Formalizing Fermat, Lecture 5
Kevin Buzzard
In the last episode...
Level 7: Introduction
Level 7: Quaternion algebras
Level 7: Finite adeles
Level 7: Hecke operators
Level 7: Maximal orders
Level 7: systems of eigenvalues
Level 7: potential automorphy

Formalizing Fermat, Lecture 5

Kevin Buzzard, Imperial College London

EPSRC TCC, 26th Feb 2026

No lecture next week!

No lecture next week!
No lecture next week!
No lecture next week!
No lecture on 5th March next week!

I'm in Oxford next week, giving a summary of this course in their number theory seminar.

Which means there are only two lectures after this one.

I might just keep going though (e.g. on 26th March and maybe even 2nd April?)

Depending on audience interest.

I'm interested in examining the entire proof of FLT modulo 1980s.

But because I'm teaching the course backwards, you can choose to leave at any time :-)

Summary of where we are

We just beat Level 6.

So we proved the following theorem:

Theorem

Modulo results proved in the 1980s, statement B6 implies FLT.

Statement B6 is the conjunction of two theorems.

The first says that an irreducible hardly ramified $\mathbb{Z}/\ell\mathbb{Z}$-representation lifts to an ℓ-adic one.

The second says that an ℓ-adic hardly ramified representation, whose reduction is an irreducible $\mathbb{Z}/\ell\mathbb{Z}$-representation, spreads out into a family of p-adic ones.

(except that we only actually used that it spread out to a 3-adic representation.)

The story so far

Some of the results we used from the 1980s are nontrivial.

Examples:

- Mazur's 1978 theorem on torsion subgroups of elliptic curves;
- Raynaud and Fontaine's theorems from the 1970s on finite flat group schemes when $e < p - 1$;
- Poitou's results about how root discriminants of number fields relate to their degree.

We will have to assume several more nontrivial results from the 1980s before we're done.

In fact today I will state a result from 1989 whose proof, when written out in full, is probably twice the length of all of the above put together.

In the last episode...

Level 7: Introduction

Level 7: Quaternion algebras

Level 7: Finite adeles

Level 7: Hecke operators

Level 7: Maximal orders

Level 7: systems of eigenvalues

Level 7: potential automorphy

Automorphy lifting theorems

Where are we going in this course?

The next big goal is to reduce both the hardly ramified lifting theorem and the hardly ramified spreading out theorem to a "final boss of the game" theorem.

This will take several levels.

The final boss of the game is an "automorphy lifting theorem."

Wiles in 1994 proved a "modularity lifting theorem."

But I hesitate to call the final boss of the game a modularity lifting theorem, because we will not be using modular forms.

We'll use *automorphic forms*, a generalization of modular forms.

We're about to start level 7, where we'll introduce the relevant automorphic forms.

In the last episode...
Level 7: Introduction
Level 7: Quaternion algebras
Level 7: Finite adeles
Level 7: Hecke operators
Level 7: Maximal orders
Level 7: systems of eigenvalues
Level 7: potential automorphy

Automorphic forms – the easy case

In full generality, the definition of automorphic forms involves analysis.

However, for the automorphic forms which concern us, “the associated symmetric spaces are 0-dimensional.”

So there will be no analysis.

Contrast with modular forms, where the associated symmetric space is the upper half plane, and modular forms are holomorphic functions on it.

Like level 4 (when we defined hardly ramified representations), we need to spend a fair amount of time here making the definitions.

Level 4 contained all the definitions we needed on the Galois side; this level contains all the definitions we need on the automorphic side.

Like level 4, the final boss will be trivial.

Let’s get going.

Level 7: Enter automorphic forms

Let K be a finite extension of $\mathbb{Q}_\ell$, with integers $\mathcal{O}$, and say $\mathcal{V}$ is a free rank 2 $\mathcal{O}$-module.

Say $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathcal{O}}(\mathcal{V})$ is a hardly ramified Galois representation.

We have seen already that a crucial invariant of ρ is the collection $t_p = trace(\rho(Frob_p))$ of traces of Frobenius elements at unramified primes.

Example: the way we moved from ℓ to 3 was via keeping track of these traces.

These t_p are coming from the "Galois" side of Langlands.

Our main goal in level 7 is to explain how to get analogous numbers t_p coming from the "automorphic" side of Langlands.

Langlands reciprocity is statements of the form "the collections of numbers coming from the automorphic and Galois side coincide".

Quaternion algebras

Automorphic forms are defined for connected reductive groups over global fields.

A number field is an example of a global field.

GL_2 is an example of a connected reductive group.

But in this course we will be concerned with inner forms of GL_2, namely $D^\times$ where D is a quaternion algebra.

So let's talk about quaternion algebras.

Quaternion algebras

Let K be a field.

Reminder: a (non-commutative) K-algebra D is a ring D equipped with a ring homomorphism $K \to D$ whose image lies in the centre of D.

A *quaternion algebra* over K is a (non-commutative) K-algebra D satisfying these three axioms:

- The centre of D is (the image of) K;
- $dim_K(D) = 4$;
- D has no non-trivial two-sided ideals.

Example (fun exercise): $M_2(K)$, the 2×2 matrices over K.

Example (characteristic of K not 2): $K \oplus Ki \oplus Kj \oplus Kk$ with $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$ etc.

Example/definition: If $K = \mathbb{R}$ then we let $\mathbb{H} := \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ be the Hamilton quaternions.

Facts about quaternion algebras

Let K be a field.

If D/K is a quaternion algebra then either $D \cong M_2(K)$ or D is what French people call a field.

(and what English people call a skew field: all nonzero elements are invertible.)

Example: $\mathbb{H}$ is a skew field because if $a + bi + cj + dk \neq 0$ then its inverse is $(a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$.

NB this proves that $\mathbb{H} \ncong M_2(\mathbb{R})$ as rings because there are nonzero noninvertible 2×2 matrices like $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

In the last episode...
Level 7: Introduction
Level 7: Quaternion algebras
Level 7: Finite adeles
Level 7: Hecke operators
Level 7: Maximal orders
Level 7: systems of eigenvalues
Level 7: potential automorphy

Classification of quaternion algebras

Here are the statements of some classification theorems.

If K is algebraically closed (e.g. $K = \mathbb{C}$) then $M_2(K)$ is the only quaternion algebra over K (up to isomorphism).

If $K = \mathbb{R}$ then the only ones are $M_2(\mathbb{R})$ and $\mathbb{H}$.

If K is a finite extension of $\mathbb{Q}_p$ then there are also 2, up to isomorphism, and one can "write down" the quaternion algebra which isn't $M_2(K)$.

For example if $K = \mathbb{Q}_2$ then it's $K \oplus Ki \oplus Kj \oplus Kk$ with $i^2 = j^2 = k^2 = -1$ etc etc.

All proofs known in the 1950s.

You can relate quat. algebras over a field K to 2-torsion in the Brauer group $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$ of K, and use class field theory to prove results like this.

Fun exercise: if $p > 2$ then prove that $\mathbb{Q}_p \oplus \mathbb{Q}_p i \oplus \mathbb{Q}_p j \oplus \mathbb{Q}_p k \cong M_2(\mathbb{Q}_p)$ as $\mathbb{Q}_p$-algebra. Then experiment with e.g. $i^2 = -3$, $j^2 = -1$, $ij = -ji = k$ etc.

Base change for quaternion algebras

Say K is a field, D/K is a quaternion algebra, and L/K is an arbitrary field extension.

Fact: $D \otimes_K L$ is a quaternion algebra over L.

We say L *splits* D if $D \otimes_K L \cong M_2(L)$.

For example, an algebraic closure of K splits any quaternion algebra over K (because the only quaternion algebra over $\overline{K}$ is $M_2(\overline{K})$.)

Example: $\mathbb{C}$ splits $\mathbb{H}$.

In other words, $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$.

Classification for number fields

Now say K is a number field.

Then there is an elementary invariant which classifies quaternion algebras over K (up to non-unique isomorphism); let me explain it.

Let A be the integers of K. (Important note: the integers of our number field will be called A throughout this lecture.)

If P is a maximal ideal of A, then let's call P a *finite place* of K.

Let $A_P = \varprojlim_n A/P^n$ be the P-adic completion of A, and let K_P be the field of fractions of A_P.

We say K_P is the *completion of* K at the finite place P.

Example: if p is a prime number then the p-adic numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ at the finite place (p). In general K_P is a finite extension of $\mathbb{Q}_p$ if $p \in P$.

There's a natural ring homomorphism $K \to K_P$.

Real infinite places

Again let K be a number field.

If $v : K \to \mathbb{R}$ is a ring homomorphism, then we call v a *real place* of K.

We define the *completion* K_v of K at the real place v to be $\mathbb{R}$.

We define the "natural map" from K to K_v to be v.

There are infinitely many finite places of a number field, but only finitely many real places.

Example: if $K = \mathbb{Q}$ then there's a finite place for each prime p, with completion $\mathbb{Q}_p$, and there's one real place (traditionally called ∞), with completion $\mathbb{R}$.

Classification of quaternion algebras over number fields

Now let K be a number field, and let D be a quaternion algebra over K.

Here's a fact: the extension K_P/K splits D for all but finitely many finite places P of K.

In other words, $D \otimes_K K_P \cong M_2(K_P)$ for all but finitely many P.

Example: $\mathbb{Q}_p$ splits $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ if $p > 2$, but not if $p = 2$.

We say D *splits* at P if K_P splits D, and D *ramifies* at P if K_P does not split D.

Similarly if v is a real place of K, the completion K_v may or may not split D.

We say v splits D, or D is split at v, if $D \otimes_K K_v \cong M_2(\mathbb{R})$.

We say D *ramifies at* v if $D \otimes_K K_v \cong \mathbb{H}$.

Note that K only has finitely many real places.

So a quaternion algebra only ramifies at a finite set of places.

Classification of quaternion algebras over number fields

Let D be a quaternion algebra over a number field K.

Let $S(D)$ be the set of finite places P and real places v where D is ramified.

Cool fact 0 (already mentioned): $S(D)$ is finite.

Example: if $K = \mathbb{Q}$ then $S(M_2(\mathbb{Q})) = \emptyset$, and $S(\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k) = \{2, \infty\}$.

Cool fact 1: $S(D)$ always has even size.

Cooler fact 2: $S(D)$ determines the isomorphism class of D.

Coolest fact 3: any finite even-sized subset S of the union of finite and real places of K is $S(D)$ for some (unique up to isomorphism) quaternion algebra D.

That's as good a classification theorem as one could expect.

The reductive group associated to a quaternion algebra

Let K be a field and let D be a quaternion algebra over K.

If R is any commutative K-algebra, then the units $(D \otimes_K R)^\times$ of the ring $D \otimes_K R$ are a group.

Let's write $D^\times(R)$ for this group.

Like elliptic curves and Hopf algebras, the map $R \mapsto D^\times(R)$ is a group functor.

The highbrow explanation of what we're about to do:

This group functor is representable over K; the corresponding algebraic group over K is connected and reductive.

Under some extra assumptions on K and D, we're going to define automorphic forms for this connected reductive algebraic group.

They will be functions on $D^\times(\mathbb{A}_K^f)$, where $\mathbb{A}_K^f$ are the *finite adeles* of K.

So I'd better talk about finite adeles next.

Finite adeles

Let me first give a nonstandard definition.

The *profinite completion* $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ is defined to be the projective limit $\varprojlim_{N\geq 1} \mathbb{Z}/N\mathbb{Z}$ with the projective limit topology.

By the chinese remainder theorem, $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.

Let K be a number field. The *finite adeles of K*, notation $\mathbb{A}_K^f$, are defined to be $K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$.

$\mathbb{A}_K^f$ is a commutative ring, a K-algebra and a $\widehat{\mathbb{Z}}$-algebra.

The definition we've given is nonstandard but cheap. The f is for finite, it's part of the notation.

The definition emphasizes that $\mathbb{A}_K^f$ is some kind of universal nonarchimedean completion of K.

Topology: give $\mathbb{A}_K^f$ the finest topology making it a topological ring and such that the $\widehat{\mathbb{Z}}$-action $\widehat{\mathbb{Z}} \times \mathbb{A}_K^f \to \mathbb{A}_K^f$ is continuous. This topology exists.

Restricted products.

The more traditional approach to finite adeles goes via restricted products.

Say X_i are sets, with i running through a (typically infinite) index set.

Say $Y_i \subseteq X_i$ are subsets.

Then there's a *restricted product* $\prod'_i X_i$ (with respect to the Y_i, although the Y_i are traditionally omitted from the notation).

It's defined to be the (x_i) in $\prod_i X_i$ such that $x_i \in Y_i$ for all but finitely many i.

If the X_i are groups/rings and the Y_i are subgroups/subrings, the restricted product is a group/ring.

If the X_i are additive abelian groups and the Y_i are subgroups then we have a short exact sequence

$$0 \to \prod_i Y_i \to \prod'_i X_i \to \bigoplus_i (X_i/Y_i) \to 0.$$

Traditional definition of the finite adeles

Now say K is a number field with integers A, and P is a finite place of K.

We have the completion $A_P = \varprojlim_n A/P^nA$ with field of fractions K_P.

The traditional definition of $\mathbb{A}_K^f$:

It's the restricted product of the fields K_P, as P runs through the finite places of K, with respect to the subrings A_P.

$\mathbb{A}_K^f = \prod'_P K_P$.

It's thus a commutative ring.

With this viewpoint, the map from K to $\mathbb{A}_K^f$ needs a little thought.

The map $K \to \prod_P K_P$ has image in $\mathbb{A}_K^f$ because any element of K only has finitely many primes in its denominator.

Topology on a restricted product

Back to $Y_i \subseteq X_i$ indexed by i in an index set.

If the X_i are topological spaces and the Y_i are open subspaces, then $\prod'_i X_i$ gets a topology, but it's *not* the subspace topology coming from $\prod_i X_i$.

The restricted product is the union of $\prod_{i \in S} X_i \times \prod_{i \notin S} Y_i$, as S runs through the finite subsets of the index set.

We decree that all of these sets are open in $\prod'_i X_i$.

And we decree that the topology on $\prod_{i \in S} X_i \times \prod_{i \notin S} Y_i$ induced from $\prod'_i X_i$ is the product topology. This defines the topology on $\prod'_i X_i$.

The traditional definition of the ring of finite adeles $\mathbb{A}_K^f$ is that it's $\prod'_P K_P$ over the open subrings A_P, with the topology described above.

It's a topological ring, and $\prod_P A_P \subseteq \mathbb{A}_K^f$ is an open subring.

With the $\mathbb{A}_K^f = K \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ definition, $\prod_P A_P$ is just $A \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$.

Automorphic forms

Now say F is a number field and D/F is a quaternion algebra.

I want to define automorphic forms for the reductive group $D^\times$ over F.

The usual definition of an automorphic form for a connected reductive group over a number field involves analysis.

Example: modular forms are automorphic forms for $\mathrm{GL}_2/\mathbb{Q}$, and they're holomorphic functions.

But we will now put some extra assumptions on D and F which makes the analysis disappear.

Our assumptions will ensure that there are no $\mathrm{GL}_2(\mathbb{R})$s or $\mathrm{GL}_2(\mathbb{C})$s lurking in $(D \otimes_{\mathbb{Q}} \mathbb{R})^\times$.

And then an automorphic form for $D^\times$ will simply be a locally constant function on $D^\times(\mathbb{A}_F^f)$ satisfying one axiom.

In the last episode...

Level 7: Introduction

Level 7: Quaternion algebras

Level 7: Finite adeles

Level 7: Hecke operators

Level 7: Maximal orders

Level 7: systems of eigenvalues

Level 7: potential automorphy

Totally real fields

First we make sure we avoid $\mathrm{GL}_2(\mathbb{C})$'s.

We say that a number field F is *totally real* if every field homomorphism $F \to \mathbb{C}$ has image lying in $\mathbb{R}$.

Examples: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{37})$.

Non-example: $\mathbb{Q}(\sqrt[3]{2})$.

Example: $\mathbb{Q}[X]/(f)$ where $f \in \mathbb{Q}[X]$ is irreducible and all of its complex roots are real.

Or the splitting field of such an f.

Note: totally real number fields are traditionally called F, so we switch notation from K to F here.

The integers of F will still be called A though.

If F is totally real, then it has $[F:\mathbb{Q}]$ real places.

Totally definite quaternion algebras

Let F be a totally real field, and say D/F is a quaternion algebra.

We say that D is *totally definite* if for *every* real place $v : F \to \mathbb{R}$ we have $D \otimes_{F,v} \mathbb{R}$ is isomorphic to $\mathbb{H}$.

In other words, D is ramified at all the real places of F. So we avoid $\mathrm{GL}_2(\mathbb{R})$.

Note to experts: What's going on is that $\mathbb{H}^\times = \mathbb{R}^4 - \{0\}$ is equal to the subgroup $\mathbb{R}^\times.S^3$ where S^3, the unit quaternions, is a maximal compact subgroup.

So $\mathbb{R}^\times\backslash\mathbb{H}^\times/S^3$ is one point.

In contrast, $\mathbb{R}^\times\backslash\,\mathrm{GL}_2(\mathbb{R})/O_2(\mathbb{R})$ is the upper half plane (not present because D is totally definite).

And $\mathbb{C}^\times\backslash\,\mathrm{GL}_2(\mathbb{C})/U_2$ is hyperbolic 3-space (not present because F is totally real).

Automorphic forms

Say F is a totally real field and D/F is a totally definite quaternion algebra.

Then $D_f := D \otimes_F \mathbb{A}_F^f$ is a topological ring (D is F^4 as F-module, so D_f is $(\mathbb{A}_F^f)^4$ as $\mathbb{A}_F^f$-module. Give it the product topology; this works).

There's a canonical injective ring homomorphism $D \to D_f$.

So there's a canonical injective group homomorphism $D^\times \to D_f^\times$.

Let M be a set(!)

An M-valued *automorphic form* for $D^\times$ over F is a locally constant function $D_f^\times \to M$ which is constant on right cosets $D^\times g$ of $D^\times$.

In other words it's a locally constant function $D^\times \backslash D_f^\times \to M$.

$D^\times$ is not normal; $D^\times \backslash D_f^\times$ means right cosets $D^\times g$, with the pushforward (coinduced) topology.

Example: a constant function is an automorphic form!

Automorphic forms

F a totally real number field; D/F quaternion algebra; $D_f := D \otimes_F \mathbb{A}_F^f$ a topological ring, $D \to D_f$, so $D^\times \to D_f^\times$.

If M is any set, let $\mathcal{A}_D(M)$ denote the set of locally constant M-valued functions on $D^\times \backslash D_f^\times$.

$\mathcal{A}_D(M)$ is the set of M-valued (weight 0) *automorphic forms for D*.

The "M is a set" thing is just nonsense (it's a Leanism).

$\mathcal{A}_D(M)$ inherits structure from M.

For example, if M is an additive abelian group (which it is in the textbooks), $\mathcal{A}_D(M)$ is too (pointwise addition on functions).

And if M is a module over a ring R, $\mathcal{A}_D(M)$ is also naturally an R-module (pointwise scalar multiplication.)

To get a feeling for $\mathcal{A}_D(M)$ we're going to have to get a feeling for $D^\times \backslash D_f^\times$.

Action of $D_f^\times$ on automorphic forms

We've been considering the space $\mathcal{A}_D(M)$ of locally constant functions $D_f^\times \to M$ satisfying $f(dg) = f(g)$ for all $g \in D_f^\times$ and $d \in D^\times$.

I claim that the group $D_f^\times$ acts on $\mathcal{A}_D(M)$ by $(x \bullet f)(g) = f(gx)$.

There are some things one has to check here to justify this claim.

Firstly one has to check that $f' := x \bullet f$ is locally constant (obvious) and satisfies $f'(dg) = f'(g)$ (obvious).

And secondly one has to check the group action axioms and especially $x \bullet (y \bullet f) = (xy) \bullet f$.

Basically we need to make sure that $x \bullet (y \bullet f)$ doesn't unravel to $(yx) \bullet f$.

One way to do this is to pretend we're in a parallel universe where people write functions on the right. Then you can do the calculation in your head!

$(g)(x \bullet f) := (gx)f$.

Automorphic forms of fixed level

A “level” in this context is an open subgroup of $D_f^\times$.

Recall that an element of $\mathcal{A}_D(M)$ is a locally constant function $D_f^\times \to M$ satisfying $f(dg) = f(g)$ for all $g \in D_f^\times$ and $d \in D^\times$.

And the group $D_f^\times$ acts on $\mathcal{A}_D(M)$ via $(x \bullet f)(g) = f(gx)$.

Now fix an open subgroup $U \subseteq D_f^\times$.

Instead of just asking that f is locally constant, one could demand the stronger statement that $f(gu) = f(g)$ for all $g \in D_f^\times$ and $u \in U$.

That is, f isn’t just locally constant, it’s constant on left U-cosets.

To put it another way, one could ask that $u \bullet f = f$ for all $u \in U$.

So in fact such f’s make up the subset $\mathcal{A}_D(M)^U$ of U-invariants of $\mathcal{A}_D(M)$.

Let’s write $\mathcal{A}_D(U; M)$ for the U-invariants $\mathcal{A}_D(M)^U$. It’s the “forms of level U”.

Automorphic forms of fixed level

One crucial fact for understanding automorphic forms of fixed level:

$D^\times\backslash D_f^\times$, with the quotient topology, is compact (known in 1960s).

So if U is an open subgroup of $D_f^\times$ then the double coset space $D^\times\backslash D_f^\times/U$ is actually finite.

In particular, an element of $\mathcal{A}_D(U;M)$ is determined by a finite amount of data.

In fact $\mathcal{A}_D(U;M)$ bijects (unnaturally) with M^n for some natural $n=n(U)$.

(cf "$\mathbb{C}$-valued modular forms of a fixed weight and level are finite-dimensional over $\mathbb{C}$.")

The bijection sends f to $(f(g_1),f(g_2),\ldots,f(g_n))$ where g_i are a set of coset representatives for the finite double coset space $D^\times\backslash D_f^\times/U$.

Another consequence of compactness

If we give M the discrete topology, elements $f \in \mathcal{A}_D(M)$ are precisely continuous functions $D^\times \backslash D_f^\times \to M$.

Compactness of $D^\times \backslash D_f^\times$ implies that the image of f is finite.

One can show that the resulting open cover of $D^\times \backslash D_f^\times$ can be refined to a cover by left cosets of an open subgroup U.

In particular, $f \in \mathcal{A}_D(U; M)$.

Equivalently, the stabiliser of f in $D_f^\times$ is open.

So in fact $\mathcal{A}_D(M) = \bigcup_U \mathcal{A}_D(U; M) = \varinjlim_U \mathcal{A}_D(U; M)$ as U runs over open subgroups.

Example: if M is a field then M is a vector space over itself, so $\mathcal{A}_D(M)$ is also an M-vector space.

Above, we're writing $\mathcal{A}_D(M)$ as a union (or filtered colimit) of finite-dimensional M-vector spaces.

Hecke operators

I'll set up the theory of Hecke operators completely abstractly.

Let G be a topological group (for example $G = D_f^\times$).

Say G acts by group automorphisms on an additive abelian group A (for example $A = \mathcal{A}_D(M)$ where M is an additive abelian group.)

Variant: G acts by R-module automorphisms on an R-module A (for example $A = \mathcal{A}_D(M)$ where M is an R-module).

Now say $g \in G$, and also that U and V are compact open subgroups of G.

We're going to define an abelian group homomorphism $[UgV] : A^V \to A^U$.

(variant: if A is an R-module then $[UgV]$ is an R-module homomorphism.)

The definition is essentially combinatorial.

In the last episode...
Level 7: Introduction
Level 7: Quaternion algebras
Level 7: Finite adeles
Level 7: Hecke operators
Level 7: Maximal orders
Level 7: systems of eigenvalues
Level 7: potential automorphy

Abstract Hecke operators

Topological group G acting on additive abelian group (resp. R-module) A.

$g \in G$, and U, V are compact open subgroups of G.

Then the double coset $UgV \subseteq G$ is compact (it is a continuous image of $U \times V$).

So it is a *finite* disjoint union $\coprod_{i=1}^{n} g_i V$ of left cosets of V (as the cosets are open).

Choose g_i as above. If $f \in A^V$, then define $[UgV]f := \sum g_i \bullet f \in A$.

This sum doesn't depend on the choice of g_i, because replacing g_i by $g_i' := g_i v$ for $v \in V$ doesn't change $g_i \bullet f$, as $v \bullet f = f$.

Furthermore, $[UgV]f$ is U-invariant. Because if $u \in U$, then $u \bullet (\sum_i g_i \bullet f) = \sum_i ug_i \bullet f$ and $\coprod_i ug_i V = uUgV = UgV$.

Finally, $[UgV]$ is a sum of additive group homs (resp. R-module homs) so it's an additive group hom (resp. R-module hom.) And that's a Hecke operator.