Computing modular forms on definite quaternion algebras.

Last modified some time in the 1990s.

Here are some notes on quaternion algebras, modular forms on definite quaternion algebras, and how they correspond to certain classical modular forms. The definition of modular forms on a definite quaternion algebra is essentially combinatorial, although somewhat long. The Jacquet-Langlands theorem gives a link between these new kinds of modular forms and certain classical modular forms, but in a rather abstract way. However it is possible to translate it down to a rather concrete statement, and that is the point of these notes.

Everything here is known to the experts, and the only thing these notes have going for them is their concreteness, something which is usually lacking in the more modern literature. Hopefully these notes will explain how one might attempt to actually do computations of spaces of modular forms in a way that as far as I know, noone has implemented. In fact, the initial motivation for these notes was to explain to William Stein (who has already written some programs for computing in spaces of modular forms) an algorithm for doing some more computations, especially computations which would work for any weight $k \geq 2$ and would perhaps be faster than the standard methods being used by people like Cremona. Whether they are in fact faster remains to be seen.

Of course, I learnt almost all of this from Richard Taylor. One reference for some of this stuff is his papers with Fred Diamond from about 1992. If anyone finds any inaccuracies in these notes or has any comments I'd love to hear about them, for example by email to `buzzard@dpmms.cam.ac.uk`.

§1. Introduction.

This section is much more vague than the others, and is an attempt to explain what the point of this note is.

The Jacquet-Langlands theorem says that if you have two quaternion algebras, then certain automorphic forms for one of them are in canonical bijection with certain automorphic forms for the other. As it stands this statement is a bit general, as well as being a bit vague, and it also has the merit of being fairly incomprehensible to many number theorists. The point is that $M_2(\mathbb{Q})$ is a quaternion algebra, and classical modular (eigen)forms can be viewed as automorphic forms for $M_2(\mathbb{Q})$. So if one translates the statement of the JL theorem down a bit, one gets that certain classical modular forms should be related to certain "modular forms" on other quaternion algebras. In some cases, though, the definition of a modular form for a quaternion algebra is (surprisingly) much easier than the definition of a classical modular form.

In fact, if D is a *definite* quaternion algebra (all definitions are to come, of course) then the modular forms for D are rather concrete algebraic objects. Vaguely speaking, classical modular forms might be thought of as an "H^1" (via the Eichler-Shimura isomorphism), and automorphic forms for a definite quaternion algebra can be thought of as an "H^0" and we all know that H^0s are easier than H^1s. Another way of saying why definite quaternion algebras are easy is that classical modular forms can be thought of as H^0 of a certain coherent sheaf on a (modular) curve, whereas modular forms for a definite quaternion

algebra are H^0 of a sheaf on a zero-dimensional thing (a finite set of points), and are hence no more than the sum of the fibres over each point.

My feeling is that computing with definite quaternion algebras must be much easier than with classical modular forms. Of course, one drawback is that one doesn't see *all* classical forms in this way (for example one will never find Δ—remember that only some automorphic forms on one quaternion algebra will correspond to automorphic forms on another one) but one can see many, and at least it's good for examples.

§2. Some definitions.

Now we become more precise. Let K be a field.

Definition. A *quaternion algebra* over K is a (necessarily non-commutative!) ring D equipped with an injective ring map $K \to D$, satisfying the following 3 axioms:

1) (The image of) K is the centre of D
2) The dimension of D, considered as a K-vector space, is 4.
3) D has no non-trivial 2-sided ideals.

The canonical example of a quaternion algebra is $D = M_2(K)$, with K being embedded as the scalar matrices.

Definition. A quaternion algebra over K which is isomorphic to $M_2(K)$ is said to be *split*.

Of course, there are examples of non-split quaternion algebras. For example, $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with the usual relations holding on i, j and k, is a quaternion algebra over $\mathbb{R}$.

Note that $\mathbb{H}$ has the interesting property that if $0 \neq h = a + bi + cj + dk \in \mathbb{H}$ then h has an inverse, namely $(a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$. Hence non-commutativity of multiplication is the only thing that stops $\mathbb{H}$ from being a field. Sometimes rings with this property are called *skew-fields*. Of course, elements like $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ stop $M_2(\mathbb{R})$, or indeed $M_2(K)$, from having this property. Rather surprisingly, this is a characterisation of whether a quaternion algebra is split or not.

Theorem. If K is a field and D is a quaternion algebra over K then D is not split iff every non-zero element of D has an inverse.

We sometimes abbreviate "Let D be a quaternion algebra over the field K" by "Let D/K be a quaternion algebra".

The actual definition of a quaternion algebra looks a bit daunting, but we shall never actually use it, I just included it for completeness. What I shall do next is simply to state, for various fields, what all the quaternion algebras are up to isomorphism, and so if you are prepared to take things on trust then you never need even digest what the definition of a quaternion algebra is.

§3. First examples of quaternion algebras.

1) If K is algebraically closed, then there is only 1 quaternion algebra over K up to isomorphism, namely $M_2(K)$, the split one.

2) If K is finite then there is also only one quaternion algebra over K and it's of course the split one again.

3) If K is $\mathbb{R}$ then there are two quaternion algebras (up to isomorphism), namely $M_2(\mathbb{R})$ and the quaternions $\mathbb{H}$ as above.

4) If K is a finite extension of $\mathbb{Q}_p$ then there are again 2, namely $M_2(K)$ and another one, which can be written down explicitly thus.

We know that finite unramified extensions of K correspond bijectively to finite extensions of the residue field of K. Now the residue field of K has a unique extension of degree 2, and hence there is a unique extension L/K of degree 2 which is unramified. Now let D be the subset of $M_2(L)$ consisting of matrices

$$\begin{pmatrix} a & b \\ \pi\sigma(b) & \sigma(a) \end{pmatrix}$$

where a and b are arbitrary elements of L, π is a uniformiser of K (and hence of L too) and σ is the non-trivial element of $\mathrm{Gal}(L/K)$. This set turns out to be a ring and indeed a quaternion algebra over K which is not split. Moreover, it's the only one, up to isomorphism.

Note that this quaternion algebra is usually *not* $K \oplus Ki \oplus Kj \oplus Kk$ with i, j and k satisfying the usual relations; even though this latter thing is a quaternion algebra, it is actually isomorphic to $M_2(K)$ a lot of the time. For example, it's a neat exercise to show that if $K = \mathbb{Q}_p$ for p odd, then this latter quaternion algebra is always $M_2(K)$.

5) For more specific local fields, one can be a bit more concrete. For example, if $K = \mathbb{Q}_p$ with p odd, then here's another description of the non-split quaternion algebra over K.

Choose $\overline{u} \in (\mathbb{Z}/p\mathbb{Z})^\times$ a non-square, and lift it to $u \in \mathbb{Z}_p$. Then set $D = \mathbb{Q}_p \oplus \mathbb{Q}_p\alpha \oplus \mathbb{Q}_p\beta \oplus \mathbb{Q}_p\alpha\beta$, where we now have to explain how to multiply everything together to make this a ring. We ask that $\alpha^2 = u$, $\beta^2 = pu$ and $\alpha\beta = -\beta\alpha$. It is now easily checked that we can extend this to a unique associative multiplication on D, and moreover it turns out that D is a non-split quaternion algebra over $\mathbb{Q}_p$.

If $K = \mathbb{Q}_2$ then it turns out that the non-split quaternion algebra is isomorphic to $\mathbb{Q}_2 \oplus \mathbb{Q}_2 i \oplus \mathbb{Q}_2 j \oplus \mathbb{Q}_2 k$ with the usual relations.

§4 Base extension, traces and norms.

If D/K is a quaternion algebra over a field, and L is a field extension of K, then $D \otimes_K L$ is a quaternion algebra over L.

Definition. Say that L *splits* D, or that D *splits over* L, or that L *is a splitting field for* D, if $D \otimes_K L$ is split, that is, isomorphic to $M_2(L)$.

Note that D may well not be split, but could become split after a field extension. For example, one can take the non-split "usual" quaternions over $\mathbb{R}$ and then tensor up to $\mathbb{C}$ and they must become split, because there is only one quaternion algebra over $\mathbb{C}$. More

generally, if D/K is a quaternion algebra and $\overline{K}$ is the algebraic closure of K then $\overline{K}$ must split D because there is only one quaternion algebra over $\overline{K}$.

Let K be an arbitrary field, and let D/K be a quaternion algebra. Choose an isomorphism $D \otimes_K \overline{K} \cong M_2(\overline{K})$, and note that this gives us a way of thinking of D as a subring of $M_2(\overline{K})$. In particular, elements of D now have traces and determinants.

Definition. If $d \in D$, define the *trace* of d to be the trace of d considered as an element of $M_2(\overline{K})$. Also define the *norm* of d to be the determinant of d considered as an element of $M_2(\overline{K})$.

Theorem. The norm and trace of an element of d are in K, and are independent of the choice of isomorphism $D \otimes_K \overline{K} \cong M_2(K)$.

§5 Quaternion algebras over number fields.

Let K be a number field and let D be a quaternion algebra over K. If v is a place of K then one can tensor up to the completion K_v of K at v, and ask whether or not this extension splits D. Let $S(D)$ denote the set of places of K for which D does *not* split. Rather surprisingly, it turns out that knowing $S(D)$ is all you need to know D, as explained by the following

Theorem.
(a) The set $S(D)$ is a finite set of places of K, with an even number of elements, none of them complex.
(b) Two quaternion algebras D and E over K are isomorphic if and only if $S(D) = S(E)$.
(c) If S is any finite set of places of K containing no complex places, and S has an even number of elements, then there is exactly one quaternion algebra D/K such that $S(D) = S$.

Put another way, there is a bijection between the set of isomorphism classes of quaternion algebras over K and the set of finite sets of non-complex places of K with even size.

For example, if $D = M_2(K)$ then D splits at every completion of K and hence $S(D)$ is the empty set. As another example, if $K = \mathbb{Q}$ and $D = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$, then D is not split, and it turns out that D splits over $\mathbb{Q}_p$ if and only if p is odd, and so $S(D) = \{2, \infty\}$.

To simplify things, let's now set $K = \mathbb{Q}$. So let $D/\mathbb{Q}$ be a quaternion algebra.

Definition. The *discriminant* $d = \mathrm{disc}(D)$ of D is the product of the primes p in $S(D)$.

Here I am distinguishing between primes of $\mathbb{Q}$ (which are all finite), and places of $\mathbb{Q}$ (where I would allow the infinite place).

By the theorem above, we see that $\mathrm{disc}(D)$ uniquely determines D, and moreover that every square-free positive integer d is the discriminant of a unique quaternion algebra over $\mathbb{Q}$.

Given a square-free positive integer d, there is a unique quaternion algebra $D/\mathbb{Q}$ with discriminant d, and it is easy to work out whether or not $D \otimes_{\mathbb{Q}} \mathbb{R}$ is split, because one knows that the total number of places in $S(D)$ is even, and so one can count the number of primes dividing d, and this number is even iff $\infty \notin S(D)$.

Definition. A quaternion algebra $D/\mathbb{Q}$ is *definite* if $\infty \in S(D)$, that is, if $D \otimes_{\mathbb{Q}} \mathbb{R} \ncong M_2(\mathbb{R})$.

Karsten once pointed out to me that a way to remember this is that definite quaternion algebras are definitely not $M_2(\mathbb{Q})$.

Given a positive squarefree integer d, it is possible to write down explicitly the quaternion algebra over $\mathbb{Q}$ with discriminant d. One method I know is to find it as a sub-$\mathbb{Q}$-space of dimension 4 of $M_2(\overline{Q})$. Another method is as follows: choose non-zero rational numbers a and b and consider the ring $D = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\alpha\beta$ with $\alpha^2 = a$, $\beta^2 = b$, and $\alpha\beta = -\beta\alpha$. This is always a quaternion algebra over $\mathbb{Q}$, and in fact all quaternion algebras over $\mathbb{Q}$ arise in this way. For example, if $a = b = -1$ then one retrieves the quaternion algebra of discriminant 2, and if p is a prime congruent to 3 mod 4 then setting $a = -1$ and $b = -p$ gives the quaternion algebra of of discriminant p. Doing exercises like this taught me a lot about quaternion algebras. It's a slightly ambitious exercise, given d positive and squarefree, to find a and b such that the quaternion algebra above has discriminant D.

§6. Orders.

Our aim in the next three or so sections is to define modular forms over definite quaternion algebras. As I remarked above, this is actually not too hard, although it will take a while. First I need to talk about orders. I shall be lazier now and just talk about quaternion algebras over $\mathbb{Q}$ and $\mathbb{Q}_p$ from now on, because this is all that we shall need.

Let p be a prime.

Definition. An *order* in a quaternion algebra $D/\mathbb{Q}_p$ is a subring $\mathcal{O} \subset D$ such that
(a) $\mathcal{O} \cong (\mathbb{Z}_p)^4$ as an abelian group, and
(b) $\mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = D$.

An order is said to be *maximal* if it is not properly contained in any larger order.

It is a theorem that maximal orders exist (and this is not a Zorn argument!). For example, $M_2(\mathbb{Z}_p)$ is a maximal order in $M_2(\mathbb{Q}_p)$, and so are all its conjugates. In fact, any maximal order of $M_2(\mathbb{Q}_p)$ is conjugate to $M_2(\mathbb{Z}_p)$. If D is the non-split quaternion algebra over K then D has a unique maximal order, consisting of the elements of D with integral norm.

Now let's consider the case $K = \mathbb{Q}$.

Definition. An *order* in a quaternion algebra $D/\mathbb{Q}$ is a subring $\mathcal{O}$ of D such that
(a) $\mathcal{O} \cong \mathbb{Z}^4$ as an abelian group, and
(b) $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = D$.

It is a theorem that every quaternion algebra over $\mathbb{Q}$ has maximal orders.

As an example, if $D = M_2(\mathbb{Q})$ then $\mathcal{O} = M_2(\mathbb{Z})$ is a maximal order, as are its conjugates. In fact, if D is any indefinite quaternion algebra over $\mathbb{Q}$ then all the maximal orders of D are conjugate.

As another example, if $D = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ with the usual relations on i, j and k, then $\mathcal{O} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$ is an order in D, and one might expect that it's a maximal order, just as one might expect that $\mathbb{Z}[\sqrt{5}]$ might be the integers in $\mathbb{Q}(\sqrt{5})$

when one first starts doing algebraic number theory. However $\mathcal{O}$ is not maximal: there is a bigger order, namely $\{a+bi+cj+dk \mid \text{either } a,b,c,d \in \mathbb{Z} \text{ or } a,b,c,d \in \mathbb{Z}+\frac{1}{2}\}$, and in fact this latter order is maximal.

If $D/\mathbb{Q}$ is definite, then there might be more than one conjugacy class of maximal orders, but a compactness argument shows that there are only finitely many.

Definition. If $D/\mathbb{Q}$ is a quaternion algebra, and p is a prime, then write D_p for the quaternion algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ over $\mathbb{Q}_p$. If $\mathcal{O} \subset D$ is an order, write $\mathcal{O}_p$ for the order $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ of D_p (it's not hard to check that $\mathcal{O}_p$ is in fact an order in D_p).

It's a neat exercise to prove that if $D/\mathbb{Q}$ is a quaternion algebra and $\mathcal{O} \subset D$ is an order, then $\mathcal{O}$ is maximal iff $\mathcal{O}_p$ is maximal in D_p for all p.

§7. Enter the adeles.

Let D be a quaternion algebra over $\mathbb{Q}$ and fix a maximal order $\mathcal{O}$ of D. Later we shall assume that D is definite but at the minute we don't need to. Let $\mathbb{A}^f$ denote the finite adeles, that is, the restricted product of $\mathbb{Q}_p$ for all primes p. Even more frightening, let D^f denote $D \otimes_{\mathbb{Q}} \mathbb{A}^f$. We shall now give a more down-to-earth description of D^f. Choose an order $\mathcal{O} \subset D$. Then an element of D^f can be thought of as the choice of an element $d_p \in D_p$ for every prime p, subject to the restriction that $d_p \in \mathcal{O}_p$ for but finitely many p. Note that this does not depend on the choice of $\mathcal{O}$ because any two orders will differ only at a finite number of primes.

I should say something about topologies, but I fear it will be unhelpful. The adeles have a topology on them. If I choose a $\mathbb{Q}$-basis for D then D^f becomes isomorphic to $(\mathbb{A}^f)^4$ and we can give it the product topology induced from the adeles. This makes D^f into a topological ring. Now one follows the usual procedure to make $(D^f)^\times$ into a topological group—one embeds it into $(D^f)^2$ via $x \mapsto (x, x^{-1})$ and then takes the subspace topology of the product topology.

On a more practical level, one can work prime by prime. Choose an order $\mathcal{O} \subset D$. Then $\mathcal{O}_p \cong \mathbb{Z}_p^4$, and so one can put a p-adic topology on $\mathcal{O}_p$ to make this an isomorphism of topological groups. Give $(\mathcal{O}_p)^\times$ the subspace topology, and set $K = \prod_p (\mathcal{O}_p)^\times$ with the product topology. Note that $K \subset D^f$, and in fact the topology that we just put on K is the subspace topology. In particular, K is compact, it being the product of compact spaces. Moreover, it turns out that K is a compact open subgroup of D^f. Knowing this actually tells us exactly what the topology on D^f is, because D^f is just the disjoint union of translates of K.

To be even more concrete, we could take $D = M_2(\mathbb{Q})$ and $\mathcal{O} = M_2(\mathbb{Z})$. Then $K = \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is a compact open subgroup of $D^f = \mathrm{GL}_2(\mathbb{A}^f)$. It's just a higher-dimensional version of the statement that $(\widehat{\mathbb{Z}})^\times$ is compact and open in $(\mathbb{A}^f)^\times$.

In fact, there are a wealth of easily-definable compact open subgroups of D^f. For example, choose any finite set of primes and for each such prime choose an open compact subgroup K_p of $(D_p)^\times$. So for example if $\mathbb{Q}_p$ splits D and we choose an isomorphism $(D_p)^\times \cong \mathrm{GL}_2(\mathbb{Q}_p)$, then K_p could be the matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$ which are congruent to the identity modulo p^n for some n. For the primes not in this chosen finite set, set $K_p = (\mathcal{O}_p)^\times$. Then again the product $K = \prod_p K_p$ will be an open compact subgroup of $(D^f)^\times$.

In practice, again, one doesn't really need to understand exactly what the topology is, one just needs to know some examples. By the way, not all the open compact subgroups of $(D^f)^\times$ will be expressible in this "product" form, but essentially all of the open compact subgroups that we are interested in will be.

Finally, let $D/\mathbb{Q}$ be a definite quaternion algebra, and let $K \subset (D^f)^\times$ be an open compact subgroup. The important result is that

Theorem. The double coset space $D^\times \backslash (D^f)^\times / K$ is finite.

This finite set is the analogue of a modular curve in the definite quaternion algebra set, although I'm actually too lazy to explain why at the minute. It turns out that the space of modular forms of weight k and "level K" can just be thought of (non-canonically) as the complex vector space of functions from this finite set to a certain finite-dimensional complex vector space. Moreover, the space of "mod p modular forms for D of weight k and level K" can be thought of as the space of functions from this finite set to a certain finite-dimensional vector space over $\mathbb{F}_p$.

§8. Weight 2 modular forms for definite quaternion algebras.

Fix $D/\mathbb{Q}$ definite and $\mathcal{O}$ a maximal order. Let $d = \mathrm{disc}(D)$. First I'll explain the weight 2 case of the Jacquet-Langlands theorem. First I have to give some names to certain maximal compact subgroups of $(D^f)^\times$. For all primes p prime to d, we have that $\mathcal{O}_p \cong M_2(\mathbb{Z}_p)$ and so let's fix such an isomorphism for all such p. Now given some positive integer N prime to d, let's define some compact open subgroups of $(D^f)^\times$. For p prime to N, set $K_p = (\mathcal{O}_p)^\times$. For p dividing N, say p^e exactly divides N and let $K_{0,p}$ be the elements in $(\mathcal{O}_p)^\times \cong \mathrm{GL}_2(\mathbb{Z}_p)$ which are congruent to $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ mod p^e. Let $K_{1,p}$ denote the elements in $K_{0,p}$ which are congruent to $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ mod p^e.

Definition. Let $U_0(N) = \prod_{p \not| N} K_p \times \prod_{p|N} K_{0,p}$ and let $U_1(N) = \prod_{p \not| N} K_p \times \prod_{p|N} K_{1,p}$.

Note that $U_0(N)$ and $U_1(N)$ are compact open subgroups of $(D^f)^\times$.

Definition. If $U = U_0(N)$ or $U_1(N)$, then set $L_2^D(U;\mathbb{C}) = \{f : D^\times \backslash (D^f)^\times / U \to \mathbb{C}\}$.

Note that $D^\times \backslash (D^f)^\times / U$ is a *finite set* on both cases, and so $L_2^D(U;\mathbb{C})$ is a finite-dimensional vector space. Moreover, this finite set is *explicitly computable* in many cases (see examples later), so one really can compute this space. It would be nice if these spaces were spaces of modular forms for D of weight 2 and level N but this isn't quite true; there is an Eisenstein series that we haven't quite removed (this strangeness only happens for weight 2). So let's remove it.

Let $U = U_0(N)$ or $U_1(N)$. Note that the constant functions are a 1-dimensional subspace of $L_2^D(U;\mathbb{C})$; call them $L_2^{D,\mathrm{triv}}(\mathbb{C})$.

Definition. The modular forms of weight 2 and level U for D are

$$S_2^D(U;\mathbb{C}) = L_2^D(U;\mathbb{C})/L_2^{D,\mathrm{triv}}(\mathbb{C}).$$

The case $U = U_1(N)$ is analogous to $\Gamma_1(N)$, and the case $U = U_0(N)$ is analogous to $\Gamma_0(N)$.

Now I'll put a Hecke action on $S_2^D(U;\mathbb{C})$, but before I tell you what it is I'll tell you the point:

Theorem. There is an isomorphism of Hecke modules

$$S_2^D(U_0(N);\mathbb{C}) \cong S_0 \subseteq S_2(\Gamma_0(Nd);\mathbb{C})$$

and an isomorphism

$$S_2^D(U_1(N);\mathbb{C}) \cong S_1 \subseteq S_2(\Gamma_1(N) \cap \Gamma_0(d);\mathbb{C}),$$

where the right hand sides are classical complex vector spaces of cusp forms, and S_0 and S_1 are the subspaces consisting of forms which are new at all primes dividing d.

In more flashy language, S_0 and S_1 are the sum of the eigenspaces coming from forms which are "special" at all primes dividing d.

For example, if d is a prime l and $N = 1$ then there are no oldforms at level d because oldforms would come from cusp forms of level 1 and weight 2, and there aren't any.

This theorem is of course just an application of the Jacquet-Langlands theorem. The idea is that modular forms on a quaternion algebra should be able to spot forms which are either special or supercuspidal at all primes dividing the discriminant of the quaternion algebra. For more on these notions, see some other notes I've written, on the local Langlands correspondence.

Now I still have to explain what the Hecke action on $S_2^D(U;\mathbb{C})$ is, for $U = U_0(N)$ or $U_1(N)$, before we can even understand the theorem. Well, first I'll explain what it is on $L_2^D(U;\mathbb{C})$, and then it will be easy to see that it preserves $L_2^{D,\mathrm{triv}}(\mathbb{C})$ and hence induces an action on $S_2^D(U;\mathbb{C})$. I have to produce Hecke operators, and in the $U_1(N)$ case, diamond operators. Because primes dividing d are rather strange in this setting, I shall just work with primes not dividing d.

So let p be a prime not dividing d. Let η_p denote the element of $(D^f)^\times$ which is the identity at all primes which are prime to p, and equal to $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ at p (remember that we fixed an isomorphism $\mathcal{O}_p \cong M_2(\mathbb{Z}_p)$, and this is indeed where we are assuming that p is prime to d). Write the double coset $U\eta_p U = \coprod_{j=1}^n \alpha_{p,j} U$ (note that this is a finite union) and, for $f \in L_2^D(U;\mathbb{C})$, define $T_p f$ by $T_p f(\gamma) = \sum_{j=1}^n f(\gamma\alpha_{p,j})$.

Similarly, if p is a prime not dividing d and $U = U_1(N)$, let ν_p be the element of $(D^f)^\times$ which is the identity at all primes which are prime to p, and which is $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$ at p. Note that this element is in the centre of $(D^f)^\times$ and hence $U_1(N)\nu_p U_1(N) = \nu_p U_1(N)$. Define $\langle p\rangle$ on $L_2^D(U_1(N);\mathbb{C})$ by $(\langle p\rangle f)(\gamma) = f(\gamma\nu_p)$. Note that this only depends on p modulo N, as if p and q are two primes which are prime to d and congruent mod N, then $\gamma\nu_p = \gamma(p/q)\nu_q u = (p/q)\gamma\nu_q u$ where $u \in U_1(N)$ and $(p/q) \in D^\times$.

I guess that's it for weight 2.

Kevin Buzzard, May 1998.

In fact, that's it for these notes, for the time being. Now let's switch to an example and some more personal notes directed to William alone.

OK, temporarily, the object of these notes isn't to explain any more about the JL theorem, it's to give you (W) something to think about, so you can decide whether or not it will be easier to do this computation or the "classical" one (and it will give you some maths to think about whilst your computer cranks about with its Γ_1 with character computations!). I haven't debugged this stuff so there might be typos.

Rather than muck about with the "easiest" case of $M_2(\mathbb{Q})$, I shall just go straight to the quat alg I'm interested in. The representation that should exist of level 5203 should be coming from a modular form which is unramified principal series at all primes other than 11 and 43, is supercuspidal at 11, and is ramified principal series at 43. In particular, because it's supercuspidal at 11, there will be a modular form on the quaternion algebra of disc 11 which will have the same Hecke eigenvalues for all diamond operators and all T_p for $p \neq 11$, by the JL theorem.

So let D be the quaternion algebra $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}\beta \oplus \mathbb{Q}i\beta$ where $i^2 = -1$, $\beta^2 = -11$ and $\beta i = -i\beta$. This is the quat alg of disc 11. We need a maximal order to establish what a $U_0(1)$-structure is. Ones first guess at a maximal order is $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\beta \oplus \mathbb{Z}i\beta$, but again we are slightly wrong. The localisation of this order is maximal at all odd primes, but not at $p = 2$. It turns out that we can adjoin $\gamma := (1 + \beta)/2$ (and $i\gamma = (i + i\beta)/2$), and consider $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\gamma \oplus \mathbb{Z}i\gamma$. Note that $\gamma^2 = \gamma - 3$ and $\gamma i = i - i\gamma$ so $\mathcal{O}$ is a ring. Moreover, $\mathcal{O}$ turns out to be a maximal order in D (because $\mathcal{O}_p$ is maximal in D_p for all p, by an explicit computation). Another way of seeing $\mathcal{O}$ is that it's the $a + bi + c\beta + di\beta$ in D such that a, c are either both integers or both in $\mathbb{Z} + \frac{1}{2}$ and b, d are also either both integers or both in $\mathbb{Z} + \frac{1}{2}$. Put another way, $2a, 2b, 2c, 2d$ are all integers and $2a, 2c$ have the same parity, and $2b, 2d$ have the same parity.

Now, essentially by definition, if $\gamma = a + bi + c\beta + di\beta \in D_p$, we have $\gamma \in \mathcal{O}_p$ iff $a, b, c, d \in \mathbb{Z}_p$ for p odd, and $\gamma \in \mathcal{O}_2$ iff $2a, 2b, a + c, b + d \in \mathbb{Z}_2$.

Let's make explicit the isomorphism between $\mathcal{O}_p$ and $M_2(\mathbb{Z}_p)$ for all $p \neq 11$. If $p \neq 11$ then there is always a solution to $x^2 + y^2 = -11$ with $x, y \in \mathbb{Z}_p$. Choose such a solution and then define the map $\mathcal{O}_p \to M_2(\mathbb{Z}_p)$ by sending i to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and β to $\begin{pmatrix} x & y \\ y & -x \end{pmatrix}$.

Let's start with the easiest compact open subgroup there is, namely $U = U_0(1) = \prod_p (\mathcal{O}_p)^\times$. One now wonders what the size of the finite set $D^\times \backslash (D^f)^\times / U$ is. Well, we know that $S_2(\Gamma_0(11)) \cong \mathbb{C}$ and hence the dimension of $L_2^D(U; \mathbb{C})$ is 2 (we add one because of the trivial 1-dimensional space of constant functions). We deduce that the size of the set $D^\times \backslash (D^f)^\times / U_0(1)$ must be 2.

So our next task is to find an explicit element c of $(D^f)^\times$ which isn't in $D^\times U$. Then we will have $(D^f)^\times = D^\times U \coprod D^\times cU$. Here's one I found earlier, although it's not clear to me whether this is the best choice. I looked for a c which only had support at a small

prime, and I found that if I set $c_p = 1$ for p odd and $c_2 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ then c can't be in $D^\times U_0(1)$ (see proof below). I have to be slightly more precise, by explicitly saying what I took the isomorphism $\mathcal{O}_2 \cong M_2(\mathbb{Z}_2)$ to be. Well, I set x be the square root of -15 which was congruent to 1 mod 8, and I set $y = 2$.

Well, here's the proof that $c \notin D^\times U_0(1)$, and it's the kind of argument that we have to use again and again. If c were in $D^\times U_0(1)$, then write $c = \delta u$. First take the determinant/norm of this, and deduce that the adele which is 2 at 2 and 1 elsewhere must be $\nu(\delta)\nu(u)$. Well, $\delta = a + bi + c\beta + di\beta$ with $a, b, c, d \in \mathbb{Q}$ and $\nu(\delta) = a^2 + b^2 + 11c^2 + 11d^2$ so in particular it's positive. And $\nu(u) \in \widehat{\mathbb{Z}}^\times$ because $U_0(1)$ is integral at every prime. Hence we have a positive rational must equal a unit times $\nu(c)$ and taking the projection to each prime we deduce that $\nu(\delta)$ has valuation 1 at 2 and valuation 0 at all odd primes. In particular, if it's a positive rational then it must be 2. So $a^2 + b^2 + 11c^2 + 11d^2 = 2$ and a, b, c, d are rational.

Next we make a more careful analysis at each prime. For all odd primes, we get that $\delta u_p = 1$ and hence $\delta = u_p^{-1} \in (\mathcal{O}_p)^\times$. In particular we must have $a, b, c, d \in \mathbb{Z}_p$. But a, b, c, d are rational, so we deduce that $a, b, c, d \in \mathbb{Z}[1/2]$.

Finally we deal with the case $p = 2$, which is the only information we have left. We get that $\delta = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} (u_2)^{-1}$ and $u_2 \in \mathrm{GL}_2(\mathbb{Z}_2)$, so $\delta = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ with $x, y, z, t \in \mathbb{Z}_2$. In particular $\delta \in M_2(\mathbb{Z}_p)$ and $\delta \equiv \begin{pmatrix} 0 & 0 \\ z & t \end{pmatrix}$ mod 2.

Next we recall our explicit isomorphism $\mathcal{O}_2 \cong M_2(\mathbb{Z}_2)$. I chose it such that $i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\beta \mapsto \begin{pmatrix} x & 2 \\ 2 & -x \end{pmatrix}$ where $x \equiv 1$ mod 8 is a square root of -15. In particular,

$$\delta = \begin{pmatrix} a + xc + 2d & b + 2c - xd \\ -b + 2c - xd & a - xc - 2d \end{pmatrix}.$$

Now we use the fact that this latter matrix, *a priori* only in $M_2(\mathbb{Q}_2)$, is in fact in $M_2(\mathbb{Z}_2)$ and even has the top row congruent to 0 mod 2.

Adding top left and bottom right, we deduce that $2a \in \mathbb{Z}_2$. Subtracting, we deduce that $2xc + 4d \in \mathbb{Z}_2$. Doing the same with the other 2 entries shows that $2b \in \mathbb{Z}_2$ and $4c - 2xd \in \mathbb{Z}_2$. Recall that a, b, c, d are rational. Solving the c, d linear equations we deduce that $2d \in \mathbb{Z}_2$ and $2c \in \mathbb{Z}_2$. Hence we deduce that all of a, b, c, d are in $\frac{1}{2}\mathbb{Z}$, because if you multiply any one of them by 2, it's integral at every prime.

Remember the one global constraint that we had: we knew that $a^2+b^2+11c^2+11d^2 = 2$, and so

$$(2a)^2 + (2b)^2 + 11(2c)^2 + 11(2d)^2 = 8.$$

Moreover, $2a, 2b, 2c, 2d$ are all integers (that is, in $\mathbb{Z}$). But there aren't that many solutions to these equations in integers. In fact, the only ones are $c = d = 0$ and $a, b = \pm 1$. So we have 4 solutions. Now go back to the *one* fact that we haven't used yet, namely that the top row of that matrix in $M_2(\mathbb{Z}_2)$ has got entries which are 0 mod 2, and observe that none of our solutions satisfy this! So $c \notin D^\times U_1(1)$, as was to be proved.

Now the next natural question to ask is the following: how do the Hecke operators act on $L_2^D(U_0(1);\mathbb{C})$? One will be able to compute them explicitly but I'm not going to at the minute. My feeling is that it would be a good exercise for you to do. I don't know whether T_2 will be harder or easier than the rest. The basic idea will be the following. An element $f \in L_2^D := L_2^D(U_0(1);\mathbb{C})$ will be determined by the complex numbers $f(1)$ and $f(c)$ so there is an obvious basis for the 2-dimensional space L_2^D, it's just e_1, the function which is 0 on c and 1 on 1, and e_2, the function which is 1 on c and 0 on 1. It must be possible to explicitly work out the matrix of T_p on this basis, for all primes not equal to 11. The answer will be the following: all the T_p will be simultaneously diagonalisable, one eigenspace will be Eisenstein and the other will be the value of a_p for the elliptic curve of conductor 11. It's weird how this "profound" information is coming out of such combinatorial data. Henri Darmon once remarked to me that it was probably something to do with theta series, I forgot exactly what he said but I remember that he was right!

Do you feel competent to work out all the matrices for T_p in this case? Basically the computation will be the same. If p is a prime and $U = U_0(1)$ then $U\eta_p U$ will be (at least for $p \neq 11$)

$$\left(\coprod_{j=0}^{p-1}\begin{pmatrix}p & j\\ 0 & 1\end{pmatrix}_p\right)\coprod\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}_p,$$

where the matrix M_p denotes the element of D^f which is M at the prime p and 1 everywhere else. Then you have to decide whether $\begin{pmatrix}p & j\\ 0 & 1\end{pmatrix}_p$ etc is in $D^\times U_0(1)$ or in $D^\times cU_0(1)$. My guess is that exactly the same computation as I did will tell you whether it's in $D^\times U_0(1)$ or not, and if it's not then it's in the other one.

There might be a cleverer way to do this based on first finding all the solutions to $A^2+B^2+11C^2+11D^2 = 4p$ and then counting something else involving congruences, but at the minute I have no idea how much of this you have digested so I won't explain that to you yet. You see, I did one of these computations before so I know what should happen.

After all this, we could think about how to do the actual computation. There are 2 choices. Either we do weight 2 and level 26015 or weight 5 and level 5203. My guess is that weight 5 will be easier because the dimension of the space will be about 3/5 the size, or something, so the computation will be easier. The hard part might be finding the analogue of c above. The problem is that with a smaller U (the U we're interested in is $U_1(43)$ intersected with some subtle structure at 11), the size of the set $D^\times\backslash(D^f)^\times/U$ will be bigger, although there might be a way of mechanising how to find it.

Kevin