Final Formalizing Fermat lecture

Kevin Buzzard, Imperial College London

Hoskinson Center, 8th December 2024

Last lecture

Welcome to the last Formalizing Fermat lecture, this week live from the Hoskinson center in Pittsburgh.

As is clear to everyone, I have been experimenting all term trying to find the right format for this class.

One thing I've noticed is that writing on the iPad was really slowing things down.

So today it's pdf slides.

Summary of today

I'm going to talk about three things today.

1) Haar characters (how units in rings scale Haar measure; I talked about this last time, but now I'm much clearer about exactly what we need).

2) Finite-dimensionality of relevant spaces of quaternionic modular forms;

3) Definition of the Hecke algebras acting on these spaces (short and easy).

Then people can go ahead and formalize stuff and I'll hang around on the Zoom call for questions.

Remark: the Hecke algebras are the "T"s in the "$R = T$ theorem" which we're going to formalize in the FLT project.

Part 1: Haar characters.

Haar characters

If R is a locally compact topological ring (doesn't have to be commutative) then $(R, +)$ is a locally compact topological abelian group and hence has a Haar measure μ (left and right measures are the same because $+$ is commutative).

Now if $u \in R^\times$ then left multiplication by u, $x \mapsto ux$, is an additive isomorphism $(R, +) \cong (R, +)$ and so it scales Haar measure by a positive real number $\delta_R(u) \in \mathbb{R}_{>0}$, or just $\delta(u)$ if R is clear.

Concretely: if $X \subseteq R$ is measurable then $\mu(uX) = \delta_R(u)\mu(X)$.

Conversely, if X has positive and finite measure, then you can use the above equation to get a formula for δ_R.

For example if you choose X such that $\mu(X) = 1$ then $\delta_R(u) = \mu(uX)$.

Examples

Example: if $R = \mathbb{R}$ then $\delta(u) = |u|$.

Proof: $u * [0,1] = [0,u]$ if $u > 0$ and this has length $|u|$.

And $u * [0,1] = [u,0]$ if $u < 0$ and this also has length $|u|$.

Example: if $R = \mathbb{C}$ then $\delta(u) = |u|^2$ (for example multiplication by 2 sends a unit square to a square of area 4).

If $R = \mathbb{Q}_p$ then $\delta(u) = |u|_p$, the usual p-adic norm.

If R is a finite extension of $\mathbb{Q}_p$ then $\delta(u)$ is the norm on R normalised in the following way: $\delta(\varpi) = q^{-1}$, where ϖ is a uniformiser and q is the size of the (finite) residue field.

This is because if $\mathcal{O}$ is the integers of R then $\varpi\mathcal{O}$ has index q in $\mathcal{O}$, and thus $\mathcal{O}$ is q times as big as $\varpi\mathcal{O}$.

Finite-dimensional vector spaces over a topological field

Now say F is a locally compact topological field (for example $\mathbb{R}$ or $\mathbb{C}$ or a finite extension of $\mathbb{Q}_p$), and R is a finite-dimensional F-algebra, and let's choose a basis so $R = F^N$ as F-module (with a random multiplication).

Now for $u \in R^\times$, left multiplication by u can be thought of as an F-linear endomorphism of F^N, so it has a determinant.

One can check that it scales Haar measure on F^N by $\delta_F(\det(u))$ (I think we may even have this in mathlib).

In other words, $\delta_R(u) = \delta_F(\det(u))$.

The non-commutative case

If R is non-commutative, then suddenly it matters whether we're doing left or right multiplication.

Example: let R be upper-triangular 2×2 matrices with real entries.

Then left multiplication by $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ sends $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ to $\begin{pmatrix} 2x & 2y \\ 0 & z \end{pmatrix}$, giving a scale factor of 4, but right multiplication sends it to $\begin{pmatrix} 2x & y \\ 0 & z \end{pmatrix}$, giving a scale factor of only 2.

What's going on here is that if we regard left and right multiplication as $\mathbb{R}$-linear maps from R to R, then their associated matrices wrt the obvious bases are $diag(2, 2, 1)$ and $diag(2, 1, 1)$, which have different determinants.

Central simple algebras

However, if F is a locally compact topological field and if B is a finite-dimensional central simple algebra over F (for example a quaternion algebra, the case we'll care about later), and if $u \in B^\times$ then $x \mapsto ux$ and $x \mapsto xu$ are both F-linear endomorphisms of $B \cong F^N$ and I claim that they have the same determinant.

Let's first check this for matrix algebras $B = M_n(F)$.

In this case, first one checks that both left and right multiplication by $g \in \mathrm{GL}_n(F)$, regarded as endomorphisms of $M_n(F) = F^{n^2}$, have determinant $\det(g)^n$.

(note a slightly confusing point: g is an $n \times n$ matrix but here we're sometimes regarding it as an n^2 by n^2 matrix).

Central simple algebras

Now let's imagine that F is a locally compact topological field and B is a general finite-dimensional central simple algebra over F.

This implies that there's some finite extension E/F such that $B \otimes_F E$ is isomorphic to $M_n(E)$ as E-algebras.

So if $u \in B^\times$ (which now isn't a matrix), left and right multiplication by u induce two F-linear maps u_l and $u_r : B \to B$ which scale Haar measure by $\delta_F(\det(u_l))$ and $\delta_F(\det(u_r))$.

Now tensor up to E. Then $u \otimes 1 \in B \otimes_F E = M_n(E)$ becomes a matrix with its own intrinsic determinant d, and we just saw that $\det(u_l) = d^n = \det(u_r)$.

Hence $\delta_F(\det(u_l)) = \delta_F(\det(u_r))$, and thus left and right multiplication by elements of $B^\times$ scale Haar measure by the same amount.

Haar character

I'm not entirely sure what to call δ, but its existence relies on the distributivity axiom, so we've called it `distribHaarChar` in the FLT Lean repo.

Easy to check: $\delta_{R\times S}(r,s)=\delta_R(r)\times\delta_S(s)$.

Another fun fact: if R is the restricted product of a bunch of topological rings R_i over a bunch of compact open subrings C_i then $\mu_R(\prod_i x_i)=\prod_i \mu_{R_i}(x_i)$ and the product is finite (in the sense that all but finitely many of the x_i are in $C_i^\times$ and hence $x_iC_i=C_i$ and thus $\mu(x_i)=1$).

Proof: look at what x does to $\prod_i C_i$ (which has nonzero positive measure).

Adeles

We have seen that if v is a place of $\mathbb{Q}$ (i.e., a prime number or $+\infty$) then $\delta_{\mathbb{Q}_v} = |\cdot|_v$.

We can deduce from this that if $(x_v)_v \in \mathbb{A}_{\mathbb{Q}}^\times$ then $\delta_{\mathbb{A}_{\mathbb{Q}}}((x_v)) = \prod_v |x_v|_v$.

The *product formula* (on the way to mathlib) says that if $x \in \mathbb{Q}^\times$ then $\prod_v |x|_v = 1$.

(proof: if $x = \pm\prod_p p^{e_p}$ then $\prod_p |x|_p = \prod_p p^{-e_p}$ and $|x|_\infty = \prod_p p^{e_p}$ so they cancel.)

Thus $\delta_{\mathbb{A}_{\mathbb{Q}}}(\mathbb{Q}^\times) = \{1\}$.

Generalization

Now say B is a possibly non-commutative $\mathbb{Q}$-algebra, finite-dimensional of dimension N over $\mathbb{Q}$, and $B_{\mathbb{A}} := B \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}$.

(note that if B is an algebra over a number field K then $B_{\mathbb{A}}$ is also $B \otimes_K \mathbb{A}_K$.)

Then as an additive topological abelian group, $B_{\mathbb{A}} \equiv \mathbb{A}_{\mathbb{Q}}^N$.

So if $u \in B^\times$, $\delta_{B_{\mathbb{A}}}(u) = \prod_v \delta_{B_v}(u)$ (a product over the places of $\mathbb{Q}$) with $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$.

And this is $\prod_v \delta_{\mathbb{Q}_v}(\mathrm{det}(u))$, where $\mathrm{det}(u) \in \mathbb{Q}^\times$ is the determinant of left muliplication by u regarded as a $\mathbb{Q}$-linear automorphism of $B = \mathbb{Q}^N$.

And this is 1 by the product formula.

I'll end by noting that if B is furthermore a central simple algebra, then right multiplication by an element $u \in B_{\mathbb{A}}^\times$ on $B_{\mathbb{A}}$ scales Haar measure by $\delta_{B_{\mathbb{A}}}(u)$, because the factor is a product of local terms, and we already saw that left and right multiplication change Haar measure locally in the same way.

Part 2: Quaternionic modular forms.

Quaternionic modular forms

Reminder of the definition of the spaces we're interested in (for simplicity let's stick to weight 2):

F a totally real number field (e.g. $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{2})$).

D/F a totally definite quaternion algebra (e.g. $F \oplus Fi \oplus Fj \oplus Fk$).

$\mathbb{A}_F^\infty$ the finite adeles of F, a huge (but locally compact) topological commutative ring containing a copy of F (it's $F \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$).

The ring $D_f := D \otimes_F \mathbb{A}_F^\infty$ is then a locally compact topological ring (finite and free of rank 4 over $\mathbb{A}_F^\infty$ as a module, with product topology).

The ring D_f is an F-algebra containing a copy of D.

Its units $D_f^\times$ are thus a locally compact topological group containing $D^\times$.

Quaternionic modular forms

We have this huge locally compact topological group $D_f^\times$, containing a copy of $D^\times$.

Let U be a "level" (that is, a compact open subgroup of $D_f^\times$).

A weight 2 modular form of level U is a function $f : D_f^\times \to \mathbb{C}$ satisfying two axioms:

(1) $f(dg) = f(g)$ for $d \in D^\times$; (weight 2)

(2) $f(gu) = f(g)$ for $u \in U$. (level U)

Note that (2) implies that f is locally constant and in particular continuous.

Weight 2 modular forms of level U are a complex vector space (addition and scalar multiplication defined via action on the target $\mathbb{C}$).

Quaternionic modular form

$U \subset D_f^\times$ compact open; weight 2 modular forms of level U is $S_2(U) := \{f : D^\times \backslash D_f^\times / U \to \mathbb{C}\}$.

Theorem

$S_2(U)$ is a finite-dimensional complex vector space.

Equivalently, $D^\times \backslash D_f^\times / U$ is a finite set.

Equivalently, $D^\times \backslash D_f^\times$ is compact.

Last time

Last time I sketched why the quotient $D\backslash(D \otimes_F \mathbb{A}_F)$ was compact.

The proof: D is finite-dimensional over F and thus finite-dimensional over $\mathbb{Q}$ (say N-dimensional), and one checks using $\mathbb{A}_F = \mathbb{A}_\mathbb{Q} \otimes_\mathbb{Q} F$ that this space is just $(\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q})^N$.

One proves that $\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q}$ is compact via an explicit calculation: the natural map from $\widehat{\mathbb{Z}} \times [0, 1]$ to this space is continuous and surjective so done.

But you can't just now "take the units".

For example $\mathbb{R}/\mathbb{Z}$ is compact but $\mathbb{R}^\times/\mathbb{Z}^\times$ is not.

Similarly here, $D^\times\backslash(D \otimes_F \mathbb{A}_F)^\times$ is also not compact if you use the full ring of adeles $\mathbb{A}_F$, because if $[F : \mathbb{Q}] = n$ then although the integers of F have $\mathbb{Z}$-rank n, the global units of F only have rank $n - 1$ (so compactness is not even true for $D = F$, let alone if D is a quaternion algebra).

The actual argument is rather more delicate, and I'll sketch it now.

The theorem we'll prove

Let K be a number field (for example a totally real field).

Let B be is a finite-dimensional division algebra over K (for example a totally definite quaternion algebra) (note that division algebras are central simple algebras.)

Let $B_{\mathbb{A}}$ denote $B \otimes_K \mathbb{A}_K$, a locally compact topological ring.

Let $\delta : B_{\mathbb{A}}^\times \to \mathbb{R}_{>0}$ be the Haar character, and let $B_{\mathbb{A}}^{(1)}$ denote the kernel of δ (so $B^\times \subset B_{\mathbb{A}}^{(1)}$ by the product formula).

Theorem

The quotient $B^\times \backslash B_{\mathbb{A}}^{(1)}$ is compact.

Application

Note: this theorem implies finite-dimensionality of the space of quaternionic modular forms over a totally real field.

Indeed take $K = F$, $B = D$. Theorem says $D^\times \backslash D_{\mathbb{A}}^{(1)}$ is compact. Want $D^\times \backslash (D_{\mathbb{A}}^f)^\times$ compact.

So it suffices to prove that the natural continuous map from $D_{\mathbb{A}}^{(1)}$ to $D_f^\times$ ("forget the infinite places") is a surjection (as cts image of compact is compact).

Just to orient you: $D_{\mathbb{A}}^{(1)}$ has stuff at infinite places, but some product must be 1; $D_f^\times$ has just stuff at finite places, but no condition on some character being 1.

Natural map is surjective

Need that the map $D_{\mathbb{A}}^{(1)} \to D_f^\times$ is surjective.

In other words, given a random element of $D_f^\times$, whose Haar character will be a random positive real number, we need to find an element of $D_\infty := D \otimes_{\mathbb{Q}} \mathbb{R}$ whose Haar character is the inverse of this.

But one checks easily that if D_∞ has dimension N over $\mathbb{R}$ and $u \in \mathbb{R}^\times$ then $\delta_{D_\infty}(u) = |u|^N$ (because this is $\delta_{\mathbb{R}}(det(u))$ with u now regarded as an $N \times N$ scalar matrix) and this takes all positive real values.

The story so far

So far we've seen that to prove that the space of quaternionic modular forms is finite-dimensional, it suffices to prove the following:

If K is a number field, B/K is a finite-dimensional division algebra, and $B_{\mathbb{A}}^{(1)}$ denotes the kernel of the Haar character on the units of $B_{\mathbb{A}} := B \otimes_K \mathbb{A}_K$, then (a) $B^\times \subset B_{\mathbb{A}}^{(1)}$ and (b) it suffices to prove that $B^\times \backslash B_{\mathbb{A}}^{(1)}$ is compact.

Remark: This $^{(1)}$ business drops a factor of $\mathbb{R}_{>0}$ and this is exactly how we get from degree n totally real fields to their units having rank $n-1$.

Remark: if $B = K$ then this theorem is equivalent to the claims that the class group of K is finite, and the unit group has rank $r+s-1$.

Proof of the theorem

Notation: B our division algebra over number field K, $B_f = B \otimes_K \mathbb{A}_K^\infty$, $B_\mathbb{A} = B \otimes_K \mathbb{A}_K$.

Step 1. There's a compact subset E of $B_\mathbb{A}$ with the property that for all $x \in B_\mathbb{A}^{(1)}$, the obvious map $xE \to B\backslash B_\mathbb{A}$ is not injective.

Proof.

We know that $B\backslash B_\mathbb{A} = (\mathbb{Q}\backslash\mathbb{A}_\mathbb{Q})^N$ is compact, and that B is discrete in $B_\mathbb{A}$ (from last time).

Fix a Haar measure μ on $B_\mathbb{A}$ and push it forward to $B\backslash B_\mathbb{A}$; this quotient has finite and positive measure, say $m \in \mathbb{R}_{>0}$.

Choose any compact $E \subseteq B_\mathbb{A}$ with measure $> m$.

Then $\mu(xE) = \mu(E) > m$ so the map can't be injective. □

Big sets

Remark: how we do know that there exists $E \subseteq B_{\mathbb{A}}$ with measure $> m$?

For example, we could choose a random lattice $\mathbb{Z}$-lattice L in B, start with the compact $L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \times X$ where X is some closed ball in $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^N$ (its interior is nonempty so the measure is positive), and then just take disjoint additive translates until the measure is big enough.

Step 2.

We have this compact E with big measure, in a topological ring, and now set $X = E - E = \{e - f : e, f \in E\}$ and $Y = X * X = \{x * y : x, y \in X\}$.

Then X and Y are also compact subsets of $B_{\mathbb{A}}$ as they're continuous images of compact sets.

Step 3. We claim that if $\beta \in B_{\mathbb{A}}^{(1)}$ then $\beta X \cap B^{\times} \neq \emptyset$.

Indeed by Step 1, the map $\beta E \to B \backslash B_{\mathbb{A}}$ isn't injective, so there are distinct $\beta e_1, \beta e_2 \in \beta E$ with $\beta e_1 - \beta e_2 = b \in B$.

And $b \neq 0$ and B is a division algebra, so $b \in B^{\times}$.

And $e_1 - e_2 \in X$ so $b = \beta(e_1 - e_2) \in \beta X$, so done.

Step 4 Similarly, if $\beta \in B_{\mathbb{A}}^{(1)}$ then I claim $X\beta^{-1} \cap B^{\times} \neq \emptyset$.

Indeed, $\beta^{-1} \in B_{\mathbb{A}}^{(1)}$, and so left multiplication by β^{-1} doesn't change Haar measure on $B_{\mathbb{A}}$, so neither does right multiplication (as they change Haar measure by the same amount, as B is a form of a matrix algebra).

So the same argument works: $E\beta^{-1} \to B\backslash B_{\mathbb{A}}$ is not injective so choose $e_1\beta^{-1} \neq e_2\beta^{-1}$ with difference $b \in B$ and then $(e_1 - e_2)\beta^{-1} \in B^{\times}$.

Step 5 Recall $Y = X * X \subset B_{\mathbb{A}}$ is compact. I claim that $Y \cap B^\times$ is finite.

Proof.

It suffices to prove that $Y \cap B$ is finite.

But $B \subseteq B_{\mathbb{A}}$ is a discrete additive subgroup, and hence closed.

And $Y \subseteq B_{\mathbb{A}}$ is compact.

So $B \cap Y$ is compact and discrete, so finite. $\square$

Now let $T = Y \cap B^\times$ be this finite subset of $B_{\mathbb{A}}$, and define $K := (T^{-1} * X) \times X \subset B_{\mathbb{A}} \times B_{\mathbb{A}}$, noting that K is compact because X is compact and T is finite.

Step 6 For every $\beta \in B_{\mathbb{A}}^{(1)}$, there exists $b \in B^\times$ and $\nu \in B_{\mathbb{A}}^{(1)}$ such that $\beta = b\nu$ and $(\nu, \nu^{-1}) \in K$.

Before we prove this, let's show that it implies what we want, namely that $B^\times \backslash B_{\mathbb{A}}^{(1)}$ is compact.

Indeed, if M is the preimage of K under the map $B_{\mathbb{A}}^{(1)} \to B_{\mathbb{A}} \times B_{\mathbb{A}}$ sending ν to (ν, ν^{-1}), then M is a closed subspace (assuming $\delta_{B_{\mathbb{A}}}$ is continuous!) of a compact space so it's compact, and step 6 shows that M surjects onto $B^\times \backslash B_{\mathbb{A}}^{(1)}$ which is thus also compact.

End of the proof

It suffices then to show that for every $\beta \in B_{\mathbb{A}}^{(1)}$, there exists $b \in B^\times$ and $\nu \in B_{\mathbb{A}}^{(1)}$ such that $\beta = b\nu$ and $(\nu, \nu^{-1}) \in K$.

By step 3, $\beta X \cap B^\times \neq \emptyset$, and by step 4, $X\beta^{-1} \cap B^\times \neq \emptyset$, so we can write $\beta x_1 = b_1$ and $x_2\beta^{-1} = b_2$ with obvious notation.

Multiplying, $x_2x_1 = b_2b_1 \in Y \cap B^\times = T$ (recall that $Y = X * X$ and $T = Y \cap B^\times$ is finite); call this element t. Note that $T \subset B^\times$ so t is a unit, and thus x_1, x_2 are units (a left or right divisor of a unit is a unit; this is a general fact about subrings of matrix rings and may be true more generally).

Then $x_1^{-1} = t^{-1}x_2 \in T^{-1} * X$, and $x_1 \in X$, so if we set $\nu = x_1^{-1}$ and $b = b_1$ then we have $\beta = b\nu$ and $(\nu, \nu^{-1}) \in K := (T^{-1} * X) \times X$.

Done!

Remark

Note that this last part of the argument was certainly long, but it was not technical, it was just inelegant.

If we can get this done before the analysts figure out how to integrate around wacky contours in the upper half plane, then we've proved finite-dimensionality of quaternionic modular forms before they've proved finite-dimensionality of classical modular forms :-)

Part 3 (all downhill from here): Hecke algebras acting on spaces of quaternionic modular forms.

Abstract set-up

Say we have some abelian group A of “forms”, and a group (or a monoid) G acting on the left on this abelian group.

If U is a subgroup of G, then we define the U-invariant forms A^U to be the $a \in A$ such that $u \bullet a = a$ for all $u \in U$.

Now say V is another subgroup of G, say $g \in G$, and assume that the double coset VgU is a *finite* union of single cosets $\coprod_{i=1}^{n} g_i U$.

Under this finiteness hypothesis, there’s a Hecke operator $[VgU] : A^U \to A^V$ defined by sending $a \in A^U$ to $\sum_i (g_i \bullet a)$.

I claim that this is a well-defined abelian group homomorphism.

Hecke operators

G acts on A, $U, V \subseteq G$, $g \in G$, $VgU = \coprod_{i=1}^{n} g_i U$.

$[VgU] : A^U \to A^V$ defined by $a \mapsto \sum_{i=1}^{n}(g_i a)$.

Clearly this map from A^U to A is independent of the choice of g_i in the coset $g_i U$, as $g_i u \bullet a = g_i \bullet a$.

Clearly an additive group homomorphism.

Suffices to prove that the image is in A^V.

And if $v \in V$ then $vg_i U$ is another left coset of U in VgU so it's $g_{i'} U$, with $i \mapsto i'$ a permutation of $\{1, 2, 3, \ldots, n\}$ (depending on v) (it's a permutation because left multiplication by v^{-1} undoes it).

Hence $v \bullet [VgU]a = [VgU]a$ (it rearranges the sum) and we're done.

Extra bells and whistles

Extra actions: if R is some random ring acting on A and making A into an R-module (for example $R = \mathbb{C}$ and A is a complex vector space) and the G-action on A is R-linear, then A^U is also an R-module, and $[VgU]$ is R-linear.

If $U = V$ then $[UgU] : A^U \to A^U$ is an additive endomorphism of A^U, and we call it the Hecke operator T_g.

Note: for all this to make sense we need the finiteness hypothesis that $VgU = \coprod_{i=1}^{n} g_i U$ is a finite union of left cosets.

Concrete application

Let A be the locally constant $\mathbb{C}$-valued functions $D^\times \backslash D_f^\times$.

Let G be $D_f^\times$.

Define $(g \bullet f)(x) = f(xg)$.

Who knows the way to check that this is a valid left action without doing any calculations?

Temporarily write maps on the right, $(x)(g \bullet f) = (xg)f$.

Then the axiom just involves shuffling brackets around and changing $\bullet$s to $*$s and back.

Concrete application

If U is a compact open subgroup of $D_f^\times$ then A^U is the weight 2 modular forms of level U.

If $g \in D_f^\times$, why is UgU a finite union of $g_i U$?

Because UgU is compact, and the cover by left cosets $g_i U$ is an cover by disjoint opens.

And those are the Hecke operators we'll be using.

Concrete Hecke operators

In fact all we'll need is the following special case.

F totally real, D/F totally definite quaternion algebra, and assume $D_v := D \otimes_F F_v \cong M_2(F_v)$ for all finite places v of F.

Remark: earlier in these slides v was the variable for "arbitrary place of $\mathbb{Q}$"; now it's the variable for "arbitrary finite place of F".

Fix an $\mathcal{O}_F$-stable $\mathbb{Z}$-lattice L in the $\mathbb{Q}$-vector space D (an "order").

Fix isomorphisms $D \otimes_F F_v = M_2(F_v)$ ensuring that for all but finitely many v we have $L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v} = M_2(\mathcal{O}_{F_v})$.

Concrete Hecke operators

Let $U = \prod_v U_v$ is a product of compact open subgroups of $D_v^\times = GL_2(F_v)$ as v runs through the finite places of F, and assume $U_v = GL_2(\mathcal{O}_v)$ for all $v \notin S$ some finite set.

For those finite $v \notin S$, set $g_v = \begin{pmatrix} \varpi & 0 \\ 0 & 1 \end{pmatrix}$.

Let T_v be $[Ug_vU]$.

Let $\mathbb{T}$ denote the subalgebra of $End_{\mathbb{C}}(S_2(U))$ generated by the T_v for $v \notin S$.

Commutativity

Claim: $\mathbb{T}$ is commutative.

Proof: it suffices to show that if $v \neq w$ then $T_v T_w = T_w T_v$.

But $T_v f = \sum_i g_{v,i} \bullet f$, and it's not hard to check that the $g_{v,i}$ can be chosen to all have support in $\mathrm{GL}_2(F_v)$.

Hence $g_{v,i}$ commutes with $g_{w,j}$ and this is all we need.

QED.

Summary/what's next

These pdf notes explain how to construct the Hecke algebra $\mathbb{T}$ which we'll plug into the abstract $R = \mathbb{T}$ theorem.

I think we have a path to a sorry-free proof of finite-dimensionality.

Finite-dimensionality of the spaces of forms can be used to show that $\mathbb{T}$ is Noetherian.

It will also then be easy to *state* an extremely profound theorem of Carayol/Langlands/Deligne/Taylor attaching Galois representations to quaternionic forms which are eigenforms for the Hecke operators.

This theorem was proved in the 1980s so we can assume it for now.

Which is good because the proof involves analysing p-adic etale cohomology of Shimura curves and surfaces parametrising families of abelian varieties with PEL structure, and the reduction theory of these varieties at bad places.

$R \to T$

The Deligne/Langlands/Carayol/Taylor theorem attaches a Galois representation to a character of $\mathbb{T}$.

This can then be massaged into the definition of the ring homomorphism $R \to \mathbb{T}$, as R is a univeral deformation ring.

Andrew's work can then hopefully be used to show that it's an isomorphism (modulo nilpotents) (assuming lots of class field theory).

And then we profit.

Sorry this course was so disorganized; I took on far too much this term.

Let's go write some Lean code. Thanks for coming.