Local Class Field Theory

Kevin Buzzard, Imperial College London

Imperial, 7th Nov 2025

Plan

This is the third of what will turn out to be 5 talks on local class field theory and how to teach it to Lean.

Plan

This is the third of what will turn out to be 5 talks on local class field theory and how to teach it to Lean.

The final two talks are on *Wed* 12th in 410 and Friday 21st in 642, both 1–3.

Plan

This is the third of what will turn out to be 5 talks on local class field theory and how to teach it to Lean.

The final two talks are on *Wed* 12th in 410 and Friday 21st in 642, both 1–3.

Plan for today: complete maths proof of upper bound for $H^2(L/K, L^\times)$ for L/K a finite Galois extension of local fields.

The story so far

Let K be a nonarchimedean local field.

The story so far

Let K be a nonarchimedean local field.

To “work out $Gal(K^{ab}/K)$” (the main point of local class field theory) most mathematicians would say that you have to prove a theorem.

The story so far

Let K be a nonarchimedean local field.

To “work out $Gal(K^{ab}/K)$” (the main point of local class field theory) most mathematicians would say that you have to prove a theorem.

But Lean (correctly) points out that identifying this object with another easier-to-understand object (the profinite completion of $K^\times$) involves making a *definition*.

The story so far

Let K be a nonarchimedean local field.

To "work out $Gal(K^{ab}/K)$" (the main point of local class field theory) most mathematicians would say that you have to prove a theorem.

But Lean (correctly) points out that identifying this object with another easier-to-understand object (the profinite completion of $K^\times$) involves making a *definition*.

After some work ("abstract theory of class formations") this boils down to giving explicit isomorphisms $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ where $d = [L : K] = |Gal(L/K)|$, for all finite Galois extensions L of all nonarch local fields K, and showing they satisfy some compatibility properties.

The story so far

Let K be a nonarchimedean local field.

To "work out $Gal(K^{ab}/K)$" (the main point of local class field theory) most mathematicians would say that you have to prove a theorem.

But Lean (correctly) points out that identifying this object with another easier-to-understand object (the profinite completion of $K^\times$) involves making a *definition*.

After some work ("abstract theory of class formations") this boils down to giving explicit isomorphisms $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ where $d = [L : K] = |Gal(L/K)|$, for all finite Galois extensions L of all nonarch local fields K, and showing they satisfy some compatibility properties.

Again this is not just a theorem, it is a definition and a theorem.

Fundamental classes

Let L/K be a finite Galois extension of nonarchimedean local fields, of degree d, and let G be its Galois group.

Fundamental classes

Let L/K be a finite Galois extension of nonarchimedean local fields, of degree d, and let G be its Galois group.

The strategy for constructing the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ is:

Fundamental classes

Let L/K be a finite Galois extension of nonarchimedean local fields, of degree d, and let G be its Galois group.

The strategy for constructing the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ is:

(1) Prove $|H^2(G, L^\times)| \leq d$ (note: still not obvious that it's finite)
(2) Write down a concrete element of order d (the "fundamental class").

Fundamental classes

Let L/K be a finite Galois extension of nonarchimedean local fields, of degree d, and let G be its Galois group.

The strategy for constructing the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ is:

(1) Prove $|H^2(G, L^\times)| \leq d$ (note: still not obvious that it's finite)
(2) Write down a concrete element of order d (the "fundamental class").

Today I'll to (1) (note: this is a theorem).

Upper bounds for H^2

We will prove $|H^2(G, L^\times)| \leq d$ by dévissage.

Upper bounds for H^2

We will prove $|H^2(G, L^\times)| \leq d$ by dévissage.

A (Cyclic): For all finite degree d Galois extensions L/K of nonarch local fields such that $G = Gal(L/K)$ is cyclic, $|H^2(G, L^\times)| \leq d$.

B (Solvable): For all finite degree d Galois extensions L/K of nonarch local fields such that $G = Gal(L/K)$ is solvable, $|H^2(G, L^\times)| \leq d$.

C (General): For all finite degree d Galois extensions L/K of nonarch local fields with $G = Gal(L/K)$, $|H^2(G, L^\times)| \leq d$.

Upper bounds for H^2

We will prove $|H^2(G, L^\times)| \leq d$ by dévissage.

A (Cyclic): For all finite degree d Galois extensions L/K of nonarch local fields such that $G = Gal(L/K)$ is cyclic, $|H^2(G, L^\times)| \leq d$.

B (Solvable): For all finite degree d Galois extensions L/K of nonarch local fields such that $G = Gal(L/K)$ is solvable, $|H^2(G, L^\times)| \leq d$.

C (General): For all finite degree d Galois extensions L/K of nonarch local fields with $G = Gal(L/K)$, $|H^2(G, L^\times)| \leq d$.

Strategy:
1) B implies C (started this last time)
2) A implies B
3) A is true.

B implies C

The key tool we need for B implies C is the theory of corestriction.

B implies C

The key tool we need for B implies C is the theory of corestriction.

If G is a group and S is a subgroup and M is a G-module, it's easy to check that there's a restriction map $H^n(G, M) \to H^n(S, M)$ (you just restrict an n-cochain $G^n \to M$ to S^n and get an n-cochain, and check it sends cocycles to cocycles and coboundaries to coboundaries).

B implies C

The key tool we need for B implies C is the theory of corestriction.

If G is a group and S is a subgroup and M is a G-module, it's easy to check that there's a restriction map $H^n(G, M) \to H^n(S, M)$ (you just restrict an n-cochain $G^n \to M$ to S^n and get an n-cochain, and check it sends cocycles to cocycles and coboundaries to coboundaries).

Last time I showed that if S has finite index in G then there's a corestriction map (like a norm or trace map) defined on H^0 by sending $x \in M^S$ to $\sum g_i x$ where $G = \coprod_i g_i S$.

B implies C

The key tool we need for B implies C is the theory of corestriction.

If G is a group and S is a subgroup and M is a G-module, it's easy to check that there's a restriction map $H^n(G, M) \to H^n(S, M)$ (you just restrict an n-cochain $G^n \to M$ to S^n and get an n-cochain, and check it sends cocycles to cocycles and coboundaries to coboundaries).

Last time I showed that if S has finite index in G then there's a corestriction map (like a norm or trace map) defined on H^0 by sending $x \in M^S$ to $\sum g_i x$ where $G = \coprod_i g_i S$.

To get $H^n(S, M) \to H^n(G, M)$ we use dimension shifting.

B implies C

The key tool we need for B implies C is the theory of corestriction.

If G is a group and S is a subgroup and M is a G-module, it's easy to check that there's a restriction map $H^n(G, M) \to H^n(S, M)$ (you just restrict an n-cochain $G^n \to M$ to S^n and get an n-cochain, and check it sends cocycles to cocycles and coboundaries to coboundaries).

Last time I showed that if S has finite index in G then there's a corestriction map (like a norm or trace map) defined on H^0 by sending $x \in M^S$ to $\sum g_i x$ where $G = \coprod_i g_i S$.

To get $H^n(S, M) \to H^n(G, M)$ we use dimension shifting.

Summary of idea: $0 \to M \to I \to up(M) \to 0$ with $H^n(S, I) = 0$ for all $n \geq 1$ and all subgroups S of G.

B implies C

The key tool we need for B implies C is the theory of corestriction.

If G is a group and S is a subgroup and M is a G-module, it's easy to check that there's a restriction map $H^n(G,M) \to H^n(S,M)$ (you just restrict an n-cochain $G^n \to M$ to S^n and get an n-cochain, and check it sends cocycles to cocycles and coboundaries to coboundaries).

Last time I showed that if S has finite index in G then there's a corestriction map (like a norm or trace map) defined on H^0 by sending $x \in M^S$ to $\sum g_i x$ where $G = \coprod_i g_i S$.

To get $H^n(S,M) \to H^n(G,M)$ we use dimension shifting.

Summary of idea: $0 \to M \to I \to up(M) \to 0$ with $H^n(S,I) = 0$ for all $n \geq 1$ and all subgroups S of G.

Then $H^n(S, up(M)) \to H^{n+1}(S,M)$ is a surjection (and an isomorphism for $n \geq 1$), so if cores is defined on H^n you can define it on H^{n+1} too.

Key commutative diagram

$$\begin{tikzcd}
H^n(G, up(M)) \arrow[r, "\delta"] \arrow[d, "res"'] & H^{n+1}(G, M) \arrow[r, "0"] \arrow[d, "res"'] & 0 \\
H^n(S, up(M)) \arrow[r, "\delta"] \arrow[d, "cores"'] & H^{n+1}(S, M) \arrow[r] \arrow[d, "cores"'] & 0 \\
H^n(G, up(M)) \arrow[r, "\delta"] & H^{n+1}(G, M) \arrow[r] & 0
\end{tikzcd}$$

The bottom half of this diagram commutes by definition.

Key commutative diagram

$$\begin{array}{ccccc}
H^n(G, up(M)) & \xrightarrow{\delta} & H^{n+1}(G, M) & \xrightarrow{0} & 0 \\
\downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \\
H^n(S, up(M)) & \xrightarrow{\delta} & H^{n+1}(S, M) & \longrightarrow & 0 \\
\downarrow{\scriptstyle cores} & & \downarrow{\scriptstyle cores} & & \\
H^n(G, up(M)) & \xrightarrow{\delta} & H^{n+1}(G, M) & \longrightarrow & 0
\end{array}$$

The bottom half of this diagram commutes by definition.

The top half is an easy explicit calculation (res is a morphism of the complexes which compute group cohomology).

Key commutative diagram

$$
\begin{tikzcd}
H^n(G, up(M)) \arrow[r, "\delta"] \arrow[d, "res"'] & H^{n+1}(G, M) \arrow[r, "0"] \arrow[d, "res"'] & 0 \\
H^n(S, up(M)) \arrow[r, "\delta"] \arrow[d, "cores"'] & H^{n+1}(S, M) \arrow[r] \arrow[d, "cores"'] & 0 \\
H^n(G, up(M)) \arrow[r, "\delta"] & H^{n+1}(G, M) \arrow[r] & 0
\end{tikzcd}
$$

The bottom half of this diagram commutes by definition.

The top half is an easy explicit calculation (res is a morphism of the complexes which compute group cohomology).

Corollary: $cores(res(x)) = dx$ where d is the index of G in S.

Key commutative diagram

$$\begin{tikzcd}
H^n(G, up(M)) \arrow[r, "\delta"] \arrow[d, "res"'] & H^{n+1}(G, M) \arrow[r, "0"] \arrow[d, "res"'] & 0 \\
H^n(S, up(M)) \arrow[r, "\delta"] \arrow[d, "cores"'] & H^{n+1}(S, M) \arrow[r] \arrow[d, "cores"'] & 0 \\
H^n(G, up(M)) \arrow[r, "\delta"] & H^{n+1}(G, M) \arrow[r] & 0
\end{tikzcd}$$

The bottom half of this diagram commutes by definition.

The top half is an easy explicit calculation (res is a morphism of the complexes which compute group cohomology).

Corollary: $cores(res(x)) = dx$ where d is the index of G in S.

Proof: true when $n = 0$ by an explicit calculation ($gx = x$ if $x \in M^G$) and then true for all n by commutativity of the diagram.

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

I've been stressing that it's not at all obvious that $H^2(G, L^\times)$ is even finite.

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

I've been stressing that it's not at all obvious that $H^2(G, L^\times)$ is even finite.

But I claim that it's at least *torsion*, and more generally that if G is a finite group of size d and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $dx = 0$.

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

I've been stressing that it's not at all obvious that $H^2(G, L^\times)$ is even finite.

But I claim that it's at least *torsion*, and more generally that if G is a finite group of size d and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $dx = 0$.

Because if G is finite we can let $S = \{1\}$ and observe that $H^n(S, M) = 0$ for $n \geq 1$ as the trivial group has no higher cohomology (an easy calculation with n-chains).

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

I've been stressing that it's not at all obvious that $H^2(G, L^\times)$ is even finite.

But I claim that it's at least *torsion*, and more generally that if G is a finite group of size d and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $dx = 0$.

Because if G is finite we can let $S = \{1\}$ and observe that $H^n(S, M) = 0$ for $n \geq 1$ as the trivial group has no higher cohomology (an easy calculation with n-chains).

Global example: $H^2(Gal(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times)$ is an infinite-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$ (the Galois group is cyclic so Tate cohomology is periodic so it's $\mathbb{Q}^\times/N(\mathbb{Q}(i)^\times)$ so a basis is (-1) and all the primes which are 3 mod 4, as there's no solution to $a^2 + b^2 = 3$ etc).

Consequences

Say $G = Gal(L/K)$, with L/K a finite Galois extension of local fields.

I've been stressing that it's not at all obvious that $H^2(G, L^\times)$ is even finite.

But I claim that it's at least *torsion*, and more generally that if G is a finite group of size d and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $dx = 0$.

Because if G is finite we can let $S = \{1\}$ and observe that $H^n(S, M) = 0$ for $n \geq 1$ as the trivial group has no higher cohomology (an easy calculation with n-chains).

Global example: $H^2(Gal(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times)$ is an infinite-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$ (the Galois group is cyclic so Tate cohomology is periodic so it's $\mathbb{Q}^\times/N(\mathbb{Q}(i)^\times)$ so a basis is (-1) and all the primes which are 3 mod 4, as there's no solution to $a^2 + b^2 = 3$ etc).

So we still don't know H^2 is finite in the local case.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Say $P \subseteq G$ is a Sylow p-subgroup of G, so it's got size p^m.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Say $P \subseteq G$ is a Sylow p-subgroup of G, so it's got size p^m.

Say M is any G-module, and $n \geq 1$.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Say $P \subseteq G$ is a Sylow p-subgroup of G, so it's got size p^m.

Say M is any G-module, and $n \geq 1$.

We've just seen that all elements in the abelian (possibly infinite) group $H^n(G, M)$ are annihiliated by $p^m t$.

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Say $P \subseteq G$ is a Sylow p-subgroup of G, so it's got size p^m.

Say M is any G-module, and $n \geq 1$.

We've just seen that all elements in the abelian (possibly infinite) group $H^n(G, M)$ are annihiliated by $p^m t$.

Because p^m and t are coprime, an easy calculation shows $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$ (this is true for any torsion abelian groups).

Sylow subgroups

Here's another funky cohomological consequence, about restricting cohomology classes to Sylow subgroups.

Say G is a finite group of size $p^m t$, with p prime and coprime to t.

Say $P \subseteq G$ is a Sylow p-subgroup of G, so it's got size p^m.

Say M is any G-module, and $n \geq 1$.

We've just seen that all elements in the abelian (possibly infinite) group $H^n(G, M)$ are annihiliated by $p^m t$.

Because p^m and t are coprime, an easy calculation shows $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$ (this is true for any torsion abelian groups).

Here $X[d]$ denotes the kernel of multiplication by d on the additive abelian group X.

Sylow subgroups

G size $p^m t$, Sylow subgroup P size p^m.

Sylow subgroups

G size $p^m t$, Sylow subgroup P size p^m.

We have $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$.

Sylow subgroups

G size $p^m t$, Sylow subgroup P size p^m.

We have $H^n(G,M) = H^n(G,M)[p^m] \times H^n(G,M)[t]$.

I claim that restriction $H^n(G,M) \to H^n(P,M)$ induces an *injection* $H^n(G,M)[p^m] \to H^n(P,M)$.

Sylow subgroups

G size $p^m t$, Sylow subgroup P size p^m.

We have $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$.

I claim that restriction $H^n(G, M) \to H^n(P, M)$ induces an *injection* $H^n(G, M)[p^m] \to H^n(P, M)$.

Because if you then compose with *cores* : $H^n(P, M) \to H^n(G, M)$ you get multiplication by t, which is injective on the p^m-torsion.

Sylow subgroups

G size $p^m t$, Sylow subgroup P size p^m.

We have $H^n(G,M) = H^n(G,M)[p^m] \times H^n(G,M)[t]$.

I claim that restriction $H^n(G,M) \to H^n(P,M)$ induces an *injection* $H^n(G,M)[p^m] \to H^n(P,M)$.

Because if you then compose with *cores* : $H^n(P,M) \to H^n(G,M)$ you get multiplication by t, which is injective on the p^m-torsion.

Rule of thumb: "Sylow subgroup of cohomology of a finite group injects into cohomology of Sylow subgroup".

B implies C

Now B implies C is easy.

B implies C

Now B implies C is easy.

Set-up: L/K a finite Galois extension of local fields, degree d, Galois group G, and let's assume that we know $|H^2(G, L^\times)| \leq d$ if G is solvable (i.e. assume B).

B implies C

Now B implies C is easy.

Set-up: L/K a finite Galois extension of local fields, degree d, Galois group G, and let's assume that we know $|H^2(G, L^\times)| \leq d$ if G is solvable (i.e. assume B).

Then we know this upper bound in general (i.e. C).

B implies C

Now B implies C is easy.

Set-up: L/K a finite Galois extension of local fields, degree d, Galois group G, and let's assume that we know $|H^2(G, L^\times)| \leq d$ if G is solvable (i.e. assume B).

Then we know this upper bound in general (i.e. C).

This is because if $p^m || d$ and P is a Sylow p-subgroup then $H^2(G, L^\times)[p^m]$ injects into $H^2(P, L^\times)$, and by Galois theory this is $H^2(Gal(L/M), L^\times)$ for some subextension M, and p-groups are solvable, so $|H^2(P, L^\times)| \leq p^m$ by B.

B implies C

Now B implies C is easy.

Set-up: L/K a finite Galois extension of local fields, degree d, Galois group G, and let's assume that we know $|H^2(G, L^\times)| \leq d$ if G is solvable (i.e. assume B).

Then we know this upper bound in general (i.e. C).

This is because if $p^m || d$ and P is a Sylow p-subgroup then $H^2(G, L^\times)[p^m]$ injects into $H^2(P, L^\times)$, and by Galois theory this is $H^2(Gal(L/M), L^\times)$ for some subextension M, and p-groups are solvable, so $|H^2(P, L^\times)| \leq p^m$ by B.

Repeat for all primes dividing $|G|$ and we're done.

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

The set-up with group cohomology, and many other cohomology theories, is that you have a natural number n and then two mathematical objects, the second one often depending on the first in some way.

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

The set-up with group cohomology, and many other cohomology theories, is that you have a natural number n and then two mathematical objects, the second one often depending on the first in some way.

In our case the objects are G and M.

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

The set-up with group cohomology, and many other cohomology theories, is that you have a natural number n and then two mathematical objects, the second one often depending on the first in some way.

In our case the objects are G and M.

Cohomology theory then gives you abelian groups $H^n(G, M)$.

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

The set-up with group cohomology, and many other cohomology theories, is that you have a natural number n and then two mathematical objects, the second one often depending on the first in some way.

In our case the objects are G and M.

Cohomology theory then gives you abelian groups $H^n(G, M)$.

Two basic questions you can ask about a cohomology theory are:

A implies B

Next step: if $|H^2(G, L^\times)| \leq d$ for cyclic groups G then it's true for solvable groups G (and in particular for Sylow subgroups, which are p-groups and thus solvable).

The main tool this is "higher inf-res".

Before I start on this, let me make some more general remarks about cohomology theories in general.

The set-up with group cohomology, and many other cohomology theories, is that you have a natural number n and then two mathematical objects, the second one often depending on the first in some way.

In our case the objects are G and M.

Cohomology theory then gives you abelian groups $H^n(G, M)$.

Two basic questions you can ask about a cohomology theory are:

1) How does it behave when M changes?
2) How does it behave when G changes?

Changing M

For changes to the second object (the “sheaf”), the theorem (which is present in a huge number of cohomology theories) is the existence of a long exact sequence.

Changing M

For changes to the second object (the “sheaf”), the theorem (which is present in a huge number of cohomology theories) is the existence of a long exact sequence.

In group cohomology, this manifests itself as follows:

Changing M

For changes to the second object (the “sheaf”), the theorem (which is present in a huge number of cohomology theories) is the existence of a long exact sequence.

In group cohomology, this manifests itself as follows:

If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then there's a long exact sequence

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to \cdots$$

$$\cdots \to H^n(G,B) \to H^n(G,C) \to H^{n+1}(G,A) \to H^{n+1}(G,B) \to \cdots .$$

Changing M

For changes to the second object (the “sheaf”), the theorem (which is present in a huge number of cohomology theories) is the existence of a long exact sequence.

In group cohomology, this manifests itself as follows:

If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then there’s a long exact sequence

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to \cdots$$

$$\cdots \to H^n(G,B) \to H^n(G,C) \to H^{n+1}(G,A) \to H^{n+1}(G,B) \to \cdots.$$

But what happens if we change G?

Changing G

If we change G things are much more subtle.

Changing G

If we change G things are much more subtle.

The fundamental construction, due to Hochschild and Serre for group cohomology, and due to Grothendieck (Tohoku paper) in huge generality, is the existence of a spectral sequence.

Changing G

If we change G things are much more subtle.

The fundamental construction, due to Hochschild and Serre for group cohomology, and due to Grothendieck (Tohoku paper) in huge generality, is the existence of a spectral sequence.

If G is a group, M is a G-module, and N is a *normal* subgroup of G, then there's a first quadrant spectral sequence $E_2^{i,j} = H^i(G/N, H^j(N, M)) => H^{i+j}(G, M)$.

Changing G

If we change G things are much more subtle.

The fundamental construction, due to Hochschild and Serre for group cohomology, and due to Grothendieck (Tohoku paper) in huge generality, is the existence of a spectral sequence.

If G is a group, M is a G-module, and N is a *normal* subgroup of G, then there's a first quadrant spectral sequence $E_2^{i,j} = H^i(G/N, H^j(N, M)) => H^{i+j}(G, M)$.

Any first quadrant spectral sequence gives rise to an exact sequence of terms of low degree, which for group cohomology is the "inf-res" exact sequence

$$0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M).$$

Changing G

If we change G things are much more subtle.

The fundamental construction, due to Hochschild and Serre for group cohomology, and due to Grothendieck (Tohoku paper) in huge generality, is the existence of a spectral sequence.

If G is a group, M is a G-module, and N is a *normal* subgroup of G, then there's a first quadrant spectral sequence $E_2^{i,j} = H^i(G/N, H^j(N, M)) => H^{i+j}(G, M)$.

Any first quadrant spectral sequence gives rise to an exact sequence of terms of low degree, which for group cohomology is the "inf-res" exact sequence

$$0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M).$$

The first map is inflation (the obvious map $G \to G/N$ gives a map from n-cochains $(G/N)^n \to M$ to n-cochains $G^n \to M$) and the second is restriction (restrict an n-cochain $G^n \to M$ to N^n).

One can extend things a little further (you can get to H^2 and just about to H^3) but you don't get a long exact sequence, you get something far more combinatorially complicated.

One can extend things a little further (you can get to H^2 and just about to H^3) but you don't get a long exact sequence, you get something far more combinatorially complicated.

$$0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M)^{G/N} \to H^2(G/N, M^N) \to$$
$$\to \ker\left(H^2(G, M) \to H^2(N, M)\right) \to H^1(G/N, H^1(N, M)) \to$$
$$\to \ker\left(H^3(G/N, M^N) \to H^3(G, M)\right)$$

and that's about it.

One can extend things a little further (you can get to H^2 and just about to H^3) but you don't get a long exact sequence, you get something far more combinatorially complicated.

$$0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M)^{G/N} \to H^2(G/N, M^N) \to$$
$$\to \ker\left(H^2(G, M) \to H^2(N, M)\right) \to H^1(G/N, H^1(N, M)) \to$$
$$\to \ker\left(H^3(G/N, M^N) \to H^3(G, M)\right)$$

and that's about it.

Exercise: learn what a spectral sequence is and then prove the above. Try and take it a step further.

One can extend things a little further (you can get to H^2 and just about to H^3) but you don't get a long exact sequence, you get something far more combinatorially complicated.

$$0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M)^{G/N} \to H^2(G/N, M^N) \to$$
$$\to \ker\left(H^2(G, M) \to H^2(N, M)\right) \to H^1(G/N, H^1(N, M)) \to$$
$$\to \ker\left(H^3(G/N, M^N) \to H^3(G, M)\right)$$

and that's about it.

Exercise: learn what a spectral sequence is and then prove the above. Try and take it a step further.

We will only need $0 \to H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M)$.

Hilbert 90

The modern interpretation of Hilbert's theorem 90 is that if L/K is a finite Galois extension of fields (not just local fields, this is general) with group G, then $H^1(G, L^\times) = 0$.

Hilbert 90

The modern interpretation of Hilbert's theorem 90 is that if L/K is a finite Galois extension of fields (not just local fields, this is general) with group G, then $H^1(G, L^\times) = 0$.

This claim is actually due to Noether; Hilbert only dealt with the case where G was cyclic.

Hilbert 90

The modern interpretation of Hilbert's theorem 90 is that if L/K is a finite Galois extension of fields (not just local fields, this is general) with group G, then $H^1(G, L^\times) = 0$.

This claim is actually due to Noether; Hilbert only dealt with the case where G was cyclic.

The proof of this is nonconstructive. Given a 1-cocycle (a twisted homomorphism $\sigma : G \to L^\times$ satisfying $\sigma(gh) = \sigma(g) \times g \bullet \sigma(h)$ for all g, h), one wants to prove it's a 1-coboundary and so one has to find a 0-cochain giving rise to it (i.e., an element $\lambda \in L^\times$ such that $\sigma(g) = g\lambda/\lambda$ for all g).

Hilbert 90

The modern interpretation of Hilbert's theorem 90 is that if L/K is a finite Galois extension of fields (not just local fields, this is general) with group G, then $H^1(G, L^\times) = 0$.

This claim is actually due to Noether; Hilbert only dealt with the case where G was cyclic.

The proof of this is nonconstructive. Given a 1-cocycle (a twisted homomorphism $\sigma : G \to L^\times$ satisfying $\sigma(gh) = \sigma(g) \times g \bullet \sigma(h)$ for all g, h), one wants to prove it's a 1-coboundary and so one has to find a 0-cochain giving rise to it (i.e., an element $\lambda \in L^\times$ such that $\sigma(g) = g\lambda/\lambda$ for all g).

The proof is to write down a certain K-linear map $L \to L$, argue that it can't be identically zero by linear independence of characters, and then choose something nonzero in the image and use this to create the nonzero element of L.

Hilbert 90

The modern interpretation of Hilbert's theorem 90 is that if L/K is a finite Galois extension of fields (not just local fields, this is general) with group G, then $H^1(G, L^\times) = 0$.

This claim is actually due to Noether; Hilbert only dealt with the case where G was cyclic.

The proof of this is nonconstructive. Given a 1-cocycle (a twisted homomorphism $\sigma : G \to L^\times$ satisfying $\sigma(gh) = \sigma(g) \times g \bullet \sigma(h)$ for all g, h), one wants to prove it's a 1-coboundary and so one has to find a 0-cochain giving rise to it (i.e., an element $\lambda \in L^\times$ such that $\sigma(g) = g\lambda/\lambda$ for all g).

The proof is to write down a certain K-linear map $L \to L$, argue that it can't be identically zero by linear independence of characters, and then choose something nonzero in the image and use this to create the nonzero element of L.

I use this example when constructivists ask me whether my proof of FLT can be made constructive.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

By Hilbert 90, $H^1(Gal(L/K), L^\times)$ and $H^1(Gal(M/K), M^\times)$ and $H^1(Gal(M/L), M^\times)$ are all zero.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

By Hilbert 90, $H^1(Gal(L/K), L^\times)$ and $H^1(Gal(M/K), M^\times)$ and $H^1(Gal(M/L), M^\times)$ are all zero.

So inf-res $0 \to H^1(G/N, (M^\times)^N) \to H^1(G, M^\times) \to H^1(N, M^\times)$ in this case tells us that $0 \to H^1(Gal(L/K), L^\times) \to H^1(Gal(M/K), M^\times) \to H^1(Gal(M/L), M^\times)$, but all these terms are zero.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

By Hilbert 90, $H^1(Gal(L/K), L^\times)$ and $H^1(Gal(M/K), M^\times)$ and $H^1(Gal(M/L), M^\times)$ are all zero.

So inf-res $0 \to H^1(G/N, (M^\times)^N) \to H^1(G, M^\times) \to H^1(N, M^\times)$ in this case tells us that $0 \to H^1(Gal(L/K), L^\times) \to H^1(Gal(M/K), M^\times) \to H^1(Gal(M/L), M^\times)$, but all these terms are zero.

I claim that
$0 \to H^2(Gal(L/K), L^\times) \to H^2(Gal(M/K), M^\times) \to H^2(Gal(M/L), M^\times)$ is exact, with the maps again being inflation and restriction.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

By Hilbert 90, $H^1(Gal(L/K), L^\times)$ and $H^1(Gal(M/K), M^\times)$ and $H^1(Gal(M/L), M^\times)$ are all zero.

So inf-res $0 \to H^1(G/N, (M^\times)^N) \to H^1(G, M^\times) \to H^1(N, M^\times)$ in this case tells us that $0 \to H^1(Gal(L/K), L^\times) \to H^1(Gal(M/K), M^\times) \to H^1(Gal(M/L), M^\times)$, but all these terms are zero.

I claim that
$0 \to H^2(Gal(L/K), L^\times) \to H^2(Gal(M/K), M^\times) \to H^2(Gal(M/L), M^\times)$ is exact, with the maps again being inflation and restriction.

One proof is: trivial from the spectral sequence.

Higher inf-res

Now say $M/L/K$ are local fields, with M/K and L/K Galois, so by Galois theory we have a group $G = Gal(M/K)$ and a normal subgroup $N = Gal(M/L)$.

By Hilbert 90, $H^1(Gal(L/K), L^\times)$ and $H^1(Gal(M/K), M^\times)$ and $H^1(Gal(M/L), M^\times)$ are all zero.

So inf-res $0 \to H^1(G/N, (M^\times)^N) \to H^1(G, M^\times) \to H^1(N, M^\times)$ in this case tells us that $0 \to H^1(Gal(L/K), L^\times) \to H^1(Gal(M/K), M^\times) \to H^1(Gal(M/L), M^\times)$, but all these terms are zero.

I claim that
$0 \to H^2(Gal(L/K), L^\times) \to H^2(Gal(M/K), M^\times) \to H^2(Gal(M/L), M^\times)$ is exact, with the maps again being inflation and restriction.

One proof is: trivial from the spectral sequence.

Here's a more concrete proof.

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0.$

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0.$

We know normal inf-res for $up(M^\times)$.

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0$.

We know normal inf-res for $up(M^\times)$.

So $0 \to H^1(L/K, up(M^\times)^{Gal(M/L)}) \to H^1(M/K, up(M^\times)) \to H^1(M/L, up(M^\times))$.

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0$.

We know normal inf-res for $up(M^\times)$.

So $0 \to H^1(L/K, up(M^\times)^{Gal(M/L)}) \to H^1(M/K, up(M^\times)) \to H^1(M/L, up(M^\times))$.

Because H^1 and H^2 vanish for $coind_1(M^\times)$ for all subgroups of $Gal(M/K)$, the last two terms are $H^2(M/K, M^\times)$ and $H^2(M/L, M^\times)$, by dimension shifting.

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0$.

We know normal inf-res for $up(M^\times)$.

So $0 \to H^1(L/K, up(M^\times)^{Gal(M/L)}) \to H^1(M/K, up(M^\times)) \to H^1(M/L, up(M^\times))$.

Because H^1 and H^2 vanish for $coind_1(M^\times)$ for all subgroups of $Gal(M/K)$, the last two terms are $H^2(M/K, M^\times)$ and $H^2(M/L, M^\times)$, by dimension shifting.

Furthermore $coind_1(M^\times)^{Gal(M/L)}$ also has trivial cohomology (we have this in the repo in some huge generality).

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0$.

We know normal inf-res for $up(M^\times)$.

So $0 \to H^1(L/K, up(M^\times)^{Gal(M/L)}) \to H^1(M/K, up(M^\times)) \to H^1(M/L, up(M^\times))$.

Because H^1 and H^2 vanish for $coind_1(M^\times)$ for all subgroups of $Gal(M/K)$, the last two terms are $H^2(M/K, M^\times)$ and $H^2(M/L, M^\times)$, by dimension shifting.

Furthermore $coind_1(M^\times)^{Gal(M/L)}$ also has trivial cohomology (we have this in the repo in some huge generality).

So the first term is $H^2(L/K, (M^\times)^{Gal(M/L)})$ and we're done.

Higher inf-res

Recall $0 \to M^\times \to coind_1(M^\times) \to up(M^\times) \to 0$.

We know normal inf-res for $up(M^\times)$.

So $0 \to H^1(L/K, up(M^\times)^{Gal(M/L)}) \to H^1(M/K, up(M^\times)) \to H^1(M/L, up(M^\times))$.

Because H^1 and H^2 vanish for $coind_1(M^\times)$ for all subgroups of $Gal(M/K)$, the last two terms are $H^2(M/K, M^\times)$ and $H^2(M/L, M^\times)$, by dimension shifting.

Furthermore $coind_1(M^\times)^{Gal(M/L)}$ also has trivial cohomology (we have this in the repo in some huge generality).

So the first term is $H^2(L/K, (M^\times)^{Gal(M/L)})$ and we're done.

Remark: there's a more general result of the form "if a bunch of cohomology groups vanish for $0 < i < n$ then inf-res works on H^n", and the proof is the same.

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

The proof is by induction on the length of a filtration on the group by subgroups each of which is normal in the next with cyclic quotient (existence of a filtration is exactly what makes a finite group solvable).

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

The proof is by induction on the length of a filtration on the group by subgroups each of which is normal in the next with cyclic quotient (existence of a filtration is exactly what makes a finite group solvable).

The base case $n = 0$ is trivial; the next case $n = 1$ is our assumption.

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L:K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

The proof is by induction on the length of a filtration on the group by subgroups each of which is normal in the next with cyclic quotient (existence of a filtration is exactly what makes a finite group solvable).

The base case $n = 0$ is trivial; the next case $n = 1$ is our assumption.

The inductive step: If N is a normal subgroup of $G = Gal(M/K)$ with cyclic quotient, and L is the corresponding intermediate field, then we have $0 \to H^2(L/K, L^\times) \to H^2(M/K, M^\times) \to H^2(M/L, L^\times)$ by higher inf-res.

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

The proof is by induction on the length of a filtration on the group by subgroups each of which is normal in the next with cyclic quotient (existence of a filtration is exactly what makes a finite group solvable).

The base case $n = 0$ is trivial; the next case $n = 1$ is our assumption.

The inductive step: If N is a normal subgroup of $G = Gal(M/K)$ with cyclic quotient, and L is the corresponding intermediate field, then we have $0 \to H^2(L/K, L^\times) \to H^2(M/K, M^\times) \to H^2(M/L, L^\times)$ by higher inf-res.

The first group has size at most $[L : K]$ by our inductive hypothesis, and the third has size at most $[M : L]$ by our assumption.

A implies B

We can now prove that if $|H^2(L/K, L^\times)| \leq [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions.

The proof is by induction on the length of a filtration on the group by subgroups each of which is normal in the next with cyclic quotient (existence of a filtration is exactly what makes a finite group solvable).

The base case $n = 0$ is trivial; the next case $n = 1$ is our assumption.

The inductive step: If N is a normal subgroup of $G = Gal(M/K)$ with cyclic quotient, and L is the corresponding intermediate field, then we have $0 \to H^2(L/K, L^\times) \to H^2(M/K, M^\times) \to H^2(M/L, L^\times)$ by higher inf-res.

The first group has size at most $[L : K]$ by our inductive hypothesis, and the third has size at most $[M : L]$ by our assumption.

Hence the middle has size at most the product, which is $[M : K]$, which is what we wanted.

Proof of A

Finally we actually need to prove that something is unconditionally true!

Proof of A

Finally we actually need to prove that something is unconditionally true!

We want: if $G = Gal(L/K)$ is a cyclic degree d extension of nonarch local fields then $|H^2(G, L^\times)| \leq d$.

Proof of A

Finally we actually need to prove that something is unconditionally true!

We want: if $G = Gal(L/K)$ is a cyclic degree d extension of nonarch local fields then $|H^2(G, L^\times)| \leq d$.

We will actually prove the stronger statement that $|H^2(G, L^\times)| = d$, because this is no harder.

Proof of A

Finally we actually need to prove that something is unconditionally true!

We want: if $G = Gal(L/K)$ is a cyclic degree d extension of nonarch local fields then $|H^2(G, L^\times)| \leq d$.

We will actually prove the stronger statement that $|H^2(G, L^\times)| = d$, because this is no harder.

Note: we still haven't proved that a single $H^2(Gal(L/K), L^\times)$ for $L \neq K$ is unconditionally finite yet! (We're always reducing).

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Then the group $\mathbb{Z}[G] = \mathbb{Z}[X]/(X^d - 1)$ is actually rather easy to work with.

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Then the group $\mathbb{Z}[G] = \mathbb{Z}[X]/(X^d - 1)$ is actually rather easy to work with.

In particular the constructions $0 \to M \to I \to up(M) \to 0$ and $0 \to down(M) \to J \to M \to 0$ which work in full generality (here I and J are induced/coinduced representations with no cohomology or homology) can be made explicit in this case.

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Then the group $\mathbb{Z}[G] = \mathbb{Z}[X]/(X^d - 1)$ is actually rather easy to work with.

In particular the constructions $0 \to M \to I \to up(M) \to 0$ and $0 \to down(M) \to J \to M \to 0$ which work in full generality (here I and J are induced/coinduced representations with no cohomology or homology) can be made explicit in this case.

Turns out that $up(M)$ and $down(M)$ are isomorphic as G-modules (see the blueprint).

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Then the group $\mathbb{Z}[G] = \mathbb{Z}[X]/(X^d - 1)$ is actually rather easy to work with.

In particular the constructions $0 \to M \to I \to up(M) \to 0$ and $0 \to down(M) \to J \to M \to 0$ which work in full generality (here I and J are induced/coinduced representations with no cohomology or homology) can be made explicit in this case.

Turns out that $up(M)$ and $down(M)$ are isomorphic as G-modules (see the blueprint).

Corollary: if $n \geq 1$ then $H^n(G, M) \cong H^{n+1}(G, down(M)) \cong H^{n+1}(G, up(M)) \cong H^{n+2}(G, M)$.

Periodicity

So let's say $G = Gal(L/K)$ is now finite cyclic of degree d.

Then the group $\mathbb{Z}[G] = \mathbb{Z}[X]/(X^d - 1)$ is actually rather easy to work with.

In particular the constructions $0 \to M \to I \to up(M) \to 0$ and $0 \to down(M) \to J \to M \to 0$ which work in full generality (here I and J are induced/coinduced representations with no cohomology or homology) can be made explicit in this case.

Turns out that $up(M)$ and $down(M)$ are isomorphic as G-modules (see the blueprint).

Corollary: if $n \geq 1$ then $H^n(G, M) \cong H^{n+1}(G, down(M)) \cong H^{n+1}(G, up(M)) \cong H^{n+2}(G, M)$.

Corollary: if n is any integer then $H^n_{Tate}(G, M) \cong H^{n+2}_{Tate}(G, M)$.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Note: from a topological point of view this shows that finite cyclic groups are infinite-dimensional.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Note: from a topological point of view this shows that finite cyclic groups are infinite-dimensional.

$H^1(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})$ is just the group homomorphisms $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ so if $d \geq 2$ this has size bigger than 1.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Note: from a topological point of view this shows that finite cyclic groups are infinite-dimensional.

$H^1(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})$ is just the group homomorphisms $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ so if $d \geq 2$ this has size bigger than 1.

Hence $H^n(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}) \neq 0$ for all $n \geq 1$ odd.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Note: from a topological point of view this shows that finite cyclic groups are infinite-dimensional.

$H^1(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})$ is just the group homomorphisms $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ so if $d \geq 2$ this has size bigger than 1.

Hence $H^n(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}) \neq 0$ for all $n \geq 1$ odd.

A topologist would say that group cohomology of G is singular cohomology of the classifying space BG of G.

Topological interpretation

Slogan: cohomology and homology of a finite cyclic group is periodic with period 2.

Note: from a topological point of view this shows that finite cyclic groups are infinite-dimensional.

$H^1(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z})$ is just the group homomorphisms $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ so if $d \geq 2$ this has size bigger than 1.

Hence $H^n(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}) \neq 0$ for all $n \geq 1$ odd.

A topologist would say that group cohomology of G is singular cohomology of the classifying space BG of G.

The classifying space of $\mathbb{Z}/2\mathbb{Z}$ is $\mathbb{P}^\infty_\mathbb{R}$, which explains why cohomology of projective space is periodic with period 2.

Herbrand quotients

If G is a finite cyclic group and M is an arbitrary G-module then we can define the *Herbrand quotient* $h_G(M)$ of M to be $|H^2(G, M)|/|H^1(G, M)|$ (a positive rational) if both of these groups are finite, and 0 (or "undefined") otherwise (Lean says 0).

Herbrand quotients

If G is a finite cyclic group and M is an arbitrary G-module then we can define the *Herbrand quotient* $h_G(M)$ of M to be $|H^2(G, M)|/|H^1(G, M)|$ (a positive rational) if both of these groups are finite, and 0 (or "undefined") otherwise (Lean says 0).

This is some kind of variant of the Euler characteristic.

Herbrand quotients

If G is a finite cyclic group and M is an arbitrary G-module then we can define the *Herbrand quotient* $h_G(M)$ of M to be $|H^2(G,M)|/|H^1(G,M)|$ (a positive rational) if both of these groups are finite, and 0 (or "undefined") otherwise (Lean says 0).

This is some kind of variant of the Euler characteristic.

In our application we want to prove $|H^2(Gal(L/K),L^\times)| = d$ for $Gal(L/K)$ cyclic degree d, and we know $H^1(Gal(L/K),L^\times) = 0$.

Herbrand quotients

If G is a finite cyclic group and M is an arbitrary G-module then we can define the *Herbrand quotient* $h_G(M)$ of M to be $|H^2(G,M)|/|H^1(G,M)|$ (a positive rational) if both of these groups are finite, and 0 (or "undefined") otherwise (Lean says 0).

This is some kind of variant of the Euler characteristic.

In our application we want to prove $|H^2(Gal(L/K),L^\times)| = d$ for $Gal(L/K)$ cyclic degree d, and we know $H^1(Gal(L/K),L^\times) = 0$.

So it will suffice to prove that $h_G(L^\times)$ is defined, and equal to d.

Multiplicativity

Recall $h_G(M)$ is $|H^2(G,M)|/|H^1(G,M)| \in \mathbb{Q}_{>0}$ if both are finite (and "undefined" or 0 otherwise).

Multiplicativity

Recall $h_G(M)$ is $|H^2(G,M)|/|H^1(G,M)| \in \mathbb{Q}_{>0}$ if both are finite (and "undefined" or 0 otherwise).

A pleasant diagram chase: if $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules and if two of $h_G(A)$, $h_G(B)$, $h_G(C)$ are nonzero, then so is the third, and $h_G(B) = h_G(A)h_G(C)$.

Multiplicativity

Recall $h_G(M)$ is $|H^2(G,M)|/|H^1(G,M)| \in \mathbb{Q}_{>0}$ if both are finite (and "undefined" or 0 otherwise).

A pleasant diagram chase: if $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules and if two of $h_G(A)$, $h_G(B)$, $h_G(C)$ are nonzero, then so is the third, and $h_G(B) = h_G(A)h_G(C)$.

Hence our claim $h_G(L^\times) = d$ will follow from the G-equivariant short exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ and the claims that $h_G(\mathcal{O}_L^\times) = 1$ and $h_G(\mathbb{Z}) = d$.

The case of $\mathbb{Z}$

The fact that $h_G(\mathbb{Z}) = d$ follows from an explicit calculation.

The case of $\mathbb{Z}$

The fact that $h_G(\mathbb{Z}) = d$ follows from an explicit calculation.

Note first that G acts trivially on $\mathbb{Z}$ because the Galois group preserves the valuation on L.

The case of $\mathbb{Z}$

The fact that $h_G(\mathbb{Z}) = d$ follows from an explicit calculation.

Note first that G acts trivially on $\mathbb{Z}$ because the Galois group preserves the valuation on L.

So $H^1(G, \mathbb{Z}) = Hom(G, \mathbb{Z}) = 0$.

The case of $\mathbb{Z}$

The fact that $h_G(\mathbb{Z}) = d$ follows from an explicit calculation.

Note first that G acts trivially on $\mathbb{Z}$ because the Galois group preserves the valuation on L.

So $H^1(G, \mathbb{Z}) = Hom(G, \mathbb{Z}) = 0$.

For $H^2(G, \mathbb{Z})$ it is possible to do a calculation, but one trick is just to use Tate cohomology, and say it is isomorphic to $H^0_{Tate}(G, \mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$.

The case of $\mathbb{Z}$

The fact that $h_G(\mathbb{Z}) = d$ follows from an explicit calculation.

Note first that G acts trivially on $\mathbb{Z}$ because the Galois group preserves the valuation on L.

So $H^1(G, \mathbb{Z}) = Hom(G, \mathbb{Z}) = 0$.

For $H^2(G, \mathbb{Z})$ it is possible to do a calculation, but one trick is just to use Tate cohomology, and say it is isomorphic to $H^0_{Tate}(G, \mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$.

So $h_G(\mathbb{Z}) = d$.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

Remark: I have no idea what this size is.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

Remark: I have no idea what this size is.

Here's the strategy: find some finite index compact open Galois-stable subgroup $U \subseteq \mathcal{O}_L^\times$ for which we can prove $H^1(G, U) \cong H^2(G, U) \cong 0$.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

Remark: I have no idea what this size is.

Here's the strategy: find some finite index compact open Galois-stable subgroup $U \subseteq \mathcal{O}_L^\times$ for which we can prove $H^1(G, U) \cong H^2(G, U) \cong 0$.

Hence $h_G(U) = 1$.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

Remark: I have no idea what this size is.

Here's the strategy: find some finite index compact open Galois-stable subgroup $U \subseteq \mathcal{O}_L^\times$ for which we can prove $H^1(G, U) \cong H^2(G, U) \cong 0$.

Hence $h_G(U) = 1$.

Then prove $h_G(\mathcal{O}_L^\times / U) = 1$.

What remains

All we have to do is to check that $h_G(\mathcal{O}_L^\times) = 1$.

In particular we now actually need to prove that the cohomology groups $H^1(G, \mathcal{O}_L^\times)$ and $H^2(G, \mathcal{O}_L^\times)$ are finite, and have equal size.

Remark: I have no idea what this size is.

Here's the strategy: find some finite index compact open Galois-stable subgroup $U \subseteq \mathcal{O}_L^\times$ for which we can prove $H^1(G, U) \cong H^2(G, U) \cong 0$.

Hence $h_G(U) = 1$.

Then prove $h_G(\mathcal{O}_L^\times / U) = 1$.

Then by multiplicativity we're done.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

Proof.

Say $G = \langle \sigma \rangle$.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

Proof.

Say $G = \langle \sigma \rangle$.

Then we have an exact sequence $0 \to H^0(G, M) \to M \to M \to H_0(G, M) \to 0$ where the middle map is $m \mapsto \sigma(m) - m$.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

Proof.

Say $G = \langle\sigma\rangle$.

Then we have an exact sequence $0 \to H^0(G, M) \to M \to M \to H_0(G, M) \to 0$ where the middle map is $m \mapsto \sigma(m) - m$.

Hence $|H^0(G, M)| = |H_0(G, M)|$ and both are finite.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

Proof.

Say $G = \langle \sigma \rangle$.

Then we have an exact sequence $0 \to H^0(G, M) \to M \to M \to H_0(G, M) \to 0$ where the middle map is $m \mapsto \sigma(m) - m$.

Hence $|H^0(G, M)| = |H_0(G, M)|$ and both are finite.

We also have an exact sequence
$0 \to H^{-1}_{Tate}(G, M) \to H_0(G, M) \to H^0(G, M) \to H^0_{Tate}(G, M) \to 0$
where the middle map is induced by the map
$m \mapsto Nm := (1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} m)$.

The case where M is finite.

Recall that G is always a finite cyclic group of order d.

Theorem

If M is a finite G-module then $h_G(M) = 1$.

Proof.

Say $G = \langle \sigma \rangle$.

Then we have an exact sequence $0 \to H^0(G, M) \to M \to M \to H_0(G, M) \to 0$ where the middle map is $m \mapsto \sigma(m) - m$.

Hence $|H^0(G, M)| = |H_0(G, M)|$ and both are finite.

We also have an exact sequence
$0 \to H^{-1}_{Tate}(G, M) \to H_0(G, M) \to H^0(G, M) \to H^0_{Tate}(G, M) \to 0$
where the middle map is induced by the map
$m \mapsto Nm := (1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} m)$.

Hence $|H^0_{Tate}(G, M)| = |H^{-1}_{Tate}(G, M)|$ and both are finite. $\square$

Consequence

Consequence: if $U \subseteq \mathcal{O}_L^\times$ is compact and open and G-stable, then it has finite index (by compactness of $\mathcal{O}_L^\times$) (note: here we are using that L is a nonarchimedean local field and not just some random complete discrete valuation field).

Consequence

Consequence: if $U \subseteq \mathcal{O}_L^\times$ is compact and open and G-stable, then it has finite index (by compactness of $\mathcal{O}_L^\times$) (note: here we are using that L is a nonarchimedean local field and not just some random complete discrete valuation field).

Hence $h_G(\mathcal{O}_L^\times/U) = 1$ by the previous argument.

Consequence

Consequence: if $U \subseteq \mathcal{O}_L^\times$ is compact and open and G-stable, then it has finite index (by compactness of $\mathcal{O}_L^\times$) (note: here we are using that L is a nonarchimedean local field and not just some random complete discrete valuation field).

Hence $h_G(\mathcal{O}_L^\times/U) = 1$ by the previous argument.

So it suffices to prove $h_G(U) = 1$.

Consequence

Consequence: if $U \subseteq \mathcal{O}_L^\times$ is compact and open and G-stable, then it has finite index (by compactness of $\mathcal{O}_L^\times$) (note: here we are using that L is a nonarchimedean local field and not just some random complete discrete valuation field).

Hence $h_G(\mathcal{O}_L^\times/U) = 1$ by the previous argument.

So it suffices to prove $h_G(U) = 1$.

And we'll do this by proving that for a carefully-chosen U we have $H^1(G, U) = H^2(G, U) = 0$.

What remains

We have still never computed an H^2 of an uncountable thing.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

The argument: we have L/K finite Galois, so by the normal basis theorem there's some $a \in L$ such that ga as g runs through G are a K-basis for L.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

The argument: we have L/K finite Galois, so by the normal basis theorem there's some $a \in L$ such that ga as g runs through G are a K-basis for L.

Note: this theorem is true for all finite Galois extensions (not just local fields), but has some content.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

The argument: we have L/K finite Galois, so by the normal basis theorem there's some $a \in L$ such that ga as g runs through G are a K-basis for L.

Note: this theorem is true for all finite Galois extensions (not just local fields), but has some content.

Multiplying a by a large power of π_K, we can assume that $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

The argument: we have L/K finite Galois, so by the normal basis theorem there's some $a \in L$ such that ga as g runs through G are a K-basis for L.

Note: this theorem is true for all finite Galois extensions (not just local fields), but has some content.

Multiplying a by a large power of π_K, we can assume that $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$.

By further multiplying by powers of π_K we can assume that $B \cdot B \subseteq \pi_K B$.

What remains

We have still never computed an H^2 of an uncountable thing.

And the computation is rather delicate.

The argument: we have L/K finite Galois, so by the normal basis theorem there's some $a \in L$ such that ga as g runs through G are a K-basis for L.

Note: this theorem is true for all finite Galois extensions (not just local fields), but has some content.

Multiplying a by a large power of π_K, we can assume that $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$.

By further multiplying by powers of π_K we can assume that $B \cdot B \subseteq \pi_K B$.

I claim that $U := 1 + B \subseteq \mathcal{O}_L^\times$ has $H^1(G, U) = H^2(G, U) = 0$.

Vanishing cohomology

We have $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$ with a small, and I claim $U := 1 + B$ works.

Vanishing cohomology

We have $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$ with a small, and I claim $U := 1 + B$ works.

The reason for this is that U has a filtration $U = 1 + B \supset 1 + \pi_K B \supset 1 + \pi_K^2 B \supset \cdots$ and all the quotients $1 + \pi_K^n B / 1 + \pi_K^{n+1} B$ are isomorphic to $B/\pi_K B = (\mathcal{O}_K/\pi_K)[G]$ via $1 + \pi_K^n b \mapsto b$.

Vanishing cohomology

We have $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$ with a small, and I claim $U := 1 + B$ works.

The reason for this is that U has a filtration $U = 1 + B \supset 1 + \pi_K B \supset 1 + \pi_K^2 B \supset \cdots$ and all the quotients $1 + \pi_K^n B / 1 + \pi_K^{n+1} B$ are isomorphic to $B/\pi_K B = (\mathcal{O}_K/\pi_K)[G]$ via $1 + \pi_K^n b \mapsto b$.

So all of the quotients are induced G-modules and have no cohomology in any degree $n \geq 1$.

Vanishing cohomology

We have $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$ with a small, and I claim $U := 1 + B$ works.

The reason for this is that U has a filtration $U = 1 + B \supset 1 + \pi_K B \supset 1 + \pi_K^2 B \supset \cdots$ and all the quotients $1 + \pi_K^n B / 1 + \pi_K^{n+1} B$ are isomorphic to $B/\pi_K B = (\mathcal{O}_K/\pi_K)[G]$ via $1 + \pi_K^n b \mapsto b$.

So all of the quotients are induced G-modules and have no cohomology in any degree $n \geq 1$.

Thus by a limiting argument (which Kenny is formalizing) U also has no cohomology in any degree $n \geq 1$.

Vanishing cohomology

We have $B := \sum_g \mathcal{O}_K ga \subseteq \pi_K \mathcal{O}_L$ with a small, and I claim $U := 1 + B$ works.

The reason for this is that U has a filtration $U = 1 + B \supset 1 + \pi_K B \supset 1 + \pi_K^2 B \supset \cdots$ and all the quotients $1 + \pi_K^n B / 1 + \pi_K^{n+1} B$ are isomorphic to $B/\pi_K B = (\mathcal{O}_K/\pi_K)[G]$ via $1 + \pi_K^n b \mapsto b$.

So all of the quotients are induced G-modules and have no cohomology in any degree $n \geq 1$.

Thus by a limiting argument (which Kenny is formalizing) U also has no cohomology in any degree $n \geq 1$.

The argument uses that not only can group cohomology be computed by a complex, but that this complex is functorial in the module and furthermore preserves all limits.

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

What's missing from the Lean?

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

What's missing from the Lean?

Edison is working on $cores(res(x)) = [G : S]x$.

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

What's missing from the Lean?

Edison is working on $cores(res(x)) = [G : S]x$.

The applications (cohomology in degree $n \geq 1$ is torsion, cohomology of Sylow subgroup contains Sylow subgroup of cohomology) are also not done.

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

What's missing from the Lean?

Edison is working on $cores(res(x)) = [G : S]x$.

The applications (cohomology in degree $n \geq 1$ is torsion, cohomology of Sylow subgroup contains Sylow subgroup of cohomology) are also not done.

Nobody is thinking about higher inf-res and I'm not sure we even have it stated in Lean.

That's it

That's all I'm going to say about the mathematics of the upper bound $|H^2(Gal(L/K), L^\times)| \leq d$.

What's missing from the Lean?

Edison is working on $cores(res(x)) = [G : S]x$.

The applications (cohomology in degree $n \geq 1$ is torsion, cohomology of Sylow subgroup contains Sylow subgroup of cohomology) are also not done.

Nobody is thinking about higher inf-res and I'm not sure we even have it stated in Lean.

We have the theory of Herbrand quotients and people are working on $H^1(G, U) = H^2(G, U) = 0$.