Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

Local Class Field Theory

Kevin Buzzard, Imperial College London

Imperial, 31st Oct 2025

Plan

I understand that the 1st year LSGNT students have something else at 3, so I'll wind down by 2:45.

Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

Plan

I understand that the 1st year LSGNT students have something else at 3, so I'll wind down by 2:45.

Plan is: first a reminder of last time, then a discussion of some technical details, then formalization of them.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time I claimed that $Gal(K^{ab}/K)$ was canonically isomorphic (in two ways) to the profinite completion of $K^{\times}$.

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time I claimed that $Gal(K^{ab}/K)$ was canonically isomorphic (in two ways) to the profinite completion of $K^\times$.

A key part of this claim is actually writing down the map.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time I claimed that $Gal(K^{ab}/K)$ was canonically isomorphic (in two ways) to the profinite completion of $K^\times$.

A key part of this claim is actually writing down the map.

More concretely, for all finite abelian extensions L of K we want a canonical map $K^\times \to Gal(L/K)$ with lots of nice compatibility properties.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time I claimed that $Gal(K^{ab}/K)$ was canonically isomorphic (in two ways) to the profinite completion of $K^\times$.

A key part of this claim is actually writing down the map.

More concretely, for all finite abelian extensions L of K we want a canonical map $K^\times \to Gal(L/K)$ with lots of nice compatibility properties.

This map is called the *Artin map*.

Last time

Let K be a nonarchimedean local field, and let K^{ab} be its maximal abelian extension.

Last time I claimed that $Gal(K^{ab}/K)$ was canonically isomorphic (in two ways) to the profinite completion of $K^\times$.

A key part of this claim is actually writing down the map.

More concretely, for all finite abelian extensions L of K we want a canonical map $K^\times \to Gal(L/K)$ with lots of nice compatibility properties.

This map is called the *Artin map*.

How to build it?

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

The Artin map

There is a *machine* called “the theory of abstract class formations” which builds the Artin map.

The Artin map

There is a *machine* called "the theory of abstract class formations" which builds the Artin map.

The machine takes an input isomorphisms $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ ($d = [L : K] = |Gal(L/K)|$) for all finite Galois extensions L/K of all nonarchimedean local fields K and produces Artin maps for all nonarchimedean local fields K.

The Artin map

There is a *machine* called "the theory of abstract class formations" which builds the Artin map.

The machine takes an input isomorphisms $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ ($d = [L : K] = |Gal(L/K)|$) for all finite Galois extensions L/K of all nonarchimedean local fields K and produces Artin maps for all nonarchimedean local fields K.

A conceptual 1-line explanation is: if $G = Gal(L/K)$ is abelian and $\sigma \in H^2(G, L^\times)$ corresponds to $1 \in \mathbb{Z}/d\mathbb{Z}$ then cup product with σ induces an isomorphism

$$G = H_1(G, \mathbb{Z}) = H^{-2}_{Tate}(G, \mathbb{Z}) \cong H^0_{Tate}(G, L^\times) = K^\times/N_{L/K}(L^\times)$$

and the Artin map is the inverse of this isomorphism.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

The Artin map

There is a *machine* called “the theory of abstract class formations” which builds the Artin map.

The machine takes an input isomorphisms $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ ($d = [L : K] = |Gal(L/K)|$) for all finite Galois extensions L/K of all nonarchimedean local fields K and produces Artin maps for all nonarchimedean local fields K.

A conceptual 1-line explanation is: if $G = Gal(L/K)$ is abelian and $\sigma \in H^2(G, L^\times)$ corresponds to $1 \in \mathbb{Z}/d\mathbb{Z}$ then cup product with σ induces an isomorphism

$$G = H_1(G, \mathbb{Z}) = H^{-2}_{Tate}(G, \mathbb{Z}) \cong H^0_{Tate}(G, L^\times) = K^\times/N_{L/K}(L^\times)$$

and the Artin map is the inverse of this isomorphism.

We actually wrote it down as $H^{-2}_{Tate}(G, \mathbb{Z}) \cong H^{-1}_{Tate}(G, aug(G)) \cong H^0_{Tate}(G, L^\times)$ where both isomorphisms are connecting homomorphisms in long exact sequences.

Today

Today I want to talk more about the isomorphism $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ for a finite Galois extension L/K of degree d.

Today

Today I want to talk more about the isomorphism $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ for a finite Galois extension L/K of degree d.

Because we've just seen that this is really the key construction.

Today

Today I want to talk more about the isomorphism $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ for a finite Galois extension L/K of degree d.

Because we've just seen that this is really the key construction.

Note that at this point in the argument we do not need to assume that $Gal(L/K)$ is abelian any more.

Today

Today I want to talk more about the isomorphism $H^2(Gal(L/K), L^\times) \cong \mathbb{Z}/d\mathbb{Z}$ for a finite Galois extension L/K of degree d.

Because we've just seen that this is really the key construction.

Note that at this point in the argument we do not need to assume that $Gal(L/K)$ is abelian any more.

But we certainly need to assume that K is a local field; this isn't true for K a number field, where the H^2 is much more complicated.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

And then we find an element of order d (this is the harder part).

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

And then we find an element of order d (this is the harder part).

Historically, results like this (especially the global analogues) were called "the first inequality" and "the second inequality".

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

And then we find an element of order d (this is the harder part).

Historically, results like this (especially the global analogues) were called "the first inequality" and "the second inequality".

It is unclear which inequality is the first one and which is the second (the conventions changed at some point).

Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

And then we find an element of order d (this is the harder part).

Historically, results like this (especially the global analogues) were called "the first inequality" and "the second inequality".

It is unclear which inequality is the first one and which is the second (the conventions changed at some point).

So I'll call them "the upper bound for H^2" and "the lower bound".

Strategy

Let L/K be a finite Galois extension of local fields with Galois group G of order d.

Here's the strategy to construct the isomorphism $H^2(G, L^\times) \cong \mathbb{Z}/d\mathbb{Z}$.

First we prove $|H^2(G, L^\times)| \leq d$.

And then we find an element of order d (this is the harder part).

Historically, results like this (especially the global analogues) were called "the first inequality" and "the second inequality".

It is unclear which inequality is the first one and which is the second (the conventions changed at some point).

So I'll call them "the upper bound for H^2" and "the lower bound".

Today let me talk about the upper bound $|H^2(G, L^\times)| \leq d$; next week I'll talk about constructing the element of order d which gives the lower bound.

The upper bound

So then the goal is this: Say L/K is a finite Galois extension of local fields with Galois group G and degree d.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

The upper bound

So then the goal is this: Say L/K is a finite Galois extension of local fields with Galois group G and degree d.

What we want: $|H^2(G, L^\times)| \leq d$ (note: it is not even obvious that $H^2(G, L^\times)$ is even finite; this will come out in the wash).

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

The upper bound

So then the goal is this: Say L/K is a finite Galois extension of local fields with Galois group G and degree d.

What we want: $|H^2(G, L^\times)| \leq d$ (note: it is not even obvious that $H^2(G, L^\times)$ is even finite; this will come out in the wash).

We will prove the result by "dévissage".

The upper bound

So then the goal is this: Say L/K is a finite Galois extension of local fields with Galois group G and degree d.

What we want: $|H^2(G, L^\times)| \leq d$ (note: it is not even obvious that $H^2(G, L^\times)$ is even finite; this will come out in the wash).

We will prove the result by “dévissage”.

First we prove it when G is cyclic, then when G is solvable (e.g., a p-group), and then for general G.

The upper bound

So then the goal is this: Say L/K is a finite Galois extension of local fields with Galois group G and degree d.

What we want: $|H^2(G, L^\times)| \leq d$ (note: it is not even obvious that $H^2(G, L^\times)$ is even finite; this will come out in the wash).

We will prove the result by "dévissage".

First we prove it when G is cyclic, then when G is solvable (e.g., a p-group), and then for general G.

In fact, it is traditional in dévissage arguments, to *reduce* from G general to G solvable to G cyclic, so let's do this.

Clarification of what we're doing

Consider the following three statements.

Clarification of what we're doing

Consider the following three statements.

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 $G = Gal(L/K)$, $|H^2(G, L^\times)| \leq d$.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Clarification of what we're doing

Consider the following three statements.

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 $G = Gal(L/K)$, $|H^2(G, L^\times)| \leq d$.

The two theorems I want to talk about today are:
1) B implies C
2) A implies B

Clarification of what we're doing

Consider the following three statements.

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 $G = Gal(L/K)$, $|H^2(G, L^\times)| \leq d$.

The two theorems I want to talk about today are:
1) B implies C
2) A implies B

Next week I'll explain why A is true, and we'll also construct the element of order d.

Preliminaries for B implies C

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

Preliminaries for 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).

Preliminaries for 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).

We have all this in mathlib.

Preliminaries for 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).

We have all this in mathlib.

More subtle is the theory of *corestriction*, which only works if S has finite index in G.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Preliminaries for 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).

We have all this in mathlib.

More subtle is the theory of *corestriction*, which only works if S has finite index in G.

We will define corestriction by dimension-shifting.

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Last week we twice saw the following phenomenon:

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Last week we twice saw the following phenomenon:

Trying to do something with $H^n(G, M)$.

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Last week we twice saw the following phenomenon:

Trying to do something with $H^n(G, M)$.

Come up with a short exact sequence $0 \to A \to B \to M \to 0$ or $0 \to M \to C \to D \to 0$ where B and C (the middle terms) have no higher cohomology.

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Last week we twice saw the following phenomenon:

Trying to do something with $H^n(G, M)$.

Come up with a short exact sequence $0 \to A \to B \to M \to 0$ or $0 \to M \to C \to D \to 0$ where B and C (the middle terms) have no higher cohomology.

Long exact sequence then tells us $H^n(G, M) \cong H^{n+1}(G, A)$ or $H^n(G, M) \cong H^{n-1}(G, D)$ so we can do something with cohomology of A or D instead.

Dimension shifting

Dimension-shifting is a common trick in group cohomology, and we saw two examples of it last week, but this week we'll see a powerful example.

Last week we twice saw the following phenomenon:

Trying to do something with $H^n(G, M)$.

Come up with a short exact sequence $0 \to A \to B \to M \to 0$ or $0 \to M \to C \to D \to 0$ where B and C (the middle terms) have no higher cohomology.

Long exact sequence then tells us $H^n(G, M) \cong H^{n+1}(G, A)$ or $H^n(G, M) \cong H^{n-1}(G, D)$ so we can do something with cohomology of A or D instead.

Last week we used this to define $H^n_{Tate}(G, \mathbb{Z}) \cong H^{n+2}(G, M)$ for example (using this trick twice, going via $H^{n+1}(G, aug(G))$).

Dimension shifting

This week we'll use a third short exact sequence

$$0 \to M \to coind_1(M) \to up(M) \to 0$$

where $coind_1(M)$ is simply the functions $G \to M$ with an appropriate action, the map sends $m \in M$ to the constant function and the cokernel is some random unwieldy thing which we'll call $up(M)$.

Dimension shifting

This week we'll use a third short exact sequence

$$0 \to M \to coind_1(M) \to up(M) \to 0$$

where $coind_1(M)$ is simply the functions $G \to M$ with an appropriate action, the map sends $m \in M$ to the constant function and the cokernel is some random unwieldy thing which we'll call $up(M)$.

The key point is that $coind_1(M)$ satisfies $H^n(S, coind_1(M)) = 0$ for all $S \subseteq G$ and for all $n \geq 1$.

Dimension shifting

This week we'll use a third short exact sequence

$$0 \to M \to coind_1(M) \to up(M) \to 0$$

where $coind_1(M)$ is simply the functions $G \to M$ with an appropriate action, the map sends $m \in M$ to the constant function and the cokernel is some random unwieldy thing which we'll call $up(M)$.

The key point is that $coind_1(M)$ satisfies $H^n(S, coind_1(M)) = 0$ for all $S \subseteq G$ and for all $n \geq 1$.

This means that $H^0(S, up(M)) \to H^1(S, M)$ is a surjection and $H^n(S, up(M)) \cong H^{n+1}(S, M)$ for all $n \geq 1$.

Corestriction

Set-up: G a group, $S \subseteq G$ a subgroup such that G is a finite union of left cosets $c_i S$, $1 \leq i \leq t$ (we say "S has index t").

Corestriction

Set-up: G a group, $S \subseteq G$ a subgroup such that G is a finite union of left cosets $c_i S$, $1 \leq i \leq t$ (we say "S has index t").

Let M be a G-module.

Corestriction

Set-up: G a group, $S \subseteq G$ a subgroup such that G is a finite union of left cosets c_iS, $1 \leq i \leq t$ (we say "S has index t").

Let M be a G-module.

We first define corestriction $H^0(S, M) \to H^0(G, M)$.

Corestriction

Set-up: G a group, $S \subseteq G$ a subgroup such that G is a finite union of left cosets $c_i S$, $1 \leq i \leq t$ (we say "S has index t").

Let M be a G-module.

We first define corestriction $H^0(S, M) \to H^0(G, M)$.

It sends $m \in M^S$ to $\sum_i c_i \bullet m$.

Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

Corestriction

Set-up: G a group, $S \subseteq G$ a subgroup such that G is a finite union of left cosets $c_i S$, $1 \leq i \leq t$ (we say "S has index t").

Let M be a G-module.

We first define corestriction $H^0(S, M) \to H^0(G, M)$.

It sends $m \in M^S$ to $\sum_i c_i \bullet m$.

Exercises:
(1) *cores* is independent of choice of coset reps, and a well-defined map to M^G.
(2) $cores(res(x)) = tx$ if $x \in H^0(G, M)$.

Dimension shifting

We'll now define *cores* : $H^n(S, M) \to H^n(G, M)$ by recursion (induction for data).

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Dimension shifting

We'll now define *cores* : $H^n(S, M) \to H^n(G, M)$ by recursion (induction for data).

We just did the base case.

Dimension shifting

We'll now define $cores : H^n(S, M) \to H^n(G, M)$ by recursion (induction for data).

We just did the base case.

Inductive step: if we've defined $cores : H^d(S, X) \to H^d(G, X)$ for all X, we now define $cores : H^{d+1}(S, M) \to H^{d+1}(G, M)$ by noting that $H^d(S, up(M)) \to H^{d+1}(S, M)$ is a surjection (and an isomorphism if $d > 0$), as is $H^d(G, up(M)) \to H^{d+1}(G, M)$ and we define cores to make square commute.

Dimension shifting

We'll now define $cores : H^n(S, M) \to H^n(G, M)$ by recursion (induction for data).

We just did the base case.

Inductive step: if we've defined $cores : H^d(S, X) \to H^d(G, X)$ for all X, we now define $cores : H^{d+1}(S, M) \to H^{d+1}(G, M)$ by noting that $H^d(S, up(M)) \to H^{d+1}(S, M)$ is a surjection (and an isomorphism if $d > 0$), as is $H^d(G, up(M)) \to H^{d+1}(G, M)$ and we define cores to make square commute.

Easy checks: *cores* is a functor, $cores(res(x)) = tx$ (induction on n). [Remark: I stopped now and we tried to do this in Lean; rest of the pdf wasn't covered in lecture 2]

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 t and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $tx = 0$.

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 t and M is any G-module (maybe infinite) and $n \geq 1$ and $x \in H^n(G, M)$ then $tx = 0$.

Because 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).

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 $p^m t$.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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 $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$.
(here $X[d]$ denotes the kernel of multiplication by d on the additive abelian group X).

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 $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$.
(here $X[d]$ denotes the kernel of multiplication by d on the additive abelian group X).

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

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 $H^n(G, M) = H^n(G, M)[p^m] \times H^n(G, M)[t]$.
(here $X[d]$ denotes the kernel of multiplication by d on the additive abelian group X).

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.

B implies C

Now B implies C is easy.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies 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. 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. B).

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

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies 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. 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 $|H^2(P, L^\times)| \leq p^m$.

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. 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 $|H^2(P, L^\times)| \leq p^m$.

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

A implies B

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) is “higher inf-res”.

A implies B

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) is “higher inf-res”.

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

A implies B

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) 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

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) 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

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) 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

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) 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

The main tool for A implies B (upper bounds for cyclic Galois groups implies upper bounds for solvable Galois groups) 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?

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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

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

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

Last time

Strategy

Corestriction

Dimension shifting

B implies C

inf-res

A implies B

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?

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

Changing G

If we change G things are much more subtle.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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).

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 but you don't get a long exact sequence, you get a spectral sequence which is more combinatorially complicated.

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 and a normal subgroup N.

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 and a normal subgroup N.

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.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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 and a normal subgroup N.

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 tells us literally nothing.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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 and a normal subgroup N.

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 tells us literally nothing.

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 and a normal subgroup N.

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 tells us literally nothing.

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.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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 and a normal subgroup N.

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 tells us literally nothing.

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.

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

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 $up(M^\times)^{Gal(M/L)}$ 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 $up(M^\times)^{Gal(M/L)}$ 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 $up(M^\times)^{Gal(M/L)}$ 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".

A implies B

The proof that A ("if $|H^2(L/K, L^\times)| = [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions") is now easy.

A implies B

The proof that A ("if $|H^2(L/K, L^\times)| = [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions") is now easy.

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

The proof that A ("if $|H^2(L/K, L^\times)| = [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions") is now easy.

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).

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

The proof that A ("if $|H^2(L/K, L^\times)| = [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions") is now easy.

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).

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.

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

Last time
Strategy
Corestriction
Dimension shifting
B implies C
inf-res
A implies B

A implies B

The proof that A ("if $|H^2(L/K, L^\times)| = [L : K]$ for all finite cyclic extensions of local fields, then it's also true for all finite solvable extensions") is now easy.

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).

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.

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

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