Local Class Field Theory

Kevin Buzzard, Imperial College London

Imperial, 24th Oct 2025

Plan for the 2 hours

I'm here 1-3pm.

In the first hour or so I'll talk about the main theorems of local class field theory (and do some background).

I'll also say something about group cohomology.

In the second hour I will be doing live lean coding, attempting to formalise statements and proofs related to the proofs of the main theorems of local class field theory.

I'll also be livestreaming on the Xena Discord.

What is class field theory?

Class field theory is about understanding the easiest possible Galois extensions of the easiest possible fields.

More precisely, let K be one of the easiest possible fields.

Class field theory is about studying the Galois extensions L/K of K which have abelian Galois groups (or "abelian extensions" of K for short).

By the joys of infinite Galois theory, this is the same as proving facts about the *maximal abelian extension* K^{ab} of K (defined for example as the union of all the finite abelian extensions of K within a fixed algebraic closure), and trying to figure out what either what K^{ab} is or what $Gal(K^{ab}/K)$ is.

The second question is easier than the first, it turns out; the first (Hilbert's 12th problem) is still largely open for fields like $\mathbb{Q}(2^{1/3})$ where Shimura variety techniques do not apply, but the second was answered 100 years ago.

Interlude: the Langlands program

Why study just the abelian extensions of K? Isn't that a bit weird?

Indeed, for quite some time people didn't understand why this worked so well and why generalizing it seemed so hard.

Then Langlands came along and observed that what was going on was that studying abelian extensions of K was the same thing as (or more precisely, the dual of) studying continuous 1-dimensional representations of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

This might explain why figuring out $\mathrm{Gal}(K^{ab}/K)$ is easier than figuring out K^{ab}.

The Langlands program is a (still largely conjectural) attempt to understand n-dimensional representations of this group.

Class field theory can be explained and reconceptualised via the Langlands program but that doesn't make the proofs any easier.

“Simple” fields

I claimed that class field theory works for “simple” fields.

The simplest fields are finite fields.

Here’s what “class field theory” looks like for finite fields (even though historically it was much earlier, and isn’t usually even called class field theory):

Theorem

Let K be a finite field. Then for each positive integer n there is (up to non-unique isomorphism if $n > 1$) exactly one extension L/K of degree n; it is Galois, with cyclic Galois group of order n, generated by the arithmetic Frobenius element $x \mapsto x^{|K|}$.

Proof omitted.

Put another way: if K is finite then $\mathrm{Gal}(K^{ab}/K) = \mathrm{Gal}(K^{sep}/K)$ is canonically isomorphic to $\widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$, a.k.a. the projective limit $\lim_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.

Normalisations

"Class field theory" for finite fields: If K is finite then $\mathrm{Gal}(K^{ab}/K) = \widehat{\mathbb{Z}}$ with $x \mapsto x^{|K|}$ being identified with 1.

Note: people who are into cohomology of Shimura varieties prefer the geometric Frobenius, which is just the inverse of the arithmetic Frobenius, giving a second canonical isomorphism to $\widehat{\mathbb{Z}}$ (which differs by a sign from the first one).

There is no "best" choice of isomorphism; in practice the best choice depends on what you're doing.

What next?

What are the next most simple fields?

In the early 1900s humans thought that finite extensions of $\mathbb{F}_p(t)$ and of $\mathbb{Q}$ were the next simplest fields – these are the so-called “global fields”; the characteristic p ones are “function fields” and the characteristic zero ones are number fields.

Indeed, historically the next developments in the study of class field theory involved figuring out $\mathrm{Gal}(K^{ab}/K)$ for these fields K, with $K = \mathbb{Q}$ going first (the Kronecker-Weber theorem: $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \widehat{\mathbb{Z}}^\times$, and even the description of $\mathbb{Q}^{ab}$ as $\bigcup_n \mathbb{Q}(\zeta_n)$).

However, when it comes to absolute Galois groups, $\mathbb{R}$ is much simpler than $\mathbb{Q}$ ($\mathrm{Gal}(\mathbb{R}^{sep}/\mathbb{R})$ has size 2, $\mathrm{Gal}(\mathbb{Q}^{sep}/\mathbb{Q})$ is incomprehensible), and after the discovery of the p-adic numbers in 1897 it was realised that their Galois theory was also easier than that of global fields.

Local fields

A *local field* is a finite extension of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ (these are the nonarchimedean local fields) or of $\mathbb{R}$ (the archimedean local fields).

Fact: When it comes to Galois theory, these are harder than finite fields, but easier than global fields.

The study of abelian extensions of these fields is called *local class field theory* and it's the topic of this lecture (and any further lectures which Edison persuades me to give).

If K is local then we know both K^{ab} and $\mathrm{Gal}(K^{ab}/K)$.

The $\mathbb{R}$ case is easy: $\mathbb{C}^{ab} = \mathbb{C}$, $\mathrm{Gal}(\mathbb{C}^{ab}/\mathbb{C})$ is trivial, $\mathbb{R}^{ab} \cong \mathbb{C}$, and $\mathrm{Gal}(\mathbb{R}^{ab}/\mathbb{R})$ is cyclic of size 2 (note that we do not need to fix a preferred square root of -1 in this statement).

So we'll spend the rest of our time thinking about the nonarchimedean case where K is a finite extension of either $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$.

Remarks we won't ever need

But just before we leave the $\mathbb{R}$ case let me say some things about why the definition ("finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$ or of $\mathbb{R}$") is so weird.

This is not really the definition, this is the conclusion of the classification theorem of local fields (which we don't need and will ignore).

Local fields can be intrinsically defined as locally compact topological fields, complete with respect to a rank one norm.

Other random facts: $\mathbb{R}$ and $\mathbb{Q}_p$ are rigid; they have no nontrivial field automorphisms (because the algebra determines the topology and $\mathbb{Q}$ is dense). However $\mathbb{F}_p((t))$ has uncountably many (e.g. $t \mapsto t + a_2t^2 + a_3t^3 + \cdots$).

On the other hand $\mathbb{C}$ has uncountably many discontinuous field automorphisms.

Every extension of $\mathbb{F}_p((t))$ is isomorphic to $k((t))$ for k a finite field.

Statement of the theorem

Let K be a nonarchimedean local field (so a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$).

We want to understand finite abelian extensions L/K of K.

In the finite field case, for any finite abelian extension L/K of degree n there was a canonical surjection $\mathbb{Z} \to \mathrm{Gal}(L/K)$, with kernel $n\mathbb{Z}$, and $\mathrm{Gal}(K^{ab}/K)$ was canonically isomorphic to the profinite completion of $\mathbb{Z}$.

Although it is far less obvious, in the local field case, for any finite abelian extension L/K there's a canonical surjection $K^\times \to \mathrm{Gal}(L/K)$, with kernel $N_{L/K}L^\times$ (the norm map from algebra), and $\mathrm{Gal}(K^{ab}/K)$ is canonically isomorphic to the profinite completion of $K^\times$.

The map $K^\times \to \mathrm{Gal}(L/K)$ is called the *Artin map* for the extension L/K.

Like in the finite field case, nobody can decide whether the Artin map or its inverse (precompose with $x \mapsto x^{-1}$ on $K^\times$) is the canonicalest.

Exercise: If K is an *archimedean* local field and L/K is finite Galois, there is also a canonial surjection $K^\times \to \mathrm{Gal}(L/K)$ with kernel $N_{L/K}(L^\times)$.

Overview of group cohomology

If G is a (finite for us, but it's not necessary) group, acting by group automorphisms on a (typically not finite) abelian group A (we say "A is a G-module"), then there are (typically not finite) abelian groups $H^n(G, A)$ and $H_n(G, A)$ associated to this set-up.

For $n = 0$ they have a direct definition ($H^0(G, A) = A^G$, the maximal G-invariant subgroup, and $H_0(G, A) = A_G$, the maximal G-invariant quotient) and for $n > 0$ they can either be defined via derived functor nonsense (giving cheap theorems but not way to calculate) or explicitly as n-(co)cycles over n-(co)boundaries (giving easy calculations but now you have to work to prove the theorems).

(If G is not finitely-generated then group cohomology is probably "the wrong object", G might well have a topology and one should use continuous cycles etc.)

Cycles/boundaries story

The cycle/boundary description gives you concrete formulae for the groups.

Say the group law for G is multiplication and the group law for A is addition, and G acts on A via $(g, a) \mapsto g \bullet a$.

Example: a 1-cocycle is $f : G \to A$ such that $f(gh) = f(g) + g \bullet f(h)$ and a 1-coboundary is $f : G \to A$ of the form $g \mapsto g \bullet a - a$ (exercise: check a 1-coboundary is a 1-cocycle; you just proved that $d^2 = 0$).

Corollary: if G acts trivially on A ($g \bullet a = a$ for all g, a) then $H^1(G, A)$ is just the group homomorphisms $G \to A$.

Example: a 2-cocycle is $\sigma : G^2 \to A$ such that $g \bullet \sigma(h, k) - \sigma(gh, k) + \sigma(g, hk) - \sigma(g, h) = 0$, so every element of $H^2(G, A)$ can be represented by such a function.

Cycles/boundaries story

Example: a 1-cycle is $f : G \to_0 A$ (finite support), satisfying $\sum_{g \in G} g^{-1} f(g) = \sum_g f(g)$ (these are finite sums).

Example: every $f : G \to_0 A$ is a 1-cocycle if G acts trivially on A.

If G acts trivially on A then there's a natural surjective map from the 1-cycles to $G^{ab} \otimes_{\mathbb{Z}} A$, sending `single g a` to $g \otimes a$ and general f to $\sum_{g \in G}(g \otimes f(g))$.

The kernel is precisely the 1-boundaries.

Category-theoretic approach

The derived functor definition of group cohomology is: $A \mapsto A^G$ is left exact; take its right derived functors. The derived functor definition of group homology is: $A \mapsto A_G$ is right exact; take its left derived functors.

This nonsense gives you that a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules gives rise to long exact sequences $0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to \cdots$ and $\cdots \to H_1(G, C) \to H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0$.

It also gives you the Hochschild–Serre spectral sequence $E_2^{i,j} := H^i(G/N, H^j(N, M)) \implies H^{i+j}(G, M)$ (see Grothendieck Tohoku).

Tate cohomology

If G is finite (not even finitely-generated is enough; finiteness is essential here) then there is a third cohomology theory in play, called Tate cohomology.

Definition: $H^n_{Tate}(G, M) = H^n(G, M)$ for $n \geq 1$, $H^{-1-n}_{Tate}(G, M) = H_n(G, M)$ for $n \geq 1$ (so that's covered H^{-2}, $H^{-3} \ldots$), and $H^{-1}_{Tate}(G, M)$ and $H^0_{Tate}(G, M)$ have bespoke definitions related to, but not equal to, $H_0(G, M)$ and $H^0(G, M)$.

Idea: there's a map $M_G = H_0(G, M) \to M^G = H^0(G, M)$ sending m to $\sum_{g \in G}(g \bullet m)$; $H^{-1}_{Tate}(G, M)$ is the kernel of this map, and $H^0_{Tate}(G, M)$ is the cokernel.

The point: given a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, there a long (in both directions) exact sequence
$\cdots \to H^{n-1}(G, C) \to H^n(G, A) \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \cdots$.

I don't know of any cohomological nonsense way to construct Tate cohomology.

Note: it only works for G finite (but we only care about this case anyway).

The Artin map

So where does this Artin map $K^\times \to \mathrm{Gal}(L/K)$ come from, where L/K is an abelian extension?

It comes from an even more magical construction.

If L/K is any Galois extension of nonarchimedean local fields, of degree n and with Galois group G (not even assumed to be abelian), then I claim that there is a canonical isomorphism $H^2(G, L^\times) = \mathbb{Z}/n\mathbb{Z}$, with $1 \in \mathbb{Z}/n\mathbb{Z}$ being identified with the so-called *fundamental class* in $H^2(G, L^\times)$.

Note: it's not obvious (to me, at least) that $H^2(G, L^\times)$ is even finite, let alone cyclic (and it's not finite for a general field K; this is specific to local fields).

This canonical isomorphism $H^2(G, L^\times) = \mathbb{Z}/n\mathbb{Z}$ is the fundamental construction in the local theory.

The Artin map $K^\times \to G$ when G is abelian, comes as a consequence, as we'll see today.

Fundamental classes

The Artin map is “local Langlands for GL_1”.

GL_1 is a basic example of a connected reductive group over K.

Turns out that even if we're only interested in abelian extensions, the fact that there's a canonical isomorphism $H^2(Gal(L/K), L^\times) = \mathbb{Z}/n\mathbb{Z}$ even for $Gal(L/K)$ nonabelian of size n, is crucial for the Langlands philosophy.

Langlands showed in the 1960s that local Langlands for an arbitrary abelian connected reductive algebraic group also follows from the existence of this canonical isomorphism.

To give a d-dimensional abelian connected reductive algebraic group over a field K is to give a finite Galois extension L/K with Galois group G (not necessaily abelian), and a group homomorphism $G \to \mathrm{GL}_d(\mathbb{Z})$ (the construction goes via via the theory of characters of tori).

Example: GL_1 corresponds to $L = K$ and G trivial and $d = 1$.

To the Artin map

The definition of the Artin map which I was taught was via "cup products in Tate cohomology".

"If $G = Gal(L/K)$ is abelian then $G = G^{ab} = G^{ab} \otimes_{\mathbb{Z}} \mathbb{Z} = H_1(G, \mathbb{Z}) = H^{-2}_{Tate}(G, \mathbb{Z})$ and then cupping with the canonical class in $H^2(G, L^\times)$ takes you to $H^0_{Tate}(G, L^\times) = K^\times / N_{L/K}(L^\times)$; turns out this is an isomorphism, and the Artin map is the inverse of this isomorphism."

However in June in Oxford, Richard Hill showed me a way to define the Artin map without defining cup products at all.

Shifting by one

Here's a trivial observation to start with.

Say $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules and $H^n_{Tate}(G, B) = 0$ for all n.

Then the long exact sequence gives $H^n_{Tate}(G, C) = H^{n+1}_{Tate}(G, A)$ for all integers n.

We have that one cohomology group equals another, but the degree shifted by 1.

To shift the degree by 2, we need to apply this twice.

The first trick

The first trick is low-level and works in huge generality.

Let G be a finite group.

Let G act on the left on $\mathbb{Z}[G]$ in the obvious way.

There's a G-equivariant surjection $\mathbb{Z}[G] \to \mathbb{Z}$ where $\mathbb{Z}$ has the trivial action, sending $\sum_i n_i g_i$ to $\sum_i n_i$. Let $aug(G)$ denote the kernel.

The G-module is both induced and coinduced so $H^n_{Tate}(G, \mathbb{Z}[G]) = 0$ for all n.

Conclusion: $H^n_{Tate}(G, \mathbb{Z}) = H^{n+1}_{Tate}(G, aug(G))$.

This is just a general fact, true for all finite groups G.

We're half way there.

Now say G is a finite group, M is a G-module and we have an element $\sigma \in H^2(G, M)$.

Lift this to a 2-cocycle $\tilde{\sigma} : G^2 \to M$.

We can use this data to construct a "splitting module" $split(\tilde{\sigma})$, which is an action of G on $M \times aug(G)$ with $g \bullet (m, f) = (g \bullet m + \sum_{\gamma \in G} f(\gamma)\tilde{\sigma}(g, \gamma), g \bullet f)$.

The 2-cocycle equation shows that this is an action.
There's a short exact sequence $0 \to M \to split(\tilde{\sigma}) \to aug(G) \to 0$.

So *if* $split(\sigma)$ has no Tate cohomology, we get an induced isomorphism $H^n_{Tate}(G, aug(G)) \to H^{n+1}_{Tate}(G, M)$ and hence an isomorphism $H^n_{Tate}(G, \mathbb{Z}) = H^{n+2}_{Tate}(G, M)$.

Of course this will not be true in general – this is general G and M.

The story so far

So far: If we have some cohomology class $\sigma \in H^2(G, M)$ lifting to a 2-cocycle $\tilde{\sigma}$ such that *split*$(\tilde{\sigma})$ has no Tate cohomology, then for all n we have isomorphisms $H^n_{Tate}(G, \mathbb{Z}) = H^{n+2}_{Tate}(G, M)$.

A theorem we proved (in the notes, not in Lean) in the Oxford workshop in June is that if it's true that for all finite degree d Galois extensions L/K of nonarchimedean local fields, $H^2(Gal(L/K), L^\times)$ is finite cyclic of order d generated by σ which lifts to the 2-cocycle $\tilde{\sigma}$, then *split*$(\tilde{\sigma})$ has no Tate cohomology.

Corollary: $H^{-2}_{Tate}(G, \mathbb{Z}) = H^0_{Tate}(G, L^\times)$ if L/K is a finite Galois extension of local fields, and thus $G^{ab} = K^\times / N(L^\times)$, which gives us the Artin map.

What's left?

A lot of the basics of this story are already formalized in Lean.
We do *not* have the hard theorem that $H^2(Gal(L/K), L^\times)$ is cyclic of size $d = [L : K]$ when K is nonarch local, and we need to work on this (and I didn't even tell you the proof yet).

But before we start on this, I want to formalize in Lean the construction of the Artin map, assuming that $split(\tilde{\sigma})$ has no Tate cohomology.

So let's start there.