet(X, B)$. Actually, you need a derived functor somewhere; $H^\bullet(X \times X, A \overset{\mathrm{L}}{\otimes} B) = H^\bullet(X, A) \overset{\mathrm{L}}{\otimes} H^\bullet(X, B)$. Composing with Δ^* gives you a map $H^\bullet(X, A) \otimes H^\bullet(X, B) \to H^\bullet(X, A \otimes B)$.

That's the sort of thing you want to do with group cohomology. But somewhere you need to do some homotopy.

$$G \longrightarrow G \times G$$

$$B_G \longrightarrow G_{G \times G} \simeq B_G \times B_G$$

A relevant buzzphrase is, "homotopy approximation of the diagonal map."

We're expecting [hoping?] to get a map $H^p(G, A) \otimes H^q(G, B) \to H^{p+q}(G, A \otimes_{\mathbb{Z}} B)$. It'll be $(a, b) \mapsto a \cup b$. Especially, if you hae a bilinear map $A \otimes_{\mathbb{Z}} B \to C$ which is G-equivariant, then you get a cup product with image in $H^{p+q}(G, C)$ using the ring structure on the coefficients.

If G is finite, we put hats on the H's and wind up with Tate cohomology.

Algebraic characterization From now on assume everything's finite, so that we can take Tate cohomology. Then for $p, q \in \mathbb{Z}$,

$$\widehat{H}^p(G, A) \otimes \widehat{H}^q(G, B) \to \widehat{H}^{p+q}(G, A \otimes B)$$

is bilinear, functorial. In other words, given $A \to A'$ and $B \to B'$, then everything commutes in the expected way.

Let's see what we know, or at least what we want.

1. $p = q = 0$. Then $\widehat{H}^0(G, A) \otimes \widehat{H}^0(G, B) \to \widehat{H}^0(G, A \otimes B)$. Well, $\widehat{H}^0(G, A) = \frac{A^G}{N_G A}$, and $\widehat{H}^0(G, B) \frac{B^G}{N_G B}$. And the image space is $\frac{(A \otimes B)^G}{N_G(A \otimes B)}$. So just do the obvious thing; take a tensor product. So the product is

$$\frac{A^G}{N_G A} \otimes \frac{B^G}{N_G B} \to \frac{(A \otimes B)^G}{N_G(A \otimes B)}.$$

2. Suppose we have an exact sequence $0 \to A' \to A \to A'' \to 0$, all maps equivariant; and further suppose that tensoring with B [on the right] preserves exactness of this sequence, e.g., B flat. Then we have

$$\begin{tikzcd}
\widehat{H}^p(G, A'') \otimes \widehat{H}^q(G, B) \arrow[r, "\cup"] \arrow[d, "\delta \otimes \mathrm{id}"'] & \widehat{H}^{p+q}(G, A'' \otimes B) \arrow[d, "\delta"] \\
\widehat{H}^{p+1}(G, A') \otimes \widehat{H}^q(G, B) \arrow[r, "\cup"] & \widehat{H}^{p+q+1}(G, A' \otimes B)
\end{tikzcd}$$

We insist that this commutes. So $\delta(a'' \cup b) = \delta a'' \cup b$.

3. $0 \to B' \to B \to B'' \to 0$; suppose tensoring with A [on the left] is exact, too.

$$\begin{tikzcd}
\widehat{H}^p(G, A) \otimes \widehat{H}^q(G, B'') \arrow[r, "\cup"] \arrow[d, "(-1)^p \mathrm{id} \otimes \delta"'] & \widehat{H}^{p+q}(G, A \otimes B'') \arrow[d, "\delta"] \\
\widehat{H}^p(G, A) \otimes \widehat{H}^{q+1}(G, B') \arrow[r, "\cup"] & \widehat{H}^{p+q+1}(G, A \otimes B')
\end{tikzcd}$$

Where's the sign from? Analogously, $d(\omega_1 \wedge \omega_2) = d\omega_1 \wedge \omega_2 + (-1)^{\deg \omega_1} \omega_1 \wedge d\omega_2$.

Actually, the sign is what makes compatibility possible; you can dimension shift in various ways, and it all comes out the same.

Lemma Suppose we have a commutative diagram, all rows exact.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d] & A' \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & B'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Then

$$\begin{tikzcd}
\widehat{H}^{p+1}(G, A'') \arrow[r, "\delta"] & \widehat{H}^{p+2}(G, A) \\
\widehat{H}^{p}(G, C'') \arrow[r, "\delta"'] \arrow[u, "-\delta"] & \widehat{H}^{p+1}(G, C) \arrow[u, "\delta"']
\end{tikzcd}$$

commutes.

Exercise Use this lemma to show that the existence of the cup product.

Proof [of lemma] "I know if I try it for a while, I'll get there."

Define a kernel K via

$$\begin{tikzcd}
 & 0 & & & \\
 & C' \arrow[u] \arrow[r, "="] & C' & & \\
0 \arrow[r] & K \arrow[u] \arrow[r] & B'' \otimes C' \arrow[u] \arrow[r] & C'' \arrow[r] & 0 \\
0 \arrow[r] & A'' \arrow[u] \arrow[r] & B'' \arrow[u] \arrow[r] & C'' \arrow[u] \arrow[r] & 0 \\
 & 0 \arrow[u] & 0 \arrow[u] & &
\end{tikzcd}$$

At the same time, we have

$$\begin{tikzcd}
 & 0 & 0 & \\
0 \arrow[r] & C \arrow[r] \arrow[u] & C' \arrow[r] \arrow[u] & C'' \\
0 \arrow[r, dashed] & K \arrow[r] \arrow[u] & B'' \oplus C \arrow[r] \arrow[u] & C'' \arrow[u, "="] \\
 & B'' \arrow[r, "="] \arrow[u] & B'' \arrow[u] & \\
 & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

Shit. I've lost the thread entirely.

We've got $\delta c'' \in \widehat{H}^{p+1}(G, K)$, and its image is either in A'' or C.

In the original diagram, call the horizontal maps α_1, α_2; β_1, β_2; and γ_1, γ_2. Similarly, denote the the vertical maps by f_i, g_i, and h_i.

There's a map $B' \to K$ given by $B' \mapsto (\beta_2 b', -g_2 b')$. And actually, there's an exact sequence $0 \to A \to B' \to K \to 0$.

Let's see. The next diagram he's draing is

$$\begin{tikzcd}
 & A \arrow[r] \arrow[d] & A' \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r] & B' \arrow[r] & K \arrow[r] & 0
\end{tikzcd}$$

$$b' \longmapsto (\beta_2 b', -g_2 b')$$

Strategy should be; produce a couple of commutative diagrams, and then by naturality show that they're really the same thing.

We're going back to the diagram chase:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "\alpha_1"] \arrow[d, "f_1"] & A' \arrow[r, "\alpha_2"] \arrow[d, "g_1"'] & A'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & B'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Then we get

$$\begin{tikzcd}
0 \arrow[r] & A'' \arrow[r] \arrow[d, "{(h_1, 0)}"] & B' \arrow[r] \arrow[d] & C'' \arrow[d, "="] & \\
0 \arrow[r] & K \arrow[r] & B'' \oplus C' \arrow[r] & C'' \arrow[r] & 0 \\
0 \arrow[r] & C \arrow[r] \arrow[u, "{(0, \gamma_1)}"] & C' \arrow[r] \arrow[u] & C'' \arrow[r] \arrow[u, "="] & 0
\end{tikzcd}$$

as well as

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha_1"] \arrow[d, "\mathrm{id}"] & A' \arrow[r, "\alpha_2"] \arrow[d, "g_1"] & A'' \arrow[r] \arrow[d, "{(h_1, 0)}"'] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r, "{(\beta_2, -g_2)}"'] & K \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r, "f_1"'] \arrow[u, "-\mathrm{id}"] & B \arrow[r, "f_2"'] \arrow[u, "-\beta_1"] & C \arrow[r] \arrow[u, "{(0, \gamma_1)}"'] & 0
\end{tikzcd}$$

And the minus signs are necessary for everything to commute.

Suppose $c'' \in H^i(G, C'')$. Then $H^{i+1}(G, K) \ni \delta_{\mathrm{mid}}(c'') = \gamma_1(\delta_l(c'')) = h_1(\delta - u(c''))$. And $H^{i+2}(G, A) \ni \delta_m(\delta_m(c'')) = -\delta_l(\delta_l(c'')) = \delta_u \delta - u(c'')$ from the upper part of the commutative diagram. So we're done.

Exercise Give another proof using $0 \to K_1 \to B' \to C'' \to 0$, and $0 \to A \to A' \oplus B \to K_1 \to 0$. This gives a sort of dual proof of the same theorem; just need something connecting these two.

Let's relate this back to cup-products. Recall that, in the appropriate setting, $\delta(a \cup b) = \delta a \cup b = (-1)^{\deg a} a \cup \delta(b)$. These two conditions are compatible, precisely because of what we just proved. Using the relation $\delta_h \delta_v = -\delta_v \delta_h$ [horizontal and vertical], we can define the cup-product by dimension shift. This is [still] an exercise; to convince yourself that this is exactly the compatibility necessary.

- Given $H \subseteq G$ a subgroup, then the restriction $\mathrm{res}_{G/H}(a \cup b) = \mathrm{res}(a) \cup \mathrm{res}(b)$, the restriction is a ring homomorphism. Geometrically this is clear; in algebraic topology, a map induced by a geometric map gives a ring homomorphism on cohomology, i.e., respects the cup product. That's an exercise; and of course, the proof is through dimension shifting.
- If, again, $H \subseteq G$, then $\mathrm{cor}(\mathrm{res}(a) \cup b) = a \cup \mathrm{cor}(b)$. This makes sense; for if $a \in H^i(G, A)$, and $b \in H^j(H, B)$, then everything winds up in $H^{i+j}(G, A \otimes B)$. Again, the proof of this is through dimension shifting. And then you just have to check in dimension zero.

These are given as exercises. Of course, they can be found in any book on group cohomology, but it's better to do it on your own.

We can write down a formula for the cup-product on the level of cocycles, or even cochains. Recall that $Q_\bullet$ is the homogeneous standard resolution. We want $\phi_{p,q}$ giving a homotopy approximation to $G \to G \times G$.

$$\phi_{p,q} : Q_{p+q} \longrightarrow Q_p \otimes Q_q$$

How do we define the map?

- If $p, q \geq 0$, then

$$\phi_{p,q} : \sigma_0 \otimes \cdots \sigma_{p+q} \mapsto (\sigma_0 \otimes \cdots \otimes \sigma_p) \otimes (\sigma_p \otimes \cdots \otimes \sigma_{p+}).$$

- If $p \geq 1$, $q \geq 1$, then

$$\phi_{-p,-q} : \sigma_1^* \otimes \cdots \otimes \sigma_{p+q}^* \mapsto (\sigma_1^* \otimes \cdots \otimes \sigma_p^*) \otimes (\sigma_{p+1}^* \otimes \cdots \otimes \sigma_{p+q}^*).$$

- $p \geq 0$, $q \geq 1$. Then

$$\begin{aligned}
\phi_{p,-p-q}(\sigma_1^* \otimes \cdots \otimes \sigma_q^*) &\mapsto \sum_{s_1,\cdots,s_p \in G} (\sigma_1 \otimes s_1 \otimes \cdots \otimes s_p) \otimes (s_p^* \otimes \cdots \otimes s_1^* \otimes \sigma_1^* \otimes \cdots \otimes \sigma_q^*) \\
\phi_{-p-q,p}(\sigma_1^* \otimes \cdots \otimes \sigma_q^*) &\mapsto \sum_{s_1,\cdots,s_p \in G} (\sigma_1^* \otimes \cdots \otimes \sigma_q^* \otimes s_1^* \otimes \cdots \otimes s_p^*) \otimes (s_p \otimes \cdots \otimes s_1 \otimes \sigma_1) \\
\phi_{p_q,-q}(\sigma_0 \otimes \cdots \otimes \sigma_p) &\mapsto \sum_{s_1,\cdots,s_q \in G} (\sigma_0 \otimes \cdots \otimes \sigma_p \otimes s_1 \otimes \cdots \otimes s_q) \otimes (s_q^* \otimes \cdots \otimes s_1^*) \\
\phi_{-q,p+q} : \sigma_0 \otimes \cdots \otimes \sigma_p &\mapsto \sum_{s_1,\cdots,s_q \in G} (s_1^* \otimes \cdots \otimes s_q^*) \otimes (s_q \otimes \cdots \otimes s_1 \otimes \sigma_0 \otimes \cdots \otimes \sigma_p)
\end{aligned}$$

Given all this, one should check that $\delta(a \cup b) = \delta a \cup b + (-1)^{\deg a} a \cup \delta b$.

It's comforting to know that these exist, though using them might be a bit unwieldly.

Exercises Formula for cup-product in low dimensions.

- $a \in \widehat{H}^1(G,A)$, $b \in \widehat{H}^{-1}(G,B)$. Recall that a class in $\widehat{H}^{-1}$ has an interpretation as an element of B. Show that $a \cup b = \overline{x_0}$ where

$$x_0 = \sum_{\tau \in G} a(\tau) \otimes \tau b$$

  Hint: Use the two exact sequences

$$0 \longrightarrow A \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \longrightarrow A'' \longrightarrow 0$$

$$0 \longrightarrow A \otimes_{\mathbb{Z}} B \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} B \longrightarrow A'' \otimes_{\mathbb{Z}} B \longrightarrow 0$$

- $a \in \widehat{H}^{-1}(G,A)$, $\overline{\sigma} \in \widehat{H}^{-2}(G,\mathbb{Z})$. The latter thing is the first homology group with coefficients in $\mathbb{Z}$, i.e., the abelianization of G G^{ab}. Then $a \cup \overline{\sigma} = \overline{s(\sigma)} \in \widehat{H}^{-1}(G,A)$.
- $a \in \widehat{H}^2(G,A)$, $\overline{\sigma} \in \widehat{H}^{-2}(G,\mathbb{Z}) = G^{\mathrm{ab}}$. Then $a \cup \overline{\sigma} = \sum_{\tau \in G} a(\tau,\sigma) \in \widehat{H}^0(G,A)$.

Cohomology of cyclic groups So let $G = \mathbb{Z}/n\mathbb{Z} = \langle s \rangle$. We can resolve it as

$$\begin{array}{ccccccc} & & 0 & & 1 & & 2 \\ \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] & \xrightarrow{s-1} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z}[G] \end{array}$$

Tensor; $\otimes_{\mathbb{Z}[G]} A$, and then dualize, to get

$$H^\bullet(\to A \overset{N}{\to} A \overset{s-1}{\to} A \overset{N}{\to} \cdots) = H^\bullet(G,A)$$

So $\widehat{H}^i(G,A) \cong \widehat{H}^{i+2}(G,A)$ for all $i \in \mathbb{Z}$.

Exercise This isomorphism depends on the choice of a generator s of G.

For example, when $A = \mathbb{Z}$, then $\widehat{H}^{\text{odd}}(G, \mathbb{Z}) = 0$. And $\widehat{H}^{\text{even}}(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. What about $\widehat{H}^2(G, \mathbb{Z})$/ Look at

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Now, $\mathbb{Q}$ has no cohomology whatsoever.[6] For it's a torsion $\mathbb{Q}$-vector space. So $\widehat{H}^(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \cong \widehat{H}^2(G, \mathbb{Z})$. But $\widehat{H}^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$. Thus, $s \,!\, \chi_s \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) - \widehat{H}^2(G, \mathbb{Z})$, and $\chi_s(s) = \frac{1}{n} \bmod \mathbb{Z}$.

Exercise Show that in $\widehat{H}^i(G, A) \cong \widehat{H}^{i+2}(G, A)$, the isomorphism is $\chi_s \cup \cdot$.

Here's the trick to doing it. If you can do it with a universal case, you win. That reduces you to $A = \mathbb{Z}$. When you do it with coeffs in $\mathbb{Z}$, well, you want to represent all these maps explicitly, and if you want you can use the formulas, though it shouldn't be necessary; just use proprties. Then ame up with explicit way of writing down this two cocycle χ_s. And after that, it's not too bad.

Herbrand quotient In general, it's harder to deal with individual cohomology groups than with Euler characterstics.

Okay, we still have G a finite cyclic group. We define the Euler characteristic by

$$h(G, A) = \frac{\#(\widehat{H}^{\text{even}}(G, A))}{\widehat{H}^{\text{odd}}(G, A))},$$

provided that both are finite. And the long exact sequence tells us that, given $0 \to A \to B \to C \to 0$ an exact sequence of $\mathbb{Z}[G]$-modules, and $h(G, \cdot)$ defined for two of the three modules, then h is defined for all of them, and

$$h(B) = h(A)h(C).$$

[6] If G is a finite group, then $\widehat{H}^i(G, A)$ is always a torsion, abelian group. And in fact, it's always killed by $\#G$. For you can take $\widehat{H}^i(G, A) \overset{\mathrm{res}_{G,\{e\}}}{\to} \widehat{H}^i(e, A) \overset{\mathrm{cor}}{\to} \widehat{H}^i(G, A)$; the thing in the middle is zero, while the composition is multiplication by $\#G$.

Herbrand's quotient As before, $G = \mathbb{Z}/n\mathbb{Z} = \langle s \rangle$, A a G-module. $h(A) \overset{\text{def}}{=} \frac{h^{\text{even}}(A)}{h^{\text{odd}}(A)}$.

Lemma If A is finite, then $h(A) = 1$.

Proof A is a cyclic group. Look at $\widehat{H}^0(A) = \frac{A^G}{N_G A}$; $\widehat{H}^1(A) = \frac{\ker(N_G|_A)}{I_G A}$. We've got

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{s-1} A \longrightarrow A_G \longrightarrow 0$$

Since A is finite, $\mathrm{Card}(A^G) = \mathrm{Card}(A_G)$. And

$$0 \longrightarrow \widehat{H}^1(A) \longrightarrow A_G \xrightarrow{N_G} A^G\ \widehat{H}^0(G, A) \longrightarrow 0$$

◇

The lemma tells you that $h(A)$ depends only on $A \otimes_{\mathbb{Z}} \mathbb{Q}$, if A is finitely generated.

We'll state the following, but defer proof as long as possible.

Definition $h_{\text{triv}}(A) = h(A \text{ with trivial } G\text{-action })$, if defined.

Proposition $G = \mathbb{Z}/p\mathbb{Z}$, $h_{\text{triv}}(A)$ defined. Then

$$h(A)^{p-1} = \frac{h_{\text{triv}}(A^G)^p}{h_{\text{triv}}(A)} = \frac{h_{\text{triv}}(A_G)^p}{h_{\text{triv}}(A)}$$

and every term is defined.

Theorem [Tate] G a finite group, A a G-module [G-representation]. G is cohomologically trivial, in the sense that $\widehat{H}^i(H, A) = 0$ for all $i \in \mathbb{Z}$ and subgroups $H \subset G$, $\iff$ $\exists i_0 \in \mathbb{Z}$ so that $\widehat{H}^{i_0}(H, A) = 0 = \widehat{H}^{i_0+1}(H, A)$ for all $H \subset G$.

Proof ($\Leftarrow$) By induction on the cardinality of G. If $\mathrm{Card}(G)$ is not a prime power, then for every p-Sylow subgroup $G_p \subsetneq G$, by induction $\widehat{H}^i(G_p, A) = 0$ for all $i \in \mathbb{Z}$. So $\widehat{H}^i(G, A) = 0$.[7]

So now we may assume that G is a p-group. G is supersolvable, so there's $H \trianglelefteq G$ so that $G/H \cong \mathbb{Z}/p\mathbb{Z}$.

Recall that, in general, given $H \trianglelefteq G$ there's a spectral sequence given by $E_2^{i,j} = H^i(G/H, H^j(H, A))$. This comes from a composition of spectral sequences; $(?)^G = ((?)^H)^{G/H}$. If $j > 0$, then $H^j(H, A) = \widehat{H}^j(H, A) = 0$; so the spectral sequence collapses, and converges to $H^{i+j}(G, A)$. Thus, $H^i(G, A) = H^i(G/H, A^H)$ for every i.

In the case at hand, $G/H = \mathbb{Z}/p\mathbb{Z}$; so if it vanishes for two it vanishes for all. For if $i \geq i_0$,

$$\widehat{H}^i(G/H, A^H) \;=\; 0.$$

And by shifting, can assume that $i_0 = 3$, $i_0 + 1 = 4$. Then

$$\widehat{H}^i(G/H, A^H) \;=\; H^i(G, A)$$

So in particular, $H^i(G, A) = 0$ for $i = 2, 5$. In other words, universal vanishing at i_0 and $i_0 + 1$ gives the same at $i_0 - 1$ and $i_0 + 2$.$\diamond$

We can seemingly strengthen this statement.

$\iff$ for every $p \mid \mathrm{Card}(G)$ there's an $i_p \in \mathbb{Z}$ so that, for all p-subgrouops $H_p \subseteq G$, $\widehat{H}^{i_p}(H_p, A) = 0 = \widehat{H}^{i_p+1}(H_p, A)$.

This looks stronger, but it really doesn't do anything.

Exercise $i > 0$, $H \trianglelefteq G$, A, a G-module, $\widehat{H}^j(H, A) = 0$ for $0 < j < i$. Then

$$0 \longrightarrow H^i(G/H, A) \xrightarrow{\text{inf}} H^i(G, A) \xrightarrow{\text{res}} H^i(H, A)$$

is exact. Convince yourself that this is an immediate consequence of the spectral sequence, and then go back and prove it directly. Then use this to avoid the argument above using Hoschild-Serre.

[7]

1. $\widehat{H}^i(G_p, A)$ is well-defined up to canonical isomorphism.
2. $\widehat{H}^i(G, A) \overset{\text{res}}{\hookrightarrow} \oplus_{p \mid \# A} \widehat{H}^i(G_p, A)$ is injective. Well, the kernel is killed by $[G : G_p]$ for every p. But every element of the source is torsion, whereas the gcd $= 1$: so the kernel is killed by one, and it's trivial.

Theorem A a G-module, G finite, for every subgroup $H \subseteq G$ we have

1. $\widehat{H}^{-1}(H, A) = 0$.
2. $\widehat{H}^0(H, A)$ is cyclic of order $\#H$.

Then for any generator $a \in \widehat{H}^0(G, A)$, the cup product gives an isomorphism $\widehat{H}^i(G, \mathrm{Z}) \overset{a\cup\cdot}{\to} \widehat{H}^i(G, A)$ for every i.

Proof We form a mapping cone, á la algebraic topology. First, make a deformation so that the map becomes a deformation.

$$0 \longrightarrow \mathrm{Z} \xrightarrow{(a,\iota)} A \oplus \mathrm{Z}[G] \longrightarrow C \longrightarrow 0$$

Write down the long exact sequence from this. Get

$$\widehat{H}^{-1}(H, \mathrm{Z}) \longrightarrow \widehat{H}^{-1}(H, A) \longrightarrow \widehat{H}^{-1}(H, C) \longrightarrow \widehat{H}^0(H, \mathrm{Z}) \longrightarrow \widehat{H}^0(H, A)\widehat{H}^0(H, C) \longrightarrow \widehat{H}^1(H, \mathrm{Z})$$

But the first two and the last one are zero; and there's an isomorphism $\widehat{H}^0(H, \mathrm{Z}) \overset{\cong}{\to} \widehat{H}^0(H, A)$. So then $\widehat{H}^i(H, C) = 0$ for all $i \in \mathrm{Z}$.$\diamond$

Theorem G finite, A a G-module. Assume for all $H \subseteq G$

1. $\widehat{H}^1(G, A) = 0$.
2. $\widehat{H}^2(H, A)$ is cyclic of order $\mathrm{Card}(H)$.

Then for every generator $a \in \widehat{H}^2(G, A)$, $a \cup \cdot : \widehat{H}^i(G, \mathrm{Z}) \overset{\cong}{\to} \widehat{H}^{i+2}(G, A)$ is an isomorphism.

Proof Dimension shift from previous theorem.

Exercise For all $H \subseteq G$, $\mathrm{res}\, a$ is a generator of $\widehat{H}^2(H, A)$.

Local class field theory Let K be a complete discrete valuation ring, with residue field $\kappa \stackrel{\text{def}}{=} \mathcal{O}_K/\mathfrak{m}_K$ is finite.[8] We'll try to understand K^{ab}, the maximal abelian extension of K. Now, Galois theory says that if we know this Galois group, then to understand fields in betwen, all we have to do is take finite quotients of this group. The main theorem in local class field theory is this: there's a map

$$\text{rec}_K\ K^\times \longrightarrow \text{Gal}(K^{\text{ab}}, k) = \text{Gal}(K^{\text{sep}}, K)^{\text{ab}}$$

Note that the right-hand side is compact, but the left isn't. So there's no way this is going to be an isomorphism. But, the image of the map is dense; and it's actually an injection.

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\cong"] & K^\times \arrow[r] \arrow[d, "\text{rec}_K"] & \mathbb{Z} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I \arrow[r] & \text{Gal}(K^{\text{ab}}, K) \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & 1
\end{tikzcd}$$

So then for every subgroup of finite index $U \subseteq K^\times$, ! a finite abelian extension L/K. L is the fixed field of the image of U. This gives us a complete understanding; we know all the abelian extensions. For $K^\times$ is something we have a pretty good grip on. And if this holds, then $U = N_{L,K}(L^\times)$.

For every abelian extension L of K, there's a map

$$\frac{K^\times}{N_{L,K}(L^\times)} \xrightarrow{\cong} \text{Gal}(L, K)$$

Furthermore, there's an existence theorem. Every subgroup of finite index is actually of type $U = N_{L,K}(L^\times)$.

Our goal in local class field theory is to demonstrate this.

[8]As a generalization, one can do almost everything we'll do here if we just assume that κ is perfect, and $\text{Gal}(\overline{\kappa}, \kappa) = \widehat{\mathbb{Z}}$ a free cyclic group. One usually says that κ is a quasifinite field.

Brauer groups of local fields We start off with a "review" of Brauer groups.

- Semisimple algebras over a field. Such a beast decomposes into a product of simple things.
- A simple algebra over a field k is a finite dimensional algebra over k with unity, with no two-sided ideals; the only ones are (0) or the whole thing, A. Every simple algebra has a center, $Z(A)$. And since A is simple, it's a field, certainly containing k. Actually, we usually assume k really is the center; $Z(A)=k$, and A is a central simple algebra.
- **Theorem** $A \cong M_{n\times n}(D)$, where D is a central division algebra; $Z(D)=k=Z(A)$.

The Brauer group of k is the set of equivalence classes of central simple algebras over k, where $A_i = M_{n_i\times n_i}(D_i)$ are equivalent $\iff$ $D_1 \cong D_2$ over k. We can put a group law on this by $[A_1]\cdot[A_2] = [A_1 \otimes_k A_2]$. It's clearly associative. And $[A]^{-1} = [A^{\mathrm{opp}}]$. For $D \otimes_k D^{\mathrm{opp}} \cong \mathrm{End}_k(D)$.[9]

Cohomological Interpretation Let k be a field. Then we can identify, in a functorial way, $\mathrm{Br}(k) \cong H^2(\mathrm{Gal}(k^{\mathrm{sep}},k),(k^{\mathrm{sep}})^\times)$. The right-hand side is $\lim_{\substack{\to\\ L}} H^2(\mathrm{Gal}(L,K),L^\times)$. If $K \subset M \subset K$, then $H^2(\mathrm{Gal}(M,k),M^\times) \overset{\inf}{\hookrightarrow} H^2(\mathrm{Gal}(L,K),L^\times)$, by Hilbert 90.

Let $\mathrm{Br}(L,k)$ be the elements in $\mathrm{Br}(k)$ which are split by L; $A\otimes_k L = 0$ in $\mathrm{Br}(L)$.

$$\begin{tikzcd}
\mathrm{Br}(k) \arrow[r, phantom, "\cong"] & H^2(\mathrm{Gal}(k^{\mathrm{sep}},k),(k^{\mathrm{sep}})^\times) \\
\mathrm{Br}(L,k) \arrow[u, hook] \arrow[r, phantom, "\cong"] & H^2(\mathrm{Gal}(L,k),k^\times) \arrow[u, hook]
\end{tikzcd}$$

$$0 \longrightarrow H^2(\mathrm{Gal}(M^{\mathrm{sep}},k),M^\times) \longrightarrow H^2(\mathrm{Gal}(k^{\mathrm{sep}},k),(k^{\mathrm{sep}})^\times) \longrightarrow H^2(\mathrm{Gal}(k^{\mathrm{sep}},M),(k^{\mathrm{sep}})^\times)$$

Can take limits, since direct limit is an exact functor.

$A \in \mathrm{Br}(K,k)$ is a central simple algebra over k which is split by M. Then $A\otimes_k K \overset{\cong}{\to} M_{n\times n}(K)$. Fix an isomorphism f. Then for every $\sigma \in \mathrm{Gal}(K,k)$, $f\sigma f^{-1} \in \mathrm{Aut}_K(M_{n\times n}(K))$.

[9]Check this.

But the automorphism group is $PGL_n(K)$. Thus, every σ gives an element in $PGL_n(K)$. This is an example of descent.[?]

So we get an element in $H^1(\mathrm{Gal}(K,k), PGL_n(K))$.

$$1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$$

By Hilbert 90, $H^1(\mathrm{Gal}(K,k), GL_n(K)) = 0$.

$$\begin{array}{l} 1 \longrightarrow K^\times \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1 \\ \qquad\qquad\qquad 0 \longrightarrow H^1(\mathrm{Gal}(K,k), PGL_n(K)) \xrightarrow{\cong} H^2(\mathrm{Gal}(K,k), K^\times) \end{array}$$

Now, take L/K a cyclic extension of order n. Insist that K is a complete discrete valuation ring, with finite residue field. Let $G = \mathrm{Gal}(L,K)$. Then $\widehat{H}^\bullet(G, L^\times) = \widehat{H}^{\bullet+2}(G, L^\times)$; cyclic of order 2. And $\widehat{H}^{\mathrm{odd}}(G, L^\times) = 0$, by Hilbert 90. So the only thing to worry about is the Brauer group.

Brief aside, in fact an essential idea. Let L/K be a finite Galois extension. Look at $\widehat{H}^\bullet(\mathrm{Gal}(L,K), L)$. The normal basis theorem says that $L = K[G]$. So this cohomology of this is zero.

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \longrightarrow \mathrm{Z} \longrightarrow 1$$

Want to compute the Herbrand quotient. We know that $h(L^\times) = h(\mathrm{Z}) \cdot h(\mathcal{O}_L^\times)$. $h(\mathrm{Z}) = n$. What about the other? Take $\Lambda \subseteq \mathcal{O}_L^\times$ stable under the Galois group. We then get $h(L^\times) = n \cdot h(\Lambda)$. With some work, perhaps we'll show that $h(\Lambda) = 1$.

Situation is this. We have L/K a cyclic Galois extension of order n. Want to show

$$h(G, L^\times) = n.$$

In other words, $\mathrm{Card}(H^2(G, L^\times)) = n$.

The valuation map gives us

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \longrightarrow \mathrm{Z} \longrightarrow 1$$

$$h(G, \mathrm{Z}) = n$$

Proposition L/K finite Galois, K a complete discretely valued field. Then there's a subgroup U so that $1+\mathfrak{P}_L^N\mathcal{O}_L \subseteq U \subseteq 1+\mathfrak{P}_L\mathcal{O}_L$[10] and U has trivial cohomology; $Hi(G, U) = 0$ for all $i \geq 1$.

Proof By the normal basis theorem, there's $x \in L$ so that as a $K[G]$-module, $L = K[G]\cdot x$. We may assume $\mathcal{O}_K[G]x \subseteq \mathfrak{P}_L^M$ for some $M \gg 0$. Let $\Lambda = \mathcal{O}_K[G]x$; think of it as a lattice. We may further assume that $\Lambda \cdot \Lambda \subseteq \Lambda$.[11] So $1+\Lambda$ is a subgroup of the principal units $1+\mathfrak{P}_L \subseteq \mathcal{O}_L^\times$. This is good, since we have a filtration $\mathrm{fil}^i(1+\Lambda) = 1+\pi_K^i\Lambda$. Clearly,

$$\frac{\mathrm{fil}^i}{\mathrm{fil}^{i+1}} \;\cong\; \Lambda \otimes_{\mathcal{O}_K} \kappa$$

where the isomorphism is as a $\kappa[G]$-module. But

$$\Lambda \otimes_{\mathcal{O}_K} \kappa \;\cong\; \kappa[G]$$

From this, we know that $H^i(G, \mathrm{fil}^i / \mathrm{fil}^{i+m}) = 0$ for all $i, m \geq 1$, which implies the proposition.$\diamond$

[10] If the residue field is finite, this just means U is of finite index.

[11] In general, you ask whether $(\pi_L^n\Lambda)(\pi^n\Lambda) \subseteq \pi^n\Lambda$. If n large eonugh, then you're okay.

Summary We've proved a substantial part of local classfield theory. Specifically, for every L/K finite Galois, $H^2(\mathrm{Gal}(L,K), L^\times) \cong n^{-1}\mathbb{Z}/\mathbb{Z}$ cyclic of order n. And using the Frobenius element and the valuation, this isomorphism is canonical. Fundamentally, $U_{L,K} \mapsto \frac{1}{n}$. The limit version is to consider $H^2(\mathrm{Gal}(K^{\mathrm{sep}}, K), (K^{\mathrm{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}$. Using the finite version, by Tate's theorem we see that

$$\widehat{H}^i(\mathrm{Gal}(L,K), \mathbb{Z}) \xrightarrow[\cong]{U_{L,K}\cup} \widehat{H}^{i+2}(\mathrm{Gal}(L,K), L^\times)$$

Take $i = -2$. This then says that

$$\mathrm{Gal}(L,K)^{\mathrm{ab}} \underset{\mathrm{rec}_{L,K}}{\overset{\cong}{\rightleftarrows}} \frac{K^\times}{N_{L,K}(L^\times)}$$

Notice that the norm group is an open subgroup of finite index. The arrow going right is often called the norm residue map, or norm residue symbol, some such nonsense. Ultimately, you get

$$\mathrm{Gal}(K^{\mathrm{sep}}, K)^{\mathrm{ab}} \longleftarrow \lim_{\leftarrow} \frac{K^\times}{\text{norm subgroups}}$$

In particular, every open subgroup U of finite index in $K^\times$ which contains a norm subgroup corresponds to an abelian extension of K.

Lubin-Tate formal groups We'll construct a commutative one-dimensional formal group F over $\mathcal{O}_K$ with $\mathcal{O}_K \hookrightarrow \mathrm{End}_{\mathcal{O}_K}(F)$. Let $\pi_K \in \mathcal{O}_K$. Anyways, we can ask for $F[\pi_K^n] = \ker(\pi_K^n)$. Can look at the points in the generic fiber, $F[\pi_K^n](\overline{K}) = F[\pi_K^n](K^{\mathrm{sep}})$ a finite set; and the group law gives you a group structure.

Can think of the inductive limit $\lim_{\rightarrow} F[\pi_K^n](\overline{K})$, an $\mathcal{O}_K$-module. And it will turn out that this is $\cong K/\mathcal{O}_K$, again as an $\mathcal{O}_K$-module. And $\mathrm{End}_{\mathcal{O}_K}(K/\mathcal{O}_K) = \mathcal{O}_K$.

The Galois group $\mathrm{Gal}(K^{\mathrm{sep}}, K)$ operates on $F[\pi_K^n](K^{\mathrm{sep}})$. Each element of the Galois group thus works on $\lim_{\rightarrow} F[\pi_K^n](\overline{K})$ as an automorphism, and this gives us a representation

$$
\begin{tikzcd}
\mathrm{Gal}(K^{\mathrm{sep}}, K) \arrow[r, "\rho_F"] \arrow[d] & \mathcal{O}_K^\times \\
\mathrm{Gal}(K^{\mathrm{ab}}, K) \arrow[ur] &
\end{tikzcd}
$$

The factorization means that it's an abelian representation. And in fact, it factors even more

$$
\begin{tikzcd}
\mathrm{Gal}(K^{\mathrm{sep}}, K) \arrow[d] \arrow[dr, "\rho_F"] & \\
\mathrm{Gal}(K^{\mathrm{ab}}, K) \arrow[r] \arrow[d] & \mathcal{O}_K^\times \\
\mathrm{Gal}(K \cdot F[\pi_K^\infty](K^{\mathrm{sep}}), K) \arrow[ur, hook, "\cong"'] &
\end{tikzcd}
$$

[Later on we'll see why this is an isomorphism.]

Let $K_n = F[\pi_K^n](\overline{k})$. The big picture is this.

$$\begin{tikzcd}
& K^{\mathrm{ab}} \arrow[d, dash, "="] & \\
& K^{\mathrm{unr}}K_\infty \arrow[dl, dash, "\mathcal{O}_K^\times"'] \arrow[dr, dash, "\hat{\mathbb{Z}}"] & \\
K^{\mathrm{unr}} \arrow[dr, dash, "\hat{\mathbb{Z}}"'] & & \cup_n K_n \arrow[dl, dash, "\mathcal{O}_K^\times"', "\text{totally ramified}"] \\
& K &
\end{tikzcd}$$

If we're lucky, we'll prove that $\mathrm{fil}^i(\mathcal{O}_K) = 1 + \pi_K^i \mathcal{O}_K$ corresponds to the upper numbering filtration under the reciprocity law rec_K.

So much for the big picture. Let's get down to specifics.

Formal group laws What we say will be for one-dimensional formal groups; but they can be generalized to higher dimensions. Let's work over a ring R. Then basically we want the formal spectrum $\mathrm{Spf}\ R[\![x]\!] \times_{\mathrm{Spec}\, R} \mathrm{Spf}\ R[\![x]\!] \to \mathrm{Spf}\ R[\![x]\!]$. The left-hand side is, essentially, $\mathrm{Spf}\ R[\![x, y]\!]$. So we have

$$\begin{array}{c}
\mathrm{Spf}\ R[\![x]\!] \times_{\mathrm{Spec}\, R} \mathrm{Spf}\ R[\![x]\!] \longrightarrow \mathrm{Spf}\ R[\![x]\!] \\[2ex]
\mathrm{Spf}\ R[\![x, y]\!] \\[2ex]
R[\![x, y]\!] \ni F(x, y) \longleftarrow\!\shortmid\ x
\end{array}$$

Definition A one-dimensional commutative formal group law over R is a power series $F(x, y) \in R[\![x, y]\!]$ satisfying

unit $F(0, y) = y$, $F(x, 0) = x$.

commutative $F(x,y) = F(y,x)$.

associative $F(x, F(y,z)) = F(F(x,y),z)$.

inverse There's a [unique] $g(x)$ so that $F(x, g(x)) = F(g(x), x) = 0$.

smooth $F(x,y) \equiv x + y \bmod \deg 2$.[12]

We're not claiming that these are all independent axioms. For example, property 4 essentially comes from the implicit function theorem and the other properties.

What's an endomorphism? Given a group law F and another one, G, well, it should certainly be some $F \xrightarrow{\alpha} G$. This means that $G(\alpha(x), \alpha(y)) = \alpha(F(x,y))$. So α itself is a power series; $\alpha \in R[\![x]\!]$. Any power series satisfing this condition is said to be an endomorphism.

Idea of constructing Lubin-Tate formal groups is as follows. Let $\mathfrak{F}_\pi = \{f(x) \in \mathcal{O}_K[\![x]\!] : f(x) \equiv \pi_K x \bmod \deg 2, f(x) \equiv x^q \bmod \pi_K\}$, where $q = p^f$ is the cardinality of the residue field κ. Take $f(x) \in \mathfrak{F}_\pi$. To first order, it looks like multiplication by π. Want $f(x)$ to be an endomorphism of a 1-dimensional commutative formal group law $\mathfrak{F}_f$.

[12] Looks like this comes from property one.

Still on Lubin-Tate groups and formal complex multiplication.[13] We've got $\mathcal{O}_K$ a complete discrete valuation ring, with finite residue field $\kappa = \mathcal{O}_K/\pi_K\mathcal{O}_K \cong \mathrm{F}_q$. Set $\mathfrak{F}_\pi = \{f \in \mathcal{O}_K[\![x]\!] : f(x) \equiv \pi x \bmod \deg 2; f(x) \equiv x^q \bmod \pi\}$. Then pick $f \in \mathfrak{F}_\pi$. The idea is that we'll construct a one-parameter formal group [law] form this, together with endomorphisms by $\mathcal{O}_K$ in such a way that the polynomial f gives the endomorphism by π.

Proposition Let $f, g \in \mathfrak{F}_\pi$. Let $\phi_1(x_1, \cdots, x_n)$ be a linear form with coefficients in $\mathcal{O}_K$. Then there's a unique formal composiiton law $\phi(x_1, \cdots, x_n) \in \mathcal{O}_K[\![x_1, \cdots, x_n]\!]$ with $\phi(x_1, \cdots, x-n) \equiv \phi_1(x_1, \cdots, x_n) \bmod \deg 2$, and $f(\phi(x_1, \cdots, x_n)) = \phi(g(x_1), \cdots, g(x_n))$.

Proof Since this is just a formal power series, we construct ϕ by successive approximation. Suppose we have already $\phi_r(x_1, \cdots, x_n)$ so that

- $\phi_r(x_1, \cdots, x_n) \equiv \phi_1(x_1, \cdots, x-n) \bmod \deg 2$.
- $f(\phi_r(x_1, \cdots, x_n)) \equiv \phi_r(g(x_1), \cdots, g(x_n))$.

Let $\phi_{r+1}(x_1, \cdots, x_n) = \phi_r(x_1, \cdots, x_n) + E_{r+1}(x_1, \cdots, x_n)$. Then

$$\begin{aligned} f(\phi_{r+1}(x_1, \cdots, x_n)) = \phi_{r+1}(g(x_1), \cdots, g(x_n)) &\equiv f(\phi_r(x_1, \cdots, x_n)) + \pi E_{r+1}(\underline{x}) - \phi_r(g(x_1), \cdots, g(x_n)) - E_{r+1}(g(x_1), \cdots, g(x_n)) \bmod \deg r+2 \\ &\equiv f(\phi_r(x_1, \cdots, x_n)) - \phi_r(g(x_1), \cdots, g(x_n)) + \pi E_{r+1}(x_1, \cdots, x_n) - \pi^{r+1} E_{r+1}(x_1, \cdots, x_n) \bmod \deg r+2 \\ &\equiv f(\phi_r(x_1, \cdots, x_n)) - \phi_r(g(x_1), \cdots, g(x_n)) + \pi(1-\pi^r) E_{r+1}(x_1, \cdots, x_n) \end{aligned}$$

Now, $1 - \pi^r \in \mathcal{O}_K^\times$. What we have left to show is that π divides $f(\phi_r(x_1, \cdots, x_n)) - \pi_r(g(x_1), \cdots, g(x_n))$. So consider it mod $\pi = \pi_K$.

$$\begin{aligned} f(\phi_r(x_1, \cdots, x_n) - \phi_r(g(x_1), \cdots, g(x_n)) &\equiv \phi_r(x_1^q, \cdots, x_n^q) - \phi_r(x_1^q, \cdots, x_n^q) \bmod \pi \\ &\equiv 0 \bmod \pi \end{aligned}$$

$\diamond$

Given $f \in \mathfrak{F}_\pi$, we can apply the proposition to get some properties.

[13]This is from a seven page paper they wrote in 1965 or so, in *Annals of Mathematics*.

- There's a unique $F(x,y) \in \mathcal{O}_K[\![x,y]\!]$ so that $F(f(x), f(y)) = f(F(x,y))$, and $F(x,y) \equiv x + y \bmod \deg 2$.

  Let's check that this is a formal group law.

  - $F(x,0) = x$, $F(-,y) = y$; $F(f(x),0) = f(F(x,0))$. In other words, the polynomial $h(x) = F(x,0)$ satisfies $h(f(x)) = f(h(x))$, $h(x) \equiv \bmod \deg 2$, and the same holds for $h'(x) = x$.
  - $F(x,y) = F(y,x)$, since $F(y,x)$ satisfies the defining conditions for $F(x,y)$.
  - Associativity; $F(x, F(y,z)) = F(F(x,y),z)$. Well, let G_1 be the left-hand side, and G_2 the right. Then we know $f(G_i(x,y,z)) = G_i(f(x), f(y), f(z))$. And $G_i(x,y,z) \equiv x + y + z \bmod \deg 2$. So they must be equal.
  - Existence of inverse. This comes from the implicit function theorem.

- For every $a \in \mathcal{O}_K$ there's a unique $[a]_f(x) \in \mathcal{O}_K[\![x]\!]$ so that $f([a]_f(x)) = [a]_f(f(x))$ and $[a]_f(x) \equiv ax \bmod \deg 2$. Note that $f(x) = [\pi]_f(x)$.

  Chekkitout.

  - $F_f([a]_f(x), [a]_f(y)) = [a]_f(F_f(x,y))$ Again, left-hand side is G_1, right-hand side is G_2. Then $f(G_i(x,y)) = G_i(f(x), f(y))$ for $i = 1,$. Then $G_i(x,y) = ax + ay \bmod \deg 2$, and we're done.

- Given $f, g \in \mathfrak{F}_\pi$, we want to construct an isomorphism intertwining the formal group laws given by f and g, and show the choice didn't really matter. Want $\psi_{f,g}(x)$ so that $\psi_{f,g}(x) \equiv x \bmod \deg 2$, and $\psi_{f,g}(F_g(x,y)) = F_f(\psi_{f,g}(x), \psi_{f,g}(y))$. Furthermore, this isomorphism $\psi_{f,g}$ should carry over the endomorphisms; $\psi_{f,g}([a]_g(x)) = [a]_f(\psi_{f,g}(x))$ So F_g and F_f both have endomorpisms b $\mathcal{O}_K$, and we want $F_g \stackrel{\psi_{f,g}}{\to} F_f$.

  From the proposition, there's a unique $\psi_{f,g}(x)$ so that

  - $\psi_{f,g}(x) \equiv x \bmod \deg 2$.
  - $\psi_{f,g}(g(x)) = f(\psi_{f,g}(x))$.

  Gotta verify that $\psi_{f,g}(F_g(x,y)) = F_f(\psi_{f,g}(x), \psi_{f,g}(y))$. LHS is G_1, G_2 is RHS. Then $f(G_i(x,y)) = G_i(g(x), g(y))$, and $G_i(x,y) \equiv x + y \bmod \deg 2$.

  Now check the thing for $[a]_\bullet$.

- $[a_1]_f([a_2]_f(x)) = [a_1 a_2]_f(x)$ for $a_1, a_2 \in \mathcal{O}_K$.

Let's try and use this stuff, I guess. Pick an F_f. The Lubin-Tate formal group is defined over $\mathcal{O}_K$. We have endomorphisms; $\mathcal{O}_K \hookrightarrow \mathrm{End}(F_f)$. Let $a \in \mathcal{O}_K$. Then $\ker([a]_f) = \mathrm{Spec}\,\frac{\mathcal{O}[\![x]\!]}{[a]_f(x)\mathcal{O}[\![x]\!]}$), a finite flat group scheme. Define $K([a]_f) = K(\ker([a]_f)(\overline{K}))$, K adjoined with the roots of $[a]_f$ in some algebraic closure of K. If $a = u\pi^n$, then the kernel is the same as that of $[\pi^n]_f$; the units are automorphisms and have trivial kernel. And all of this depends only on π, not f, because of the isomorphism $\psi_{f,g}$. So it makes sense to define $K_{\pi,n} = K(\ker[\pi^n]_f(\overline{K}))$ for any $f \in \mathfrak{F}_\pi$. Now, $\ker[\pi^n](\overline{K})$ is a finite group with action b $\mathcal{O} = \mathcal{O}_K$.

Choose $f(x) = \pi x + x^q$.[14] Then $[\pi^n]_f(x) = f \circ \cdots \circ f(x) = f_n(x)$. And

$$\begin{aligned} f_n(x) &= f(f_{n-1}(x)) \\ &= f_{n-1}(x) \cdot (\pi + f_{n-1}(x)^{q-1}) \end{aligned}$$

$\ker[\pi^n] - \ker[\pi^{n-1}]$ are roots of f_n which aren't roots of f_{n-1}, i.e., roots of $\pi + f_{n-1}(x)^{q-1}$. And $\pi + f_{n-1}(x)^{q-1}$ is irreducible by the Eisenstein criterion; the polynomial is $\equiv x^{q^{n-1}(q-1)} \bmod \pi$.

Thus, we know that $K_{\pi,n}$ has degree $[K_{\pi,n} : K] = (q-1)q^{n-1}$.[?]

And all these polynomials are actually separable.

[14]That's the simplest possible choice; might as well use it.

Still working with Lubin-Tate groups. We have $K \supseteq \mathcal{O}_K \supseteq \mathfrak{m}_K \ni \pi$, and $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong \mathrm{F}_q$. Let $f \in \mathfrak{F}_\pi$. Then we can construct a Lubin-Tate formal group F_f, where f is an endomorphism of this formal group, and in fact every element of $\mathcal{O}_K$ extends to an endomorphism on the formal group; the correspondence is that $a \in \mathcal{O}_K$ specifies the linear term of the endomorphism; $\mathcal{O}_K \hookrightarrow \mathrm{End}(F_f)$. We then considered $\ker([\pi^n]_f) \subseteq F_f$, a finite flat group scheme over $\mathcal{O}_K$. Set $K_{\pi,n}$ to be the field extension obtained by adjoining the kernel; $K(\ker[\pi^n](\overline{K}))$. Then $\mathrm{Gal}(K_{\pi,n}, K)$ will turn out to be an abelian extension, so that $\mathrm{Gal}(K^{\mathrm{sep}}, K) \rightharpoonup \mathrm{Gal}(K_{\pi,n}, K) \to \mathrm{Aut}(\ker[\pi^n]_f(\overline{K}))$. In the limit version, one has

$$\mathrm{Gal}(K^{\mathrm{sep}}, K) \twoheadrightarrow \mathrm{Gal}(\cup K_{1,n}, K) \longrightarrow \mathrm{Aut}(\lim \ker[\pi^n]_f(\overline{K}))$$

Oddly enough, the limit can be direct or inverse.

Let's analyze $K_{\pi,n}$ over K. Well, $\ker[\pi^n]$ comes from the equation $f_{(n)} = f \circ \cdots \circ f$ n-times; and $\ker[\pi^n] - \ker[\pi^{n-1}]$! $f_{(n)}/f_{(n-1)}$. Choose$f(x) = \pi x + x^q$, the simplest one we have any hope of analyzing. We saw that $f_{(n)}/f_{(n-1)} = f_{(n-1)}^{q-1} + \pi$, an Eisenstein polynomial and thus irreducible over K. Its degree is $q^{n-1}(q-1)$, and so $[K_{\pi,n} : K] = q^{n-1}(q-1)$. Furthermore, $K_{\pi,n}/K$ is automagically Galois; it's the splitting field of $f_{(n)}$.[15] The Galois action commutes with the $\mathcal{O}_K$-action.

Let's verify separability. Clearly $\ker[\pi]$ has all distinct roots, as $f(x) = \pi x + x^q$. We go up inductively then; take the $[\pi^n]$ points, divide by the action of $[\pi]$, and then you're done The key thing to show is that if $a \in \mathfrak{m}(\mathcal{O}_{\overline{K}})$, then $x^q + \pi x + a$ is separable, and all roots are again in $\mathfrak{m}(\mathcal{O}_{\overline{K}})$. Proof is omitted here, though it was sort of amusing.

Anyways, $\mathrm{Card}(\ker[\pi^n]) = q^n$; that's no surprise. And we've proved that there's a surjection

$$0 \longrightarrow \ker[\pi](\overline{K}) \longrightarrow \ker[\pi^{n+1}]_f(\overline{K}) \xrightarrow{[\pi]_f} \ker[\pi^n]_f(\overline{K})$$

The conclusion is that $\lim_{\to} \ker[\pi^{n+1}]_f$ is π-divisible. And $\ker[\pi]_f(\overline{K})$ is a module under $\mathcal{O}_K/\mathfrak{m}_K$, and thus is a 1-dimensional vector space over κ. From some sort of structure theorem, $\ker[\pi^n](\overline{K}) \cong \pi^{-n}\mathcal{O}_K/\mathcal{O}_K$. Thus, as an $\mathcal{O}_K$-module,

$$\lim_{\vec{n}} \ker[\pi^n] \cong \frac{K}{\mathcal{O}_K}.$$

Furthermore,

[15] In doing this stuff we make use of the following; if A an abelian group, and $B \subsetneq A$, then $A - B$ generates the whole thing.

$$\lim_{\overleftarrow{n}} \ker[\pi^n] \cong \mathcal{O}_K.$$

$$\begin{tikzcd}
\mathrm{Gal}(K_{\pi,n}, K) \arrow[r, hook, "\cong"] & \mathrm{Aut}_{\mathcal{O}_K}(\ker[\pi^n](\overline{K})) \arrow[d, phantom, "\cong"] \\
\mathrm{Gal}(K^{\mathrm{sep}}, K) \arrow[u, two heads] & \left(\dfrac{\mathcal{O}_K}{\pi^n \mathcal{O}_K}\right)^{\times}
\end{tikzcd}$$

The top thing is an isomorphism just from counting cardinalities. So everything is isomorphic.

We thus have the following diagram of fields and Galois groups.

$$\begin{tikzcd}
K_{\pi,n} \arrow[d, dash, "(\mathcal{O}_K/\mathfrak{m}_K^{n+1})^{\times}"'] \\
K
\end{tikzcd}$$

$$\begin{tikzcd}
\cup K_{\pi,n} \arrow[dd, dash] & & \\
& \mathrm{Gal}(\cup K_{\pi,n}, K) \arrow[r, "\cong"] & \mathrm{Aut}(\lim_{\overrightarrow{n}} [\pi^n]_f) = \mathcal{O}_K^{\times} \\
K & \mathrm{Gal}(K^{\mathrm{sep}}, K) \arrow[u, two heads] &
\end{tikzcd}$$

We've explicitly constructed this nice, abelian extension.

Uh-oh. The diagram's getting even more complicated.

$$\begin{tikzcd}
K^{\mathrm{ab}} = K^{\mathrm{unr}} \cdot K_\pi \arrow[dd, no head] \arrow[dr, no head] & \\
& \cup K_{\pi,n} = K_\pi \arrow[dd, no head] \\
K^{\mathrm{unr}} \arrow[dr, no head, "\widehat{\mathbb{Z}}"'] & \\
& K
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathrm{Gal}(\cup K_{\pi,n}, K) \arrow[r, "\cong"] & K^{\mathrm{unr}} \\
\mathrm{Gal}(K^{\mathrm{sep}}, K) \arrow[u] &
\end{tikzcd}
\qquad
\mathrm{Aut}(\varinjlim_n [\pi^n]_f) = \mathcal{O}_K^\times$$

So $\mathrm{Gal}(K^{\mathrm{unr}}, K) = \widehat{\mathbb{Z}} \times \mathcal{O}_K^\times \cong (\widehat{K^\times})$, the profinite completion of $K^\times$. And we've constructed the maximal abelian extension.

Since the $f_{(n)}$'s are Eisenstein polynomials, K_π is totally ramified, and as such is disjoint from K^{unr}. I think.

Write

$$f_{(n)}/f_{(n-1)} \quad = \quad \prod_i (x - a_i)$$

where $a_i \in \ker[\pi^n](\overline{K}) - \ker[\pi n - 1](\overline{K})$. So the norm is $N_{K_{\pi,n},K}(a_i) = \pi$, for all i; so π is always the norm.

Inside the tower, we have the reciprocity law. Try it at a finite level. $\mathrm{rec}_{K_{\pi,n},K}(\pi) = \mathrm{id}_{K_{\pi,n}}$. Out of our hat, we pull $\mathrm{rec}_{K^{\mathrm{unr}}_{q^n}}(\pi^m \cdot \mathcal{O}_K^\times) = \mathrm{Fr}_q^m$. That's actually something we'll prove later.

$$\begin{tikzcd}
\varprojlim K^\times \text{norm subgroups} \arrow[rr, "\mathrm{rec}_{K^{\mathrm{unr}}K_\pi,K}"] \arrow[dr, "\cong"'] & & \mathrm{Gal}(K^{\mathrm{unr}}K_\pi, K) = \widehat{K^\times} \\
& \mathrm{Gal}(K^{\mathrm{ab}}, K) \arrow[ur] &
\end{tikzcd}$$

The conclusion is that the reciprocity map is an isomorphism. The point is, every subgroup of finite index in $K^\times$ is a norm subgroup. And when all is said and done,

$$K^{\text{ab}} = K^{\text{unr}} \cdot K_\pi.$$

This is an explicit construction of the maximal abelian extension.

Let's backrack a bit. We picked π, a uniformizer. Suppose ϖ is another uniformizer. K_π and K_ϖ are different, and there's not a hell of a lot you can do about it.

Example time? Consider $\mathbb{Q}_p$. Want to understand the Lubin-Tate formal group associated to this local field. The Lubin-Tate group will turn out to be the multiplicative group, $\mathbb{G}_m$. We wan $(1+x)(1+y) = 1+x+y+xy$. The formal group law is $x+y+xy$. As a uniformizer we have p. Choose f to be $(1+x)^p - 1 = px + \binom{p}{2}x^2 + \cdots + px^{p-1} + x^p$. Choosing this f fixes the group. Every formal group is entitled to multiplication by $\mathbb{Z}_p$.[16]

Anyways, $\ker[p^n](\overline{\mathbb{Q}_p}) = \{\zeta_{p^n}^i - 1 : i \in \mathbb{Z}/p^n\mathbb{Z}\}$. We're looking at

$$\begin{array}{c} \mathbb{Q}_p(\zeta_{p^n}) \\ \Big| \\ \mathbb{Q}_p \end{array}$$

Let's compute the reciprocity law. Think of the global situation $\mathbb{Q}(\zeta_{p^n})$ over $\mathbb{Q}$. This Galois group is $(\mathbb{Z}/p^n\mathbb{Z})^\times$; and ditto for the local case, actually. The reciprocity law is, take an element of $\mathbb{Q}_p\times$ and have it operate on the extension.[?] Let $a \in \mathbb{Q}_p^\times$. Want to find its reciprocity law image. Well, write $a = p^m u$, $u \in \mathbb{Z}_p^\times$. Now, $u \equiv \frac{c}{d} \bmod p^N$ for some really big N, with c, d relatively prime and prime to c. Then $\text{rec}_p(a) = \text{rec}_a(p^m \frac{c}{d})$. Now a leap of faith; local and global reciprocity laws are compatible. And if we take a global element in $\mathbb{Q}$, lok at its reciprocity law map at every p, it'll be trivial at almost all places; and they all multiply together to give a trivial image under the reciprocity law map; the product is 1. So

$$\begin{aligned} \text{rec}_p(a) &= \text{rec}_p(p^m \frac{c}{d}) \\ &= (\prod_{l \neq p} \text{rec}_l(p^m \frac{c}{d}))^{-1} \end{aligned}$$

[16]Remember that, in the multiplicative group, the usual coordinate for *blah* is $1 + blah$.

For finite l, what do you get? In general, the l-adic valuation, times l; some power of Frobenius. At infinity, you pick up a sign. So the product, at the end, becomes $(\frac{c}{d})^{-1}$.

The conclusion is that $\mathrm{rec}_p(a) = u^{-1} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$.

No class on Wednesday.[!]

We've got $\mathcal{O}_K$ a complete DVR, and $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$. We choose $f \in \mathfrak{F}_\pi$, as usual. From this we construct F_f a Lubin-Tate formal group. By considering its division points $\ker[\pi^n]_f(\overline{K})$, well, the coordinates are separable; adjoin them to K, and this gives us a separable field extension $K_{\pi,n}$. And actually, $K_{\pi,n}/K$ is totally ramified. On the other hand, it's a finite abelian extension, with group $(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times$. Let $K_\pi = \cup_n K_{\pi,n}$. Then K_π/K is abelian, with group $\mathcal{O}_K^\times$. On the other hand, we know that we can construct the maximal unramified extension K^{unr}, with group $\widehat{\mathbb{Z}}$. And then $K_\pi K^{\mathrm{unr}}$ is an abelian extension, whose Galois group is the profinite completion of $\mathcal{O}_K^\times$. We'll shortly identify this with the maximal abelian extension of K.

Remember we had a reciprocity law isomorphism, inverse to the following. Suppose we have L over K, with $\mathrm{Gal}(L,K) = G$. We'll try to understand it via the dual.

$$\begin{array}{ccc}
H^{-2}(G,\mathbb{Z}) & \underset{\mathrm{rec}}{\overset{u_{L,K}\cup\cdot}{\underset{\longleftarrow}{\overset{\longrightarrow}{\cong}}}} & H^0(G,L^\times) \\
G^{\mathrm{ab}} & & K^\times/N_{L,K}(L^\times) \\
& & \\
\mathrm{rec}_{L,K}(\overline{a}) & \longleftarrow\!\!\shortmid & \overline{a}
\end{array}$$

And for all $\chi \in \mathrm{Hom}_{\mathrm{gp}}(G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z})$, $\chi(\mathrm{rec}_{L,K}(\overline{a})) = ?$. We've got the long exact sequence

$$\mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G,\mathbb{Z})$$

coming from $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Let's just compute $\chi(\mathrm{rec}_{L,K}(\overline{a}))$ and get it over with. Let $s_a = \mathrm{rec}_{L,K}(\overline{a})$. Then $u_{L,K} \cup s_a = \overline{a}$. Recall $\mathbb{Q}/\mathbb{Z}$ comes from the Brauer group. Well,

$$\begin{aligned}
u_{L,K} \cup s_a \cup \delta\chi &= \overline{a} \cup \delta\chi \\
s_a \cup \delta\chi &= \delta(s_a \cup \chi)
\end{aligned}$$

And $\delta(s_a \cup \chi)$ is what we want to compute. Let $n = \mathrm{Card}\, G$. Then $s_a \cup \chi \in H^{-1}(G, \mathbb{Q}\mathbb{Z}) \cong n^{-1}\mathbb{Z}/\mathbb{Z}$. Mercifully this is one of the cases where we have a formula. Specifically, $s_a \cup \chi =$

$\chi(s_a) = \frac{i}{n} \bmod \mathrm{Z}$; I mean, what else could it be? Now we have to take δ of that, to wind up in $H^0(G, \mathrm{Z}) \cong \mathrm{Z}/n\mathrm{Z}$. Then $\delta(s_a \cup \chi) = i \bmod n$. So far we have

$$u_{L,K} \cup (i \bmod n) = \overline{a} \cup \delta\chi$$

where $\delta\chi \in H^2(G, L^\times)$.

Proposition $\chi(\mathrm{rec}_{L,K}(\overline{a})) = \mathrm{inv}_K(a \cup \delta\chi)$.

This shows you that the reciprocity law is tied to the Brauer invariant. Furthermore, we'll use it to see how reciprocity operates on maximal unramified extensions.

Let L/K be unramified; L is the unique unramified extension with $[L : K] = n$. We want to understand a little better how the reciprocity law operates. So let $a \in K^\times$; want to get a hold of s_a. We'll see that $s_a = \mathrm{Fr}_K$ raised to some power, namely, the valuation of s_a.

Well, $G^{\mathrm{ab}} \in \mathrm{Z}/n\mathrm{Z}$. Let $\chi \in \mathrm{Hom}_{\mathrm{gp}}(G^{\mathrm{ab}}, \mathrm{Q}/\mathrm{Z})$. Let $\chi(\mathrm{Fr}_K) = \frac{1}{n} \bmod \mathrm{Z}$. Want to see that

$$\begin{aligned} \chi(s_a) &= \mathrm{inv}_K(\delta\chi \cup \overline{a}) \\ &\stackrel{?}{=} \frac{v_K(a)}{n} \bmod \mathrm{Z}. \end{aligned}$$

Well, certainly the invariant is in $H^2(G, L^\times)$, and G is cyclic. We've got

$$\begin{tikzcd}
H^2(G, L^\times) \arrow[r, "v_L"] \arrow[d, dash] & H^2(G, \mathrm{Z}) \arrow[d, dash] & H^1(G, \mathrm{Q}/\mathrm{Z}) \arrow[l, "\cong"'] \\
H^2(G, \mathrm{Z}) \times H^0(G, L^\times) \arrow[r, "\mathrm{id} \times v_L"'] & H^2(G, \mathrm{Z}) \times H^0(G, \mathrm{Z}) & \\
\delta\chi \cup \overline{a} \arrow[r, mapsto] & v_K(a)\delta\chi & v_k(a)\chi \arrow[l, mapsto]
\end{tikzcd}$$

Use $\delta\chi \in H^2(G, \mathrm{Z})$, etc. Now specialize to our χ, and get the desired result;

$$\chi(_a) = \mathrm{inv}_K(\delta\chi \cup \overline{a}) = \frac{v_K(a)}{n} \bmod \mathrm{Z}.$$

Goal At this point, our goal is to identify K^{ab} with $K_\pi \cdot K^{\mathrm{unr}}$, and $\mathrm{rec}_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, and $K^\times = \pi_K^{\mathbb{Z}} \cdot \mathcal{O}_K^\times$.

Now, π operates trivially on K_π. More precisely, $\mathrm{rec}_K(\pi)$ does. Essentially, this is because $\pi \in N_{K_{\pi,n},K}(K_{\pi,n}^\times)$ for all n. And it operates as Frobenius on K^{unr}.

So it remains to understand what $\mathcal{O}_K^\times$ does to K_π; this is the only thing which isn't immediatley clear. Want to understand $\mathcal{O}_K^\times \to \mathrm{Gal}(K_\pi, K)$. But the map is $u \mapsto u^{-1}$, where we've identified $\mathrm{Gal}(K_\pi, K)$ with $\mathcal{O}_K^\times$.

This shows that $K^{\mathrm{ab}} \cong K_\pi K^{\mathrm{unr}}$, as soon as we know that the map is really just $u \mapsto u^{-1}$.

We'll show:

$$\begin{array}{ccc} \mathrm{Gal}(K^{\mathrm{ab}}, K) & \twoheadrightarrow & \mathrm{Gal}(K_\pi, K) \times \mathrm{Gal}(K^{\mathrm{unr}}, K) \\ & & \mathcal{O}_K^\times \times \widehat{\mathbb{Z}} \\ \pi^n \cdot u & \longmapsto & (u^{-1}, n) \end{array}$$

And this will follow from:

1. $K^{\mathrm{unr}} \cdot K_\pi$ is independent of π.
2. Let $r = r_\pi : K^\times \to \mathrm{Gal}(K_\pi, K) \times \mathrm{Gal}(K^{\mathrm{unr}}, K)$ be $\pi^n u \mapsto ([u^{-1}]_f, n)$, where we'd chosen f starting with π^x, and is congruent to $x^q \bmod \pi$. The statement is that r_π is independent of the choice of π.

Admit this. Then for $r = r_\pi$, r and the reciprocity law map $r, \mathrm{rec}_K : K^\times \to \mathrm{Gal}(K^{\mathrm{unr}} \cdot K_\pi, K)$ coincide on *all* uniformizers.

So let's go prove that stuff.

Lemma Choose π, ϖ two uniformizers, $f \in \mathfrak{F}_\pi$, $g \in \mathfrak{F}_\varpi$. These correspond to formal laws F_f and F_g. Let $A = \widehat{\mathcal{O}_{K^{\mathrm{unr}}}}$.

1. There's a polynomial $\theta \in A[\![x]\!]$ so that $F_g(\theta(x), \theta(y)) = \theta(F_f(x, y))$.
2. This isomorphism is compatible with formal multiplication; $\theta([a]_f(x)) = [a]_g(\theta(x))$ for all $a \in \mathcal{O}_K$.
3. $\theta^{-1}\theta\sigma(x) = [u]_f(x)$ where $\varpi = u\pi$, and $\sigma = \mathrm{Fr}_q$. In other words, $\theta\sigma(x) = \theta([u]_f(x))$.

$K \supseteq \mathcal{O}_K$ a complete discrete vauation ring, with residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$. Supose $\pi = u\varpi$ are uniformizers, $u \in \mathcal{O}_K^\times$. Suppose $f \in \mathfrak{F}_\pi \rightsquigarrow F_f$, and $g \in \mathfrak{F}_\varpi \rightsquigarrow F_g$. They're not isomorphisc [necessarily] over $\mathcal{O}_K$.

Let A be the Witt vectors $A = W(\overline{\kappa})\mathcal{O}_K$, and $B = \operatorname{Frac} A = B(\overline{\kappa})K = \widehat{K}^{\mathrm{unr}}$. Take the maximal unramified extension of K: complete it with respect to the topology given by the uniformizer. Since there's no ramification, the old uniformizer is still a uniformizer.

$$\begin{tikzcd}
 & B \arrow[dl, dash] \arrow[dr, dash] & \\
B(\overline{\kappa}) \arrow[dr, dash] & & {} \arrow[dl, dash] \\
 & ? &
\end{tikzcd}$$

Lemma There is a $\theta : F_f \xrightarrow{\cong}_A F_g$ so that

- $\theta F_f(x, y) = F_g(\theta(x), \theta(y))$.
- For every $a \in \mathcal{O}_K$, $\theta([a]_f(x)) = [a]_g(\theta(x))$.
- $\theta(x) \equiv \epsilon x \bmod \deg 2$ for some $\epsilon \in A^\times$.
- There's a technical condition we want, too:

  $$\theta^\sigma(x) = \theta([u]_f(x))$$

  where σ is the Frobenius element.

Suppose we know the lemma. Let's see what we get out of it. Well, there's a canonical ismorphism and then we actually get

$$K^{\mathrm{unr}}K_f \xrightarrow[\cong]{\theta} K^{\mathrm{unr}}K_g$$

Now, before we had

$$\begin{tikzcd} K^\times \arrow[r, "r_\pi"] & \mathrm{Gal}(K^{\mathrm{unr}}K_f, K) \arrow[d, "\cong"', "\theta"] \\ K^\times \arrow[r, "r_\varpi"'] & \mathrm{Gal}(K^{\mathrm{unr}}K_g, K) \end{tikzcd}$$

What we want is to show $r_\pi = r_\varpi$. Well, $r_\pi(\varpi) = r_\pi(u) = r_\pi(\pi)$. And $r_\varpi(\varpi)$ is trivial on K_g, and Fr_q on K^{unr}.

On K_g, well, let's see what we have. For $x \in F_f[\pi^n]$, $\theta(x) \in F_g[\varpi^n]$. And

$$\begin{aligned} r_\pi(\varpi)\theta(x) &= \theta^\sigma(r_\pi(\varpi)x) \\ &= \theta^\sigma(r_\pi(u)r_\pi(\pi)x) \\ &= \theta^\sigma(r_\pi(u)x) \\ &= \theta^\sigma([u^{-1}]_f(x)) \\ &= \theta([u]_f[u^{-1}]_f x) \\ &= \theta(x). \end{aligned}$$

Thus, $r_\pi(\varpi)$ operates trivially on K_g. So now we know $r_\pi(\varpi) = r_\varpi(\varpi)$.

For $v \in \mathcal{O}_K^\times$,

$$\begin{aligned} r_\pi(v)\theta(x) &\stackrel{?}{=} r_\varpi(v)\theta(x) \\ r_\pi(v)\theta(x) &= \theta(r_\pi(v)x) \\ &= \theta([v^{-1}]_f(x)) \\ r_\varpi(v)\theta(x) &= [v^{-1}]_g(\theta(x)). \end{aligned}$$

But θ commute with formal multiplication, so $r_\pi(v) = r_\varpi(v)$ for every $v \in \mathcal{O}_K^\times$ and we're done.

Remark Why would we expect $\theta^\sigma(x) = \theta([u]_f(x))$? Want to figure out a relation between $\theta^{-1}\theta^\sigma(x)$ and $[u]_f(x)$. Consider $\theta^{-1}\theta^\sigma f(x)$. We want $\theta^{-1}\theta^\sigma f = [\varpi]_f(x) = \theta^{-1}g\theta(x)$.

And θ^σ should give an isomorphism $\theta^\sigma : F_f^\sigma \overset{\cong}{\to} F_g^\sigma$. But all coefficients are in $\mathcal{O}_K$, so it's actually $\theta^\sigma : F_f \overset{\cong}{\to} F_g$ And $\theta^{-1} \circ \theta^\sigma \in \mathrm{End}(F_f)$.

$$
\begin{aligned}
\theta^{-1} \circ \theta^\sigma \circ f &\in \mathrm{End}(F_f) \\
\theta^{-1} g \theta &\in \mathrm{End}(F_f)
\end{aligned}
$$

Look at them modulo π. The second one is

$$
\begin{aligned}
\theta^{-1}g\theta(x) &\equiv \theta^{-1}(\theta(x))^q \bmod \pi \\
&\equiv \theta^{-1}\theta^\sigma(x^q) \\
&\equiv \theta^{-1}\theta^\sigma f(x).
\end{aligned}
$$

By the uniqueness of lifting of endomorphisms [to characteristic zero] $\theta^{-1}\theta^\sigma f = \theta^{-1}g\theta$, and so $\theta^\sigma = \theta \circ [u]_f$.

Proof of Lemma We'll construct θ coefficient by coefficient, satisfying $\theta(x) \equiv \epsilon x \bmod \deg 2$ and $\theta^\sigma = \theta \circ [u]_f$. There's a condition on ϵ. Well, $\theta^\sigma(x) \equiv \epsilon^\sigma x \bmod \deg 2$; and $\theta \circ [u]_f(x) \equiv \epsilon u x$. Need $\epsilon \in A^\times$ so that $\epsilon^\sigma \epsilon^{-1} = u$. But all we know is that u is a unit.

Exercise Interpret this condition $\epsilon^\sigma \epsilon^{-1} = u$ as a statement on Galois cohomology.[17]

Okay. Suppose we've constructed $\theta_{r-1}(x) \in A[\![x]\!]/x^r$. Want $\theta_r(x) = \theta_{r-1}(x) + b_r x^r \bmod \deg r+1$ so that $\theta_r^\sigma(x) \equiv \theta_r \circ [u]_f \bmod \deg r+1$. Well,

$$
\begin{aligned}
\theta_r^\sigma(x) &\equiv \theta_{r-1}^\sigma(x) + b_r^\sigma x^r \bmod \deg r+1 \\
\theta_r \circ [u]_f(x) &= \theta_{r-1} \circ [u]_f(x) + b_r(u_f(x))^r \\
&= \theta_{r-1} \circ [u]_f(x) + b_r u^r x^r \\
\theta_{r-1}^\sigma(x) - \theta_{r-1} \circ [u]_f(x) &= c_r x^r \\
b_r^\sigma + c_r &= b_r u^r
\end{aligned}
$$

[17] Hint: σ is the topological generator of K^{unr}. So we're looking at the cohomology of this profinite gorup with cofficients in $A^\times$ or $B^\times$.

Now, $u = \epsilon^\sigma \epsilon^{-1}$. So

$$b_r^\sigma + c_r \;\; = \;\; b_r \epsilon^{r\sigma} \epsilon^{-r}.$$

We need

$$(b_r \epsilon^r)^\sigma - (b_r \epsilon^r) = -\frac{c_r \epsilon^{r\sigma}}{\epsilon^r}.$$

And this is another cohomological statement.

Last time we used two facts. Let $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$, $A = \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$, $F = \sigma = \mathrm{Fr}_K = \mathrm{Fr}_q$. Then

$$A^\times \xrightarrow{F-1} A^\times \ni u$$

$$A \xrightarrow{F-1} A \ni b$$

In other words, there's $\epsilon \in A^\times$ with $u = \epsilon^\sigma \epsilon^{-1}$, and $a \in A$ so that $b = a^\sigma - a$.

Trying to formulate this in Galois cohomology. The first sally didn't quite work out, but we'll try it again. Think about $A^\times$ as $A^\times = \lim_{\overleftarrow{n}} (A/\pi^n A)^\times$, and $A = \lim_{\overleftarrow{n}} (A/\pi^n A)$. It suffices to show that, on each associated graded level, this is surjective. Hmm. The ground level of the filtration is $\overline{\kappa}^\times \overset{\sigma-1}{\to} \overline{\kappa}^\times$. In general, $\mathrm{fil}^n = (1 + \pi^n A)^\times$, and $\mathrm{fil}^n / \mathrm{fil}^{n+1} \cong \overline{\kappa}$, and this behaves nicely with respect to the Galois group. So on each graded piece we get either $\overline{\kappa}^\times \overset{\sigma-1}{\to} \overline{\kappa}^\times$ or $\overline{\kappa} \overset{\sigma-1}{\to} \overline{\kappa}$. We have to show that these are surjective.[18]

Now, these things are discrete $\mathrm{Gal}(\widehat{K}^{\mathrm{unr}}, K)$-modules.

$$H^i(\mathrm{Gal}(\widehat{K}^{\mathrm{unr}}, K), \overline{\kappa}^\times) = \lim_{\substack{\rightarrow \\ U \text{ open normal}}} H^i(G/U, {\overline{\kappa}^\times}^U)$$

In our case, G is $\widehat{\mathbb{Z}}$; take $U = n\widehat{\mathbb{Z}}$. Then the quotient is $G/u \cong \mathbb{Z}/n\mathbb{Z}$, cyclic. Which is good, since we know something about them. In general, $H^1(\mathbb{Z}/n\mathbb{Z},) = \frac{\ker N}{\mathrm{im}(\sigma - 1)}$. Something about transition maps. When all's said and done, we get $H^1 = \overline{\kappa}^\times / \mathrm{im}(\sigma - 1)$, and for the other open $H^1 = \overline{\kappa}(\mathrm{im}(\sigma - 1)$. By Hilbert 90, these are dead.

[18] I think the graded thing is just $\mathrm{fil}^i / \mathrm{fil}^{i+1}$.

We're declaring ourselves done with local class field theory, and moving on to

Global Class Field Theory What is class field theory, anyway? It has a few goals.

- Understand/describe abelian extensions, possibly in terms of the arithmetic of the base field, K. F'rinstance, stuff involving $K^\times$ or $\mathbb{A}_K^\times/K^\times$.
- Understand ramifications of [abelian] Galois extensions. F'rinstance, let K be a global field, and L a [finite] Galois extension. Chebotarev sez, inter alia, the following. Let v be an unramified place; then there's a frobenius element, or conjugacy class, anyway, $\mathrm{Fr}_v \in G^\flat \ni \langle g \rangle$, the conjugacy clases of G. Then density of $\{v : \mathrm{Fr}_v \in \langle g \rangle\}$ is $\frac{1}{\mathrm{Card}(G^\flat)}$. Furthermore, $\{v \in \Sigma_K : \mathrm{Fr}_v = e\}$, which is just the set of [totally] split primes, completely determines L.
- Ultimately, we're interested in $\mathrm{Gal}(K^{\mathrm{sep}}, K)$. And apparently, these days one dualizes the problem and attempts to describe the representations $\mathrm{Gal}(K^{\mathrm{sep}}, K) \to GL_n(\mathbb{Q}_l)$.

Main theorem of global class field theory:

Let K be a global field, L/K a finite abelian extension.

1. There's a map

$$\begin{tikzcd} \frac{\mathbb{A}_K^\times}{K^\times N_{L,K}(\mathbb{A}_L^\times)} \arrow[r, "\mathrm{rec}_{L,K}", "\cong"'] & \mathrm{Gal}(L,K) \\ & \mathrm{Fr}_v \\ K \arrow[uu] \arrow[uur] & \\ \pi_v \arrow[uur, mapsto] & \end{tikzcd}$$

   for v an unramified prime, $v \in \Sigma_K$; and this gives a map from the group of unramified ideals I^{unr} to $\mathrm{Gal}(L, K)$.

Existence *Any* open normal subgroup of finite index in $\mathbb{A}_K^\times/K^\times$ corresponds to a [unique] abelian extension of K, as a norm subgroup.

Remark $K^\times$ is dense in $\prod_{i=1}^m K_{v_i}^\times$, by weak approximation or independence of valuations. This tells us that $\mathrm{rec}_{L,K}$, if it exists, must be unique. [Exercise.]

Existence of the reciprocity law used to be written like this: There's a finite set of primes S containing all ramified primes and all archimedean primes and, for $v \in S$ an $a_v \in \mathbb{R}$, so that for $x \in K^\times$ with $|x-1|_v \le a_v$, $\prod_{v \notin S} \mathrm{Fr}_v^{v(x)} = e \in \mathrm{Gal}(L,K)$. Exercise to verify that this is really equivalent.

$$\begin{tikzcd} \mathbb{A}_K^\times/K^\times \arrow[dr] & \\ \mathbb{A}_{K,S}^\times \arrow[u] \arrow[r, "\text{naive reciprocity}"'] & \mathrm{Gal}(L,K) \end{tikzcd}$$

Recall $\mathbb{A}_{K,S}^\times = \prod'_{v \notin S} K_v^\times$. Anyways, this factorization of the bottom map is equivalent to the classical formulation.

Here's the strategy of the proof. Three main steps.

- First inequality.
- Second inequality.
- Existence of abelian extensions. [Kummer theory in numberfield case; Artin-Schreier in function field case, which we'll probably blow off anyway. The function field case is better handled in Serre, *Algebraic Groups and Class Fields*, using algebraic geometry.]

Classically, that is, before Chevalley, second was first; first, second.

Let L/K a cyclic Galois extension of degree n. [This'll work for any abelian extension, actually.] The first inequality is

$$\mathrm{Card}\left(\frac{\mathbb{A}_K^\times}{K^\times N_{L,K}(\mathbb{A}_L^\times)}\right) \ge n.$$

And you can guess what the other one says; and these combine to give equality.

Maybe we'll go and prove something now. Let L/K be cyclic of order n; $\mathrm{Gal}(L,K) \cong \mathbb{Z}/n\mathbb{Z}$. Want to say something about $\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times)$. Well,

$$\begin{aligned}\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) &= (\mathbb{A}_L^\times/L^\times)^G/N_{L,K}(\mathbb{A}_L^\times/L^\times)\\ &= \mathbb{A}_K^\times/K^\times N_{L,K}(\mathbb{A}_L^\times)\end{aligned}$$

In the second line, we used Hilbert 90 to get

$$\begin{aligned}(\mathbb{A}_L^\times)^G/(L^\times)^G \cong & \quad (\mathbb{A}_L^\times/L^\times)^G\\ (L^\times)^G &= K^\times\\ \mathbb{A}_L^\times &= \varinjlim_{\Sigma_K^\infty \subseteq S \subseteq \Sigma_K} (\prod_{w|v\notin S} \mathcal{O}_w^\times) \times (\prod_{w|v\in S} L_v^\times)\\ (\mathbb{A}_L^\times)^G &= \varinjlim_{\Sigma_K^\infty \subseteq S \subseteq \Sigma_K} ((\prod_{w|v\notin S} \mathcal{O}_w^\times) \times (\prod_{w|v\in S} L_v^\times))^G\\ &= \varinjlim (\prod_{v\notin S} \mathcal{O}_v^\times) \times \prod_{\in S} K_v^\times\\ &= \mathbb{A}_K^\times\end{aligned}$$

[Since G is finite, cohomology commutes with direct limits, etc.]

Now, you'd expect to get a map $\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) \leftarrow \widehat{H}^{-2}(G, \mathbb{Z})$, cup product with some element in H^2 with coefficients in the idele class gorup; and we'll produce that element.

We'll actually prove that the Herbrand quotient is $h(G, \mathbb{A}_L^\times/L^\times) = n$.

We've got L/K a cyclic extension of number fields, $G = \mathrm{Gal}(L, K) = \mathbb{Z}/n\mathbb{Z}$. Then $h(G, \mathbb{A}_L^\times/L^\times) = n$, so

Theorem [First inequality]

$$\mathrm{Card}\left(\frac{\mathbb{A}_K^\times}{K^\times N_{L,K}(\mathbb{A}_L^\times)}\right) \geq n.$$

Now, there's some $\Sigma_{K,\infty} \subseteq S \subseteq \Sigma_K$, S finite containing infinite primes and ramified primes, so that $\mathbb{A}_{L,S}^\times L^\times = \mathbb{A}_L^\times$.[19] This is from finiteness of class number, or whatever. From this, we can represent idele classes by S-ideles:

$$\mathbb{A}_L^\times/L^\times \xleftarrow{\cong} \mathbb{A}_{L,S}^\times/L_S^\times$$

where $L_S^\times = L^\times \cap \mathbb{A}_{L,S}^\times$. We'll try to compute cohomologies with these.

$$\begin{aligned}
H^0(\prod_{w|v} L_w^\times) &= K_v^\times \\
H^0(\prod_{w|v} \mathcal{O}_w^\times) &= \mathcal{O}_v^\times \\
\widehat{H}^0(\prod_{w|v} \mathcal{O}_w^\times) &= 0 \text{ for } v \notin S \\
\widehat{H}^0(G, \mathbb{A}_{L,S}^\times) &= \prod_{v\in S} \widehat{H}^0(G_w, L_w^\times) \\
&= \prod \frac{K_v^\times}{N_{w,v}(L_w^\times)} \\
\text{for } v \notin S, & \\
H^1(G, \prod_{w|v} \mathcal{O}_w^\times) &= H^1(G_w, \mathcal{O}_w^\times) \text{ Shapiro's lemma} \\
&= 0
\end{aligned}$$

since it's complete, and you have a filtration; on the bottom step is the residue class field with cohomology zero, by Hilbert 90, and then successive quotients are still the residue fields, again zero. This being complete, everything is zero.

[19] Recall that this is $\mathbb{A}_{L,S}^\times = (\prod_{w|v\in S} L_w^\times) \times \prod_{w|v\notin S} \mathcal{O}_w^\times$, since S contains all archimedean places.

Conclusion of all this is that $h(G, \mathbb{A}_{L,S}^\times) = \prod_{v \in S} h(G_w, L_w^\times) = \prod_{v \in S}[L_w : K_v]$.[20]

Now, what about $h(G, L_S)^\times$? We need the log map:

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & \mu_L & \longrightarrow & L_S^\times & \xrightarrow{\log} & (\prod_{w|v \in S} \mathbb{R}_w)^1 & \longrightarrow & \text{real torus} & \longrightarrow & 1 \\ & & & & l & \longmapsto & (\log \|l\|_w)_{w|v\in S} & & & & \end{array}$$

Notice that the image lies in the hyperplane where the sum of the coordinates is zero; that's what the superscript ^{1} means. However, it is cocompact; it goes to a torus. Anyways, elet $\Gamma = \in (L_S^\times) \subseteq (\prod_{v \in S} \mathbb{R}_v)^1$. It's a lattice, essentially because of the Dirichlet unit theorem.

Hmm. $\Gamma' \stackrel{\text{def}}{=} (\prod_{w|v\in S} \mathbb{Z}_w)^1 \subseteq (\prod_{w|v \in S} \mathbb{Z}_w)$. Actually,

$$0 \longrightarrow (\prod_{w|v\in S} \mathbb{Z}_w)^1 \longrightarrow (\prod_{w|v\in S} \mathbb{Z}_w) \longrightarrow \mathbb{Z} \longrightarrow 0$$

where $\mathbb{Z}$ has the trivial action. As such, its Herbrand quotient is $h(G, \mathbb{Z}) = n$. By Shapiro's lemma,

$$\begin{aligned} h(G, \prod_{w|v\in S} \mathbb{Z}_w) &= \prod_{v \in S} h(G_w, \mathbb{Z}) \\ &= \prod_{v\in S}[L_w : K_v] \\ h((\prod_{w|v\in S} \mathbb{Z}_w)^1) &= \frac{\prod_{v\in S}[L_w : K_v]}{n}. \end{aligned}$$

Now, $h(G, L_S^\times) = h(G, \Gamma)$, since the Herbrand quotient doesn't see finite differences. SO it suffices to compute for the lattice Γ.

We know that $\Gamma \otimes_{\mathbb{Z}} \mathbb{R} \cong \Gamma' \otimes_{\mathbb{Z}} \mathbb{R}$ G-equivariantly. Then we can thus conclude that $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q} \cong \Gamma' \otimes_{\mathbb{Z}} \mathbb{Q}$, G-equivariantly as well. That's an easy algebra fact; figure it out if you don't see it.[21] But once these two representations are isomorphic over $\mathbb{Q}$, we ca n produce a map beween them with finite kernel and cokernel, which $h(\cdot)$ ignores. So $h(G, \Gamma) = h(G, \Gamma')$ which we just computed.

Putting everything together, $h(G, \mathbb{A}_L^\times / L^\times) = n$.$\diamond$

[20] By the way, a lot of times I'm just picking some w lying over v; it doesn't really matter which one.

[21] Briefly, G-equivariant homomorphisms are a findim $\mathbb{Q}$ vector space. Tensoring with $\mathbb{R}$ gives you the earlier thing. That's a general statement.

Consequences If L/K is an abelian extension split almost everywhere, then $K = L$. For take some cyclic subextension, L'.

Claim that $K^\times N_{L',K}(\mathbb{A}_{L'}^\times) = \mathbb{A}_K^\times$. That's essentially weak approximation plus our hypothesis; use weak approximation to take care of the nonsplit primes. Then $[L' : K] = 1$, a contradiction.

Review of Kummer theory K a field of characteristic p, possibly 0, and n prime to the characteristic; $n \in K^\times$. Assume K contains n^{th} roots of unity. Kummer theory looks at the part of the abelianized Galois group killed by n.

Well, let's try it. We look at the Kummer sequence

$$1 \longrightarrow \mu_n(\overline{K}) \longrightarrow K^{\mathrm{sep}\,\times} \xrightarrow{n} K^{\mathrm{sep}\,\times} \quad 1$$

Our assumption is that $\mu_n(\overline{K})$ is a trivial Galois module. So we get, upon taking cohomology, letting $G = \mathrm{Gal}(K^{\mathrm{sep}}, K)$ and $\mu_n = \mu_n(\overline{K})$,

$$1 \longrightarrow K^\times/(K^\times)^n \longrightarrow \mathrm{Hom}(G, \mu_n) \longrightarrow 1$$

$$\mathrm{Hom}(G^{\mathrm{ab}}/(G^{\mathrm{ab}})^n, \mu_n)$$

[exact on right from Hilbert 90.] In some sense, $\mathrm{Hom}(G^{\mathrm{ab}}/(G^{\mathrm{ab}})^n, \mu_n)$ is the dual of $G^{\mathrm{ab}}/(G^{\mathrm{ab}})^n$. Anyways, how do we write down this isomorphism? It comes down to the connecting δ thing. Let $k \in K^\times = H^0(G, K^{\mathrm{sep}\,\times})$. Pick $\sqrt[n]{k} \in K^{\mathrm{sep}\,\times}$; we've lifted back the cochain. Take the derivative; $G \ni \sigma \mapsto \sqrt[n]{k}^{\sigma-1} \in \mu_n$. And this is independent of our choice of an n^{th} root.

Let $K(n) = \mathrm{Gal}(K^{\mathrm{sep}}, K)^{\mathrm{ab}}/\,\mathrm{Gal}(K^{\mathrm{sep}}, K)^n$. For next time – Friday, actually – think about $K(n) \supseteq L \supseteq K$. Figure out which things kill L. Let $H = \mathrm{Gal}(K(n), L)$. Consider all characters of G killing H. That's a subgroup of $\mathrm{Hom}(G, \mu_n)$, , and therefore corresponds to a subgroup of $K^\times/K^{\times n}$. How do we explicitly relate this to L?

We've got a tower of fields and Galois groups

$$\begin{array}{cc}
L_n & G \\
\Big| & \Big| \\
L & H \\
\Big| & \Big| \\
K & (e)
\end{array}$$

Here, we have

$$\begin{aligned}
G &= \mathrm{Gal}(L_n, K) \\
&= \frac{\mathrm{Gal}(K^{\mathrm{sep}}, K)^{\mathrm{ab}}}{\mathrm{Gal}(K^{\mathrm{sep}}, K)^n} \\
&= \mathrm{Hom}(K^\times/(K^\times)^n, \mu_n) \\
H &= \{\sigma \in G : \sigma|_L = \mathrm{id}\} \\
&= \mathrm{Hom}(\frac{K^\times}{(K^\times)^n \cdot ?}, \mu_n) \\
? &= \{a \in K^\times : \forall \sigma \in \mathrm{Gal}(L_n, L) k \sqrt[n]{a}^{\sigma - 1} = 1\} \\
&= \{a \in K^\times : \sqrt[n]{a} \in L\} \\
&= K^\times \cap (L^\times)^n \\
H &= \mathrm{Hom}(\frac{K^\times}{(L^\times)^n \cap K^\times}, \mu_n)
\end{aligned}$$

So,

$$G/H \cong \mathrm{Hom}((L^\times)^n \cap K^\times/(K^\times)^n, \mu_n).$$

In particular,

$$[L : K] = [(L^\times)^n \cap K^\times : (K^\times)^n].$$

Move it on.

Suppose we have L/K a Galois extension of number fields with Galois group G. Want

$$[\mathbb{A}_K^\times : K^\times N_{L,K}\mathbb{A}_L^\times] \leq [L:K].$$

By a previous lemma, more or less, we may [and do!] assume that $n = [L:K]$ is prime.

We will see shortly that we can further assume that all n^{th} roots of unity are in K; $\mu_n(\overline{K}) \subset K$.

$$\begin{tikzcd}
 & L(\mu_n) \arrow[d, dash, "G'"', "n"] \\
L \arrow[ur, dash, "m", "H"'] \arrow[d, dash, "n"', "G"] & K(\mu_n) \\
K \arrow[ur, dash, "m|(n-1)"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
G & \dfrac{\mathbb{A}_K^\times}{K^\times N(\mathbb{A}_L^\times)} \arrow[d, "\text{res}"] \arrow[dd, bend left=60, "m"] \\
G' & \dfrac{\mathbb{A}_{K(\mu_n)}^\times}{K(\mu_n)^\times \cdot N(\mathbb{A}_{L(\mu_n)}^\times)} \arrow[d, "\text{cor}"] \\
G & \dfrac{\mathbb{A}_K^\times}{K^\times N(\mathbb{A}_L^\times)}
\end{tikzcd}$$

In this case, corestriction is essentially just the norm; and the composition is multiplication by m.

Try this over again, as what we did certainly isn't right.

abort

Let $\widetilde{G} = \mathrm{Gal}(L(\mu_n), K)$, and G and H as above. Then we have

$$\begin{tikzcd}
\widehat{H}^{(}\widetilde{G}, \mathbb{A}_L^\times/L^\times) \arrow[d, "\mathrm{res}"] \arrow[r, phantom, "="] & \dfrac{\mathbb{A}_K^\times}{K^\times N_{L,K}(\mathbb{A}_{L(\mu_n)}^\times)} \\
\widehat{H}^0(G', \mathbb{A}_{L(\mu_n)}^\times/L(\mu_n)^\times) \arrow[d, "\mathrm{cor}"] & \\
\widehat{H}^0(G, \mathbb{A}_L^\times/L^\times) &
\end{tikzcd}$$

The composition might be multiplication by m.

abort

the second map of groups induces the first one.

$$\begin{tikzcd}
\widehat{H}^{(}\widetilde{G}, \mathbb{A}_{L(\mu_n)}^\times/L^\times) \arrow[r] \arrow[d, "\mathrm{res}"] & \dfrac{\mathbb{A}_K^\times}{K^\times N(\mathbb{A}_L^\times)} \arrow[d, "\mathrm{res}"] \\
\widehat{H}^0(G', \mathbb{A}_{L(\mu_n)}^\times/L(\mu_n)^\times) \arrow[r] \arrow[d, "\mathrm{cor}"] & \dfrac{\mathbb{A}_{K(\mu_n)}^\times}{K(\mu_n)^\times \cdot N(\mathbb{A}_{L(\mu_n)}^\times)} \arrow[d, "\mathrm{cor}"] \\
\widehat{H}^0(\widetilde{G}, \mathbb{A}_{L(\mu_n)}^\times/L^\times) \arrow[r] & \dfrac{\mathbb{A}_K^\times}{K^\times N(\mathbb{A}_L^\times)}
\end{tikzcd}$$

Now, the composite on the right is multiplication by m, a surjection, since $\mathbb{A}_K^\times/K^\times N(\mathbb{A}_L^\times)$ is killed by n.

At this point, what we want to do is bound $\mathbb{A}_K^\times/(K^\times N(\mathbb{A}_L^\times))$. The only way to do that is show that there are a lot of norms.

Now, assume that $\mathrm{Gal}(L,K) = G \cong (\mathbb{Z}/n\mathbb{Z})^r$, n prime, and $n \in K^\times$, $\mu_n(\overline{K}) \subseteq K^\times$. Fix S a finite set of places containing the archimedean places, and larg enough so that $K^\times \mathbb{A}_{K,S}^\times = \mathbb{A}_K^\times$. Can do this, essentially, by the finitude of class numbers. Want n to be an S-unit, that is, for all $\mathfrak{p}|n$, $\mathfrak{p} \in S$. Also, S should contain all ramified places. Anyways, that's our S, for now; we may have to expand it a bit, but who cares?

$$K_S^\times = K^\times \cap \mathbb{A}_{K,S}^\times.$$

Let $M = K((K_S^\times)^{\frac{1}{n}})$; and $\mathrm{Gal}(M,L) = H \cong (\mathbb{Z}/n\mathbb{Z})^t$. And $[M : K] = [K_S^\times : (K_S^\times)^n]$. But $K_S^\times \cong \mathbb{Z}^{\#S-1} \times \mu_N$ for some $n|N$. Then $[M : K] = n = \mathrm{Card}(S)$.

So, $M \supset L \supset K$. There are $w_1, \cdots, w_t$ unramified places of L, disjoint from S, such that the Frobenii F_{w_i} generate $\mathrm{Gal}(M,L)$. Assume each w_i lies over some v_i of K. Then $\mathcal{O}_{w_i} \supset \mathcal{O}_{v_i}$ is an unramified extension; so the decomposition group is cyclic. And actually, this is an isomorphism; the extension is split here. Why? Because the Frobenius from L to M is already cyclic of order n, and n is prime, or something like that. v_i split in L. And the Frobenii detect whether a global element of M is actually in L.

Let $a \in K_S$. If $a \in L_{w_i}^n$ for all i, then we conclude that the n^{th} root of a is in L; a is globally an n^{th} power of L.

With a little bit of work, we argue that certainly there are local norms

$$N = \prod_{v \in S} (K_v^\times)^n \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} \mathcal{O}_v^\times.$$

And it'll turn out that these are enough. Specifically, $[{}^\times \mathbb{A}_{K,S}^\times : K^\times N] \leq n$. But this index is just

$$\frac{[\mathbb{A}_{K,S}^\times : N]}{[K^\times \cap \mathbb{A}_{K,S}^\times, K^\times \cap N]}.$$

Notes from Kate. Thanks.

We want to show:

1. For all $a \in K^\times$, $\prod_v \mathrm{rec}_v(a) = 1$.
2. We just explained that for all $x \in \mathrm{Br}(K)$, if we localize we get an element in $\mathrm{Br}(K_v)$, namely, $\mathrm{inv}_v(x)$. We want to show $\sum_v \mathrm{inv}_v(x) = 0$.

Here's the connection between the two of them. We've sort of seen this already. That is, fix an abelian extension. L_w/K_v local, so for all $x_v \in \mathrm{Hom}(G_v, \mathrm{Q}/\mathrm{Z}) \cong H^1(G_v, \mathrm{Q}/\mathrm{Z})$ [since the action is trivial]. But by the coboundary map there's an isomorphism

$$H^1(G_v, \mathrm{Q}/\mathrm{Z}) \xrightarrow[\cong]{\delta} \mathrm{Hom}(G_v, \mathrm{Z})$$

Then for all $a_v \in K_v^\times$, $\mathrm{rec}_v(a_v) \in G_v$, so we can evaluate χ_v on it; $\chi_v(\mathrm{rec}_v(a_v))$ makes sense. But this is also an element $\mathrm{inv}_v(\cdot)$, where to get this we use:

$a_v \in K_v^\times$¡ $\overline{a_v} \in K_v^\times/$ norms, and $\overline{a_v} \in H^0(G_w, L_w^\times)$, then $\overline{a_v} \cup \delta\chi \in H^2(G_v, L_w^\times)$, and $\chi_v(\mathrm{rec}_v(a_v)) = \mathrm{inv}_v(\overline{a_v} \cup \delta\chi)$.

So much for the explnation. We begin with showin g(1) for L/K a cyclotomic extension.

Just cmpute it; for cyclotomic fields we can compute this over Q; and it suffices to check for extensions $\mathrm{Q}(\mu_{l^n})$ over Q.

Let's show it in this case. Let $\mathrm{Q}(\mu_{l^n}) = \mathrm{Q}(l^n)$; $G = (\mathrm{Z}/l^n\mathrm{Z})^\times$.

Check that $\prod_v \mathrm{rec}_v(\frac{a}{b}) = 1$ for $a, b \in \mathrm{Q}$. It suffices to check for primes and -1. So le tn be a prime number.

- What's $\prod_v \mathrm{rec}_v(-1)$? A few cases to worry about.

$v = \infty$ Then C/Q depends on $\mathrm{R}/N_{\mathrm{C},\mathrm{R}}(\mathrm{C})$; -1 isn't a norm because norms have to be positive. Then $\mathrm{rec}_v(-1) = i = -1$; the complex onjugate is its own inverse.

$v = p \neq l$ Then we have $\mathrm{Q}(l^n)_p$ over Q_p. And $p \neq l$ means we're unramified; -1 is a unit[?]. So $\mathrm{rec}_v(-1) = 1$.

$v = p = l$ Well, -1 is a unit. And $\mathrm{rec}_v(\mathrm{unit}) = \frac{1}{\mathrm{unit}}$, by the formal group law stuff. So $\mathrm{rec}_v(-1) = -1$.

Then $\prod_v \mathrm{rec}_v(-1) = -1 \cdot 1 \cdot -1 = 1$.

- $\prod_v \mathrm{rec}_v(n)$ for n
  not $= l$. As we'll see shortly,

$$\mathrm{rec}_v(n) = \begin{cases} 1 & v = \infty \\ 1 & v = p \neq l, n \neq p \\ n & v = p \neq l, n = p \\ n^{-1} & v = p = l, n \neq p \end{cases}.$$

  Given this, it's clear that $\prod_v \mathrm{rec}_v(n) = 1$.

  Let's look at a few of the cases.

$v = p \neq l$, $n \neq l$ Since $p \neq l$, the thing is unramified. And $n \neq l$ means it's a unit $\Rightarrow \mathrm{rec}_v(n)$ operates trivially if $n \neq p$, and $\mathrm{Zrec}_v(n) = n$ if $n = p$.

$v = p = l$, $n \neq l$ Then $\mathrm{Q}(l^m)$ over Q_l is totally ramified. $n \neq p \Rightarrow n$ is a unit $\Rightarrow \mathrm{rec}_p(n) = \frac{1}{n}$.

- Look at $n = l$. Then

$$\mathrm{rec}_v(n) = \begin{cases} 1 & v = \infty \\ 1 & v = p \neq l \\ 1 & v = p = l, l \text{ a norm} \end{cases}.$$

From all of this nonsense it follows that $\prod_v \mathrm{rec}_v(a) = 1$; and so (1) holds for all cyclotomic extensions.

Now let's do (2) for cyclotomic / cyclic extensions L over K.

Proof Cyclic means that the cohomology groups are cyclic. So if $x \in \mathrm{Br}(L/K)$, then $x = a \cup \delta\chi$ for some $a \in K^\times/N(L^\times)$ and $\chi \in H^1(G, \mathrm{Q}/\mathrm{Z})$.

Thus we have $\delta\chi$[22] defining a map $H^0(\cdot) \to H^2(\cdot)$. Want to show that $\sum \mathrm{inv}_v(x) = 0$. Well,

$$\begin{aligned} \sum_v \mathrm{inv}_v(x) &= \sum_v \mathrm{inv}_v(a \cup \delta\chi) \\ \text{from above} &= \sum_v \chi_v(\mathrm{rec}_v(a)) \\ &= \chi(\sum_v \mathrm{rec}_v(a)) \\ &= \chi(0) \\ &= 0. \end{aligned}$$

Now we want (2) for arbitrary $x \in \mathrm{Br}(K)$.

[22] Think of this as an element of $H^2(G_v, \mathrm{Z})$

Claim There' some cyclotomic and cyclic extension L over K which splits x, and thus $x \in \mathrm{Br}(L, K)$.

Proof Hasse principle, essentially. We know that $x_v \in \mathrm{Br}(K_v)$, and x_v is trivial for all but a finite set $v \in \{v_1, \cdots, v_N\}$. Take L/K a cylotomic cyclic extension so that $L_w : K_{v_i}] - \mathrm{inv}_{v_i}(x) \equiv 0 \bmod \mathrm{Z}$ for all i. And next class, I guess, we'll see how to do this.

Stil working on the second inequality. As a general principle, observe that cohomology often allows you to reduce to a very simple case; but once there, you may have to work sort of hard anyway.

So suppose given a tower of fields

$$\begin{array}{ll} M & K(\sqrt[n]{K_S^\times}) \\ | & \\ L & \\ | & G \cong (\mathbb{Z}/n\mathbb{Z})^r \\ K & \end{array}$$

Assume n a prime number, and $\mu_n(\overline{K}) \subseteq K^\times$, $n \in K^\times$. Let $\Sigma_K^\infty \subseteq S \subset \Sigma_K$ be a sufficiently large finite set of primes. Then $\mathrm{Gal}(M, KJ) \cong \mathrm{Hom}(K_S^\times / K_S^\times \cap (K^\times)^n, \mu_n)$. So $[M+K] = n^s$, since the group of homomorphisms is abstractly $(\mathbb{Z}/n\mathbb{Z})^s$. Then $w_1, \cdots, w_t \in \Sigma_L$, unramified so that $\{\mathrm{Fr}_{w_i}\}$ generates $\mathrm{Gal}(M, L)$. Since the decomposition groups are always cyclic, $\mathrm{Gal}(M, K) \cong (\mathbb{Z}/n\mathbb{Z})^s$; we know that w_i is split over v_i. In other words, all the v_i are split. Let $T = \{v_1, \cdots, v_t\}$.

We wanted

$$[\mathbb{A}_K^\times : K^\times N_{L,K}(\mathbb{A}_L^\times)] | [L : K] = n^r.$$

If we could show this, then we'd know the same thing for an arbitrary extension L.[23]

Now, we'd made up some norms,

[23]Combined with the first inequality; when L/K is cyclic, $G = \mathrm{Gal}(L, K) \cong \mathbb{Z}/n\mathbb{Z}$, then the Herbrand quotient was $h(G, \mathbb{A}_L^\times / L^\times) = n$. Thus, if L/K cyclic, and $[L : K] = n$ prime, then the two inequalities yield $H^1(G, \mathbb{A}_L^\times / L^\times) = (0)$, and $\hat{H}^1(G, \mathbb{A}_L^\times / L^\times)$ is cyclic of order n. Then for L/K an arbitrary Galois extension, $H^1(\mathrm{Gal}(L, K), \mathbb{A}_L^\times / L^\times) = (0)$. Also, the second inequality gives $\mathrm{Card}(\hat{H}^0(\mathrm{Gal}(L, K), \mathbb{A}_L^\times / L^\times)) | [L : K]$. And by inflation-restriction, etc., the same is true of H^2.

$$N = \prod_{v \in S} (K_v^\times)^n \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} \mathcal{O}_v^\times \subseteq N_{L,K}(\mathbb{A}_L^\times).$$

With luck, these'll be enough to get the inequality. It suffices to prove $[\mathbb{A}_K^\times : K^\times N] | n^r$. We know that

$$\begin{aligned}
\mathbb{A}_K^\times &= K^\times \mathbb{A}_{K,S}^\times \\
&= K^\times \mathbb{A}_{K,S\cup T}^\times \\
[\mathbb{A}_K^\times : K^\times N] &= \frac{[\mathbb{A}_{K,S\cup T}^\times : N]}{[K_{S\cup T} : K^\times \cap N]} \\
[\mathbb{A}_{K,S\cup T}^\times : N] &= \prod_{v \in S} [K_v^\times : (K_v^\times)^n]
\end{aligned}$$

So now we need to compute $[K_v^\times : (K_v^\times)^n]$.

$$\begin{aligned}
\frac{K_v^\times}{(K_v^\times)^n} &= \hat{H}^0_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, K_v^\times) \\
\hat{H}^1_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, K_v^\times) &= \mu_n(K_v) \\
h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, K_v^\times) &= \frac{[K_v^\times : (K_v^\times)^n]}{n}
\end{aligned}$$

Now try to get at the Herbrand quotient.

$$1 \longrightarrow \mathcal{O}_v^\times \longrightarrow K_v^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 1$$

$$\begin{aligned}
h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, K_v^\times) &= h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_v^\times) \cdots h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \\
&= h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_v^\times) \cdot n \\
\text{use exp} &= h_{\mathrm{triv}}(\mathbb{Z}/n\mathbb{Z}, \mathcal{O}_v) \cdot n \\
&= \frac{n}{|n|_v} \cdot n \\
[K_v^\times : (K_v^\times)^n] &= \frac{n^2}{|n|_v}
\end{aligned}$$

So much for finite places. What about the infinite ones? We're either talking about $[\mathbb{R}\times : (\mathbb{R}\times)^n]$ or $[\mathbb{C}\times : (\mathbb{C}\times)^n]$. The latter is just one; the former, 1 or 2 depending on n odd or even. But we'll actually only get $\mathbb{C}$, since the n^{th} roots of unity are lying around.

$$\begin{aligned} [\mathbb{A}^\times_{K,S\cup T} : N] &= \prod_{v\in S} \frac{n^2}{|n|_v} \\ &= n^{2s} \end{aligned}$$

Move on to the next part. We've got a global problem, namely,

$$[K^\times_{S\cup T} : K^\times \cap N] \stackrel{?}{=} n^{s+t} = n^r.$$

We know that

$$K^\times_{S\cup T} \subseteq K^\times \cap N \subseteq (K^\times_{S\cup T})^n.$$

It suffices to prove $K^\times \cap N = (K^\times_{S\cup T})^n$.

Recall that if $x \in K^\times_S$, and $x \in (L^\times_{w_i})^n$ for all i, then $x \in (L^\times)^n$. For $\sqrt[n]{x}$ is fixed by Fr_{w_i}, hence fixed by $\mathrm{Gal}(M, L)$, i.e., $\sqrt[n]{x} \in L$.

Hmm. Things seem a little rocky. Define $N' = \prod_{v\in S}(K^\times_v)^n \times \prod_{v\notin S} \mathcal{O}^\times_v$. Want $K^\times_S : K^\times \cap N'] = n^{s+t}$.

Here's the situation. We've got S, a large though finite set of places, and

$$\begin{array}{ccl} & M = K(\sqrt[n]{K_S^\times}) & \\ & \Big| & H \cong (\mathbb{Z}/n\mathbb{Z})^t = \{\mathrm{Fr}_{w_i}\}_{i=1,\cdots,t} \\ w_i & L & \\ & \Big| & G \cong (\mathbb{Z}/n\mathbb{Z})^r \\ v_i & K & \end{array}$$

Set $T = \{v_1, \cdots, v_t\}$, and

$$N = \prod_{v \in S} (K_v^\times)^n \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} \mathcal{O}_v^\times.$$

What we want is

$$K^\times \cap N = (K_{S \cup T}^\times)^n.$$

We're going to try a trick which usually doesn't work, but will hopefully bail us out here. It should be clear that $K^\times \cap N \supseteq (K_{S\cup T}^\times)^n$. And what we really need is $K(\sqrt[n]{K^\times \cap N}) = K$. But we know that $K^\times \cap N \subseteq K_{S \cup T}^\times$ which is finitely generated. By the first inequality, to show that these two fields are the same it suffices to show that, setting $F \stackrel{\text{def}}{=} K(\sqrt[n]{K^\times \cap N})$,

$$K^\times \cdot N_{F,K}(\mathbb{A}_F^\times) = \mathbb{A}_K^\times.$$

We certainly have

$$N_{F,K}(\mathbb{A}_F^\times) \supseteq \prod_{v \in S} K_v^\times \times \prod_{v \in T} (K_v^\times)^n \times \prod_{v \notin S \cup T} \mathcal{O}_v^\times$$

It now suffices to show

$$K^\times \cdot (\prod_{v\in S} K_v^\times \times \prod_{v\in T} (\mathcal{O}_v^\times)^n \times \prod_{v\notin S\cup T} \mathcal{O}_v^\times) = \mathrm{A}_K^\times.$$

By our choice of S,

$$\mathrm{A}_K^\times \;=\; K^\times(\prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times).$$

So now it's enough that $K^\times$ gives the difference;

$$K_S^\times \longrightarrow \prod_{v\in T} \frac{\mathcal{O}_v^\times}{(\mathcal{O}_v^\times)^n}$$

And you can't use a general approximation argument to prove this. What we'll try to show is that the cardinality of the image, and that of the target set, are the same. Well, the kernel is

$$\begin{aligned}\ker &= K_S^\times \cap \prod_{v\in T} (\mathcal{O}_v^\times)^n\\ &= K_S^\times \cap (L^\times)^n.\end{aligned}$$

By Kummer theory, $L = K(\sqrt[n]{K_S^\times \cap (L^\times)^n})$.

$$\begin{array}{rcl}\mathrm{Card}(K_S^\times/\ker) & = & [M:L]\\ & = & n^t\\ \mathrm{Card}(\mathcal{O}_v^\times/(\mathcal{O}_v^\times)^n) & \overset{\text{Hensel's lemma}}{=} & \mathrm{Card}(\kappa_v^\times/(\kappa_v^\times)^n)\\ \kappa_v & \supseteq & \mu_n(\overline{\kappa}_v)\\ n & \mid & q_v - 1\\ \mathrm{Card}(\kappa_v^\times/(\kappa_v^\times)^n) & = & n \text{ for all } v\in T\end{array}$$

[Remember n is prime to the characterstic of the residue field at $v \in T$.]

Then $\mathrm{Card}(\prod_{v\in T} \mathcal{O}_v^\times/(\mathcal{O}_v^\times)^n$, proving the second inequality.$\diamond$

Remark Historically, the second inequality is proved by analytic methods using L-functions, etc. Let L/K be a finite extension of number fields. We want to show that $[\mathbb{A}_K^\times : K^\times N_{L,K}(\mathbb{A}_L^\times)] \leq [L:K]$. Now, $N \stackrel{\text{def}}{=} K^\times N_{L,K}(\mathbb{A}_L^\times)/K^\times$ is an open subgroup of finite index in $\mathbb{A}_K^\times/K^\times$. Following an idea of Dirichlet, we want to look at characters $\chi \in \operatorname{Hom}(\mathbb{A}_K^\times/(K^\times \cdot H), \mathbb{C}_1^\times)$, and the associated L-functions $L_S(\chi, s)$, where S is a finite set of places including the infinite and ramified places, and L_S means ignore the places in S. We'll look at it for real s close to 1, say, $s \in \mathbb{R}_{>1}$. Look at the analytic behavior there. If χ is a nontrivial idele class character, then the function is holomorphic and nonzero; so it looks like $L_S(\chi, s) \sim 0 \neq c_\chi + O(s-1)$. If χ is trivial, then we're essentially talking about the Dedekind ζ function of K, and it looks like $\frac{1}{s-1} + O(1)$.

$$\begin{aligned}
L_S(\chi, s) &= \prod_{v \notin S} (1 - \chi(\pi_v) q_v^{-s})^{-1} \\
\log(1-x)^{-1} &= \sum_{m \geq 1} \frac{x^m}{m} \\
\log L_S(\chi, s) &= \sum_{v \notin S} \sum_{m \geq 1} \frac{\chi(\pi_v)^m q_v^{-ms}}{m} \\
\frac{d}{ds} \log L_S(\chi, s) &= -\sum_{v \notin S} \sum_{m \geq 1} (\log q_v) \chi(\pi_v)^m q_v^{-ms} \\
\sum_\chi \log L_S(\chi, s) &= -\sum_\chi \sum_{v \notin S} \sum_{m \geq 1} (\log q_v) \chi(\pi_v)^m q_v^{-ms} \\
\text{the rest is convergent, leaving} &\sim -\sum \chi \sum_{v \notin S} (\log q_v) \chi(\pi_v) q_v^{-s}
\end{aligned}$$

Let $h = [\mathbb{A}_K^\times : K^\times N_{L,K}(\mathbb{A}_L^\times)]$. Then we have

$$\begin{aligned}
&\sim \sum_\chi \sum_{v \notin S} (\log q_v) \chi(\pi_v) q_v^{-s} \\
&\sim h \sum_{v \notin S, \pi_v \in H} (\log q_v) q_v^{-s}
\end{aligned}$$

A miracle occurs and we're done, sorry.$\diamond$

We still need to prove the reciprocity law, and the existence theorem. The reciprocity law will make essential use of cyclotomic extensions; the existence theorem relies on Kummer extensions.

Last time we proved the first inequality; we gave Chevalley's algebraic proof, and sketched a more classical one. If L/K is the Galois of group G, then we can bound the norm index as $[\mathbb{A}_K^\times : K^\times N_{L,K}\mathbb{A}_L^\times] | [L : K]$, the second inequality. When G is cyclic, we showed $h(G, \mathbb{A}_L^\times/L^\times) = n$, and thus that $n | [\mathbb{A}_K^\times : K^\times N_{L,K}(\mathbb{A}_L^\times)]$; that's the first inequality. Ultimately, we'll show that all of these are equalities. Move on to

Reciprocity law The reciprocity law is a map $\mathrm{rec} : \mathbb{A}_K^\times/K^\times \to G = \mathrm{Gal}(L, K)$, where L/K is assumed abelian. Inside this picture is $\mathrm{rec}_v : K_v^\times \to G_v$. For v unramified, units must go to the trivial element. Put the local ones together to give $\mathbb{A}_K^\times \to G$; and the image must be G itself. That's a consequence of the first inequality; since if an extension is split almost everywhere, it's trivial.

Want sto show that for $a \in K^\times$, $\prod_v \mathrm{rec}_v(a) = 1$. This implies that $\mathrm{rec} : \mathbb{A}_K^\times/K^\times N_{L,K}(\mathbb{A}_L^\times) \rightharpoonup G$. The second inequality shows that this is actually an isomorphism.

The proof, perhaps a bit unnaturally, uses cyclotomic fields.

We start wth $1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times/L^\times$. Recall that $H^1(G, \mathbb{A}_L^\times/L^\times)$ is trivial. This gives a lon exact sequence involving brauer groups

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(G, L^\times) & \longrightarrow & H^2(G, \mathbb{A}_L^\times) & \longrightarrow & H^2(G, \mathbb{A}_L^\times/L^\times) \\ & & & & & & \\ & & \mathrm{Br}(L, K) & & \oplus_v H^2(G_w, L_w^\times) & & \\ & & & & & & \\ & & & & \oplus_v \mathrm{Br}(L_w, K_v) & & \end{array}$$

as always, w is a place lying over v. The fact that this is an injection is the Hasse principle. Eventually, we'll show that $H^2(G, \mathbb{A}_L^\times/L^\times) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, canonically. We'll use this and Tate's theorem to show that $\hat{H}^r(G, \mathbb{Z}) \xrightarrow{?\cup u_{L,K}} \hat{H}^{r+2}(G, \mathbb{A}_L^\times/L^\times)$ When $r = -2$, we interpret this as $G^{\mathrm{ab}} = G \xrightarrow{\cong} \mathbb{A}_K^\times/K^\times N_{L,K}(\mathbb{A}_L^\times)$. Keep interpreting.

$$\begin{aligned} n_v &\stackrel{\mathrm{def}}{=} [L_w : K_v] \\ \oplus_v \mathrm{Br}(L_w, K_v) &= \oplus_v \frac{1}{n_v}\mathbb{Z}/\mathbb{Z} \end{aligned}$$

Notes from Seon-In. Thanks.

Reciprocity law map We've proved it for cyclotomic field extensions. So for any $x \in \mathrm{Br}(L, K)$ with L/K cyclic and contained in a cylcotomic field, we know

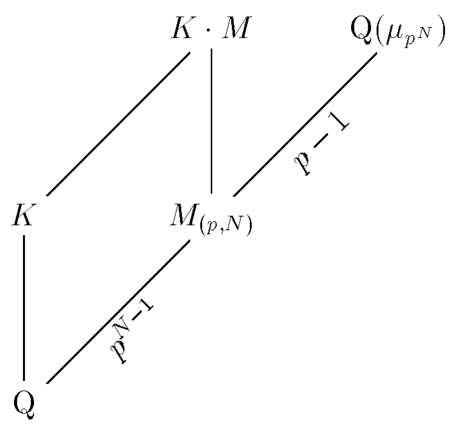
$$(*) \sum_v \mathrm{inv}_v(x) = \ 0 \in \mathrm{Q}/\mathrm{Z}$$

We want to show $(*)$ is true for any extension. Since for any $x \in \mathrm{Br}(K)$, $x \in \mathrm{Br}(L, K)$, $\mathrm{Br}(K) \hookrightarrow \prod_v \mathrm{Br}(K_v)$.

Proof Given $x \in \mathrm{Br}(K)$, $\mathrm{inv}_v(x) = 0$ for all $v \neq v_1, \cdots, v_N$. There's an m so that $m\,\mathrm{inv}_v(x) = 0$ for $v = v_1, \cdots, v_N$. Hence for all v, $m\,\mathrm{inv}_v(x) = 0$. It suffices to find an extension L/K cyclotomic and cyclic so that $[L_w : K_{v_i}] \equiv 0 \bmod m$.

We may assume m is a prime power, as $m = \prod_j p_j^{e_j}$; and if we can find L_j/K so that $[L_{j,w_i}; K_{v_i}] \equiv 0 \bmod p_j^{e_j}$, then we can just take $L = \prod_j L_j$.

So we may assume $m = p^e$.



Here, $\mathrm{Gal}(\mathrm{Q}(\mu_{p^N}), M_{(p,N)})$ is the order $p-1$ subgroup of $\mathrm{Z}/p^{N_1}(p-1)$. Then $[K \cdot M)_{w_i} : K_i]$ is a multiple of $\frac{[M_{p_i}:\mathrm{Q}_{p_i}]}{[K_{v_i}:\mathrm{Q}_{p_i}]}$. The local degree at KM/K can be decreased only by the local degree of K/Q. We want the local degree of M/Q big.

So w may assume $K = \mathrm{Q}$.

For simplicity's sake assume $p \neq 2$ is a finite prime.[24] Let $l_1, \cdots, l_k$ be rational primes; consider the extension $M_{(p,N)}/\mathbb{Q}$. If $l = p$, then $[M_w : \mathbb{Q}_p] = p^{N-1}$. If $l \neq p$, then $[\mathbb{Q}_l(\mu_{p^N}) : \mathbb{Q}_l]$ is the order of $\bar{l}$ in $(\mathbb{Z}/p^N)^\times$. Make N big, then the order of $\bar{l}$ gets big.

So we want to show that for L/K abelian, $\prod_v \mathrm{rec}_v(x) = 1$. This is $\iff$ for all $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, $\sum_v \chi(\mathrm{rec}_v(x)) = 0 \bmod \mathbb{Z}$. But $\chi(\mathrm{rec}_v(x)) = \mathrm{inv}_v(x \cdot \delta\chi)$, where $x \cdot \delta\chi \in \mathrm{Br}(K)$.

Given

$$\begin{tikzcd}[column sep=small] & LK_1 \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[dr, dash] & & K_1 \arrow[dl, dash] \\ & K & \end{tikzcd}$$

We get a commuting diagram

$$\begin{tikzcd} \mathbb{A}_{K,1}^\times / K_1^\times \arrow[r, dashed] \arrow[d] & \mathbb{A}_K^\times / K^\times \\ \mathrm{Gal}(LK_1, K_1) \arrow[r] & \mathrm{Gal}(L, K) \arrow[u] \end{tikzcd}$$

This gives us

$$\mathrm{Gal}(K_1^{\mathrm{ab}}, K_1) \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}, K)$$

corresponding to $N_{K_1,K}$. On the other hand, we have

[24] $p = \infty$ is trivial to handle.

$$\begin{array}{ccc} \mathbb{A}_K^\times/K^\times & \longrightarrow & \mathbb{A}_{K_1}^\times/K_1^\times \\ x & \longmapsto & x \end{array}$$

This corresponds to $\mathrm{Gal}(K^{\mathrm{ab}}, K) \to \mathrm{Gal}(K_1^{\mathrm{ab}}, K_1)$ by transfer. So

$$\lim_{\overleftarrow{L}} \frac{\mathbb{A}_K^\times}{K^\times N_{L,K}(\mathbb{A}_L^\times)} \xrightarrow{\cong} \mathrm{Gal}(K^{\mathrm{ab}}, K)$$

The existence theorem says that $\{N(\mathbb{A}_L^\times)\}$ is the same as the set of all open subgroups of finite index. Then $\pi_0(\mathbb{A}_K^\times/K^\times) \stackrel{\cong}{\to} \mathrm{Gal}(K^{\mathrm{ab}}, K)$.

Existence theorem Situation is this. We've got a number field K, and an open subgroup $H \subset \mathbb{A}_K^\times / K^\times$ of finite index. We want to produce a finite abelian extension L of K so that $N_{L,K}(\mathbb{A}_L^\times / L^\times) = H$.

We've already made it past the crux move: suppose $\mathbb{A}_K^\times / K^\times H \cong \mathbb{Z}/p\mathbb{Z}$ and $K \supseteq \mathbb{Q}(\mu_p)$. We did the following. Pick S a finite set of places containing all archimedean places. It should be large, in the sense that $K^\times \mathbb{A}_{K,S}^\times = \mathbb{A}_K^\times$. Further assume that $p \in K_S^\times$, and $H \supseteq \prod_{v \in S} \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} (K_v^\times)^p$; H is unramified outside S.

So we're really ocnsidering $K(\sqrt[p]{K_S^\times})$. In the course of the proof of the second inequality, we actually produced something contained in the norm group, whose index is already that required by the second inequality.

$$N \stackrel{\text{def}}{=} \prod_{v \in S} (K_v^\times)^p \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

Then

$$[\mathbb{A}_K^\times : K^\times \cdot N] = [K(\sqrt[p]{K_S^\times}) : K].$$

Of course, at this point we also know that

$$[\mathbb{A}_K^\times : K^\times \cdot N_{K(\sqrt[p]{K_S^\times}),K}(\mathbb{A}_{K(\sqrt[p]{K_S^\times})}^\times) = [K(\sqrt[p]{K_S^\times}) : K].$$

The conclusion is that

$$\begin{aligned} K^\times \cdot N &= N_{K(\sqrt[p]{K_S^\times}),K}(\mathbb{A}_{K(\sqrt[p]{K_S^\times})}^\times) \\ &\subseteq H \end{aligned}$$

So taking L to be $K(\sqrt[p]{K_S^\times})$ produces the desired extension.

Next, we make a reduction step. There's a nice norm map nm from the idele class group of L down to that of K. Assme L/K cyclic of prime order [?], and $\mathrm{nm}^{-1}(H) \subseteq \mathbb{A}_L^\times / L$. Want to show that H is a norm, that is, contains the group of all norms from some abelian extension. The reduction says that if we let $H' = \mathrm{nm}^{-1}(H)$, it suffices to verify the statement for L and H'.

Whyizzat? Assume H' is a norm group, that is, that there's an abelian extension M/L so that $H' = N_{M,L}(\mathbb{A}_M^\times / M^\times)$. Well, $N_{M,K}(\mathbb{A}_M^\times / M^\times) \subseteq H$; but then we're just about done. We have a norm subgroup contained in H. The big question is, is M/K abelian? Yes, but it requires a bit of argumentation.

1. M is Galois over K. That's because, for every $\sigma \in \mathrm{Gal}(L,K)$, $\sigma(H') = H'$.
2. Now we want to show that $\mathrm{Gal}(M,L) \subseteq Z(\mathrm{Gal}(M,K))$.

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(M,L) \arrow[r] & \mathrm{Gal}(M,K) \arrow[r] & \mathrm{Gal}(L,K) \arrow[r] & 1 \\
 & {} \arrow[u, "\mathrm{rec}"', "\cong"] & \mathbb{A}_L^\times / L^\times \cdot H' & &
\end{tikzcd}$$

There's a general functoriality.[25]

Want to figure out how conjugation by $\sigma \in \mathrm{Gal}(L,K)$ operates.

$$\begin{tikzcd}
\dfrac{\mathbb{A}_L^\times}{L^\times N_{M,L}(\mathbb{A}_M^\times)} \arrow[r, "\mathrm{rec}"] \arrow[d, "\sigma"] & \mathrm{Gal}(M,L) \arrow[d, "\text{via transport by } \sigma"] \\
\dfrac{\mathbb{A}_{L'}^\times}{L'^\times N_{M',L'}(\mathbb{A}_{M'}^\times)} \arrow[r, "\mathrm{rec}"] & \mathrm{Gal}(M',L')
\end{tikzcd}$$

Check that if $x \in \mathbb{A}_L^\times / L^\times \cdot H'$, then $\sigma x = x$. Equivalently, is $(\sigma x)x^{-1} \in H'$? That's the same as $N_{L,K}(\sigma(x)x^{-1}) \in H$; but $N_{L,K}(\sigma(x)x^{-1}) = 1$, which is clearly in H, so we're fine.

So much for that. Let's do the general case.

25

$$\begin{tikzcd}
M \arrow[rr, "\sigma"] \arrow[d, dash, "\mathrm{rec}"] & & M' \arrow[d, dash, "\mathrm{rec}"] \\
L \arrow[rr, "\sigma"] \arrow[dr, dash] & & L' \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

What?

Proof For $H \subsetneq \widetilde{H} \subsetneq \mathbb{A}_K^\times/K^\times$. Proof is by induction on $[\mathbb{A}_K^\times/K^\times : H]$. By the reduction we just did, we can assume whatever roots of unity we want are in there; it just gives a cyclic extension. Suppose $p|[\mathbb{A}_K^\times/K^\times : H]$. The base case is trivial. Assume $[\mathbb{A}_K^\times/K^\times : \widetilde{H}] = p$. We may assume that $K \supseteq \mathbb{Q}(\mu_p)$.

So there's L/K cyclic isomorphic to $\mathbb{Z}/p\mathbb{Z}$, $N_{L,K}(\mathbb{A}_L^\times) = \widetilde{H}$. The crux move, using Kummer theory, takes care of that.

$$\begin{tikzcd}
\mathbb{A}_L^\times \arrow[r, "N_{L,K}"] & \widetilde{H} & \subseteq & \mathbb{A}_K^\times \\
N_{L,K}^{-1}(H) \arrow[u, hook] \arrow[r] & H \arrow[u, hook]
\end{tikzcd}$$

Induction sez that $N_{L,K}^{-1}(H)$ is a norm subgroup. So L/K cyclic means that H is a norm subgroup.$\diamond$

In case you blinked, or something, we just finished the main parts of class field theory.

Suppose L/K finite Galois, $[L:K] = n$, $G = \mathrm{Gal}(L,K)$. We've got

$$1 \longrightarrow L^\times \longrightarrow \mathbb{A}_L^\times \longrightarrow \mathbb{A}_L^\times/L^\times \longrightarrow 1$$

$H^1(\cdot) = 0$ for these; something happens at H^2. Get

$$0 \longrightarrow H^2(G, L^\times) \longrightarrow H^2(G, \mathbb{A}_L^\times) \longrightarrow H^2(G, \mathbb{A}_L^\times/L^\times)$$

$$\oplus_v H^2(G_v, L_w^\times)$$

$$\oplus_v \mathrm{Br}(L_w, K_v)$$

We assert that the right-hand map is actually a surjection, and that

$$H^2(G, \mathbb{A}_L^\times/L^\times) \cong n^{-1}\mathbb{Z}/\mathbb{Z}.$$

So the map $\oplus \mathrm{Br}(L_w, K_v) \to n^{-1}\mathbb{Z}/\mathbb{Z}$ is essentially summation.

Cohomology of profinite groups What we usually use for coefficients are discrete modules. In that case, nothing much happens. Then

$$\begin{aligned} H^\bullet(G, M) &= \varinjlim_{U \trianglelefteq G \text{ open}} H^\bullet(G/U, M^U) \\ &= H^\bullet(\text{std cochain complex}) \end{aligned}$$

If M is not discrete, you can quickly get into trouble. But with any luck we'll be able to avoid that case, for the time being anyway.

Definition [Cohomological dimensions] The cohomological dimension of G is

$$\begin{aligned} \mathrm{cd}(G) &\stackrel{\text{def}}{=} \inf\{i \in \mathrm{N} : H^j(G, M) = 0 \forall i > 0 \\ &\qquad \text{and discrete torsion } G\text{-modules } M\} \\ \mathrm{scd}(G) &\stackrel{\text{def}}{=} \inf\{i \in \mathrm{N} : H^j(G, M) = 0 \forall i > 0 \\ &\qquad \text{and discrete } G\text{-modules } M\} \end{aligned}$$

Here, scd is the strict cohomological dimension. It turns out that $\mathrm{cd}(G) \leq \mathrm{scd}(G) \leq \mathrm{cd}(G)+1$. That's an easy exercise. Use a long exact sequence, no doubt.

There are local versions of these, cd_p and scd_p. You can define 'em as

$$\begin{aligned} \mathrm{cd}_p(G) &\stackrel{\text{def}}{=} \inf\{i \in \mathrm{N} : H^j(G, M)_{(p)} = 0 \forall i > 0 \\ &\qquad \text{and discrete torsion } G\text{-modules } M\} \\ \mathrm{scd}_p(G) &\stackrel{\text{def}}{=} \inf\{i \in \mathrm{N} : H^j(G, M) = 0 \forall i > 0 \\ &\qquad \text{and discrete } G\text{-modules } M\} \end{aligned}$$

Just look where the p-torsion is killed.

Exercise If G is a nontrivial finite group, then $\mathrm{cd}(G) = \infty$.[26]

[26] Idea: If you start with a cyclic group, it's not going to have finite cohomological dimension, since it's periodic [of period 2], and so never stops. By Shapiro's lemma, you can induce to bigger groups. Work it out.

Exercise Compute $\mathrm{cd}(\hat{\mathbb{Z}})$ and $\mathrm{scd}(\hat{\mathbb{Z}})$. Should turn out to have $\mathrm{cd}(\hat{\mathbb{Z}}) = 1$.

Fact K a nonarchimedean locally compact local field.[27] Let $G = \mathrm{Gal}(K^{\mathrm{sep}}, K)$. Then $\mathrm{scd}_l(G) = \mathrm{cd}_l(G) = 2$ if $l \neq \mathrm{char}\, K$.[28] If $l = \mathrm{char}\, K$, then $\mathrm{scd}_l(G) = 2$, $\mathrm{cd}_l(G) = 1$.[29]

For the rest of the year, we'll be doing some sort of arithmetic duality.

Let's think about local class field theory for a bit. The key was this. Let L/K be a finite extension of local fields. Then $H^1(\mathrm{Gal}(L,K), L^\times) = 0$; that's Hilbert 90. And $H^2(\mathrm{Gal}(L,K), L^\times) = n^{-1}\mathbb{Z}/\mathbb{Z}$, where $n = [L : K]$. Now, $\mathrm{Gal}(L,K)$ is a finite quotient $\frac{\mathrm{Gal}(K^{sep},K)}{\mathrm{Gal}(K^{sep},L)}$. And $L^\times = (K^{\mathrm{sep}})^{\times\,\mathrm{Gal}(K^{sep},L)}$. Take limits. Then $H^2(\mathrm{Gal}(K^{\mathrm{sep}}, K), (K^{\mathrm{sep}})^\times) = \mathbb{Q}/\mathbb{Z}$. And inflation corresponds to injection, restriction to multiplication by the degree of the extension.

On the other hand, we have global class field theory. Let L/K be a finite extension of global fields, $[L : K] = n$. Again, $H^1(\mathrm{Gal}(L,K), \mathbb{A}_L^\times/L^\times) = 0$.[30] And $H^2(\mathrm{Gal}(L,K), \mathbb{A}_L^\times/L^\times) = n^{-1}\mathbb{Z}/\mathbb{Z}$. If $M \supset L \supset K$, then $(\mathbb{A}_M^\times/M^\times)^{\mathrm{Gal}(M,L)} = \mathbb{A}_L^\times/L^\times$. Why is this? General trick to verify it. Well, $\mathbb{A}_L^\times$ is the Galois invariants of $\mathbb{A}_M^\times$; and $M^\times$ those of $L^\times$. Want to measure whether the invariant of the quotient is the quotient of the invariant. So take cohomology of $1 \to M^\times \to \mathbb{A}_M^\times \to \frac{\mathbb{A}_M^\times}{M^\times} \to 1$. And whether or not ths is everything is precisely $H^1(G, M^\times)$, which is zero by Hilbert 90. BTW, $H^2(\mathrm{Gal}(K^{\mathrm{sep}}, K), \mathbb{A}_{K^{\mathrm{sep}}}^\times/K^{\mathrm{sep}\times}) = \mathbb{Q}/\mathbb{Z}$.

In such situations, there's a theorem of Tate – which we proved, actually – that $H^r(G, \mathbb{Z}) \overset{\cup}{\to} H^{r+2}(G, \cdot)$; take $r = -2$, and recover the inverse reciprocity law.

A class formation abstracts from these two examples.

Definition A class formation for a profinite group G is a discrete G-module C such that:

1. For every open normal subgroup $U \trianglelefteq G$, $H^1(G/U, C^U) = 0$.
2. There's an isomorphism $i : H^2(G, C) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}$ so that for every open normal $U \trianglelefteq G$, we have

[27] This just means the residue field is finite.
[28] Serre, *Cohomologie Galoisienne* II.5., Prop 15.
[29] Serre, I.3.3, Cor 4, III.2.2 Prop 3.
[30] Not Hilbert 90, but the second fundamental inequality.

$$\begin{tikzcd} H^2(G,C) \arrow[r, "i", "\cong"'] & \mathrm{QZ} \\ H^2(U,C) \arrow[u] \arrow[r, "i", "\cong"'] & n^{-1}\mathrm{Z}/\mathrm{Z} \arrow[u, hook] \end{tikzcd}$$

where $n = [G : U]$. This tells you that inflation maps are good. What about restriction? If U E V E G are all open subgroups, then

Class formation G a profinite group, C a discrete G-module, subject to the following axioms.

1. $H^1(G, C) = 0$¿ More generally, for all $U \subseteq G$ open, $H^1(U, C) = 0$.
2. $\mathrm{inv} : H^2(G, C) \overset{\cong}{\to} \mathbb{Q}/\mathbb{Z}$. More generally, for all $U \subseteq G$ open,

$$H^2(U, C) \xrightarrow[\mathrm{inv}_U]{\cong} \mathbb{Q}/\mathbb{Z}$$

3. If $U_1 \subseteq U_2 \subseteq G$ both open, then we have

$$\begin{tikzcd} H^2(U_2, C) \arrow[r, "\mathrm{inv}_{U_2}"] \arrow[d, "\mathrm{res}_{U_2,U_1}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[U_2 : U_1]}"] \\ H^2(U_1, C) \arrow[r, "\cong", "\mathrm{inv}_{U_1}"'] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

This isn't quite the same formulation as Artin-Tate, but it's pretty close.

Here's a variant. Let P be a collection of prime numbers. Take the l-primary part everywhere for all $l \in P$, in all diagrams and statements above.

Anyways, from this setup you can get some sort of reciprocity law[s]:

$$C^G \xrightarrow{\mathrm{rec}_G} G^{\mathrm{ab}}$$

And get a similar law for every open $U \subseteq G$. This is from Tate's theorem, which says that for all i we have

$$\hat{H}^i(G/U, \mathbb{Z}) \xrightarrow[\cong]{\cup u_{G/U}} \hat{H}^{i+2}(G/U, C^U)$$

For $I = -2$, get

$$\begin{array}{ccc} (G/U)^{\mathrm{ab}} & \longrightarrow & \dfrac{C^G}{N_{G,U}(C^U)} \\ \dfrac{G^{\mathrm{ab}}}{\operatorname{im} U} & & \end{array}$$

Take limit over U's to get rec_G. The image of the reciprocity law is dense in the target space, even though this isn't an honest surjection. The kernel is the universal norms.

Here's another example of a class formation. Suppose $G \cong \hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$. What should we take C to be? Exercise: make this make sense.

Duality theory We'll start off with dimension 2. Want the target to be $\mathbb{Q}/\mathbb{Z} = (\hat{\mathbb{Z}})^\vee$.[31] So we use

$$\begin{tikzcd} & \mathbb{Q}/\mathbb{Z} \\ H^i(G,M) \times H^{2-i}(G, \mathrm{Hom}_{\mathbb{Z}}(M,C)) \arrow[r] & H^2(G,C) \arrow[u, "\mathrm{inv}_G"', "\cong"] \end{tikzcd}$$

This isn't what we'll use in the end, but it's close enough that maybe you can figure out what we're talking about. We got the Hom thing by a "what else could it be?" argument. But this is basically just the extension group $\mathrm{Ext}^{2-i}_G(M,C)$, since there's a spectral sequence at work here. In general, $E_2^{a,b} = H^a(G, \mathrm{Ext}^b_{\mathbb{Z}}(M,C)) \Rightarrow \mathrm{Ext}^{a+b}(M,C)$. Well, that's the motivation, hope you enjoyed it.

Let's start in. There's the Yoneda pairing

$$\mathrm{Ext}^i_G(M,C) \times \mathrm{Ext}^j_G(N,M) \longrightarrow \mathrm{Ext}^{i+j}_G(N,C)$$

How do we think about this? Resolve M by $M \to M^\bullet$ an injective resolution. Then an element of $\mathrm{Ext}^j_G(N,M)$ is represented by a G-equivariant homorphism $h_1 : N \to M^\bullet$ of degree j. In this case, it sends N to M^j. What about $\mathrm{Ext}^i_G(M,C)$? We've already chosen

[31] In the DeRham contex, we had $H^i(M,\mathbb{R}) \times H^{n-i}(M,\mathbb{R}) \to H^n(M,\mathbb{R}) \overset{\cong}{\to} \mathbb{R}$, where the last isomorphism is the trace map $\alpha \mapsto \int_M \alpha$.

$M \to M^\bullet$; now resolve C, $C \to C^\bullet$. Then we represent an element of $\mathrm{Ext}^i_G(M, C)$ as a map $H_2 : M^\bullet \to C^\bullet$ of degree i. The obvious way to get in $\mathrm{Ext}^{i+j}_G(N, C)$ is to compose these two homomorphisms; $h_2 \times h_1 \mapsto h_2 \circ h_1$.

Here's another way to think about it; think of the equivalence classes of extensions $0 \to M \to \bullet \to \cdots \to \bullet \to N \to$ with j things between them; that's $\mathrm{Ext}^j_G(N, M)$. And $\mathrm{Ext}^i_G(M, C)$ is similar; then just concatenate them to get an $\mathrm{Ext}^{i+j}_G(N, C)$.

In our situation, we specialize to $N = \mathbb{Z}$ with the trivial action. But $\mathrm{Ext}^j_G(\mathbb{Z}, M) = H^j(G, M)$, by definition; and $\mathrm{Ext}^{i+j}_G(\mathbb{Z}, C) = H^{i+j}(G, C)$. Take $j = 2-i$. And $H^2(G, C) \stackrel{\mathrm{inv}_G}{\to} \mathbb{Q}/\mathbb{Z}$;

$$\mathrm{Ext}^i_G(M, C) \longrightarrow H^{2-i}(G, M)^\vee = \mathrm{Hom}_{\mathbb{Z}}(H^{2-i}(G, M), \mathbb{Q}/\mathbb{Z})$$

That's the natural map. Let's figure out what it is.

Special case. Take $M = \mathbb{Z}$; look at this map.

- $i = 0$ Then $\mathrm{Ext}^i_G(M, C) = C^G$; and it gets sent to $H^1(G, \mathbb{Q}/\mathbb{Z})^\vee = G^{\mathrm{ab}}$. So it's

$$C^G \longrightarrow G^{\mathrm{ab}}$$

  That's gotta be the reciprocity law.

- $i = 1$. Then $\mathrm{Ext}^i_G(M, C) = 0$ by our axiom for class field formations. And the target is $H^1(G, \mathbb{Z})^\vee$, which is also trivial:

$$0 \longrightarrow 0$$

- $i = 2$. Left-hand is $H^2(G, C)$; and right-hand is $H^0(G, \mathbb{Z})^\vee = \mathbb{Q}/\mathbb{Z}$.

$$H^2(G, C) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

  And this really oughta be the invariant map inv_G.

- $i > 2$, then everything's zero; remember the cohomological dimension.

Let's prove that last little bit. Assume $i > 2$. Let $n_U = [G : U]$; assume $V \subset U$ open. Use the inflation map:

$$\begin{tikzcd}
H^{i-2}(G/U, \mathbb{Z}) \arrow[r, "\cong", "\mathrm{inv}_U"'] \arrow[d, "?"] & H^i(G/U, C^U) \arrow[d, "\mathrm{inf}_{U,V}"] \\
H^{i-2}(G/V, \mathbb{Z}) \arrow[r, "\cong", "\mathrm{inv}_V"'] & H^i(G/V, C^V)
\end{tikzcd}$$

The left-hand side is multiplication by the index;

$$\begin{tikzcd}
x \arrow[r, mapsto] & x \cup u_{G/U} \arrow[dd, mapsto, shift left=20] \\
H^{i-2}(G/U, \mathbb{Z}) \arrow[r, "\cong", "\mathrm{inv}_U"'] \arrow[d, "{[U:V]\,\mathrm{inf}_{U,V}}"] & H^i(G/U, C^U) \arrow[d, "\mathrm{inf}_{U,V}"] \\
H^{i-2}(G/V, \mathbb{Z}) \arrow[r, "\cong", "\mathrm{inv}_V"'] & H^i(G/V, C^V) \quad \mathrm{inf}(x) \cup \mathrm{inf}(u_{G/U})
\end{tikzcd}$$

$$\mathrm{inf}(x) \cup [U : V] u_{G/V}$$