Local Class Field Theory

Kevin Buzzard, Imperial College London

Imperial, 12th Nov 2025

Plan

Say L/K is a finite Galois extension of nonarchimedean local fields and $[L : K] = d$. Say $G = Gal(L/K)$.

Last time I talked about why $|H^2(G, L^\times)| \leq d$.

Today I'll construct an explicit element of order d, called the *fundamental class*.

That will give us an isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

[Recall that then some general group-cohomological nonsense gives us an isomorphism $K^\times/N_{L/K}(L^\times) = G^{ab}$ (which depends on the choice of the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$, or equivalently on the fundamental class) and hence the local Artin map.]

The strategy: first construct the element of order d for unramified extensions, and then for general extensions.

Valuations

Before I explain what unramified extensions are, let me talk a little more about the internals of nonarchimedean local fields.

If K is a nonarchimedean local field then it comes equipped with a canonical valuation $v : K^\times \to \mathbb{Z}$, giving rise to a (equivalence class of) norm(s) $|0| = 0$ and $|k| = 0.37^{v(k)}$ and hence a metric $d(k_1, k_2) := |k_1 - k_2|$.

The map v is a surjective group homomorphism.

It's usually normalised such that if ϖ_K is a uniformiser, i.e., a generator of the maximal ideal of the integer ring (closed unit disc) $\mathcal{O}_K$ of K, then $v_K(\varpi_K) = 1$.

Note that the integer ring $\mathcal{O}_K = \{0\} \cup \{x : v_K(x) \geq 0\}$ is a (complete) discrete valuation ring, and every nonzero ideal of $\mathcal{O}_K$ is principal and of the form (ϖ_K^n) for some natural number n.

The ideal (ϖ_K^n) is just $\{0\} \cup \{x : v_K(x) \geq n\}$.

If you know about fractional ideals, they're just $\varpi_K^n \mathcal{O}_K$ for $n \in \mathbb{Z}$.

Extensions

Let's talk about what a finite extension L/K of nonarchimedean local fields looks like.

There are two ways that L can be "bigger than" K, and one way is that the valuation can change.

Because $K \subseteq L$ we have $K^\times \subseteq L^\times$, and we can ask how v_L and v_K compare on $K^\times$.

One checks that there exists a positive integer e such that $ev_K(k) = v_L(k)$ for all $k \in K^\times$.

One can compute e by figuring out $v_L(k)/v_K(k)$ for any k such that $v_L(k) \neq 0$ or equivalently such that $v_K(k) \neq 0$.

For example one could use a unformiser of K; this gives that the ideals ϖ_K and $(\varpi_L)^e$ of $\mathcal{O}_L$ are equal.

This e is called the *ramification index* of L/K.

Example

Example: if $K = \mathbb{Q}_p$ then any element x of $K^\times$ is uniquely of the form $x = p^n u$ with $u \in \mathbb{Z}_p^\times$, and we set $v_K(x) = n$.

If now $L = \mathbb{Q}_p(\sqrt{p})$ then $\mathcal{O}_L = \mathbb{Z}_p[\sqrt{p}]$, the maximal ideal is $(\sqrt{p})$, the residue field is still $\mathbb{F}_p$, and $v_L(\sqrt{p}) = 1$ so $v_L(p) = 2$ because v_L is a group homomorphism.

So $v_L(k) = 2v_K(k)$ for $k = p$ and thus for all $k \in K^\times$.

So $e(\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p) = 2$.

More generally $e(\mathbb{Q}_p(\sqrt[n]{p})/\mathbb{Q}_p) = n$.

Example

Example: if $K = \mathbb{Q}_3$ then -1 isn't a square mod 3 so it's not a 3-adic square, by Hensel's lemma. Set $L = \mathbb{Q}_3(i) = \mathbb{Q}_3(\sqrt{-1})$.

Then $\mathcal{O}_L = \mathbb{Z}_3[i]$ and if we quotient out by the ideal (3) we get $\mathbb{F}_3[i] = \mathbb{F}_9$, the field with 9 elements.

Hence (3) is maximal, so 3 is a uniformiser of L, so $v_L(3) = 1$, so $v_L(3) = v_K(3)$ so $e = 1$.

If $e = 1$ we say the finite extension L/K is *unramified*.

More generally if $k/\mathbb{F}_p$ is a finite field extension of degree d and $k = \mathbb{F}_p(g)$ then we can take the minimal polynomial $\overline{f(X)} \in \mathbb{F}_p[X]$ for g over $\mathbb{F}_p$, lift to $f(X) \in \mathbb{Z}[X]$ monic of the same degree d, and then the splitting field of $f(X)$ is an extension of $\mathbb{Q}_p$ with residue field k and uniformiser p, so $e = 1$.

Residue field extension

We've seen that the valuation for an extension L/K can change, and this is meaured by the positive integer $e = e(L/K)$.

Another way that a finite extension L of K can be "bigger than" K is that the residue field can get bigger, as we just saw.

We have $K \subseteq L$, so $\mathcal{O}_K \subseteq \mathcal{O}_L$, and the induced map $\mathcal{O}_K \to \mathbb{F}_L$ (the residue field of the local ring $\mathcal{O}_L$) induces a map $\mathbb{F}_K \to \mathbb{F}_L$, making $\mathbb{F}_L$ into a field extension of $\mathbb{F}_K$.

Turns out that this field extension is always finite of degree at most $[L : K]$.

Let $f(L/K)$ denote the degree of this field extension.

Examples

Example: If $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\sqrt{p})$ then the residue fields are both $\mathbb{Z}/p\mathbb{Z}$ so $f = 1$.

Example: if $K = \mathbb{Q}_3$ and $L = \mathbb{Q}_3(i)$ then $\mathbb{F}_L = \mathbb{F}_9$ and $\mathbb{F}_K = \mathbb{F}_3$ so $f = 2$.

The big theorem is that $ef = [L : K]$.

This is the local analogue of the theorem $\sum_i e_i f_i = [L : K]$ for number fields, where $P \subset \mathcal{O}_K$ is a maximal ideal downstairs which factors as $\prod_i Q_i^{e_i}$ upstairs.

Function field example: if l/k is a finite extension of finite fields of degree f, then $l((T^{1/e}))/k((T))$ is an extension of degree ef with basis $b_i T^{j/e}$ where $0 \leq j < e$ and the b_i for $1 \leq i \leq f$ run through a basis of l/k.

Unramified extension

If L/K is an unramified extension of degree d, then $e = 1$ so $f = d$ which means that the residue field extension $\mathbb{F}_L/\mathbb{F}_K$ is also an extension of degree d (this time of finite fields).

It turns out that in some sense the residue field extension "controls" the local field extension.

Fancy way to say it: for a fixed nonarch local field K, the category of finite unramified extensions of K is equivalent to the category of finite extensions of the residue field $\mathbb{F}_K$.

Given unramified L/K, the corresponding extension of $\mathbb{F}_K$ is just $\mathbb{F}_L$.

The dictionary going the other way ("given $l/\mathbb{F}_K$ make L") depends on whether the local field has characteristic 0 or p.

In characteristic p we have $K \cong \mathbb{F}_K((t))$ and we just let $L = l((t))$.

Witt vectors

In the characteristic zero case it's more complex and the nicest way to do it is via the theory of Witt vectors.

If K is a finite extension of $\mathbb{Q}_p$ with residue field k then K is naturally an algebra over the ring $W(k)$ of Witt vectors of k (sometimes called p-Witt vectors).

If l/k is a finite extension then the corresponding unramified extension of K is just $K \otimes_{W(k)} W(l)$.

Examples: $W(\mathbb{F}_p) = \mathbb{Z}_p$.

Example: $W(\mathbb{F}_9) = \mathbb{Z}_3[i]$.

Example: the field of fractions of $W(k)$ for k any finite field of size $q = p^f$ is the splitting field of $X^q - X$ (or of $X^{q-1} - 1$) over $\mathbb{Q}_p$, and $W(k)$ is the ring of integers of this nonarchimedean local field.

Unramified extensions

A consequence of unramified extensions being controlled up to isomorphism by their residue fields is that given a nonarchimedean local field K and a positive integer f there is a unique (up to non-unique isomorphism) extension L/K of K which is unramified of degree f.

This extension is Galois with Galois group canonically isomorphic to $Gal(\mathbb{F}_L/\mathbb{F}_K)$ which is canonically cyclic of order f.

In particular, $Gal(L/K)$ has a canonical generator, which we'll call the Frobenius element.

Now let's construct fundamental classes for unramified extensions.

The unramified case

Last time I raced through how to prove $|H^2(Gal(L/K), L^\times)| = [L : K]$ if $Gal(L/K)$ was cyclic (so we could use the theory of Herbrand quotients).

Remember that this was the only point where we actually computed a cohomology group.

The crucial lemma (which I didn't even state precisely last time) is this:

Theorem
If $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ is a G-module with a decreasing sequence of G-submodules such that $M = \varprojlim_i M/M_i$, if $n \geq 1$ is a positive integer, and if $H^n(G, M_i/M_{i+1}) \cong 0$ for all i then $H^n(G, M) \cong 0$.

The proof is: given a cohomology class in $H^n(G, M)$ show by induction on i that it can be represented by a cocycle with values in M_i, and then using $M = \varprojlim_i M/M_i$ that it is a coboundary.

Vanishing of cohomology

Theorem

If $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ is a G-module with a decreasing sequence of G-submodules such that $M = \varprojlim_i M/M_i$, if $n \geq 1$ is a positive integer, and if $H^n(G, M_i/M_{i+1}) \cong 0$ for all i then $H^n(G, M) \cong 0$.

We used this to prove vanishing of cohomology of U for U some uncontrolled finite index subgroup of $\mathcal{O}_L^\times$, and deduced that if G is cyclic (so the theory of Herbrand quotients is available) then $h_G(\mathcal{O}_L^\times) = 1$, so $|H^1(G, \mathcal{O}_L^\times)| = |H^2(G, \mathcal{O}_L^\times)|$.

In the unramified case we can do better.

The unramified case

Say L/K is a finite unramified extension of degree f, with residue field extension $\mathbb{F}_L/\mathbb{F}_K$ also of degree f.

This time we consider the filtration $\mathcal{O}_L^\times \supseteq 1 + \varpi_L\mathcal{O}_L \supset 1 + \varpi_L^2\mathcal{O}_L \supset \cdots$.

The first of the subquotients is isomorphic to $\mathbb{F}_L^\times$ as a G-module, and all of the others are isomorphic to $\mathbb{F}_L$.

I claim that both $\mathbb{F}_L^\times$ and $\mathbb{F}_L$ have trivial cohomology in all degrees $n \geq 1$.

If you believe this, then by the cocycle-gluing lemma (which Kenny is working on formalizing) we have $H^n(G, \mathcal{O}_L^\times) \cong 0$ for all $n \geq 1$.

Cohomology of finite fields

The trick here is that $G = Gal(L/K) = Gal(\mathbb{F}_L/\mathbb{F}_K)$ because we're unramified.

So $\mathbb{F}_L$ has trivial cohomology because as a G-module it's isomorphic to $\mathbb{F}_K[G]$ by the normal basis theorem for $\mathbb{F}_L/\mathbb{F}_K$, so it's an induced module so has no higher cohomology.

For $\mathbb{F}_L^\times$ the argument is a bit more of a hack.

It's a finite set, so $h_G(\mathbb{F}_L^\times) = 1$.

By Hilbert 90, $H^1(G, \mathbb{F}_L^\times) \cong 0$ (this works because G is the Galois group of the residue field too).

So by Herbrand quotient $H^2(G, \mathbb{F}_L^\times) \cong 0$ and now by periodicity of cohomology for cyclic groups, $H^n(G, \mathbb{F}_L^\times) \cong 0$ for all $n \geq 1$.

The upshot

The upshot is that $\mathcal{O}_L^\times$ has no higher cohomology, so the boundary maps in the long exact sequence of cohomology associated to $1 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ are isomorphisms, and in particular $H^2(G, L^\times) \cong H^2(G, \mathbb{Z})$ where $\mathbb{Z}$ has the trivial G-action.

We've already proved last time that $|H^2(G, L^\times)|$ has order f, but we can do better here because $H^2(G, \mathbb{Z}) = H^0_{Tate}(G, \mathbb{Z}) = \mathbb{Z}/f\mathbb{Z}$ by periodicity of Tate cohomology and an explicit easy calculations.

So we know abstractly that $H^2(G, L^\times)$ is cyclic of order f in the unramified case.

But that's not good enough: we don't just want a theorem, we want a definition.

We want an explicit element of order f in $H^2(G, L^\times)$.

I'll now write one down.

The fundamental class

Recall that $H^2(G, M)$ is 2-cocycles modulo 2-coboundaries.

Recall also that $G \cong \mathbb{Z}/f\mathbb{Z}$ here, with the Frobenius element $F \in G$ going to 1.

We know that v induces an isomorphism $H^2(G, L^\times) = H^2(G, \mathbb{Z})$ so let's write down an explicit element of order n in $H^2(G, \mathbb{Z})$ and then "un-v it" in the obvious way.

Let's consider the "carry cocycle" $\sigma : G^2 \to \mathbb{Z}$ defined by (for $0 \leq i, j < f$) sending (F^i, F^j) to 0 if $i + j < f$ and 1 if $i + j \geq f$.

Exercise: σ is a 2-cocycle, i.e. $\sigma(g, h) - \sigma(g, hj) + \sigma(gh, j) - \sigma(h, j) = 0$ for all $g, h, j \in \mathbb{Z}/f\mathbb{Z}$.

Claim: the corresponding cohomology class $\overline{\sigma} \in H^2(G, \mathbb{Z}) \cong \mathbb{Z}/f\mathbb{Z}$ is a generator.

Modulo this: Corollary: the $L^\times$-valued 2-cocycle sending (F^i, F^j) to 1 if $i + j < f$ and ϖ_L (or ϖ_K) if $i + j > f$ gives rise to an element of $H^2(G, L^\times)$ of order f, which we'll call the canonical class.

Proof of claim

The trick is to write down an explicit group isomorphism $inv_G : H^2(G, \mathbb{Z}) \to \mathbb{Z}/f\mathbb{Z}$, where we recall that G is cyclic of order f with a canonical generator F.

The isomorphism sends a 2-cocycle σ to $\sum_{i=0}^{f-1} \sigma(F^i, F)$ modulo f.

One checks that this is trivial on 2-coboundaries and thus induces a group homomorphism $H^2(G, \mathbb{Z}) \to \mathbb{Z}/f\mathbb{Z}$.

It's easy to evaluate on the carry cocycle: because $1 + i$ only gives you a carry digit if $i = f - 1$, it gets mapped to 1.

So it has order f in $\mathbb{Z}/f\mathbb{Z}$, so must have order at least f in $H^2(G, \mathbb{Z})$, a cyclic group of order f.

This proves everything.

Upshot: if L/K is unramified of degree f then we've written down an explicit isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/f\mathbb{Z}$ and we have a fundamental class which is the thing sent to 1.

The general case

Now say L/K is an arbitrary finite Galois extension of degree d, with $G = Gal(L/K)$ (not necessarily cyclic or even abelian).

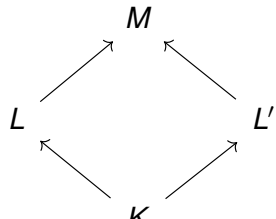
Recall: our goal is to write down an element of $H^2(G, L^\times)$ of order d.

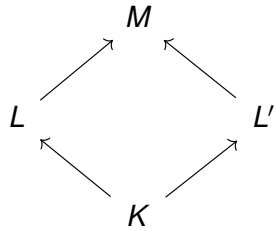
Then $H^2(G, L^\times)$ will be cyclic and this element will be a generator because we already know $|H^2(G, L^\times)| \leq d$ from last time.

We're going to be juggling four fields and four field extensions, so I'm going to write $H^2(L/K, L^\times)$ instead of $H^2(Gal(L/K), L^\times)$.

Here's the trick: let L' denote the unramified extension of K of degree d.

And let's let $M = LL'$ so we have a diagram





with $[L : K] = [L' : K] = d$, L'/K and hence M/L unramified, and everything is Galois over everything else.

By higher inf-res we have short exact sequences

$$0 \to H^2(Gal(L'/K), L'^{\times}) \to H^2(Gal(M/K), M^{\times}) \to H^2(Gal(M/L'), M^{\times})$$

and

$$0 \to H^2(Gal(L/K), L'^{\times}) \to H^2(Gal(M/K), M^{\times}) \to H^2(Gal(M/L), M^{\times}).$$

By the argument in the unramified case we have an element of order d in $H^2(Gal(L'/K), L'^{\times})$, and we want one in $H^2(Gal(L/K), L^{\times})$.

The diagram chase

$$0 \to H^2(Gal(L'/K), L'^\times) \to H^2(Gal(M/K), M^\times) \to H^2(Gal(M/L'), M^\times)$$

and

$$0 \to H^2(Gal(L/K), L'^\times) \to H^2(Gal(M/K), M^\times) \to H^2(Gal(M/L), M^\times).$$

and L'/K and M/L are unramified, $[L : K] = [L' : K] = d$.

So let's take our unramified fundamental class in $H^2(Gal(L'/K), L'^\times)$ and push it forward to get an element of order d in $H^2(Gal(M/K), M^\times)$.

Claim: it's in the image of $H^2(Gal(L/K), L^\times)$, or equivalently its image in $H^2(Gal(M/L), M^\times)$ is zero. This suffices, because it will still have order d in this subgroup.

You should believe it's in the image, because a posteriori each of these groups is cyclic of the obvious size, so these sequences are all exact and the images of $H^2(Gal(L/K), L^\times)$ and $H^2(Gal(L'/K), L'^\times)$ are equal.

But we have to prove it.

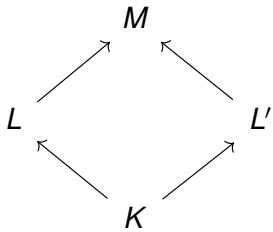
The story so far

We have a fundamental class in $H^2(L'/K, L'^\times)$, and we have a formula for it because L'/K is unramified.

We take its image in $H^2(M/K, M^\times)$ and then restrict to $H^2(M/L, M^\times)$, where M/L is also unramified.

We have a formula for the isomorphism $H^2(M/L, M^\times) = \mathbb{Z}/[M : L]\mathbb{Z}$ because it's unramified, so we can just compute.

But first we'd better compute $[M : L]$.



Let $e = e(L/K)$ and $f = f(L/K)$ be the ramification index and inertial degree for L/K.

Then the residue field of M is generated by the residue fields of L and L' which have degrees f and ef, so the residue field of M has size ef, so $f(M/L) = e$.

Moreover L'/K is unramified so M/L is unramified, so $e(M/L) = 1$. thus $[M : L] = e$.

And so now we can do the calculation.

The calculation

We have the fundamental class for L'/K, coming from a 2-cocycle sending (F_K^i, F_K^j) to 1 if $i+j < d$ and ϖ_K if $i+j \geq d$.

I'll write F_K to mean "the automorphism which on the residue field sends x to $x^{|\mathbb{F}_K|}$."

We inflate the 2-cocycle to M/K and get a 2-cocycle whose value on (g,h) is computed by restricting g and h to the quotient group $Gal(L'/K)$ and then just applying the old 2-cocycle.

Now we restrict to M/L and again get the obvious 2-cocycle.

Its value on (g,h) is: they're automorphisms of M, so restrict them to L' and then use the formula on the top of this slide.

So to do the calculation, we need to know:

(1) Starting with $F_L \in Gal(M/L)$, what power of $F_K \in Gal(L'/K)$ is it?
(2) If there is a carry, then the value of the cocycle we're chasing is ϖ_K. What power of ϖ_L is this?

The answers

F_K sends x in the residue field to $x^{|\mathbb{F}_K|}$ and F_L sends x to $x^{|\mathbb{F}_L|}$, so it's the $f(L/K)$'th power of F_K.

And $\varpi_L^e = \varpi_K$ up to units (which we can ignore) where $e = e(L/K)$.

The calculation now: if σ is the fundamental cocycle in $H^2(L/K, L^\times)$ then we inflate and restrict to $H^2(M/L, M^\times)$ and now we need to apply the isomorphism to $\mathbb{Z}/e\mathbb{Z}$ sending τ to $\sum_{0\le i<e} v_M(\tau(F_L^i, F_L)) \in \mathbb{Z}/e\mathbb{Z}$ and check it's zero; then we're done.

We have $\tau(F_L^i, F_L) = \sigma(F_K^{fi}, F_K^f)$, and F_K has order ef, so in the range $0 \le i < e$ we only get a carry when $i = e - 1$.

So $\sum_{0\le i<e} v_M(\tau(F_L^i, F_L)) = v_M(\varpi_K)$.

And this is $v_L(\varpi_K) = e$, which is 0 in $\mathbb{Z}/e\mathbb{Z}$.

So we have a definition of a fundamental cocycle, and even a formula for it.

Next time I'll discuss some mathematics which I don't understand yet, namely: in what way these cocycles are compatible when we change K and L, and what this says about compatibility of Artin maps.