Computing with algebraic automorphic forms

David Loeffler

Abstract These are the notes of a five-lecture course presented at the *Computations with modular forms* summer school, aimed at graduate students in number theory and related areas. Sections 1–4 give a sketch of the theory of reductive algebraic groups over $\mathbf{Q}$, and of Gross's purely algebraic definition of automorphic forms in the special case when $G(\mathbf{R})$ is compact. Sections 5–9 describe how these automorphic forms can be explicitly computed, concentrating on the case of definite unitary groups; and sections 10 and 11 describe how to relate the results of these computations to Galois representations, and present some examples where the corresponding Galois representations can be identified, giving illustrations of various instances of Langlands' functoriality conjectures.

1 A user's guide to reductive groups

References for this section: Springer's lecture notes in the Corvallis proceedings [20] give a very readable summary. For more details, see e.g. Humphreys [14] or Springer [21], or chapter 2 of Platonov–Rapinchuk [18].

Let F be a field. An *algebraic group* over F is a group object in the category of algebraic varieties over F. More concretely, it is an algebraic variety G over F together with:

- a "multiplication" map $G \times G \to G$,
- an "inversion" map $G \to G$,
- an "identity", a distinguished point of $G(F)$.

These are required to satisfy the obvious analogues of the usual group axioms. Then $G(A)$ is a group, for any F-algebra A. It's clear that we can define a *morphism* of

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK, e-mail: d.a.loeffler@warwick.ac.uk

algebraic groups over F in an obvious way, giving us a category of algebraic groups over F.

Some important examples of algebraic groups include:

- Finite groups (considered as zero-dimensional algebraic groups)
- The additive and multiplicative groups (usually written $\mathbb{G}_a$ and $\mathbb{G}_m$),
- Elliptic curves (with the group law given by the usual chord-and-tangent process),
- The group GL_n of $n \times n$ invertible matrices, and the subgroups of symplectic matrices, orthogonal matrices, etc.

We say an algebraic group G over F is *linear* if it is isomorphic to a closed subgroup of GL_n for some n. In particular, every linear algebraic group is an affine variety, so elliptic curves are not linear groups. One can show that the converse is true: every affine algebraic group is linear. In this course we'll be talking exclusively about linear groups.

Exercise 1. Show that PGL_2, the quotient of GL_2 by the subgroup of diagonal matrices, is a linear algebraic group, without using the above theorem.

We'll also mostly assume our algebraic groups are *connected*, by which we mean that they're connected in the Zariski topology. Be warned that if F has a topology, it may happen that G is connected but the group of F-points is not connected with the topology it inherits from F, as the example of $\mathbb{G}_m$ over $\mathbf{R}$ shows.

The final restriction we'll impose is a rather technical one. Let $\mathrm{Unip}(n)$ be the group of upper-triangular matrices with 1's on the diagonal (unipotent matrices). We say G is *reductive* if there is no connected normal subgroup $H \triangleleft G$ which is isomorphic to a subgroup of $\mathrm{Unip}(n)$ for any n.

This is a horrible definition; one can make it a bit more natural by developing some general structure theory of linear algebraic groups, but we sadly don't really have time. I'll just mention that reductive groups have many nice properties non-reductive groups don't; if G is reductive (and the base field F has characteristic 0), the category of representations[1] of G is semisimple (every representation is a direct sum of irreducibles). For non-reductive groups this can fail. For instance $\mathrm{Unip}(2)$, which is just another name for the additive group $\mathbb{G}_a$, has its usual 2-dimensional representation, and this representation has a trivial 1-dimensional sub with no invariant complement.

For instance, the group GL_n is reductive for any n, as are the symplectic and orthogonal groups. If F is algebraically closed (and let's say of characteristic 0, just to be on the safe side), then there is a classification of reductive groups over F using linear algebra widgets called *root data*. One finds that they are all built up from products of copies of GL_1 ("tori") and other building blocks called "simple" algebraic groups. The simple algebraic groups are: four infinite families A_n, B_n, C_n, D_n; and five exceptional simple groups E_6, E_7, E_8, F_4, G_2.

[1] Here "representation" is in the sense of algebraic groups: just a morphism of algebraic groups from G to GL_n for some n.

Over non-algebraically-closed fields F, life is much more difficult, since we can have pairs of groups G, H which are both defined over F, with G not isomorphic to H over F, but $G \cong H$ over some finite extension of F. For instance, let $F = \mathbf{R}$, and consider the "circle group"

$$C = \{(x,y) \in \mathbb{A}^2 : x^2 + y^2 = 1\}, \quad (x,y) \cdot (x',y') = (xx - yy', xy' + yx').$$

One can show that C becomes isomorphic to $\mathbb{G}_m$ over $\mathbf{C}$, although these two groups are clearly not isomorphic over $\mathbf{R}$.

Exercise 2. Check this.

If G and H are groups over F which become isomorphic after extending to some extension E/F, then we say H is an *E/F-form* of G. One can show that if E/F is Galois, the E/F-forms of G are parametrised by the cohomology group $H^1(E/F, \mathrm{Aut}(G_E))$, where $\mathrm{Aut}(G_E)$ is the (abstract) group of algebraic group automorphisms of G over E. To return to our circle group example for a moment, if $G = \mathbb{G}_m$ then $\mathrm{Aut}(G_E) = \pm 1$ for any E, and $H^1(\mathbf{C}/\mathbf{R}, \pm 1)$ has order 2, so the only $\mathbf{C}/\mathbf{R}$-forms of G are the circle group C and $\mathbb{G}_m$ itself.

If G is connected and reductive, then there's a unique "best" form of G, the *split form*, which is characterised by the property that it contains a subgroup isomorphic to a product of copies of $\mathbb{G}_m$ (a *split torus*) of the largest possible dimension. So the group C above is not split, and its split form is $\mathbb{G}_m$.

For more details on linear algebraic groups, consult a book. There are several excellent references for the theory over an algebraically closed field, such as the books of . For the theory over a non-algebraically-closed field, the book by Platonov and Rapinchuk [18] is a good reference; this is also useful reading for some of the later sections of this course.

2 Algebraic groups over number fields

One standard reference for this section is [18], particularly chapters 4 and 5. The first few sections of [13] give a useful summary with pointers to the original literature. For more on the theory over local fields see [22] or chapter 3 of [18].

Let's consider a linear algebraic group over a number field F.

In fact, it'll suffice for everything we do here to consider an algebraic group over $\mathbf{Q}$. That's because there's a functor called "restriction of scalars" (sometimes "Weil restriction") from algebraic groups over F to algebraic groups over $\mathbf{Q}$; if G is an algebraic group over F, there is a unique algebraic group H over $\mathbf{Q}$ with the property that for any $\mathbf{Q}$-algebra A we have

$$H(A) = G(F \otimes_{\mathbf{Q}} A).$$

This group H is the restriction of scalars of G, and we call it $\mathrm{Res}_{F/\mathbf{Q}}(G)$. See Paul Gunnells' lecture notes in this volume for an explicit description of this functor and

lots of examples; alternatively, see [18, §2.1.2]. If G is reductive, so is $\mathrm{Res}_{F/\mathbf{Q}}(G)$, and for the purposes of computing automorphic forms, one can more or less forget the original group over F and just work with this new group over $\mathbf{Q}$.

So let G be a linear algebraic group over $\mathbf{Q}$, which (largely for simplicity) we'll suppose is connected. Then we can consider the groups $G(\mathbf{Q}_v)$ for each place v of $\mathbf{Q}$. These are topological groups, since the field $\mathbf{Q}_v$ has a topology.

If v is a finite prime p, then $G(\mathbf{Q}_p)$ "looks like the p-adics"; it's totally disconnected. In particular, it has many open compact subgroups, and these form a basis of neighbourhoods of the identity. (This is obvious for GL_n – the subgroups of matrices in $\mathrm{GL}_n(\mathbf{Z}_p)$ congruent to the identity mod p^m, for $m \geq 1$, work – and hence follows for any linear algebraic group.) In the other direction, one can show that $G(\mathbf{Q}_p)$ has *maximal* compact subgroups if and only if G is reductive; compare the additive group $\mathbb{G}_a$, whose $\mathbf{Q}_p$-points clearly admit arbitrarily large open compact subgroups. There is a beautiful theory due to Bruhat and Tits which describes the maximal compact subgroups of $G(\mathbf{Q}_p)$, for connected reductive groups G over $\mathbf{Q}_p$, in terms of a geometric object called a *building*, but we won't go into that here.

One thing that'll be useful to us later is this: if we fix a choice of embedding of G into GL_n, and let $K_p = G(\mathbf{Z}_p) = G(\mathbf{Q}_p) \cap \mathrm{GL}_n(\mathbf{Z}_p)$, then for all but finitely many primes p, K_p is a maximal compact subgroup. In fact we can do better than this; for all but finitely many p, K_p is *hyperspecial*, a technical condition from Bruhat–Tits theory, which will crop up again later when we talk about Hecke algebras. For instance, $\mathrm{GL}_n(\mathbf{Z}_p)$ is a hyperspecial maximal compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$ for all p.

Exercise 3. Find an embedding $\iota : \mathrm{GL}_2 \hookrightarrow \mathrm{GL}_n$ of algebraic groups over $\mathbf{Q}_p$, for some n, such that $\iota^{-1}(\mathrm{GL}_n(\mathbf{Z}_p))$ is a proper subgroup of $\mathrm{GL}_2(\mathbf{Z}_p)$.

For the real points of a reductive group, the story is a bit different. If G is Zariski connected, then it needn't be the case that $G(\mathbf{R})$ is connected (for instance $\mathbb{G}_m$), but $G(\mathbf{R})$ will have finitely many connected components. Hence it can't have open compact subgroups unless it's compact itself.

It turns out that the maximal compact subgroups can be very nicely described in terms of Lie group theory (more specifically, in terms of the action of complex conjugation on the Lie algebra of $G(\mathbf{C})$). In particular, they're all conjugate, so in most applications it doesn't matter very much which one you work with.

For example, in $SL(2,\mathbf{R})$ the maximal compact subgroups are conjugates of the group

$$SO(2,\mathbf{R}) = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x^2 + y^2 = 1 \right\}.$$

Exercise 4. Check that the group $SO(2,\mathbf{R})$ is the stabiliser of i, for the usual left action of $SL(2,\mathbf{R})$ on the upper half-plane $\mathfrak{h}$; the action of $SL(2,\mathbf{R})$ on $\mathfrak{h}$ is transitive; and the resulting bijection

$$\mathfrak{h} \cong SL(2,\mathbb{R})/SO(2,\mathbb{R})$$

is a diffeomorphism.

In general, if $K \subseteq G(\mathbb{R})$ is maximal compact, the quotient $G(\mathbb{R})/K$ is a very interesting manifold, called a *symmetric space*. As the above exercise shows, these are the appropriate generalisations of the upper half-plane $\mathfrak{h}$, so they will come up all over the theory of automorphic forms. Many of these symmetric spaces have names, such as "hyperbolic 3-space" or the "Siegel upper half-space".

Now let's consider all primes simultaneously. Let $\mathbf{A}$ be the ring of adeles of $\mathbf{Q}$, and consider the group $G(\mathbf{A})$. This inherits a topology[2] from the topology of $\mathbf{A}$. Since $\mathbf{A}$ is a restricted direct product of the completions of $\mathbf{Q}$, we have a corresponding decomposition

$$G(\mathbf{A}) = \prod_v{}' G(\mathbf{Q}_v),$$

where the dash means to take elements whose component at v lies in $G(\mathbf{Z}_p)$ for all but finitely many[3] primes p.

We'll also need to consider the *finite adeles* $\mathbf{A}_f = \prod'_{v<\infty} \mathbf{Q}_v$, and the corresponding group

$$G(\mathbf{A}_f) = \prod_{v<\infty}{}' G(\mathbf{Q}_v)$$

of $\mathbf{A}_f$-points of G. Note that $G(\mathbf{Q})$ sits inside $G(\mathbf{A})$, via the diagonal embedding $\mathbf{Q} \hookrightarrow \mathbf{A}$. We will also sometimes consider $G(\mathbf{Q})$ as a subgroup of $G(\mathbf{A}_f)$, by neglecting the component at ∞; hopefully it will always be clear which we are using!

The first key result about these groups is the following (see e.g. chapter 5 of [18]):

Theorem 5 (Harish-Chandra, Borel). *The group $G(\mathbf{Q})$ is discrete in $G(\mathbf{A})$; and if G has no quotient isomorphic to $\mathbb{G}_m$, then the quotient $G(\mathbf{Q})\backslash G(\mathbf{A})$ has finite Haar measure.*

The quotient space $G(\mathbf{Q})\backslash G(\mathbf{A})$ is immensely important for us, as it is the home of automorphic forms.

3 Automorphic forms

References: the books of Bump [2] and Gelbart [11], or the more recent book of Cogdell–Kim–Murty [5], are very useful, although they tend to concentrate mainly

[2] One has to be a little careful in defining this topology. One can equip $\mathrm{GL}_n(\mathbf{A})$ with the subspace topology that comes from regarding it as an open subset of $\mathrm{Mat}_{n\times n}(\mathbf{A})$, where $\mathrm{Mat}_{n\times n}(\mathbf{A}) \cong \mathbf{A}^n$ has the product topology; but this is not the right topology, as inversion is not continuous (exercise!). Much better is to regard $\mathrm{GL}_n(\mathbf{A})$ as a *closed* subset of $\mathrm{Mat}_{n\times n}(\mathbf{A}) \times \mathbf{A} \cong \mathbf{A}^{n+1}$, given by $\{(m,x) : \det(m)x = 1\}$. We then get a topology on $G(\mathbf{A})$ for every linear group G by embedding it in GL_n for some n.

[3] Note that to define $G(\mathbf{Z}_p)$ we need to choose an embedding into GL_n, as above; but changing our choice of embedding will only affect finitely many primes, so it introduces no ambiguity in the restricted product.

on $G = \mathrm{GL}_n$ (or often just on GL_2). For a clear presentation of the theory for a general reductive group, the article of Borel and Jacquet in the Corvallis proceedings [1] is a good place to look.

Let G be a connected reductive group over $\mathbf{Q}$, as above. Let $K_\infty \subseteq G(\mathbf{R})$ be a maximal compact subgroup, and V a finite-dimensional irreducible complex representation of K_∞.

Definition 6. An *automorphic form* for G of weight V is a function

$$\phi : G(\mathbf{A}) \to V$$

such that:

1. $\phi(\gamma g k) = \phi(g)$ for all $g \in G(\mathbf{A})$, $\gamma \in G(\mathbf{Q})$, and $k \in K_f$, where K_f is some open compact subgroup of $G(\mathbf{A}_f)$;
2. $\phi(g k_\infty) = k_\infty^{-1} \circ f(g)$ for all $g \in G(\mathbf{A})$ and $k \in K_\infty$;
3. various conditions of smoothness and boundedness hold.

If ϕ satisfies (1) for some specific open compact subgroup K_f, we say ϕ is an automorphic form of *level* K_f.

I won't explain exactly what kind of smoothness and boundedness conditions are involved here; for a precise statement, see the books listed above. (As we'll see in the next section, the purpose of these notes is precisely to focus on the cases where these analytic hypotheses are not relevant.)

Let's now see how this relates to more familiar things, like modular curves. For an open compact subgroup $K_f \subset G(\mathbf{A})$ as above, we write

$$Y(K_f) = G(\mathbf{Q}) \backslash G(\mathbf{A}) / K_f K_\infty.$$

This might look like a horrible mess, but it's actually not so bad. A general theorem (again due to Borel and Harish-Chandra) shows that the double quotient

$$\mathrm{Cl}(K_f) = G(\mathbf{Q}) \backslash G(\mathbf{A}_f) / K_f,$$

which we call the *class set* of K_f, is *finite*. Moreover, from the discreteness of $G(\mathbf{Q})$ in $G(\mathbf{A})$ it follows that for any $\mu \in G(\mathbf{A}_f)$, the group

$$\Gamma_\mu = G(\mathbf{Q}) \cap \mu K_f \mu^{-1}$$

is discrete in $G(\mathbf{R})$. Unravelling the definitions, we find that if $\mu_1, \dots, \mu_r$ is a set of representatives for $\mathrm{Cl}(K_f)$, we have

$$Y(K_f) = \bigsqcup_{i=1}^{r} \Gamma_\mu \backslash Y_\infty$$

where Y_∞ is the symmetric space $G(\mathbf{R})/K_\infty$. Automorphic forms show up as sections of various vector bundles on these spaces, with the vector bundle encoding the representation V of K_∞.

If G is SL_2, the space Y_∞ is the upper half-plane, as we saw above; so each of the pieces $\Gamma_\mu \backslash Y_\infty$ is just the quotient of the upper half-plane by a discrete subgroup of $\mathrm{SL}_2(\mathbf{R})$ – in other words, a modular curve!

Exercise 7. To get some idea of the power of the theorems of Borel and Harish-Chandra, let's use them to prove the two most important basic results of algebraic number theory.

1. Show that if $G = \mathrm{Res}_{F/\mathbf{Q}} \mathbb{G}_m$ where F is a number field, and K_f is $\prod_{v \nmid \infty} \mathscr{O}_{K,v}^\times$, the class set $\mathrm{Cl}(K_f)$ is just the ideal class group of the field F.
2. Describe the groups Γ_μ in the above case, and the space Y_∞; how is this related to Dirichlet's unit theorem?

So applying the theorems of Borel and Harish–Chandra to this one rather simple example of a reductive group gives both the finiteness of the class group of K, and Dirichlet's theorem on the rank of the unit group $\mathscr{O}_K^\times$.

In general, working with automorphic forms involves lots of hard analysis with functions on the symmetric spaces Y_∞, and it's not at all clear how one might hope to explicitly compute these objects. But there's a special case where everything becomes very easy:

Definition 8. We say G is *definite* if the group $G(\mathbf{R})$ is compact.

If G is definite, then the only possible maximal compact subgroup $K_\infty \subseteq G(\mathbf{R})$ is $G(\mathbf{R})$ itself; so the quotient Y_∞ is just a point, and the quotients $Y(K_f)$ are just the finite sets $\mathrm{Cl}(K_f)$. As was apparently first noticed by Gross in his beautiful paper "Algebraic modular forms" ([13]), automorphic forms on these groups are in many ways much simpler than in the non-definite case, and yet are still very interesting objects.

4 Algebraic automorphic forms (after Gross)

This section follows Gross's article [13] closely.

Let's take a definite connected reductive group $G/\mathbf{Q}$. Since any automorphic form for G of weight V must transform in a specified way under K_∞, which is the whole of $G(\mathbf{R})$, it is uniquely determined by its restriction to $G(\mathbf{A}_f)$, and we can precisely describe what this restriction must look like:

Definition 9 (Gross). An *algebraic automorphic form* for G of level K_f and weight V is a function

$$\phi : G(\mathbf{A}_f) \to V$$

such that

1. $\phi(gk) = \phi(g)$ for all $g \in G(\mathbf{A}_f)$ and $k \in K_f$;
2. $\phi(\gamma g) = \gamma \circ \phi(g)$ for all $g \in G(\mathbf{A}_f)$ and $\gamma \in G(\mathbf{Q})$.

We write $\mathrm{Alg}(K_f, V)$ for the space of algebraic automorphic forms of level K_f and weight V.

Exercise 10. Show that if $\phi : G(\mathbf{Q})\backslash G(\mathbf{A}) \to V$ is any function satisfying conditions (1) and (2) in the definition of an automorphic form from the previous section, then $\phi|_{G(\mathbf{A}_f)}$ is an algebraic automorphic form (of the same weight and level).

Remark 11. We've taken V to be a $\mathbf{C}$-vector space in order to compare with the previous definition; but in fact any continuous representation of $G(\mathbf{R})$ on a $\mathbf{C}$-vector space arises by taking $\mathbf{R}$-points from an algebraic representation of G defined over a number field. This remark will be useful when we carry out computations later, since it implies that all of our linear algebra can be done over number fields, so we don't need to worry about precision issues that arise when doing matrix calculations over $\mathbf{C}$.

It's clear that any $\phi \in \mathrm{Alg}(K_f, V)$ is uniquely determined by its values on any set $\mu_1, \dots, \mu_r$ of representatives of the class set $\mathrm{Cl}(K_f) = G(\mathbf{Q})\backslash G(\mathbf{A}_f)/K_f$. In particular, the space $\mathrm{Alg}(K_f, V)$ is finite-dimensional.

We can actually do a little better than this. Recall that for $\mu \in G(\mathbf{A}_f)$ we defined groups

$$\Gamma_\mu = G(\mathbf{Q}) \cap \mu K_f \mu^{-1}.$$

Notice that in the definite case these groups are finite (since they are discrete subgroups of the compact group $G(\mathbf{R})$). If $g \in \Gamma_\mu$, then we have

$$\begin{aligned} g \circ \phi(\mu) &= \phi(g\mu) \quad (\text{as } g \in G(\mathbf{Q})) \\ &= \phi(\mu \cdot \mu^{-1} g \mu) \\ &= \phi(\mu) \quad (\text{as } \mu^{-1} g \mu \in K_f.) \end{aligned}$$

So $f(\mu) \in V^{\Gamma_\mu}$. Hence if $\mu_1, \dots, \mu_r$ are a set of representatives for $\mathrm{Cl}(K_f)$, as above, we have a map

$$\begin{aligned} \mathrm{Alg}(K_f, V) &\to \bigoplus_{i=1}^{r} V^{\Gamma_{\mu_i}}, \\ \phi &\mapsto (f(\mu_1), \dots, f(\mu_r)). \end{aligned}$$

This is clearly well-defined, and injective (since ϕ is determined by its values on the μ_i). In fact it is also surjective, and thus an isomorphism.

Exercise 12. Prove carefully that the above map is surjective.

Remark 13. There's a possible risk of confusion in the terminology here, in that various authors (notably [3]) have proposed a variety of definitions of what it should mean for an automorphic form, or an automorphic representation, on a general non-definite reductive group to be "algebraic". For instance, a lot of important research has been done recently on "RAESDC" (regular algebraic essentially self-dual cuspidal) automorphic representations of GL_n. These are very different, and much more

complicated, objects than our algebraic automorphic forms (which are the "algebraic modular forms" of [13]).

5 Hecke operators

References: see Gross's article [13] for the general theory; for algorithmic aspects, see the references listed in the next section.

We've now seen how to define spaces $\mathrm{Alg}(K_f, V)$ of algebraic automorphic forms, for a definite reductive group. As with classical modular forms, spaces alone are not terribly interesting, but they come with a natural family of operators – Hecke operators – and the deep number-theoretical importance of automorphic forms is encoded in the action of these operators.

Let's run through some general formalism. The *Hecke algebra* $\mathscr{H}(G(\mathbf{A}_f), K_f)$ is the free $\mathbf{Z}$-module with basis the set of double cosets $\{KgK : g \in G(\mathbf{A}_f)\}$, equipped with an algebra structure which I won't define. Two properties we'll need of this space are:

- If $K_f = \prod_p K_p$ for open compact subgroups $K_p \subseteq G(\mathbf{Q}_p)$, then $\mathscr{H}(G(\mathbf{A}_f), K_f)$ decomposes as a restricted tensor product of local Hecke algebras,

$$\mathscr{H}(G(\mathbf{A}_f), K_f) = \bigotimes_p{}' \mathscr{H}(G(\mathbf{Q}_p), K_p).$$

- If K_p is *hyperspecial* – which, as we saw in §2, is the case for all but finitely many p – the algebra $\mathscr{H}(G(\mathbf{Q}_p), K_p)$ is commutative and is generated by an explicit finite set of elements lying in a maximal torus.

For example, the local Hecke algebra $\mathscr{H}(\mathrm{GL}_n(\mathbf{Q}_p), \mathrm{GL}_n(\mathbf{Z}_p))$ is isomorphic to $\mathbf{Z}[T_1, \ldots, T_n, T_n^{-1}]$, where T_i is the double coset of a diagonal matrix with i diagonal entries equal to p and the remaining $(n-i)$ equal to 1.

Exercise 14. Show that $\mathscr{H}(\mathrm{GL}_n(\mathbf{Q}_p), \mathrm{GL}_n(\mathbf{Z}_p))$ is spanned as a vector space by the double cosets of diagonal matrices with ascending powers of p along the diagonal. [Hint: Google the phrase "Smith normal form".]

It's a general fact that if Π is a representation of $G(\mathbf{A}_f)$, the K_f-invariants Π^{K_f} pick up an action of $\mathscr{H}(G(\mathbf{A}_f), K_f)$. To see how these Hecke operators act on the space $\mathrm{Alg}(K_f, V)$, note that any KgK can be written as a finite union of left cosets $\bigsqcup_{s=1}^{t} g_s K$. We then define, for $\phi \in \mathrm{Alg}(K_f, V)$,

$$([KgK] \circ \phi)(x) = \sum_{s=1}^{t} \phi(x g_s).$$

Exercise 15. Show that $[KgK] \circ \phi$ is in $\mathrm{Alg}(K_f, V)$.

We'll need to make this operator $[KgK]$ on $\mathrm{Alg}(K_f, V)$ a little more explicit, using the isomorphism of the previous section

$$\begin{aligned}\mathrm{Alg}(K_f,V) &\to \bigoplus_{i=1}^{r} V^{\Gamma_{\mu_i}},\\ \phi &\mapsto (f(\mu_1),\dots,f(\mu_r)).\end{aligned}$$

where $\mu_1,\dots,\mu_r \in G(\mathbf{A}_f)$ are a set of representatives for $\mathrm{Cl}(K_f)$. To find

$$([KgK]\circ\phi)(\mu_i) = \sum_{s=1}^{t} \phi(\mu_i g_s),$$

we need to find out in which $\big(G(\mathbf{Q}), K_f\big)$ double cosets the products $\mu_i g_s$ lie. Indeed, if $\gamma \in G(\mathbf{Q})$ is such that $\mu_i g_s \in \gamma\mu_j K$, then we have

$$\phi(\mu_i g_s) = \phi(\gamma\mu_j) = \gamma\circ f(\mu_j).$$

There won't be very many possibilities for γ. The possibilities are the elements of the set

$$G(\mathbf{Q}) \cap \mu_i g_s K \mu_j^{-1},$$

and any two elements of this set differ by right multiplication by an element of the group Γ_{μ_j}, which we already know is finite.

So for each pair (i,s) we need to find the unique j such that $\mu_i g_s K \mu_j^{-1} \cap G(\mathbf{Q})$ is non-empty. If we consider all s at once, we can present this in the following way:

- For each $(i,j) \in \{1,\dots,r\}^2$, calculate $A_{ij}(g) = G(\mathbf{Q}) \cap \mu_i K g K \mu_j^{-1}$, a finite set.
- Find representatives for $B_{ij}(g) = A_{ij}(g)/\Gamma_{\mu_j}$ (which is well-defined, as $A_{ij}(g)$ is preserved by right multiplication by Γ_{μ_j}).
- Then for any $\phi \in \mathrm{Alg}(K,V)$, we have

$$([KgK]\circ\phi)(\mu_i) = \sum_{j=1}^{r} \sum_{[\gamma]\in B_{ij}(g)} \gamma\circ f(\mu_j).$$

Much of the work in computing with algebraic automorphic forms goes into finding the sets $B_{ij}(g)$, for various elements KgK of the Hecke algebra. Once you know the data of: a set of representatives $\mu_1,\dots,\mu_r$; the corresponding groups $\Gamma_{\mu_1},\dots,\Gamma_{\mu_r}$; and the sets $B_{ij}(g)$ for all i,j and your favourite g, it's essentially routine to calculate a basis of $\mathrm{Alg}(K,V)$ and the matrix of $[KgK]$ acting on this basis for absolutely any V. That is, a large part of the computation is independent of the weight, which is perhaps surprising if you're used to computing with modular forms and modular symbols.

Remark 16. The matrix whose i,j entry is $b_{ij} = \#B_{ij}$ is called the *Brandt matrix* of g, and it gives the action of KgK on the automorphic forms of level K_f and weight the trivial representation (sometimes called the *Brandt module* of level K_f). The term

"Brandt matrix" goes back to the very first case in which algebraic automorphic forms were studied, for G the group of units of a definite quaternion algebra over $\mathbf{Q}$; here $\mathrm{Cl}(K_f)$ is in bijection with the left ideal classes in D.

6 Examples of this idea in the literature

As far as I know, the examples of definite (or definite-modulo-centre) groups G where people have computed algebraic automorphic forms are:

- $D^\times$, where D is a definite quaternion algebra over $\mathbf{Q}$: Pizer [17] (a special case which preceded the general theory by several decades)
- $\mathrm{Res}_{F/\mathbf{Q}}(D^\times)$, where F is a totally real number field and D a totally definite quaternion algebra over F: Dembele [7, 8], Dembele–Donnelly [9]
- Unitary groups: my article [16], the article by Greenberg and Voight in this volume [12], and unpublished work of Dembele.
- Compact forms of the symplectic group Sp_4 and the exceptional Lie group G_2: Lansky–Pollack [15]
- Compact forms of Sp_{2n}, $n \geq 2$: Cunningham–Dembele [6]

In the remaining sections of these notes, I'm going to explain one specific example, the case of definite unitary groups, following my paper [16].

7 Hermitian spaces and unitary groups

Let F be a number field, and E/F a quadratic extension. For $x \in E$, we write $\bar{x}$ for the image of x under the nontrivial element of $\mathrm{Gal}(E/F)$.

Definition 17. A *Hermitian space* for E/F is a finite-dimensional E-vector space V with a pairing $\langle\ ,\ \rangle : V \times V \to E$ which is linear in the first variable and satisfies

$$\langle y, x\rangle = \overline{\langle x, y\rangle}$$

for all $x, y \in V$.

If V is a Hermitian space, then there is an associated algebraic group U over F, whose R-points (for any F-algebra R) are given by

$$U(F) = \left\{u \in \mathrm{Aut}_{R\otimes_F E}(R \otimes_F V) : \langle ux, uy\rangle = \langle x, y\rangle\ \forall x, y \in V\right\}.$$

This group becomes isomorphic to GL_d over E, where $d = \dim_E V$. In particular, it's connected and reductive.

Exercise 18. Prove this. (You should find that there are two possible isomorphisms, related by the inverse transpose map $\mathrm{GL}_d \to \mathrm{GL}_d$.)

We say that V is *totally positive definite* if F is totally real, and $\langle x,x\rangle$ is totally positive for all $x \in V$. (Note that $\langle x,x\rangle$ is in F, so this makes sense.) Note that this in particular implies that $\lambda\bar{\lambda}$ is totally positive for all $\lambda \in E$, so E/F must be a CM extension (a totally imaginary quadratic extension of a totally real field). Then we have the following fact:

Proposition 19. *If V is totally positive definite, then the group $G = \mathrm{Res}_{F/\mathbf{Q}}(U)$ is a definite reductive group.*

We'll also need (occasionally) to consider some integral structures on these objects. A *lattice* in V is an $\mathscr{O}_E$-lattice $\mathscr{L} \subset V$ (a finitely-generated $\mathscr{O}_E$-module containing an E-basis of V). Any choice of such a lattice $\mathscr{L}$ defines an integral structure on G, for which $G(\mathbf{Z})$ is the stabilizer of $\mathscr{L}$.

Theorem 20. *If V is totally positive definite, $\mathscr{L} \subset V$ is a lattice, and $r \in \mathscr{O}_F$, then the set*

$$\{x \in \mathscr{L} : \langle x,x\rangle = r\}$$

is finite and can be algorithmically computed.

Proof. By choosing a basis for $\mathscr{L}$ as a $\mathbf{Z}$-module, and equipping it with the quadratic form $q(x) = \mathrm{Tr}_{F/\mathbf{Q}}\langle x,x\rangle$, this reduces to the problem of enumerating all short vectors for a quadratic form, which can be solved using the LLL (Lenstra-Lenstra-Lovasz) reduction method. □

From this, we have the following corollary:

Theorem 21. *For any lattice $\mathscr{L}$ as above, and any $r \in \mathscr{O}_F$, the set*

$$\Sigma(\mathscr{L},r) \coloneqq \{\varphi \in \mathrm{End}_E(V) : \varphi(\mathscr{L}) \subseteq \mathscr{L}, \langle \varphi x, \varphi y\rangle = r \cdot \langle x,y\rangle \ \forall x,y \in V\}$$

is finite and algorithmically computable.

Proof. There are clearly only finitely many possibilities for where φ can send each vector in a set of generators[4] of $\mathscr{L}$. □

For example, if V is the "standard" rank d Hermitian space, by which I mean $E^{\oplus d}$ with the Hermitian form

$$\langle (x_1,\dots,x_d),(y_1,\dots,y_d)\rangle = \sum_{i=1}^{d} x_i\bar{y}_i,$$

and $\mathscr{L}$ is the obvious sublattice $\mathscr{O}_E^{\oplus d}$, then $\Sigma(\mathscr{L},r)$ is simply the set of all matrices whose columns (or rows) are orthogonal vectors in V with entries in $\mathscr{O}_E$ and length r. So one can enumerate them pretty quickly by simply listing all vectors of length r, and then looking for d-tuples that are orthogonal.

[4] Note that I didn't write "basis" here, since it may very well happen that $\mathscr{L}$ is not free as an $\mathscr{O}_E$-module if the class number of E is > 1.

How does this help? Let's define

$$\widehat{\mathscr{L}} = \prod_p (\mathscr{L} \otimes_{\mathbf{Z}} \mathbf{Z}_p).$$

This is contained in $V \otimes_{\mathbf{Q}} \mathbf{A}_f$, which has an action of $G(\mathbf{A}_f)$, and one easily checks that the stabilizer of $\widehat{\mathscr{L}}$ is an open compact subgroup $K_{\mathscr{L}}$. (More concretely, $K_{\mathscr{L}} = \prod_p K_p$ where K_p is the stabilizer of $\mathscr{L} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ in $V \otimes_{\mathbf{Q}} \mathbf{Q}_p$.)

Let $K \subseteq G(\mathbf{A}_f)$ be an open compact subgroup contained in $K_{\mathscr{L}}$, for some choice of lattice $\mathscr{L}$.

We want to find the following data for K:

1. a set of representatives $\mu_1, \ldots, \mu_r$ for $\mathrm{Cl}(K)$;
2. the finite groups Γ_{μ_i};
3. the sets $A_{ij}(g) = G(\mathbf{Q}) \cap \mu_i K g K \mu_j^{-1}$, for each pair (i, j) and various $g \in G(\mathbf{A}_f)$.

Note that (2) is in fact a special case of (3), by taking $g = 1$ and $j = i$.

Let's assume that we know the solution to (1). Then we can solve (3) as follows: we choose

$$\begin{aligned} \lambda \in \mathscr{O}_E \quad \text{such that} \quad \lambda \mu_i \widehat{\mathscr{L}} \subseteq \widehat{\mathscr{L}}; \\ \lambda' \in \mathscr{O}_E \quad \text{such that} \quad \lambda' g \widehat{\mathscr{L}} \subseteq \widehat{\mathscr{L}}; \\ \lambda'' \in \mathscr{O}_E \quad \text{such that} \quad \lambda'' \mu_j^{-1} \widehat{\mathscr{L}} \subseteq \widehat{\mathscr{L}}. \end{aligned}$$

It's clear that we can always do this: we just need to make the λ's divisible by sufficiently high powers of a certain finite set of primes. Then if $\gamma \in A_{ij}(g)$, the element $\tilde{\gamma} = \lambda \cdot \lambda' \cdot \lambda'' \cdot \gamma \in \mathrm{End}_E(V)$ lies in the set $\Sigma(\mathscr{L}, r)$, where $r = \mathrm{N}_{E/F}(\lambda \lambda' \lambda'')$. Not every element of $\Sigma(\mathscr{L}, r)$ comes from an element of $A_{ij}(g)$, of course, but for each element of $\Sigma(\mathscr{L}, r)$ it is a finite, purely local computation to check whether it gives us an element of $A_{ij}(g)$, and we know that we must get every element of $A_{ij}(g)$ this way. So this solves (3).

So how do we solve problem (1), of finding the class set? We can do this using a "bootstrap" technique. We know one double coset – the identity – so we can start by letting $\mu_1 = 1$ and plunging on with calculating the sets $A_{11}(g)$ for some elements g. For each such g, we can also calculate by purely local methods how many single K-cosets the double coset KgK should break up into, and we can find elements $g_1, \ldots, g_m$ in $G(\mathbf{A}_f)$ such that $KgK = \bigsqcup_{i=1}^m g_i K$. (We can take the g_i to be 1 outside the finite set of primes at which g is not integral).

On the other hand, we've calculated the set $A_{11}(g) = G(\mathbf{Q}) \cap KgK$, so we can check which of the single K-cosets in KgK are represented by some element of $G(\mathbf{Q})$ (which is, again, a local computation). If there's a single K-coset $g_i K \subset KgK$ which doesn't have a representative in $G(\mathbf{Q})$, then g_i is an explicit element of $G(\mathbf{A}_f)$ that isn't in $G(\mathbf{Q})K$. We can then define μ_2 to be this element, and using (3) we can find the set $A_{12}(g)$, which will account for some more of the single K-cosets in KgK. Continuing in this way will eventually give us representatives $\mu_1, \ldots, \mu_s$ for

the subset of $\mathrm{Cl}(K)$ consisting of double cosets having non-empty intersection with KgK. We then go back and calculate the sets $A_{21}(g),\dots,A_{ss}(g)$, using (3) again.

If we try enough g's, then eventually we'll find every element of $\mathrm{Cl}(K)$ this way. The only question now is: when do we stop? How do we know if we've found all of $\mathrm{Cl}(K)$? One way to do this is to use a *mass formula*.

8 Mass Formulae

Let's return (temporarily) to thinking about a general connected reductive group G. Recall that the quotient $G(\mathbf{Q})\backslash G(\mathbf{A}_f)$ is compact. This implies that it has finite Haar measure; but the Haar measure h on a locally compact group such as $G(\mathbf{A}_f)$ is only defined up to scaling.

Definition 22. If K is an open compact subgroup of $G(\mathbf{A}_f)$, we define the *mass* of K to be the ratio

$$m(K) = \frac{h\left(G(\mathbf{Q})\backslash G(\mathbf{A}_f)\right)}{h(K)}$$

This is independent of the normalisation we use for the Haar measure h, obviously; and it's easy to see that we can write it as

$$m(K) = \sum_{\mu \in \mathrm{Cl}(K)} \frac{1}{\#\Gamma_\mu}.$$

(This sum is well-defined, since although Γ_μ depends on the choice of μ, if μ and μ' are in the same class in $\mathrm{Cl}(K)$ the groups Γ_μ and $\Gamma_{\mu'}$ are conjugate, and hence have the same order.)

Notice that if $K' \subseteq K$, then we have $m(K') = [K : K']m(K)$. So if we know the mass of one open compact K, we know them all, as all open compact subgroups of $G(\mathbf{A}_f)$ are commensurable.

Theorem 23 (Gan–Hanke–Yu, [10]). *If G is a definite unitary group corresponding to an n-dimensional Hermitian space for $E/\mathbf{Q}$, where E is imaginary quadratic, and $K_{\mathscr{L}}$ is the open compact subgroup corresponding to a lattice $\mathscr{L}$ satisfying a certain maximality property, we have*

$$m(K_{\mathscr{L}}) = \frac{1}{2^{n-1}} L(M) \prod_{p \in S} \lambda_p,$$

where $L(M)$ is a product of special values of Dirichlet L-functions, S is a finite set of primes and λ_p are certain explicit constants depending on V.

(This is actually a special case of the theorem of Gan–Hanke–Yu, which applies more generally to definite unitary groups and definite orthogonal groups over arbitrary totally real fields.)

So we can find the mass by evaluating special values of L-functions! This allows us to tell when we have found the whole set $\mathrm{Cl}(K)$, by comparing the result of the mass formula with the sizes of the groups Γ_{μ_i} for the coset representatives μ_i we know so far.

Remark 24. The mass formula gives us a criterion for checking whether we've found the whole of $\mathrm{Cl}(K)$ using the algorithm of the previous section, but it doesn't guarantee that the algorithm will terminate: if we are unlucky in our choice of g's, we might potentially never find the whole of $\mathrm{Cl}(K)$.

One can check that if G is a unitary group for an extension $E/\mathbf{Q}$ where the imaginary quadratic field E has unique factorization, then for any prime p which splits in E, every element of $\mathrm{Cl}(K)$ has a representative in $G(\mathbf{Q}_p)$. Since we can calculate the local Hecke algebra at good primes explicitly (Exercise 14 above) this gives us an explicit list of double cosets to try which are guaranteed to eventually exhaust $\mathrm{Cl}(K)$.

In practice, one finds that for a "randomly chosen" g, the single cosets in KgK tend to be distributed among the classes in $\mathrm{Cl}(K)$ in proportion to the factors $\frac{1}{\#\Gamma_{\mu_i}}$, so if we choose g such that the number of single K-cosets in KgK is large enough, then KgK will contain representatives for the entirety of $\mathrm{Cl}(K)$. This is related to various subtle issues involving the norms of Hecke eigenvalues of automorphic forms.

9 An example in rank 2

I carried out the above computation for various standard Hermitian spaces of ranks 2 and 3 attached to imaginary quadratic fields $E/\mathbf{Q}$ of class number 1, taking $K = K_{\mathscr{L}}$ for $\mathscr{L}$ the standard lattice.

For $n = 2$, and $E = \mathbf{Q}(\sqrt{-d})$ for $d = 1, 2, 3, 7$, we find that the mass of the obvious double coset equals the whole mass. The first case where something interesting happens is $d = 11$. Here the mass formula gives $m(K) = \frac{5}{24}$. The obvious double coset $G(\mathbf{Q})K$ generated by $\mu_1 = 1$ has corresponding Γ group

$$\Gamma_{\mu_1} = G(\mathbf{Z}) = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \cup \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$$

of order 8. That leaves a mass of $\frac{5}{24} - \frac{1}{8} = \frac{1}{12}$ unaccounted for. So we launch into decomposing some Hecke operators.

The prime $p = 3$ splits in E, and choosing the prime $\mathfrak{p}$ above p generated by $\alpha = (1 + \sqrt{-11})/2$ gives an isomorphism $G(\mathbf{Q}_3) \cong \mathrm{GL}_2(\mathbf{Q}_3)$; this isomorphism identifies $K \cap G(\mathbf{Q}_3)$ with $\mathrm{GL}_2(\mathbf{Z}_3)$. So the interesting element of the local Hecke algebra corresponds to the double coset of $g = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}_3)$, which splits into $p + 1 = 4$ double cosets; these are represented by the elements of $G(\mathbf{A}_f)$ which are 1 at all primes away from 3, and at 3 correspond to the matrices

$$\left\{\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&0\\1&3\end{pmatrix},\begin{pmatrix}1&0\\2&3\end{pmatrix},\begin{pmatrix}3&0\\0&1\end{pmatrix}\right\}$$

in $\mathrm{GL}_2(\mathbf{Q}_3)$.

The set $A_{11}(g)$ has order 16, so $B_{11}(g) = A_{11}(g)/G(\mathbf{Z})$ has order 2, represented by the elements $\begin{pmatrix}\alpha/\bar{\alpha}&0\\0&1\end{pmatrix}$ and $\begin{pmatrix}1&0\\0&\alpha/\bar{\alpha}\end{pmatrix}$. The images of these in $\mathrm{GL}_2(\mathbf{Q}_3)$ obviously land in

$$\begin{pmatrix}3&0\\0&1\end{pmatrix}\mathrm{GL}_2(\mathbf{Z}_3) \quad \text{and} \quad \begin{pmatrix}1&0\\0&3\end{pmatrix}\mathrm{GL}_2(\mathbf{Z}_3)$$

respectively, since $\bar{\alpha}$ is a unit at $\mathfrak{p}$. So we have found representatives in $G(\mathbf{Q})$ for two of the four elements of KgK/K; but the element μ_2 of $G(\mathbf{A}_f)$ which is 1 away from the prime 3 and whose component at 3 corresponds under our isomorphism to $\begin{pmatrix}1&0\\1&3\end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}_3)$ represents a non-trivial element in $\mathrm{Cl}(K)$. Calculating the corresponding group Γ_{μ_2} we find that it has order 12, so the mass formula implies that we have now found the whole of $\mathrm{Cl}(K)$.

Since $\#\mathrm{Cl}(K) = 2$, we must in particular have a 2-dimensional space of automorphic forms of level K and weight the trivial representation. This space contains the 1-dimensional space of constant functions, which are obviously Hecke eigenvectors, with the eigenvalue for the Hecke operator at a split prime $\mathfrak{p}$ of E being $1+p$ where p is the rational prime below $\mathfrak{p}$; this is not especially exciting. However, there is another eigenfunction which is rather more interesting. It turns out that for this eigenfunction it is also true that the eigenvalue of the Hecke operator at a split prime $\mathfrak{p}$ of E only depends on the rational prime p below $\mathfrak{p}$, and we find that its Hecke eigenvalues at the split primes are:

Prime	3	5	23	31	37	47	53
Eigenvalue	-1	1	-1	7	3	8	-6

Maybe this isn't so easy to spot, but these are also the Hecke eigenvalues of a modular form! We've rediscovered (half of) the Hecke eigenvalues of the unique newform of weight 2 and level 11.

10 Galois representations

In the last section, we saw an example of a (non-constant) automorphic form for a unitary group of rank 2 for $\mathbf{Q}(\sqrt{-11})/\mathbf{Q}$, and I said that the Hecke eigenvalues "look like" those of a modular form. In this section, we'll see an interpretation of how and why this works.

Recall that if f is a modular eigenform of weight k and level N, which is new, cuspidal, normalized, and a Hecke eigenform, then for any prime ℓ, we can construct a Galois representation

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell)$$

which is continuous, semisimple, unramified outside $N\ell$, and for each prime $p \nmid N\ell$, satisfies

$$\mathrm{Tr}\,\rho_{f,\ell}(\mathrm{Frob}_p) = a_p(f)$$

where $a_p(f)$ is the T_p-eigenvalue of f.

Much more is known about the properties of $\rho_{f,\ell}$, of course, but the properties I've just written down specify it uniquely, so we'll content ourselves with those.

Now let G be a definite unitary group of rank n attached to an imaginary quadratic field $E/\mathbf{Q}$, and π an algebraic automorphic form for G of some level K_f. Let S be the set of primes p that are split in E, so $G(\mathbf{Q}_p) \cong \mathrm{GL}_n(\mathbf{Q}_p)$, and such that $K_f \cap G(\mathbf{Q}_p) = \mathrm{GL}_n(\mathbf{Z}_p)$. Suppose that for all primes $p \in S$, π is an eigenvector for the Hecke operator corresponding to

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p \end{pmatrix}$$

under the isomorphism $G(\mathbf{Q}_p) \cong \mathrm{GL}_n(\mathbf{Q}_p)$ determined by a choice of prime $\mathfrak{p}$ above p. Let $a_{\mathfrak{p}}(\pi)$ be the corresponding eigenvalue. Then we have the following theorem:

Theorem 25 (Shin [19], Chenevier–Harris [4]). *There exists a unique semisimple Galois representation*

$$\rho_{\pi,\ell} : \mathrm{Gal}(\overline{E}/E) \to \mathrm{GL}_n(\overline{\mathbf{Q}}_\ell)$$

satisfying

$$\mathrm{Tr}\,\rho_{f,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = a_{\mathfrak{p}}(\pi)$$

for all primes $\mathfrak{p}$ of E above a prime $p \in S$.

The set S contains all but finitely many degree 1 primes of E, so the Frobenius elements at these primes are dense in $\mathrm{Gal}(\overline{E}/E)$; thus $\rho_{\pi,\ell}$ is clearly unique.

Note that $\mathrm{Gal}(\overline{E}/E)$ is an index 2 subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and conjugation by the nontrivial element $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})/\mathrm{Gal}(\overline{E}/E)$ interchanges the conjugacy classes of $\mathrm{Frob}_{\mathfrak{p}}$ and $\mathrm{Frob}_{\overline{\mathfrak{p}}}$ for $p = \mathfrak{p}\bar{\mathfrak{p}} \in S$. So unless we have $a_{\bar{\mathfrak{p}}}(\pi) = a_{\mathfrak{p}}(\pi)$ for all such p, which doesn't usually happen, the conjugate $\rho_{\pi,\ell}^{\sigma}$ can't be isomorphic to $\rho_{\pi,\ell}$ and hence $\rho_{\pi,\ell}$ cannot be extended to a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. However, the representations $\rho_{\pi,\ell}$ and $\rho_{\pi,\ell}^{\sigma}$ are related: we have an isomorphism

$$\rho_{\pi,\ell}^{\sigma} \cong \rho_{\pi,\ell}^{\vee}(n-1) \quad (\text{“polarization”})$$

where $\rho_{\pi,\ell}^{\vee}$ is the dual representation and $(n-1)$ denotes twisting by the $(n-1)$-st power of the ℓ-adic cyclotomic character $\chi_\ell : \mathrm{Gal}(\overline{E}/E) \to \mathbf{Z}_\ell^\times$.

So our observation about the non-constant trivial weight form on the standard rank 2 unitary group for $\mathbf{Q}(\sqrt{-11})/\mathbf{Q}$ can be interpreted as follows: if π is this form (and ℓ is any prime), it looks as if the Galois representation $\rho_{\pi,\ell}$ is isomorphic to the restriction of $\rho_{f,\ell}$ to $\mathrm{Gal}(\overline{E}/E)$, where f is the weight 2 cusp form of level 11.

Exercise 26. Show that $\rho = \rho_{f,\ell}|_{\mathrm{Gal}(\overline{E}/E)}$ does satisfy the polarization identity, so our conjecture that $\rho \cong \rho_{\pi,\ell}$ is consistent with what we know about the latter. (Note that in this case $\rho^\sigma \cong \rho$, so we need to check that $\rho \cong \rho^\vee(1)$.)

There is a very general philosophy, sometimes referred to as the "global Langlands program", which predicts (among other things) that:

- "Nice" automorphic forms on $\mathrm{Res}_{K/\mathbf{Q}}\mathrm{GL}_n$, where K is any number field, should correspond to compatible families of n-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$.
- Automorphic forms on a subgroup $G \subseteq \mathrm{Res}_{K/\mathbf{Q}}\mathrm{GL}_n$ should correspond to Galois representations preserving some extra structure (such as a symplectic form on $\overline{\mathbf{Q}}_\ell^n$, or a polarization as above).
- Natural operations on Galois representations correspond to maps between automorphic forms ("Langlands functoriality").

These are all very much open conjectures in general, although many important special cases are known. Let me just give a few examples of what I mean by "natural operations on Galois representations".

For instance, let's say f is a modular eigenform; then, thanks to Deligne, we know how to construct the corresponding 2-dimensional ℓ-adic representations $\rho_{f,\ell}$. For each $m \geq 2$, we can take the *symmetric power* $\mathrm{Sym}^m \rho_{f,\ell}$; this is an $(m+1)$-dimensional ℓ-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and one might reasonably expect that it corresponds to some automorphic form on GL_{m+1}. This form – which, I stress, is only conjectured to exist – is called the "symmetric power lifting" of f. At the moment I believe the existence of the symmetric power lifting is only known for $m = 2, 3, 4$ and 9.

Here's another example. Let's say we take two definite unitary groups $U(n_1)$ and $U(n_2)$ associated to the same CM extension E/F, and we consider eigenforms π_1 and π_2 on $U(n_1)$ and $U(n_2)$ respectively. We know these have Galois representations $\rho_{\pi_1,\ell}$ and $\rho_{\pi_2,\ell}$, of dimensions n_1 and n_2. So we can consider the representation $\rho_{\pi_1,\ell} \oplus \rho_{\pi_2,\ell}$, and ask: does this come from an automorphic form on $U(n_1+n_2)$? This can't quite work as I've stated it, since the direct sum doesn't satisfy the polarization identity; but we can fix this by twisting the two representations by appropriately chosen characters. The corresponding automorphic forms on $U(n_1+n_2)$ are known as *endoscopic lifts*, since they are associated to the *endoscopic subgroup*[5] $U(n_1) \times U(n_2)$ of $U(n_1+n_2)$.

[5] Informally, an endoscopic subgroup is "the Levi factor of a parabolic subgroup that isn't there". Notice that definite groups cannot have parabolic subgroups, since their split rank is 0.

11 Some examples in rank 3

I've done some calculations of automorphic forms on the definite unitary group attached to the standard 3-dimensional Hermitian space for $\mathbf{Q}(\sqrt{-7})/\mathbf{Q}$. I took the level group to be the group $K_{\mathscr{L}}$ attached to the standard lattice $\mathscr{O}_E^{\oplus 3}$.

In this case, the possible weights are the irreducible representations of the compact Lie group $G(\mathbf{R}) \cong U(3)$. These are indexed by pairs[6] of integers (a,b), with the representation corresponding to (a,b) being a certain explicit subspace of $\mathrm{Sym}^a(W) \otimes \mathrm{Sym}^b(W^\vee)$ where W is the 3-dimensional standard representation.

It turns out that if $a \neq b$, then Galois representation attached to a form of weight (a,b) cannot possibly extend from $\mathrm{Gal}(\overline{E}/E)$ to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, because if π has weight (a,b), the conjugate representation $\rho_{\pi,\ell}^\sigma$ is the Galois representation attached to an eigenform of weight (b,a) and thus cannot be isomorphic to $\rho_{\pi,\ell}$. So let's look at some examples in "parallel" weights (a,a).

In table 1, I've listed each eigenform of parallel weight ≤ 4 (or, rather, each orbit of eigenforms up to the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the eigenvalues, which is well-defined since the parallel weight representations of G are defined over $\mathbf{Q}$). For each of these, one can try to test whether the Galois representation looks like it might extend to $\mathbf{Q}$, by checking whether the Hecke eigenvalues at pairs of primes above the same prime of $\mathbf{Q}$ coincide. One can also try to recognise the form as an endoscopic lift from $U(1) \times U(2)$, in which case the form will have Hecke eigenvalues at split primes given by $a_{\mathfrak{p}}(\pi) = \omega_1(\mathfrak{p}) + \omega_2(\mathfrak{p}) a_p(f)$, for some modular form f and Groessencharacters ω_1, ω_2 of E, and the Galois representation $\rho_{\pi,\ell}$ would be isomorphic to $\omega_{1,\ell} \oplus \left(\omega_{2,\ell} \otimes \rho_{f,\ell}|_{\mathrm{Gal}(\overline{E}/E)}\right)$, where $\omega_{i,\ell}$ are the ℓ-adic characters attached to the Groessencharacters ω_i via class field theory. (It may even happen that the modular form f has CM by E, in which case $\rho_{f,\ell}|_{\mathrm{Gal}(\overline{E}/E)}$ is reducible and $\rho_{\pi,\ell}$ is a direct sum of three characters.)

So one can see here explicit examples of several kinds of Langlands functoriality at work, as well as some examples of automorphic forms that genuinely come from $U(3)$ and not from any simpler group.

References

1. Borel, A., Jacquet, H.: Automorphic forms and automorphic representations. In: Automorphic forms, representations and *L*-functions (Corvallis, 1977), *Proc. Sympos. Pure Math.*, vol. 33 part 1, American Mathematical Society (1979).
2. Bump, D.: Automorphic forms and representations, *Cambridge Studies in Advanced Mathematics*, vol. 55. Cambridge Univ. Press (1997)
3. Buzzard, K., Gee, T.: The conjectural connections between automorphic representations and galois representations (2011). Preprint.

[6] Actually triples, but the third parameter is a twist by a power of the determinant and so doesn't give you anything new.

Table 1 Galois orbits of automorphic forms for the group $U(3)$ attached to $\mathbf{Q}(\sqrt{-7})$ in parallel weights ≤ 4

a	Form	Endoscopic?	Extends to $\mathbf{Q}$?	Notes
0	0a	Yes	Yes	Constant fcn; $\rho_{\pi,\ell} \cong 1 \oplus \chi_\ell \oplus \chi_\ell^2$
	0b	Yes	Yes	Direct sum of 3 characters
1	-	-	-	(no forms in this weight)
2	2a	Yes	Yes	Direct sum of 3 characters
	2b	Yes	Yes	Character $\oplus$ twist of a weight 7 modular form
3	3a	Yes	Yes	Character $\oplus$ twist of a weight 9 modular form
	3b	No	No	First "interesting" example
4	4a	Yes	Yes	Direct sum of 3 characters
	4b	No	Yes	$\mathrm{Sym}^2(\rho_{f,\ell})$ for a weight 6 modular form
	4c	Yes	Yes	Character $\oplus$ twist of a weight 11 modular form
	4d	Yes	No	Character $\oplus$ twist of a weight 6 modular form
	4e	No	No	

4. Chenevier, G., Harris, M.: Construction of automorphic Galois representations. In: Stabilisation de la formule des traces, variétés de Shimura, et applications arithmétiques. To appear.
5. Cogdell, J., Kim, H., Murty, M.R.: Lectures on automorphic *L*-functions, *Fields Institute Monographs*, vol. 20. American Mathematical Society (2004)
6. Cunningham, C., Dembélé, L.: Computing genus-2 Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$ via the Jacquet-Langlands correspondence. Experiment. Math. **18**(3), 337–345 (2009).
7. Dembélé, L.: Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$. Experiment. Math. **14**(4), 457–466 (2005).
8. Dembélé, L.: Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms. Math. Comp. **76**(258), 1039–1057 (2007).
9. Dembélé, L., Donnelly, S.: Computing Hilbert modular forms over fields with nontrivial class group. In: Algorithmic number theory, *Lecture Notes in Comput. Sci.*, vol. 5011, pp. 371–386. Springer, Berlin (2008).
10. Gan, W.T., Hanke, J.P., Yu, J.K.: On an exact mass formula of Shimura. Duke Math. J. **107**(1), 103–133 (2001)
11. Gelbart, S.S.: Automorphic forms on adèle groups. Princeton University Press (1975) Annals of Mathematics Studies, No. 83
12. Greenberg, M., Voight, J.: Lattice methods for algebraic modular forms on classical groups, this volume.
13. Gross, B.H.: Algebraic modular forms. Israel J. Math. **113**, 61–93 (1999).
14. Humphreys, J.E.: Linear algebraic groups. Springer-Verlag, New York (1975). Graduate Texts in Mathematics, No. 21
15. Lansky, J., Pollack, D.: Hecke algebras and automorphic forms. Compositio Math. **130**(1), 21–48 (2002).
16. Loeffler, D.: Explicit calculations of automorphic forms for definite unitary groups. LMS J. Comput. Math. **11**, 326–342 (2008)
17. Pizer, A.: An algorithm for computing modular forms on $\Gamma_0(N)$. J. Algebra **64**(2), 340–390 (1980).
18. Platonov, V., Rapinchuk, A.: Algebraic groups and number theory, *Pure and Applied Mathematics*, vol. 139. Academic Press Inc., Boston, MA (1994). Translated from the 1991 Russian original by Rachel Rowen
19. Shin, S.W.: Galois representations arising from some compact Shimura varieties. Ann. of Math. (2) **173**(3), 1645–1741 (2011).
20. Springer, T.A.: Reductive groups. In: Automorphic forms, representations and *L*-functions (Corvallis, 1977), *Proc. Sympos. Pure Math.*, vol. 33 part 1, American Mathematical Society (1979).

21. Springer, T.A.: Linear algebraic groups, *Progress in Mathematics*, vol. 9, second edn. Birkhäuser Boston Inc., Boston, MA (1998)
22. Tits, J.: Reductive groups over local fields. In: Automorphic forms, representations and *L*-functions (Corvallis, 1977), *Proc. Sympos. Pure Math.*, vol. 33 part 1, American Mathematical Society (1979).