Formalizing Fermat, Lecture 2

Kevin Buzzard, Imperial College London

EPSRC TCC, 5th Feb 2026

Review

So far we have proved the following thing.

Recall: a Frey Package is integers (a, b, c, p) with $p \geq 5$ prime, $a^p + b^p = c^p$ and some coprimality/congruence conditions.

Suppose (a, b, c, p) is a Frey package and $\overline{\mathbb{Q}}$ is any separable closure of $\mathbb{Q}$.

Suppose E is the Frey curve with defining polynomial $Y^2 - X(X - a^p)(X + b^p)$ associated to the package, and assume the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}})[p]$ is reducible.

Assume all theorems which were known in the 1980s (and in particular Mazur's 154 page theorem on torsion subgroups of elliptic curves over $\mathbb{Q}$).

Then Fermat's Last Theorem is true.

An apology

Last time I promised that today I would explain more about the route we're going to take to the proof.

However, level 4 needs *so many definitions* that in fact this lecture will be very definition-heavy.

Explanations about our general route to the top will have to take place next time.

This lecture is quite gruelling and will test your endurance.

Only the strongest will survive until next week.

Let's go.

Level 4: hardly ramified representations

"Hardly ramified representation" is another phrase which is unique to this course.

Being hardly ramified is a predicate on certain representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ where $\overline{\mathbb{Q}}$ is any separable closure of $\mathbb{Q}$.

Defining what "hardly ramified" means is a very long journey, but it is a fundamental concept in the proof we're formalizing.

In fact the concept was isolated as part of thinking about a natural way to explain the proof we're formalizing.

The definition will probably take the entire 2 hours.

Units of a monoid.

If R is a multiplicative monoid (e.g. a ring) (not necessarily commutative) then recall that the *units* $R^\times$ of R are $\{x : R \mid \exists y : R, xy = yx = 1\}$.

Easy check: the units of a monoid are a group.

The only lemma worth knowing about general monoids is the following:

Lemma

If M is a monoid, if $x \in M$, and if there exists $a, b \in M$ such that $ax = xb = 1$, then $a = b$ and hence x is a unit.

In other words, the units of a monoid are just the elements which have both left and right inverses.

Proof.

$a = a1 = a(xb) = (ax)b = 1b = b$. □

Remark: I love how this proof uses all the hypotheses of the lemma and all the axioms of a monoid exactly once.

Topological algebraic objects

A *topological group* (resp. monoid resp. ring) is a group (resp. monoid resp. ring) with a topology, such that the group law and inverse function (resp. monoid law resp. both addition and multiplication) are continuous.

Examples: any algebraic object with the discrete topology.

Examples: $\mathbb{R}$, $\mathbb{C}$, with their usual topologies (coming from the metric): these are additive topological groups, multiplicative topological monoids and topological rings.

Example: $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ (matrix rings) are topological rings, if they have the product topology coming from $M_n(R) \cong R^{n^2}$.

In fact if K is a topological field (which means a topological ring which happens to be a field) then $M_n(K)$ is a topological ring, a topological K-vector space (addition and scalar multiplication are continuous) and thus a topological K-algebra (addition, multiplication and scalar multiplication are continuous).

Topology on units

If R is a topological monoid, then we have no control over the continuity of the inverse function on $R^\times$, if we give it the subspace topology coming from R.

Example (if you know about the adeles of a number field): inverse is not continuous on the units of the adeles of a number field, if you give it the subspace topology.

So one topologises $R^\times$ by embedding it into $R \times R$ via $g \mapsto (g, g^{-1})$ and then giving it the subspace topology of the product topology.

The "flip" map $(x, y) \mapsto (y, x)$ is continuous on R^2 and this means that inversion is continuous on $R^\times$ with this topology.

Topology on $GL_n(R)$

We now have everything to define a topology on $GL_n(R)$ if R is a topological ring.

More precisely: if R is a topological ring and n is a natural then $M_n(R)$, the $n \times n$ matrices with entries in R, is a topological ring when given the product topology $M_n(R) \cong R^{n^2}$.

We define $GL_n(R)$ to be the units of this ring, and we give it the units topology from the last slide, making it into a topological group.

(Remark: if R isn't commutative then everything here works, but it's not clear to me what the answer is, and $SL_n(R)$ doesn't work as there's no good notion of determinant).

(Remark: we will only care about commutative R in this course.)

Variant

Here's something a little more general.

Say R is a topological ring and V is an R-module which is free of finite rank n.

Pleasant exercise: if we choose an R-basis for V and give $End_R(V) \cong M_n(R) \cong R^{n^2}$ the product topology, then this topology on the ring $End_R(V)$ is independent of the choice of basis, and makes $End_R(V)$ into a topological ring.

We define $Aut_R(V)$ to be the units of this topological ring, with the units topology.

If we pick a basis then $Aut_R(V)$ becomes isomorphic to $GL_n(V)$ both algebraically and topologically.

Upshot of this bit: if R is a topological ring and V is a finite free R-module then $Aut_R(V)$ has a natural topology making it a topological group.

Coefficient rings

In this course, we define a *coefficient ring* to be a compact Hausdorff commutative local topological ring.

Example: $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ with the discrete topology.

Example (if you know about the p-adic integers): the p-adic integers $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Example (if you know about complete Noetherian local rings): any complete Noetherian local ring R with the $\mathfrak{m}$-adic topology ($\mathfrak{m}$ the maximal ideal) and finite residue field.

Indeed such R is (by definition of completeness) the projective limit of the finite rings $R/\mathfrak{m}^n$, and thus is compact and Hausdorff.

Coefficient rings

The coefficient rings we saw so far were Noetherian (all ideals finitely-generated); here's a non-Noetherian example.

Let $A_0 := \mathbb{F}_p$ and set $\epsilon_0 = 1$ so $A_0 = \mathbb{F}_p\epsilon_0$.

Let $A_1 := A_0[\epsilon_1]/(\epsilon_1^2) = \mathbb{F}_p\epsilon_0 \oplus \mathbb{F}_p\epsilon_1$.

Idea: A_{n+1} will be $A_n \oplus \mathbb{F}_p\epsilon_{n+1}$ as an abelian group.

For $n \geq 0$, define $A_{n+1} := A_n[\epsilon_{n+1}]/\langle \forall 1 \leq i \leq n+1, \epsilon_{n+1}\epsilon_i \rangle$, and note that there's an obvious map $A_{n+1} \to A_n$ sending ϵ_{n+1} to 0.

As a vector space, $A_{n+1} = A_n \oplus \mathbb{F}_p\epsilon_{n+1}$.

So $A_n = \mathbb{F}_p\epsilon_0 \oplus \mathbb{F}_p\epsilon_1 \oplus \cdots \oplus \mathbb{F}_p\epsilon_n$.

Give all the A_n the discrete topology; then $\varprojlim_n A_n = \prod_n \mathbb{F}_p\epsilon_n$ under the obvious maps and with the projective limit topology, is a coefficient ring.

Note that the maximal ideal is open, but its square is zero.

The ring is local, but it doesn't have the $\mathfrak{m}$-adic topology.

Cool fact about compact Hausdorff rings

The examples of coefficient rings we just saw were all projective limits of finite rings.

Crazy fact: if R is a compact Hausdorff commutative ring, then R is automatically a projective limit of finite rings, with the projective limit topology.

In particular R is profinite as a topological space.

This is in stark contrast to compact Hausdorff groups, of which non-profinite ones abound (for example the circle).

Hendrik Lenstra (personal communication) tells me that he learnt of this fact in the IHES in 1978, and in particular it was known in the 1980s.

This is good because all the proofs I found online assumed Pontrjagin duality!

Units of a compact Hausdorff ring

Compact Hausdorff rings are cool.

Let R be a compact Hausdorff topological ring.

The image J of $R^\times$ in $R \times R$ via $u \mapsto (u, u^{-1})$ is the intersection of the preimages of the closed set $\{1\}$ under the two continuous map $(x, y) \mapsto xy$ and $(x, y) \mapsto yx$.

Proof: use the only lemma you need to know about monoids.

Hence J is a closed subset of the compact space $R \times R$, and is thus compact.

So $R^\times$, the image of J under the first projection map $R^2 \to R$ is also compact and hence closed.

Upshot: units of a compact Hausdorff ring are closed (note: not true for $\mathbb{R}$).

Maximal ideal and residue field of a coefficient ring

If R is a coefficient ring (so commutative local, as well as compact Hausdorff) then we just saw that $R^\times$ was closed in R.

Hence the maximal ideal of a coefficient ring is open (it's the complement of the units).

Additive cosets of this ideal cover R, so by compactness we deduce that the residue field of R is finite.

So we can talk about the *residue characteristic* (a prime number) of a coefficient ring.

Units of a coefficient ring

Let R be a coefficient ring with maximal ideal $\mathfrak{m}$.

We just saw that $\mathfrak{m}$ was open.

Because the additive cosets of $\mathfrak{m}$ are a disjoint cover of R, we deduce that $\mathfrak{m}$ is clopen.

Hence the set $R^\times$ is clopen in R (it's the complement of a clopen).

And in particular it's a closed subset of R, so it's compact Hausdorff with the subspace topology (which is the wrong topology).

Recall that we showed that J, the solutions to $xy = yx = 1$ in $R \times R$, is compact.

If we temporarily give $R^\times \subseteq R$ the subspace topology then the projection $J \to R^\times$ is now a continuous bijection between compact Hausdorff spaces and thus a homeomorphism.

Thus the units topology on $R^\times$ is actually equal to the subspace topology, if R is a coefficient ring.

Topology on an infinite Galois group

The last bit of topology I want to do is to talk about the topology on a Galois group.

Let K be a field and let $\overline{K}$ denote a separable closure.

Remark: we only care in this lecture about the case of K a number field, in which case we can embed K into $\mathbb{C}$ and choose $\overline{K}$ to be the algebraic numbers, but any choice of $\overline{K}$ will do.

I make this remark for the person two weeks ago who asked if we'd used the axiom of choice yet (answer: not really).

The definition of $Gal(\overline{K}/K)$ is simply the K-algebra automorphisms of $\overline{K}$.

Let me say a few words about how to put a topology on this group which makes it into a topological group.

The Galois representations

The group $\mathrm{Gal}(\overline{K}/K)$ has a topology making it into a topological group; a basis of open neighbourhoods of the identity is given by the subgroups $Gal(\overline{K}/L)$ as L runs through the finite extensions of K in $\overline{K}$.

More generally, $U \subset \mathrm{Gal}(\overline{K}/K)$ is open iff for every $f \in U$ there's a finite extension L of K in $\overline{K}$ such that if $g \in \mathrm{Gal}(\overline{K}/K)$ and $g|L = f|L$ then $g \in U$ as well.

This is a topology making $\mathrm{Gal}(\overline{K}/K)$ into a topological group (known in 1980s).

Another way of thinking about it: $\mathrm{Gal}(\overline{K}/K) = \varprojlim_L Gal(L/K)$ where L runs through the finite Galois extensions of K in $\overline{K}$, $Gal(L/K)$ is a finite group with the discrete topology, and $\mathrm{Gal}(\overline{K}/K)$ gets the projective limit topology.

The fundamental theorem: closed subgroups of the Galois group correspond to intermediate field extensions $K \subseteq L \subseteq \overline{K}$.

Continuous Galois representations

We're ready to talk about continuous Galois representations.

A lot of the papers in this area spend a lot of time studying continuous group homomorphisms $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(R)$ where R is a coefficient ring.

For formalization purposes it's easier to stick to continuous group homomorphisms $\rho : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V)$ where R is a coefficient ring and V is a free rank 2 module over R.

Remember: if you pick a basis then $Aut_R(V) = GL_2(R)$, and the choice doesn't affect the topology (it just changes things by conjugation).

Let's discuss the example we're motivated by.

Mod p Galois representation associated to an elliptic curve

Say $E/\mathbb{Q}$ is an elliptic curve and p is a prime number.

Say $\overline{\mathbb{Q}}$ is a separable closure of $\mathbb{Q}$.

I claim that $E(\overline{\mathbb{Q}})[p]$ is a free rank 2 module over $\mathbb{Z}/p\mathbb{Z}$.

Proof: known in the 1980s (see Silverman, for example).

Continuity

I also claim that the induced map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathbb{Z}/p\mathbb{Z}}(E(\overline{\mathbb{Q}})[p])$ is continuous.

Indeed, topology on $\mathbb{Z}/p\mathbb{Z}$ is discrete and it's easy to check that this implies the topology on the finite set $Aut_{\mathbb{Z}/p\mathbb{Z}}(E(\overline{\mathbb{Q}})[p])$ is discrete.

So it will suffice to prove that the kernel of this map is open.

But the elements of $E(\overline{\mathbb{Q}})[p]$ are 0 and $p^2 - 1$ points of the form (x_i, y_i) with $x_i, y_i \in \overline{\mathbb{Q}}$ (because it's 2-dimensional over $\mathbb{Z}/p\mathbb{Z}$).

These finitely many elements of $\overline{\mathbb{Q}}$ generate a finite extension L of $\mathbb{Q}$.

And $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ (the kernel) is open in $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ by definition.

Hardly ramified representations

Upshot so far: if R is a coefficient ring (e.g., $\mathbb{Z}/p\mathbb{Z}$), if V is a free rank 2 R-module (e.g., $E(\overline{\mathbb{Q}})[p]$) then we now know what it means for $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ to be continuous.

What we don't yet know is what it means for ρ to be *hardly ramified*.

So let's start by talking about ramification.

Ramification

Let K be a number field (so a field containing $\mathbb{Q}$ and finite-dimensional as a $\mathbb{Q}$-vector space).

Let A be its ring of integers (the elements of K which are roots of monic polynomials with integer coefficients).

Let P be a maximal ideal of A.

Fact: A/P is a finite field, called the residue field of P.

Let's call it k and say it has size q.

I want to talk about decomposition and inertia subgroups and Frobenius elements associated to P.

But these definitions rely on yet more auxiliary choices.

Ramification

K number field, integers A, maximal ideal P, residue field k of size q.

Let $\overline{K}$ be any separable closure of K.

Let $\overline{A}$ be the algebraic integers in $\overline{K}$ (again, the roots of monic polynomials with integer coefficients).

Here's a cool theorem: there is at least one maximal ideal $\overline{P}$ of $\overline{A}$ which contains P.

We say $\overline{P}$ *lies over* P.

In fact there are uncountably many such maximal ideals.

Choose $\overline{P}$ and define $\overline{k}$ to be $\overline{A}/\overline{P}$.

There's a canonical map $k \to \overline{k}$, identifying the latter field with a separable closure of the former.

Ramification

K, A, P, k, choose $\overline{K}$, $\overline{A}$, choose $\overline{P}$, $\overline{k}$.

If $g \in \mathrm{Gal}(\overline{K}/K)$ then the bijection $g : \overline{K} \to \overline{K}$ induces a ring automorphism $g : \overline{A} \to \overline{A}$. Thus $\mathrm{Gal}(\overline{K}/K)$ acts on the maximal ideals of $\overline{A}$.

Cool fact: this action is transitive on the maximal ideals containing P.

The *decomposition group* $D_{\overline{P}}$ associated to $\overline{P}$ is the stabiliser of $\overline{P}$ in $\mathrm{Gal}(\overline{K}/K)$ (acting on maximal ideals of $\overline{A}$).

The action of $D_{\overline{P}}$ on $\overline{A}$ fixes $\overline{P}$ (as a set, not pointwise), so there's an induced action of $D_{\overline{P}}$ on $\overline{A}/\overline{P} = \overline{k}$, fixing $A/P = k$.

We thus get a group homomorphism $D_{\overline{P}} \to Gal(\overline{k}/k)$, which is easily checked to be continuous.

The *inertia group* $I_{\overline{P}}$ associated to $\overline{P}$ is the kernel of this map.

A *Frobenius element* associated to $\overline{P}$ is any element of $D_{\overline{P}}$ whose image in $Gal(\overline{k}/k)$ is $x \mapsto x^q$, where $q = |k|$.

Decomposition/Inertia/Frobenius

K a number field, integers A, max ideal P, residue field k of size q.

$\overline{K}$ any separable closure, integers $\overline{A}$, max ideal $\overline{P}$ containing P, residue field $\overline{k}$.

We are talking about elements and subgroups of $\mathrm{Gal}(\overline{K}/K)$ so we have to choose a $\overline{K}$.

But I don't want to choose $\overline{P}$ so we make the following definitions.

A subgroup D_P of $\mathrm{Gal}(\overline{K}/K)$ is a *decomposition group at P* if there exists $\overline{P}$ such that $D_P = D_{\overline{P}}$.

A subgroup I_P of $\mathrm{Gal}(\overline{K}/K)$ is an *inertia subgroup at P* if there exists $\overline{P}$ such that $I_P = I_{\overline{P}}$.

An element $Frob_P$ of $\mathrm{Gal}(\overline{K}/K)$ is a *Frobenius element at P* if there exists $\overline{P}$ such that $Frob_P$ is a Frobenius element associated to $\overline{P}$.

Any questions about the definitions, before we go on to a bunch of facts about them?

Decomposition/Inertia/Frobenius

K, A, P, k, choose $\overline{K}$, get $\overline{A}$.

Facts:

- Maximal ideals $\overline{P}$ of $\overline{A}$ containing P exist.
- They're all in one $\mathrm{Gal}(\overline{K}/K)$-orbit.
- Hence decomposition groups $D_P \subseteq \mathrm{Gal}(\overline{K}/K)$ exist, and are all conjugate.
- Similarly inertia subgroups I_P exist and are all conjugate.

Frobenius elements are not all conjugate, because a Frobenius element for $\overline{P}$ was only defined via its action on $\overline{A}/\overline{P}$ so was only well-defined up to multiplication by an element of $I_{\overline{P}}$.

So how do we explain that mathematicians constantly talk about $\rho(Frob_P)$ where ρ is a Galois representation?

Decomposition/Inertia/Frobenius

K, A, P as usual.

Say N is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$.

Then TFAE: (i) N contains one inertia subgroup at P; (ii) N contains all inertia subgroups at P.

This is because inertia subgroups exist (because $\overline{P}$ over P exists), and they're all conjugate (because the Galois action on the choices of $\overline{P}$ is transitive).

So in $\mathrm{Gal}(\overline{K}/K)/N$, Frobenius elements at P exist and they're all conjugate.

Unramified Galois representations

I owe you a definition of *hardly ramified* and I'm currently able to give you a definition of *unramified*.

Let K be a number field with integers A and let $\overline{K}$ be a separable closure.

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

We say that ρ is *unramified* at a maximal ideal P of A if the kernel of ρ contains one (or equivalently all) inertia subgroup(s) at P.

If ρ is unramified at P then people talk about $\rho(Frob_P) \in Aut_R(V)$ and this element is only well-defined up to conjugation in $Aut_R(V)$.

So we need to be careful to only do things with $\rho(Frob_P)$ which are invariant under conjugation (such as taking trace, determinant or characteristic polynomial).

Unramified Galois representations

If R is a *finite* ring and V is free of finite rank then the kernel of $\rho : \mathrm{Gal}(\overline{K}/K) \to Aut_R(V)$ has finite index in $\mathrm{Gal}(\overline{K}/K)$.

The fundamental theorem of Galois theory then gives us a finite Galois extension L/K corresponding to this kernel.

It's a fact that if P does not divide the discriminant ideal of this extension, then ρ is unramified at P.

In particular ρ is unramified outside a finite set of primes.

If R is infinite then in examples coming from geometry ρ is also unramified outside a finite set of primes, but it's possible to write down pathological examples ramified at infinitely many primes.

Coefficient rings are $\mathbb{Z}_\ell$-algebras

Here's a cool fact about coefficient rings.

Say R is a coefficient ring with residue characteristic ℓ.

Then R/J is a finite local ring for all open ideals J, and thus a $\mathbb{Z}/\ell^n\mathbb{Z}$-algebra for some $n = n(J)$.

So $R = \varprojlim_J R/J$ is naturally an algebra for $\varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} = \mathbb{Z}_\ell$, the ℓ-adic integers.

The maps $\mathbb{Z}_\ell \to R/J$ are all continuous, so the map $\mathbb{Z}_\ell \to R$ is also continuous.

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

The cyclotomic character

Another thing we need for hardly ramified representation is the cyclotomic character.

Say K is any field and p is any prime number.

If $\overline{K}$ is a separable closure of K and if n is a natural number then $\mathrm{Gal}(\overline{K}/K)$ acts on the set $\mu_{p^n}(\overline{K})$ of roots of $X^{p^n} = 1$ in $\overline{K}$.

If the characteristic of K is p then this set has size 1, but if not then it has size p^n. Assume from now on that the characteristic of K is not p.

In this case $\mu_{p^n}(\overline{K})$ is cyclic of order p^n (typically with no canonical generator).

If you choose a generator ζ_0 then there's a unique $\chi_n(g) \in \mathbb{Z}/p^n\mathbb{Z}$ such that $g(\zeta_0) = \zeta_0^{\chi_n(g)}$.

Then $g(\zeta) = \zeta^{\chi_n(g)}$ for all $\zeta \in \mu_{p^n}(\overline{K})$, as g acts via ring homomorphisms.

The associated monoid homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/p^n\mathbb{Z}$ is continuous, because it factors through the finite extension $Gal(K(\zeta_0)/K)$.

The cyclotomic character

K a field, p a prime number, $p \neq 0$ in K.

We just saw that for any natural n there's a unique $\chi_n(g) \in \mathbb{Z}/p^n\mathbb{Z}$ such that if $\zeta \in \overline{K}$ and $\zeta^{p^n} = 1$ then $g(\zeta) = \zeta^{\chi_n(g)}$.

These χ_n are compatible as n changes, giving us a continuous monoid homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p$ and thus a continuous group homomorphism $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p^\times$ (monoid homomorphisms from groups have image in the units).

This is called the *cyclotomic character* associated to K, $\overline{K}$ and p.

Where is the cyclotomic character ramified?

The cyclotomic character is beautifully canonical and functorial.

It depends only on the choice of a prime number ℓ and works for any field of characteristic not equal to ℓ.

So if K is a number field, we can ask what the cyclotomic character does to things like decomposition groups, inertia groups and Frobenius elements.

Where is the cyclotomic character ramified?

So say K is a number field with integers A, $\overline{K}$ is a separable closure, and say ℓ is a prime.

Because K has characteristic $0 \neq \ell$, we have the ℓ-adic cyclotomic character $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_\ell^\times = GL_1(\mathbb{Z}_\ell)$.

Now say P is a maximal ideal of A with residue field k of size q.

Let $\overline{A}$ be the integers of $\overline{K}$ and let $\overline{P}$ be a maximal ideal containing P.

The roots of unity $\mu_{\ell^n}(\overline{K})$ in $\overline{K}$ are all in $\overline{A}$.

So one can ask about the induced map $\mu_{\ell^n}(\overline{K}) \to \overline{A}/\overline{P}$.

There are two cases: if $\ell \in P$ (equivalently $\ell \in \overline{P}$, or $char(k) = \ell$, or $char(\overline{k}) = \ell$) then this map is the constant map sending everything to 1.

But if $\ell \notin P$ then this map can be checked to be injective.

(key point: if ζ_1 and ζ_2 are unequal ℓ-power roots of unity then $\zeta_1 - \zeta_2$ divides ℓ in $\overline{A}$ so cannot be in $\overline{P}$, which is maximal).

Where is the cyclotomic character ramified?

K number field, $\overline{K}$, A, P, ℓ, $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_\ell^\times$.

Say $Frob_P \in \mathrm{Gal}(\overline{K}/K)$ is a Frobenius element at P.

By definition of Frobenius element, there's some $\overline{P} \subset \overline{A}$ such that $Frob_P(\overline{P}) = \overline{P}$ and $Frob_P(x) = x^q$ if $x \in \overline{A}/\overline{P}$.

By definition of ℓ-adic cyclotomic character, $Frob_P(\zeta) = \zeta^{\chi(Frob_P)}$ if ζ is an ℓ-power root of unity.

Now assume $\ell \notin P$.

By injectivity of $\mu_{\ell^n}(\overline{K}) \to \overline{A}/\overline{P}$, $\chi(Frob_P) = q \bmod \ell^n$.

This is true for all n, so $\chi(Frob_P) = q$, for all Frobenius elements $Frob_P$.

Where is the cyclotomic character ramified?

K number field, A, P, ℓ a prime, χ the ℓ-adic cyclotomic character.

We just saw that $\chi(Frob_P) = q = |A/P|$ for all Frobenius elements $Frob_P$, if $\ell \notin P$.

So we can deduce that χ is unramified at P if $\ell \notin P$ (because if $i \in I_{\overline{P}}$ then $\chi(i \times Frob_{\overline{P}}) = \chi(Frob_{\overline{P}})$ as both are Frobenii, so $\chi(i) = 1$).

In contrast, if $\ell \in P$ then one can check that $\chi(I_P)$ is uncountably infinite, and in particular χ is really really badly ramified at the maximal ideals containing ℓ.

Conclusion: "unramified at P" isn't the right "nice" condition for Galois representations of a number field, taking values in a coefficient ring whose residue characteristic is in P.

Flatness

The right "nice" condition is *flatness*, which I'll now explain.

Once we have that, we will be able to define hardly ramified representations and state the main boss theorem of Level 4.

Flatness is a predicate on several different kinds of objects, which makes things a little confusing.

The most basic definition involves some basic theory of finite extensions of $\mathbb{Q}_p$, so let me race through these.

The p-adic integers.

Let p be a prime number.

Let $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ be the projective limit of the rings $\mathbb{Z}/p^n\mathbb{Z}$.

Then $\mathbb{Z}_p$ is a commutative ring.

It's even a local ring; its unique maximal ideal is $p\mathbb{Z}_p$ (principal) and the residue field is canonically isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

If we give $\mathbb{Z}_p$ the projective limit topology then it's a commutative topological ring.

It's compact and Hausdorff, so it's a coefficient ring.

p-adic numbers

Let p be a prime number.

The ring $\mathbb{Z}_p$ is an integral domain; let $\mathbb{Q}_p$ be its field of fractions.

We have $\mathbb{Q}_p = \varinjlim_n p^{-n}\mathbb{Z}_p$ so we can give it the inductive limit topology.

One can check that $\mathbb{Q}_p$ with this topology is a topological field.

Finite extensions of $\mathbb{Q}_p$.

Let p be a prime number.

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

We define the integers A of K to be the integral closure of $\mathbb{Z}_p$ in K, that is, the elements of K which are roots of monic polynomials with coefficients in $\mathbb{Z}_p$.

Just like for number fields (finite extensions of $\mathbb{Q}$) we can set up a theory of decomposition and inertia groups, and Frobenius elements.

But here it's easier, because other than a choice of $\overline{K}$ we don't need to make any other choices.

Finite extensions of $\mathbb{Q}_p$.

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

The ring A is local so it has a unique maximal ideal P.

Now choose a separable closure $\overline{K}$ of K.

The integral closure $\overline{A}$ of A in $\overline{K}$ is also local.

So it has a unique maximal ideal $\overline{P}$, which contains P.

Set $A/P = k$ (a finite field) and $\overline{A}/\overline{P} = \overline{k}$, which is a separable closure of k.

Because $\overline{A}$ has a unique maximal ideal, we could call all of $\mathrm{Gal}(\overline{K}/K)$ a decomposition group for $\overline{P}$ or for P.

The induced continuous group homomorphism $\mathrm{Gal}(\overline{K}/K) \to Gal(\overline{k}/k)$ has kernel which we can call the inertia group I_P for P.

Back to flatness

Our first goal in our definition of flatness is to say what it means for a finite abelian group equipped with a continuous action of $\mathrm{Gal}(\overline{K}/K)$ to be *flat*.

The definition will be: "comes from a certain kind of Hopf algebra" so let's define these.

NB Hopf algebras and flatness are the last definitions we'll need to define hardly ramified Galois representations.

Hopf algebras

All rings are commutative in this Hopf algebra section.

Let R be any commutative ring.

I'm about to define a *commutative co-commutative R-Hopf algebra*.

But this is a mouthful so I'm just going to call then R-Hopf algebras.

An R-Hopf algebra is a commutative R-algebra A with some extra structure and satisfying some extra axioms.

The extra structure is:

- A *comultiplication*: an R-algebra map $m^* : A \to A \otimes_R A$;
- A *coinverse*: an R-algebra map $i^* : A \to A$;
- A *counit*: an R-algebra map $e^* : A \to R$.

The extra axioms are the co-(abelian group) axioms. What does this mean?

co-(abelian group) axioms

R a commutative ring, A a commutative R-algebra.

Say we have R-algebra maps $m^* : A \to A \otimes_R A$, $i^* : A \to A$ and $e^* : A \to R$. What do these give us?

By "$Hom(X, Y)$" in the below I *always* mean R-algebra homomorphisms.

Let's define G to be the "functor on commutative R-algebras corepresented by A".

In other words, say S is any commutative R-algebra, and let's define $G(S) := Hom(A, S)$ to be the set of R-algebra maps from A to S.

Note that $Hom(A \otimes_R A, S)$ is canonically $G(S) \times G(S)$, because to give an R-algebra map $A \otimes_R A \to S$ is to give a pair of R-algebra maps $A \to S$.

So $m^* : A \to A \otimes_R A$ induces maps $G(S) \times G(S) \to G(S)$ (just compose $f : A \otimes_R A \to S$ with m^* to get a map $f \circ m^* : A \to S \in G(S)$).

Maybe you're beginning to guess why m^* is called "comultiplication".

co-stuff

$i^* : A \to A$ induces a map $G(S) \to G(S)$ for all S, again just by precomposing $f : A \to S \in G(S)$ with i^*.

Finally note that $Hom(R, S)$ is a set with one element.

So $e^* : A \to R$ gives us an element of $G(S)$ (because composing with it gives a map $Hom(R, S) \to Hom(A, S)$).

The co-(abelian group) axioms on m^*, i^*, e^* will imply that for all choices of S, these maps are the multiplication, inverse and identity making $G(S)$ into an abelian group.

Upshot

That was a lot to take in, so let me say it again. R a commutative ring.

An R-Hopf algebra is a commutative R-algebra A plus some extra structure (this co-stuff) and some extra axioms (which I've not yet stated).

The extra structure means that for any commutative R-algebra S, the set of R-algebra maps $G(S) := Hom(A, S)$ gets some extra structure (a "multiplication", "inverse" and "unit"),

The extra axioms on a Hopf algebra will mean that this structure on $G(S)$ makes it into an abelian group, for all S.

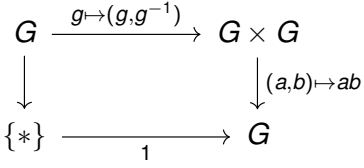
What's left: I have to convince you that the group axioms for all the $G(S)$ can be translated into statements which only involve m^*, i^*, e^*.

And those will be the axioms of a Hopf algebra.

A group axiom

Let's take the abelian group axiom $gg^{-1} = 1$.

First we write the axiom as a picture:



The group axiom is the claim that this diagram commutes.

I claim there is a condition on m^*, i^*, e^* which guarantees that this square commutes when $G = Hom(A, S)$, for all S.

A co-group axiom

We want this to commute:

$$\begin{array}{ccc} G & \xrightarrow{g\mapsto(g,g^{-1})} & G\times G \\ \downarrow & & \downarrow{\scriptstyle (a,b)\mapsto ab} \\ \{*\} & \xrightarrow[1]{} & G \end{array}$$

So let's make this square commute:

$$\begin{array}{ccc} A & \xleftarrow{c\circ(id_A\otimes_R i^*)} & A\otimes_R A \\ \uparrow{\scriptstyle s} & & \uparrow{\scriptstyle m^*} \\ R & \xleftarrow[e^*]{} & A \end{array}$$

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

A co-group axiom

$$\begin{array}{ccc} A & \xleftarrow{c\circ(id_A\otimes_R i^*)} & A\otimes_R A \\ {\scriptstyle s}\uparrow & & \uparrow{\scriptstyle m^*} \\ R & \xleftarrow[e^*]{} & A \end{array}$$

If this second square commutes, then applying $Hom(-, S)$ to it will turn it into the first square and that will hence also commute. For any S!

The statement that this square commutes is thus one of the co-(abelian group) axioms for an R-Hopf algebra.

In symbols, if $s : R \to A$ is the structure map, and $c : A \otimes_R A \to A$ is the R-algebra map sending $x \otimes y$ to xy, then the axiom is $s \circ e^* = c \circ (1_A \otimes i^*) \circ m^*$.

Now write down all the axioms for an abelian group, translate them all into statements about m^*, i^* and e^* in this way, and there's your definition of a Hopf algebra.