Abelian Varieties and Moduli

Donu Arapura

April 19, 2012

A complex abelian variety is a smooth projective variety which happens to be a complex torus. This simplifies many things compared to general varieties, but it also means that one can ask harder questions. Abelian varieties are indeed abelian groups (unlike elliptic curves which aren't ellipses), however the use "abelian" here comes about from the connection with abelian integrals which generalize elliptic integrals.

Contents

Chapter 1

The classical story

1.1 Elliptic and hyperelliptic integrals

As all of us learn in calculus, integrals involving square roots of quadratic polynomials can be evaluated by elementary methods. For higher degree polynomials, this is no longer true, and this was a subject of intense study in the 19th century. An integral of the form

$$\int \frac{p(x)}{\sqrt{f(x)}}dx \tag{1.1}$$

is called elliptic if $f(x)$ is a polynomial of degree 3 or 4, and hyperelliptic if f has higher degree.

It was Riemann who introduced the geometric point of view, that we should really be looking at the curve X'

$$y^2 = f(x)$$

in $\mathbb{C}^2$. When $f(x) = \prod(x - a_i)$ has distinct roots (which we assume from now on), X' is nonsingular, so we can regard it as a Riemann surface or one dimensional complex manifold. It is convenient to add points at infinity to make it a compact Riemann surface X called a (hyper)elliptic curve. Projection to the x-axis gives a map from X to the Riemann sphere, that we prefer to call $\mathbb{P}^1$, which is two to one away from a finite set of points called branch points, which consist of the roots a_i and possibly ∞. The classical way to understand the topology of X is to take two copies of the sphere, slit them along nonintersecting arcs connecting pairs of branch points (there are would be an even number of such points). When $n = 3, 4$, we get a torus. In general, it is a g-holed surface, where g is half the number of branch points minus one. The number g is called the *genus*.

The integrand of (1.1) can be regarded a 1-form on X, which can be checked to be holomorphic when $\deg p < g$. Let $V = \mathbb{C}^g$. Choose a base point $x_0 \in X$, and define the Abel-Jacobi "map" α from X to V by

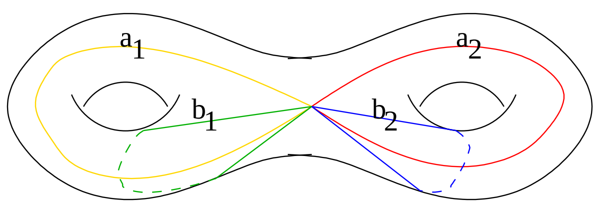
$$x \mapsto \left(\int_{x_0}^{x} \frac{1}{y} dx, \ldots \int_{x_0}^{x} \frac{x^{g-1}}{y} dx \right)$$

Note that these integrals depend on the path, so as written α is a multivalued function in classical language. In modern language, it is well defined on the universal cover $\tilde{X}$ of X. Instead of going to $\tilde{X}$, we can also solve the problem by working modulo the subgroup $L = (\int_\gamma \frac{x^i}{y} dx)$, as γ varies over closed loops of X.

Theorem 1.1.1. *L is a lattice in V; in other words, L is generated by a real basis of V.*

Corollary 1.1.2. *V/L is a torus called the Jacobian of X.*

To explain the proof, we introduce some modern tools. First we need the homology group $H_1(X, \mathbb{Z})$. The elements can be viewed equivalence classes of formal linear combinations $\sum n_i \gamma_i$, where γ_i are smooth closed curves on X. Basic algebraic topology shows that this is very computable, and in fact $H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$ with generators as pictured below when $g = 2$.



The next player is the first (de Rham) cohomology $H^1(X, \mathbb{R})$ (resp. $H^1(X, \mathbb{C})$) which is the space of real (resp. complex) valued closed 1-forms modulo exact 1-forms. Locally closed forms are expression $f dx + g dy$ such that

$$\frac{\partial f}{\partial y} - \frac{\partial g}{\partial x} = 0$$

By calculus, such things are locally of the form

$$dh = \frac{\partial h}{\partial x} dx + \frac{\partial h}{\partial y} dy,$$

but this need not be true globally. H^1 precisely measures this failure. Stokes' theorem says that pairing

$$(\gamma, \omega) \mapsto \int_\gamma \omega$$

induces a pairing

$$H_1(X, \mathbb{Z}) \times H^1(X, K) \to K, \quad K = \mathbb{R}, \mathbb{C}$$

The universal coefficients theorem tells that

$$H^1(X,K) = Hom(H_1(X,\mathbb{Z}),K) \cong K^{2g}$$

where the identification is given by the above pairing.

Proof. We are now ready to outline the proof of the theorem. Clearly, we can identify $L = H_1(X,\mathbb{Z})$. This sits as a lattice inside $H_1(X,\mathbb{Z})\otimes\mathbb{R} = H^1(X,\mathbb{R})^*$. If we could identify the last space with V, we would be done. We do this in the in the special case where the f is an odd degree polynomial with real roots, although it is true in general. Arrange the roots in order $a_1 < \ldots < a_n$. The assumptions guarantee that the integrals (written in real notation)

$$\int_{-\infty}^{a_1} \frac{x^j}{\sqrt{f(x)}}dx \tag{1.2}$$

are purely imaginary, while

$$\int_{a_n}^{\infty} \frac{x^j}{\sqrt{f(x)}}dx \tag{1.3}$$

and purely real. Note that the preimages of the paths of integration above are closed loops in X. We can think of the real dual V^* as the space spanned by the differentials $dx/y, \ldots x^{g-1}dx/y$. This sits naturally inside $H^1(X,\mathbb{C})$. By taking real parts, we can map this to $H^1(X,\mathbb{R})$. We claim that it is an isomorphism of real vector spaces. These spaces have the same real dimension, so it is enough to prove that it is injective. Suppose that $\sum a_j x^j dx/y$ lies in the kernel. Then the integrals $\int_\gamma \sum a_j x^j dx/y$ would have to be purely imaginary for all closed loops γ. In view of (1.2) and (1.3), this is impossible unless the coefficients are zero. □

1.2 Elliptic curves

From the previous discussion, given an elliptic curve, we have an map to a one dimensional torus which turns out to be an isomorphism. We now work backwards starting with a torus $E = \mathbb{C}/L$ of the complex plane by a lattice. Recall that this means that L is a subgroup spanned by two $\mathbb{R}$-linearly independent numbers ω_i. Since $E \cong \mathbb{C}/\omega_1^{-1}L$, there is no loss in assuming that $\omega_1 = 1$, and that $Im(\omega_2) > 0$ (replace ω_2 by $-\omega_2$).

Now consider complex function theory on E. Any function on E can be pulled back to a function f on $\mathbb{C}$ such that

$$f(z+\lambda) = f(z), \quad \lambda \in L \tag{1.4}$$

As a consequence

Lemma 1.2.1. *Any holomorphic function on E is constant.*

Proof. Any holomorphic pulls back to a bounded holomorphic function, which is constant by Liouville's theorem. □

To get interesting global functions, we should either allow poles or relax the periodicity condition. A meromorphic function f is called *elliptic* if it satisfies (1.4). A nontrivial example is the Weirstrass $\wp$-function

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right]$$

It is instructive to note that the more naive series $\sum 1/(z-\lambda)^2$ won't converge, but this will because

$$\left| \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right| \le \frac{const}{\lambda^3}$$

See [S] for a proof that this converges to an elliptic function. This will have double poles at the points of L and no other singularities.

The next step is to relate this to algebraic geometry by embedding E into projective space. There are various ways to do this. We use $\wp$-function. To begin with $\wp$ defines a holomorphic map from $\mathbb{C} - L$ to $\mathbb{C}$, which necessarily factors through E minus (the image) of 0. To complete this, we should send 0 to the point ∞ on the Riemann sphere (which algebraic geometers prefer to call $\mathbb{P}^1$). Since $\wp(-z) = \wp(z)$ the map is not one to one. To get around that, we send $z \in \mathbb{C} - L$ to $(\wp(z), \wp'(z)) \in \mathbb{C}^2$. This gives a well defined map of E minus 0 to $\mathbb{C}^2$ which is one to one. We would like to characterize the image.

Theorem 1.2.2. *$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ for the appropriate choice of constants g_i.*

Sketch. The idea is to choose the constants so that the difference $(\wp')^2 - 4\wp^3 - g_2\wp - g_3$ vanishes at 0. But then it is elliptic with no poles, so it vanishes everywhere. See [S]. □

Corollary 1.2.3. *The image of $E - L$ is given by the cubic curve $y^2 = 4x^3 - g_2x - g_3$.*

To complete the picture we recall that we can embed $\mathbb{C}^2$ into the complex projective plane $\mathbb{P}^2 = \mathbb{C}^3 - \{0\}/\mathbb{C}^*$ by sending (x, y) to the point $[x, y, 1] \in \mathbb{P}^2$. Then can be identified with the closure of the image of the above curve is given by the homogeneous equation

$$zy^2 = 4x^3 - g_2xz^2 - g_3z^3$$

The point $0 \in E$ maps to $[0, 1, 0]$. It follows from Chow's theorem that the group law $E \times E \to E$ is a morphism of varieties, i.e. it can be defined algebraically. It is determined explicitly by the rule that points $p + q + r = 0$ if and only if they are colinear.

Not all elliptic curves are the same. For example some of them, such as $\mathbb{C}/\mathbb{Z}+\mathbb{Z}i$ have extra symmetries. To make this precise, we consider the endomorphism ring $End(E$ which is the set of holomorphic endomorphisms of E. If $E = \mathbb{C}/L$, we can identify E with the set of complex numbers α such that $\alpha L \subseteq L$.

Theorem 1.2.4. *Let $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$, then either*

1. *$End(E) = \mathbb{Z}$ or*
2. *$\mathbb{Q}(\tau)$ is an imaginary quadratic field, and $End(E)$ is an order in $\mathbb{Q}(\tau)$ i.e. a finitely generated subring such that $End(E) \otimes \mathbb{Q} = \mathbb{Q}(\tau)$.*

Proof. Let $L = \mathbb{Z} + \mathbb{Z}\tau$. Then $End(E)$ can be identified with $R = \{\alpha \in \mathbb{C} \mid \alpha L \subseteq L\}$. For $\alpha \in R$, there are integers ab, c, d such that

$$\alpha = a + b\tau,\ \alpha\tau = c + d\tau$$

By Cayley-Hamilton, or direct calculation, we see that

$$\alpha^2 - (a + d)\tau + ad - bc = 0$$

Therefore R is an integral extension of $\mathbb{Z}$.

Suppose that $R \neq \mathbb{Z}$, and choose $\alpha \in R$ but $\alpha \notin \mathbb{Z}$. Then eliminating α from the previous equations yields

$$b\tau^2 - (a - d)\tau - c = 0$$

Therefore $\mathbb{Q}(\tau)$ is quadratic imaginary and $R \subset \mathbb{Q}(\tau)$ is an order. □

1.3 Jacobi's Theta function

The alternative approach of relaxing the periodicity (1.4) leads to the theory of theta functions. The higher dimensional analogue will play an important role later below Basically, we want holomorphic functions that satisfy

$$f(z + \lambda) = (\text{some factor}) f(z)$$

which we refer to as quasi-periodicity with respect to $L = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau = \omega_2$ in the upper half plane, We can obtain elliptic functions by taking ratios of two such functions with the same factors. To make it more precise, we want

$$f(z + \lambda) = \phi_\lambda(z) f(z) \tag{1.5}$$

where $\phi_\lambda(z)$ is a nowhere zero entire function. To guarantee nonzero solutions, we require some compatibility conditions

$$f(z + (\lambda_1 + \lambda_2)) = \phi_{\lambda_1+\lambda_2}(z) f(z)$$

$$f((z + \lambda_1) + \lambda_2) = \phi_{\lambda_2}(z + \lambda_2)\phi_{\lambda_1}(z) f(z)$$

which suggests that we should impose

$$\phi_{\lambda_1+\lambda_2}(z) = \phi_{\lambda_2}(z + \lambda_2)\phi_{\lambda_1}(z)$$

This is called the cocycle identity. As it turns out, there is a cheap way to get solutions, choose a nowhere 0 function $g(z)$ and let $\phi_\lambda(z) = g(z+\lambda)/g(z)$ such as cocycle is called a coboundary. From the point of view of constructing interesting solutions of (1.5), it is not very good. Any solution would be a constant multiple of $g(z)$. Taking ratios of two functions would result in a constant.

The problem of constructing cocycles which are not coboundaries is not completely obvious. As a first step since ϕ is entire and nowhere 0, we can take a global logarithm $\psi(z) = \log\phi(z)$. Then

$$\psi_{\lambda_1+\lambda_2}(z) = \psi_{\lambda_2}(z+\lambda_2) + \psi_{\lambda_1}(z) \mod 2\pi i\mathbb{Z}$$

It is not entirely obvious how to find nontrivial solutions, but here is one

$$\psi_{n\tau+m}(z) = -n^2\pi i\tau + 2\pi inz$$

With this choice, we can find an explicit solution to (1.5). The Jacobi θ-function is given by the Fourier series

$$\theta(z) = \sum_{n\in\mathbb{Z}} \exp(\pi in^2\tau + 2\pi inz) = \sum_{n\in\mathbb{Z}} \exp(\pi in^2\tau)\exp(2\pi inz)$$

Writing $\tau = x+iy$, with $y>0$, shows that on a compact subset of the z-plane the terms are bounded by $O(e^{-n^2y})$. So uniform convergence on compact sets is guaranteed. This is clearly periodic

$$\theta(z+1) = \theta(z)$$

In addition it satifies the function equation

$$\begin{aligned}\theta(z+\tau) &= \sum \exp(\pi in^2\tau + 2\pi in(z+\tau))\\ &= \sum \exp(\pi i(n+1)^2\tau - \pi i\tau + 2\pi inz)\\ &= \exp(-\pi i\tau - 2\pi iz)\theta(z)\end{aligned}$$

and more generally

$$\theta(z+n\tau+b) = \exp(\psi_{n\tau+m}(z))\theta(z)$$

We can get a larger supply of quasiperiodic functions by translating. Given a rational number b, define

$$\theta_{0,b}(z) = \theta(z+b)$$

Then

$$\theta_{0,b}(z+1) = \theta_{0,b}(z), \quad \theta_{0,b}(z+\tau) = \exp(-\pi i\tau - 2\pi iz - 2\pi ib)\theta(z)$$

We can construct elliptic functions by taking ratios: $\theta_{0,b}(Nz)/\theta_{0,b'}(Nz)$ is a (generally nontrivial) elliptic function when $b, b' \in \frac{1}{N}\mathbb{Z}$. More generally given rational numbers $a, b \in \frac{1}{N}\mathbb{Z}$, we can form the theta functions with characteristics

$$\theta_{a,b}(z) = \exp(\pi ia^2\tau + 2\pi a(z+b))\theta(z+a\tau+b) \tag{1.6}$$

Fix $N \geq 1$, and let V_N denote the set of linear combinations of these functions.

Lemma 1.3.1. *Given nonzero $f \in V_N$, it has exactly N^2 zeros in the parallelogram with vertices $0, N, N\tau, N+\tau$.*

Sketch. Complex analysis tells us that the number of zeros is given by the integral

$$\frac{1}{2\pi i}\int_\gamma \frac{f'dz}{f}$$

over the boundary of the parallelogram. This can be evaluated to N^2 using the identities $f(z+N) = f(z)$, $f(z+N\tau) = Const.\exp(-2\pi i N z)f(z)$ following from (1.6). □

These can be used to construct a projective embedding different from the previous.

Theorem 1.3.2. *Choose an integer $N > 1$ and the collection of all θ_{a_i,b_i}, as (a_i, b_i) runs through representatives of $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$. The the map of $\mathbb{C}/L$ into $\mathbb{P}^{N^2-1}$ by $z \mapsto [\theta_{a_i,b_i}(z)]$ is an embedding.*

Sketch. Suppose that this is not an embedding. Say that $f(z_1) = f(z_1')$ for some $z_1 \neq z_1'$ in $\mathbb{C}/L$ and all $f \in V_N$. By translation by $(a\tau + b)/N$ for $a, b \in \frac{1}{N}\mathbb{Z}$, we can find another such pair z_2, z_2' with this property. Since $\dim V_N = N^2$, we can find additional points $z_2, \ldots z_{N^2-3}$, distinct in $\mathbb{C}/NL$, so that

$$f(z_1) = f(z_2) = f(z_3) = \ldots f(z_{N^2-3}) = 0$$

for some $f \in V_N - \{0\}$. Notice that we are forced to also have $f(z_1') = f(z_2') = 0$ which means that f has at least $N^2 + 1$ zeros which contradicts the lemma.

Further details can be found in [M2]. □

1.4 Riemann's conditions

We now turn our attention to higher dimensions. Let $T = \mathbb{C}^n/L$ where L is a lattice. This is a complex manifold called a complex torus. As before, we can view functions on X as L-periodic functions on $\mathbb{C}^n$. The first major difference is that *most tori will have no constant meromorphic functions.* Riemann found necessary and sufficient conditions to guarantee the existence of interesting functions.

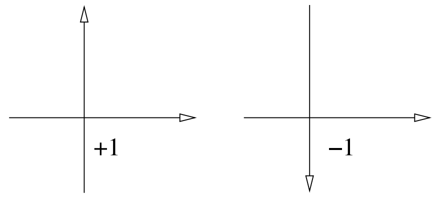
To see where this comes from, we return to the situation of a compact (not necessarily hyperelliptic) surface X of genus g. Set $L = H_1(X, \mathbb{Z}) \cong \mathbb{Z}^{2g}$. We have an intersection pairing

$$E : L \times L \to \mathbb{Z}$$

where $E(\gamma, \gamma')$ counts the number of times γ intersects γ', with signs. That is if the curves are transverse

$$E(\gamma, \gamma') = \sum_{p \in \gamma \cap \gamma'} \pm 1$$

according to



There are various ways to construct this rigorously. One way is to construct the dual pairing on $H^1(X,\mathbb{Z})$ using the cup product. In terms of the embedding $H^1(X,\mathbb{Z}) \subset H^1(X,\mathbb{R})$, this given by integration

$$E(\alpha,\beta) = \int_X \alpha \wedge \beta$$

The key point is that E is skew symmetric with determinant $+1$. By linear algebra, we can find a basis for L, called a symplectic basis, so that E is represented by the matrix

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

To simply notation, let us identify $L \cong L^* = H^1(X,\mathbb{Z})$ using E.

Let $H^{1,0}(X) \subset H^1(X,\mathbb{C})$ be the subspace spanned by holomorphic 1-forms. The are forms given locally by $\omega = f(z)dz$ where f is holomorphic. Since

$$\omega \wedge \bar{\omega} = -2i|f(z)|^2 dx \wedge dy$$

we conclude that

$$H(\omega,\eta) = i\int_X \omega \wedge \bar{\eta}$$

is a positive definite Hermitian form on $H^{1,0}$. To finish the story, we should observe that the real part determines an isomorphism $H^{1,0}(X) \cong H^1(X,\mathbb{R})$. (We checked this in a special case, but it is true in general.) Thus $H^1(X,\mathbb{Z})$ embeds into $H^{10}(X)$ as a lattice. Clearly, $E = imH$ on L. We now generalize.

Definition 1.4.1. *Given lattice L in finite dimensional a complex vector space V. A Riemann form or polarization is a positive definite Hermitian form H on V such that $E = imH$ is integer valued on L. The torus V/L is called an abelian variety if such a polarization exists.*

It follows from the above conditions, that E is a nondegenerate integral symplectic form. It is not hard to see that E determines H by

$$H(u,v) = E(iu,v) + iE(u,v)$$

so we sometimes refer to E as the polarization. In terms of a basis we have the following interpretation:

Proposition 1.4.2. *Identify $V \cong \mathbb{C}^g$ and choose a basis of L and let Π be the $g \times 2g$ matrix having these vectors as columns. A $2g \times 2g$ integral skew symmetric matrix E determines a polarization if and only if*

1. $\Pi E^{-1}\Pi^T = 0$ *and*

2. $\Pi E^{-1}\bar{\Pi}^T$ *is positive definite.*

Proof. [BL, §4.2]. □

By linear algebra [L], we can represent E by a matrix

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$$

where D is integer diagonal matrix with positive entries on the diagonal. In the special case where $D = I$, as in the Riemann surface case, we call this a *principal polarization*. Let assume this for simplicity. Classically, one normalizes the matrix $\Pi = (I, \Omega)$. Then the above conditions say that

1. Ω is symmetric and

2. The imaginary part of Ω is positive definite.

We refer to set of such matrices as the *Siegel upper half plane* H_g. We now construct the Riemann theta function on $\mathbb{C}^g$

$$\theta(z) = \sum_{n\in\mathbb{Z}^g} \exp(\pi i n^t \Omega n + 2\pi i n^t z)$$

This is a generalization of the Jacobi function. Proof of convergence is similar. With this function in hand, we can build up a large class of auxillary functions $\theta_{a,b}$ on $\mathbb{C}^g/\mathbb{Z}^g + \Omega\mathbb{Z}^g$ which can be used to construct an embedding in projective space as before. This will be explained later.

The significance is given by

Theorem 1.4.3 (Chow)**.** *Any complex submanifold of a complex projective space is an algebraic variety, i.e. it is defined by homogeneous polynomials.*

Therefore as a corollary, we see that

Theorem 1.4.4. *A principally polarized abelian variety is a projective algebraic variety.*

We will see that this true for any abelian variety, and conversely, that any torus which a projective variety is an abelian variety.

Chapter 2

The modern viewpoint

2.1 Cohomology of a torus

In this section, we can ignore the complex structure and work with a real torus $X = \mathbb{R}^n/\mathbb{Z}^n$. Let $e_1, \ldots, e_n$ (resp. $x_1, \ldots, x_n$) denote the standard basis (resp. coordinates) of $\mathbb{R}^n$. A k-form is an expression

$$\alpha = \sum f_{i_1,\ldots i_k}(x_1, \ldots, x_n) dx_{i_1} \wedge \ldots \wedge dx_{i_k}$$

where the coefficient are L-periodic C^∞-functions. We let $\mathcal{E}^k(X)$ denote the space of these. As usual

$$d\alpha = \sum \frac{\partial f_{i_1,\ldots i_k}}{\partial x_j} dx_j \wedge dx_{i_1} \wedge \ldots \wedge dx_{i_k}$$

This satisfies $d^2 = 0$. So we defined k-th de Rham cohomology as

$$H^k(X, \mathbb{R}) = \frac{ker[\mathcal{E}^k(X) \xrightarrow{d} \mathcal{E}^{k+1}(X)]}{im[\mathcal{E}^{k-1}(X) \xrightarrow{d} \mathcal{E}^k(X)]}$$

The constant form $dx_{i_1} \wedge \ldots \wedge dx_{i_k}$ certainly defines an element of this space, which is nonzero because it has nonzero integral along the subtorus spanned by e_{i_j}. (Integration can be interpreted as pairing between cohomology and homology.) These form span by the following special case of Künneth's formula:

Theorem 2.1.1. *A basis is given by cohomology classes of constant forms* $\{dx_{i_1} \wedge \ldots \wedge dx_{i_k}\}$. *Thus* $H^k(X, \mathbb{R}) \cong \wedge^k \mathbb{R}^n$.

It is convenient to make this independent of the basis. Let us suppose that we have a torus $X = V/L$ given as quotient of real vector space by a lattice. Then we can identify $\alpha \in H^k(X, \mathbb{R})$ with the alternating k-linear map

$$L \times \ldots \times L \to \mathbb{R}$$

sending $(\lambda_1, \ldots, \lambda_k)$ to the integral of α on the torus spanned by λ_j. Thus we have an natural isomorphism

$$H^k(X, \mathbb{R}) = \wedge^k Hom(L, \mathbb{R})$$

This works with any choice of coefficients such as $\mathbb{Z}$. For our purposes, we can identify $H^k(X, \mathbb{Z})$ the group of integer linear combinations of constant forms. Then

$$H^k(X, \mathbb{Z}) = \wedge^k L^*, \ L^* = Hom(L, \mathbb{Z})$$

We are now in a position to understand what a polarization on an abelian variety $X = V/L$ means geometrically. We will eventually construct an embedding $X \subset \mathbb{P}^N$. To make a long story short, the de Rham cohomology $H^k(\mathbb{P}^N, \mathbb{R})$, and the subgroup $H^k(\mathbb{P}^N, \mathbb{Z})$, can be defined as above. It is known that $H^2(\mathbb{P}^N, \mathbb{Z})$ is an infinite cyclic group with a natural generator. Restricting this class to $H^2(X, \mathbb{Z})$ which corresponds to skew symmetric form on L. This is precisely our polarization E.

2.2 Line bundles on tori

A manifold X is a metric space which locally looks like Euclidean space. More formally, for an n dimensional C^∞ (resp. complex) manifold we require an open covering $\{U_i\}$ together with homeomorphisms to the unit ball in $\phi_i : U_i \cong B \subset \mathbb{R}^n$ (resp. $\mathbb{C}^n$) such that the transition functions $\phi_i \circ \phi_j^{-1}$ are C^∞ (resp. holomorphic). A more detailed treatment can be found in Griffiths and Harris [GH] for example. For us, the main class of examples of either type of manifold are tori.

Fix a manifold X. The trivial rank r complex vector bundle is simply $X \times \mathbb{C}^r$ viewed as manifold with a projection $X \times \mathbb{C}^r \to X$. In general, a rank n vector bundle is manifold $\pi : V \to X$ which is locally isomorphic to a trivial vector bundle. This means that there exists an open cover $\{U_i\}$ and isomorphisms $\pi^{-1}(U_i) \cong U_i \times \mathbb{C}^n$ compatible with projections and linear on the fibres. A rank 1 vector bundle is also called line bundle. To be clear, when X is a complex manifold, which is the case we really care about, we will say that V is also a complex manifold and the above maps are holomorphic.

Example 2.2.1. *Let $X = \mathbb{P}^n$. View it as the set of one dimensional subspaces of $\mathbb{C}^{n+1}$. Then the the tautological line bundle $\mathcal{O}(-1)$ is the holomorphic line bundle defined by a the manifold*

$$\{(v, \ell) \in \mathbb{C}^{n+1} \times \mathbb{P}^n \mid v \in \ell\}$$

with its projection to $\mathbb{P}^n$.

Given a holomorphic line bundle $\pi : \Lambda \to X$, the set of sections over an open set $U \subseteq X$

$$\mathcal{L}(U) = \{s : U \to \pi^{-1}(U) \mid \pi \circ s = id\}$$

is naturally a module over the ring of holomorphic functions $\mathcal{O}_X(U)$. The collection $\mathcal{L}(U)$ is a so called rank one locally free sheaf of modules, which determines Λ. In fact, algebraic geometers generally conflate the two notions. It is not hard to show that $\mathcal{O}(-1)(\mathbb{P}^n) = 0$, and therefore that $\mathcal{O}(-1)$ is not trivial.

We come to the main point, which is a general construction for line bundles on a complex torus $X = V/L$. A "system of multipliers" or an " automorphy factor" is a collection of nowhere zero holomorphic functions $\phi_\lambda \in \mathcal{O}(V)^*$ such that

$$\phi_{\lambda+\lambda'}(z) = \phi_{\lambda'}(z+\lambda)\phi_\lambda(z) \tag{2.1}$$

The multipliers ϕ_λ can be used to construct a right action of L on $V \times \mathbb{C}$ by

$$(z, x) \cdot \lambda = (z + \lambda, \phi_\lambda(z)x)$$

Indeed (2.1) shows the required associativity condition

$$(z, x) \cdot (\lambda + \lambda') = ((z, x) \cdot \lambda) \cdot \lambda'$$

holds. Then we can define the quotient

$$\Lambda_\phi = (V \times \mathbb{C})/L$$

using this action. When equipped with the obvious projection to $\Lambda_\phi \to X$, this becomes a line bundle. We can construct the associated sheaf $\mathcal{L}_\phi$ directly. A holomorphic function on (a subset of) V is a theta function with respect to ϕ if

$$f(z + \lambda) = \phi_\lambda(z)f(z). \tag{2.2}$$

Note that $f(z + \lambda + \lambda')$ can be expressed in several ways, and the consistency of these expressions follows from (2.1). Let $\pi : V \to T$ denote the projection. For any open set $U \subset T$, let $\mathcal{L}_\phi(U)$ denote the set of θ-functions on $\pi^{-1}U$.

In general, different systems of multipliers could give rise to the same line bundle.

Example 2.2.2. *Given a nowhere zero function ψ, $\phi_\lambda(z) = \psi(z + \lambda)\psi(z)^{-1}$ is system of multipliers. Such an example is called a coboundary.*

Lemma 2.2.3. *If $\phi_\lambda, \phi'_\lambda$ are two systems of multipliers such that the ratio $\phi_\lambda/\phi'_\lambda$ is a coboundary, then the corresponding line bundles are isomorphic,*

Proof. By assumption, $\phi_\lambda(z)/\phi'_\lambda(z) = \psi(z + \lambda)/\psi(z)$ Then $f \mapsto \psi f$ is an invertible transformation from the space of theta function for ϕ'_λ to the space of theta function for ϕ'_λ for each U. □

For the record, we note that

Theorem 2.2.4. *All line bundles on X arise from this construction using a system of multipliers uniquely up to multiplication by a coboundary.*

Proof. Here is a "sledgehammer" proof. If it doesn't make sense, don't worry, we (probably) won't need it. A slightly lower tech, and longer but equivalent, argument can be found in [M, chap 1,§2]. Equation (2.1) is precisely the cocycle rule for defining an element of group cohomology $H^1(L, \mathcal{O}(V)^*)$. Two cocycles define the same element precisely when their ratio is a coboundary. On the other hand, we know that line bundles are classified by sheaf cohomology $H^1(X, \mathcal{O}_X^*)$. To see that these two are the same, use the exact sequence

$$0 \to H^1(L, \mathcal{O}(V)^*) \to H^1(X, \mathcal{O}_X^*) \to H^0(L, H^1(V, \mathcal{O}_V^*))$$

which comes from the spectral sequence

$$E_2^{pq} = H^p(\Gamma, H^q(V, \mathcal{O}_V^*)) \Rightarrow H^{p+q}(X, \mathcal{O}_X^*)$$

So we are reduced to proving that $H^1(V, \mathcal{O}_V^*) = 0$. But this sits in an exact sequence

$$0 = H^1(V, \mathcal{O}_V) \to H^1(V, \mathcal{O}_V^*) \to H^2(V, \mathbb{Z}) = 0$$

The vanishing of the left and right hand groups comes from the fact that V is both Stein and contractible. □

2.3 Theorem of Appell-Humbert

We want to specialize the previous construction to an abelian variety $X = V/L$. We choose forms H, E as in definition 1.4.1, but we now we relax the requirement that H is positive definite. More explicitly, H is a Hermitian form such that $E = ImH$ is integer valued on L. For example $H = E = 0$ is allowed. In this case, we have method for describing explicit multipliers. Let $U(1) \subset \mathbb{C}$ denote the unit circle.

Lemma 2.3.1. *There exists a (nonunique) map $\alpha : L \to U(1)$, called a semicharacter, satisfying*

$$\alpha(\lambda_1 + \lambda_2) = (-1)^{E(\lambda_1,\lambda_2)}\alpha(\lambda_1)\alpha(\lambda_2) = \pm\alpha(\lambda_1)\alpha(\lambda_2) \tag{2.3}$$

For any α as above,

$$\phi_\lambda(z) = \alpha(\lambda)\exp(\pi[H(z, \lambda) + \frac{1}{2}H(\lambda, \lambda)]) \tag{2.4}$$

is a system of multipliers.

Proof. Choose a basis $\lambda_i \in L$, and assign values $\alpha(\lambda_i) \in U(1)$. Then it is not hard to see that for each tuple $(n_1, n_2, \ldots)$, there is a unique choice of sign below

$$\alpha(\sum n_i\lambda_i) = \pm\alpha(\lambda_1)^{n_1}\alpha(\lambda_2)^{n_2}\ldots$$

which makes (2.3) true.

Using the identity

$$H(\lambda+\lambda',\lambda+\lambda') + 2iImH(\lambda,\lambda') = H(\lambda,\lambda) + H(\lambda',\lambda') + 2H(\lambda,\lambda')$$

and

$$\alpha(\lambda+\lambda') = \exp(i\pi ImH(\lambda,\lambda'))\alpha(\lambda)\alpha(\lambda')$$

we can check (2.1).

$$\begin{aligned}
\phi_{\lambda+\lambda'}(z) &= \alpha(\lambda)\alpha(\lambda')\exp(\pi[iImH(\lambda,\lambda') + H(z,\lambda+\lambda') + \frac{1}{2}H(\lambda+\lambda',\lambda+\lambda')]) \\
&= \alpha(\lambda')\exp(\pi[H(z+\lambda,\lambda') + \frac{1}{2}H(\lambda',\lambda')])\alpha(\lambda)\exp(\pi[H(z,\lambda) + \frac{1}{2}H(\lambda',\lambda')]) \\
&= \phi_{\lambda'}(z+\lambda)\phi_\lambda(z)
\end{aligned}$$

□

We refer to the pairs (H,α) as Appell-Humbert data. These form a group under the rule

$$((H_1,\alpha_1),(H_1,\alpha_1)) \mapsto (H_1+H_2,\alpha_1\alpha_2)$$

Theorem 2.3.2 (Appell-Humbert)**.** *Any system of multipliers is a product of a coboundary and a system of multipliers associated to an (H,α). Consequently the group of multipliers modulo coboundaries is isomorphic to the group of Appell-Humbert data.*

Proof. [BL, M]. □

The set of line bundles on X also forms a group with respect tensor product. This is called the Picard group and denoted by $Pic(X)$. To each pair (H,α) we have a system of multipliers and therefore a line bundle, which we denote by $\mathcal{L}(H,\alpha)$.

Corollary 2.3.3. *The map $(H,\alpha)\mapsto\mathcal{L}(H,\alpha)$ induces an isomorphism between the group of pairs (H,α) and $Pic(X)$.*

To each pair (H,α), we can associate the element $E\in\wedge^2L^* = H^2(X,\mathbb{Z})$. This gives a group homomorphism $Pic(X)\to H^2(X,\mathbb{Z})$. This can be identified with the first Chern class c_1 [BL, M]. The kernel denoted by $Pic^0(X)$ can be identified with the subgroup of pairs $(0,\alpha)$. Note $\alpha: L\to U(1)$ is necessarily a homomorphism. Thus

Corollary 2.3.4.

$$Pic^0(X)\cong Hom(L,U(1))$$

In particular, we see that $Pic^0(X)$ is also a real torus. We claim that this can be realized as a complex torus. Let V^* be the space of complex *antilinear* maps $V\to\mathbb{C}$. This means that $f(av_1+a_2v_2) = \bar{a}_1f(v_1)+\bar{a}_2f(v_2)$. This is can be understood as complex conjugate of the usual dual. Let $L^*\subset V^*$ denote the subset of those maps which are integer valued on L.

Lemma 2.3.5. *The map $f \mapsto e^{2\pi\sqrt{-1}Imf(-)}$ induces an isomorphism $V^*/L^* \cong Pic^0(X)$. When X is abelian variety, then so is the dual V^*/L^**

Proof. The first is part is pretty straight forward. By linear algebra a polarization E on L gives rise to a dual polarization E^* on L^*. If E is represented by a matrix with respect to a basis of L, E^* is represented by the same matrix with respect to the dual basis. □

We let $\hat{X} = V^*/L^*$. This is called the *dual abelian variety.* The key property is the following:

Proposition 2.3.6. *There exists a line bundle P on $X \times \hat{X}$ called a Poincaré line bundle such that every line bundle in $Pic^0(X)$ is isomorphic to the restriction $P|_{X\times L}$ for a unique $L \in \hat{X}$.*

Sketch. P is determined by (H, α) where H is the Hermitian form H on $(V \times V^*)$ given by

$$H((v_1, f_1), (v_2, f_2)) = \overline{f_2(v_1)} + f_1(v_2)$$

We can choose any compatible semicharacter $\alpha : L \times L^* \to U(1)$. □

Remark 2.3.7. *We can normalize the choice of α so that $P|_{X\times L} \cong L$ and $P_{0\times\hat{X}} = \mathcal{O}_{\hat{X}}$. Then P is uniquely determined. In this case*

$$\alpha(\lambda, f) = \exp(\pi\sqrt{-1}Imf(\lambda))$$

2.4 The number of theta functions

Let $X = V/L$ be a g dimensional abelian variety with a polarization (H, E). In a suitable integral basis of L, called a symplectic basis,

$$E = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \tag{2.5}$$

where D is a diagonal matrix with positive integer entries d_i. In particular, $\sqrt{\det E} = \det(D) = \prod d_i$ is an integer. Choose a semicharacter α as in lemma 2.3.1.

Theorem 2.4.1 (Frobenius)**.** *The dimension of the space of theta functions $\mathcal{L}(H, \alpha)(X)$ is exactly $\sqrt{\det E}$. In particular, it is a finite nonzero number.*

The basic idea is to count Fourier coefficients. This can be illustrated by what is in fact a special case:

Lemma 2.4.2. *Let τ be in the upper half plane. The space of holomorphic functions satisfying*

$$f(z + 1) = f(z)$$

$$f(z + \tau) = \exp(-2\pi ik + b)f(z)$$

is k dimensional.

Proof. By periodicity, we can express

$$f(z) = \sum a_n \exp(2\pi i n z)$$

The second equation above implies

$$\begin{aligned}\sum a_n \exp(2\pi i n\tau)\exp(2\pi i n z) &= f(z+\tau)\\ &= \sum a_n \exp(2\pi i(n+k)z)\exp(b)\\ &= \sum a_{n-k}\exp(b)\exp(2\pi i n z)\end{aligned}$$

Leading to recurrence relations

$$a_n = a_{n-k}\exp(b - 2\pi i n\tau)$$

Thus $a_0, \ldots, a_{k-1}$ can be chosen freely, and they determine the other coefficients. The proof of convergence is similar to the proof for the Jacobi function. □

The proof of the theorem is in principle similar, but the reductions are somewhat involved. Complete details can be found in [BL, M]. Implicit in the above theorem is the assertion:

Lemma 2.4.3. *$\dim \mathcal{L}(H,\alpha)(X)$ is independent of α.*

Sketch. This can be checked directly. Given another semicharacter α', an isomorphim $\mathcal{L}(H,\alpha)(X) \cong \mathcal{L}(H,\alpha')(X)$ is given by multiplication by $\exp(q(z))$ for an appropriately chosen quadratic function q. □

Proof of theorem. In brief outline, the theorem is proved as follows. By the previous lemma, we may choose α in a convenient manner. For a suitably chosen basis of L, we can split $L = L_1 \oplus L_2$ where L_1 spanned by the first g basis vectors, and L_2 by the remaining vectors. We can choose $\alpha(\lambda_i) = 1$ as explained in the proof of lemma 2.3.1. The space of theta functions $\mathcal{L}(H,\alpha)(X)$ is the space of functions $f(z)$ satisfying (2.2) for (2.4). Multiplying ϕ_λ by a coboundary leads to an isomorphic space. By choosing an appropriate coboundary, we can arrange that the functions in the new space are periodic with respect L_2. Thus they can expanded in a Fourier series. The remaining quasiperiodicity conditions can be used to find recurrence relations on the Fourier coefficients as above.

To flesh this out, we need to make the choices explicit. Choose $L_1 = \Omega\mathbb{Z}^g$ and $L_2 = D\mathbb{Z}^g$ where Ω is a matrix in the Siegel upper half space (the set of symmetric matrices with positive definite imaginary part). Then $L = L_1 \oplus L_2$ is our lattice. Let $V_i = \mathbb{R}L_i$. Then $V = \mathbb{C}^g = V_1 \oplus V_2$ is a decomposition into real subspaces. Let H, B be Hermitean and symmetric forms represented by the same matrix

$$H(u,v) = u^T (Im\Omega)^{-1}\bar{v}$$

$$B(u,v) = u^T (Im\Omega)^{-1} v$$

Since V_2 consists of real vectors, the difference $(H - B)(u, v) = 0$ when $v \in V_2$. We choose the unique semicharacter α so that it is trivial on each basis vector of L. We define the *classical system of multipliers* by

$$\begin{aligned}\psi_\lambda(z) &= \alpha(\lambda)\exp(\pi(H-B)(z,\lambda) + \frac{\pi}{2}(H-B)(\lambda,\lambda)) \\ &= \phi_\lambda(z)\underbrace{\exp(\frac{\pi}{2}B(z,z))\exp(\frac{\pi}{2}B(z+\lambda,z+\lambda))^{-1}}_{\text{coboundary}}\end{aligned}$$

The main advantage of this is that $\psi_\lambda(z) = 1$ when $\lambda \in L_2$ by the previously stated properties of α and $H - B$. It follows that a theta function for ψ_λ can be expanded as Fourier series

$$f(z) = \sum_{\lambda \in L_2} a_\lambda \exp(2\pi i z \cdot \lambda)$$

The remaining conditions

$$f(z+\lambda) = \psi_\lambda(z) f(z), \quad \lambda \in L_1$$

yield recurrence relations which show that the coefficients are determined by $a_{(n_1,n_2,\ldots)}$ with $0 \le n_i < d_i$ (cf [BL, p 51]). Moreover, it can be shown that these formal solutions converge and are independent. When $D = I$, there is exactly one solution up to scalars, and this is the Riemann theta function. □

In fancier language, the expression $\sqrt{\det E}$ can be identified with the Chern number $\frac{1}{g!}c_1(\mathcal{L}(H,\alpha)^g$. In this form, the theorem can be understood as a special case of the Hirzebruch-Riemann-Roch theorem when combined with Kodaira's vanishing theorem. Of course, this is much less elementary.

2.5 Lefschetz's embedding theorem

Let $X = V/L$ be an abelian variety. Our goal is to construct a projective embedding as we said we would. Actually, the result is a bit stronger. Let H denote a *polarization*. Choose a semicharacter α as lemma 2.3.1. Then Lefschetz showed, in modern language that $\mathcal{L}(nH, \alpha^n)$ is very ample when $n \ge 3$. Let us spell this out. The space of theta functions $\mathcal{L}(nH, \alpha^n)(X)$ is nonzero and finite dimensional by the previous theorem. Let $f_0, \ldots, f_N$ be a basis. By quasiperiodicity the map $V \dashrightarrow \mathbb{P}^N$ sending $x \to [f_0(x), \ldots, f_N(x)]$ descends to a map $\iota : X \dashrightarrow \mathbb{P}^N$. The dotted arrow indicates that the domain need not, a priori, be all of X. It consists of the points where $f_i(x)$ are not all simultaneously 0.

Theorem 2.5.1 (Lefschetz)**.** *When $n \ge 3$, the above map ι is defined on all of X and it yields an embedding as a submanifold.*

The key is that given $a \in V$, we have an automorphism $T : X \to X$ given by translation $x \mapsto x + a$ which acts on everything.

Lemma 2.5.2. *If $f \in \mathcal{L}(H,\alpha)$, then $(T_a^* f)(z) = f(z+a)$ lies in $\mathcal{L}(H, \alpha \cdot \exp(E(a,-))$.*

Proof. [BL, 2.3.2]. □

We will sketch the proof of the theorem when $n = 3$. Here is the first step:

Lemma 2.5.3. *The map ι is defined on all of X.*

Proof. We know by Frobenius' theorem that there exists a nonzero function $\theta \in \mathcal{L}(H,\alpha)(X)$. Given $a, b \in V$, let

$$\theta_{ab}(x) = \theta(x+a+b)\theta(x-a)\theta(x-b)$$

By the previous lemma, this lies in $\mathcal{L}(3H, \alpha^3)(X)$. Now fix $x \in V$. Since $\theta \neq 0$, it follows that $\theta(x-a) \neq 0$ for almost all $a \in V$. Thus $\theta_{ab}(x) \neq 0$ for some a, b. This proves the assertion. □

Proposition 2.5.4. *The map ι is injective.*

Proof. We outline the proof and refer to [BL, §4.5] for details. It is convenient to rephrase the problem in more geometric language. A divisor is a formal linear combination of hypersurfaces in X. Given a nonzero theta function f, its zero set $D = Z(f)$ defines a divisor in X. The divisor of $T_a^* f$ is just the divisor D translated by $-a$. We denote this by $T_a^* D$ for consistency. It follows that

(*) $b \in T_a^* D$ if and only $f(b+a) = 0$ if and only $a \in T_b^* D$.

Let $\theta \in \mathcal{L}(H,\alpha)(X)$ and $\theta_{a,b}$ be as above. Let Θ be the divisor of θ. Then the divisor of $\theta_{a,b}$ is

$$\Theta_{a,b} = T_{a+b}^* \Theta + T_{-a}^* \Theta + T_{-b}^* \Theta$$

The key fact we need is that if $\theta \in \mathcal{L}(H,\alpha)$ is chosen generically, then $T_a^* \Theta \neq \Theta$ only unless $a = 0$ [loc. cit.].

Suppose $x, y \in X$ are distinct points. In the language of divisors we have to show that there that there exists a divisor of a function in $\mathcal{L}(3H, \alpha^3)(X)$ containing x but not y. In fact, we show that exists a, b such that $x \in \Theta_{ab}$ but $y \notin \Theta_{ab}$. Suppose not, then $x \in \Theta_{ab} \Leftrightarrow y \in \Theta_{ab}$ for all a, b.

Claim: $x \in T_{-a}^* \Theta \Leftrightarrow y \in T_{-a}^* \Theta$ for all a.

If $x \in T_{-a}^* \Theta$ then $x \in \Theta_{ab}$ for all b. So $y \in \Theta_{ab}$ for all b. This is possible only if $y \in T_{-a}^* \Theta$. The other direction is identical. So the claim is proved.

By the earlier remark (*), the claim can be stated as $-a \in T_x \Theta \Leftrightarrow -a \in T_y^* \Theta$ Therefore $T_x^* \Theta = T_y^* \Theta$ or equivalently $T_{x-y}^* \Theta = \Theta$. Thus $x = y$, which is a contradiction.

□

Although this proves that ι is a set theoretic embedding, the theorem actually asserts that it is a closed immersion or equivalently that derivative is nowhere zero. This can be proved in a very similar way. See [BL, §4.5].

Corollary 2.5.5. *An abelian variety is a projective algebraic variety.*

Proof. This follows from Chow's theorem stated earlier. □

As we remarked earlier. Conversely, if a complex torus X embeds into projective space $X \subset \mathbb{P}^N$, the restriction of the canonical generator of $H^2(\mathbb{P}^N, \mathbb{Z}) = \mathbb{Z}$ can be interpreted as polarization on X. Thus we arrive at a geometric characterization of abelian varieties:

Theorem 2.5.6. *A complex torus is an abelian variety if and only if it is a projective algebraic variety.*

In the purely algebraic theory of abelian varieties [M], the conclusion of this theorem is taken as the definition. More precisely, an abelian variety over a field k, is defined as a projective variety over k which also has a group structure such that the group operations are morphisms of algebraic varieties.

Chapter 3

The endomorphism algebra

3.1 Poincaré reducibility

A *homomorphism* between abelian varieties $f : V/L \to W/M$ is given by a $\mathbb{C}$-linear map $F : V \to W$ such that $F(L) \subseteq M$. A homomorphism f is called an *isogeny* if F is an *isomorphism*, and an isomorphism if in addition $F(L) = M$. Isomorphisms are always bijections, while isogenies a finite to one surjections. For example, multiplication by a nonzero integer $n : V \to V$ induces an isogeny, which is not an isomorphism unless $n = \pm 1$. Two abelian varieties X and Y are called isogenous if there exists an isogeny from X to Y.

Lemma 3.1.1. *This is an equivalence relation.*

We give two proofs.

Proof 1. We prove symmetry which is the only nonobvious assertion. If $f : V/L \to W/M$ is isogeny, then $F(L) \subseteq M$ is a finite index subgroup. It follows that $nM \subset F(L)$ for some $n \gg 0$. Therefore nF^{-1} induces an isogeny in the opposite direction. □

For the second proof, we start by interpreting isogeny in a fancier way. The collection of abelian varieties and homomorphisms forms an additive category $AbVar$. We can form a new category $AbVar_{\mathbb{Q}}$ with the same objects but with morphisms given by $Hom_{\mathbb{Q}}(X, Y) = Hom(X, Y) \otimes \mathbb{Q}$. We also set $End(X) = Hom(X, X)$ and $End_{\mathbb{Q}}(X) = End(X) \otimes \mathbb{Q}$. These are both rings. The last lemma is now an immediate consequence of the observation:

Lemma 3.1.2. *Two abelian varieties are isogenous if and only if they are isomorphic in $AbVar_{\mathbb{Q}}$.*

Corollary 3.1.3. *$End_{\mathbb{Q}}(X)$ depends only on the isogeny class of X.*

Theorem 3.1.4 (Poincaré)**.** *If $X \subset Y$ is an injective homomorphism of abelian varieties, then Y is isogenous to a product X with another abelian variety.*

Proof. Suppose that $Y = V/L$ then $X = W/L \cap W$ for some subspace $W \subset V$ Let $W^{\perp}$ be the orthogonal complement with respect to a polarization H. Then this is also the orthogonal complement with respect to $E = ImH$. Therefore $L \cap W^{\perp}$ has maximal rank. The torus $Z = W^{\perp}/L \cap W^{\perp}$ is an abelian variety polarized by the restriction of H. The identity map $W \oplus W^{\perp} = V$ defines an isogeny $X \times Z \to Y$. □

An abelian variety is *simple* if it contains no nontrivial abelian subvarieties.

Corollary 3.1.5. *An abelian variety is isogenous to a product of simple abelian varieties.*

We turn now to the structure of the endomorphism ring $End_{\mathbb{Q}}(X)$. This is a standard argument in representation theory.

Theorem 3.1.6. *If X is simple, then $End_{\mathbb{Q}}(X)$ is a finite dimensional division algebra over $\mathbb{Q}$. In general, $End_{\mathbb{Q}}(X)$ is a product of matrix algebras over finite division algebras over $\mathbb{Q}$.*

Proof. The finite dimensionality is clear from construction, since $End_{\mathbb{Q}}(X) \subset End(L \otimes \mathbb{Q})$ where L is the lattice. Suppose that $f \in End_{\mathbb{Q}}(X)$ is nonzero. We have to show that f has an inverse. After replacing f by nf, we can assume that it is a homomorphism $f : X \to X$. It is enough to show that it is an isogeny. Since $f(X) \subset X$ is nonzero abelian subvariety, it follows that $f(X) = X$. Consider $\ker(f) \subset X$. It must be finite, since otherwise the connected component of the identity would give a nonzero abelian subvariety.

For the second statement, we can can assume that $X = \prod X'_i$ where X'_i simple. We can arrange this as $X = \prod X_i^{n_i}$ where X_i and X_j are nonisogenous when $i \neq j$. Then a morphism from $f : X_i \to X_j$ is trivial by the same argument as above. We have $ker(f) \otimes \mathbb{Q} = 0$ and that either $f(X_i)$ is 0 or X_j. The last case is impossible because X_i and X_j are not isogenous. Let $D_i = End_Q(X_i)$. Then

$$End_{\mathbb{Q}}(X) = \prod Hom(X'_i, X'_j) = \prod Mat_{n_i \times n_i}(D_i)$$

□

3.2 The Rosati involution

There is an extra bit of structure which will be play a very important role. Given an algebra R over a field. An involution is a map $r \mapsto r^*$ which is linear over the field, such that $(rs)^* = s^* r^*$. For example, transpose gives an involution of on the algebra of matrices.

Let $X = V/L$ be an abelian variety with polarization H. The adjoint with respect to H:

$$H(Ax, y) = H(x, A^* y)$$

defines an involution on $End(V)$. The algebra $End_{\mathbb{Q}}(X)$ sits naturally inside this. It can be identified with the endomorphisms which preserve the rational lattice $L_{\mathbb{Q}} = L \otimes \mathbb{Q}$.

Theorem 3.2.1. *The subring $End_{\mathbb{Q}}(X) \subset End(V)$ is stable under the involution $*$.*

Proof. If $A \in End(L_{\mathbb{Q}})$ define $A^{\dagger} \in End(L_{\mathbb{Q}})$ to be the adjoint with respect to $E = ImH$ i.e. $E(Ax, y) = E(x, A^{\dagger}y)$. This is defined because E is nonsingular. Given $A \in End_{\mathbb{Q}}(X)$, it preserves $L_{\mathbb{Q}}$, so we can form $A^{\dagger} \in End(L_{\mathbb{Q}})$. This coincides with the usual adjoint $A^* \in End(V)$ because $ImH(Ax, y) = ImH(x, A^*y)$. Therefore A^* preserves the rational lattice $L_{\mathbb{Q}}$, and thus defines an element of $End_{\mathbb{Q}}(X)$. □

The restriction of $*$ to $End_{\mathbb{Q}}(X)$ is called the *Rosati involution*. Although the construction would seem to be based on a linear algebra trick, there is a way to make it more geometric. The map $v \mapsto H(v, -)$ induces an isogeny ϕ_H between X and its dual $\hat{X} = V^*/L^*$ introduced earlier. Thus we have an isomorphism $\Phi : End_{\mathbb{Q}}(X) \cong End_{\mathbb{Q}}(\hat{X})$. This can be realized geometrically by identifying $Pic^0(X) = \hat{X}$. Then we have

Proposition 3.2.2. *If $L = \mathcal{L}(H, \alpha)$ for some semicharacter α, then $\phi_H(x) = T_x^* L \otimes L^{-1} \in \hat{X}$.*

Proof. [BL, M]. □

An endomorphism $A : X \to X$ induces a dual endomorphism $\hat{A} : \hat{X} \to \hat{X}$, which can be identified with the map $Pic^0(X) \to Pic^0(X)$ given by $M \mapsto A^*M$. This can be defined for $A \in End_{\mathbb{Q}}(X)$ by extension of scalars. Then $A^* \in End_{\mathbb{Q}}(X)$ is $\Phi^{-1}(\hat{A})$.

Given any finite dimensional $\mathbb{Q}$-algebra R, and element r defines a vector space endomorphism of R by left multiplication. This is the so called regular representation. Thus we have a well defined trace $Tr(r) \in \mathbb{Q}$. An involution $*$ on R is called *positive* if $Tr(r^*r) > 0$ when $r \neq 0$. Transpose on the algebra of matrices has this property.

Theorem 3.2.3. *The Rosati involution is positive.*

3.3 Division rings with involution

In the first chapter, we showed that $End_{\mathbb{Q}}$ of an elliptic curve was either $\mathbb{Q}$ or an imaginary quadratic field. In higher dimensions, things are more complicated, but that they can be understood. Given a simple abelian variety X, $End_{\mathbb{Q}}(X)$ is a finite dimensional division algebra with a positive involution. Our goal is to describe all such rings with involution. Over $\mathbb{R}$, things are much are easier. There are only two (finite dimensional) division algebras over it the complex numbers $\mathbb{C}$ and the quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with $i^2 = j^2 = -1$ and $ij = -ji = k$. Both of these algebras have a positive involution given by ordinary complex conjugation and quaternionic conjugation $(x+yi+zj+wk)^* = x-yi-zj-wk$. The construction of quaternions can be generalized to an algebra H' by replacing $\mathbb{R}$ by an arbitrary field F, and by modifying the relations to

$i^2 = a$, $j^2 = b$ and $ij = -ji = k$ for $a, b \in F$. There are two possibilities, either H' is a division algebra, or it is the algebra of 2×2 matrices. The latter happens precisely when $ax^2 + bx^2 = 1$ has a solution over F. For an explicit example, choose $a = b = 1$. Then $H' \cong Mat_{2\times 2}(F)$ by

$$i \mapsto \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Over $\mathbb{Q}$, there are 4 types division algebras with positive involution (written out of order).

Type I. A totally real number field F is a finite extension of $\mathbb{Q}$ such any embedding $F \subset \mathbb{C}$ lies in $\mathbb{R}$. For example the real quadratic field $\mathbb{Q}(\sqrt{d}), d > 0$, is totally real. We give this the trivial involution $x^* = x$.

Type III. A division algebra of type III is a division algebra D over a totally real number field F such that $D \otimes_F \mathbb{R} \cong \mathbb{H}$, as algebras, for every embedding of $F \subset \mathbb{R}$. Under this isomorphism the given involution should map to conjugation. For example, we could take a quaternion algebra with $i^2 = a, j^2 = b$, and $a, b \in F$ totally negative.

Type II. This is division algebra D over a totally real number field F such that $D \otimes_F \mathbb{R} \cong Mat_{2\times 2}(\mathbb{R})$ for every embedding. Here $Mat_{2\times 2}$ is algebra of 2×2 matrices. The involution is conjugate to the transpose on the matrix algebra.

Type IV. A CM field is a quadratic extension F of a totally real field K such that no embedding of $F \subset \mathbb{C}$ lies in $\mathbb{R}$. For example, an imaginary quadratic field is CM. A division algebra D of type IV is a division algebra whose centre is a CM field F. For every embedding $F \subset \mathbb{C}$, $D \otimes_F \mathbb{C} \cong Mat_{d\times d}(\mathbb{C})$, for some d, and the involution corresponds to conjugate transpose.

One way to distinguish the cases II and III is in terms of the Brauer group. The set of isomorphism classes of finite dimensional division algebras with centre F form a group called the Brauer group $Br(F)$. The identity of $Br(F)$ is simply F. Alternatively, we can take $Br(F)$ to be the set matrix algebras over division algebras modulo the relation that two algebras are equivalent if the underlying division algebras are the same. The second description is better because the class of matrix algebras is stable under various operations such as tensor product or extension of scalars. In particular, given a field extension $F \subset F'$ we have a map $Br(F) \to Br(F')$ given by $D \mapsto F' \otimes_F D$. We note that the $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ with the generator given by $\mathbb{H}(\mathbb{R})$.

Then to summarize briefly:

Type I A totally real field.

Type II A quaternion algebra D which is totally indefinite in the sense that it lies in the kernel of $Br(F) \to Br(\mathbb{R})$ for every embedding of $F \subset \mathbb{R}$.

Type III A quaternion algebra D which is totally definite which mean that it never lies in the kernel of $Br(F) \to Br(\mathbb{R})$

Type IV An algebra over a CM field.

Theorem 3.3.1 (Albert)**.** *The set of finite dimensional division algebras over $\mathbb{Q}$ with a positive involution are exactly the ones described above.*

Proof. [BL, M]. ☐

So we deduce

Corollary 3.3.2. *The endomorphism algebra of a simple abelian variety must be one of the above 4 types; the abelian variety is labelled accordingly.*

We will see later that all of the categories I-IV occur for abelian varieties, and almost all of the subcases. The idea is easy to explain for elliptic curves.. In theorem 1.2.4, we saw that an elliptic curve $E = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$ has either $End_{\mathbb{Q}}(E) = \mathbb{Q}$ (special case of type I) or $End_{\mathbb{Q}}(E)$ imaginary quadratic (special case of type IV). Furthermore, in the second case, $End_{\mathbb{Q}}(E) = \mathbb{Q}(\tau)$. The converse is simple.

Lemma 3.3.3. *Given $\mathbb{Q}$ or an imaginary quadratic field, it arises as above.*

Proof. To build an elliptic curve with E with $End_{\mathbb{Q}}(E) = \mathbb{Q}(\sqrt{-d})$ we can use $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\sqrt{-d}$. For $End_{\mathbb{Q}}(E) = \mathbb{Q}$, suffices to take $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ with $\mathbb{Q}(\tau)$ not imaginary quadratic. For example, we can take τ transcendental. ☐

It is clear that "most" E have $End_{\mathbb{Q}}(E) = \mathbb{Q}$. Making this idea work in higher dimensions will require some understanding of moduli spaces.

Chapter 4

Moduli spaces

4.1 Moduli of elliptic curves

Our goal is to describe all elliptic curves up to isomorphism. This is equivalent to describing all lattices in $\mathbb{C}$ up to multiplication by a nonzero scalar; or all based lattices modulo scalars and change of bases. We can form the set

$$B = \left\{ \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2 \mid \omega_i \text{ are } \mathbb{R}\text{-linear independent} \right\}$$

of based lattices. We have $GL_2(\mathbb{Z})$ acting on the left, and $t \in \mathbb{C}^*$ on the right by

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \mapsto \begin{pmatrix} t\omega_1 \\ t\omega_2 \end{pmatrix}$$

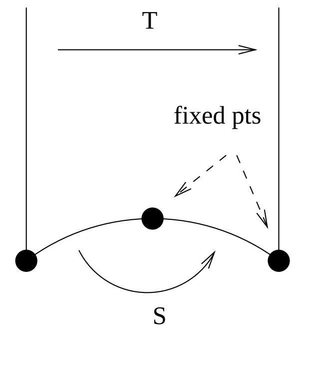
We observe that B has two connected components $B^{\pm}$ corresponding to whether $\tau = \omega_1/\omega_2$ is in the upper or lower half plane. We can simplify our task by restricting B^+ and its stabilizer $SL_2(\mathbb{Z})$. Then we can identify $B^+/\mathbb{C}^*$ with the upper half plane H $SL_2(\mathbb{Z})$-equivariantly. The action of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on H is given by

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}$$

Thus the quotient space $A_1 = SL_2(\mathbb{Z})\backslash H$ is what we are after. Since the $-I$ acts trivially, we can factor it out can view $A_1 = PSL_2(\mathbb{Z})\backslash H$. We refer to A_1 as the *moduli space of elliptic curves*, although at the moment it is just a set.

Theorem 4.1.1. *$SL_2(\mathbb{Z})$ is generated by the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The region $D = \{z \mid |z| \geq 1, |Re(z)| \leq \frac{1}{2}\}$ is a* fundamental domain *for the action i.e. all points in H lie in the orbit of a point of D and the orbits of the interior of D are disjoint.*

From this, we see that the quotient A_1 carries a reasonable topology obtained by identifying the sides of the domain D as indicated in the picture.



The quotient A_1 can actually be identified with $\mathbb{C}$. The can be done using the j-function. Given an elliptic curve E in Weirstrass form $y^2 = 4x^3 - g_2x - g_3$, the j-invariant

$$j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

The strange normalization is explained by setting $j(\tau) = j(\mathbb{C}/\mathbb{Z} + \tau)$ then expanding

$$j(\tau) = \frac{1}{\exp(2\pi i\tau)} + 744 + \dots$$

we see that the leading coefficient is 1. As a function of τ, it is invariant under $PSL_2(\mathbb{Z})$ by the way defined it.

Theorem 4.1.2. *The j-function yields a bijection $PSL_2(\mathbb{Z})\backslash H \cong \mathbb{C}$.*

Proof. [Se] □

4.2 Moduli functors

We now we have a set A_1 of isomorphism classes of elliptic curves, although this is hardly saying anything, since any two sets with same cardinality are in bijection. The key property was discovered rather late in the game by Grothendieck and Mumford. It involves changing to a more abstract viewpoint. A family of elliptic curves over a complex manifold T, is a proper holomorphic map $f : \mathcal{E} \to T$ with a section $o := T \to \mathcal{E}$ such that every fibre $\mathcal{E}_t = f^{-1}(t)$ is an elliptic curve with $o(t)$ as its origin. A product of T with an elliptic curve would give a family called a trivial family. The space

$$\mathcal{E}(\infty) = \{(\tau, x) \mid \tau \in H, x \in \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau\} \tag{4.1}$$

with its projection gives a nontrivial family of elliptic curves over the upper half plane H. Let $Ell(T)$ denote the set of isomorphisms classes of such families.

Given a holomorphic map $f : S \to T$ and $\pi : \mathcal{E} \to T \in Ell(T)$, we obtain a new family $f^*\mathcal{E} \in Ell(S)$ given by

$$f^*\mathcal{E} = \{(s, x) \in S \times \mathcal{E} \mid f(s) = \pi(x)\}$$

Given a third map $g : Z \to S$, we have $g^* f^* \mathcal{E} \cong (f \circ g)^* \mathcal{E}$. Thus Ell gives a contravariant functor from the category of complex manifolds to sets.

We can now spell out the universal property that we would like to hold. A *fine* moduli space of elliptic curves is a complex manifold M with $\mathcal{U} \in Ell(M)$ which is universal in the sense that for any manifold T and $\mathcal{E} \in Ell(T)$, there exists a unique map $f : T \to M$ such that $f^*\mathcal{U} \cong \mathcal{E}$. An equivalent way to express this is:

Lemma 4.2.1. *M is a fine moduli space for elliptic curves if and only if there is a natural isomorphism*

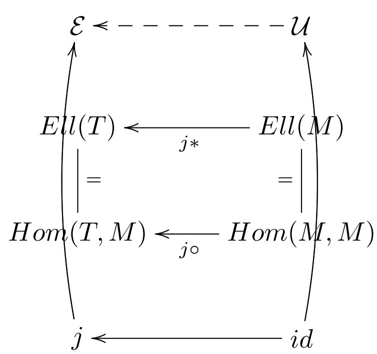
$$Ell(T) \cong Hom(T, M)$$

where the right side denotes the set of holomorphic maps from T to M. One also says that Ell is representable *by M.*

The result is an entirely formal result in category theory called Yoneda's lemma.

Proof. If M was fine, then $f \in Hom(T, M) \mapsto f^*\mathcal{U} \in Ell(T)$ is a natural isomorphism by definition.

Conversely, suppose that there was a natural isomorphism $Ell(T) \cong Hom(T, M)$. Let $\mathcal{U} \in Ell(M)$ denote the image of the identity $id \in Hom(M, M)$. Suppose that $\mathcal{E} \in Ell(T)$. Then it corresponds to $j \in Hom(T, M)$. Chasing the diagram



shows that $j^*\mathcal{U} = \mathcal{E}$. This shows that it is universal. $\square$

The property of being a fine moduli space characterize the space up to isomorphism. So there can be at most one. Now for the bad news

Lemma 4.2.2. *A fine moduli space for elliptic curves does not exist.*

Proof. If such a space existed, we would have to have $M \cong A_1$ an f would just be the function $t \mapsto j(\mathcal{E}_t)$. The bad news, is that there is no fine moduli space because there are curves such as $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}i$ with extra automorphisms. To see this, observe that existence of a universal family would imply that any family with constant j-function would be trivial. However, if the generator $\sigma \in \mathbb{Z}/4\mathbb{Z}$ acts by multiplication by (i, i) on $\mathbb{C}^* \times E$, then quotient would give a nontrivial family over $\mathbb{C}^*/\sigma$ with constant j-function. □

We have to settle for a weaker property. A *coarse* moduli space of elliptic curves is a complex manifold M with a morphism of functors $J : Ell(T) \to Hom(T, M)$, which is universal in a suitable sense[1], and induces a bijection when T is a point.

Lemma 4.2.3. *$A_1 = \mathbb{C}$ is the coarse moduli space of elliptic curves.*

Indeed given $\mathcal{E} \in Ell(T)$, we get holomorphic map $T \to \mathbb{C}$ given by $t \mapsto j(\mathcal{E}_t)$. This induces a bijection with $Ell(point)$ as we have seen.

4.3 Level structure

For some purposes, the coarse moduli property is too weak. There are a couple of ways to fix this. The first method is consider instead of just $Ell(T)$, elliptic curves with enough extra structure to kill the automorphism group. For example, we can consider elliptic curves together with a basis of first homology. Then H is the fine moduli space, with universal family given by (4.1). However H lies outside of the realm of algebraic geometry. It is more convenient to use a basis modulo $n \gg 0$ (actually $n > 2$ is enough). This is referred to as level n structure. More explicitly, if $E = \mathbb{C}/L$, then the

$$H_1(E, \mathbb{Z}/n\mathbb{Z}) \cong \frac{1}{n}L/L \cong n\text{-torsion of } E$$

So a level n-structure can be understood as a basis for the n-torsion points as an $\mathbb{Z}/n\mathbb{Z}$-module. Obviously the set $\{1/n, \tau/n\}$ gives a level n-structure for the curve $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$. The principal congruence subgroup $\Gamma(n) = \ker[SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})]$ preserves this structure. We define the *modular curve* $Y(n) = \Gamma(n)\backslash H$. The points correspond to elliptic curves with level n-structure. We have map $Y(n) \to A_1$, induced by the inclusion of groups $\Gamma(n) \subset SL_2(\mathbb{Z})$, which is finite to one. This corresponds to forgetting the level structure. This can be used to show that $Y(n)$ is an affine algebraic curve. The coordinate ring can be described using modular forms.

From the group theory perspective, the fact that A_1 is not a fine moduli space is related to the fact that $SL_2(\mathbb{Z})$ acts on H with fixed points, namely the $i, \exp(2\pi i/3)$ and their orbits.

[1]Any other natural transformation $Ell(T) \to Hom(T, N)$ must be induced by a unique holomorphic $M \to N$.

Proposition 4.3.1. *When $n > 2$, $\Gamma(n)/\{\pm I\}$ is torsion free.*

Proof. See [Se]. □

Corollary 4.3.2. *$\Gamma(n)/\{\pm I\}$ acts on H without fixed points.*

Proof. The isotropy group of any fixed point would consist of torsion elements. □

Given $A_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in SL_2(\mathbb{Z})$, we let it act on $H \times \mathbb{C}$ by

$$(\tau, z) \mapsto (\frac{a_i\tau + b_i}{c_i\tau + d_i}, (c_i\tau + d_i)^{-1}z)$$

A calculation shows that

$$\begin{aligned} A_1(A_2(\tau; z)) &= (A_1A_2 \cdot \tau; [(c_1a_2 + d_1c_2)\tau + (c_1b_2 + d_1d_2)]^{-1}z) \\ &= (A_1A_2)(\tau, z) \end{aligned}$$

as required. The group $\mathbb{Z}^2$ acts on $H \times \mathbb{C}$ by $(\tau, z) \mapsto (\tau, z + m + n\tau)$. The quotient $\mathcal{E}(\infty) = H \times \mathbb{C}/\mathbb{Z}^2$ is the same space described in (4.1). We claim that the action of $SL_2(\mathbb{Z})$ given above induces a well defined action on $\mathcal{E}(\infty)$. This follows from the next lemma and some calculation.

Lemma 4.3.3. *Suppose that H, G are groups acting on X such that for all $g \in G, h \in H$, there exist $h' \in H$ for which $ghx = h'gx$ for all $x \in X$. Then G induces an action on X/H.*

Let $\mathcal{E}(n)$ be the quotient of $\mathcal{E}(\infty)$ by the action of $\Gamma(n)$. Alternatively, we can do this in one step by defining action of the semidirect product and then taking the quotient

$$\mathcal{E}(n) = (\Gamma(n) \ltimes \mathbb{Z}^2)\backslash H \times \mathbb{C} \to Y(n)$$

This is a family of elliptic curves over $Y(n)$ when $n > 2$. This has a pair of sections $1/n, \tau/n$ which give a level n-structure on the fibres.

Theorem 4.3.4. *Let $n > 2$, then $\mathcal{E}(n)$ is a universal family of elliptic curves over $Y(n)$. Therefore $Y(n)$ is a fine moduli space for elliptic curves with level n structure.*

Sketch. Suppose that $\mathcal{E} \to T$ is a family of elliptic curves with level n-structure. This gives a basis for $H_1(\mathcal{E}_t, \mathbb{Z}/n\mathbb{Z})$ which varies continuously with t. In general, there is no way to extend this to basis of $H_1(\mathcal{E}_t, \mathbb{Z})$ because the so called monodromy representation of $\rho : \pi_1(T, t) \to Aut(H^1(\mathcal{E}_t, \mathbb{Z}))$ may be nontrivial. However, we can find a such an extension for the pull back $\tilde{\mathcal{E}}$ of $\mathcal{E}$ to the universal cover $\tilde{T} \to T$. This determines a map $p : \tilde{T} \to H$ such that $\tilde{E} = p^*\mathcal{E}(\infty)$. The map can be assumed to be equivariant in the sense that $\gamma t = \rho(\gamma)p(t)$. Note that by assumption the image of ρ lies in $\Gamma(n)$. Thus p descends to map $q : T \to \Gamma(n)\backslash H = Y(n)$ such that $\mathcal{E} = q^*\mathcal{E}(n)$. □

4.4 Moduli stacks

If we identify $A_1 = PSL_2(\mathbb{Z}/n\mathbb{Z})\backslash Y(n)$ but keep track of the fixed points and their isotropy groups, we get the notion of an *orbifold*. A related but more general notion was given by Deligne and Mumford [DM]; it is now known as Deligne-Mumford or DM *stack*. The precise definition is extremely technical, so we will just try to convey the basic idea. (A detailed reference with proofs is [LM].) Let us describe what is in some sense the prototypical example of the quotient of a complex manifold M by a finite group G of holomorphic automorphisms. We denote the quotient stack by $[G\backslash M]$ to distinguish it from the usual quotient $G\backslash M$. A point of $G\backslash M$ is just a G-orbit of an $x \in M$. While a point of $[G\backslash M]$ would be a G-orbit together with its isotropy group G_x. Clearly it is more than a set. The most convenient way to encode this information is in terms of groupoids. A groupoid is a category where all the morphisms are invertible. For example, a set can be regarded as a groupoid in which the only morphisms are the identities. However, groupoids are more general. To each object x of a groupoid, one can attach the isotropy group $G_x = Hom(x, x)$. The groupoid is equivalent, in the sense of category theory, to a set if and only if all the isotropy groups G_x are trivial. Yoneda's lemma (cf 4.2.1), says that a complex manifold M is determined by the functor $T \mapsto Hom(T, M)$ on the category of complex manifolds. So to understand what $[G\backslash M]$ is, we should describe the holomorphic maps to it from any manifold T. However, $Hom(T, [G\backslash M])$ is a groupoid rather than just a set:

$$
\begin{aligned}
Objects &= \{T \xleftarrow{f} \tilde{T} \xrightarrow{p} M \mid \tilde{T} \text{ is a manifold with a free } G\text{-action,} \\
&\qquad \text{and } p \text{ is equivalent and holomorphic}\}
\end{aligned}
$$

$$
Morphisms = \left\{ \begin{array}{ccc} \tilde{T} & \longrightarrow & M \\ \downarrow & \searrow^{\cong} & \uparrow \\ T & \longleftarrow & \tilde{T}' \end{array} \right\}
$$

So we can identify $[G\backslash M]$ with the groupoid valued functor given above. Note that we are suppressing some technicalities here; this is not quite a functor but rather a pseudo-functor. Alternatively, this can be understood in the language of fibered categories, which is explained in the previous references.

At first, $[G\backslash M]$ looks like a strange beast. So let us consider some special cases. When G is trivial, $[M] = [\{1\}\backslash M]$ is nothing but the functor represented by M, so essentially $M = [M]$ by Yoneda's lemma. Next suppose that G is nontrivial, but that the action is free. Then $G\backslash M$ has the structure of complex manifold. Given a map $f : T \to G\backslash M$, the fibre product $\tilde{T} = T \times_{G\backslash M} M$ gives an element of $[G\backslash M]$. In fact, $[G\backslash M]$ is equivalent to the functor represented by $G\backslash M$ in this case. In general, however, $[G\backslash M]$ should be thought of as a kind of idealized quotient; it is usually a richer invariant than the quotient space. This is clear in the extreme example, where $M = pt$ consists of a single point. The functor represented by pt is trivial. Whereas the stack $BG := [G\backslash pt]$ is not. $Hom(T, BG)$ consists of all possibly disconnected G-coverings of T.

The class of quotient stacks $[G\backslash M]$ is too restrictive for many purposes. For example, the disjoint union $[G_1\backslash M_1]\coprod[G_2\backslash M_2]$ is usually not a quotient by any group. It is however a quotient of $M_1\coprod M_2$ by a groupoid. To elaborate, a groupoid in the category of complex manifolds consists of manifold M of "objects", a manifold R of "morphisms" and various holomorphic structure maps: source $s : R \to M$, target $t : R \to M$, composition $R \times_{s,M,t} R \to R$ etc[2]. If a group G acts on M we can form a groupoid $R = G \times M$ with s, t given by the projection and action maps. The group law determines the remaining maps. We can modify this to handle the previous example by taking the groupoid $R = G_1 \times M_1 \coprod G_2 \times M_2$. We have now almost arrived at the notion of a DM stack in general. An analytic DM stack is determined by a groupoid in the category of complex manifolds such that s, t are finite unramified coverings. To complete the picture, we should say in what sense the stack is determined by the groupoid, or equivalently when do two groupoids yield the same stack? This part of the story is somewhat technical, and so we give the broad outline, referring to the above references for precise details. As above, we may view a stack as a groupoid valued functor or more accurately pseudo-functor, on the category of manifolds. It is clear that given an analytic groupoid $\mathcal{G} = (M, R, \ldots)$, we get a such a functor $T \mapsto \text{pre-Stk}_{\mathcal{G}}(T) = (Hom(T, M), Hom(T, R), \ldots)$. However, when applied to the groupoid $(M, G \times M, \ldots)$, this will not give us $[G\backslash M]$. There is an extra step, analogous to sheafication, that needs to be performed on pre-$\text{Stk}_{\mathcal{G}}$ before we get the correct groupoid valued functor, i.e. the actual stack $\text{Stk}_{\mathcal{G}}$. In particular, two analytic groupoids $\mathcal{G}, \mathcal{G}'$ give the same stack, if $\text{Stk}_{\mathcal{G}}$ and $\text{Stk}_{\mathcal{G}'}$ are equivalent.

Returning to elliptic curves. We define the moduli stack of elliptic curves by $\mathcal{A}_1 = [SL_2(\mathbb{Z}/n\mathbb{Z})\backslash Y(n)]$ for some fixed $n > 2$. Note that n plays an auxillary role.

Proposition 4.4.1. *Given T, $Hom(T, \mathcal{A}_1)$ is the category of all families of elliptic curves and isomorphisms between them.*

Sketch. In one direction, given $T \leftarrow \tilde{T} \to Y(n)$, we can pull $\mathcal{E}(n)$ back to $\tilde{T}$ and quotient out by $SL_2(\mathbb{Z}/n\mathbb{Z})$ to get a family of elliptic curves over T.

Conversely, given a family of elliptic curves $\mathcal{E} \to T$, we have an associated monodromy representation $\rho : \pi_1(T) \to SL_2(\mathbb{Z})$. Let $\rho_n : \pi_1(T) \to SL_2(\mathbb{Z}/n\mathbb{Z}) = G$ denote the induced map, and let N denote the index of $\rho_n(\pi_1(T))$ in G. Let T' denote the cover of T corresponding to $\ker \rho_n$. And let T be the disjoint union of N copies of T'. By identifying T with $(G \times T')/H$, with $h \in H$ acting by $(g, t) \mapsto (gh, h^{-1}t)$, we see that G acts freely on $\tilde{T}$ with T as a quotient. Thus $T \leftarrow \tilde{T} \to Y(n)$ defines an element of $Hom(T, \mathcal{A}_1)$. □

[2]Further conditions need to be imposed to ensure that the fibre product $R \times_{s,M,t} R$ is a manifold, or else one could interpret this as analytic space

A_1 is the closest approximation to $\mathcal{A}_1$ by an ordinary manifold, but for some problems $\mathcal{A}_1$ is the better object. To get a sense of how the difference manifests itself in geometric problems, let us study line bundles on these spaces. On $A_1 \cong \mathbb{C}$, all line bundles are trivial. For $\mathcal{A}_1$, we first need to explain what a line bundle means. Since $\mathcal{A}_1$ is the universal space, any line bundle would pullback to a line bundle on any T equipped with a family of elliptic curves. Conversely, any natural family of line bundles would have to come from $\mathcal{A}_1$. Here is an example. Given a family of elliptic curves $\pi : \mathcal{E} \to T$, the pullback of the relative canonical sheaf $\sigma^*\Omega^{\dim \mathcal{E}}_{\mathcal{E}/T}$ along the zero section yields family of line bundles. By explicit calculation, this is nontrivial for suitable $\mathcal{E} \to T$. Therefore:

Lemma 4.4.2. *$\mathcal{A}_1$ carries a nontrivial line bundle.*

4.5 Moduli space of principally polarized abelian varieties

We want to generalize the construction from elliptic curves to higher dimensions. Recall that the Siegel upper half plane

$$H_g = \{\Omega \in Mat_{g\times g}(\mathbb{C}) \mid \Omega = \Omega^T,\, Im(\Omega) > 0\}$$

This is an open subset of the space of symmetric matrices. So its dimension is $g(g+1)/2$.

Given $\Omega \in H_g$ we can construct a torus $X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$. This carries a principal polarization H_Ω represented by the matrix Ω^{-1}. The associated symplectic form $E = ImH_\Omega$ is the standard one

$$E = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

Thus (X_Ω, H_Ω) is an abelian variety with principal polarization. There is another representation of H_g which is often convenient. Consider the set of $2g \times g$ P_g matrices satisfying the conditions of proposition 1.4.2. Then $M \in Gl_g(\mathbb{C})$ acts by $M \mapsto (MA, MB)$. Matrices of the form (Ω, I) lie in P_g if and only if $\Omega \in H_g$. Therefore we can identify H_g with the quotient of P_g by Gl_g.

Lemma 4.5.1. *Given any g dimensional principally polarized abelian variety (X, H), there exists $\Omega \in H_g$ and an isomorphism $(X, H) \cong (X_\Omega, H_\Omega)$. That is there is an isomorphism of vector spaces, which carries the lattice to the lattice, and H to H_Ω.*

Proof. We apply proposition 1.4.2 to write $X = \mathbb{C}^g$ modulo the lattice generated by the columns of Π as given there. Now do a change of basis to get $\Pi = (\Omega, I)$ for some $\Omega \in H_g$. $\square$

This suggests that the natural moduli problem should involve pairs (X, H). The proposition gives the first step. The next problem is to deal with the nonuniqueness of (X_Ω, H_Ω). A point of H_g gives rise to a polarized abelian variety with a preferred basis (Ω, I) for the lattice. We need to mod out the choice of basis. It is important to restrict to change of bases which are compatible with the polarization. For any commutative ring R (e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) we define the symplectic group

$$Sp_{2g}(R) = \left\{ M \in GL_{2g}(R) \mid M^T \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} M = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \right\}$$

In other words, this is the group of matrices with preserves the symplectic form E.

Lemma 4.5.2. *Given $\Omega \in H_g$ and $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{R})$*

$$(A\Omega + B)(C\Omega + D)^{-1} \in H_g$$

This defines an action of $Sp_{2g}(\mathbb{R})$ on H_g.

Proof. For M as above, one checks the following identities: $A^T C$ and $B^T D$ are symmetric, and $A^T D - C^T B = I$. Let $M(\Omega) = (A\Omega + B)(C\Omega + D)^{-1}$. After expanding, using the above identities, and canceling, we obtain

$$(C\Omega + D)^T (M(\Omega) - M(\Omega)^T)(C\Omega + D) = \Omega - \Omega^T = 0$$

Therefore $M(\Omega)$ is symmetric. Similarly

$$(C\Omega + D)^T Im M(\Omega)(C\Omega + D) = Im\Omega > 0$$

which implies that $M(\Omega)$ is positive definite. □

One can put the Siegel space in the more general framework of symmetric spaces using the following:

Lemma 4.5.3. *The action of $Sp_{2g}(\mathbb{R})$ on H_g is transitive and the stabilizer of iI is*

$$\left\{ \begin{pmatrix} A & B \\ -B & A \end{pmatrix} \mid AB^T = BA^T, AA^T + BB^T = I \right\} \cong U_g(\mathbb{R})$$

where the isomorphism is given by sending

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix} \mapsto A + iB$$

Proof. Let $\Omega = X + iY \in H_g$. Since Y is symmetric and positive definite, we can find an $A \in GL_g(\mathbb{R})$ so that $Y = AA^T$. Then $M = \begin{pmatrix} A & X(A^T)^{-1} \\ 0 & (A^T)^{-1} \end{pmatrix}$ sends iI to Ω. The formula for the stabilizer can be checked by calculation. □

Corollary 4.5.4. *Thus* $H_g \cong Sp_{2g}(\mathbb{R})/U_g(\mathbb{R})$.

We define

$$A_g = Sp_{2g}(\mathbb{Z})\backslash H_g = Sp_{2g}(\mathbb{Z})\backslash Sp_{2g}(\mathbb{R})/U_g(\mathbb{R})$$

An easy modification of previous arguments shows:

Lemma 4.5.5. $X_\Omega \cong X_{\Omega'}$ *if and only if there exists* $M \in Sp_{2g}(\mathbb{Z})$ *with* $\Omega' = M \cdot \Omega$. *In particular,* A_g *can be identified with the set of isomorphism classes of principally polarized abelian varieties.*

At the moment this is just a set. However:

Lemma 4.5.6. *The action of* $Sp_{2g}(\mathbb{Z})$ *is properly discontinuous. Therefore the quotient is a Hausdorff space.*

Proof. Given compact sets $K_1, K_2 \subset H_g$, we have to show that $S = \{M \in Sp_{2g}(\mathbb{Z}) \mid M(K_1) \cap K_2 \neq \emptyset\}$ is finite. Let us identify $H_g = Sp_{2g}(\mathbb{R})/U_g(\mathbb{R})$ as above. Note that the group $U_g(\mathbb{R})$ is compact, so that the projection $p : Sp_{2g}(\mathbb{R}) \to H_g$ is proper. $M \in Sp_{2g}(\mathbb{Z})$ lies in S if and only if $Mp^{-1}K_1 \cap p^{-1}K_2 \neq \emptyset$ if and only if $M \in T = (p^{-1}(K_1))^{-1}p^{-1}(K_2)$. Now T is compact because it is the image of $K_1 \times K_2$ under $(M_1, M_2) \mapsto M_1^{-1}M_2$. Therefore S is the intersection of a compact set with a discrete set, so it's finite. ☐

As in the case of elliptic curves, A_g is only a coarse moduli space. The problem stems from nontrivial automorphisms. The remedy, as before, is to add a level structure. A level n-structure on an abelian variety $A = \mathbb{C}^g/L$ is a choice of symplectic basis

$$H^1(A, \mathbb{Z}/n\mathbb{Z}) \cong Hom(L, \mathbb{Z}/n\mathbb{Z})$$

The key fact is the following

Proposition 4.5.7. *Let* $n \geq 3$. *Suppose that* γ *is an automorphism of a principally polarized abelian variety* (A, H) *which acts trivially on the lattice mod* n. *Then* $\gamma = 1$.

Proof. We assume that $\gamma \neq 1$. Then it has finite order, which we can assume is a prime p, by replacing γ a power. Then by assumption, $1 - \gamma = n\phi$ where $\phi \in End(A)$. Let ζ be a nontrivial eigenvalue of γ, and let η be the corresponding eigenvalue of ϕ. ζ is a primitive pth root of unity and η is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta)$. We have a relation $n\eta = 1 - \zeta$. Taking the norm with respect to $\mathbb{Q}(\zeta)/\mathbb{Q}$ yields an equality of integers

$$n^{p-1}N(\eta) = (1 - \zeta)(1 - \zeta^2) \ldots (1 - \zeta^{p-1}) = p$$

But this impossible because p is prime and $n \geq 3$. ☐

Let

$$\Gamma(n) = \ker[Sp_{2g}(\mathbb{Z}) \to Sp_{2g}(\mathbb{Z}/n\mathbb{Z})]$$

and define

$$A_{g,n} = \Gamma(n)\backslash H_g$$

Lemma 4.5.8. *$A_{g,n}$ can be identified with the set of isomomorphism classes of principally polarized g-dimensional abelian varieties with level n-structure.*

Theorem 4.5.9. *Suppose that $n \geq 3$. Then the action of $\Gamma(n)$ on H_g is fixed point free. Therefore $A_{g,n}$ is a manifold. The semidirect product $\Gamma(n) \ltimes \mathbb{Z}^g$ acts naturally on $H_g \times \mathbb{C}^g$ and the quotient is the universal family of principally polarized g-dimensional abelian varieties with level n-structure. In particular $A_{g,n}$ is a fine moduli space.*

Proof. Suppose that $\gamma \in \Gamma(n)$ fixes a point of $\Omega \in H_g$. Then γ fixes X_Ω with its standard level n-structure. Therefore By proposition 4.5.7 $\gamma = 1$. So the action is free. It is also properly discontinuous by lemma 4.5.6. Therefore the $A_{g,n}$ is a manifold. The remaining statements are similar to case of $g = 1$ discussed earlier. □

We can also define the DM stack of abelian varieties $\mathcal{A}_g$ by taking the quotient of $[Sp_{2g}(\mathbb{Z}/n\mathbb{Z})\backslash A_{g,n}]$.

4.6 Algebraic construction of A_g

Although A_g was constructed analytically above, we have the following important result.

Theorem 4.6.1. *A_g is a quasiprojective variety.*

Mumford gave a direct algebro-geometric construction of A_g which has the advantage of working over any field or even over $\mathbb{Z}$. The idea is best explained in the case $g = 1$, which was known before. Any elliptic curve is given as double cover of $\mathbb{P}^1$ branched at 4 distinct points. Let

$$U = \{\{p_1, \ldots, p_4\} \subset \mathbb{P}^1 \mid p_i \neq p_j\}$$

be the set of distinct unordered 4-tuples. Then

$$A_1 = U/PGL_2(\mathbb{C})$$

provided we understand how to make this into a variety. Making sense of this, is precisely what Mumford's geometric invariant theory (GIT) is all about. Fortunately this case can be done explicitly. U can be identified with the subset of the projective space $\mathbb{P}^4$ of homogenous quartic polynomials in x, y. We have $PGL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{\pm I\}$, and it is more convenient to work with $SL_2(\mathbb{C})$. This acts on $\mathbb{P}^4$ by the substitutions

$$a_0x^4 + a_1x_0^3x_1 + \ldots = f(x, y) \mapsto f(ax + by, cx + dy)$$

It is reasonable to try to define $\mathbb{P}^4/SGL_2(\mathbb{C})$ first, and then pass to A_1. It is natural to identify the second space with the projective variety (i.e. $Proj$) of the graded ring $R = \mathbb{C}[a_0, \ldots, a_4]^{SL_2(\mathbb{C})}$ of invariants. The ring R is known to be generated by an explicit quadratic polynomial P and a cubic polynomial Q with no relations. It follows that R is a polynomial ring, although with a nonstandard grading, but in any case $Proj R = \mathbb{P}^1$. The geometry underlying this is more subtle. First of all, there are no nonconstant maps from $\mathbb{P}^4$ to $\mathbb{P}^1$, so there is no quotient map. A point $p \in \mathbb{P}^4$ is called *semistable* if there exists a constant polynomial $f \in R$ such that $f(p) \neq 0$. A point is called *stable* if in addition, the orbit is closed and the isotropy group is finite. There is a map from the locus $\mathbb{P}^4_{ss}$ of semistable points to $\mathbb{P}^1$, and one usually writes $\mathbb{P}^1 = \mathbb{P}^4_{ss}//SL_2(\mathbb{C})$ to distinguish it from the orbit space $\mathbb{P}^4_{ss}/SL_2(\mathbb{C})$ which is different. However, on the stable locus, the quotients $\mathbb{P}^4_s//SL_2(\mathbb{C}) = \mathbb{P}^4_s/SL_2(\mathbb{C})$ The set U consists of points, where the discriminant Δ, which is known to equal $P^3 - 6Q^2$, is nonzero. Thus $U \subset \mathbb{P}^4_{ss}$. In fact, U lies in $\mathbb{P}^4_s$. Under the quotient map $\mathbb{P}^4_{ss}/PG_2(\mathbb{C}) \to \mathbb{P}^1$, $U/PGL_2(\mathbb{C})$ is identified with $\mathbb{C} \subset \mathbb{P}^1$.

The case of $g = 2$ was also studied prior to Mumford by Igusa. One way to get two dimensional abelian varieties are as Jacobians of genus two curves. Any genus two curve is a double cover of $\mathbb{P}^1$ branched at 6 points. Proceeding as above, the set of unordered 6-tuples can be identified with the space of U of degree 6 polynomials with distinct roots. The moduli space of genus two curves

$$M_2 = U/PGL_2(\mathbb{C})$$

The invariant theory is harder, but it can still be worked out explicitly (and indeed much of this was done in the 19th century). The key facts are that M_2 exists as a variety with $\dim M_2 = \dim U - \dim PGL_2(\mathbb{C}) = 3$. We have $\dim A_2 = 2(2+1)/2 = 3$, and in fact M_2 is contained in A_2 as an open set. Igusa gave a much more precise analysis of this case.

Mumford's construction in the general case, uses Grothendieck's theory of Hilbert schemes. U above should be replaced by the so called Hilbert scheme of g dimensional principally polarized abelian varieties (A, Θ) embedded in some big projective space say $\mathbb{P}^N$, using $k\Theta$ for $k \gg 0$. Then

$$A_g = U/PGL_{N+1}(\mathbb{C})$$

Mumford used his GIT methods to show that the right side is a quasiprojective variety.

The last step above is quite hard, since the verification of the stability condition is very delicate. Fortunately, there now exist alternative methods for constructing moduli spaces in algebraic geometry. The first step is to enlarge the class of varieties. This is necessitated by the following example:

Example 4.6.2 (Hironaka)**.** *There exists an algebraic variety X with an action by finite group G such that quotient is not an algebraic variety over even a scheme.*

Artin constructed the theory of algebraic spaces which is big enough to contain such finite quotient examples. We won't give the precise definition, but it is very close to the definition of a stack, but less radical in the sense that the associated functor is set valued rather than groupoid valued. Over $\mathbb{C}$, a compact algebraic space is the same thing as a Moishezon manifold, which is a compact complex manifold with as many meromorphic functions as possible. With this preparation, the quotient problem can now be handled using the following general result:

Theorem 4.6.3 (Keel-Mori [KM]). *Suppose that an algebraic group G acts properly with finite isotropy groups on a scheme X of finite type, or more generally an algebraic space. (Properness means that the map $G \times X \to X \times X$, given by $(g, x) \to (x, gx)$ is proper.) Then the quotient exists as an algebraic space.*

4.7 Endomorphism rings of generic abelian varieties

With the basic moduli theory in hand, we can now go back and tie up some loose ends. Up to now, we have not proved that simple higher dimensional abelian varieties exist. We do so now. A g dimensional principally polarized abelian variety A is isogenous to a product $A_1 \times A_2$ with $g_i = \dim A_i > 0$. A simple dimension count shows that a typical p.p. abelian variety is a least not *isomorphic* to a product. The dimension of A_g is $g(g+1)/2$. While the dimension of the space of abelian varieties which are products with factors of dimension g_i is

$$\dim A_{g_1} + \dim A_{g_2} = \frac{g_1(g_1+1)}{2} + \frac{g_2(g_2+1)}{2} < \frac{g(g+1)}{2}$$

In fact, there is a more direct argument which proves more. A subset of a complex manifold such as H_g is called analytic if it is given as the zero set of a collection of analytic functions.

Theorem 4.7.1. *For every g, there exists a countable union of proper analytic sets $S \subset H_g$ such $End_{\mathbb{Q}}(X_\Omega) = \mathbb{Q}$ for $\Omega \in H_g - S$ where $X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g + \mathbb{Z}^g$.*

Corollary 4.7.2. *For every g, there exists a simple g dimensional abelian variety X with $End_{\mathbb{Q}}(X) = \mathbb{Q}$.*

Proof. A proper analytic set is nowhere dense. Therefore $H_g - S \neq \emptyset$ by the Baire category theorem. Take $X = X_\Omega$ with $\Omega \in H_g - S$, then $End(X)_{\mathbb{Q}} = \mathbb{Q}$ and this implies simplicity. □

Given $e \in End_{\mathbb{Q}}(X_\Omega)$, we can view this as an endomorphism of $\mathbb{C}^g$ which takes the lattice $\Omega\mathbb{Z}^g + \mathbb{Z}^g$ to itself. Thus e can be represented by $g \times g$ complex matrix $E = E_{e,\Omega}$ or a $2g \times 2g$ rational matrix $M = M_{e,\Omega}$. These are related by the matrix equation

$$E(\Omega, I) = (\Omega, I)M \tag{4.2}$$

To each matrix $M \in M_{2g\times 2g}(\mathbb{Q})$, let

$$S(M) = \{\Omega \mid \exists e \in End_{\mathbb{Q}}(X_\Omega), M = M_{e,\Omega}\}$$

The theorem will follow from

Proposition 4.7.3. *If M is not scalar matrix, then $S(M)$ is a proper analytic set.*

Proof. Let $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Then expanding (4.2) yields

$$E\Omega = \Omega A + C, \quad E = \Omega B + D$$

and therefore

$$(\Omega B + D)\Omega = \Omega A + C \tag{4.3}$$

It follows that $S(M)$ is an analytic set. Suppose that it is all of H_g. Setting $\Omega = \sqrt{-1}tI$, with arbitrary $t \in \mathbb{R}_{>0}$, shows that $B = C = 0$ and $D = A$. Substituting back into (4.3), taking the real part and setting $Z = Re\Omega$, shows $[Z, A] = 0$. Since Z can be chosen to be an arbitrary symmetric matrix, this forces A to be scalar matrix aI. Therefore $M = aI_{2g}$.

□

4.8 Hilbert modular varieties

We turn now to the converse to corollary 3.3.2 for algebras of type I, i.e. for a totally real number field K. Let n be the degree K over $\mathbb{Q}$. We have n distinct embeddings $\sigma_j : K \to \mathbb{R}$. Let O_K be the ring of integers, which is the integral closure of $\mathbb{Z}$ in K. More explicitly,

$$O_K = \{x \in K \mid \exists a_i \in \mathbb{Z}, x^N + a_{N-1}x^{N-1} + \ldots + a_0 = 0\}$$

An example to keep in mind is $K = \mathbb{Q}(\sqrt{2})$, $O_K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. In general, as a $\mathbb{Z}$-module, $O_K \cong \mathbb{Z}^n$. For each vector $\tau = (\tau_j) \in H^n$ define $L_\tau \subset \mathbb{C}^n$ to be the image of $(O_K)^2$ under the map

$$\iota_\tau(\alpha, \beta) = (\sigma_j(\alpha)\tau_j + \sigma_j(\beta))$$

Proposition 4.8.1. *L_τ is a lattice, and the quotient $A_\tau = \mathbb{C}^n/L_\tau$ is an abelian variety with $K \subseteq End_{\mathbb{Q}}(A_\tau)$.*

Proof. We note that $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^n$ where the projections to the factors are the σ_j. It follows that $O_K \subset K \subset \mathbb{R}^n$ is lattice, and therefore so is $L_\tau \subset \mathbb{C}^n$. Thus A_τ is a torus. It is an abelian variety because it has a polarization given by

$$E(u, v) = \sum \frac{1}{\tau_j} Im(u_j \bar{v}_j)$$

Finally, we have an embedding $O_K \subset M_{n\times n}(\mathbb{C})$ which sends α to the diagonal matrix with entries $\sigma_j(\alpha)$. L_τ is stable under the resulting O_K-action. Therefore $O_K \subset End(A_\tau)$, so that $K \subset End_{\mathbb{Q}}(A_\tau)$. □

Theorem 4.8.2. *The subset of $\tau \in H^n$ where $K \neq End_{\mathbb{Q}}(A_\tau)$ is a countable union of proper analytic subvarieties.*

Proof. This is similar to the previous argument, cf [BL, §9.9]. □

Corollary 4.8.3. *There exists τ such that $K = End_{\mathbb{Q}}(A_\tau)$.*

Proof. This follows by the Baire category theorem. □

Although this solves the original problem, there is much more to the story. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(O_K)$ acts on H^n by

$$(\tau_j) \mapsto (\frac{\sigma_j(a)\tau_j + \sigma_j(b)}{\sigma_j(c)\tau_j + \sigma_j(d)})$$

The quotient

$$SL_2(O_K)\backslash H^n$$

can be viewed as the moduli space of n-dimensional principally polarized abelian varieties with endomorphism algebra containing O_K. It and related spaces are referred to as a Hilbert modular varieties or sometimes Hilbert-Blumenthal varieties. As in the previous cases, this is not too far from a manifold. Namely, a suitable finite index subgroup $\Gamma \subset SL_2(O_K)$ will act freely and properly discontinuously, so therefore $\Gamma\backslash H^n$ is a manifold.

We can consider the same problem, where the dimension g might be bigger than n. In general, $n|g$. Setting $m = g/n$, we have an n homomorphisms $h_i : Sp_{2m}(O_K) \to Sp_{2m}(\mathbb{R})$ induced by $\sigma_1, \ldots, \sigma_n$. Then we have an action of $Sp_{2m}(O_K)$ on H_m^n, where it acts on the ith factor through h_i. The quotient

$$Sp_{2m}(O_K)\backslash H_m^n$$

gives the coarse moduli space of g-dimensional principally polarized abelian varieties with endomorphism algebra containing O_K. This general construction goes back to Shimura [Sh], and it is now known as a Shimura variety. Note that this class includes Hilbert modular varieties as well as A_g. An introduction to the general topic is given in [Mi].

4.9 Some abelian varieties of type II and IV

We will be content to work out a few more cases of the converse to corollary 3.3.2. To start off, let us say $K = \mathbb{Q}$. Fix totally indefinite quaternion division algebra D, or algebra of type II, over $\mathbb{Q}$. Recall that this means that $D \otimes \mathbb{R} = Mat_{2\times 2}(\mathbb{R})$. Choose a lattice $M \subset D$, M can be viewed a lattice in $Mat_{2\times 2}(\mathbb{R})$

via the embedding $D \subset Mat_{2\times 2}(\mathbb{R})$. We choose $\tau \in H$. Then M generates a sublattice $M\begin{pmatrix}\tau\\1\end{pmatrix} \subset \mathbb{C}^2$. Let

$$X_\tau = \mathbb{C}^2/M\begin{pmatrix}\tau\\1\end{pmatrix}$$

This is polarized by the form represented by the matrix $\begin{pmatrix}1/Im\tau & 0\\0 & 1/Im\tau\end{pmatrix}$. Finally, note that $M \otimes \mathbb{Q} = D$ is stable under the obvious action of F, so that $End_{\mathbb{Q}}(X_\tau) \subseteq D$. For a general choice of τ we will have an equality.

This can be generalized to any algebra of type II. Let us fix a totally real number field K of degree n, and a totally indefinite quaternion division algebra D over K. Choose a lattice $M \subset D$ and a vector $(\tau_i) \in H^n$ as above. We have an embedding $D \subset (Mat_{2\times 2}(\mathbb{R}))^n$ given as a product of the maps $D \subset D \otimes_{\sigma_i} \mathbb{R} \cong Mat_{2\times 2}(\mathbb{R})$ over the embeddings $\sigma_i : K \to \mathbb{R}$. Thus elements of D will act on $\mathbb{C}^{2n} = (\mathbb{C}^2)^n$. The image $L = M(\tau_1, 1, \tau_2, 1, \ldots)^T$ will be a lattice in $\mathbb{C}^{2n}$. The quotient $X = \mathbb{C}^{2n}/L$ will be an abelian variety, and $End_{\mathbb{Q}}(X) = D$ when (τ_j) is general.

***

We now turn the case of type IV. We concentrate on the important special where the algebra is a CM field F. This means that there is totally real field K and a totally positive element $\beta \in K$, such that $F = K(\sqrt{-\beta})$. Let suppose that the degree of K is n, then F has degree $2n$. Choose n distinct embeddings $\sigma_1, \ldots, \sigma_n$ of $F \subset \mathbb{C}$, so that $\sigma_i \neq \bar{\sigma}_j$. In fact, this is the only choice. There are no parameters. Let O_F be the ring of integers of F. We embed $O_F \subset \mathbb{C}^n$ as a lattice, by sending $\lambda \mapsto (\sigma_i(\lambda))$. We form the torus $X = \mathbb{C}^n/O_F$. This is polarized by the form represented by the diagonal matrix with $\sigma_i(\sqrt{-\beta})$ down the diagonal. We have $End_{\mathbb{Q}}(X) = F$. Such an abelian variety is a called an abelian variety with complex multiplication.

***

The reason why we skipped over type III, is because there is no really easy case. The simplest algebra of this type is the standard quaternion algebra $D = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ over $\mathbb{Q}$. The natural thing to do is form the lattice $L = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$. We can view this as a lattice in $\mathbb{C}^2 = \mathbb{C} \oplus \mathbb{C}j$. Then $X = \mathbb{C}^2/L$ gives an abelian variety with $End_{\mathbb{Q}}(X) \supset D$. So far, so good. But $X \cong (\mathbb{C}/\mathbb{Z} + \mathbb{Z}i)^2$ so that

$$End_{\mathbb{Q}}(X) = Mat_{2\times 2}(\mathbb{Q}(i)) \neq D$$

In fact, one cannot achieve equality with such a construction unless the dimension is large with parameters chosen generically.

4.10 Baily-Borel-Satake compactification

We want to generalize an earlier result:

Theorem 4.10.1 (Baily-Borel)**.** *A_g, and the various related Shimura varieties, are quasiprojective varieties.*

This means that A_g is a Zariski open subset of a projective variety $\bar{A}_g$. Let us first look at the case, when $g = 1$. Then $A_g = \mathbb{C}$ and $\bar{A}_1 = \mathbb{P}^1 = A_1 \cup \{\infty\}$. It useful to see how this works group theoretically. The action of $SL_2(\mathbb{Z})$ on H_1 extends to the boundary $\mathbb{R} \cup \{\infty\}$. The orbit of 0 is easily to consist of $\mathbb{Q} \cup \{\infty\}$. Define the extended half plane by $H_1^* = H_1 \cup \mathbb{Q} \cup \{\infty\}$. The quotient can then be identified with $\bar{A}_1$ as a set. The set H^* can

be endowed with a topology that makes the projection continuous. The basic neighbourhoods of ∞ are strips

$$\{z \in \mathbb{C} \mid Imz > C\} \cup \{\infty\}$$

The higher dimensional case, due to Satake, is more complicated but follows same idea. Baily and Borel [BB] gave a more general construction that applies all Shimura varieties such as Hilbert modular varieties. This case is a lot easier to describe, so we start with this. Suppose we are given a totally real field K of degree n, with embeddings $\sigma_i : K \to \mathbb{R}$. We add $\sigma_i(K \cup \{\infty\})$ to the ith copy of H, to get a new space $(H^n)^*$. The action of $SL_2(K)$ will extend to this space, with the boundary constituting a single orbit. We extend the topology from H^n to an $SL_2(K)$-invariant topology on $(H^n)^*$. It is enough to say what the basic neighbourhoods are for one point on the boundary. For ∞, we use sets of the form

$$\{(z_1, \ldots, z_n) \in \mathbb{C}^n \mid \prod Im(z_i) > C\} \cup \{\infty\}$$

A Hilbert modular form of weight $k \in \mathbb{N}$ is a holomorphic function $f : H^n \to \mathbb{C}$ such that

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z) = \prod (\sigma_i(c) z_i + \sigma_i(d))^k f(z)$$

for all matrices in $SL_2(O_K)$.

Theorem 4.10.2 (Baily-Borel)**.** *The quotient topology of $Y = SL_2(O_K) \backslash (H^n)^*$ is compact and Hausdorff. Y can be embedded into some $\mathbb{P}^N$ as a projective variety by using Hilbert modular forms of sufficiently large weight.*

Returning to A_g, we follow the same method. We wish to extend H_g by adding extra points on the boundary. To describe this more precisely we switch to the disk model:

Lemma 4.10.3. *H_g is isomorphic to*

$$D_g = \{Z \in Mat_{g\times g}(\mathbb{C}) \mid Z^T = Z, I - \bar{Z}Z \text{ pos. definite}\}$$

by sending

$$\Omega \mapsto (\Omega - \sqrt{-1} I)(\Omega + \sqrt{-1} I)^{-1}$$

Let $\bar{D}_g$ denote the closure of D_g in the set of symmetric matrices. For $r < g$, we can embed $D_r \hookrightarrow \bar{D}_g$ by identifying it with

$$\{\begin{pmatrix} Z & 0 \\ 0 & I \end{pmatrix} \mid Z \in D_r\}$$

Let D_g^* denote D_g union the of images of D_r under $Sp_{2g}(\mathbb{Z})$ for all $r < g$. Then define

$$\bar{A}_g := Sp_{2g}(\mathbb{Z}) \backslash D_g^*$$

which for the moment is only a set.

Theorem 4.10.4 (Satake, Baily-Borel)**.** *$\bar{A}_g$ has a structure of a normal projective variety such that $\bar{A}_g \supset A_g$ as an open subvariety, and the boundary can be stratified as $A_{g-1} \cup A_{g-2} \cup \ldots$.*

Bibliography

[BB] W. Baily, A. Borel, *Compactifications of arithmetically defined quotients of bounded symmetric domains*, Ann of Math (1966)

[BL] C. Birkenhake, H. Lange, *Complex Abelian Varieties*, Springer (2003)

[BG] J. Brunier, G. van der Geer, G. Harder, D. Zagier, *The 123 of modular forms*, Springer (2008)

[DM] P. Deligne, D. Mumford, *Irreducibility of the space of curves of a given genus*, IHES (1969)

[GH] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, J. Wiley (1978)

[KM] S. Keel, S. Mori, *Quotients by groupoids.* Ann. of Math. 145 (1997)

[Kn] D. Knutson, *Algebraic spaces*, Springer (1971)

[L] S. Lang, *Algebra*, Springer (2002)

[LM] G. Laumon. L. Morret-Bailly, *Champ Algebriques*, Springer (2000)

[Mi] J. Milne, *Shimura Varieties and Moduli* (2011), http://www.jmilne.org/math/

[M] D. Mumford, *Abelian varieties*, Tata Inst. (1974)

[M2] D. Mumford, *Tata lectures on theta 1*, Birkhauser (1983)

[MF] D. Mumford, J. Forgarty, *Geometric invariant theory*, Springer (1982)

[Se] J.P. Serre, *A course in arithmetic*, Springer (1973)

[S] J. Silverman, *The arithmetic of elliptic curves*, Springer (1992)

[Sh] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Annals (1963)