Fine structures of moduli spaces in positive characteristics: Hecke symmetries and Oort foliation

§1. Moduli of Elliptic curves

§1.1. **Def**. An elliptic curve over $\mathbb{C}$ is the quotient of a one dimensional vector space V over $\mathbb{C}$ by a lattice Γ in V.

Concretely, we can take $V = \mathbb{C}$, and a lattice Γ in $\mathbb{C}$ has the form

$$\Gamma = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$$

$\omega_1, \omega_2 \in \mathbb{C}$, linearly independent over $\mathbb{R}$.

The quotient $E(\Gamma) = \mathbb{C}/\Gamma$ of $\mathbb{C}$ by a lattice Γ is a compact one-dimensional complex manifold, and is also an abelian group.

§1.2. The Weistrass $\wp$-function

$$\wp_\Gamma(u) = \frac{1}{u^2} + \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \left[\frac{1}{(u - m\omega_1 - n\omega_2)^2} - \frac{1}{(m\omega_1 + n\omega_2)^2}\right]$$

is a meromorphic function on $E(\Gamma)$.

Define complex numbers $g_2(\Gamma), g_3(\Gamma)$ by Eisenstein series

$$g_2(\Gamma) = 60 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^4}$$

$$g_3(\Gamma) = 140 \sum_{\substack{m,n\in\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m\omega_1 + n\omega_2)^6}$$

Let $x_\Gamma = \wp_\Gamma(u)$, $y_\Gamma = \frac{d}{du}\wp_\Gamma(u)$. Then the two meromorphic functions x_Γ, y_Γ on $E(\Gamma)$ satisfy the polynomial equation

$$y_\Gamma^2 = 4x_\Gamma^3 - g_2(\Gamma)\, x_\Gamma - g_3(\Gamma)$$

This equation tells us that the pair (x_Γ, y_Γ) defines a map $\imath$ from the elliptic curve $E(\Gamma)$ to *algebraic curve* in $\mathbb{P}^2$ cut out by the cubic homogeneous equation

$$Y^2 Z = 4\, X^3 - g_2(\Gamma)\, X Z^2 - g_3(\Gamma) Z^3\,;$$

the map $\imath$ turns out to be an isomorphism. (The affine equation

$$y^2 = 4\, x^3 - g_2(\Gamma)\, x - g_3(\Gamma)$$

with $x = \frac{X}{Z}, y = \frac{Y}{Z}$ describes $E(\Gamma) \smallsetminus \{0\}$.)

§1.3 Moduli of elliptic curves

Two elliptic curves E_1, E_2 attached to lattices Γ_1, Γ_2 in $\mathbb{C}$ are isomorphic iff they are homothetic, i.e.

$$\exists\, \lambda \in \mathbb{C}^\times \text{ s.t. } \lambda \cdot \Gamma_1 = \Gamma_2$$

To parametrize lattices, for $\Gamma = \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2$, write

$$(\omega_1, \omega_2) = \lambda(\tau, 1), \tau \in \mathbb{C} - \mathbb{R} =: X^\pm$$

The group $\mathrm{GL}_2(\mathbb{Z})$ operates on the right of $X^\pm$ by

$$(\tau, 1) \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = (c\tau + d) \cdot (\frac{a\tau + b}{c\tau + d}, 1)$$

$a, b, c, d \in \mathbb{Z}$, $ad - bd = \pm 1$.

Elliptic curves corresponding to lattices $\mathbb{Z}\,\tau_i + \mathbb{Z}$, $i = 1, 2$ are isomorphic iff $\tau_1 \cdot \gamma = \tau_2$ for some $\gamma \in \mathrm{GL}_2(\mathbb{Z})$.

Algebraically, one can attach to every elliptic curve E a complex number $j(E)$, such that E_1 and E_2 are isomorphic iff $j(E_1) = j(E_2)$. For an elliptic curve E given by a Weistrass equation

$$y^2 = 4\,x^3 - g_2\,x - g_3, \;\; \Delta := g_2^3 - 27g_3^2 \neq 0,$$

the j-invariant is $\; j(E) = 1728\,\dfrac{g_2^3}{g_2^3 - 27g_3^2}$

For an elliptic curve defined by

$$y^2 = x(1-x)(\lambda - x), \;\; \lambda \neq 0, 1,$$

the j-invariant is $\; j(\lambda) = 2^8\,\frac{(1-\lambda(1-\lambda))^3}{\lambda^2\,(1-\lambda)^2}$

§1.4 Hecke symmetries

(1) A Hecke correspondence on $X^{\pm}/\operatorname{GL}_2(\mathbb{Z})$ is defined by a diagram

$$X^{\pm}/\operatorname{GL}_2(\mathbb{Z}) \xleftarrow{\pi} X^{\pm} \xrightarrow{\gamma} X^{\pm}/\operatorname{GL}_2(\mathbb{Z})$$

with $\gamma \in \operatorname{GL}_2(\mathbb{Z})$.

(2) The Hecke orbit of an element $\pi(x)$ of $X^{\pm}/\operatorname{GL}_2(\mathbb{Z})$ is the countable subset $\pi(x \cdot \operatorname{GL}_2(\mathbb{Q}))$ of $X^{\pm}/GL_2(\mathbb{Z})$.

(3) Geometrically, the Hecke orbit of the modular point $[E]$ is the subset consisting of all $[E_1]$ such that there exists a surjective holomorphic homomorphism from $E \longrightarrow E_1$ (called an *isogeny*.)

(4) Another way to look at Hecke orbits:

Let $G(n)$ be the set of all 2×2 matrices in $\mathrm{GL}_2(\mathbb{Z})$ which are congruent to Id_2 modulo n. We have a projective system

$$\widetilde{X} := \left(X^{\pm}/G(n)\right)_{n \in \mathbb{N}_{\geq 1}}$$

of modular curves, with the indexing set $\mathbb{N}_{\geq 1}$ ordered by by divisibility. We have a large group $\mathrm{GL}_2(\mathbb{A}_f)$ operating on the tower $\widetilde{X}$, and $\widetilde{X}/\operatorname{GL}_2(\widehat{\mathbb{Z}})$ is isomorphic to the j-line $X/\operatorname{GL}_2(\mathbb{Z})$. (Here $\widehat{\mathbb{Z}} := \varprojlim(\mathbb{Z}/n\mathbb{Z})$, $\mathbb{A}_f = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$.)

The Hecke correspondences on $\widetilde{X}/\operatorname{GL}^2(\widehat{\mathbb{Z}})$ are induced by the action of $\mathrm{GL}_2(\mathbb{A}_f)$ on $\widetilde{X}$.

§2. Moduli of abelian varieties

§2.1. **Def**. A *complex torus* is a compact complex group variety of the form V/Γ, where V is a finite dimensional complex vector space and Γ is a cocompact discrete subgroup of Γ; $\mathrm{rank}(\Gamma) = 2\dim_{\mathbb{C}}(V)$.

Def. A complex torus V/Γ is an *abelian variety* if it can be holomorphically embedded in $\mathbb{P}^N$; this happens iff there exists a definite hermitian form on V whose imaginary part induces a $\mathbb{Z}$-valued symplectic form on Γ. Such a form, called a *polarization*, is *principal* iff the discriminant of the symplectic form is 1.

§2.2. A lattice in $\mathbb{C}^g$ which admits a principal polarization can be written as

$$C \cdot (\Omega \cdot \mathbb{Z}^g + \mathbb{Z}^g)$$

for some $C \in \mathrm{GL}_g(\mathbb{C})$ and some symmetric $\Omega \in \mathrm{M_g}(\mathbb{C})$ with definite imaginary part. The set $X_g^{\pm}$ of all such period matrices Ω's is called the Siegel upper-and-lower half-space.

The group $\mathrm{GSp}_{2g}(\mathbb{Q})$ operates on the right of $X_g^{\pm}$ by:

$$\Omega \cdot \begin{pmatrix} A & C \\ B & D \end{pmatrix} = (\Omega\, C + D)^{-1}\, (\Omega\, A + B)$$

Here GSp_{2g} denotes the group of $2g \times 2g$ matrices which preserve the standard symplectic pairing up to scalars.

§2.3. The isomorphism classes of g-dimensional abelian principally polarized abelian varieties is parametrized by

$$X_g^{\pm} / \operatorname{GSp}_{2g}(\mathbb{Z})$$

Just as in the elliptic curve case, we have a projective system

$$\tilde{X} = \left(X_g^{\pm}/G(n)\right)_{n \in \mathbb{N}_{\geq 1}}$$

Here $G(n)$ consists of elements of $\operatorname{GSp}_{2g}(\mathbb{Z})$ which are congruent to Id_{2g} modulo n. Again the group $\operatorname{GSp}_{2g}(\mathbb{A}_f)$ operates on the tower $\tilde{X}$. This action induces *Hecke correspondences* on $X_g^{\pm} / \operatorname{GSp}_{2g}(\mathbb{Z})$. The Hecke orbit of a point $[A]$ is the countable subset consisting of all principally polarized abelian varieties which are *symplectically isogenous* to A.

$\S$3. Modular varieties with Hecke symmetries

$\S$3.1. Generalizing $\S$2, consider (a special class of) Shimura varieties $\left(\widetilde{X} = (X_n)_{n\in\mathbb{N}_{\geq 1}}, G\right)$, where

G is a connected reductive group over $\mathbb{Q}$,

$\widetilde{X}$ is a moduli space of abelian varieties with prescribed symmetries (of a fixed type)

The group G is the symmetry group of the "prescribed symmetries", giving the "type" of the prescribed symmetries.

§3.2. Hecke symmetries on Shimura varieties

The group $G(\mathbb{A}_f)$ operates on the tower $\widetilde{X}$:

$$\curvearrowleft G(\mathbb{A}_f)$$
$$\widetilde{X} = (\cdots \to \underbrace{X_n \to \cdots X_0 = X}_{G(\mathbb{Z}/n\mathbb{Z})})$$

On the "bottom level" $X = X_0$, the symmetries from $G(\mathbb{A}_f)$ induces *Hecke correspondences*; these correspondences are parametrized by $G(\widehat{\mathbb{Z}})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$.

Remark: For a fixed finite level $X_n \to X_0$, the symmetry subgroup preserving the covering map is $G(\mathbb{Z}/n\mathbb{Z})$.

§3.3. Modular varieties in characteristic p

Abelian varieties can be defined in purely algebraic terms (Weil), so are the modular varieties classifying them. In particular one can define these modular varieties over a field k of characteristic $p > 0$.

In the case of elliptic curves, if $p \neq 2, 3$, then every elliptic curve is defined by a Weistrass equation

$$y^2 = 4\,x^3 - g_2\,x - g_3, \;\; \Delta := g_2^3 - 27g_3^2 \neq 0,$$

the moduli is given by the j-invariant; the j-invariant is $j(E) = 1728\,\dfrac{g_2^3}{g_2^3 - 27g_3^2}$

The diagram for Hecke symmetries in characteristic p is

$$\curvearrowleft G(\mathbb{A}_f^{(p)})$$

$$\widetilde{X} = (\cdots \to \underbrace{X_n \to \cdots X_0 = X}_{G(\mathbb{Z}/n\mathbb{Z})})$$

The indices n are relatively prime to p, and the Hecke correspondences come from prime-to-p isogenies between abelian varieties.

§4. The Hecke orbit problem

Problem Characterize the Zariski closure of Hecke orbits in a modular variety X.

– The closed subsets for the Zariski topology of X consists of algebraic subvarieties of X.

– Each Hecke orbit is a countable subset of X.

§5. Solution in characteristic 0.

Prop In characteristic 0, every Hecke orbit is dense in the modular variety X.

Proof in the Siegel case: May assume that the base field is $\mathbb{C}$.

Claim: Every Hecke orbit is dense for the finer metric topology on X.

The Hecke symmetries come from the action of the group $\mathrm{GSp}_{2g}(\mathbb{Q})$ on $X_g^{\pm}$. Conclude by

- $\mathrm{GSp}_{2g}(\mathbb{Q})$ is dense in $\mathrm{GSp}_{2g}(\mathbb{R})$
- $\mathrm{GSp}_{2g}(\mathbb{R})$ operates transitively on $X_g^{\pm}$

§6. Fine structures in char. p

The base field k has char. p from now on.

§6.1. Elliptic curves have *Hasse invariant*; explicitly, for

$$E : y^2 = x(1-x)(\lambda - x),\ p \neq 2$$

$$j(\lambda) = 2^8\,\frac{(1-\lambda(1-\lambda))^3}{\lambda^2\,(1-\lambda)^2}$$, then

$$A(\lambda) = (-1)^r \sum_{i=0}^{r} \binom{r}{i}^2 \lambda^i\,, \quad r = \frac{1}{2}(p-1)$$

gives the Hasse invariant of E.

Def. The elliptic curve E is *supersingular* if its Hasse invariant vanishes, otherwise E is *ordinary*; E is ordinary iff E has p points which are killed by p.

The (finite) set of supersingular elliptic curves is stable Hecke correspondences. So the Hecke orbit of $[E]$ is dense iff E is ordinary.

§6.2 From now on $X = \mathcal{A}_g$ denotes the Siegel modular variety in char. p; it classifies g-dimensional principally polarized abelian varieties.

Source of fine structure on X (or $\widetilde{X}$): Every family of abelian varieties $A \to S$ gives rise to a *Barsotti-Tate group*

$$A[p^\infty]_S := \varinjlim_n A[p^n]_S \, ,$$

an inductive system of finite locally free group schemes $A[p^n] := \mathrm{Ker}([p^n] : A \to A)$; the *height* of $A[p^\infty]$ is $2g = 2\dim(A/S)$. The Frobenius $F_A : A \to A^{(p)}$ and Verschiebung $V_A : A^{(p)} \to A$ pass to $A[p^\infty]$.

§6.3. The slope stratification

The slopes of a Barsotti-Tate group $A[p^\infty]$ over a field $k/\mathbb{F}_p$ is a sequence $2g$ of rational numbers

$$\lambda = (\lambda_j)\,, \quad 0 \leq \lambda_1 \leq \cdots \leq \lambda_{2g} \leq 1,$$

such that $\lambda_j + \lambda_{2g+1-j} = 1$. The denominator of each λ_j divides its multiplicity. The slopes are defined using divisibility properties of iterations of the Frobenius.

The slope sequence, a discrete invariant, defines a *stratification*

$$X = \coprod_\lambda X_\lambda$$

The Zariski closure of each stratum X_α is equal to a union of (smaller) strata.

(a) $\mathcal{A}_1$ is the union of two strata.

(b) The open dense stratum of $\mathcal{A}_g$ corresponds to *ordinary* abelian varieties, with slopes $(0, \ldots, 0, 1, \ldots, 1)$. The minimal stratum of $\mathcal{A}_g$ corresponds to *supersingular* abelian varieties, with slopes $(\frac{1}{2}, \ldots, \frac{1}{2})$, and has dimension $\lfloor g^2/4 \rfloor$ (Li-Oort).

§6.4. Ekedahl–Oort stratification

The isomorphism type $A[p]$ of the p-torsion subgroup of a principally polarized abelian variety A, together with the *Weil pairing* on it, turns out to be a discrete invariant and gives rise to a stratification of X.

§7. Foliation and a conjecture of Oort

§7.1 Replacing the discrete invariants (such as slopes) of the Barsotti-Tate groups by their **isomorphism types**, one gets a much finer decomposition of the modular variety $X = \mathcal{A}_g$, introduced by Oort. One can also define the foliation structure for more general modular varieties.

Def. The locus of X with a fixed isomorphism type of $(A[p^\infty] + \text{polarization})$ is called a *leaf*.

- Each leaf is a locally closed subset of X, smooth over $\overline{\mathbb{F}_p}$.
- (With a one exception) there are infinitely many leaves on M. For instance the leaf containing a supersingular point in $\mathcal{A}_g$ is *finite*.
- The dense open slope stratum of X is a leaf. For instance if there exists an ordinary fiber A_x, then the ordinary locus in X is a leaf.

§7.2. Characterize leaves by Hecke symmetries

Clearly the foliation structure of M is stable under all prime-to-p Hecke correspondences. A recent conjecture of Oort predicts that the leaves are determined by the Hecke symmetries.

Conj. (HO). The foliation structure is characterized by the prime-to-p Hecke symmetries: For each point $x \in X$, the prim-to-p Hecke orbit of x is dense in the leaf containing x.

Note: Each Hecke orbit is a countable subset of X.

§8. Hecke orbits of ordinary points

The first piece of evidence supporting Conj. (HO) is the case of the dense open leaf in X.

Thm. Conj. (HO) holds for the ordinary locus of $\mathcal{A}_g$. Every ordinary symplectic prime-to-p isogeny class is dense in $\mathcal{A}_g$.

Rmk: The same holds for modular varieties of PEL-type C (CLC). But the density of Hecke orbits on the dense open leaf has not been established for all PEL-type modular varieties.

§9. Canonical coordinates for leaves.

Thm. (Serre-Tate) The formal completion of any closed point of the ordinary locus of X has a natural structure as a formal torus over the base field k.

This classical result generalizes to every leaf in X:

Thm. The formal completion of every leaf is the maximal member of a finite projective system $(Y_\alpha)_{\alpha\in I}$ of smooth formal varieties, indexed by a finite partially ordered set I. The poset I is the set of all segments of a linearly ordered finite set $S = \{1, \dots, n\}$. Each map

$$\pi_{i,j} : X_{[a,b]} \to X_{[a+1,b]} \times_{X_{[a+1,b-1]}} X_{[a,b-1]}$$

has a natural structure as a torsor for a p-divisible formal group over k.

§10. Known cases of Conj. (HO):

§10.1. Examples

(1) $\mathcal{A}_g$ for $g = 1, 2, 3$ (with Oort)

(2) The HB varieties (work in progress with C.-F. Yu). Write $F \otimes_{\mathbb{Q}} \mathbb{Q}_p = \oplus_i F_{\mathfrak{p}_i}$, $A_x[p^\infty] = \oplus A_x[\mathfrak{p}_i^\infty] =: B_i$. Each B_i has two slopes $\frac{r_i}{g_i}, \frac{s_i}{g_i}$ with multiplicity $g_i = [F_{\mathfrak{p}_i} : \mathbb{Q}_p]$. Then the dimension of the leaf passing through x is $\sum_i |r_i - s_i|$.

(3) The Hecke orbit of a "very symmetric" ordinary point of a modular variety of PEL-type is dense.

(4) PEL-type modular varieties attached to a quasi-split $U(n, 1)$.

§10.2. Local Hecke orbits

The following result is a local version of the Hecke orbit problem.

Thm. Let k be an algebraically field of char. $p > 0$. Let X be a finite dimensional p-divisible smooth formal group over k. Let $E = \mathrm{End}(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Let G be a connected linear algebraic group over $\mathbb{Q}_p$. Let $\rho : G \to \underline{E}^\times$ be a homomorphism of algebraic groups over $\mathbb{Q}_p$ such that the trivial representation $\mathbf{1}_G$ is not a subquotient of (ρ, E). Suppose that Z is a reduced and irreducible closed formal subscheme of the p-divisible formal group X which is closed under the action of an open subgroup U of $G(\mathbb{Z}_p)$. Then Z is stable under the group law of X and hence is a p-divisible smooth formal subgroup of X.

Rem. It is helpful to consider first the case when X is a formal torus and G is $\widehat{\mathbb{G}_m}$. We sketch a proof.

Prop. Let X be a finite dimensional p-divisible smooth formal group over p. Let k be an algebraically closed field. Let R be a topologically finitely generated complete local domain over k. In other words, R is isomorphic to a quotient $k[[x_1, \ldots, x_n]]/P$, where P is a prime ideal of the power series ring $k[[x_1, \ldots, x_n]]$. Then there exists an injective local homomorphism $\iota : R \hookrightarrow k[[y_1, \ldots, y_d]]$ of complete local k-algebras, where $d = \dim(R)$.

Prop. Let k be a field of characteristic $p > 0$. Let $q = p^r$ be a positive power of p, $r \in \mathbb{N}_{>0}$. Let $F(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$ be a polynomial with coefficients in k. Suppose that we are given elements $c_1, \ldots, c_m$ in k and a natural number $n_0 \in \mathbb{N}$ such that $F(c_1^{q^n}, \ldots, c_m^{q^n}) = 0$ in k for all $n \geq n_0$, $n \in \mathbb{N}$. Then $F(c_1^{q^n}, \ldots, c_m^{q^n}) = 0$ for all $n \in \mathbb{N}$; in particular $F(c_1, \ldots, c_m) = 0$.

Prop. Let k be a field of characteristic $p > 0$. Let $f(\mathbf{u},\mathbf{v}) \in k[[\mathbf{u},\mathbf{v}]]$, $\mathbf{u} = (u_1,\ldots,u_a)$, $\mathbf{v} = (v_1,\ldots,v_b)$, be a formal power series in the variables $u_1,\ldots,u_a,v_1,\ldots,v_b$ with coefficients in k. Let $\mathbf{x} = (x_1,\ldots,x_m)$, $\mathbf{y} = (y_1,\ldots,y_m)$ be two new sets of variables. Let $\mathbf{g}(\mathbf{x}) = (g_1(\mathbf{x}),\ldots,g_a(\mathbf{x}))$ be an a-tuple of power series without the constant term: $g_i(\mathbf{x}) \in (\mathbf{x})k[[\mathbf{x}]]$ for $i = 1,\ldots,a$. Let $\mathbf{h}(\mathbf{y}) = (h_1(\mathbf{y}),\ldots,h_b(\mathbf{y}))$, with $h_j(\mathbf{y}) \in (\mathbf{y})k[[\mathbf{y}]]$ for $j = 1,\ldots,b$. Let $q = p^r$ be a positive power of p. Let $n_0 \in \mathbb{N}$ be a natural number, and let b' be a natural number with $1 \leq b' \leq b$. Let $(d_n)_{n\in\mathbb{N}}$ be a sequence of natural numbers such that $\lim_{n\to\infty} \frac{q^n}{d_n} = 0$. Suppose we are given power series $R_{j,n}(\mathbf{v}) \in k[[\mathbf{v}]]$, $j = 1,\ldots,b$, $n \geq n_0$, such that $R_{j,n}(\mathbf{v}) \equiv 0 \mod (\mathbf{v})^{d_n}$ for all $j = 1,\ldots,b$ and all $n \geq n_0$.

For each $n \geq n_0$, let $\phi_{j,n}(\mathbf{v}) = v_j^{q^n} + R_{j,n}(\mathbf{v})$ if $1 \leq j \leq b'$, and let $\phi_{j,n}(\mathbf{v}) = R_{j,n}(\mathbf{v})$ if $b' + 1 \leq j \leq b$. Let $\Phi_n(\mathbf{v}) = (\phi_{1,n}(\mathbf{v}), \ldots, \phi_{b,n}(\mathbf{v}))$ for each $n \geq n_0$. Assume that $0 = f(\mathbf{g}(\mathbf{x}), \Phi_n(\mathbf{h}(\mathbf{x}))) = f\left(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), \phi_{1,n}(h(\mathbf{x})), \ldots, \phi_{b,n}(h(\mathbf{x}))\right)$ in $k[[\mathbf{x}]]$, for all $n \geq n_0$. Then $0 = f(g_1(\mathbf{x}), \ldots, g_a(\mathbf{x}), h_1(\mathbf{y}), \ldots, h_{b'}(\mathbf{y}), 0, \ldots, 0)$ in $k[[\mathbf{x}, \mathbf{y}]]$.