LOCAL PROPERTIES OF MODULAR GALOIS REPRESENTATIONS

ANDREW SNOWDEN

1. Introduction

Let f be a cuspidal eigenform of weight 2 and level $\Gamma_0(N)$. Let p be a prime, which we assume does not divide N. We have stated (though have not proved) that there exists a Galois representation $\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$, where S is the set of primes dividing pN, which satisfies and is characterized by the following two properties: (1) the determinant of ρ is the cyclotomic character $\chi = \chi_p$; and (2) for a prime $\ell \nmid pN$ the trace of $\rho(\mathrm{Frob}_\ell)$ is equal to the eigenvalue of the Hecke operator T_ℓ acting on f. We have also stated (and not proved) that for $\ell \mid N$ the representation $\rho|_{G_{\mathbf{Q}_\ell}}$ corresponds under local Langlands to the local component of the automorphic representation of f at ℓ. We have not yet examined the local representation $\rho|_{G_{\mathbf{Q}_p}}$. For the purposes of this seminar, we will need only one result: if f is ordinary (in the sense of modular forms) then $\rho|_{G_{\mathbf{Q}_p}}$ is crystalline and ordinary (in the sense of Galois representations). The definitions of ordinary are recalled below.

The purpose of this lecture is to sketch the construction of ρ and the proofs that it satisfies the above local conditions, at least for $\ell \nmid N$. The representation ρ is found as a quotient of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$, and is not difficult to construct. To establish the properties of ρ at the unramified places and at p, we use the Eichler-Shimura relation. To formulate and prove this identity, we use the reduction of $X_0(N)$ modulo p. This requires us to introduce some of the theory of moduli of elliptic curves over integers; fortunately, we are in a rather easy situation. At the end of these notes, we explain a bit about what happens in the Hilbert modular case.

I should say here that I am not extremely familiar with this material. I believe I have the main points correct, but I might have some details wrong. Certainly, some details have been omitted. For certain topics, more complete treatments can be found in the references.

2. Moduli of elliptic curves

In this section we define moduli spaces of elliptic curves and establish some of their basic properties.

2.1. The moduli space.

Let S be a scheme. An *elliptic curve* over S is a smooth proper group scheme $E \to S$ whose geometric fibers are connected genus 1 curves. Let Y be the functor which assigns to a scheme S the groupoid $Y(S)$ of elliptic curves over S; that is, $Y(S)$ is the category whose objects are elliptic curves over S and where morphisms are isomorphisms of group schemes over S. We call Y the *moduli space of elliptic curves.*

Proposition 1. *The functor Y is a stack.*

Proof. Let E/S be an elliptic curve. The zero section $0 : S \to E$ defines an ample divisor D on E (in the relative sense) and $3D$ is very ample. Let A_E be the projective coordinate ring of E in this embedding, that is, A_E is $\bigoplus_{n \ge 0} f_*(\mathscr{O}(3nD))$ where $f : E \to S$ is the structure map. Then A_E is a quasi-coherent sheaf of graded rings on S and E is identified with $\mathrm{Proj}(A_E)$. The functor $E \mapsto A_E$ identifies $Y(S)$ with a subcategory of the category of quasi-coherent graded algebras on S. The latter forms a stack in the fppf topology by Grothendieck's theory of flat descent. It is easy to conclude from this that Y itself forms a stack. More precisely, let E_i be elliptic curves on a cover U_i of a scheme S and let f_{ij} be an isomorphism of E_i and E_j on U_{ij} satisfying the 1-cocycle condition. Then A_{E_i} and $A_{f_{ij}}$ define descent data for algebras on S. By flat descent, one obtains a quasi-coherent graded algebra A on S. Put $E = \mathrm{Proj}(S)$. One has a canonical identification $E|_{U_i} = E_i$, which allows one to establish the geometric properties required of E, as these properties are fppf local. (One must say a bit more along the same lines to get the zero section and group law on E.) □

Date: September 11, 2010.

Proposition 2. *The functor Y is formally smooth (over $\mathbf{Z}$).*

Proof. Let S be an affine scheme and let S_0 be a closed subscheme defined by a square zero ideal I. Let E_0 be an elliptic curve over S_0. We must extend E_0 to an elliptic curve over S. Note that any such curve will have the same underlying topological space as E, just a different structure sheaf. Let $U_{0,i}$ be an open affine cover of E_0. Since smooth affine schemes always lift, we can find a smooth affine U_i over S extending $U_{0,i}$. We have thus extended $\mathscr{O}_{E_0}$ to an $\mathscr{O}_S$-algebra on an open cover. These bigger algebras may not patch together, but we can try to modify them so that they do. There is an obstruction class in $H^2(E_0, T_{E_0})$ measuring if such a modification is possible; here T_{E_0} is the tangent sheaf of E_0. Now, since S_0 is affine, this cohomology group is equal to $H^0(S_0, R^2 f_* T_{E_0})$, where $f : E_0 \to S_0$ is the structure map. As $E_0 \to S_0$ is a curve, $R^2 f_*$ vanishes. This shows that $H^2(E_0, T_{E_0})$ vanishes as well, and thus there is no obstruction to the modification procedure. We have thus found a smooth scheme E over S such that E_{S_0} is canonically identified with E_0. One then needs to extend the zero section from S_0 to S; we leave this to the reader. □

2.2. **Level structure in good characteristic.** Let N be an integer. For an elliptic curve E/S we write $E[N]$ for the N-torsion of E. It is a finite flat group scheme over S. If N is invertible on S then $E[N]$ is a finite étale group scheme over S. We define three additional moduli spaces $Y(N)$, $Y_1(N)$ and $Y_0(N)$ over $\mathbf{Z}[1/N]$, as follows:

- $Y(N)(S)$ is the category of tuples (E, P, Q) where E/S is an elliptic curve $P, Q \in E[N]$ form a basis of $E[N]$, i.e., the map $((\mathbf{Z}/N\mathbf{Z})^2)_S \to E[N]$ defined by (P, Q) is an isomorphism of sheaves.
- $Y_1(N)(S)$ is the category of pairs (E, P) where E/S is an elliptic curve and $P \in E[N]$ is a point of exact order N, i.e., the map $(\mathbf{Z}/N\mathbf{Z})_S \to E$ defined by P is an injection of sheaves.
- $Y_0(N)(S)$ is the category of pairs (E, G) where E/S is an elliptic curve and $G \subset E[N]$ is a subgroup scheme which is fppf locally isomorphic to $(\mathbf{Z}/N\mathbf{Z})_S$.

For $N \geq 3$ the category $Y(N)$ is discrete; the same holds for $Y_1(N)$ and $Y_0(N)$ for N large enough. We assume from now on that N is sufficiently large for this to be the case. We now have the following result:

Proposition 3. *Each of $Y(N)$, $Y_1(N)$ and $Y_0(N)$ is a smooth affine curve over $\mathbf{Z}[1/N]$. The natural map from each to Y is finite and étale.*

Proof. We consider only $Y(N)$, leaving the others to the reader. First, it follows easily from Proposition 1 that $Y(N)$ is itself a stack; it is therefore a sheaf of sets since it is discrete. We now show that $Y(N) \to Y$ is relatively representable, finite and étale. Let $S \to Y$ be a map, corresponding to an elliptic curve E/S. The fiber product $Y(N) \times_Y S$ is then identified with the subsheaf of $E[N] \times E[N]$ consisting of those pairs of sections which form a basis. This is clearly a finite étale scheme over S. This establishes the claim. The formal smoothness of $Y(N)$ now follows from Proposition 2.

Here is the main idea of one approach to get representability. The group $G = \mathrm{GL}(2, \mathbf{Z}/3\mathbf{Z})$ acts on $Y(3)$. One can write down explicit equations for $Y(3)$ demonstrating that it is a smooth affine curve over $\mathbf{Z}[1/3]$. One can also show that G acts freely on $Y(N) \times_Y Y(3)$ and that the quotient is identified with $Y(N)$. Since $Y(N)$ is relatively representable and finite étale, the product $Y(N) \times_Y Y(3)$ is a smooth affine curve over $\mathbf{Z}[1/3N]$. It follows that the same holds for the quotient by G, which establishes the required properties of $Y(N)$, at least over $\mathbf{Z}[1/3N]$. There is another explicit moduli problem and finite group one can use to obtain the required properties over $\mathbf{Z}[1/2N]$. This implies the results over $\mathbf{Z}[1/N]$. (One can probably avoid the use of $Y(3)$ by appealing to more general results, such as Artin's representability theorem.) □

Remark 4. The finite étale covers of Y provided by $Y(N)$ show that Y is a Deligne-Mumford stack. The same is true for $Y(N)$, $Y_0(N)$ and $Y_1(N)$ when N is small.

2.3. **Compactification.** The modular curve Y constructed in the previous section is affine. We would now like to compactify it. To do this we must add a few points to it. These points correspond to curves which are limits of elliptic curves. To see what a "limit of an elliptic curve" is, it is useful to think about the situation over the complex numbers: to degenerate an elliptic curve, one can take a few cycles on it and pinch them each to a point. The result is a bunch of $\mathbf{P}^1$s glued together. This motivates the formal definitions which follow.

Let n be an integer. Let C be the scheme obtained by taking $\mathbf{P}^1 \times \mathbf{Z}/n\mathbf{Z}$ and identifying the point 0 in the ith $\mathbf{P}^1$ with the point ∞ in the $(i+1)$st $\mathbf{P}^1$. We call C an *n-gon*. We let C° denote the smooth part of C. The space C° is identified with $\mathbf{G}_m \times \mathbf{Z}/n\mathbf{Z}$, and is thus naturally a group. Furthermore, the group law on C° extends to an action on all of C.

A *generalized elliptic curve* over a scheme S is a proper flat curve $E \to S$ together with a multiplication map $E^\circ \times E \to E$ which gives E° the structure of a group scheme, in such a way that the fibers of E are elliptic curves or polygons (respecting the obvious structure). Here E° denotes the open subset of E where the fibers are smooth. We define $X(S)$ to be the groupoid of generalized elliptic curves E/S whose fibers are all irreducible, i.e., elliptic curves or 1-gons.

Proposition 5. *The functor X is a proper smooth Deligne-Mumford stack over $\mathbf{Z}$.*

Proof. This is proved in [DR] using Artin's representability theorem. I imagine one could give an argument similar to the one we gave for Y. Properness can be seen from the valuative criterion. Let A be a valuation ring with fraction field K and let E/K be an elliptic curve. The semi-stable reduction theorem implies that there is a finite extension K'/K such that the base change E' of E to K' has good or multiplicative reduction — that is, its minimal Weierstrass equation defines a scheme over A' having semi-stable reduction. This shows that the point of $X(K)$ coming from E, when mapping into $X(K')$, comes from an element of $X(A')$. Thus X satisfies the valuative criterion for properness. (Note that this criterion is a little bit different than the one for schemes: we are allowed to extend the field K.) □

We can also compactify the spaces $Y(N)$, $Y_0(N)$ and $Y_1(N)$ over $\mathbf{Z}[1/N]$. To do this, we need to define the notion of a level structure on a generalized elliptic curve. Thus let E/S be a generalized elliptic curve. We let $E[N]$ be the N-torsion of the group E°. The only subtlety concerning level structures is that we require them to be ample, which amounts to them meeting every irreducible component of the fibers of E. Thus a $\Gamma_0(N)$ structure is a subgroup $G \subset E[N]$ which is locally isomorphic to $\mathbf{Z}/N\mathbf{Z}$ and such that G meets each irreducible component of the fibers of E. Note that this imposes a restriction on what the fibers can be: their component group must be a quotient of $\mathbf{Z}/N\mathbf{Z}$. We define $X_0(N)$ to be pairs (E, G) where E is a generalized elliptic curve whose fibers are elliptic curves or N-gons and $G \subset E[N]$ is a $\Gamma_0(N)$ structure, as defined above. The spaces $X(N)$ and $X_1(N)$ are defined similarly.

Proposition 6. *The functors $X(N)$, $X_0(N)$ and $X_1(N)$ are smooth proper schemes over $\mathbf{Z}[1/N]$ (assuming N large enough).*

2.4. The space $X_0(p)$ over $\mathbf{Z}$.

The compactified space $X_0(N)$ — and indeed, even the open curve $Y_0(N)$ — has only been defined over $\mathbf{Z}[1/N]$. It is a bit tricky to formulate what these spaces should be over $\mathbf{Z}$ since one has to specify what it means for a (non étale) group scheme to be cyclic. However, when N is a prime, this is not hard: every group of order p should be considered cyclic! We thus define $Y_0(p)(S)$ (resp. $X_0(p)(S)$) to be the groupoid of pairs (E, G) where E is an elliptic curve (resp. generalized elliptic curve) over S and $G \subset E[p]$ is a finite flat subgroup scheme of order p which is ample (this condition is only relevant for $X_0(p)$). We then have the following result:

Proposition 7. *The functor $X_0(p)$ is a proper flat curve over $\mathbf{Z}$ (for p large).*

We will actually need to extend this a bit for our application. Let N be an integer prime to p. A cyclic group of order Np decomposes canonically as a product of a cyclic group of order N and one of order p. We thus have $X_0(Np) = X(N) \times_X X(p)$ over $\mathbf{Z}[1/Np]$. We take this formula as the *definition* of $X_0(Np)$ over $\mathbf{Z}[1/N]$. That is, $X_0(Np)$ consists of tuples (E, G, H) where E/S is a generalized elliptic curve whose fibers are elliptic curves or pN-gons, $G \subset E[N]$ is a group locally isomorphic to $\mathbf{Z}/NZ$ and $H \subset E[p]$ is a finite flat subgroup such that GH meets every irreducible component of the fibers of E. We then have:

Proposition 8. *The functor $X_0(pN)$ is a proper flat curve over $\mathbf{Z}[1/N]$ (for Np large).*

3. Elliptic curves in characteristic p

We now examine elliptic curves in characteristic p and their moduli. We establish the Eichler-Shimura relation.

3.1. Group schemes.

Let k be a finite field. Let G/k be a finite commutative group scheme. We say that G is *local* if it is connected. There is a canonical exact sequence

$$1 \to G^\circ \to G \to G^{\mathrm{et}} \to 1$$

where G° is local and G^{et} is étale. If the order of G is prime to p then G is automatically étale.

Define a functor $G^\vee$ by $G^\vee(T) = \mathrm{Hom}(G_T, (\mathbf{G}_m)_T)$. Then $G^\vee$ is again a finite group scheme over k. We call $G^\vee$ the *Cartier dual* of G. Cartier duality is an anti-equivalence of categories. The properties "local" and "étale" interact in an interesting manner with Cartier duality. First of all, if G has order prime to p then $G^\vee$ does as well and both are étale. However, the dual of p-power étale group is never étale, and is always connected: for example, $(\mathbf{Z}/p\mathbf{Z})^\vee = \mu_p$. The converse to this is *not* true: for example, if α_p is the kernel of Frobenius on $\mathbf{G}_a$, i.e., $\mathrm{Spec}(k[x]/x^p)$, then α_p is connected and self-dual. We thus find that we can define four classes of groups: étale-étale, étale-local, local-étale and local-local depending on the properties of G and $G^\vee$. Here are examples from the respective classes: $\mathbf{Z}/N\mathbf{Z}$ with N prime to p, $\mathbf{Z}/p\mathbf{Z}$, μ_p and α_p. Every group canonically decomposes as a sum of four groups of these types, so in many circumstances, it suffices to consider groups of only one type. Each type of group forms an abelian category, and with the exception of the étale-étale case, each has only one simple object over $\overline{k}$ (the examples we have listed).

Let G/k be a group scheme. We then have the relative Frobenius map $F : G^F \to G$, which is a map of groups. Here G^F is the Frobenius twist of G; note that $(G^F)^\vee = (G^\vee)^F$. The Cartier dual of the relative Frobenius map is a map $G^\vee \to (G^\vee)^F$. This is not the Frobenius map on $G^\vee$ (it goes in the wrong direction), but a new map, called *Verschebung*, and denoted V. Precisely, this is the Verschebung for $G^\vee$. The Verschebung for G is defined by taking the Cartier dual of the Frobenius map on $G^\vee$; it is a map $V : G \to G^F$. Here are some examples, with $k = \mathbf{F}_p$ (note then that $G^F = G$ for any G). On $\mathbf{Z}/p\mathbf{Z}$ the Frobenius is the identity. On μ_p and α_p the Frobenius is the zero map; these groups are by definition the kernel of Frobenius on $\mathbf{G}_m$ and $\mathbf{G}_a$. Since $\mathbf{Z}/p\mathbf{Z}$ and μ_p are Cartier dual, it follows that $V = 0$ on $\mathbf{Z}/p\mathbf{Z}$ while V is the identity on μ_p. As α_p is self-dual, $V = 0$ on it. Clearly, on the étale-étale groups, F and V are both the identity.

The Frobenius and Vershebung maps in fact allows us to determine which of the four types G is. For instance, G is local if and only if F is nilpotent (meaning $F^n : G^{F^n} \to G$ is zero for $n \gg 0$) and étale if and only if F is an isomorphism. Thus $G^\vee$ is local is and only if V is nilpotent on G and étale if and only if V is an isomorphism on G.

Let A be an abelian variety over k. Then the p-torsion $A[p]$ is an example of a finite group. The Frobenius map on $A[p]$ is nothing other than the Frobenius map on A restricted to $A[p]$. This Frobenius map $F : A^F \to A$ is an isogeny, and thus has a dual $V : A^\vee \to (A^F)^\vee$. We can thus define a map $V : A \to A^F$ by taking the dual to Frobenius on $A^\vee$. The map induced on $A^\vee[p]$ by V is in fact the dual of the Frobenius map on $A[p]$ since Cartier duality and abelian variety duality interact nicely. This is useful when dealing with the torsion groups of abelian varieties, as we will below.

3.2. **Elliptic curves.** Let E be an elliptic curve over k. The group scheme $E[p]$ is finite of order p^2. The Weil pairing

$$E[p] \times E[p] \to \mu_p \subset \mathbf{G}_m$$

implies that $E[p]$ is its own Cartier dual. This implies that there are two possibilities for E: either it is a sum of a local-étale group and an étale-local group each of order p and dual to each other, or else it is local-local. In the first case, $E[p]$ has $\overline{k}$ points while in the second case it does not. We call E *ordinary* in the first case and *supersingular* in the second.

The group scheme $E[p]$ can be exactly determined over $\overline{k}$. In the ordinary case, the étale quotient of $E[p]$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ and so the local part, its dual, must be μ_p. Thus $E[p] = \mu_p \oplus \mathbf{Z}/p\mathbf{Z}$. In the supersingular case, $E[p]$ is local-local, and so it is an extension

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0.$$

There are four such (total spaces of) extensions up to isomorphism: the direct sum (on which $F = 0$ and $V = 0$), the kernel of Frobenius on the Witt scheme W_2 (on which $F = 0$ and $V \neq 0$), the kernel of the square of Frobenius on $\mathbf{G}_a$, namely α_{p^2} (on which $F \neq 0$ and $V = 0$; it is Cariter dual to W_2), and one other (which can be described as the Yoneda sum of the other two non-trivial extensions and on which F and V are each non-zero). The group $E[p]$ is the last one: since F and V on $E[p]$ are the restriction of degree p isogenies on E, their kernels must be order p and therefore cannot be all of $E[p]$; thus F and V are each non-zero on $E[p]$.

3.3. **The space** $X_0(p)$**.** We now consider $X_0(p)$ over k. This is the space of generalized elliptic curves together with a subgroup of order p (satisfying some condition in the generalized case, which we will ignore). Let E/k be an elliptic curve. How many subgroups of order p does it have? If E is ordinary, then it has two: the local one and the étale one. It cannot have more than these two, because they are distinct simple objects. If E is supersingular, then it has at most one subgroup of order p, since over $\overline{k}$ it is a non-trivial extension of two simples.

The above discussion shows that we can define two maps $i_1, i_2 : X \to X_0(p)$, by letting $i_1(E)$ be $(E^F, \ker F)$ and $i_2(E)$ be $(E, \ker V)$. It is clear that each map is injective; in fact, each is a closed immersion. Furthermore, the previous discussion shows that they are jointly surjective. To be clear, say that (E, G) is a point of $X_0(p)$. If E is supersingular, then G must coincide with $\ker V$, since there is only one subgroup of order p, and so $(E, G) = i_2(E)$. If E is ordinary and G is étale, then $(E, G) = i_2(E)$, while if E is ordinary and G is local then $(E, G) = i_1(E')$, where E' is such that $(E')^F = E$. Note that if E is ordinary then $i_1(E)$ and $i_2(E)$ are unequal, since in $i_1(E)$ the level structure is étale while in $i_2(E)$ it is local. If E is supersingular so is E^F and thus $i_1(E) = i_2(E^F)$. We therefore find that $X_0(p)$ can be described as two copies of X glued along their supersingular loci identified via $(-)^F$ (at the supersingular points there are nodal singularities). The same discussion applies to $X_0(Np)$: it is two copies of $X_0(N)$ glued along supersingular points by $(-)^F$.

As a side comment, we note that this result shows that the genus of $X_0(p)$ is one less than the number of supersingular curves.

3.4. **Correspondences.** We quickly review the basics of correspondences on curves. Let X be a regular curve over a field k. A *correspondence* on X is a pair $f = (f_1, f_2)$ where f_1 and f_2 are maps from some reduced curve C (the total space) to X such that f_1 is finite. Given two correspondences f and f' with total spaces C and C' we define their *sum*, denoted $f + f'$, to be the natural correspondence with total space $C \amalg C'$. Given a correspondence f with total space C, we get a natural correspondence $\widetilde{f}$ with total space $\widetilde{C}$, the normalization of $\widetilde{C}$, coming from the finite map $\widetilde{C} \to C$. We consider f and $\widetilde{f}$ to be equivalent; note that $\widetilde{C}$ is always regular.

Let $f : X \to Y$ be a map of regular curves over k. We then have a map $f_* : \mathrm{Div}(X) \to \mathrm{Div}(Y)$. This map is characterized by the following two properties: $\deg f_*(D) = \deg D$ and $\sup f_*(D) = f_*(\sup(D))$. If k is algebraically closed, so that divisors correspond to points, then $f_*([x])$ is just $[f(x)]$. Now assume that f is a finite map. Then we have a map $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$, (almost) characterized by two properties: $\deg(f^*(D)) = \deg(f)\deg(D)$ and $\sup(f^*(D)) = f^{-1}(\sup(D))$. (Here f^{-1} is just taken at the topological level.) If k is algebraically closed, then for $y \in Y(k)$ we have

$$f^*([y]) = \sum_{x \in X(k)} \mathrm{len}_x(X_y)[x]$$

where here $X_y = X \times_Y y$. Note that X_y is a finite subscheme of X, but may not be reduced.

Now let $f = (f_1, f_2)$ be a correspondence of X with total space C. We define a map $f_* : \mathrm{Div}(X) \to \mathrm{Div}(X)$ by $(f_2)_* f_1^*$. (If C is not regular, use $\widetilde{f}$.) This map carries principal divisors into principal divisors and therefore induces a map $f_* : \mathrm{Pic}(X) \to \mathrm{Pic}(X)$, and a map $f_* : \mathrm{Jac}(X) \to \mathrm{Jac}(X)$. (We have only defined these maps on field points, but they exist as maps of schemes.) Let $g : X \to X$ be a finite map of curves. The $f = (\mathrm{id}, g)$ and $f' = (g, \mathrm{id})$ are correspondences of X. The map f_* of $\mathrm{Jac}(X)$ coincides with the map g_*, while the map $(f')_*$ is the dual to g_*.

3.5. **The Eichler-Shimura identity.** There are two natural maps $p_1, p_2 : X_0(Np) \to X_0(N)$, taking (E, G) to E or E/G, where here G is a subgroup of order p and the level N structure is implicit. These two maps define a correspondence from $X_0(N)$ to itself over $\mathbf{Z}[1/N]$, called the *Hecke correspondence*, and denoted T_p. The Eichler–Shimura identity computes this correspondence in characteristic p:

Proposition 9. *We have $T_p = (F, 1) + (1, F)$ as correspondences on $X_0(N)$. Thus $(T_p)_* = F + V$ as endomorphisms of $J_0(N)$. (All of this takes place over $\mathbf{F}_p$.)*

Proof. Recall that we have defined maps $i_1, i_2 : X_0(N) \to X_0(pN)$ and that the map

$$i_1 \amalg i_2 : X_0(N) \amalg X_0(N) \to X_0(pN)$$

is the normalization of $X_0(pN)$. Thus, since we are allowed to replace the total space of a correspondence with its normalization, the correspondence T_p is just the sum of the correspondences $(p_1 \circ i_1, p_2 \circ i_1)$ and $(p_1 \circ i_2, p_2 \circ i_2)$, each with total space $X_0(N)$. Some short computations show that

$$p_1 \circ i_1 = F, \qquad p_1 \circ i_2 = \mathrm{id}, \qquad p_2 \circ i_1 = \mathrm{id}, \qquad p_2 \circ i_2 = F.$$

Thus $T_p = (F, 1) + (1, F)$, as claimed. The correspondence $(1, F)$ induces the map F on the Jacobian while the correspondence $(F, 1)$ induces the dual map V. This completes the proof. □

4. Applications to modular Galois representations

We have defined correspondences T_p on $X_0(N)$ for all primes p not dividing N. These correspondences induce endomorphisms of the abelian variety $J_0(N)$ and generate a commutative subalgebra $\mathbf{T}$ of $\mathrm{End}(J_0(N))$ which is finite over $\mathbf{Z}$. Let f be a cuspidal weight 2 newform of level N. Let $K_f \subset \mathbf{C}$ be the coefficient field of f. The action of $\mathbf{T}$ on f determines a homomorphism $\lambda : \mathbf{T} \to K_f$. Let $\mathfrak{a}$ be the kernel of λ, an ideal of $\mathbf{T}$, and let A_f be the quotient of $J_0(N)$ by $\mathfrak{a}J_0(N)$. We wish to understand A_f as best we can. We begin by computing its dimension:

Proposition 10. *The dimension of A_f is the degree of K_f.*

Proof. The dimension of A_f is the dimension of the space of global 1-forms on it. Global 1-forms on A_f correspond to global 1-forms on $J_0(N)$ which are killed by $\mathfrak{a}$. The latter space is precisely the space of modular forms with eigenvalue some $\mathrm{Aut}(\mathbf{C})$ conjugate of λ. Thus the dimension of this space is the number of conjugates of λ, which is equal to the degree of K_f. □

The abelian variety A_f actually has an action of K_f by isogenies, that is, there is a canonical map $K_f \to \mathrm{End}(A_f) \otimes \mathbf{Q}$. We can therefore regard the Tate module $T_\ell(A_f)$ as a two dimensional vector space over $K_f \otimes \mathbf{Q}_\ell$. The following proposition (combined with Faltings' theorem on isogenies of abelian varieties) determines A_f up to isogeny.

Proposition 11. *Let p be a prime not dividing N. Then A_f has good reduction at p and the trace of Frob_p on any Tate module $T_\ell A_f$ with $\ell \neq p$ is equal to a_p, the eigenvalue of T_p on f.*

Proof. We consider only the case $K = \mathbf{Q}$ for simplicity. The abelian variety $J_0(N)$ has good reduction at p since $X_0(N)$ is a smooth proper curve over $\mathbf{Z}[1/N]$, from which it follows that the quotient A_f does as well. Working modulo p, we have $T_p = F + V$ on $J_0(N)$, which implies the same on the quotient A_f. On this quotient, T_p acts by multiplication by the integer $a_p = \lambda(T_p)$. We thus find that $F^2 - a_pF + p = 0$ on A_f, which shows that a_p is the trace of F on $T_\ell A_f$. (There is a slight gap in this proof. In this section, we have simply stated that $\mathbf{T}$ acts on $J_0(N)$ without explaining how. To prove the Eichler–Shimura correspondence, we used a precise definition of the action of T_p on $J_0(N)$, and equated it with the action of the correspondence gotten by passing to the normalization of the total space. One must show that these two actions of T_p on $J_0(N)$ coincide to have a complete proof. We leave these details to the reader.) □

We now turn to ordinarity. We say that f is *ordinary* at p if its T_p eigenvalue is a p-adic unit. We say that a Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_p)$ is *ordinary* at p if on inertia it is an extension of 1 by χ_p. Furthermore, we say that ρ is *ordinary crystalline* if this extension class is represented by a unit in Kummer theory. We now have the following result:

Proposition 12. *If f is ordinary at $p \nmid N$ then T_pA_f is ordinary crystalline.*

Proof. We again assume $K = \mathbf{Q}$. As in the previous proposition, A_f has good reduction at p and $F^2 - a_pF + p$ holds as an endomorphism of $\overline{A}_f$, the reduction of A_f modulo p. Assume for the moment that $\overline{A}_f$ were supersingular. Then we would have $F^2 = 0$ on $\overline{A}_f[p]$ (since $F = V$ in the supersingular case and $FV = p$), and so a_pF would be zero on $\overline{A}_f[p]$. Since a_p is a p-adic unit, and integer, this would imply that F vanishes on $\overline{A}_f[p]$. This is impossible since the kernel of F has order p. Thus $\overline{A}_f$ is ordinary. The result now follows from the following proposition. □

Proposition 13. *Let $E/\mathbf{Z}_p$ be an elliptic curve with ordinary reduction. Then T_pE is crystalline ordinary.*

Proof. It is not difficult to see that $E[p]$ is an extension of $\mathbf{Z}/p$ by μ_p over $\mathbf{Z}_p^{\mathrm{un}}$. In fact, we have an extension

$$0 \to \mu_{p^n} \to E[p^n] \to \mathbf{Z}/p^n \to 0$$

over $\mathbf{Z}_p^{\mathrm{un}}$. This shows that T_pE is an extension of 1 by χ_p, and thus ordinary. To see that it is crystalline, note that the above extension, regarded simply as an extension of sheaves of groups on the fppf site of $\mathbf{Z}_p^{\mathrm{un}}$, defines an element of $H^1_f(\mathbf{Z}_p^{\mathrm{un}}, \mu_{p^n})$. Here H_f is cohomology in the fppf site. We can compute this group via Kummer theory. Since $H^1_f(\mathbf{Z}_p^{\mathrm{un}}, \mathbf{G}_m) = 0$, we have

$$H^1_f(\mathbf{Z}_p^{\mathrm{un}}, \mu_{p^n}) = (\mathbf{Z}_p^{\mathrm{un}})^\times / ((\mathbf{Z}_p^{\mathrm{un}})^\times)^{p^n}.$$

This isomorphism is compatible with Kummer theory over $\mathbf{Q}_p^{\mathrm{un}}$, which shows that the extension class for T_pE is represented by a p-adic unit. □

5. Galois representations coming from Hilbert modular forms

Let f be a Hilbert cuspidal eigenform of parallel weight 2 for a totally real field F. We know that one can associate a Galois representation to f, and that its local properties are determined by those of f. Can this be proved in the same manner as the classical modular case?

If F has odd degree over $\mathbf{Q}$ or f is square-integrable at some finite place, then the Jacquet-Langlands correspondence shows that f can be transferred to a Shimura curve X. The curve part is the key point. One can then construct a quotient of the Jacobian of X, as we did for the Jacobian of $J_0(N)$, and obtain an abelian variety A_f. Everything goes through as before. (Some points may even be more simple, as Shimura curves are naturally compact — that is, there is no need to add cusps.)

When F has even degree over $\mathbf{Q}$ and f is principal series at all finite places, this procedure does not work. In fact, it is not known if the Galois representation associated to f appears as the Tate modular of an abelian variety, though I imagine this is expected. However, the Galois representation has been constructed and its local properties established, by more indirect means. If f is ordinary, then it can be put into a p-adic family. Other members of this family have Galois representations which are easier to construct, and the representation for f can be constructed as a limit. If f is not ordinary, this approach is not feasible. However, one can find enough congruences between f and forms for which the Galois representation is known to exist to construct the Galois representation of f. This was Richard Taylor's thesis.

References

[KM] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves.*

[DR] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques.*