1 Analytic Definitions

A *lattice* in a $\mathbb{C}$-vector space V is the $\mathbb{Z}$-submodule generated by an $\mathbb{R}$-basis of V, i.e. $\mathbb{R}\otimes_{\mathbb{Z}}\Lambda\cong V$. (We'll use notation like $\Lambda_{\mathbb{R}}$ to denote tensor products). The quotient V/Λ is a compact connected complex manifold with distinguished point $0\in V/\Lambda$. In fact V/Λ is a Lie group.

Conversely, given a complex manifold M with distinguished point $0\in M$. Suppose the exponential map $\mathrm{Tgt}_0(M)\to M$ realizes M as a quotient of $\mathrm{Tgt}_0(M)$ by a lattice. Then, we can recover the complex torus V/Λ (this is called canonical uniformization).

Here is a nice property (which we don't prove).

Proposition 1.1. For complex tori $M_1\cong V_1/\Lambda_1, M_2\cong V_2/\Lambda_2$. A $\mathbb{C}$-linear map $\alpha: V_1\to V_2$ such that $\alpha(\Lambda_1)\subseteq\Lambda_2$ defines a holomorphic map $\alpha: M_1\to M_2$ sending 0 to 0. Conversely, a holomorphic map $M_1\to M_2$ sending 0 to 0 is necessarily a $\mathbb{C}$-linear map α of the above form.

Thus, any map $\alpha: V_1/\Lambda_1\to V_2/\Lambda_2$ as defined above is called a *homomorphism* (of complex tori). Denote by $\mathrm{Hom}(M,N)$ the group of homomorphisms $M\to N$ of complex torii. We also put $\mathrm{Hom}^0(M,N)=\mathrm{Hom}(M,N)\otimes_{\mathbb{Z}}\mathbb{Q}$.

Now, given two complex tori M,N. An *isogeny* $\lambda: M\to N$ is a surjective homomorphism with finite kernel. Isogeny implies same dimension. An isogeny corresponds to an invertible element of $\mathrm{Hom}^0(M,N)$.

A *Riemann pair* (Λ,J) is a free $\mathbb{Z}$-module Λ of finite rank and a complex structure $J:\Lambda_{\mathbb{R}}\to\Lambda_{\mathbb{R}}$. What this means is $J:\Lambda_{\mathbb{R}}\to\Lambda_{\mathbb{R}}$ is $\mathbb{R}$-linear and $J\circ J=-1$. So this makes $\Lambda_{\mathbb{R}}$ a $\mathbb{C}$-vector space. A *homomorphism of Riemann pairs* $(\Lambda,J)\xrightarrow{\alpha}(\Lambda',J')$ is a $\mathbb{Z}$-linear map $\Lambda\to\Lambda'$ such that $1\otimes\alpha:\Lambda_{\mathbb{R}}\to\Lambda_{\mathbb{R}}$ is $\mathbb{C}$-linear.

Why study Riemann pairs? Well, the functor $(\Lambda,J)\rightsquigarrow M(\Lambda,J):=(\Lambda_{\mathbb{R}},J)/\Lambda$ is an equivalence of categories between the category of Riemann pairs, by Prop 1.1.

Now, let (V,J) be a pair where V is a real vector space and $J:V\to V$ is an $\mathbb{R}$-linear map with $J\circ J=-1$. A *Hermitian form* on (V,J) is a conjugate-symmetric $\mathbb{R}$-bilinear map $(\cdot|\cdot):V\times V\to\mathbb{C}$ such that $(Ju|v)=i(u|v)$. Writing

$$(u|v)=\varphi(u,v)-i\psi(u,v)\quad\varphi(u,v),\psi(u,v)\in\mathbb{R},$$

note φ,ψ are $\mathbb{R}$-bilinear. Some other properties: φ is symmetric, ψ is alternating, and $\varphi(u,v)=\psi(u,Jv)$. Note $(\cdot|\cdot)$ is positive definite if and only if φ is.

Finally we are ready to define abelian varieties. First: an integral *Riemann form* on a Riemann pair (Λ,J) is a bilinear map $\psi:\Lambda\times\Lambda\to\mathbb{Z}$ such that $\psi_{\mathbb{R}}$ is the imaginary part of a Hermitian form on $(\Lambda_{\mathbb{R}},J)$. Finally, a *complex abelian variety* is a complex torus $A:=V/\Lambda$ admitting a Riemann form (the Riemann pair comes from the equivalence of categories).

The idea of complex multiplication of abelian varieties is that A has lots of endomorphisms. Given an abelian variety A, we want to study its endomorphisms $\mathrm{End}(A)$. Essentially by definition of homomorphism of complex tori, if $A\cong\mathbb{C}^g/\Lambda$ is g-dimensional.

$$\mathrm{End}(A)\cong\{\alpha\in M_g(\mathbb{C}):\alpha(\Lambda)\subseteq\Lambda\}.$$

It is more useful to study $\mathrm{End}^0(A)$ (recall this is $\mathrm{End}(A)\otimes\mathbb{Q}$). There is an analagous characterization

$$\mathrm{End}^0(A)\cong\{\alpha\in M_g(\mathbb{C}):\alpha(\Lambda_{\mathbb{Q}})\subseteq\Lambda_{\mathbb{Q}}\}$$

called the *analytic representation* of $\mathrm{End}^0(A)$. Since $\Lambda_{\mathbb{R}}=\mathbb{C}^g$, any α acting as the identity on $\Lambda_{\mathbb{Q}}$ does so on all of $\mathbb{C}^g$, so that $\mathrm{End}^0(A)$ **acts faithfully on** $\Lambda_{\mathbb{Q}}$. One can identify $\Lambda_{\mathbb{Q}}:=H_1(A,\mathbb{Q})$ via basic topology.

Here is another fundamental theorem. The proof is easy so we skip it.

Theorem 1.2 (Poincaré Reducibility)**.** For any abelian subvariety $B\subseteq A$, there exists another abelian subvariety $B'\subseteq A$ such that $B\times B'\to A,\ (b,b')\mapsto b+b'$ is an isogeny.

This is in analogy with a lot of decomposition theorems in algebra.

An abelian variety A is said to be *simple* if it has no proper nonzero abelian subvarieties. Then, $\mathrm{End}^0(A)$ is a $\mathbb{Q}$-division algebra.

In general, A is isogenous to $A_1^{n_1} \times A_2^{n_2} \times \cdots \times A_s^{n_s}$ for $A_i \subseteq A$ simple, A_i, A_j not isogenous for $i \neq j$. Then, if we put $D_i = \mathrm{End}^0(A_i)$, one directly computes

$$\mathrm{End}^0(A) = \prod_{i=1}^{s} M_{n_i}(D_i),$$

and $\mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra. While tempting to immediately conclude, it is somewhat subtle to prove that $\mathrm{End}^0(A)$ is actually *finite dim* over $\mathbb{Q}$. I also do not know of an "easy" proof of this[1]. But the main consequence of this is: each D_i is a division algebra, of finite degree over its center k_i, and each k_i is a finite field extension of $\mathbb{Q}$.

Now we take a brief diversion to do some algebra. Let k be a char 0 field. An étale algebra over k is a finite product of finite separable field extensions of k.

Let B be a finite dimensional semisimple k-algebra, and let $B = \prod_i B_i$ be its decomposition into simple algebras by Wedderburn Artin. The center of each B_i is a field k_i, and each degree $[B_i : k_i]$ is square. The *reduced degree* of B over k is defined as

$$[B : k]_{\mathrm{red}} = \sum_i [B_i : k_i]^{\frac{1}{2}} [k_i : k]$$

Lemma 1.3. Notation as above:

(a) A (strictly) maximal étale k-subalgebra of B has dimension $[B : k]_{\mathrm{red}}$.
(b) If M is a faithful B-module, then $\dim_k M \geq [B : k]_{\mathrm{red}}$. Equality can hold if and only if B is a product of matrix algebras over their centers.

Proof. (a) Recall that when B is central simple over k, that a maximal subfield of B is of dimension $[B : k]^{\frac{1}{2}}$. Thus, in the case B is simple with center $k' \supset k$, a maximal subfield of B is of dimension $[B : k']^{\frac{1}{2}} [k' : k]$. The general case follows immediately. (b) Let $B_i = M_{n_i}(D_i)$ where D_i is a central simple division algebra over k_i. Thus, $S_i = D_i^{n_i}$ is a simple B_i-module. Every B-module M is isomorphic to a sum $\bigoplus_{i=1}^{s} m_i S_i$, with M faithful if and only if $m_i \geq 1$ for all i. Thus M faithful implies

$$\dim_k M = \sum_i m_i \cdot n_i \cdot [D_i : k_i] \cdot [k_i : k] \geq \sum_i n_i \cdot [D_i : k_i] \cdot [k_i : k].$$

However,

$$[B : k]_{\mathrm{red}} = \sum_i n_i [D_k : k_i]^{\frac{1}{2}} [k_i : k],$$

so the Lemma follows. □

Back to the original setup of $A \cong \mathbb{C}^g/\Lambda$. Applying this lemma to the case of the $\mathrm{End}^0(A)$-module $\Lambda_{\mathbb{Q}}$ (which is dimension $2g$ over $\mathbb{Q}$), we obtain the following crucial inequality:

$$2 \dim A \geq [\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} \tag{1}$$

Definition 1.4. A complex abelian variety A is said to have **complex multiplication** (or be of CM-type, or be a CM abelian variety), if

$$2 \dim A = [\mathrm{End}^0(A) : \mathbb{Q}]_{\mathrm{red}} \tag{2}$$

Thus, a CM abelian variety is one that has "lots of endomorphisms".

[1] See `https://math.uchicago.edu/~may/REU2022/REUPapers/Sheng.pdf`.

1.1 Connection to Algebraic Theory

Now, let k be any arbitrary field. Recall that an abelian variety A over k is a complete algebraic variety over k together with a group structure on A defined by regular maps.

Every abelian variety A is projective. Its group structure is determined by the 0 element.

Let A be an abelian variety over $\mathbb{C}$. Then, $A(\mathbb{C})$ is a complex torus. It is a *nontrivial theorem by Mumford* that the functor $A \rightsquigarrow A(\mathbb{C})$ is an equivalence between the category of abelian varieties over $\mathbb{C}$ and the category of complex tori admitting a Riemann form.

For A over arbitrary k, the inequality (1) holds, and A is said to have **complex multiplication** if equality (2) holds

In what follows we shall pass between the analytic and the algebraic theory freely based off of what I think is more convenient.

2 CM-field and CM-type

A *CM-field* K is a totally imaginary quadratic extension of a totally real number field. For clarification $K := \mathbb{Q}[\alpha] = \mathbb{Q}(x)/(f(x))$ is totally real if all the roots of $f(x)$ are real, and is totally imaginary when all the roots of $f(x)$ are non-real.

Example: cyclotomic field $\mathbb{Q}(\zeta_n)$ for $n \geq 3$. This is to say K has *exactly one complex conjugation*, i.e. complex conjugation on $\mathbb{C}$ induces an automorphism of K of order 2 independent of the embedding $K \hookrightarrow K$. A finite composite of CM-fields is CM.

A CM-algebra E is a finite product of CM-fields. In this case, there is an automorphism $\iota_E : E \to E$, nontrivial on each factor, such that $\iota \circ \rho = \rho \circ \iota_E$ for every homomorphism $\rho : E \to \mathbb{C}$. Note that ι is the usual complex conjugation.

There are $[E : \mathbb{Q}]$ total $\mathbb{Q}$-algebra homomorphisms $E \to \mathbb{C}$, and they come in complex conjugate pairs $\{\varphi, \iota \circ \varphi\}$. To this end, define a *CM-type* on a CM-algebra E is a subset $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ such that

$$\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \iota\Phi \qquad \iota\Phi := \{\iota \circ \varphi : \varphi \in \Phi\}. \tag{3}$$

The pair (E, Φ) is called a *CM-pair*. Let us see how this data may construct a CM abelian variety.

Example 2.1. Let (E, Φ) be a a CM-pair, and let $\Lambda \subset E$ be a lattice, so that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \cong E$. Let $F \subset E$ be the maximal totally real subalgebra. Since the CM-type Φ is equivalent data to choosing an extension $\rho' : E \to \mathbb{C}$ of each homomorphism $\rho : F \to \mathbb{C}$, there is an isomorphism of $\mathbb{R}$-algebras

$$E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\Phi} \prod_{\rho : F \to \mathbb{R}} \mathbb{C} =: \mathbb{C}^{\Phi}, \quad a \otimes r \mapsto (\rho'(a) \cdot r)_{\rho},$$

from which we deduce

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{R} \cong E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\Phi},$$

i.e. $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ acquires a complex structure J_{Φ}. Hence, we have a Riemann pair (Λ, J_{Φ}), hence a complex torus $A_{\Phi} := \mathbb{C}^{\Phi}/\Phi(\Lambda)$. We also obtain a homomorphism $i_{\Phi} : E \to \mathrm{End}^0(A_{\Phi})$ such that $i_{\Phi}(a)$ corresponds to the $\mathbb{C}$-linear map $\mathbb{C}^{\Phi} \to \mathbb{C}^{\Phi}, z \mapsto \Phi(a)z$.

One can show that (Λ, J_{Φ}) admits a Riemann form, and in fact i_{Φ} is injective. Thus, we say that the pair (A_{Φ}, i_{Φ}) is a CM abelian variety of CM-pair (E, Φ).

Proposition 2.2.

(a) A simple abelian variety A has CM if and only if $\mathrm{End}^0(A)$ is a CM-field of degree $2 \dim A$ over $\mathbb{Q}$.

(b) An isotypic abelian variety A has CM if and only if $\mathrm{End}^0(A)$ contains a field of degree $2\dim A$ over $\mathbb{Q}$.

(c) An abelian variety A has CM if and only if $\mathrm{End}^0(A)$ contains an étale $\mathbb{Q}$-algebra of degree $2\dim A$ over $\mathbb{Q}$.

Note: for part (b), suppose $A \sim A_0^{n_0}$ with A_0 simple. Then, $E_0 = \mathrm{End}^0(A_0)$ is a CM-field. Then, if F is a totally real field of degree n_0 over $\mathbb{Q}$ linearly disjoint with E_0, then $E := E_0 \cdot F$ is a CM-field of degree $2\dim A$ over $\mathbb{Q}$ which may be embedded in $M_{n_0}(E_0) \cong \mathrm{End}^0(A)$. Similar idea for part (c).

Thus, we often write the pair (A,i), where A is a CM abelian variety, and $i : E \to \mathrm{End}^0(A)$ is an embedding of a CM-algebra E of $\mathbb{Q}$-dimension $2\dim A$. We say that A has *complex multiplication* by E.

Now, given a CM abelian variety (A,i) with an embedding $i : E \to \mathrm{End}^0(A)$ as above. Each $a \in E$ induces an isogeny $\lambda : A \to A$, hence a pushforward linear map $\lambda_0 : \mathrm{Tgt}_0(A) \to \mathrm{Tgt}_0(A)$. Hence, $\mathrm{Tgt}_0(A)$ is a module over

$$\mathbb{C} \otimes_{\mathbb{Q}} E \cong \prod_{\varphi \in \mathrm{Hom}(E,\mathbb{C})} \mathbb{C}_\varphi,$$

so that $\mathrm{Tgt}_0(A) \cong \prod_{\varphi \in \mathrm{Hom}(E,\mathbb{C})} (\mathrm{Tgt}_0(A))_\varphi$ is an isotypic decomposition. By the complex analytic theory **clarify with Roy on more details here**, there is a set of g distinct homomorphisms Φ of $E \to \mathbb{C}$ and a basis of $\mathrm{Tgt}_0(A)$ such that the matrix of a (in the pushforward) is the diagonal matrix $\mathrm{diag}\{\varphi(a)\}_{\varphi \in \Phi}$. Thus, put $\mathrm{Tgt}_0(A) \cong \bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$. Since $H_1(A,\mathbb{R}) = \mathrm{Tgt}_0(A)$, the Hodge decomposition implies

$$H_1(A,\mathbb{C}) \cong \mathrm{Tgt}_0(A) \oplus \overline{\mathrm{Tgt}_0(A)},$$

so that Φ is in fact a CM-type on E. We say that (A,i) is of *CM-type* (E,Φ). Intuitively, the CM-type encodes the action of E on A

Furthermore, one can exhibit a bijection from the set of isogeny classes of CM pairs (A,i) to the set of isomorphism classes of CM pairs (E,Φ).

Of course, one can develop the theory of CM type for A defined over arbitrary field k of characteristic 0, with a good idea of "base change."

3 Shimura-Taniyama Formula

We are going to give the local formulation of the Shimura-Taniyama formula. As we have already discussed, the theory of CM abelian varieties is essentially the same over any base field. In this situation, let A be of CM type (K,Φ), (let K be a field, for simplicity), over a finite extension F of $\mathbb{Q}_p$, the p-adic numbers. There is something called the proper Neron model of A over $\mathscr{O}_F$, which is the *abelian scheme* $\mathscr{A}$ over $\mathrm{Spec}(\mathscr{O}_F)$ (an abelian scheme is a generalization of abelian variety to "nice" rings). Thus, $\mathscr{A}_k$ is the reduction of $\mathscr{A}$ by the residue field k of $\mathscr{O}_F$. This residue field is finite of cardinality q. Since A is CM by K, we have an injective map

$$K \hookrightarrow \mathrm{End}_F^0(A) \hookrightarrow \mathrm{End}_{\mathscr{O}_K}^0(A) \hookrightarrow \mathrm{End}_k^0(\mathscr{A}_k).$$

This mechanism suggests we should reduce via the residue field to better understand the original abelian variety A.

Note there is a distinguished element $\mathrm{Frob}_q \in \mathrm{End}_k(\mathscr{A}_k) \subset \mathrm{End}_k^0(\mathscr{A}_k)$, namely, the *absolute q-Frobenius*, of great interest in this setup. On an affine scheme $\mathrm{Spec}(R)/\mathbb{F}_q$, this is the map on $\mathrm{Spec}(R)$ induced by the homomorphism $R \to R, x \mapsto x^q$ (hence resembles the classical Frobenius endomorphism). By a "universal commutativity" property of Frob_q, this Frobenius actually lifts to an element $\pi \in K$. In fact, $\pi \in K^*$, since the Frobenius is an isogeny in $\mathscr{A}_k$.

Since $\mathrm{Frob}_q \in \mathrm{End}_k(\mathscr{A}_k)$ which is finitely generated as a $\mathbb{Z}$-module, Frob_q lies in a $\mathbb{Z}$-finite subring of K, meaning $\mathrm{Frob}_q \in \mathscr{O}_K$. Shimura and Taniyama wanted to compute the factorization of the ideal (π).

To do this, more notation is needed. Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$. Any embedding $K \hookrightarrow \overline{\mathbb{Q}_p}$ of our CM field induces a place w of K over p. In particular,

$$H := \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}_p}) = \mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Q}} K, \overline{\mathbb{Q}_p}) = \mathrm{Hom}_{\mathbb{Q}_p}\left(\prod_{w|p} K_w, \overline{\mathbb{Q}_p}\right) = \bigsqcup_{w|p} \mathrm{Hom}_{\mathbb{Q}_p}(K_w, \overline{\mathbb{Q}_p}).$$

Here, $H_w := \mathrm{Hom}_{\mathbb{Q}_p}(K_w, \overline{\mathbb{Q}_p})$ is identified with the set of embeddings $K \hookrightarrow \overline{\mathbb{Q}_p}$ inducing the place $w \mid p$, and $\#H_w = [K_w, \mathbb{Q}_p]$. Thus, given the CM-type Φ, we may define $\Phi_w = \Phi \cap H_w$.

Theorem 3.1 (Shimura-Taniyama Formula)**.** With notation as above,

$$\frac{\mathrm{ord}_w(\pi)}{\mathrm{ord}_w(q)} = \frac{\#\Phi_w}{\#H_w}.$$

This theorem is indeed quite powerful: we have got a complete factorization of π just from the CM-type of our original abelian variety A.

Ask for proof-sketch/ideas of proof from Roy (without deferring to p-divisible groups.

Clarify why the Frobenius is important.

4 Mantovan Paper

Now, having seen the Shimura-Taniyama formula, we will study one particular application to a paper by Mantovan: Newton Polygons of Cyclic Covers of the Projective Line Branched at Three Points. This will also serve as a light introduction to Galois coverings, Jacobian varieties, and p-divisible groups.

Context for the paper: given a smooth projective curve C of genus g, one may form an associated abelian variety $\mathrm{Jac}(C)$ called the *Jacobian*. This construction can be carried out over arbitrary field. One of the long standing problems in number theory, the Schottky problem, is the classification of abelian varieties that arise as Jacobians of curves. Number theorists are interested in the positive characteristic p case, in which one studies abelian abelian varieties by computing certain *p-invariants*. The p-invariant Mantovan et al are interested in is the *Newton polygon*.

Let's set up the paper. Given m positive integer, let μ_m be the mth roots of unity of $\mathbb{C}$. Let $K_d = \mathbb{Q}(\zeta_d)$ be the dth cyclotomic field. Notice

$$\mathbb{Q}[\mu_m] \cong \frac{\mathbb{Q}[x]}{(x^m - 1)} \cong \prod_{d|m} K_d$$

is a CM algebra. In lieu of the ideas of CM-type, let $\mathscr{T}$ be the set of homomorphisms $\tau : \mathbb{Q}[\mu_m] \to \mathbb{C}$. We can identify $\mathscr{T} = \mathbb{Z}/m\mathbb{Z}$ by the rule ($n \in \mathbb{Z}/m\mathbb{Z}$)

$$\tau_n(\zeta) := \zeta^n \quad \text{for all } \zeta \in \mu_m.$$

Remark. Identifying $\tau \in \mathscr{T}$ with a linear representation $\mu_m \to \mathbb{C}^*$. note if d is the order of τ, then τ "arises" from the simple Wedderburn component K_d (note: this "assertion" isn't rigorous, but it isn't hard to prove with a little bit of rep theory).

Let p be a rational prime not dividing m. We have

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{\mathrm{un}} \subset \overline{\mathbb{Q}_p} \subset \mathbb{C}_p \cong \mathbb{C}$$

Here $\mathbb{C}_p$ is the p-adic closure of $\overline{\mathbb{Q}_p}$, the algebraic closure of $\mathbb{Q}_p$, and $\mathbb{Q}_p^{\mathrm{un}}$ is the maximal unramified extension. Since $\mathbb{Q}[\mu_m]$ is unramified at p, any homomorphism $\mathbb{Q}[\mu_m] \to \mathbb{C}$ factors through the maximal unramified extension. Recall that $\mathbb{Q}_p^{\mathrm{un}}$ has a p-Frobenius σ. Thus, σ acts on $\mathscr{T}$. **Not so familiar with this**.

Elementary language: σ acts on $\mathbb{Z}/m\mathbb{Z}$ by multiplication by p. In particular, this is just the obvious action of the subgroup $\langle p\rangle \leq (\mathbb{Z}/m\mathbb{Z})^*$ on the set $\mathbb{Z}/m\mathbb{Z}$.

With this in mind, we may classify $\mathbb{Q}[\mu_m]\otimes_{\mathbb{Q}}\mathbb{Q}_p$. Let $\mathfrak{D}$ be the set of orbits $\mathfrak{o}$ of $\mathscr{T}$ by σ. Recall this is in one-to-one correspondence with the set of primes $\mathfrak{p}$ of $\mathbb{Q}[\mu_m]$ above p, so we can write $\mathfrak{p}_\mathfrak{o}$ for the prime above p corresponding to orbit $\mathfrak{o}\in\mathfrak{D}$. For every orbit $\mathfrak{o}$, the orbit of every $\tau\in\mathfrak{o}$ is the same, denote this by $d_\mathfrak{o}$. We have

$$K_d\otimes_{\mathbb{Q}}\mathbb{Q}_p=\prod_{\mathfrak{o}\in\mathfrak{D}\text{ s.t.}d_\mathfrak{o}=d}K_{d_\mathfrak{o},\mathfrak{p}_\mathfrak{o}}.$$

4.1 Galois cover and Jacobian variety

Given integers $0<a_1,a_2,a_3<m$. Suppose $a_1+a_2+a_3\equiv 0 \pmod m$ and that the elements a_1,a_2,a_3 generate $\mathbb{Z}/m\mathbb{Z}$. Put $a=(a_1,a_2,a_3)$. Then, (m,a) is called a *datum*.

Given a datum (m,a), the equation

$$y^m=x^{a_1}(x-1)^{a_2}$$

is a smooth projective curve defined over $\mathbb{Q}$. There is a map $C\to\mathbb{P}^1,\ (x,y)\mapsto x$, which commutes with the μ_m-action $\zeta\cdot(x,y)=(x,\zeta\cdot y)$. This is called a *$\mu_m$-Galois cover of $\mathbb{P}^1$*. It is branched at $0,1,\infty$, of ramification indices $n_i:=\gcd(a_i,m),\ i=1,2,3$ respectively (the order of a_i in m). Thus, by the Riemann-Hurwitz formula, the genus of C is

$$g=1+\frac{m-\gcd(a_1,m)-\gcd(a_2,m)-\gcd(a_3,m)}{2}.$$

(over any field of characteristic $p\nmid m$).

Now let us define the *Jacobian of C* (assume C is defined over $\mathbb{C}$). This is given by the following quotient. Let $H^0(C,\Omega_1^C)$ be the group of holomorphic 1-forms; this is a g-dimensional complex space. Note that $H_1(C,\mathbb{Z})$ embeds in the dual $H^0(C,\Omega_1^C)^*$ via the map

$$[\gamma]:\omega\mapsto\int_\gamma\omega.$$

Thus, $H^0(C,\Omega_1^C)^*/H_1(C,\mathbb{Z})$ is a complex torus, and in fact an abelian variety of dimension g. We denote this by $\mathrm{Jac}(C)$, called the *Jacobian variety of C*. Of course, there is a Hodge decomposition

$$H_1(C,\mathbb{C})\cong H^0(C,\Omega_1^C)\oplus\overline{H^0(C,\Omega_1^C)}$$

by the Betti-de Rham comparison.

The Jacobian can be defined for any smooth projective curve C of genus g, and there is a general construction over arbitrary fields by Weil.

4.2 Jacobian has Complex Multiplication

Setup from before. Since μ_m acts on C, there is an induced action of $\mathbb{Q}[\mu_m]$ on $\mathrm{Jac}(C)$. In fact, $H^0(C,\Omega_1^C)$ is a complex μ_m-representation, whereas $H_1(C,\mathbb{Q})$ is a *rational* μ_m-representation.

Now, recall that $\mathbb{Q}[\mu_m]$ is the product of simple Wedderburn components K_d. Let $e_d\in\mathbb{Q}[\mu_m]$ be the primitive central idempotent of $\mathbb{Q}[\mu_m]$ corresponding to K_d. This is in fact the *sum of all primitive central idempotents $e\in\mathbb{C}[\mu_m]$ corresponding to K_d*. Thus, the action of e_d on $H^0(C,\Omega_1^C),H_1(C,\mathbb{Q})$ acts as the identity on the subrepresentations corresponding to K_d, and annihilates all the other representations. Moreover, $e_d\cdot(H^0(C,\Omega_1^C)/H_1(C,\mathbb{Q}))$ is an abelian subvariety $A_d\subset\mathrm{Jac}(C)$, and we obtain an isogeny

$$\mathrm{Jac}(C)\sim\prod_{d|m}A_d,$$

since all the "mutual intersections" are finite. **Note: some subvarieties A_d may very well be 0.**

However, since K_d is simple, there is an embedding $K_d \hookrightarrow \mathrm{End}^0(A_d)$ so long as A_d is nonzero. This makes $\mathbb{Q}[\mu_m]$ a great candidate for choosing a CM-algebra of $\mathrm{Jac}(C)$. But first, we must compute the representation $H^0(C,\Omega_1^C)$. Fortunately, Hurwitz, Chevalley, and Weil have already solved that problem for us. The consequence of the *Hurwitz-Chevalley-Weil formula* is reflected by the following lemma:

Lemma 4.1. Let $\tau_n \in \mathscr{T}$ (recall this is given by $\tau_n(\zeta) = \zeta^n$). The multiplicity of τ_n in the representation $H^0(C,\Omega_1^C)$ is

$$\mathfrak{f}(\tau_n) = \begin{cases} -1 + \sum_{i=1}^3 \left\langle \frac{-na_i}{m} \right\rangle & \text{if } n \not\equiv 0 \pmod m \\ 0 & \text{if } n \equiv 0 \pmod m, \end{cases} \tag{4}$$

where $\langle\cdot\rangle$ is the fractional part.

Now, by Hodge decomposition, the multiplicity of τ_n in $\overline{H^0(C,\Omega_1^C)}$ is just $\mathfrak{f}(\tau_{-n})$. Hence, the multiplicity of τ_n in $H_1(C,\mathbb{C})$ is just $\mathfrak{F}(\tau_n) := \mathfrak{f}(\tau_n) + \mathfrak{f}(\tau_{-n})$. We are ready to prove

Theorem 4.2. The abelian variety $\mathrm{Jac}(C)$ has CM by $E := \prod_d K_d$, where the product is taken over all d such that $1 < d \mid m$ and $d \nmid a_i$ for any $i = 1,2,3$.

Proof. The multiplicity of the trivial representation in $H_1(C,\mathbb{C})$ is 0, i.e. $A_1 = 0$. In general, let $0 \neq n \in \mathbb{Z}/m\mathbb{Z}$, suppose n is order d. Let x_n be the number of a_i's not divisible by d. The conditions on the a_i's force $x_n \in \{2,3\}$, and (4) implies $\mathfrak{F}(\tau_n) = \mathfrak{f}(\tau_n) + \mathfrak{f}(\tau_{-n}) = x_n - 2$. Since $e_d \cdot H_1(C,\mathbb{C})$ is the direct sum of exactly $\mathfrak{F}(\tau_n)$ copies of $\bigoplus_{n' \text{ of order } d} \tau_{n'}$, we have that $\mathfrak{F}(\tau_n) \cdot [K_d : \mathbb{Q}]$ is exactly the dimension $\dim_{\mathbb{C}} (e_d \cdot H_1(C,\mathbb{C}))$ In turn, notice $\dim_{\mathbb{C}} (e_d \cdot H_1(C,\mathbb{C})) = 2 \dim A_d$. Hence, $A_d = 0$ if $x_n = 2$; otherwise, $A_d \neq 0$ and the embedding $K_d \hookrightarrow \mathrm{End}^0(A_d)$ is of CM type. □

What is the CM-type of $\mathrm{Jac}(C)$? Well, the representation of $\mathrm{Jac}(C)$ by $\mathbb{Q}[\mu_m]$ defines an action on the underlying tangent space. But the Hodge decomposition yields an identification of $\mathrm{Tgt}_0(\mathrm{Jac}(C))$ with the representation space $H^0(C,\Omega_1^C)$, so that the CM-type of $\mathrm{Jac}(C)$ is just the $(n-1)$-tuple $\mathfrak{f}$ (omitting $\mathfrak{f}(\tau_0)$). To be more precise: for each d such that $1 < d \mid m$ and $d \nmid a_i$ for any $i = 1,2,3$, the CM-type of $A_d \subset \mathrm{Jac}(C)$ is the type of K_d given by the embeddings τ_n, n of order d, such that $\mathfrak{f}(\tau_n) = 1$.

In what follows, we let $\mathfrak{D}' \subset \mathfrak{D}$ be the set of orbits $\mathfrak{o}$ such that $d_{\mathfrak{o}}$ satisfies the criterion of Theorem 4.2. Thus, the primes $\mathfrak{p}$ of E above p are indexed by the orbits $\mathfrak{o} \in \mathfrak{D}'$.

4.3 Definition of Newton Polygon

Let us now give an informal introduction to p-divisible groups, one which will hopefully illustrate their usage in classifying and computing p-invariants in number theory. I am following Mantovan's paper and `https://www.math.uci.edu/~lxiao/files/notes/p-Divisble%20Groups.pdf`.

Let A be an g-dim abelian variety over the algebraically closed field k. For each $n \in \mathbb{N}$, consider the multiplication by p^n morphism $[p^n] : A \to A$ and its kernel $A[p^n]$. Observe:

$$A[p^n] = \begin{cases} (\mathbb{Z}/p^n\mathbb{Z})^{2g} & \mathrm{char}(k) \neq p \\ (\mathbb{Z}/p^n\mathbb{Z})^i & \mathrm{char}(k) = p \end{cases} \tag{5}$$

for $i \leq 2g$ depending on n. In particular, $A[p^n]$ is "nice" in the $\mathrm{char}(k) \neq p$ case, since A may be realized as a complex torus, the p^n-torsion subgroup is easy to visualize. You can think of the $\mathrm{char}(k) = p$ as the "singular" case; this is interesting to study.

The *p-divisible group* of A is denoted by $A[p^\infty] := \varinjlim A[p^n]$ (to give a precise definition of p-divisible group is technical, so we won't do it today). If $\mathrm{char}(k) \neq p$, then the direct limit $A[p^\infty] := \varinjlim A[p^n]$ is just the p-adic quotient $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$. The question is, what if $\mathrm{char}(k) = p$?

Now, let G be an arbitrary p-divisible group. Note that G is an *inductive system* (G_ν, i_ν) over the integers $\nu \geq 1$ where each G_ν is a group scheme. Let us discuss what the important invariants of a p-divisible group are. The *height* h of G encodes the fact that G_ν should a group scheme of finite rank $p^{h\nu}$ over the base ring. Note that G has a "connected part," which may be realized by some Lie theory. The dimension n of this part is called the *dimension* of G.

Now return to the original setup. By the "Dieudonné-Manin" classification, there is an isogeny of p-divisible groups

$$A[p^\infty] \sim \bigoplus_{\lambda = \frac{d}{c+d}} G_{c,d}^{m_\lambda},$$

where $G_{c,d}$ is a p-divisible group of dimension d and height $c+d$. The *Newton polygon* is the multiset of values of the slopes λ. To be precise: the multiplicity of λ is $m^\lambda(c+d)$. The p-divisible group $A[p^\infty]$ is of dimension g and height $2g$, and the Newton polygon of $A[p^\infty]$ is symmetric, i.e the slopes λ and $1-\lambda$ have the same multiplicity.

In view of (5), the Newton polygon can be viewed as the measure of the "failure" in which $A[p^\infty]$ is "deformed" from the p-adic quotient $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$.

We can also define Newton polygon for characteristic 0, namely, in the local field situation. If A is an abelian variety over a local field L of mixed characteristic $(0,p)$, then we write $\nu(A)$ for the Newton polygon of the *special fiber* of A. For instance, if $\mathbb{Q}_p \subset L \subset \overline{\mathbb{Q}_p}$ is a finite extension of $\mathbb{Q}_p$, and we can "define" $A[p^\infty]$ over $\mathscr{O}_L$, then if k_L is the residue field of L, we obtain a p-divisible group $A_0 := A[p^\infty] \times_{\mathscr{O}_L} k_L$.

ask Roy about this definition.

4.4 Tate's Formulation of Shimura-Taniyama Formula

Again ask Roy about this section This section is heavy on technical algebraic geometry, so I am basically sketching the ideas here. Here, we consider an abelian variety A over F a finite extension of $\mathbb{Q}_p$. It is possible to define an associated "abelian scheme" $\mathscr{A}$ over $\mathrm{Spec}(\mathscr{O}_F)$ via something called the "proper Neron model." As usual, we have p^n-torsion group schemes $\mathscr{A}[p^n]$, and the p-divisible group $\mathscr{A}[p^\infty]$. If A admits CM of type (K,Φ), then $\mathscr{A}$ is as well.

In what follows, denote by $w \in \mathscr{O}_K$ a place over p. Note that $\mathscr{A}[p^n]$ is a finite flat group scheme over $\mathscr{O}_F$, with action by $\mathscr{O}_K$ which factors through

$$\mathscr{O}_K/(p^n) \cong \prod_{w|p} \mathscr{O}_{K_w}/(p^n);$$

decomposing by idempotents, there is a functorial decomposition

$$\mathscr{A}[p^n] \cong \prod_{w|p} G_{w,n}, \tag{6}$$

where each $G_{w,n}$ has action by $\mathscr{O}_{K_w}/(p^n)$. Then, it is fairly easy to check that the inductive system $G_w := \{G_{w,n}\}_{n\geq 1}$ is a group scheme of height $\#H_w = [K_w : \mathbb{Q}_p]$.

The more subtle result concerns the dimension of of the group scheme $G_{w,n}$. To do so, one needs a construction called the *connected-étale short-exact sequence* (by Tate). For any arbitrary group scheme G,

$$0 \to G^0 \to G \to G^{\mathrm{et}} \to 0,$$

where G^0 is initial w.r.t the property of connectedness and G^{et} terminal w.r.t to the property of étale-ness. Thus, we have group schemes $\mathscr{A}[p^n]^0, G^0_{w,n}$ for each $w \mid p$ and $n \geq 1$. One in fact, can argue that $\{G^0_{w,n}\}$ is a p-divisible group, and that their product is the p-divisible group $\mathscr{A}[p^\infty]^0$.

The p-divisible groups $\mathscr{A}[p^\infty]^0, \{G^0_{w,n}\}$ satisfy certain strong topological properties. The main result is due to Serre and Tate, which asserts that we can recover a well-defined dimension d for the connected p-divisible groups $\mathscr{A}[p^\infty]^0, \{G^0_{w,n}\}$. Furthermore, this dimension d is given exactly by $\#\Phi_w = \#(\Phi \cap H_w)$.

Given all this theory on p-divisible groups, admits a fairly "easy" proof of the Shimura-Taniyama formula. **Ask Roy for intuition on why the two concepts are related**.

The main moral of the story here, which we may apply to the situation of the Jacobian $\mathrm{Jac}(C)$, is the functorial decomposition (6). First, we must define an "integral model" $\mathscr{J}$ of the Jacobian $\mathrm{Jac}(C)$ as an abelian scheme over $\mathbb{Z}_p$. Intuitively, this is possible, since the equation $C : y^m = x^{a_1}(x-1)^{a_2}$ has integer coefficients, and that C has good reduction at p.

Now, since $\mathscr{J}$ is of CM-type $(E, \mathfrak{f})$ (recall $E := \prod_d K_d$), the functorial decomposition (6) yields

$$\mathscr{J}[p^\infty] \cong \prod_{\mathfrak{o} \in \mathfrak{D}'} \mathscr{J}[\mathfrak{p}_\mathfrak{o}^\infty],$$

where $\mathscr{J}[\mathfrak{p}_\mathfrak{o}^\infty]$ is a p-divisible group of height $\#\mathfrak{o}$ and dimension

$$\#\{\tau \in \mathfrak{o} : \mathfrak{f}(\tau) = 1\}.$$

The Newton polygon $\nu(\mathscr{J})$ follows immediately.

4.5 Example

(Explain notation for Newton polygon slopes, i.e. $(\frac{1}{3}, \frac{2}{3})$).

$m = 9$					
	p	$1 \pmod 9$	$2,5 \pmod 9$	$4,7 \pmod 9$	$8 \pmod 9$
	prime orbits	split	$(1,2,4,8,7,5)$, $(3,6)$	$(1,4,7),(2,8,5)$, $(3),(6)$	$(1,8),(2,7)$, $(4,5),(3,6)$
a	signature				
$(1,1,7)$	$(1,1,1,1,0,0,0,0)$	ord^4	ss^4	$(\frac{1}{3},\frac{2}{3}) \oplus ord$	ss^4
$(1,2,6)$	$(1,1,0,0,1,0,0,0)$	ord^3	ss^3	$(\frac{1}{3},\frac{2}{3})$	ss^3
$(1,3,5)$	$(1,1,0,1,0,0,0,0)$	ord^3	ss^3	$(\frac{1}{3},\frac{2}{3})$	ss^3

What is the main result of all these computations? Well, number theorists are especially interested in the examples of supersingular curves over characteristic p, because those correspond to certain "unlikely intersections" within the *Torelli locus*. Essentially working towards a classification of Jacobian abelian varieties in the characteristic p case. Using the Shimura-Taniyama formula to compute the Newton polygon in the CM case, Mantovan et al obtained many new examples of supersingular curves over the algebraic closure $\overline{\mathbb{F}_p}$ of genus $g \leq 11$, for many different congruence cases of p. They also found many other new examples of Newton polygons by using this computational method. This is also a preliminary paper in which Mantovan et al attacked the far more complicated case of computing Newton polygons for "positive dimensional" families of cyclic Galois covers, a "base case" of the induction process.