Formalizing Fermat, Lecture 3

Kevin Buzzard, Imperial College London

EPSRC TCC, 12th Feb 2026

Review

We're in the middle of a gruelling level 4.

Our current goal is to define what it means for a Galois representation to be *hardly ramified* (a bespoke definition for this course).

Last time we did unramified representations and the cyclotomic character.

So we have everything we need apart from Hopf algebras and flat representations.

Let's get back to Hopf algebras.

Review of Hopf algebras

Let R be a fixed commutative ring.

We consider only commutative R-algebras in this bit.

A (commutative co-commutative) *Hopf algebra* is an R-algebra A equipped with R-algebra homomorphisms $m^* : A \to A \otimes_R A$, $i^* : A \to A$ and $e^* : A \to R$ and satisfying some axioms.

Instead of giving the axioms, I tried to *motivate* them last time.

Hopf algebras

R, A an R-algebra, $m^* : A \to A \otimes_R A$, $i^* : A \to A$, $e^* : A \to R$.

Now let S be any R-algebra and define $G(S) := Hom_{R-alg}(A, S)$.

Then $G(S)$ is naturally a *set* and nothing more.

The extra Hopf algebra structure data on A induces $m : G(S) \times G(S) \to G(S)$, $i : G(S) \to G(S)$ and $e \in G(S)$.

The Hopf algebra axioms will force m to be an abelian group law with inverse i and identity e.

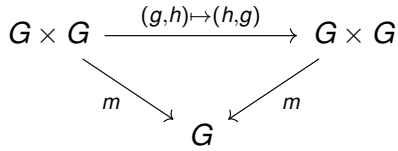
Let $s : R \to A$ be the structure map, and let $c : A \otimes_R A \to A$ be the R-algebra map sending $x \otimes y$ to xy.

Last time I showed that the axiom $gg^{-1} = 1$ for $G(S)$, for all S, is implied by the one equation $s \circ e^* = c \circ (1_A \otimes i^*) \circ m^*$ on A.

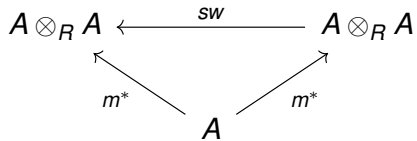
So that'll be one of the axioms for a Hopf algebra. Let's do another one.

An axiom

Consider the axiom $xy = yx$ for an abelian group.



So the corresponding Hopf algebra axiom will be commutativity of



where $sw : A \otimes_R A \to A \otimes_R A$ sends $a \otimes b$ to $b \otimes a$. Idea: if the bottom triangle commutes, applying $Hom(-, S)$ makes the top diagram commute.

The axioms

Here's a full list of axioms for a Hopf algebra.

Our data is $m^* : A \to A \otimes_R A$, $i^* : A \to A$ and $e^* : A \to R$.

Other R-algebra maps: $s : R \to A$ canonical, $c : A \otimes_R A \to A$ satisfies $c(x \otimes y) = xy$, $sw : A \otimes_R A \to A \otimes_R A$ satisfies $sw(a \otimes b) = b \otimes a$, and $i : (A \otimes_R A) \otimes_R A \cong A \otimes_R (A \otimes_R A)$ and $j : A \cong R \otimes_R A$ the canonical isomorphisms.

The axioms:

- $(xy = yx) : sw \circ m^* = m^*$;
- $((xy)z = x(yz)) : i \circ (m^* \otimes id) \circ m^* = (id \otimes m^*) \circ m^*$;
- $(gg^{-1} = 1) : s \circ e^* = c \circ (1_A \otimes i^*) \circ m^*$;
- $(1g = g) : (e^* \otimes id) \circ m^* = j$.

Upshot: if A is a Hopf R-algebra then for any R-algebra S we have a natural abelian group structure on $Hom_{R-alg}(A, S)$.

Example

Here's an example of a Hopf algebra.

Let R be any commutative ring base and let A be the finite free R-algebra $R[X]/(X^n - 1)$.

If S is any commutative R-algebra and $G(S) = Hom_{R-alg}(A, S)$ then we can identify $G(S)$ with the nth roots of unity in S (send $f : A \to S$ to $f(X)$).

The nth roots of unity in a commutative ring are a group under multiplication.

If $m^* : R[X]/(X^n - 1) \to R[Y, Z]/(Y^n - 1, Z^n - 1) \cong A \otimes_R A$ sends X to YZ then the induced map $G(S) \times G(S) \to G(S)$ is multiplication on nth roots of unity.

Define i^* by $i^*(X) = X^{n-1} = X^{-1}$. Define $e^*(X) = 1$.

These induce the group structure on $G(S)$ for all R-algebras S, and we've made $R[X]/(X^n - 1)$ into a Hopf algebra.

Exercise: if M is any abelian group, make the Hopf algebra whose S-points $G(S)$ are group homomorphisms $M \to S^\times$. (We just did $M = \mathbb{Z}/n\mathbb{Z}$.)

From Hopf algebras to group functors

We saw in the first lecture that an elliptic curve E over a field K gives rise to two things:

(1) a group $E(L)$ for each K-field L;
(2) a group homomorphism $E(\phi) : E(L) \to E(M)$ for each morphism $\phi : L \to M$ of K-fields.

Furthermore, we had $E(id) = id$ and $E(\phi \circ \psi) = E(\phi) \circ E(\psi)$.

("E is a group functor on K-fields")

That set-up gave us an action of the group $\mathrm{Gal}(\overline{K}/K)$ on the abelian group $E(\overline{K})$ by "pure thought".

Let me convince you that Hopf algebras also give you a group functor, this time on commutative R-algebras.

From Hopf algebras to group functors

Say S and T are R-algebras, and $\phi : S \to T$ is an R-algebra morphism.

If A is an R-Hopf algebra and $G(S) := Hom_{R-alg}(A, S)$, $G(T)$ are the corresponding groups, then composition $f \mapsto \phi \circ f$ gives a map of *sets* $G(\phi) : G(S) \to G(T)$.

When is this a group homomorphism?

In other words, when does

$$\begin{array}{ccc} G(S) \times G(S) & \xrightarrow{m} & G(S) \\ {\scriptstyle G(\phi)\times G(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ G(T) \times G(T) & \xrightarrow[m]{} & G(T) \end{array}$$

commute?

From Hopf algebras to group functors

$\phi : S \to T$ an R-algebra map, $G(\phi) : G(S) \to G(T)$ sends f to $\phi \circ f$.

$$\begin{array}{ccc} G(S) \times G(S) & \xrightarrow{m} & G(S) \\ {\scriptstyle G(\phi)\times G(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ G(T) \times G(T) & \xrightarrow[m]{} & G(T) \end{array}$$

Say $\alpha : A \otimes_R A \to S$ is an element of $G(S) \times G(S)$.

Going right-then-down gives us the element $\phi \circ (\alpha \circ m^*)$ of $G(T)$.

Going down-then-right gives us $(\phi \circ \alpha) \circ m^*$.

So $G(\phi)$ is *automatically* a group homomorphism!

Clearly $G(id) = id$ (as $id \circ f = f$) and $G(\phi \circ \psi) = G(\phi) \circ G(\psi)$ (as $(\phi \circ \psi) \circ f = \phi \circ (\psi \circ f)$).

So the same yoga applies as in the elliptic curve case.

The yoga

An isomorphism $\phi : S \cong T$ of R-algebras has a two-sided inverse ψ such that $\phi\psi$ and $\psi\phi$ are the identity.

So $G(\phi) : G(S) \to G(T)$ is an isomorphism, with inverse $G(\psi)$.

So if our base R is a field K, any K-algebra isomorphism $g : \overline{K} \to \overline{K}$ gives us a group isomorphism $G(g) : G(\overline{K}) \to G(\overline{K})$.

We have $G(gh)x = G(g)G(h)x$ so we have a group action of $\mathrm{Gal}(\overline{K}/K)$ on $G(\overline{K})$.

Upshot: a Hopf algebra over K gives us an action of $\mathrm{Gal}(\overline{K}/K)$ on an abelian group $G(\overline{K})$.

In this generality, I am pretty sure that this action isn't in general continuous.

We'd better add some finiteness conditions onto A to fix this.

A finite free hypothesis

In our application of Hopf algebras we will only ever care about base rings R which are local and Noetherian (they will be finite extensions of $\mathbb{Q}_p$ or their integer rings).

So although everyone uses the word "flat" or "finite flat", we are just going to talk about finite *free* R-Hopf algebras, which just means Hopf algebras A which are finite and free as R-modules.

(the point, if you know about flatness: a finite flat R-module is free, if R is a Noetherian local ring.)

Let's see how this extra finiteness assumption permeates through the theory we've set up.

Associated Galois module

Say K is a field, and A is a finite free K-Hopf algebra.

We know that $G(\overline{K}) := Hom_{K-alg}(A, \overline{K})$ is an abelian group.

And we just saw that it has an action of $\mathrm{Gal}(\overline{K}/K)$. (in fact the action is just $g \bullet f := g \circ f$.)

I claim that finiteness of A implies that the abelian group $G(\overline{K})$ is finite, and that if we give it the discrete topology then the $\mathrm{Gal}(\overline{K}/K)$-action is continuous.

Let's check this now.

Finiteness of Galois module

We have K a field, A a finite free K-algebra.

The claim is that there are only finitely many K-algebra maps $A \to \overline{K}$.

Well if we choose a K-basis $\{e_1, e_2, \ldots, e_n\}$ of A, then a K-algebra map $A \to \overline{K}$ is K-linear so is determined by the images of the e_i.

Furthermore each e_i is the root of a monic degree n polynomial $f_i(X) \in K[X]$ (by Cayley–Hamilton).

So each e_i must be mapped to a root of $f_i(X)$ in $\overline{K}$, and there are only finitely many of these.

Conclusion: $Hom_{K-alg}(A, \overline{K})$ is a finite set.

Continuity

K a field, A a finite free K-Hopf algebra, G the associated abelian group functor.

We have an action of $\mathrm{Gal}(\overline{K}/K)$ on the finite abelian group $G(\overline{K})$.

Say $x \in G(\overline{K})$, so $x : A \to \overline{K}$ is a K-algebra map.

In particular x is K-linear so it's determined by $x(e_i)$ for $1 \leq i \leq n$.

These $x(e_i)$ generate a finite subextension L of $\overline{K}$.

The corresponding open subgroup $Gal(\overline{K}/L)$ fixes x.

Upshot: if our Hopf algebra A is finite and free over K, then stabilisers are open and the action of $\mathrm{Gal}(\overline{K}/K)$ on $G(\overline{K})$ is continuous.

Base change

It is a tedious but straightforward check that Hopf algebras base change.

In other words, say R is our base ring, A is an R-Hopf algebra, and R' is a commutative R-algebra.

Then I claim that the base changed R'-algebra $A' := A \otimes_R R'$ inherits a comultiplication, coinverse and counit which make it into an R'-Hopf algebra.

Example: the comultiplication $A' \to A' \otimes_{R'} A'$ is given by noting that $A' \otimes_{R'} A' = (A \otimes_R R') \otimes_{R'} (A \otimes_R R') \cong A \otimes_R A \otimes_R R'$.

So if $m^* : A \to A \otimes_R A$ then $m^* \otimes_R (id_{R'}) : A \otimes_R R' \to (A \otimes_R A) \otimes_R R'$ can be thought of as an R'-algebra map $A' \to A' \otimes_{R'} A'$.

etc etc.

Base change

Now say R is a commutative ring and A is a *finite free* R-Hopf algebra.

Then for R' a commutative R-algebra, $A' = A \otimes_R R'$ is a finite free R'-Hopf algebra.

So being finite and free is stable under base change.

Flatness

We are finally ready to give the last definitions we need in order to state the boss theorem for this chapter!

Let K be a finite extension of $\mathbb{Q}_p$.

Let $\mathcal{O}$ be its ring of integers.

If we have a finite free Hopf algebra over $\mathcal{O}$, we've just seen that we can base change it to K and then build a continuous action of $\mathrm{Gal}(\overline{K}/K)$ on a finite abelian group $G(\overline{K})$.

We say that a continuous action of $\mathrm{Gal}(\overline{K}/K)$ on a finite abelian group G is *flat* if it is isomorphic to a $\mathrm{Gal}(\overline{K}/K)$-module arising from a finite free Hopf algebra over $\mathcal{O}$ in this way.

Examples

Example: if $A = \mathcal{O}[X]/(X^n - 1)$ represents nth roots of unity, then A is finite and free over $\mathcal{O}$.

Its base change to K is $K[X]/(X^n - 1)$, the associated finite group is $G(\overline{K}) = \mu_n(\overline{K}) = \{x \in \overline{K} : x^n = 1\}$ under multiplication.

$\mathrm{Gal}(\overline{K}/K)$ acts in the obvious way, and so this is a flat $\mathrm{Gal}(\overline{K}/K)$-module.

Example: If M is a finite abelian group of size n and $A = Hom_{set}(M, \mathcal{O}) = \mathcal{O}^n$ as a ring, then the group structure on M induces a Hopf algebra structure on A.

For example $A \otimes_{\mathcal{O}} A \cong Hom_{set}(M^2, \mathcal{O})$, so multiplication $M^2 \to M$ induces $A \to A \otimes_{\mathcal{O}} A$.

There's a canonical identification $G(K) = M$ and $G(\overline{K}) = M$ with the $\mathrm{Gal}(\overline{K}/K)$-action being trivial.

So a finite abelian group with the trivial $\mathrm{Gal}(\overline{K}/K)$-action is also flat.

Flatness of Galois representations

We've seen what it means for a finite abelian group with a continuous $\mathrm{Gal}(\overline{K}/K)$-action to be flat.

Now let's talk about what it means for a Galois representation to be flat.

First, say R is a *finite* coefficient ring with the discrete topology (i.e., a finite local ring, for example $\mathbb{Z}/p^n\mathbb{Z}$), and V is a finite free R-module with the discrete topology.

Say K is a finite extension of $\mathbb{Q}_p$.

Say $\rho : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V)$ is a continuous Galois representation.

Then ρ gives rise to a continuous $\mathrm{Gal}(\overline{K}/K)$-action on the finite abelian group V (simply forget that V is an R-module).

We say that ρ is *flat* if this action is flat.

Note: we forget the R-module structure; flatness is just a property of the Galois action on the underlying abelian group.

Example

If K is a finite extension of $\mathbb{Q}_p$ and $\mu_{p^n}(\overline{K})$ denotes the p^nth roots of unity in K (a finite abelian group) with its obvious action of $\mathrm{Gal}(\overline{K}/K)$, then we just saw that this $\mathrm{Gal}(\overline{K}/K)$-module is flat.

Now choose a generator of the finite cyclic group $\mu_{p^n}(\overline{K})$, making it non-canonically $\mathbb{Z}/p^n\mathbb{Z}$.

The induced action of $\mathrm{Gal}(\overline{K}/K)$ on this $\mathbb{Z}/p^n\mathbb{Z}$ is via the mod p^n cyclotomic character $\chi_n : \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.

In particular, the mod p^n cyclotomic character $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{Z}/p^n\mathbb{Z})$ is flat.

Even though the cyclotomic character is highly ramified.

Slogan: for p-adic or mod p representations of p-adic fields, a “good” condition is “flat” rather than “unramified”.

Flatness

Here's yet another generalization of flatness.

Say K is a finite extension of $\mathbb{Q}_p$ and R is now a general coefficient ring (like $\mathbb{Z}_p$ for example).

So R might not be finite, but R is a projective limit of finite rings R/J as J runs through the open ideals of R.

Say V is a finite free R-module with the product topology, and $\rho : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V)$ is a continuous Galois representation.

We say that ρ is *flat* if for every open ideal J of R, the induced mod J representation $\rho \bmod J : \mathrm{Gal}(\overline{K}/K) \to Aut_{R/J}(V/J)$ is flat in the previous sense.

Who can spot an issue with this definition?

Flatness

If R is a *finite* coefficient ring then we now have *two* definitions of what it means for $\rho : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V)$ to be flat.

The first says "the $\mathrm{Gal}(\overline{K}/K)$-action on V is flat".

The second says "The $\mathrm{Gal}(\overline{K}/K)$-action on V/J for all ideals J of R is flat."

So the second definition looks stronger. However we have this:

Theorem

If M is a flat $\mathrm{Gal}(\overline{K}/K)$-module then any $\mathrm{Gal}(\overline{K}/K)$-stable submodule N is flat, and the quotient M/N by any $\mathrm{Gal}(\overline{K}/K)$-stable submodule is flat.

Proof.

Known in the 1980s (it's in section 2.1 of Raynaud's 1974 paper on group schemes of type $(p, p, \ldots, p)$). □

So the two definitions are equivalent. (this is provable from first principles and it will teach you a lot if you try.)

One more flatness fact

Final fact we'll need about finite flat $\mathrm{Gal}(\overline{K}/K)$-modules: product of two flat $\mathrm{Gal}(\overline{K}/K)$-modules is flat.

Proof: take the tensor product of the Hopf algebras (long but elementary check that this works).

Consequence: if $\rho_1 : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V_1)$ and $\rho_2 : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V_2)$ are flat then $\rho_1 \oplus \rho_2 : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V_1 \oplus V_2)$ is flat.

Example

If K is a finite extension of $\mathbb{Q}_p$ then the cyclotomic character $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p^\times$ is flat.

Indeed, the open ideals of $\mathbb{Z}_p$ are just the $p^n\mathbb{Z}_p$.

So we just need to check that the mod p^n cyclotomic characters are all flat, which we already did.

Hardly ramified representations

We are finally ready to define hardly ramified representations!

Let R be a coefficient ring with *odd* residue characteristic ℓ.

Let V be an R-module which is finite and free of rank 2.

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ be a continuous Galois representation.

Definition. We say that ρ is *hardly ramified* if it satisfies the following four conditions.

The first condition

We have $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ 2-dimensional.

The first condition is that the determinant of ρ is the cyclotomic character.

What does this mean?

The determinant of ρ is a map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to R^\times$.

But a coefficient ring with residue characteristic ℓ is a $\mathbb{Z}_\ell$-algebra.

So I just mean that the map factors through $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ via the canonical map $\mathbb{Z}_\ell \to R$.

The first condition is our only global condition.

(although by Kronecker–Weber we could write down local conditions which imply this.)

The second condition

The second condition is that ρ is unramified outside 2 and ℓ.

Recall that this means that if $p \neq 2, \ell$ is a prime, then one (or equivalently all) inertia groups $I_{(p)}$ are in the kernel of ρ.

So we now have local conditions at all primes other than 2 and ℓ.

The third condition

The third condition is that ρ is "flat at ℓ".

This is going to be a local condition at ℓ.

What does it mean though? We only defined flatness for representations of absolute Galois groups of finite extensions of $\mathbb{Q}_\ell$, not for $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We need to somehow get a local Galois representation from a global one.

Local v global Galois groups

Let K be a number field, with integers A, and let P be a maximal ideal of A.

The completion $A_P := \varprojlim A/P^nA$ of A at P is an integral domain with field of fractions K_P, a finite extension of $\mathbb{Q}_p$ if p is the characteristic of A/P.

Let's choose a separable closure $\overline{K}_P$ of K_P.

Then $\overline{K}_P$ is separably closed and contains a copy of K, so if we choose $\overline{K}$ a separable closure of K, then $\overline{K}$ embeds into $\overline{K}_P$.

In fact there are uncountably many ways to embed $\overline{K}$ into $\overline{K}_P$, but all of them have the same image (the separable closure of K in $\overline{K}_P$).

Let's fix an embedding of fields $\overline{K} \to \overline{K}_P$.

This lets us identify various local and global constructions.

Local v global Galois groups

K number field, A, P, $\overline{K}$, $\overline{A}$, A_P, K_P, $\overline{K}_P$.

Now the integral closure $\overline{A}_P$ of A_P in $\overline{K}_P$ is a local ring.

So we can look at the preimage of its maximal ideal in $\overline{A}$ and get a maximal ideal $\overline{P}$ containing P.

So now we have a global decomposition group $D_{\overline{P}} \subset \mathrm{Gal}(\overline{K}/K)$.

Moreover, any field automorphism of $\overline{K}_P$ fixing K_P induces an automorphism of the subfield $\overline{K}$, fixing K.

So we get a hugely non-canonical continuous group homomorphism $Gal(\overline{K}_P/K_P) \to \mathrm{Gal}(\overline{K}/K)$.

One can check that the image is the decomposition group $D_{\overline{P}}$ of $\mathrm{Gal}(\overline{K}/K)$, and the map sends the local inertia group to $I_{\overline{P}}$.

Different choices

A different choice of field embedding $\overline{K} \to \overline{K}_P$ gives a typically different map $Gal(\overline{K}_P/K_P) \to \mathrm{Gal}(\overline{K}/K)$.

But the image of any $\overline{K} \to \overline{K}_P$ will always be the separable closure of K in $\overline{K}_P$ so any two choices will differ by a K-automorphism of $\overline{K}$.

So two different maps $i_1, i_2 : Gal(\overline{K}_P/K_P) \to \mathrm{Gal}(\overline{K}/K)$ coming from different embeddings will give rise to some $g \in \mathrm{Gal}(\overline{K}/K)$ such that $i_2(x) = g i_1(x) g^{-1}$ for all x.

The third condition

We have $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_R(V)$.

We just defined a hugely non-canonical map $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We compose with this and get a map $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathit{Aut}_R(V)$.

The isomorphism class of this representation is independent of the choice of $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$. Because there's an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ conjugating one into the other.

The third condition for hardly ramified representations is that this local representation is flat in the sense defined before.

(That is, all quotients V/J for J an open ideal come from Hopf algebras over $\mathbb{Z}_\ell$.)

The fourth condition

The fourth condition is a local condition at 2, the only prime which we haven't considered yet.

We allow a little extra leeway at 2 – this is why we called it "hardly ramified".

First choose $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_2$ giving us a continuous group homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Composing with ρ we get a continuous representation $\rho_2 : Gal(\overline{\mathbb{Q}}_2/\mathbb{Q}_2) \to Aut_R(V)$.

The condition at 2 is that there a free rank 1 $Gal(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-stable submodule W of V such that the induced 1-dimensional representation ψ of $Gal(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ on the quotient V/W is unramified (that is, has I_2 in its kernel) and satisfies $\psi^2 = 1$.

The fourth condition

The fourth condition: there is an unramified character ψ of $Gal(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ satisfying $\psi^2 = 1$ and a choice of basis such that

So $\rho_2 \cong \begin{pmatrix} \psi\chi & * \\ 0 & \psi \end{pmatrix}$

with χ cyclotomic and $*$ unspecified.

Hardly ramified

Summary:
A 2-dimensional representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_R(V)$ over a coefficient ring R with odd residue characteristic ℓ is *hardly ramified* if

1. $\mathit{det}(\rho) = \chi$;
2. ρ is unramified outside 2ℓ;
3. ρ is flat at ℓ;
4. ρ is upper-triangular at 2 with an unramified rank 1 quotient whose square is trivial.

Any questions on the definition of hardly ramified (because it's going to come up again and again)?

Your first question should be: *why?*

Here's the answer.

Frey curves

Let (a, b, c, ℓ) be a Frey package and let E be the associated Frey curve.

Let $\overline{\mathbb{Q}}$ be any algebraic closure of $\mathbb{Q}$.

Theorem
The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the 2-dimensional space* $E(\overline{\mathbb{Q}})[\ell]$ *is hardly ramified.*

Proof.
It's in that same 1987 Duke paper "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$" by Serre. □

Let me briefly say why this is true.

But this was known in the 1980s, so the following comments are off the record.

ℓ-torsion in Frey curve is hardly ramified

The global condition (determinant is cyclotomic) comes from the existence of the Weil pairing on an elliptic curve.

The fact that the representation is unramified away from the primes dividing $2\ell abc$ is because the curve is unramified at these primes.

The fact that it is unramified at primes not equal to 2 or ℓ but dividing abc is a consequence of the theory of the Tate curve (the Frey curve is semistable at these primes by pairwise coprimality of a, b, c).

The fact that the behaviour at 2 is hardly ramified is also a consequence of the theory of the Tate curve.

Let me say a little more about this; this is where the conditions $a = 3 \bmod 4$ and $b = 0 \bmod 2$ come in.

Condition at 2

The curve is $Y^2 = X(X - a^\ell)(X + b^\ell)$.

Change variables $X = 4x$ and $Y = 8y + 4x$ (so $x = X/4$, $y = (Y - X)/8$) to get $64y^2 + 64xy + 16x^2 = 4x(4x - a^\ell)(4x + b^\ell)$.

Now put $16x^2$ on the other side and multiply out.

We get $64y^2 + 64xy = 64x^3 + 16x^2(b^\ell - a^\ell - 1) - 4xa^\ell b^\ell$.

Because $2 \mid b$ and $\ell \geq 5$ (by definition of a Frey package) we have $32 \mid b^\ell$, and because $-a$ is 1 mod 4 we have $4 \mid (b^\ell - a^\ell - 1)$, so we can divide out a factor of 64.

We get $y^2 + xy = x^3 + ix^2 - ex$ where i is an integer and e is an even integer.

Mod 2 there are no linear terms (so the cubic is singular at the origin) but the quadratic part is $y^2 + xy = x^2$ or $y^2 + xy = 0$ so it's an ordinary double point.

Thus the theory of the Tate curve applies; one checks that the reduction is split iff i is even iff $a = 7$ mod 8.

Condition at ℓ

Finally there's the condition at ℓ (which is odd by assumption).

We need to check that the ℓ-torsion in the Frey curve is flat.

If $\ell \nmid abc$ (historically called "the first case") then E has good reduction at ℓ and flatness is a standard fact.

If $\ell \mid abc$ then again by the theory of the Tate curve the Galois representation is locally an extension of the trivial representation by the cyclotomic character.

An extension of a flat representation by another flat representation might not be flat :-/

But the extension is given by taking the root of a unit (as $v_\ell(j_E)$ is a multiple of ℓ) and again this can be checked to be flat.

All of this was known in the 1980s so I'll go into no more detail.

Thinking about hardly ramified representations

We just spent ages defining what it means for a 2-dimensional Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ over a coefficient ring R to be hardly ramified.

Now say $\ell \geq 5$ is a prime, V is a 2-dimensional vector space over $R = \mathbb{Z}/\ell\mathbb{Z}$ and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathbb{Z}/\ell\mathbb{Z}}(V)$ is a continuous hardly-ramified Galois representation.

What could ρ be? It could come from a Frey curve – but there are no Frey curves!

Well one concrete example is $\rho = 1 \oplus \chi$, the direct sum of the trivial character and the cyclotomic character.

Indeed, the contents of this and the previous lecture imply that this representation is hardly ramified.

What about other examples?

Examples of hardly ramified representations?

Because we allow some ramification at 2, maybe there are also non-split extensions of the trivial representation by the cyclotomic extension which are hardly ramified.

(Probably one could allow an ℓth root of 2 sometimes.)

But again this is a reducible representation.

Can we find an irreducible hardly ramified representation?

The kernel of such a representation cuts out a number field unramified outside 2 and ℓ and with strong constraints at these primes too.

So it's hard for such an extension to have a complicated Galois group like $GL_2(\mathbb{Z}/\ell\mathbb{Z})$.

The level 4 boss

Indeed the level 4 boss says that this can't happen.

Say $\ell \geq 5$ is a prime, V is a 2-dimensional vector space over $R = \mathbb{Z}/\ell\mathbb{Z}$ and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathbb{Z}/\ell\mathbb{Z}}(V)$ is a continuous hardly-ramified Galois representation.

Statement B4: Any such ρ is reducible.

(Remark: reducibility is implied by the conjecture Serre makes in his 1987 paper, but Serre's conjecture was not proved until the 21st century)

Theorem (boss theorem): Statement B4 implies FLT.

Note that we already proved in level 3 that B3 implied FLT, so all we need to do is to prove that B4 implies B3.

However we've probably forgotten what B3 was.

B4 implies B3

Reminder of B3 (which we know from level 3 implies FLT modulo 1980s):

B3: If E is the Frey curve associated to a Frey package (a, b, c, ℓ) then then $E[\ell]$ is reducible.

Reminder of B4:

B4: if $\ell \geq 5$ then any continuous hardly-ramified representation over $\mathbb{Z}/\ell\mathbb{Z}$ is reducible.

Proof of level 4 boss theorem:

It suffices to prove that B4 implies B3. So assume B4 and let E be a Frey curve. Then $E[\ell]$ is hardly ramified, by Serre. So it's reducible by B4. QED.

Moral of level 4: it is not the destination, it is the journey.

That is the last we'll see of Frey curves (but not the last we'll see of elliptic curves).

Level 4 epilogue

After our journey through the definitions of level 4, we are much stronger.

In Level 4 we reduced FLT to proving B4: a hardly ramified 2-dimensional representation over $\mathbb{Z}/\ell\mathbb{Z}$ is reducible when $\ell \geq 5$.

As is pretty clear, this reduction was known to Serre in 1987, and all the arguments in the course so far can be found in Serre's 1987 Duke paper "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$" or its references.

B4 was a consequence of the conjecture made by Serre in that paper, but was not known, in the 1980s.

Wiles' work does not prove B4 (it proved B3 using other techniques).

Serre's conjecture (which implies B4) was proved in the 21st century by Khare and Wintenberger.

We will be using simplifications of some of their ideas to prove B4.