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,

$$H^{\bullet}(G, A) = \operatorname{Ext}_{\mathbf{Z}[G]}^{\bullet}(\mathbf{Z}, A)$$
  
 $H_{\bullet}(G, A) = \operatorname{Tor}_{\bullet}^{\mathbf{Z}[G]}(\mathbf{Z}, A)$ 

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  $H\to G$ , 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  $H^1(G, A)$ .

Jeff Achter 1 Ching-Li Chai

<sup>&</sup>lt;sup>1</sup>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,

$$E_2^{0,1} = H^0(G/H, H^1(H, A))$$
  
=  $H^1(H, A)^G$ 

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  $A \cdot A^G$ , the fixed part. But this is a composition of two functors;  $A \cdot A^H$ , a G/H-module. And then use  $A^H \cdot (A^H)^{G/H}$ . 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  $cor_{G,H}$ . 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.

Jeff Achter 2 Ching-Li Chai

$$H^{0}(G, A) \longleftarrow H^{0}(H, A)$$

$$A^{G} \qquad A^{H}$$

$$\sum_{s \in G/H} sa \longleftarrow a$$

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

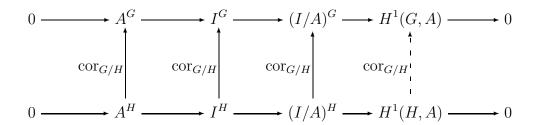
$$0 \longrightarrow A^G \longrightarrow I^G \longrightarrow (I/A)^G \longrightarrow H^1(G,A) \longrightarrow 0$$

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

$$\operatorname{Hom}_{H}(?, I) = \operatorname{Hom}_{G}(\mathbf{Z}[G] \otimes_{\mathbf{Z}[H]}?, I)$$

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

Jeff Achter 3 Ching-Li Chai



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

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

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow$$

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

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.

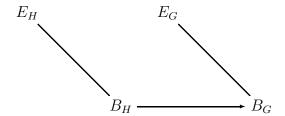
Use the standard resolution of, say, the inhomogeneous complex, for G. Call the resolution C. Observe that this is also a free resolution of Z by free Z[H]-modules;  $C_{\bullet} \to Z$ . We can use this complex to compute the cohomology of the group H.

$$H^{\bullet}(\operatorname{Hom}_{H}(C_{\bullet}, A)) = H^{\bullet}(H, A).$$

So if we can define a map  $\operatorname{Hom}_H(C_{\bullet}, A) \to \operatorname{Hom}_G(C_{\bullet}, A)$  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  $\operatorname{Hom}_H$  This gives a map on the level of cochains, which induces everything.

Jeff Achter 4 Ching-Li Chai

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; and the universal cover  $E_H$ . And we can think of A as a sheaf of coefficients.<sup>2</sup>



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  $G = \mathbf{Z}/n\mathbf{Z} = \langle s \rangle$ . 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;  $N = N_G = \sum_{i=0}^{n-1} s^i$ .

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

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  $B_G=\mathrm{P}_{\mathrm{R}}^\infty$ .  $E_G=S^\infty$ ; and  $S^\infty \rightharpoonup \mathrm{P}_{\mathrm{R}}^\infty$ .

So much for the examples. The map  $H_i(H,A) \to H_i(G,A)$  is  $\operatorname{cor}_{G/H}$ . 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  $\operatorname{res}_{G/H}$ .

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

res : 
$$H_0(G, A) \rightarrow H_0(H, A)$$
  
 $A_G \rightarrow A_H$   
 $\overline{a} \mapsto \sum_{s \in H \setminus G} \overline{sa}$ 

Jeff Achter 5 Ching-Li Chai

 $<sup>^{2}</sup>$ 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  $(\sigma - 1)b \mapsto \sum_{s \in H \setminus G} s(\sigma - 1)b$ . Exercise to verify this.

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

**Proposition**  $H^i(G,A) \leftrightarrow_{\operatorname{cor}}^{\operatorname{res}} H_i(H,A)$ . Then  $\operatorname{cor}_{G/H} \circ \operatorname{res}_{G/H} = [G:H]$  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; res $\circ$  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  $H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Z})$ .

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

$$G^{\rm ab} = \frac{G}{G'}$$
  $H^{\rm ab} = \frac{H}{H'}$ 

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.

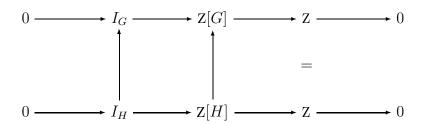
$$0 \longrightarrow I_G \longrightarrow \mathbf{Z}[G] \longrightarrow \mathbf{Z} \longrightarrow 0$$

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.

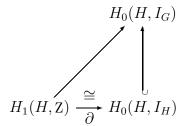
$$0 \longrightarrow H_1(G, \mathbf{Z}) \xrightarrow{\partial} H_0(G, I_G) = I_G/I_G^2 \longrightarrow 0$$

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

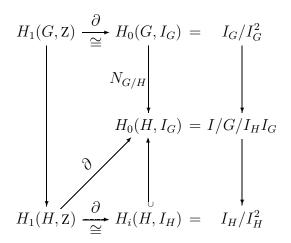
Jeff Achter 6 Ching-Li Chai



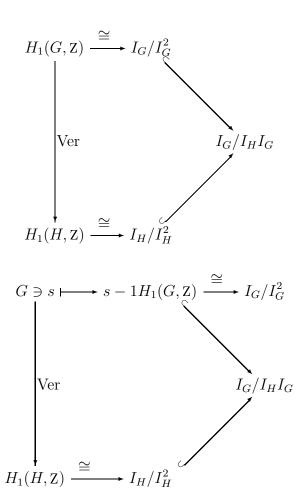
So maybe what we want is



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



Moving on, somewhat.



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

$$\sum_{t \in H \setminus G} t(s-1) = \sum_{i} h_{i} t_{j(i)} - t_{j(i)}$$

$$= \sum_{i} (h_{i} - 1) t_{j(i)}$$

$$= \sum_{i} (h_{i} - 1) (t_{j(i)} - 1) + \sum_{i} (h_{i} - 1)$$

$$\sum_{i} (h_{i} - 1) (t_{j(i)} - 1) \in I_{H} I_{G}$$

$$\sum_{i} (h_{i} - 1) \in I_{H}$$

We summarize the conclusions of this computation.

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

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  $H \setminus G$ .

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  $\{w_1, w_1s, w_1s^2, \dots, w_1s^{f_1-1}, w_2, \dots, w_js^{f_j-1}\}$ Then  $\operatorname{Ver}(\overline{s}) = \overline{\prod_j h_j}$ .

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  $G = \operatorname{Gal}(L,K)$ , and  $L \supset M \supset K$ ;  $H = \operatorname{Gal}(L,M)$ . Then there's a map  $\operatorname{Ver}_{L/M}: G^{ab} \to H^{ab}$ . 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  $\mathfrak{p} \cdot (\mathfrak{p}, L/K)$ . Anyways,  $\mathfrak{p} \cdot (\mathfrak{p}, L/K) \in G^{ab}$ . Since all reps are conjugate, this is well-defined. We apply  $\operatorname{Ver}_{L,M}$  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  $\mathfrak{p} = \prod_i \mathfrak{q}_i$ , etc.

Jeff Achter 9 Ching-Li Chai

<sup>&</sup>lt;sup>3</sup>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  $Gal(\lambda_{\mathfrak{P}_i}, \kappa)$ . 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 Gal(L, K).

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

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

where  $w_i s^{f^j} = h_i w_i$ . So then we know that

$$\overline{(\prod_{j} h_{j})} = \operatorname{Ver}(s)$$

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,

$$h_{j} = w_{j}s^{f_{j}}w_{j}^{-1}$$

$$= \operatorname{Fr}_{\mathfrak{P}_{i},\mathfrak{q}_{j}}$$

$$\overline{(\prod_{j}h_{j})} = \prod_{j}\operatorname{Fr}_{\mathfrak{q}_{j}}$$

$$= \operatorname{Ver}(\prod_{j}\mathfrak{q}_{j}, L/M)$$

$$= \operatorname{Ver}(\mathfrak{p}\mathcal{O}_{M}, L/M)$$

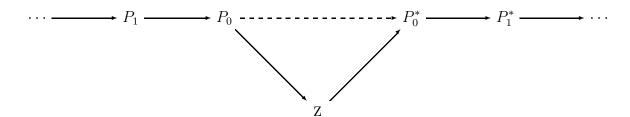


We'll now discuss cohomology of *finite* groups. So let G be a finite group. The following is basically said to be Tate's fault; Tate cohomology groups. Recall how we defined homology and cohomology. They're defined by, well, let  $P_{\bullet} \to Z \to 0$  be a standard resolution of Z. Take the dual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

Jeff Achter 10 Ching-Li Chai

$$0 \to Z \to P_{\bullet}^* = \operatorname{Homz}(P_{\bullet}, Z)$$

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



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,  $P_0 = \mathbf{Z}[G]$ . And the map there is the only one possible;  $\sum n_{\sigma}\sigma \mapsto \sum n_{\sigma}$ . That's  $\epsilon$ ; feels a little like the degree map. And  $P_0^* = \operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], \mathbf{Z})$ . So we've got  $\mathbf{Z} \to P_0^*$ , via  $1 \mapsto (\sigma \mapsto 1)$ ;  $1 \mapsto \sum \sigma^*$ .

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

$$P_0 \longrightarrow P_0^*$$

$$Z[G] \qquad Z[G]$$

If  $g \in G$  then

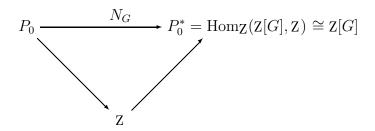
$$(g\sigma^*)(t) \stackrel{\text{def}}{=} \sigma^*(g^{-1}t)$$

$$= \delta_{\sigma,g^{-1}t}$$

$$= \begin{cases} 1 & t = g\sigma \\ 0 \end{cases}.$$

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

At the end of the day, we conclude that



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

**Definition** For a G-module A,

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

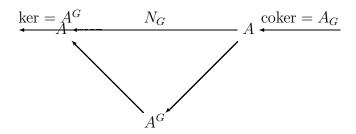
4

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  $\mathbf{Z}[G] \xrightarrow{N_G} \mathbf{Z}[G]$ . Take  $\mathrm{Hom}(\cdot, A)$  to get  $A \leftarrow A$ . And actually, we've got



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

Jeff Achter 12 Ching-Li Chai

<sup>&</sup>lt;sup>4</sup>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  $\mathbf{Z}[G]^{\otimes n}$ .

## **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,

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

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

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

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

$$\widehat{H}^{-1}(G, A'') \xrightarrow{\delta} \widehat{H}^{0}(G, A')$$

$$\uparrow \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \downarrow \qquad \qquad \qquad \qquad \qquad$$

The assertion is that these commute.<sup>5</sup>

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

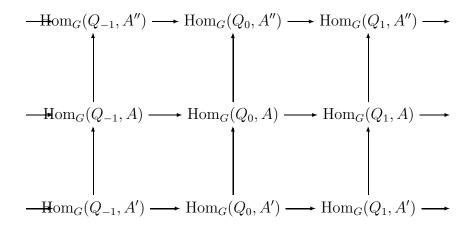
$$\widehat{H}^{-1}(G, A'') \xrightarrow{\delta} \widehat{H}^{0}(G, A')$$

$$\frac{\ker N_{G}}{I_{G}A''} \qquad \frac{A'^{G}}{N_{G}A'}$$

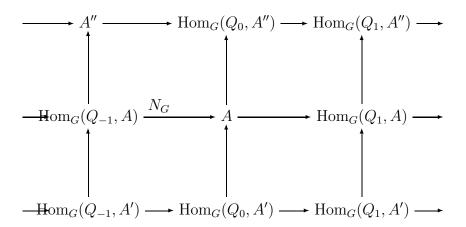
Jeff Achter 13 Ching-Li Chai

<sup>&</sup>lt;sup>5</sup> "This isn't going to be hard. If it's really hard, you can't do it."

Go for the proof.



Do the usual diagram chase to get from  $\operatorname{Hom}_{G}(_{-1}, A'')$  to  $\operatorname{Hom}_{G}(Q_{0}, A')$ . But we know what some of these objects are.



So the map we were worrying about before is, essentially, given by the norm  $N_G$ ; the map  $\widehat{H}^{-1}(G, A'') \stackrel{\delta}{\to} \widehat{H}^0(G, A')$  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.

Jeff Achter 14 Ching-Li Chai

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;  $H^{\bullet}(X \times X, A \otimes B) = H^{\bullet}(X, A) \otimes H^{\bullet}(X, B)$ . Composing with  $\Delta^*$  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 have 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,  $\widehat{H}^0(G,A)=\frac{A^G}{N_GA}$ , and  $\widehat{H}^0(G,B)\frac{B^G}{N_GB}$ . 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

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

Jeff Achter 15 Ching-Li Chai

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

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

$$\delta \otimes \operatorname{id}^{p} \qquad \delta \widehat{H}^{p+1}(G, A') \otimes \widehat{H}^{q}(\widehat{E}, B)^{+1}(G, A' \otimes B)$$

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.

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

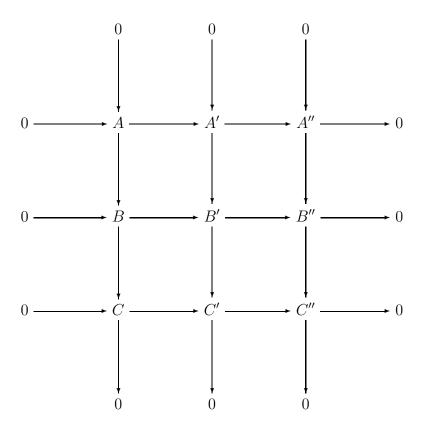
$$(-1)^{p} \operatorname{id} \otimes \delta \downarrow \qquad \qquad \delta \downarrow$$

$$\widehat{H}^{p}(G, A) \otimes \widehat{H}^{q+1}(G, B') \xrightarrow{\bigcup} \widehat{H}^{p+q+1}(G, A \otimes B')$$

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.



Then

$$\widehat{H}^{p+1}(G, A'') \xrightarrow{\delta} \widehat{H}^{p+2}(G, A)$$

$$-\delta \qquad \qquad \delta \qquad \qquad \delta \qquad \qquad \delta \qquad \qquad \delta \qquad \qquad \widehat{H}^{p}(G, C'') \xrightarrow{\delta} \widehat{H}^{p+1}(G, C)$$

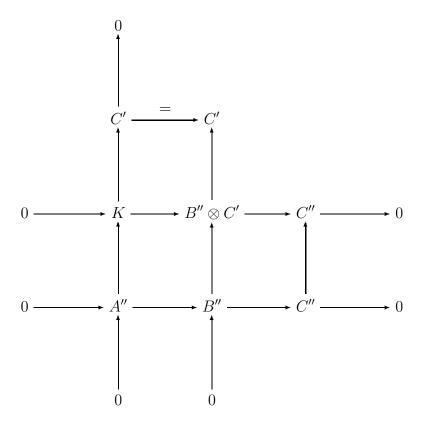
commutes.

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

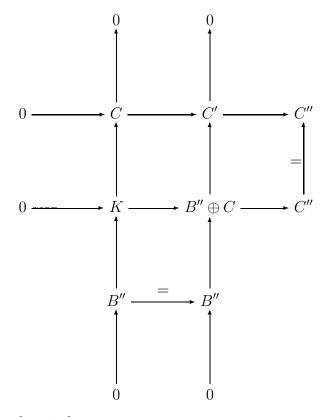
**Proof** [of lemma] "I know if I try it for a while, I'll get there."

Jeff Achter 17 Ching-Li Chai

Define a kernel K via



At the same time, we have



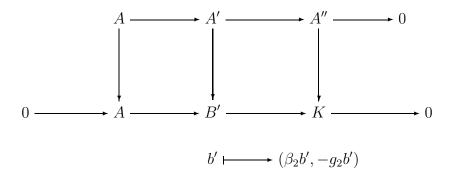
Shit. I've lost the thread entirely.

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  $\alpha_1, \alpha_2$ ;  $\beta_1, \beta_2$ ; and  $\gamma_1, \gamma_2$ . 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

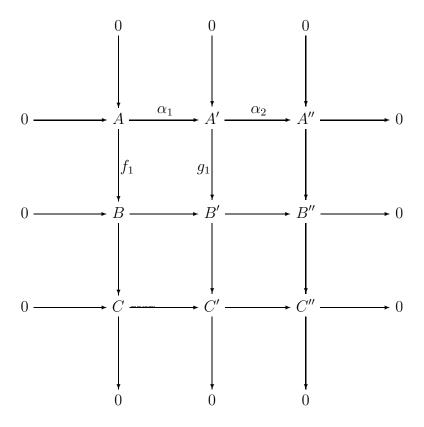


Jeff Achter 19 Ching-Li Chai

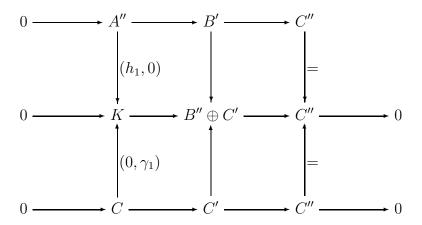
Strategy should be; produce a couple of commutative diagrams, and then by naturality show that they're really the same thing.

Jeff Achter 20 Ching-Li Chai

We're going back to the diagram chase:

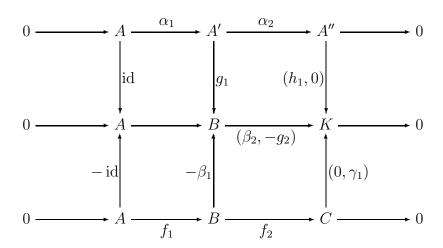


Then we get



as well as

Jeff Achter 21 Ching-Li Chai



And the minus signs are necessary for everything to commute.

Suppose  $c'' \in H^i(G, C'')$ . Then  $H^{i+1}(G, K) \ni \delta_{\text{mid}}(c'') = \gamma_1(\delta_l(c'')) = h_1(\delta - u(c''))$ . 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  $\operatorname{res}_{G/H}(a \cup b) = \operatorname{res}(a) \cup \operatorname{res}(b)$ , 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  $\operatorname{cor}(\operatorname{res}(a) \cup b) = a \cup \operatorname{cor}(b)$ . 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.

Jeff Achter 22 Ching-Li Chai

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  $p, q \ge 0$ , then

$$\phi_{p,q}:\sigma_0\otimes\cdots\sigma_{p+q}\mapsto(\sigma_0\otimes\cdots\otimes\sigma_p)\otimes(\sigma_p\otimes\cdots\otimes\sigma_{p+1}).$$

• If  $p \ge 1$ ,  $q \ge 1$ , then

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

•  $p \ge 0, q \ge 1$ . Then

$$\phi_{p,-p-q}(\sigma_1^* \otimes \cdots \otimes \sigma_q^*) \mapsto \sum_{\substack{s_1, \dots, s_p \in G}} (\sigma_1 \otimes s_1 \otimes \cdots \otimes s_p) \otimes (s_p^* \otimes \cdots \otimes s_1^* \otimes \sigma_1^* \otimes \cdots \otimes \sigma_q^*)$$

$$\phi_{-p-q,p}(\sigma_1^* \otimes \cdots \otimes \sigma_q^*) \mapsto \sum_{\substack{s_1, \dots, s_p \in G}} (\sigma_1^* \otimes \cdots \otimes \sigma_q^* \otimes s_1^* \otimes \cdots \otimes s_p^*) \otimes (s_p \otimes \cdots \otimes s_1 \otimes \sigma_1)$$

$$\phi_{p_q,-q}(\sigma_0 \otimes \cdots \otimes \sigma_p) \mapsto \sum_{\substack{s_1, \dots, s_q \in G}} (\sigma_0 \otimes \cdots \otimes \sigma_p \otimes s_1 \otimes \cdots \otimes s_q) \otimes (s_q^* \otimes \cdots \otimes s_1^*)$$

$$\phi_{-q,p+q}: \sigma_0 \otimes \cdots \otimes \sigma_p \mapsto \sum_{\substack{s_1, \dots, s_q \in G}} (s_1^* \otimes \cdots \otimes s_q^*) \otimes (s_q \otimes \cdots \otimes s_1 \otimes \sigma_0 \otimes \cdots \otimes \sigma_p)$$

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.

Jeff Achter 23 Ching-Li Chai

**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

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

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

$$0 1 2$$

$$\mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G] \xrightarrow{s-1} \mathbf{Z}[G] \xrightarrow{N} \mathbf{Z}[G]$$

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

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

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

Jeff Achter 24 Ching-Li Chai

**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  $\widehat{H}^2(G,\mathbb{Z})/\text{Look}$  at

$$0 \to Z \to Q \to Q/Z \to 0$$

Now, Q has no cohomology whatsoever.<sup>6</sup> For it's a torsion Q-vector space. So  $\widehat{H}^{0}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \cong \widehat{H}^{2}(G, \mathbb{Z})$ . But  $\widehat{H}^{1}(G, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$ . Thus,  $s ! \chi_{s} \in \operatorname{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) - \widehat{H}^{2}(G, \mathbb{Z})$ , and  $\chi_{s}(s) = \frac{1}{n} \mod \mathbb{Z}$ .

**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 = Z. When you do it with coeffs in 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  $\chi_s$ . 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 Z[G]-modules, and  $h(G,\cdot)$  defined for two of the three modules, then h is defined for all of them, and

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

Jeff Achter 25 Ching-Li Chai

<sup>&</sup>lt;sup>6</sup>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  $\widehat{H}^i(G,A) \stackrel{\operatorname{res}_{G,\{e\}}}{\to} \widehat{H}^i(e,A) \stackrel{\operatorname{cor}}{\to} \widehat{H}^i(G,A)$ ; 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.  $h(A) \stackrel{\text{def}}{=} \frac{h^{\text{even}}(A)}{h^{\text{odd}}(A)}$ .

**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,  $Card(A^G) = Card(A_G)$ . And

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

 $\Diamond$ 

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  $H \subset G$ .

Jeff Achter 26 Ching-Li Chai

**Proof** ( $\Leftarrow$ ) By induction on the cardinality of G. If  $\operatorname{Card}(G)$  is not a prime power, then for every p-Sylow subgroup  $G_p$  (G, by induction  $\widehat{H}^i(G_p, A) = 0$  for all  $i \in \mathbb{Z}$ . So  $\widehat{H}^i(G, A) = 0$ . So now we may assume that G is a p-group. G is supersolvable, so there's  $H \to G$  so that  $G/H \cong \mathbb{Z}/p\mathbb{Z}$ .

Recall that, in general, given  $H \to G$  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  $i_0 + 2$ .

We can seemingly strengthen this statement.

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

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

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

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

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.

Jeff Achter 27 Ching-Li Chai

<sup>1.</sup>  $\widehat{H}^i(G_p, A)$  is well-defined up to canonical isomorphism.

<sup>2.</sup>  $\widehat{H}^{i}(G,A) \stackrel{\text{res}}{\hookrightarrow} \bigoplus_{p | \# A} \widehat{H}^{i}(G_{p},A)$  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  $\widehat{H}^i(G, \mathbf{Z}) \stackrel{a \cup \cdot}{\to} \widehat{H}^i(G, A)$  for every i.

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

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

Write down the long exact sequence from this. Get

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

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

**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 Card(H).

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

**Proof** Dimension shift from previous theorem.

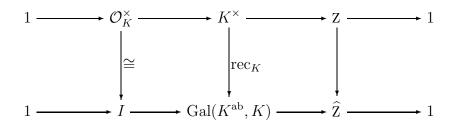
**Exercise** For all  $H \subseteq G$ , res a is a generator of  $\widehat{H}^2(H, A)$ .

Jeff Achter 28 Ching-Li Chai

**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.<sup>8</sup> We'll try to understand  $K^{\text{ab}}$ , 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

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

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.



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

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

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.

Jeff Achter 29 Ching-Li Chai

<sup>&</sup>lt;sup>8</sup>As a generalization, one can do almost everything we'll do here if we just assume that  $\kappa$  is perfect, and  $\operatorname{Gal}(\overline{\kappa},\kappa) = \widehat{Z}$  a free cyclic group. One usually says that  $\kappa$  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  $[A]^{-1} = [A^{\text{opp}}]$ . For  $D \otimes_k D^{\text{opp}} \cong \text{End}_k(D)$ .

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

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

$$\operatorname{Br}(k) \cong H^{2}(\operatorname{Gal}(k^{\operatorname{sep}}, k), (k^{\operatorname{sep}})^{\times})$$

$$\downarrow \qquad \qquad \qquad \downarrow$$

$$\operatorname{Br}(L, k) \cong H^{2}(\operatorname{Gal}(L, k), k^{\times})$$

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

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

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

Jeff Achter 30 Ching-Li Chai

<sup>&</sup>lt;sup>9</sup>Check this.

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

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

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

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

$$1 \longrightarrow K^{\times} \longrightarrow GL_n(K) \longrightarrow PGL_n(K) \longrightarrow 1$$
$$0 \longrightarrow H^1(Gal(K, k), PGL_n(K)) \stackrel{\cong}{\longrightarrow} H^2(Gal(K, k), K^{\times})$$

Now, take L/K a cyclic extension of order n. Insist that K is a complete discrete valuation ring, with finite residue field. Let  $G = \operatorname{Gal}(L, K)$ . Then  $\widehat{H}^{\bullet}(G, L^{\times}) = \widehat{H}^{\bullet+2}(G, L^{\times})$ ; cyclic of order 2. And  $\widehat{H}^{\operatorname{odd}}(G, L^{\times}) = 0$ , 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  $\widehat{H}^{\bullet}(\operatorname{Gal}(L,K),L)$ . The normal basis theorem says that L=K[G]. So this cohomology of this is zero.

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

Want to compute the Herbrand quotient. We know that  $h(L^{\times}) = h(\mathbf{Z}) \cdot h(\mathcal{O}_{L}^{\times})$ .  $h(\mathbf{Z}) = n$ . 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  $h(\Lambda) = 1$ .

Jeff Achter 31 Ching-Li Chai

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

The valuation map gives us

$$1 \longrightarrow \mathcal{O}_L^{\times} \longrightarrow L^{\times} \longrightarrow Z \longrightarrow 1$$
$$h(G, \mathbf{Z}) = n$$

**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  $\Lambda \cdot \Lambda \subseteq \Lambda$ .<sup>11</sup> 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,

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

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

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

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

Jeff Achter 32 Ching-Li Chai

 $<sup>\</sup>overline{}^{10}$ If the residue field is finite, this just means U is of finite index.

<sup>&</sup>lt;sup>11</sup>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,  $H^2(\text{Gal}(L,K),L^{\times}) \cong n^{-1}\mathbf{Z}/\mathbf{Z}$  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  $H^2(\text{Gal}(K^{\text{sep}},K),(K^{\text{sep}})^{\times}) \cong \mathbb{Q}/\mathbb{Z}$ . Using the finite version, by Tate's theorem we see that

$$\widehat{H}^i(\operatorname{Gal}(L,K),\mathbf{Z}) \xrightarrow{U_{L,K} \cup} \widehat{H}^{i+2}(\operatorname{Gal}(L,K),L^{\times})$$

Take i = -2. This then says that

$$\operatorname{Gal}(L,K)^{\operatorname{ab}} \xrightarrow{\cong} \frac{K^{\times}}{\operatorname{rec}_{L,K}} \frac{K^{\times}}{N_{L,K}(L^{\times})}$$

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

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

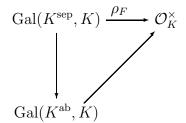
In particular, every open subgroup U of finite index in  $K^{\times}$  which contains a norm subgroup corresponds to an abelian extension of K.

**Lubin-Tate formal groups** We'll construct a commutative one-dimensional formal group F over  $\mathcal{O}_K$  with  $\mathcal{O}_K \hookrightarrow \operatorname{End}_{\mathcal{O}_K}(F)$ . 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,  $F[\pi_K^n](\overline{K}) = F[\pi_K^n](K^{\operatorname{sep}})$  a finite set; and the group law gives you a group structure.

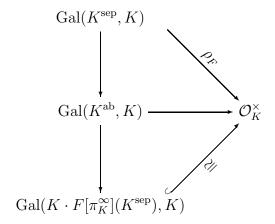
Can think of the inductive limit  $\lim_{\to} F[\pi_K^n](\overline{K})$ , an  $\mathcal{O}_K$ -module. And it will turn out that this is  $\cong K/\mathcal{O}_K$ , again as an  $\mathcal{O}_K$ -module. And  $\operatorname{End}_{\mathcal{O}_K}(K/\mathcal{O}_K) = \mathcal{O}_K$ .

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

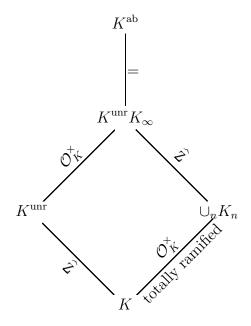
Jeff Achter 33 Ching-Li Chai



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



[Later on we'll see why this is an isomorphism.] Let  $K_n = F[\pi_K^n](\overline{k})$ . The big picture is this.



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

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  $\operatorname{Spf} R[\![x]\!] \times_{\operatorname{Spec} R} \operatorname{Spf} R[\![x]\!] \to \operatorname{Spf} R[\![x]\!]$ . The left-hand side is, essentially,  $\operatorname{Spf} R[\![x,y]\!]$ . So we have

$$\operatorname{Spf} R[\![x]\!] \times_{\operatorname{Spec} R} \operatorname{Spf} R[\![x]\!] \longrightarrow \operatorname{Spf} R[\![x]\!]$$

$$\operatorname{Spf} R[\![x,y]\!]$$

$$R[\![x,y]\!] \ni F(x,y) \longleftarrow x$$

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

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

Jeff Achter 35 Ching-Li Chai

```
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 mod 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  $F \stackrel{\alpha}{\to} G$ . This means that  $G(\alpha(x), \alpha(y)) = \alpha(F(x, y))$ . So  $\alpha$  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  $\mathfrak{F}_{\pi} = \{f(x) \in \mathcal{O}_K[\![x]\!] : f(x) \equiv \pi_K x \mod \deg 2, f(x) \equiv x^q \mod \pi_K \}$ , where  $q = p^f$  is the cardinality of the residue field  $\kappa$ . Take  $f(x) \in \mathfrak{F}_{\pi}$ . To first order, it looks like multiplication by  $\pi$ . Want f(x) to be an endomorphism of a 1-dimensional commutative formal group law  $\mathfrak{F}_f$ .

Jeff Achter 36 Ching-Li Chai

<sup>&</sup>lt;sup>12</sup>Looks like this comes from property one.

Still on Lubin-Tate groups and formal complex multiplication.<sup>13</sup> We've got  $\mathcal{O}_K$  a complete discrete valuation ring, with finite residue field  $\kappa = \mathcal{O}_K/\pi_K\mathcal{O}_K \cong \mathbb{F}_q$ . Set  $\mathfrak{F}_q = \{f \in \mathcal{O}_K[\![x]\!]: f(x) \equiv \pi x \mod \deg 2; f(x) \equiv x^q \mod \pi\}$ . 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  $\pi$ .

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

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

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

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

$$f(\phi_{r+1}(x_1, \dots, x_n)) = \phi_{r+1}(g(x_1), \dots, g(x_n)) \equiv f(\phi_r(x_1, \dots, x_n)) + \pi E_{r+1}(\underline{x}) - \phi_r(g(x_1), \dots, g(x_n)) - E_r(g(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi E_{r+1}(x_1, \dots x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_{r+1}(x_1, \dots x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) + \pi (1 - \pi^r) E_r(x_n) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) = f(\phi_r(x_1, \dots, x_n)) - \phi_r(g(x_1), \dots, g(x_n)) = f(\phi_r(x_1, \dots, x_n)) - f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x_1, \dots, x_n)) - f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x_1, \dots, x_n)) - f(\phi_r(x_1, \dots, x_n)) = f(\phi_r(x$$

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

$$f(\phi_r(x_1, \dots, x_n) - \phi_r(g(x_1), \dots, g(x_n)) \equiv \phi_r(x_1^q, \dots, x_n^q) - \phi_r(x_1^q, \dots, x_n^q) \mod \pi$$
$$\equiv 0 \mod \pi$$

 $\Diamond$ 

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

Jeff Achter 37 Ching-Li Chai

<sup>&</sup>lt;sup>13</sup>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  $F(x,y) \equiv x + y \mod \deg 2$ .

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)),  $h(x) \equiv \text{mod deg } 2$ , 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  $G_i(x, y, z) \equiv x + y + z \mod \deg 2$ . 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  $[a]_f(x) \equiv ax \mod \deg 2$ . 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  $G_i(x, y) = ax + ay \mod \deg 2$ , 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  $\psi_{f,g}(x) \equiv x \mod \deg 2$ , 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 endomorphisms b  $\mathcal{O}_K$ , and we want  $F_g \stackrel{\psi_{f,g}}{\to} F_f$ .

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

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

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  $G_i(x,y) \equiv x+y \mod \deg 2$ .

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

•  $[a_1]_f([a_2]_f(x)) = [a_1a_2]_f(x)$  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;  $\mathcal{O}_K \hookrightarrow \operatorname{End}(F_f)$ . Let  $a \in \mathcal{O}_K$ . Then  $\ker([a]_f) = \operatorname{Spec} \frac{\mathcal{O}[\![x]\!]}{[a]_f(x)\mathcal{O}[\![x]\!]}$ ), 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  $\pi$ , 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  $f(x) = \pi x + x^q$ . Then  $[\pi^n]_f(x) = f \circ \cdots \circ f(x) = f_n(x)$ . And

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

 $\ker[\pi^n] - \ker[\pi^{n-1}]$  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  $\equiv x^{q^{n-1}(q-1)} \mod \pi$ .

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.

Jeff Achter 39 Ching-Li Chai

<sup>&</sup>lt;sup>14</sup>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  $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong \mathbb{F}_q$ . 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;  $\mathcal{O}_K \hookrightarrow \operatorname{End}(F_f)$ . 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  $\operatorname{Gal}(K_{\pi,n},K)$  will turn out to be an abelian extension, so that  $\operatorname{Gal}(K^{\operatorname{sep}},K) \hookrightarrow \operatorname{Gal}(K_{\pi,n},K) \to \operatorname{Aut}(\ker[\pi^n]_f(\overline{K}))$ . In the limit version, one has

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

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

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

The conclusion is that  $\lim_{\to} \ker[\pi^{n+1}]_f$  is  $\pi$ -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  $\kappa$ . 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,

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

Furthermore,

Jeff Achter 40 Ching-Li Chai

 $<sup>^{-15}</sup>$ In doing this stuff we make use of the following; if A an abelian group, and B ( A, then A-B generates the whole thing.

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

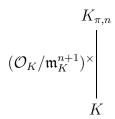
$$\operatorname{Gal}(K_{\pi,n}, K) \stackrel{\cong}{\hookrightarrow} \operatorname{Aut}_{\mathcal{O}_K}(\ker[\pi^n](\overline{K}))$$

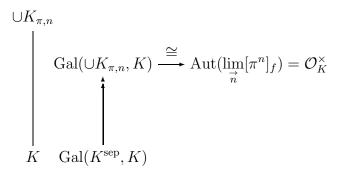
$$\cong$$

$$\operatorname{Gal}(K^{\operatorname{sep}}, K) \qquad \left(\frac{\mathcal{O}_K}{\pi^n \mathcal{O}_K}\right)^{\times}$$

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

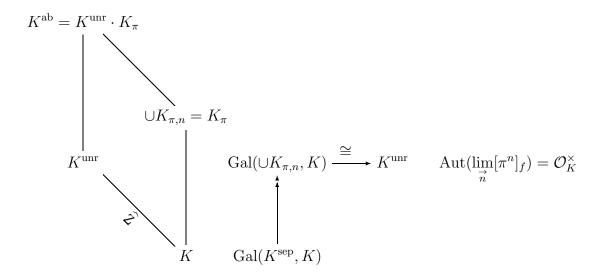
We thus have the following diagram of fields and Galois groups.





We've explicitly constructed this nice, abelian extension.

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



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

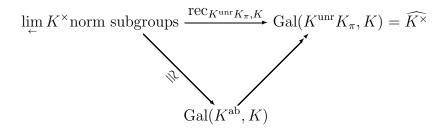
Since the  $f_{(n)}$ 's are Eisenstein polynomials,  $K_{\pi}$  is totally ramified, and as such is disjoint from  $K^{\text{unr}}$ . I think.

Write

$$f_{(n)}/f_{(n-1)} = \prod_{i} (x - a_i)$$

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  $\pi$  is always the norm.

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



Jeff Achter 42 Ching-Li Chai

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,

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

This is an explicit construction of the maximal abelian extension.

Let's backrack a bit. We picked  $\pi$ , a uniformizer. Suppose  $\varpi$  is another uniformizer.  $K_{\pi}$  and  $K_{\varpi}$  are different, and there's not a hell of a lot you can do about it.

Example time? Consider  $Q_p$ . 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,  $G_m$ . 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  $(1+x)^p - 1 = px + {p \choose 2}x^2 + \cdots + px^{p-1} + x^p$ . Choosing this f fixes the group. Every formal group is entitled to multiplication by  $Z_p$ . <sup>16</sup>

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



Let's compute the reciprocity law. Think of the global situation  $Q(\zeta_{p^n})$  over Q. This Galois group is  $(Z/p^nZ)^{\times}$ ; and ditto for the local case, actually. The reciprocity law is, take an element of  $Q_p \times$  and have it operate on the extension.[?] Let  $a \in Q_p^{\times}$ . Want to find its reciprocity law image. Well, write  $a = p^m u$ ,  $u \in Z_p^{\times}$ . Now,  $u \equiv \frac{c}{d} \mod p^N$  for some really big N, with c, d relatively prime and prime to c. Then  $\operatorname{rec}_p(a) = \operatorname{rec}_a(p^m \frac{c}{d})$ . Now a leap of faith; local and global reciprocity laws are compatible. And if we take a global element in 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

$$\operatorname{rec}_{p}(a) = \operatorname{rec}_{p}(p^{m}\frac{c}{d})$$
$$= (\prod_{l \neq p} \operatorname{rec}_{l}(p^{m}\frac{c}{d}))^{-1}$$

Jeff Achter 43 Ching-Li Chai

<sup>&</sup>lt;sup>16</sup>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  $\operatorname{rec}_p(a) = u^{-1} \in (\mathbf{Z}/p^n\mathbf{Z})^{\times}$ .

Jeff Achter 44 Ching-Li Chai

No class on Wednesday.[!]

We've got  $\mathcal{O}_K$  a complete DVR, and  $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong F_q$ . 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  $K_{\pi} = \bigcup_n K_{\pi,n}$ . Then  $K_{\pi}/K$  is abelian, with group  $\mathcal{O}_K^{\times}$ . On the other hand, we know that we can construct the maximal unramified extension  $K^{\text{unr}}$ , with group  $\widehat{Z}$ . And then  $K_{\pi}K^{\text{unr}}$  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 Gal(L, K) = G. We'll try to understand it via the dual.

$$H^{-2}(G,\mathbf{Z}) \xrightarrow{\cong} H^{0}(G,L^{\times})$$

$$G^{ab} \qquad K^{\times}/N_{L,K}(L^{\times})$$

$$\operatorname{rec}_{L,K}(\overline{a}) \longleftarrow \overline{a}$$

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

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

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

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

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

Jeff Achter 45 Ching-Li Chai

 $\chi(s_a) = \frac{i}{n} \mod Z$ ; I mean, what else could it be? Now we have to take  $\delta$  of that, to wind up in  $H^0(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ . Then  $\delta(s_a \cup \chi) = i \mod n$ . 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**  $\chi(\operatorname{rec}_{L,K}(\overline{a})) = \operatorname{inv}_K(a \cup \delta \chi).$ 

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  $s_a = \operatorname{Fr}_K$  raised to some power, namely, the valuation of  $s_a$ .

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

$$\chi(s_a) = \operatorname{inv}_K(\delta\chi \cup \overline{a})$$

$$\stackrel{?}{=} \frac{v_K(a)}{n} \operatorname{mod} Z.$$

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

$$H^{2}(G, L^{\times}) \xrightarrow{v_{L}} H^{2}(G, \mathbf{Z}) \xleftarrow{\cong} H^{1}(G, \mathbf{Q}/\mathbf{Z})$$

$$\downarrow \qquad \qquad \downarrow$$

$$H^{2}(G, \mathbf{Z}) \times H^{0}(G, L^{\times}) \xrightarrow{\operatorname{id} \times v_{L}} H^{2}(G, \mathbf{Z}) \times H^{0}(G, \mathbf{Z})$$

$$\delta \chi \cup \overline{a} \longmapsto v_{K}(a) \delta \chi \longleftarrow v_{k}(a) \chi$$

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

$$\chi(a) = \operatorname{inv}_K(\delta \chi \cup \overline{a}) = \frac{v_K(a)}{n} \mod Z.$$

Jeff Achter 46 Ching-Li Chai

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

Now,  $\pi$  operates trivially on  $K_{\pi}$ . More precisely,  $\operatorname{rec}_K(\pi)$  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  $K^{\operatorname{unr}}$ .

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

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

$$\operatorname{Gal}(K^{\operatorname{ab}}, K) \longrightarrow \operatorname{Gal}(K_{\pi}, K) \times \operatorname{Gal}(K^{\operatorname{unr}}, K)$$

$$\mathcal{O}_{K}^{\times} \times \widehat{\mathbf{Z}}$$

$$\pi^{n} \cdot u \longmapsto (u^{-1}, n)$$

And this will follow from:

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

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

So let's go prove that stuff.

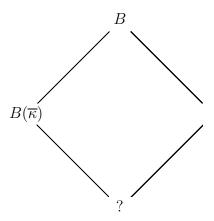
**Lemma** Choose  $\pi$ ,  $\varpi$  two uniformizers,  $f \in \mathfrak{F}_{\pi}$ ,  $g \in \mathfrak{F}_{\varpi}$ . These correspond to formal laws  $F_f$  and  $F_g$ . Let  $A = \widehat{\mathcal{O}_{K^{\mathrm{unr}}}}$ .

- 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  $\sigma = \operatorname{Fr}_q$ . In other words,  $\theta\sigma(x) = \theta([u]_f(x))$ .

Jeff Achter 47 Ching-Li Chai

 $K \supseteq \mathcal{O}_K$  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  $f \in \mathfrak{F}_{\pi} \cdot F_f$ , and  $g \in \mathfrak{F}_{\varpi} \cdot F_g$ . They're not isomorphise [necessarily] over  $\mathcal{O}_K$ .

Let A be the Witt vectors  $A = W(\overline{\kappa})\mathcal{O}_K$ , and  $B = \operatorname{Frac} A = B(\overline{\kappa})K = \widehat{K}^{\operatorname{unr}}$ . 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.



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

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

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

where  $\sigma$  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

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

Jeff Achter 48 Ching-Li Chai

Now, before we had

$$K^{\times} \xrightarrow{r_{\pi}} \operatorname{Gal}(K^{\operatorname{unr}}K_f, K)$$

$$\cong \theta$$

$$K^{\times} \xrightarrow{r_{\varpi}} \operatorname{Gal}(K^{\operatorname{unr}}K_g, K)$$

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

$$r_{\pi}(\varpi)\theta(x) = \theta^{\sigma}(r_{\pi}(\varpi)x)$$

$$= \theta^{\sigma}(r_{\pi}(u)r_{\pi}(\pi)x)$$

$$= \theta^{\sigma}(r_{\pi}(u)x)$$

$$= \theta^{\sigma}([u^{-1}]_{f}(x))$$

$$= \theta([u]_{f}[u^{-1}]_{f}x)$$

$$= \theta(x).$$

Thus,  $r_{\pi}(\varpi)$  operates trivially on  $K_g$ . So now we know  $r_{\pi}(\varpi) = r_{\varpi}(\varpi)$ . For  $v \in \mathcal{O}_K^{\times}$ ,

$$r_{\pi}(v)\theta(x) \stackrel{?}{=} r_{\varpi}(v)\theta(x)$$

$$r_{\pi}(v)\theta(x) = \theta(r_{\pi}(v)x)$$

$$= \theta([v^{-1}]_{f}(x))$$

$$r_{\varpi}(v)\theta(x) = [v^{-1}]_{g}(\theta(x)).$$

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

Jeff Achter 49 Ching-Li Chai

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

$$\theta^{-1} \circ \theta^{\sigma} \circ f \in \operatorname{End}(F_f)$$
  
 $\theta^{-1}g\theta \in \operatorname{End}(F_f)$ 

Look at them modulo  $\pi$ . The second one is

$$\theta^{-1}g\theta(x) \equiv \theta^{-1}(\theta(x))^q \mod \pi$$
$$\equiv \theta^{-1}\theta^{\sigma}(x^q)$$
$$\equiv \theta^{-1}\theta^{\sigma}f(x).$$

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  $\theta$  coefficient by coefficient, satisfying  $\theta(x) \equiv \epsilon x \mod \deg 2$  and  $\theta^{\sigma} = \theta \circ [u]_f$ . There's a condition on  $\epsilon$ . Well,  $\theta^{\sigma}(x) \equiv \epsilon^{\sigma} x \mod \deg 2$ ; 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  $e^{\sigma}e^{-1} = u$  as a statement on Galois cohomology.<sup>17</sup>

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

$$\begin{array}{rcl} \theta^{\sigma}_{r}(x) & \equiv & \theta^{\sigma}_{r-1}(x) + b^{\sigma}_{r}x^{r} \bmod \deg r + 1 \\ \theta_{r} \circ [u]_{f}(x) & = & \theta_{r-1} \circ [u]_{f}(x) + b_{r}(u_{f}(x))^{r} \\ & = & \theta_{r-1} \circ [u]_{f}(x) + b_{r}u^{r}x^{r} \\ \theta^{\sigma}_{r-1}(x) - \theta_{r-1} \circ [u]_{f}(x) & = & c_{r}x^{r} \\ b^{\sigma}_{r} + c_{r} & = & b_{r}u^{r} \end{array}$$

Jeff Achter 50 Ching-Li Chai

Thint:  $\sigma$  is the topological generator of  $K^{\text{unr}}$ . 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  $\kappa = \mathcal{O}_K/\mathfrak{m}_K \cong F_q$ ,  $A = \mathcal{O}_{\widehat{K}^{\mathrm{unr}}}$ ,  $F = \sigma = \mathrm{Fr}_K = \mathrm{Fr}_q$ . 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  $A^{\times} = \lim_{\overline{h}} (A/\pi^n A)^{\times}$ , and  $A = \lim_{\overline{h}} (A/\pi^n A)$ . It suffices to show that, on each associated graded level, this is surjective. Hmm. The ground level of the filtration is  $\overline{\kappa}^{\times} \stackrel{\sigma^{-1}}{\to} \overline{\kappa}^{\times}$ . In general, fil<sup>n</sup> =  $(1 + \pi^n A)^{\times}$ , and fil<sup>n</sup> / fil<sup>n+1</sup>  $\cong \overline{\kappa}$ , and this behaves nicely with respect to the Galois group. So on each graded piece we get either  $\overline{\kappa}^{\times} \stackrel{\sigma^{-1}}{\to} \overline{\kappa}^{\times}$  or  $\overline{\kappa} \stackrel{\sigma^{-1}}{\to} \overline{\kappa}$ . We have to show that these are surjective.<sup>18</sup>

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

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

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

Jeff Achter 52 Ching-Li Chai

<sup>&</sup>lt;sup>18</sup>I think the graded thing is just  $\operatorname{fil}^{i}/\operatorname{fil}^{i+1}$ .

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

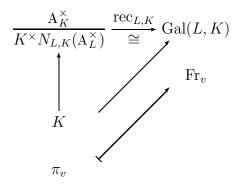
Global Class Field Theory What is class field theory, anyway? It has a few goals.

- Understand/describe abelian extensions, possibly in terms of the arithmetic of the base field, K. F'rinstance, stuff involving  $K^{\times}$  or  $A_K^{\times}/K^{\times}$ .
- 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,  $\operatorname{Fr}_v \in G^{\flat} \ni \langle g \rangle$ , the conjugacy clases of G. Then density of  $\{v : \operatorname{Fr}_v \in \langle g \rangle\}$  is  $\frac{1}{\operatorname{Card}(G^{\flat})}$ . Furthermore,  $\{v \in \Sigma_K : \operatorname{Fr}_v = e\}$ , which is just the set of [totally] split primes, completely determines L.
- Ultimately, we're interested in  $Gal(K^{sep}, K)$ . And apparently, these days one dualizes the problem and attempts to describe the representations  $Gal(K^{sep}, K) \to GL_n(Q_l)$ .

Main theorem of global class field theory:

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

## 1. There's a map



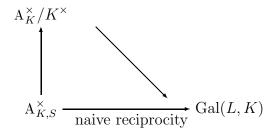
for v an unramified prime,  $v \in \Sigma_K$ ; and this gives a map from the group of unramified ideals  $I^{\text{unr}}$  to Gal(L, K).

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

Jeff Achter 53 Ching-Li Chai

**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  $\operatorname{rec}_{L,K}$ , 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  $|x-1|_v \leq a_v$ ,  $\prod_{v \notin S} \operatorname{Fr}_v^{v(x)} = e \in \operatorname{Gal}(L,K)$ . Exercise to verify that this is really equivalent.



Recall  $A_{K,S}^{\times} = \prod_{v \notin S}' K_v^{\times}$ . 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

$$\operatorname{Card}(\frac{\mathbf{A}_K^{\times}}{K^{\times}N_{L,K}(\mathbf{A}_L^{\times})}) \ge n.$$

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;  $Gal(L, K) \cong \mathbb{Z}/n\mathbb{Z}$ . Want to say something about  $\widehat{H}^0(G, A_L^{\times}/L^{\times})$ . Well,

Jeff Achter 54 Ching-Li Chai

$$\widehat{H}^{0}(G, \mathbf{A}_{L}^{\times}/L^{\times}) = (\mathbf{A}_{L}^{\times}/L^{\times})^{G}/N_{L,K}(\mathbf{A}_{L}^{\times}/L^{\times})$$
$$= \mathbf{A}_{K}^{\times}/K^{\times}N_{L,K}(\mathbf{A}_{L}^{\times})$$

In the second line, we used Hilbert 90 to get

$$(\mathbf{A}_{L}^{\times})^{G}/(L^{\times})^{G} \cong (\mathbf{A}_{L}^{\times}/L^{\times})^{G}$$

$$(L^{\times})^{G} = K^{\times}$$

$$\mathbf{A}_{L}^{\times} = \lim_{\substack{\Sigma_{K}^{\infty} \subseteq S \subseteq \Sigma_{K} \\ \Sigma_{K}^{\infty} \subseteq S \subseteq \Sigma_{K}}} (\prod_{w|v \notin S} \mathcal{O}_{w}^{\times}) \times (\prod_{w|v \in S} L_{v}^{\times})$$

$$(\mathbf{A}_{L}^{\times})^{G} = \lim_{\substack{\Sigma_{K}^{\infty} \subseteq S \subseteq \Sigma_{K} \\ \Sigma_{K}^{\infty} \subseteq S \subseteq \Sigma_{K}}} ((\prod_{w|v \notin S} \mathcal{O}_{w}^{\times}) \times (\prod_{w|v \in S} L_{v}^{\times}))^{G}$$

$$= \lim_{\substack{\Sigma_{K}^{\infty} \subseteq S \subseteq \Sigma_{K} \\ \Sigma_{K}^{\infty} \subseteq S}} (\prod_{w|v \notin S} \mathcal{O}_{v}^{\times}) \times \prod_{e \in S} K_{v}^{\times}$$

$$= \mathbf{A}_{K}^{\times}$$

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

Now, you'd expect to get a map  $\widehat{H}^0(G, \Lambda_L^{\times}/L^{\times}) \leftarrow \widehat{H}^{-2}(G, \mathbf{Z})$ , 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  $h(G, A_L^{\times}/L^{\times}) = n$ .

Jeff Achter 55 Ching-Li Chai

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

**Theorem** [First inequality]

$$\operatorname{Card}(\frac{\mathbf{A}_K^{\times}}{K^{\times} N_{L,K}(\mathbf{A}_L^{\times})}) \ge n.$$

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

$$\mathbf{A}_{L}^{\times}/L^{\times} \stackrel{\cong}{\longleftarrow} \mathbf{A}_{LS}^{\times}/L_{S}^{\times}$$

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

$$H^{0}(\prod_{w|v} L_{w}^{\times}) = K_{v}^{\times}$$

$$H^{0}(\prod_{w|v} \mathcal{O}_{w}^{\times}) = \mathcal{O}_{v}^{\times}$$

$$\widehat{H}^{0}(\prod_{w|v} \mathcal{O}_{w}^{\times}) = 0 \text{ for } v \notin S$$

$$\widehat{H}^{0}(G, \mathbf{A}_{L,S}^{\times}) = \prod_{v \in S} \widehat{H}^{0}(G_{w}, L_{w}^{\times})$$

$$= \prod \frac{K_{v}^{\times}}{N_{w,v}(L_{w}^{\times})}$$
for  $v \notin S$ ,
$$H^{1}(G, \prod_{w|v} \mathcal{O}_{w}^{\times}) = H^{1}(G_{w}, \mathcal{O}_{w}^{\times}) \text{ Shapiro's lemma}$$

$$= 0$$

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.

Jeff Achter 56 Ching-Li Chai

<sup>&</sup>lt;sup>19</sup>Recall that this is  $A_{L,S}^{\times} = (\prod_{w|v \in S} L_w^{\times}) \times \prod_{w|v \notin S} \mathcal{O}_w^{\times}$ , since S contains all archimedean places.

Conclusion of all this is that  $h(G, A_{L,S}^{\times}) = \prod_{v \in S} h(G_w, L_w^{\times}) = \prod_{v \in S} [L_w : K_v]^{20}$ Now, what about  $h(G, L_S)^{\times}$ ? We need the log map:

$$1 \longrightarrow \mu_L \longrightarrow L_S^{\times} \xrightarrow{\log} (\prod_{w|v \in S} R_w)^1 \longrightarrow \text{real torus} \longrightarrow 1$$
$$l \longmapsto (\log ||l||_w)_{w|v \in S}$$

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

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

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

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

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

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  $\Gamma$ .

We know that  $\Gamma \otimes_{\mathbb{Z}} R \cong \Gamma' \otimes_{\mathbb{Z}} R$  *G*-equivariantly. Then we can thus conclude that  $\Gamma \otimes_{\mathbb{Z}} Q \cong \Gamma' \otimes_{\mathbb{Z}} Q$ , *G*-equivariantly as well. That's an easy algebra fact; figure it out if you don't see it.<sup>21</sup> But once these two representations are isomorphic over Q, we can 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,  $h(G, \mathbf{A}_L^{\times}/L^{\times}) = n. \diamondsuit$ 

Jeff Achter 57 Ching-Li Chai

<sup>&</sup>lt;sup>20</sup>By the way, a lot of times I'm just picking some w lying over v; it doesn't really matter which one.

 $<sup>^{21}</sup>$ Briefly, G-equivariant homomorphisms are a findim Q vector space. Tensoring with 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  $K^{\times}N_{L',K}(A_{L'}^{\times}) = A_K^{\times}$ . 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

$$1 \longrightarrow \mu_n(\overline{K}) \longrightarrow K^{\text{sep}\times} \stackrel{n}{\longrightarrow} K^{\text{sep}\times} \qquad 1$$

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

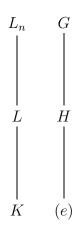
$$1 \longrightarrow K^{\times}/(K^{\times})^{n} \longrightarrow \operatorname{Hom}(G, \mu_{n}) \longrightarrow 1$$
$$\operatorname{Hom}(G^{\operatorname{ab}}/(G^{\operatorname{ab}})^{n}, \mu_{n})$$

[exact on right from Hilbert 90.] In some sense,  $\operatorname{Hom}(G^{\operatorname{ab}}/(G^{\operatorname{ab}})^n, \mu_n)$  is the dual of  $G^{\operatorname{ab}}/(G^{\operatorname{ab}})^n$ . Anyways, how do we write down this isomorphism? It comes down to the connecting  $\delta$  thing. Let  $k \in K^{\times} = H^0(G, K^{\operatorname{sep}\times})$ . Pick  $\sqrt[n]{k} \in K^{\operatorname{sep}\times}$ ; 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  $K(n) = \operatorname{Gal}(K^{\operatorname{sep}}, K)^{\operatorname{ab}}/\operatorname{Gal}(K^{\operatorname{sep}}, K)^n$ . For next time – Friday, actually – think about  $K(n) \supseteq L \supseteq K$ . Figure out which things kill L. Let  $H = \operatorname{Gal}(K(n), L)$ . Consider all characters of G killing H. That's a subgroup of  $\operatorname{Hom}(G, \mu_n)$ , , and therefore corresponds to a subgroup of  $K^{\times}/K^{\times n}$ . How do we explicitly relate this to L?

Jeff Achter 58 Ching-Li Chai

We've got a tower of fields and Galois groups



Here, we have

$$G = \operatorname{Gal}(L_n, K)$$

$$= \frac{\operatorname{Gal}(K^{\operatorname{sep}}, K)^{\operatorname{ab}}}{\operatorname{Gal}(K^{\operatorname{sep}}, K)^n}$$

$$= \operatorname{Hom}(K^{\times}/(K^{\times})^n, \mu_n)$$

$$H = \{\sigma \in G : \sigma|_L = \operatorname{id}\}$$

$$= \operatorname{Hom}(\frac{K^{\times}}{(K^{\times})^n \cdot ?}, \mu_n)$$

$$? = \{a \in K^{\times} : \forall \sigma \in \operatorname{Gal}(L_n, L) k \sqrt[n]{a}^{\sigma-1} = 1\}$$

$$= \{a \in K^{\times} : \sqrt[n]{a} \in L\}$$

$$= K^{\times} \cap (L^{\times})^n$$

$$H = \operatorname{Hom}(\frac{K^{\times}}{(L^{\times})^n \cap K^{\times}}, \mu_n)$$

So,

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

In particular,

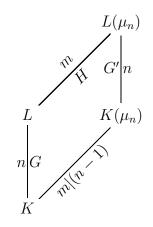
$$[L:K] = [(L^\times)^n \cap K^\times : (K^\times)^n].$$

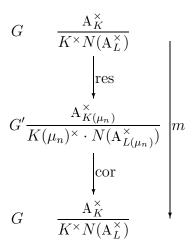
Move it on.

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

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

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;  $\mu_n(\overline{K}) \subset K$ .



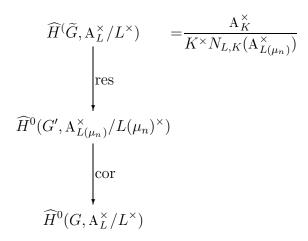


In this case, corestriction is essentially just the norm; and the composition is multiplication by m.

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

## abort

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



The composition might be multiplication by m.

## abort

the second map of groups induces the first one.

$$\widehat{H}^{0}(\widetilde{G}, \mathcal{A}_{L(\mu_{n})}^{\times}/L^{\times}) \xrightarrow{\qquad} \frac{\mathcal{A}_{K}^{\times}}{K^{\times}N(\mathcal{A}_{L}^{\times})}$$

$$\downarrow^{\text{res}} \qquad \qquad \downarrow^{\text{res}}$$

$$\widehat{H}^{0}(G', \mathcal{A}_{L(\mu_{n})}^{\times}/L(\mu_{n})^{\times}) \xrightarrow{\qquad} \frac{\mathcal{A}_{K(\mu_{n})}^{\times}}{K(\mu_{n})^{\times} \cdot N(\mathcal{A}_{L(\mu_{n})}^{\times})}$$

$$\downarrow^{\text{cor}} \qquad \qquad \downarrow^{\text{cor}}$$

$$\widehat{H}^{0}(\widetilde{G}, \mathcal{A}_{L(\mu_{n})}^{\times}/L^{\times}) \xrightarrow{\qquad} \frac{\mathcal{A}_{K}^{\times}}{K^{\times}N(\mathcal{A}_{L}^{\times})}$$

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

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

Jeff Achter 61 Ching-Li Chai

Now, assume that  $Gal(L, K) = G \cong (\mathbb{Z}/n\mathbb{Z})^r$ , 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  $K^{\times}A_{K,S}^{\times} = A_K^{\times}$ . 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?

$$K_S^{\times} = K^{\times} \cap A_{K,S}^{\times}.$$

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

So,  $M \supset L \supset K$ . There are  $w_1, \dots, w_t$  unramified places of L, disjoint from S, such that the Frobenii  $F_{w_i}$  generate  $\operatorname{Gal}(M, L)$ . 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,  $[{}^{\times}A_{K,S}^{\times}:K^{\times}N] \leq n$ . But this index is just

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

Jeff Achter 62 Ching-Li Chai

Notes from Kate. Thanks.

We want to show:

- 1. For all  $a \in K^{\times}$ ,  $\prod_{v} rec_{v}(a) = 1$ .
- 2. We just explained that for all  $x \in Br(K)$ , if we localize we get an element in  $Br(K_v)$ , namely,  $inv_v(x)$ . We want to show  $\sum_v inv_v(x) = 0$ .

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  $x_v \in \text{Hom}(G_v, \mathbf{Q}/\mathbf{Z}) \cong H^1(G_v, \mathbf{Q}/\mathbf{Z})$  [since the action is trivial]. But by the coboundary map there's an isomorphism

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

Then for all  $a_v \in K_v^{\times}$ ,  $\operatorname{rec}_v(a_v) \in G_v$ , so we can evaluate  $\chi_v$  on it;  $\chi_v(\operatorname{rec}_v(a_v))$  makes sense. But this is also an element  $\operatorname{inv}_v(\cdot)$ , 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  $\chi_v(\operatorname{rec}_v(a_v)) = \operatorname{inv}_v(\overline{a_v} \cup \delta \chi)$ .

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

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

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

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

- What's  $\prod_v \operatorname{rec}_v(-1)$ ? A few cases to worry about.
- $v = \infty$  Then C/Q depends on R/N<sub>C,R</sub>(C); -1 isn't a norm because norms have to be positive. Then  $rec_v(-1) = i = -1$ ; the complex onjugate is its own inverse.
- $v = p \neq l$  Then we have  $Q(l^n)_p$  over  $Q_p$ . And  $p \neq l$  means we're unramified; -1 is a unit[?]. So  $rec_v(-1) = 1$ .
- v = p = l Well, -1 is a unit. And  $rec_v(unit) = \frac{1}{unit}$ , by the formal group law stuff. So  $rec_v(-1) = -1$ .

Then  $\prod_{v} rec_{v}(-1) = -1 \cdot 1 \cdot -1 = 1$ .

Jeff Achter 63 Ching-Li Chai

•  $\prod_v \operatorname{rec}_v(n)$  for nnot = l. As we'll see shortly,

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

Given this, it's clear that  $\prod_{v} rec_v(n) = 1$ .

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  $\Rightarrow \operatorname{rec}_v(n)$  operates trivially if  $n \neq p$ , and  $\operatorname{Zrec}_v(n) = n$  if n = p.

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

• Look at n = l. Then

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

From all of this nonsense it follows that  $\prod_v \operatorname{rec}_v(a) = 1$ ; 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  $x \in Br(L/K)$ , then  $x = a \cup \delta \chi$  for some  $a \in K^{\times}/N(L^{\times})$  and  $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ .

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

$$\sum_{v} inv_{v}(x) = \sum_{v} inv_{v}(a \cup \delta\chi)$$
from above 
$$= \sum_{v} \chi_{v}(rec_{v}(a))$$

$$= \chi(\sum_{v} rec_{v}(a))$$

$$= \chi(0)$$

$$= 0.$$

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

<sup>&</sup>lt;sup>22</sup>Think of this as an element of  $H^2(G_v, \mathbb{Z})$ 

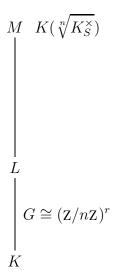
**Claim** There' some cyclotomic and cyclic extension L over K which splits x, and thus  $x \in Br(L, K)$ .

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

Jeff Achter 65 Ching-Li Chai

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



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  $\operatorname{Gal}(M,KJ) \cong \operatorname{Hom}(K_S^{\times}/K_S^{\times} \cap (K^{\times})^n, \mu_n)$ . So  $[M+K] = n^s$ , since the group of homomorphisms is abstractly  $(\mathbf{Z}/n\mathbf{Z})^s$ . Then  $w_1, \dots, w_t \in \Sigma_L$ , unramified so that  $\{\operatorname{Fr}_{w_i}\}$  generates  $\operatorname{Gal}(M,L)$ . Since the decomposition groups are always cyclic,  $\operatorname{Gal}(M,K) \cong (\mathbf{Z}/n\mathbf{Z})^s$ ; we know that  $w_i$  is split over  $v_i$ . In other words, all the  $v_i$  are split. Let  $T = \{v_1, \dots, v_t\}$ .

We wanted

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

If we could show this, then we'd know the same thing for an arbitrary extension L.<sup>23</sup> Now, we'd made up some norms,

Jeff Achter 66 Ching-Li Chai

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

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

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

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

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

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

Now try to get at the Herbrand quotient.

$$h_{\text{triv}}(\mathbf{Z}/n\mathbf{Z}, K_v^{\times}) = h_{\text{triv}}(\mathbf{Z}/n\mathbf{Z}, \mathcal{O}_v^{\times}) \cdots h_{\text{triv}}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z})$$

$$= h_{\text{triv}}(\mathbf{Z}/n\mathbf{Z}, \mathcal{O}_v^{\times}) \cdot n$$

$$\text{use exp} = h_{\text{triv}}(\mathbf{Z}/n\mathbf{Z}, \mathcal{O}_v) \cdot n$$

$$= \frac{n}{|n|_v} \cdot n$$

$$[K_v^{\times} : (K_v^{\times})^n] = \frac{n^2}{|n|_v}$$

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

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

$$[\mathbf{A}_{K,S \cup T}^{\times} : N] = \prod_{v \in S} \frac{n^2}{|n|_v}$$

$$= n^{2s}$$

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

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

We know that

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

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

Recall that if  $x \in K_S^{\times}$ , and  $x \in (L_{w_i}^{\times})^n$  for all i, then  $x \in (L^{\times})^n$ . For  $\sqrt[n]{x}$  is fixed by  $\operatorname{Fr}_{w_i}$ , hence fixed by  $\operatorname{Gal}(M, L)$ , i.e.,  $\sqrt[n]{x} \in L$ .

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

Jeff Achter 68 Ching-Li Chai

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

$$M = K(\sqrt[n]{K_S^{\times}})$$

$$H \cong (\mathbf{Z}/n\mathbf{Z})^t = \{\mathrm{Fr}_{w_i}\}_{i=1,\dots,t}$$

$$w_i \qquad L$$

$$G \cong (\mathbf{Z}/n\mathbf{Z})^r$$

$$v_i \qquad K$$

Set  $T = \{v_1, \dots, v_t\}$ , 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  $F \stackrel{\text{def}}{=} K(\sqrt[n]{K^{\times} \cap N})$ ,

$$K^{\times} \cdot N_{F,K}(A_F^{\times}) = A_K^{\times}.$$

We certainly have

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

It now suffices to show

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

By our choice of S,

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

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

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

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

$$\operatorname{Card}(K_{S}^{\times}/\ker) = [M:L]$$

$$= n^{t}$$

$$\operatorname{Card}(\mathcal{O}_{v}^{\times}/(\mathcal{O}_{v}^{\times})^{n}) \stackrel{\text{Hensel's lemma}}{=} \operatorname{Card}(\kappa_{v}^{\times}/(\kappa_{v}^{\times})^{n})$$

$$\kappa_{v} \supseteq \mu_{n}(\overline{\kappa}_{v})$$

$$n \mid q_{v} - 1$$

$$\operatorname{Card}(\kappa_{v}^{\times}/(\kappa_{v}^{\times})^{n}) = n \text{ for all } v \in T$$

[Remember n is prime to the characteristic of the residue field at  $v \in T$ .] Then  $\operatorname{Card}(\prod_{v \in T} \mathcal{O}_v^{\times}/(\mathcal{O}_v^{\times})^n$ , 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  $[A_K^{\times}: K^{\times}N_{L,K}(A_L^{\times})] \leq [L:K]$ . Now,  $N \stackrel{\text{def}}{=} K^{\times}N_{L,K}(A_L^{\times})/K^{\times}$  is an open subgroup of finite index in  $A_K^{\times}/K^{\times}$ . Following an idea of Dirichlet, we want to look at characters  $\chi \in \text{Hom}(A_K^{\times}/(K^{\times} \cdot H), C_1^{\times})$ , 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  $\chi$  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  $\chi$  is trivial, then we're essentially talking about the Dedekind  $\zeta$  function of K, and it looks like  $\frac{1}{s-1} + O(1)$ .

$$L_{S}(\chi, s) = \prod_{v \notin S} (1 - \chi(\pi_{v})q_{v}^{-s})^{-1}$$

$$\log(1 - x)^{-1} = \sum_{m \geq 1} \frac{x^{m}}{m}$$

$$\log L_{S}(\chi, s) = \sum_{v \notin S} \sum_{m \geq 1} \frac{\chi(\pi_{v})^{m}q_{v}^{-ms}}{m}$$

$$\frac{d}{ds} \log L_{S}(\chi, s) = -\sum_{v \notin S} \sum_{m \geq 1} (\log q_{v})\chi(\pi_{v})^{m}q_{v}^{-ms}$$

$$\sum_{\chi} \log L_{S}(\chi, s) = -\sum_{\chi} \sum_{v \notin S} \sum_{m \geq 1} (\log q_{v})\chi(\pi_{v})^{m}q_{v}^{-ms}$$
the rest is convergent, leaving  $\sim -\sum_{\chi} \sum_{v \notin S} (\log q_{v})\chi(\pi_{v})q_{v}^{-s}$ 

Let  $h = [A_K^{\times} : K^{\times} N_{L,K}(A_L^{\times})]$ . Then we have

$$\sim \sum_{\chi} \sum_{v \notin S} (\log q_v) \chi(\pi_v) q_v^{-s}$$

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

A miracle occurs and we're done, sorry.

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.

Jeff Achter 71 Ching-Li Chai

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  $[A_K^{\times}: K^{\times}N_{L,K}A_L^{\times}]|[L:K]$ , the second inequality. When G is cyclic, we showed  $h(G, A_L^{\times}/L^{\times}) = n$ , and thus that  $n|[A_K^{\times}: K^{\times}N_{L,K}(A_L^{\times})]$ ; 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  $\operatorname{rec}: \operatorname{A}_K^\times/K^\times \to G = \operatorname{Gal}(L,K)$ , where L/K is assumed abelian. Inside this picture is  $\operatorname{rec}_v: K_v^\times \to G_v$ . For v unramified, units must go to the trivial element. Put the local ones together to give  $\operatorname{A}_K^\times \to G$ ; 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  $a \in K^{\times}$ ,  $\prod_{v} \operatorname{rec}_{v}(a) = 1$ . This implies that  $\operatorname{rec}: A_{K}^{\times}/K^{\times}N_{L,K}(A_{L}^{\times}) \rightharpoonup G$ . The second inequality shows that this is actually an isomorphism.

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

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

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

$$\operatorname{Br}(L, K) \qquad \oplus_{v} H^{2}(G_{w}, L_{w}^{\times})$$

$$\oplus_{v} \operatorname{Br}(L_{w}, K_{v})$$

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  $H^2(G, \mathbf{A}_L^{\times}/L^{\times}) \cong \frac{1}{[L:K]}\mathbf{Z}/\mathbf{Z}$ , canonically. We'll use this and Tate's theorem to show that  $\hat{H}^r(G, \mathbf{Z}) \stackrel{? \cup u_{L,K}}{\to} \hat{H}^{r+2}(G, \mathbf{A}_L^{\times}/L^{\times})$  When r = -2, we interpret this as  $G^{ab} = G \stackrel{\cong}{\to} \mathbf{A}_K^{\times}/K^{\times}N_{L,K}(\mathbf{A}_L^{\times})$ . Keep interpreting.

$$n_v \stackrel{\text{def}}{=} [L_w : K_v]$$

$$\bigoplus_v \operatorname{Br}(L_w, K_v) = \bigoplus_v \frac{1}{n_v} \mathbf{Z}/\mathbf{Z}$$

Jeff Achter 72 Ching-Li Chai

MA 620 3 April 1994

Notes from Seon-In. Thanks.

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

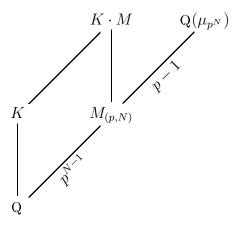
$$(*)\sum_{v} \operatorname{inv}_{v}(x) = 0 \in Q/Z$$

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

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

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  $[L_{j,w_i}; K_{v_i}] \equiv 0 \mod p_j^{e_j}$ , then we can just take  $L = \prod_j L_j$ .

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



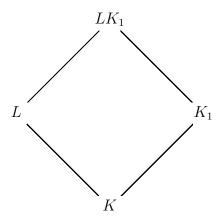
Here,  $\operatorname{Gal}(\operatorname{Q}(\mu_{p^N}), M_{(p,N)})$  is the order p-1 subgroup of  $\operatorname{Z}/p^{N_1}(p-1)$ . Then  $[K\cdot M)_{w_i}:K_i]$  is a multiple of  $\frac{[M_{p_i}:\operatorname{Q}_{p_i}]}{[K_{v_i}:\operatorname{Q}_{p_i}]}$ . The local degree at KM/K can be decreased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

So w may assume K = Q.

MA 620 3 April 1994

For simplicity's sake assume  $p \neq 2$  is a finite prime.<sup>24</sup> Let  $l_1, \dots, l_k$  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,  $\prod_v \operatorname{rec}_v(x) = 1$ . This is  $\iff$  for all  $\chi \in \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$ ,  $\sum_v \chi(\operatorname{rec}_v(x)) = 0 \mod \mathbb{Z}$ . But  $\chi(\operatorname{rec}_v(x)) = \operatorname{inv}_v(x \cdot \delta \chi)$ , where  $x \cdot \delta \chi \in \operatorname{Br}(K)$ . Given



We get a commuting diagram

$$A_{K,1}^{\times}/K_1^{\times} - - - - A_K^{\times}/K^{\times}$$

$$\downarrow \qquad \qquad \downarrow$$

$$\operatorname{Gal}(LK_1, K_1) \longrightarrow \operatorname{Gal}(L, K)$$

This gives us

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

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

 $<sup>^{24}</sup>p = \infty$  is trivial to handle.

MA 620 3 April 1994

$$A_K^{\times}/K^{\times} \longrightarrow A_{K_1}^{\times}/K_1^{\times}$$

$$x \longmapsto x$$

This corresponds to  $\operatorname{Gal}(K^{\operatorname{ab}},K) \to \operatorname{Gal}(K^{\operatorname{ab}}_1,K_1)$  by transfer. So

$$\lim_{\stackrel{\leftarrow}{L}} \frac{\mathbf{A}_K^{\times}}{K^{\times} N_{L,K}(\mathbf{A}_L^{\times})} \xrightarrow{\cong} \operatorname{Gal}(K^{\operatorname{ab}}, K)$$

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

Jeff Achter 75 Ching-Li Chai

MA 620 6 April 1994

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

We've already made it past the crux move: suppose  $A_K^{\times}/K^{\times}H \cong \mathbb{Z}/p\mathbb{Z}$  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  $K^{\times}A_{K,S}^{\times} = A_K^{\times}$ . 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

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

Of course, at this point we also know that

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

The conclusion is that

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

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  $\operatorname{nm}^{-1}(H) \subseteq \operatorname{A}_L^{\times}/L$ . 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  $H' = \operatorname{nm}^{-1}(H)$ , 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  $H' = N_{M,L}(A_M^{\times}/M^{\times})$ . Well,  $N_{M,K}(A_M^{\times}/M^{\times}) \subseteq H$ ; 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.

Jeff Achter 76 Ching-Li Chai

MA 620 6 April 1994

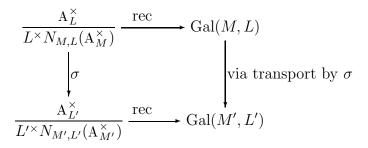
- 1. M is Galois over K. That's because, for every  $\sigma \in Gal(L,K)$ ,  $\sigma(H') = H'$ .
- 2. Now we want to show that  $Gal(M, L) \subseteq Z(Gal(M, K))$ .

$$1 \longrightarrow \operatorname{Gal}(M, L) \longrightarrow \operatorname{Gal}(M, K) \longrightarrow \operatorname{Gal}(L, K) \longrightarrow 1$$

$$\operatorname{rec} \cong \operatorname{A}_{L}^{\times}/L^{\times} \cdot H'$$

There's a general functoriality.<sup>25</sup>

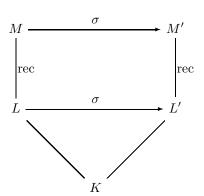
Want to figure out how conjugation by  $\sigma \in Gal(L, K)$  operates.



Check that if  $x \in A_L^{\times}/L^{\times} \cdot H'$ , 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



What?

Jeff Achter 77 Ching-Li Chai

MA 620 6 April 1994

**Proof** For H ( $\widetilde{H}$  ( $\mathcal{A}_K^{\times}/K^{\times}$ . Proof is by induction on  $[\mathcal{A}_K^{\times}/K^{\times}:H]$ . 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  $p[[\mathcal{A}_K^{\times}/K^{\times}:H]$ . The base case is trivial. Assume  $[\mathcal{A}_K^{\times}/K^{\times}:\widetilde{H}]=p$ . We may assume that  $K \supseteq \mathcal{Q}(\mu_p)$ .

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

$$A_{L}^{\times} \xrightarrow{N_{L,K}} \widetilde{H} \subseteq A_{K}^{\times}$$

$$\downarrow \qquad \qquad \downarrow$$

$$N_{L,K}^{-1}(H) \longrightarrow H$$

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

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

$$1 \longrightarrow L^{\times} \longrightarrow A_{L}^{\times} \longrightarrow A_{L}^{\times}/L^{\times} \longrightarrow 1$$

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

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

$$\bigoplus_{v} H^{2}(G_{v}, L_{w}^{\times})$$

$$\bigoplus_{v} \operatorname{Br}(L_{w}, K_{v})$$

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

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

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

Jeff Achter 78 Ching-Li Chai

MA 620 8 April 1994

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

$$H^{\bullet}(G, M) = \lim_{\substack{U \to M \text{ open}}} H^{\bullet}(G/U, M^{U})$$
  
=  $H^{\bullet}(\text{std cochain complex})$ 

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

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

Here, scd is the strict cohomological dimension. It turns out that  $cd(G) \le scd(G) \le cd(G) + 1$ . 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

$$\operatorname{cd}_p(G) \stackrel{\text{def}}{=} \inf\{i \in \mathbb{N} : H^j(G, M)_{(p)} = 0 \forall i > 0 \\ \text{and discrete torsion } G\text{-modules } M\}$$

$$\operatorname{scd}_p(G) \stackrel{\text{def}}{=} \inf\{i \in \mathbb{N} : H^j(G, M) = 0 \forall i > 0 \\ \text{and discrete } G\text{-modules } M\}$$

Just look where the *p*-torsion is killed.

**Exercise** If G is a nontrivial finite group, then  $cd(G) = \infty$ .

Jeff Achter 79 Ching-Li Chai

<sup>&</sup>lt;sup>26</sup>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.

MA 620 8 April 1994

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

Fact K a nonarchimedean locally compact local field.<sup>27</sup> Let  $G = Gal(K^{sep}, K)$ . Then  $scd_l(G) = cd_l(G) = 2$  if  $l \neq char K$ .<sup>28</sup> If l = char K, then  $scd_l(G) = 2$ ,  $cd_l(G) = 1$ .<sup>29</sup>

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  $H^1(\operatorname{Gal}(L,K),L^{\times})=0$ ; that's Hilbert 90. And  $H^2(\operatorname{Gal}(L,K),L^{\times})=n^{-1}\mathbf{Z}/\mathbf{Z}$ , where n=[L:K]. Now,  $\operatorname{Gal}(L,K)$  is a finite quotient  $\frac{\operatorname{Gal}(K^{\operatorname{sep}},K)}{\operatorname{Gal}(K^{\operatorname{sep}},L)}$ . And  $L^{\times}=(K^{\operatorname{sep}})^{\times \operatorname{Gal}(K^{\operatorname{sep}},L)}$ . Take limits. Then  $H^2(\operatorname{Gal}(K^{\operatorname{sep}},K),(K^{\operatorname{sep}})^{\times})=Q/\mathbf{Z}$ . 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,  $H^1(\operatorname{Gal}(L,K), \operatorname{A}_L^{\times}/L^{\times})=0.^{30}$  And  $H^2(\operatorname{Gal}(L,K), \operatorname{A}_L^{\times}/L^{\times})=n^{-1}\mathbf{Z}/\mathbf{Z}$ . If  $M\supset L\supset K$ , then  $(\operatorname{A}_M^{\times}/M^{\times})^{\operatorname{Gal}(M,L)}=\operatorname{A}_L^{\times}/L^{\times}$ . Why is this? General trick to verify it. Well,  $\operatorname{A}_L^{\times}$  is the Galois invariants of  $\operatorname{A}_M^{\times}$ ; 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  $1\to M^{\times}\to\operatorname{A}_M^{\times}\to \operatorname{A}_M^{\times}\to 1$ . And whether or not this is everything is precisely  $H^1(G,M^{\times})$ , which is zero by Hilbert 90. BTW,  $H^2(\operatorname{Gal}(K^{\operatorname{sep}},K),\operatorname{A}_{K^{\operatorname{sep}}}^{\times}/K^{\operatorname{sep}\times})=\operatorname{Q}/\operatorname{Z}$ .

In such situations, there's a theorem of Tate – which we proved, actually – that  $H^r(G, \mathbb{Z}) \xrightarrow{\cup} H^{r+2}(G, \cdot)$ ; 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  $U \to G$ ,  $H^1(G/U, C^U) = 0$ .
- 2. There's an isomorphism  $i: H^2(G,C) \stackrel{\cong}{\to} \mathbb{Q}/\mathbb{Z}$  so that for every open normal  $U \to G$ , we have

Jeff Achter 80 Ching-Li Chai

<sup>&</sup>lt;sup>27</sup>This just means the residue field is finite.

<sup>&</sup>lt;sup>28</sup>Serre, Cohomologie Galoisienne II.5., Prop 15.

<sup>&</sup>lt;sup>29</sup>Serre, I.3.3, Cor 4, III.2.2 Prop 3.

<sup>&</sup>lt;sup>30</sup>Not Hilbert 90, but the second fundamental inequality.

MA 620 8 April 1994

$$H^{2}(G,C) \xrightarrow{i} \mathrm{QZ}$$

$$\downarrow \qquad \qquad \downarrow$$

$$H^{2}(U,C) \xrightarrow{i} n^{-1}\mathrm{Z}/\mathrm{Z}$$

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

Jeff Achter 81 Ching-Li Chai

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. inv:  $H^2(G,C) \stackrel{\cong}{\to} Q/Z$ . More generally, for all  $U \subseteq G$  open,

$$H^2(U,C) \xrightarrow{\cong} Q/Z$$

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

$$H^{2}(U_{2}, C) \xrightarrow{\operatorname{inv}_{U_{2}}} Q/Z$$

$$\downarrow \operatorname{res}_{U_{2}, U_{1}} \qquad \downarrow [U_{2} : U_{1}]$$

$$H^{2}(U_{1}, C) \xrightarrow{\cong} Q/Z$$

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]:

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

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

$$\hat{H}^{i}(G/U, \mathbf{Z}) \xrightarrow{\bigcup u_{G/U}} \hat{H}^{i+2}(G/U, C^{U})$$

For I = -2, get

Jeff Achter 82 Ching-Li Chai

$$(G/U)^{\mathrm{ab}} \longrightarrow \frac{C^G}{N_{G,U}(C^U)}$$

$$\frac{G^{\mathrm{ab}}}{\mathrm{im}\,U}$$

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  $G \cong \hat{\mathbf{z}}$  the profinite completion of  $\mathbf{z}$ . 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  $Q/Z = (\hat{Z})^{\vee}$ . So we use

$$\inf_{G} \cong H^{i}(G, M) \times H^{2-i}(G, \operatorname{Homz}(M, C)) \longrightarrow H^{2}(G, C)$$

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  $\operatorname{Ext}_G^{2-i}(M,C)$ , since there's a spectral sequence at work here. In general,  $E_2^{a,b} = H^a(G,\operatorname{Ext}_{\mathbf{Z}}^b(M,C)) \Rightarrow \operatorname{Ext}^{a+b}(M,C)$ . Well, that's the motivation, hope you enjoyed it.

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

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

How do we think about this? Resolve M by  $M \to M^{\bullet}$  an injective resolution. Then an element of  $\operatorname{Ext}_G^j(N,M)$  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  $\operatorname{Ext}_G^i(M,C)$ ? We've already chosen

Jeff Achter 83 Ching-Li Chai

<sup>&</sup>lt;sup>31</sup>In the DeRham contex, we had  $H^i(M, \mathbb{R}) \times H^{n-i}(M, \mathbb{R}) \to H^n(M, \mathbb{R}) \stackrel{\cong}{\to} \mathbb{R}$ , 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  $\operatorname{Ext}_{G}^{i}(M, C)$  as a map  $H_{2}: M^{\bullet} \to C^{\bullet}$  of degree i. The obvious way to get in  $\operatorname{Ext}_{G}^{i+j}(N, C)$  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  $0 \to M \to 0 \to \cdots \to 0$  with j things between them; that's  $\operatorname{Ext}_G^j(N,M)$ . And  $\operatorname{Ext}_G^i(M,C)$  is similar; then just concatenate them to get an  $\operatorname{Ext}_G^{i+j}(N,C)$ .

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

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

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

Special case. Take M = Z; look at this map.

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

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

That's gotta be the reciprocity law.

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

$$0 \longrightarrow 0$$

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

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

And this really oughta be the invariant map  $inv_G$ .

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

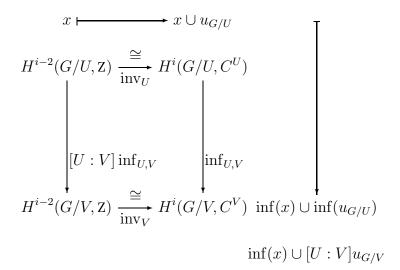
Jeff Achter 84 Ching-Li Chai

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

$$H^{i-2}(G/U,\mathbf{Z}) \xrightarrow{\cong} H^{i}(G/U,C^{U})$$

$$\downarrow : \qquad \qquad \downarrow \inf_{U,V} H^{i-2}(G/V/\mathbb{Z}^{i}) (G/V/\mathbb{Z}^{i}) (G/V/\mathbb{Z}^{i}) (G/V/\mathbb{Z}^{i})$$

The left-hand side is multiplication by the index;



Jeff Achter 85 Ching-Li Chai