Lectures on Abelian Varieties, Milan, February 2014

Igor Dolgachev

Lecture 1

Complex abelian varieties

Let $A = V/\Lambda$ be a complex torus of dimension g over $\mathbb{C}$. Here V is a complex vector space of dimension $g > 0$ and Λ is a discrete subgroup of V of rank $2g$.[1] The complex space V is identified with the tangent space of A at the origin or with the space of holomorphic vector fields $\Theta(A)$ on A. It is the universal cover of A. The group Λ can be identified with the fundamental group of A that coincides with $H_1(A, \mathbb{Z})$. The dual space V^* can be identified with the space $\Omega^1(A)$ of holomorphic 1-forms on A, the map

$$\alpha : \Lambda = H_1(A, \mathbb{Z}) \to \Omega^1(A)^* = V, \quad \alpha(\gamma) : \omega \mapsto \int_\gamma \omega,$$

can be identified with the embedding of Λ in V. Let $(\gamma_1, \ldots, \gamma_{2g})$ be a basis of Λ and let $(\omega_1, \ldots, \omega_g)$ be a basis of V^*. The map $H_1(A, \mathbb{Z}) \to V$ is given by the matrix

$$\Pi = \begin{pmatrix} \int_{\gamma_1} \omega_1 & \int_{\gamma_2} \omega_1 & \ldots & \int_{\gamma_{2g}} \omega_1 \\ \int_{\gamma_1} \omega_2 & \int_{\gamma_2} \omega_2 & \ldots & \int_{\gamma_{2g}} \omega_2 \\ \vdots & \vdots & \vdots & \vdots \\ \int_{\gamma_1} \omega_g & \int_{\gamma_2} \omega_g & \ldots & \int_{\gamma_{2g}} \omega_g \end{pmatrix} \tag{1.1}$$

called the *period matrix* of A. The *columns of the period matrix* are the coordinates of $\gamma_1, \ldots, \gamma_{2g}$ in the dual basis $(e_1, \ldots, e_g)$ of the basis $(\omega_1, \ldots, \omega_g)$, i.e. a basis of V. The *rows of the period matrix* are the coordinates of $(\omega_1, \ldots, \omega_g)$ in terms of the dual basis $(\gamma_1^*, \ldots, \gamma_{2g}^*)$ of $H^1(A, \mathbb{C})$.

Let W denote V considered as a real vector space of dimension $2g$ by restriction of scalars. We can identify it with $\Lambda_\mathbb{R} := \Lambda \otimes_\mathbb{Z} \mathbb{R}$. A complex structure on V is defined by the $\mathbb{R}$-linear operator $I : W \to W, w \mapsto iw$, satisfying $I^2 = -1$. The space $W_\mathbb{C} := W \otimes_\mathbb{R} \mathbb{C}$ decomposes into the direct sum $V_i \oplus V_{-i}$ of eigensubspaces with eigenvalues i and $-i$. Obviously, $V_{-i} = \bar{V}_i$. We can identify V_i with the subspace $\{w - iI(w), w \in W\}$ and V_{-i} with $\{w + iI(w), w \in W\}$ (since $I(w \pm iI(w)) = I(w) \mp iw = \mp i(w \pm iI(w))$). The map $V_i \to V, w - iI(w) \to w$, is an isomorphism of complex linear spaces. Thus a complex structure $V = (W, I)$ on W defines a decomposition $W_\mathbb{C} = V \oplus \bar{V}$.

The space V (resp. $\bar{V}$) can be identified with the holomorphic part $T^{1,0}$ (resp. anti-holomorphic part $T^{0,1}$) of the complexified tangent space of the real torus W/Λ at the origin. Passing to the

[1] A subgroup Γ of V is discrete if for any compact subset K of V the intersection $K \cap \Gamma$ is finite, or, equivalently, Γ is freely generated by r linearly independent vectors over $\mathbb{R}$, the number r is the rank of Γ.

duals, and using the De Rham Theorem, we get the Hodge decomposition

$$H^1_{\mathrm{DR}}(A,\mathbb{C}) \cong H^1(A,\mathbb{C}) = W^*_{\mathbb{C}} = H^{1,0}(A) \oplus H^{0,1}(A), \tag{1.2}$$

where $H^{1,0}(A) = \Omega^1(A) = V^*$ (resp. $H^{0,1}(A) = \bar{V}^*$) is the space of holomorphic (resp. anti-holomorphic) differential 1-forms on A. Note that $H^{1,0}(A)$ embeds in $H^1(A,\mathbb{C})$ by the map that assigns to $\omega \in \Omega^1(A)$ the linear function $\gamma \mapsto \int_\gamma \omega$. If we choose the bases $(\gamma_1,\ldots,\gamma_{2g})$ and $(\omega_1,\ldots,\omega_g)$ as above, then $H^{1,0}$ is a subspace of $H^1(A,\mathbb{C})$ spanned by the vectors $\omega_j = \sum_{i=1}^{2g} a_{ij}\gamma_i^*$, where $(\gamma_1^*,\ldots,\gamma_{2g}^*)$ is the dual basis in $H^1(A,\mathbb{C})$, and (a_{ij}) is equal to the transpose ${}^t\Pi$ of the period matrix (1.1).

A complex torus is a Kähler manifold, a Kähler form Ω is defined by a Hermitian positive definite form H on V. In complex coordinates $z_1,\ldots,z_g$ on V, the Kähler metric is defined by $\sum h_{ij} z_i \bar{z}_j$, where (h_{ij}) is a positive definite Hermitian matrix. The Kähler form Ω of this metric is equal $\frac{i}{2}\sum h_{ij} dz_j \wedge d\bar{z}_i$. Its cohomology class $[\Omega]$ in the De Rham cohomology belongs to $H^2(A,\mathbb{R})$.

A complex torus is called an *abelian variety* if there exists an ample line bundle L on A, i.e. a line bundle such that the holomorphic sections of some positive tensor power of L embed A in a projective space. By Kodaira's Theorem, this is equivalent to that one can find a Kähler form Ω on A with $[\Omega] \in H^2(A,\mathbb{Z})$. In our situation this means that the restriction of the imaginary part $\mathrm{Im}(H)$ to $\Lambda\times\Lambda$ takes integer values. Recall that a Hermitian form $H : V\times V \to \mathbb{C}$ on a complex vector space can be characterized by the properties that its real part $\mathrm{Re}(H)$ is a real symmetric bilinear form on the corresponding real space W and its imaginary part $\mathrm{Im}(H)$ is a skew-symmetric bilinear form on W. The form H is positive definite if $\mathrm{Re}(H)$ is positive definite and $\mathrm{Im}(H)$ is non-degenerate (a *symplectic form*). Using the isomorphism

$$H^2(A,\mathbb{Z}) \cong \bigwedge^2 H^1(A,\mathbb{Z}) = \bigwedge^2 \Lambda^*,$$

we can identify $\mathrm{Im}(H)$ with $c_1(L)$, where L is an ample line bundle on A. Explicitly, a line bundle L trivializes under the cover $\pi : V \to V/\Lambda$ and it is isomorphic to the quotient of the trivial bundle $V\times\mathbb{C}$ by the action of Λ defined by

$$\lambda : (z,t) \mapsto (z+\lambda, e^{\pi H(z,\lambda)+\frac{\pi}{2}H(\lambda,\lambda)}\chi(\lambda)t),$$

where $\chi : \Lambda \to U(1)$ is a *semi-character* of Λ, i.e. a map $\Lambda \to U(1)$ satisfying $\chi(\lambda\lambda') = \chi(\lambda)\chi(\lambda')e^{\pi i \mathrm{Im}(H(\lambda,\lambda'))}$. It follows that

$$\mathrm{Pic}^0(A) := \mathrm{Ker}(c_1 : \mathrm{Pic}(A) \to H^2(A,\mathbb{Z})) \cong \mathrm{Hom}(\Lambda, U(1)).$$

Note that the Hermitian form H can be uniquely reconstructed from the restriction of $\mathrm{Im}(H)$ to $\Lambda\times\Lambda$, first extending it, by linearity, to a real symplectic form E on W, and then checking that

$$H(x,y) = E(ix,y) + iE(x,y). \tag{1.3}$$

In fact, $H(x,y) = A(x,y) + iE(x,y)$ implies

$$H(ix,y) = A(ix,y) + iE(ix,y) = iH(x,y) = iA(x,y) - E(x,y),$$

hence, comparing the real and imaginary parts, we get $A(x,y) = E(ix,y)$. Since $H(x,y) = H(ix,iy)$ and its real part is a positive definite symmetric bilinear form, we immediately obtain that E satisfies

$$E(ix,iy) = E(x,y), \quad E(ix,y) = E(iy,x), \quad E(ix,x) > 0,\ x \neq 0. \tag{1.4}$$

We say that a complex structure (W, I) on W is *polarized* with respect to a symplectic form E on W if E satisfies (1.4) (where $ix := I(x)$).

We can extend E to a Hermitian form $H_{\mathbb{C}}$ on $W_{\mathbb{C}}$, first extending E to a skew-symmetric form $E_{\mathbb{C}}$, by linearity, and then setting

$$H_{\mathbb{C}}(x, y) = \tfrac{1}{2} i E_{\mathbb{C}}(x, \bar{y}). \tag{1.5}$$

Let $x = a + ib, y = a' + ib' \in W_{\mathbb{C}}$. We have

$$H_{\mathbb{C}}(a + bi, a' - ib') = \tfrac{1}{2}(-E_{\mathbb{C}}(b, a') + E_{\mathbb{C}}(a, b')) + \tfrac{1}{2} i(E_{\mathbb{C}}(a, a') + E_{\mathbb{C}}(b, b')).$$

The real part of $H_{\mathbb{C}}$ is symmetric and the imaginary part is alternating, so $H_{\mathbb{C}}$ is Hermitian. Also, by taking a standard symplectic basis $e_1, \ldots, e_{2g}$ of W and a basis $(f_1, \ldots, f_g, \bar{f}_1, \ldots, \bar{f}_g)$ of $W_{\mathbb{C}}$, where $f_k = e_k + ie_{k+g}, \bar{f}_k = e_k - ie_{k+g}$, we check that $H_{\mathbb{C}}$ is of signature (g, g).

Now, if $x = w - iI(w), x' = w' - iI(w') \in V$, then, we easily check that

$$H_{\mathbb{C}}(x, x) = \tfrac{1}{2} i E_{\mathbb{C}}(w - iI(w), w + iI(w)) = E(I(w), w) > 0$$

and

$$E_{\mathbb{C}}(x, x') = E_{\mathbb{C}}(w - iI(w), w' - iI(w'))$$
$$= E_{\mathbb{C}}(w, w') - E_{\mathbb{C}}(I(w), I(w')) - i(E_{\mathbb{C}}(I(w), w') + E_{\mathbb{C}}(w, I(w')) = 0.$$

Thus $V = (W, I)$ defines a point in the following subset of the Grassmann variety $G(g, W_{\mathbb{C}})$:

$$G(g, W_{\mathbb{C}})_E := \{V \in G(g, W_{\mathbb{C}}) : H_{\mathbb{C}}|V > 0, E_{\mathbb{C}}|V = 0\}. \tag{1.6}$$

It is obvious, that V and $\bar{V}$ are orthogonal with respect of $H_{\mathbb{C}}$ and $H_{\mathbb{C}}|\bar{V} < 0$.

Conversely, let us fix a real vector space W of dimension $2g$ that contains a lattice Λ of rank $2g$, so that W/Λ is a real torus of dimension $2g$. Suppose we are given a symplectic form $E \in \bigwedge^2 W^*$ on W. We extend E to a skew-symmetric form $E_{\mathbb{C}}$ on $W_{\mathbb{C}}$, by linearity, and define the Hermitian form of signature (g, g) by using (3.3).

Suppose $V = (W, I) \in G(g, W_{\mathbb{C}})_E$. It is immediate to check that $E_{\mathbb{C}}(\bar{x}, y) = \overline{E_{\mathbb{C}}(x, \bar{y})}$. Thus, $H(\bar{x}, \bar{x}) = -H(x, y) < 0$. This implies that $V \cap \bar{V} = \{0\}$, hence $W_{\mathbb{C}} = V \oplus \bar{V}$. Now $W = \{v + \bar{v}, v \in V\}$ and the complex structure I on W defined by $I(w) = iv - i\bar{v}$ is isomorphic to the complex structure on V via the projection $W \to V, v + \bar{v} \to v$. Now it is easy to check that $E_{\mathbb{C}}$ restricted to W is equal to E, and $E(I(w), w) > 0, E(I(w), I(w)) = E(w, w)$. We obtain that the set of complex structures on W polarized by E is parameterized by (1.6).

The group $\mathrm{Sp}(W, E) \cong \mathrm{Sp}(2g, \mathbb{R})$ acts transitively on $G(g, W_{\mathbb{C}})_E$ with isotropy subgroup of V isomorphic to the unitary group $\mathrm{U}(V, H_{\mathbb{C}}|V) \cong U(g)$. Thus

$$G(g, W_{\mathbb{C}})_E \cong \mathrm{Sp}(2g, \mathbb{R})/U(g)$$

is a Hermitian symmetric space of type III in Cartan's classification. Its dimension is equal to $g(g + 1)/2$.

Remark 1. According to Elie Cartan's classification of Hermitian symmetric spaces there are 4 classical types I,II, III and IV and two exceptional types E_6 and E_7. We will see type IV spaces later when we discuss K3 surfaces and other classical types when we will discuss special subvarieties of the moduli spaces of abelian varieties. The exceptional types so far have no meaning as the moduli spaces of some geometric objects.

So far, we have forgot about the lattice Λ in the real vector space W. The space $G(g, W_{\mathbb{C}})_E$ is the *moduli space of complex structures on a real vector space W of dimension $2g$ which are polarized with respect to a symplectic form E on W* or, in other words, it is the *moduli space of complex tori equipped with a Kahler metric H defined by a symplectic form $E = \mathrm{Im}(H)$*. Now we put an additional *integrality condition* by requiring that

$$\mathrm{Im}(H)(\Lambda \times \Lambda) \subset \mathbb{Z}.$$

Recall that a skew-symmetric form E on a free abelian group of rank $2g$ can be defined in some basis by a skew-symmetric matrix

$$J_{\mathsf{D}} = \begin{pmatrix} 0_g & \mathsf{D} \\ -\mathsf{D} & 0_g \end{pmatrix},$$

where D is the diagonal matrix $\mathrm{diag}(d_1, \ldots, d_g)$ with $d_i | d_{i+1}, i = 1, \ldots, g-1$. The sequence $(d_1, \ldots, d_g)$ defines the skew-symmetric form uniquely up to a linear isomorphism preserving the skew-symmetric form. In particular, if E is non-degenerate, the product $d_1 \cdots d_g$ is equal to the determinant of any skew-symmetric matrix representing the form. If H is a positive definite Hermitian form defining a polarization on A, the sequence $(d_1, \ldots, d_g)$ defining $\mathrm{Im}(H)|\Lambda \times \Lambda$ is called the *type of the polarization*. A polarization is called *primitive* if $(d_1, \ldots, d_g) = 1$ It is called *principal* if $(d_1, \ldots, d_g) = (1, \ldots, 1)$.

Choose a basis $\underline{\gamma} = (\gamma_1, \ldots, \gamma_{2g})$ of Λ such that the matrix of the symplectic form $E|\Lambda \times \Lambda$ is equal to the matrix J_{D}.

We know that the matrix $(E(i\gamma_a, \gamma_b))_{g+1 \le a,b \le 2g}$ is positive definite. This immediately implies that the $2g$ vectors $\gamma_a, i\gamma_a, a = g+1, \ldots, 2g$, are linearly independent over $\mathbb{R}$, hence we may take $\frac{1}{d_1}\gamma_{g+1}, \ldots, \frac{1}{d_g}\gamma_{2g}$ as a basis $(e_1, \ldots, e_g)$ of V. It follows that the period matrix Π in this basis of V and the basis $(\gamma_1, \ldots, \gamma_{2g})$ of Λ is equal to a matrix $(\tau\ \mathsf{D})$. Write $\tau = X + iY$, where $X = \mathrm{Re}(\tau)$ and $Y = \mathrm{Im}(\tau)$ are real matrices. We have

$$A \cong \mathbb{C}^g / \mathbb{Z}^g \oplus \mathsf{D}\mathbb{Z}^g.$$

Then $\gamma_k = \sum_{s=1}^{g} x_{ks} e_s + \sum y_{ks} i e_s, k = 1, \ldots, g$. Then the matrix of E on $W = \Lambda_{\mathbb{R}}$ in the basis $(e_1, \ldots, e_g, ie_1, \ldots, ie_g)$ of W is equal to

$$^t\begin{pmatrix} X & D \\ Y & 0 \end{pmatrix}^{-1} J_{\mathsf{D}} \begin{pmatrix} X & D \\ Y & 0 \end{pmatrix}^{-1} = {}^t\begin{pmatrix} X & \mathsf{D} \\ Y & 0 \end{pmatrix}^{-1} J_{\mathsf{D}} \begin{pmatrix} 0 & Y^{-1} \\ \mathsf{D}^{-1} & -\mathsf{D}^{-1} X Y^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & -Y^{-1} \\ {}^tY^{-1} & -{}^tY^{-1}(X - {}^tX)Y^{-1} \end{pmatrix}.$$

Since $E(e_i, e_j) = E(ie_i, ie_j) = \frac{1}{d_i d_j} E(\gamma_{g+i}, \gamma_{g+j}) = 0$ and $(E(ie_i, e_j))$ is a symmetric positive definite matrix, we obtain that Y is a symmetric positive definite matrix, and X is a symmetric matrix. In particular, $\tau = X + iY$ is a symmetric complex matrix.

We have proved one direction of the following theorem.

Theorem 2 (Riemann-Frobenius conditions)**.** *A complex torus $A = V/\Lambda$ is an abelian variety admitting a polarization of type D if and only if one can choose a basis of Λ and a basis of V such that the period matrix Π is equal to the matriz $(\tau\ \mathsf{D})$, where*

$$^t\tau = \tau, \quad \mathrm{Im}(\tau) > 0.$$

We leave the proof of the converse to the reader.

Note that the matrix of the Hermitian form H in the basis $e_1, \dots, e_g$ as above is equal to $S = (E(ie_a, e_b))$. Since

$$d_b\delta_{ab} = E(\gamma_a, \gamma_{g+b}) = \sum_{k=1}^{g} E((x_{ka} + iy_{ka})e_k, d_b e_b)$$

$$= \sum_{k=1}^{g} y_{ka} E(ie_k, d_b e_b) = \sum_{k=1}^{g} E(ie_b, d_b e_k) y_{ka} = d_b \sum_{k=1}^{g} E(ie_b, e_k) y_{ka},$$

we obtain that

$$S = \text{Im}(\tau)^{-1}. \tag{1.7}$$

So, we see that we can choose a special basis $\gamma_1, \dots, \gamma_{2g}$ such that the period matrix Π of A is equal to $(\tau\ \mathsf{D})$, where τ belongs to the *Siegel upper-half space of degree g*

$$\mathcal{Z}_g := \{\tau \in \text{Mat}_n(\mathbb{C}) : {}^t\tau = \tau, \text{Im}(\tau) > 0\}.$$

Every abelian variety with a polarization of type D is isomorphic to the complex torus

$$A \cong \mathbb{C}^g/\tau\mathbb{Z}^g + \mathsf{D}\mathbb{Z}^g.$$

Note that $\mathcal{Z}_g \cong G(g, \mathbb{C}^g)_E$, where $E : \mathbb{R}^{2g} \times \mathbb{R}^{2g} \to \mathbb{R}$ is defined by the matrix $\mathsf{D}\text{Im}(\tau)^{-1}$. However, this isomorphism depends on a choice of a special basis in $\mathbb{R}^{2g}$. One must view $\mathcal{Z}_g$ as the moduli space of polararized complex structures on a symplectic vector space W of dimension $2g$ equipped with a linear symplectic isomorphism $\mathbb{R}^{2n} \to W$, where the symplectic form $\mathbb{R}^{2n}$ is defined by the matrix D.

Two such special bases are obtained from each other by a change of a basis matrix that belongs to the group

$$\text{Sp}(J_{\mathsf{D}}, \mathbb{Z}) = \{X \in \text{Sp}(2g, \mathbb{Q}) : X \cdot J_{\mathsf{D}} \cdot {}^tX = J_{\mathsf{D}}\}.$$

If $X = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$, where A_1, A_2, A_3, A_4 are square matrices of size g, then $X \in \text{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ if and only if

$$A_1\mathsf{D}^t A_2 = A_2\mathsf{D}_1^A, \quad A_3\mathsf{D}^t A_4 = A_4\mathsf{D}^t A_3, \quad A_1\mathsf{D}^t A_4 - A_2\mathsf{D}^t A_3 = \mathsf{D}.$$

Thus, we obtain that the coarse moduli space for the isomorphic classes of abelian varieties with polarization of type D is isomorphic to the orbit space

$$\mathcal{A}_{g,\mathsf{D}} = \mathcal{Z}_g/\text{Sp}(J_{\mathsf{D}}, \mathbb{Z}).$$

The group $\text{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ acts on $\mathcal{Z}_g$ by

$$\tau \mapsto (\tau A_1 + A_2)(A_3\tau + A_4)^{-1}\mathsf{D}.$$

If $J_{\mathsf{D}} = J$, then we denote $\text{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ by $\text{Sp}(2g, \mathbb{Z})$ and $\mathcal{A}_{g,\mathsf{D}}$ by $\mathcal{A}_g$ and get

$$\mathcal{A}_g = \mathcal{Z}_g/\text{Sp}(2g, \mathbb{Z}).$$

As we see from above that, so far, the geometry of abelian varieties is reduced to linear algebra. One can pursue it further by interpreting in these terms the intersection theory on A. It assigns to any line bundles $L_1, \ldots, L_g$ an integer $(L_1, \ldots, L_g)$ that depends only on the images of L_i under the first Chern class map. Of course, it is also linear in each L_i with respect to the tensor product of line bundles. Let $c_1(L_i) = \alpha_i \in \bigwedge^2 \Lambda^*$. Consider each α_i as a linear map $\alpha_i : \Lambda \to \Lambda^*$ and take the exterior power of these maps

$$\alpha_1 \wedge \cdots \wedge \alpha_g \in \bigwedge^{2g} \Lambda^*.$$

A choice of a basis in Λ defines an isomorphism $\bigwedge^{2g} \Lambda^* \cong \mathbb{Z}$. This isomorphism depends only on the orientation of the basis. We choose an isomorphism such that $L^g := (L, \ldots, L) > 0$ if L is an ample line bundle. For example, if L corresponds to a polarization of type D, we have $\alpha = \sum n_i \gamma_i \wedge \gamma_{i+g}$ and

$$L^g = g! n_1 \cdots n_g.$$

By constructing explicitly a basis in the space of holomorphic sections of an ample line bundle L in terms of *theta functions*, one can prove that

$$h^0(L) = \frac{L^g}{g!} = \text{Pf}(\alpha),$$

where $\text{Pf}(\alpha)$ is the pfaffian of the skew-symmetric matrix defining α. More generally, for any line bundle L, the Riemann-Roch Theorem gives

$$\chi(L) = \sum_{i=0}^{g} H^i(A, L) = \frac{L^g}{g!}.$$

Let us now define a duality between abelian varieties. Of course this should correspond to the duality of the complex vector spaces.

Let $A = V/\Lambda$ be a complex g-dimensional torus. Consider the Hodge decomposition (1.2), where we identify the space $H^{1,0}(A)$ with V^*. Using the Dolbeault's Theorem, one can identify $H^{0,1}(A)$ with the cohomology group $H^1(A, \mathcal{O}_A)$. The group $H^1(A, \mathbb{Z}) = \Lambda^*$ embeds in $H^1(A, \mathbb{C})$ and its projection to $H^{0,1}$ is a discreet subgroup Λ' of rank $2g$ in $H^{0,1}$. The inclusion $H^1(A, \mathbb{Z}) \to H^1(A, \mathcal{O}_A)$ corresponds to the homomorphism derived from the exponential exact sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_A \xrightarrow{e^{2\pi i}} \mathcal{O}_{\hat{A}} \to 0$$

by passing to cohomology. It also gives an exact sequence

$$H^1(A, \mathcal{O}_A)/\Lambda' \to H^1(A, \mathcal{O}_A^*) \xrightarrow{c_1} H^2(A, \mathbb{Z}),$$

where the group $H^1(A, \mathcal{O}_A^*)$ is isomorphic to $\text{Pic}(A)$. Thus, we obtain that the group of points of the complex torus $H^1(A, \mathcal{O}_A)/\Lambda'$ is isomorphic to the group $\text{Pic}^0(A)$. It is called the *dual complex torus* of A and will be denoted by $\hat{A}$.

Now, we assume that A is an abelian variety equipped with a polarization L of type D. The corresponding Hermitian form H defines an isomorphism from the space V to the space $\bar{V}^*$ of $\mathbb{C}$-antilinear functions on V (where $\bar{V}$ is equal to V with the complex structure $I(v) = -iv$). [2]

[2] It also defines an isomorphism of complex vector spaces $\bar{V} \to V^*$

Considered as a vector space over $\mathbb{R}$, it is isomorphic to the real vector space $W^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ by means of the isomorphism

$$\bar{V}^* \to W^*, \ l \mapsto k = \mathrm{Im}(l)$$

with the inverse defined by $k \to -k(iv) + ik(v)$. We may identify $\bar{V}^*$ with $H^{0,1}(A)$. We have

$$\Lambda' = \Lambda^* := \{l \in \bar{V}^* : l(\Lambda) \subset \mathbb{Z}\},$$

so that

$$\hat{A} = \bar{V}^*/\Lambda^*.$$

Also, $\mathrm{Im}(H)$ defines a homomorphism $\Lambda \to \Lambda^*$. Composing it with the homomorphism $\Lambda^* = H^1(A, \mathbb{Z}) \to H^{0,1}(A)$, we obtain a homomorphism $\Lambda \to \Lambda^*$. Let

$$\phi_L : A \to \hat{A} \tag{1.8}$$

be the homomorphism defined by the maps $V \to H^{0,1}$ and $\Lambda \to \Lambda'$. It is a finite map, and

$$K(L) := \mathrm{Ker}(\phi_L) \cong \Lambda^*/\Lambda \cong (\mathbb{Z}^g/\mathsf{D}\mathbb{Z}^g)^2 \cong \bigoplus_{i=0}^{g} (\mathbb{Z}/d_i\mathbb{Z})^2.$$

In particular, ϕ_L is an isomorphism if L is a principal polarization. The dual abelian variety can be defined over any field as the Picard variety $\mathbf{Pic}^0(A)$ and one can show that an ample line bundle L defines a map (1.8) by using the formula

$$\phi_L(a) = t_a^*(L) \otimes L^{-1},$$

where t_a denotes the translation map $x \mapsto x + a$ of A to itself.

If we identify $\hat{A}$ with A by means of this isomorphism, then the map ϕ_L corresponding to the polarization L of type $(n, \ldots, n)$ can be identified with the multiplication map $[n] : x \to nx$. Its kernel is the subgroup $A[n]$ of n-torsion points in A. Let e_L be the exponent of the group K_L, i.e. the smallest positive integer that kills the group, then $\hat{A} \cong A/K_L$ and the multiplication map $[e_L] : A \to A$ is equal to the composition of the map $\phi_L : A \to \hat{A}$ and a finite map $\hat{A} \to A$ with kernel isomorphic to the group $(\mathbb{Z}/e_L\mathbb{Z})^{2g}/K_L$ of order $\frac{d_g^{2g-2}}{(d_1 \cdots d_{g-1})^2}$. Abusing the notation, we denote this map by ϕ_L^{-1}. so, by definition, $\phi_L^{-1} \circ \phi_L = [e_L]$. In the ring $\mathrm{End}(A)_{\mathbb{Q}}$ the element ϕ_L^{-1} is the inverse of $\frac{1}{e_L}\phi_L$.

Lecture 2

Endomorphisms of abelian varieties

A morphism $f : A = V/\Lambda \to A' = V'/\Lambda'$ of complex tori that sends zero to zero is called a *homomorphism* of tori. It is easy to see that this is equivalent to that f is a homomorphism of complex Lie groups. Obviously, it is defined by a linear $\mathbb{C}$-map $f_a : V \to V'$ (called an *algebraic representation* of f) and a $\mathbb{Z}$-linear map $f_r : \Lambda \to \Lambda'$ (called a emphrational representation of f) such that the restriction of f_a to Λ coincides with f_r.

Let $\mathrm{End}(A)$ be the set of *endomorphisms* of an abelian variety $A = V/\Lambda$, i.e. homomorphisms of A to itself. As usual, for any abelian group, it is equipped with a structure of an associative unitary ring with multiplication define d by the composition of homomorphisms and the addition defined by value by value addition of homomorphisms. By above, we obtain two injective homomorphisms of rings

$$\rho_a : \mathrm{End}(A) \to \mathrm{End}_{\mathbb{C}}(V) \cong \mathrm{Mat}_g(\mathbb{C}), \quad \rho_r : \mathrm{End}(A) \to \mathrm{End}_{\mathbb{Z}}(\Lambda) \cong \mathrm{Mat}_{2g}(\mathbb{Z}).$$

They are called the *analytic* and *rational* representations, respectively.

We fix a polarization L_0 on A of type $\mathsf{D} = (d_1, \ldots, d_g)$. The corresponding Hermitian form on H_0 and the symplectic form $E_0 = \mathrm{Im}(H_0)$ on Λ allow us to define the involutions in the rings $\mathrm{End}_{\mathbb{C}}(V)$ (resp. $\mathrm{End}_{\mathbb{Z}}(\Lambda)$) by taking the adjoint operator with respect to H_0 (resp. $\mathrm{Im}(H_0)$).[1] Using the representations ρ_a and ρ_r, we transfer this involution to $\mathrm{End}(A)$. It is called the *Rosati involution* and, following classical notation, we denote it by $f \mapsto f'$. One can show that the Rosati involution can be defined as

$$f' = \phi_{L_0}^{-1} \circ f^* \circ \phi_{L_0} : A \to \hat{A} \to \hat{A} \to A.$$

Here $(f^*)_a : \bar{V}^* \to \bar{V}^*$ is the transpose of f. If we view $\hat{A}$ as the Picard variety, then f^* is the usual pull-back map of line bundles on A.

For any $f \in \mathrm{End}(A)$, let

$$P_a(f) = \det(tI_g - f_a) = \sum_{i=0}^{g} t^{g-i}(-1)^i c_i^a$$

[1]Recall that the *adjoint operator* of a linear operator $T : V \to V$ of complex spaces equipped with a non-degenerate Hermitian form H is the unique operator T^* such that $H(T(x), y) = H(x, T^*(y))$ for all $x, y \in V$.

be the characteristic polynomial of f_a and

$$P_r(f) = \det(tI_{2g} - f_r) = \sum_{i=0}^{2g}(-1)^i c_i^r t^{2g-i}$$

be the characteristic polynomial of f_r. It is easy to check that

$$P_a(f') = \overline{P_a(f)},$$

so all eigenvalues of f_a' are conjugates of the eigenvalues of f_a.

We have

$$(f_r)_{\mathbb{C}} = f_a \oplus \bar{f}_a,$$

where $(f_r)_{\mathbb{C}}$ is considered as a linear operator on $\Lambda_{\mathbb{C}}$. (see Proposition (5.1,2) in Lange-Birkenhake, Complex Abelian Varieties, cited [CAV] in the future). In particular,

$$P_r(t) = P_a(f)P_a(\bar{f}).$$

An endomorphism $f \in \mathrm{End}(A)$ is called *symmetric* if $f = f'$. Let $\mathrm{End}^s(A)$ denote the subring of symmetric endomorphisms. It follows from above that, if $f \in \mathrm{End}^s(A)$, then f_a is a self-adjoint operator with respect to H_0, and its eigenvalues are real numbers. Also, we see that $P_r(f) = P_a(f)^2$.

Let $\mathrm{NS}(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ be the *Néron-Severi group* of A. We define a homomorphism

$$\alpha : \mathrm{NS}(A) \to \mathrm{End}(A), \quad L \mapsto \phi_{L_0}^{-1} \circ \phi_L.$$

If f is in the image, then $\phi_L = \phi_{L_0} \circ f$. This means that $H_0(f_a(z), z') = H(z, z')$ for some Hermitian form H and $\mathrm{Im}(H)(\Lambda \times \Lambda) \subset \mathbb{Q}$. Since $H(z, z') = \overline{H(z', z)}$, this means that the operator f_a is self-adjoint, hence f is symmetric. This easily implies that α defines an isomorphism of $\mathbb{Q}$-linear spaces

$$\alpha : \mathrm{NS}(A)_{\mathbb{Q}} \to \mathrm{End}^s(A)_{\mathbb{Q}}.$$

If L_0 is a principal polarization, we can skip the subscript $\mathbb{Q}$ [CAV], 5.2.1.

Note that $\alpha(L_0) = \mathrm{id}_A$, hence the subgroup generated by L_0 is mapped isomorphically to the subgroup of $\mathrm{End}^s(A)$ of endomorphisms of the form $[m], m \in \mathbb{Z}$. Also, it follows from the definition of $\alpha(L)$ is an isomorphism if and only if L is a principal polarization.

If we identify $\mathrm{NS}(A)$ with the space of Hermitian forms H such that $\mathrm{Im}(H)(\Lambda \times \Lambda) \subset \mathbb{Z}$, then the inverse map α^{-1} assigns to f the Hermitian form

$$H = H_0(f_a(z), z'). \tag{2.1}$$

Suppose $f \in \mathrm{End}(A)$ and f_a is given by a complex matrix M of size g. Then we must have

$$M \cdot (\tau|\mathsf{D}) = (\tau|\mathsf{D}) \cdot N, \tag{2.2}$$

where the matrix

$$N = \begin{pmatrix} A_1 & A_3 \\ A_2 & A_4 \end{pmatrix} \in \mathrm{Mat}_{2g}(\mathbb{Z})$$

defines f_r. Thus we get

$$M = (\tau \cdot A_3 + \mathsf{D}A_4)\mathsf{D}^{-1},$$

hence :

$$M\tau = (\tau \cdot A_3 + \mathsf{D}A_4)\mathsf{D}^{-1}\tau = \tau A_1 + \mathsf{D}A_2. \tag{2.3}$$

Thus the period matrix τ must satisfy a "quadratic equation". Now assume, additionally, that $f \in \mathrm{End}^s(A)$ is a symmetric endomorphism. This means that f_r and f_r' considered as linear operators on $W = \Lambda_{\mathbb{R}}$ are adjoint operators with respect to the alternating form $E = \mathrm{Im}(H)$ defined by the matrix J_{D}. Thus the matrix N must satisfy ${}^tN \cdot J_{\mathsf{D}} = -J_{\mathsf{D}}{}^t \cdot N$. This gives

$${}^tA_1\mathsf{D} = \mathsf{D}A_4, {}^tA_3\mathsf{D} = -\mathsf{D}A_3, {}^tA_3\mathsf{D} = -\mathsf{D}A_3 \tag{2.4}$$

If $\mathsf{D} = I_g$, then

$$N = \begin{pmatrix} A & B \\ C & {}^tA \end{pmatrix}, \tag{2.5}$$

where B and C are skew-symmetric matrices of size $g \times g$.

The coefficients of the characteristic polynomial have the following geometric meaning.

For any $f = \alpha(L) \in \mathrm{End}^s(A)$,

$$dc_i^a = \frac{(L_0^{g-i}, L^i)}{(g-i)!i!},\ i = 0, \ldots, g, \tag{2.6}$$

where $d = d_1 \cdots d_g$ [CAV], (5.2.1). In particular, L is ample if and only if all eigenvalues of f_a are positive.[2] In the last statement, we use that a line bundle L is ample if and only if $(L_0^{g-i}, L^i) > 0$ for all $i = 0, \ldots, g$.

A homomorphism $f : A \to A'$ of abelian varieties of the same dimension is called an *isogeny* if its kernel is a finite group. The order of the kernel is called the *degree* of the isogeny and is denoted by $\deg(f)$. It is equal to the topological degree of the map. Equivalently, f is an isogeny if its image is equal to A'. An example of an isogeny is a map $\phi_L : A \to \hat{A}$, where L is an ample line bundle. The *inverse isogeny* is the map $g : A' \to A$ such that $g \circ f = [e]$, where e is the exponent of the kernel of f. For example, ϕ_L^{-1} is the inverse isogeny of ϕ_L. One checks that the isogeny is an equivalence relation on the set of isomorphism classes of abelian varieties.

Suppose $\alpha(L)$ defines $f \in \mathrm{End}^s(A)$ which is an isogeny. By definition, $\phi_{L_0} \circ f = \phi_L$ It follows that $\deg(\phi_{L_0})\deg(f) = \deg(\phi_L)$. We know that $\deg(\phi_{L_0}) = d = \det \mathsf{D}$ and $\deg(\phi_L) = d' = \det \mathsf{D}'$, where D' is the type of L. This gives $\deg(f) = d'/d$. Applying (2.6) with $i = g$, we obtain

$$c_g^a = \frac{d'g!}{g!d} = \deg(f). \tag{2.7}$$

One can also compute the coefficients c_i in the characteristic polynomial $P_{f \circ f'}^a$

$$c_i = \tbinom{g}{i} \frac{(f^*(L_0)^i, L_0^{g-i})}{(L_0^g)} \tag{2.8}$$

[2] This follows from Sturm's theorem relating the number of positive roots with the number of changes of signs of the coefficients of a polynomial.

(see [CAV], (5.1.7)). We set

$$\mathrm{Tr}(f)_a = c_1^a,\ \mathrm{Tr}_r = c_1^r,\ \mathrm{Nm}(f)_a = c_g^a,\ \mathrm{Nm}(f)_r = c_g^r.$$

We have

$$\mathrm{Tr}(f \circ f') = \frac{2}{(g-1)!}\frac{(f^*(L_0), L_0^{g-1})}{(L_0^g)}, \quad \mathrm{Nm}(f \circ f') = \frac{(f^*(L_0)^g)}{(L_0^g)}. \tag{2.9}$$

The first equality implies that the symmetric form $(f, g) \to \mathrm{Tr}(f \circ g')$ on $\mathrm{End}(A)$ is positive definite.

We know that $\mathrm{End}(A)_{\mathbb{Q}}$ is isomorphic to a subagebra of the matrix algebra and hence it is finite-dimensional algebra over $\mathbb{Q}$. A finite-dimensional associative algebra over a field F is called *simple* if it has no two-sided ideals. An example of a simple algebra is a matrix algebra $\mathrm{Mat}_n(F)$. An algebra is called *semi-simple* if it is isomorphic to the direct product of simple algebras. An example of a simple algebra a *skew field* where every nonzero element is invertible. An example of a non-commutative skew field is the *quaternion algebra* $H(a, b) = F + F\mathbf{i} + F\mathbf{j} + F\mathbf{k}$ with $\mathbf{i}^2 = a, \mathbf{j}^2 = b, \mathbf{k} = \mathbf{ij} = -\mathbf{ji}$. It is equipped with anti-involution $x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} \mapsto x' = x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k}$ such that $Nm(x) := xx' = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \in F$. If $\mathrm{Nm}(x) \neq 0$ for any $x \neq 0$, then $\frac{1}{\mathrm{Nm}(x)}x$ is the inverse of x, so $H(a, b)$ is a skew field. A quaternion algebra over a number field K is called *totally definite* if for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$, the change of scalars algebra H_σ over R is a skew field. If R splits over any real embedding of K, it is called *totally indefinite*.

If K is the center of a skew field D, then the degree of D over K is always a square. This is proved by showing that over some finite extension L of K, the algebra $R_L = R \otimes_K L$ *splits*, i.e. becomes isomorphic to a matrix algebra over L. For example, for the quaternion algebra $\mathbb{H} = \mathbb{Q}(-1, -1)$, the splitting field is $\mathbb{Q}(\sqrt{-1})$, and $\mathbb{H}$ becomes isomorphic to $\mathrm{Mat}_2(\mathbb{Q}(\sqrt{-1}))$.

A simple algebra R is isomorphic to the matrix algebra $\mathrm{Mat}_r(D)$ with coefficients with some skew field D over K. In particular, its dimension over K is always a square of some number.

A finite-dimensional algebra comes equipped with the *trace* F-bilinear map $R \times R \to F$ defined $(x, y) \mapsto \mathrm{Tr}(xy')$, where $\mathrm{Tr}(r)$ is the trace of the linear operator $R \to R, x \mapsto xr$. We can also define a *reduced trace* by considering R as an algebra over its center K.

The possible structure of the $\mathbb{Q}$-algebra $\mathrm{End}(A)_{\mathbb{Q}}$ is known. It is a finite-dimensional associative algebra R admitting an anti-involution[3] $x \to x'$ and a symmetric bilinear form $\mathrm{Tr} : R \times R \to \mathbb{Q}$ such that the quadratic form $x \mapsto \mathrm{Tr}(xx')$ is positive definite. An equivalent definition is that R is a semi-simple algebra over $\mathbb{Q}$ admitting a positive definite anti-involution. Such algebras have been classified by G. Scorza and A. Albert. Assume that R is a simple algebra over $\mathbb{Q}$. Let K be the center of R, it is a field admitting an involution σ, the restriction of the anti-involution of R. Let $K_0 = K^\sigma$ be the subfield of invariants. Then K_0 is a totally real algebraic number field and $K = K_0$ or is an imaginary quadratic extension of K_0. Since R is semi-simple, its dimension over K is equal to n^2 for some number n. Let $e = [K : \mathbb{Q}], e_0 = [K_0 : \mathbb{Q}]$. Each such algebra is isomorphic to the product of simple algebras.

An abelian variety is called *simple* if it is not isogenous to the product of positive-dimensional abelian varieties. An equivalent definition uses *Poincaré Reducibility Theorem* and asserts that an abelian variety is simple if and only if it does not contain an abelian subvariety of dimension

[3] An anti-involution means an involutive isomorphism from the algebra to the opposite algebra, i.e. the algebra with the same abelian group but with the multiplication law $x \cdot y := y \cdot x$.

$0 < k < g$. The endomorphism algebra $\mathrm{End}(A)_{\mathbb{Q}}$ of a simple abelian variety A is a skew-field. We have four possible cases for a simple algebra:

I $n = 1$, $R = K$ is a totally real field, $e = e_0 = \rho$, $e|g$;

II $n = 2$, R is totally indefinite quaternion algebra over K, $e = e_0$, $\rho = 3e, 2e|g$;

III $n = 2$, R is totally definite quaternion algebra over K, $e = e_0 = \rho$, $2e|g$;

IV $K_0 \neq K, e = 2e_0, \rho = e_0 d^2, e_0 d^2 |g$.

If A is not simple, its endomorphism algebra is not a skew-field, it is a simple or a semi-simple algebra.

Lecture 3

Elliptic curves

An *elliptic curve* is a one-dimensional abelian variety $A = \mathbb{C}/\Lambda$. We can find a special symplectic basis in Λ of the form $(\tau, 1)$, where $\tau \in \mathbb{H}$. The matrix of the symplectic form E on Λ with respect to this basis is the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since $i = -\frac{x}{y} + \frac{1}{y}\tau$, we get $E(i,1) = \frac{1}{y}$. By (1.7), the corresponding Hermitian form is equal to $\frac{1}{y} z\bar{z}'$ in agreement with (1.7). The Hermitian form H defines a principal polarization on E. It is defined by a line bundle L_0 of degree 1. We will always consider E as a one-dimensional principally polarized abelian variety.

Note that $\mathrm{Sp}(2,\mathbb{Z}) \cong \mathrm{SL}(2,\mathbb{Z})$, so the moduli space of elliptic curves is

$$\mathcal{A}_1 = \mathbb{H}/\mathrm{SL}(2,\mathbb{Z}),$$

where $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$. The quotient space is known to be isomorphic to $\mathbb{C}$, the isomorhism is defined by a holomorphic function $j : \mathbb{H} \to \mathbb{C}$ which is invariant with respect to $\mathrm{SL}(2,\mathbb{Z})$. It is called the *absolute invariant*. If τ is the period of E, then $j(\tau)$ is called the absolute invariant of E. We refer to the explicit definition of j to any (good) text-book on functions of one complex variable.

Let f be an endomorphism of A, then f_a is a complex number z and $f_r : \Lambda \to \Lambda$ is the map $\lambda \mapsto z\lambda$. In the basis $(\tau, 1)$ of Λ, the transformation f_r is given by an integer matrix $N = \left(\begin{smallmatrix} a_1 & a_3 \\ a_2 & a_4 \end{smallmatrix}\right)$ so that we have $(z\tau, z) = (a_1\tau + a_2, a_3\tau + a_4)$. This gives $z = a_3\tau + a_4$ and $(a_3\tau + a_4)\tau = a_1\tau + a_2$, and hence a quadratic equations for τ

$$a_3\tau^2 + (a_4 - a_1)\tau - a_2 = 0. \qquad (3.1)$$

It agrees with (2.2). The discriminant of the quadratic equation (2.2) is equal to

$$D = (a_4 - a_1)^2 + 4a_2a_3 = (a_1 + a_4)^2 - 4(a_1a_4 - a_2a_3) = \mathrm{Tr}(N)^2 - 4\det(N). \qquad (3.2)$$

Since $\mathrm{Im}(\tau) > 0$, we must have $a_3 \neq 0, D < 0$ or $a_3 = a_4 - a_1 = a_2 = 0$. In the latter case, the matrix N is a scalar matrix, and the endomorphism is just the multiplication $[a_1]$ and there is no condition on τ. In the former case

$$\tau = \frac{a_1 - a_4 + i\sqrt{-D}}{2a_3}.$$

It shows that $\tau \in \mathbb{Q}(\sqrt{D})$, i.e. it is an an imaginary quadratic algebraic number. Also

$$z = a_3\tau + a_4 = \tfrac{1}{2}(a_1 + a_4 + i\sqrt{-D})$$

belongs to the same field. For this reason an elliptic curve A is called an *elliptic curve with complex multiplication* by $K = \mathbb{Q}(\sqrt{D})$.

Multiplying (3.1) by a_3, we obtain that $a_3\tau$ and, hence z, satisfies a monic equation over $\mathbb{Z}$, hence belongs to the ring $\mathfrak{o}_K$ of integers of the field K. Note that formula (3.2) shows that, D is divisible by 4 if $\text{Tr}(N) = a_1 + a_4$ is even, and $D \equiv 1 \mod 4$ otherwise.

Recall that, if D is square-free, then $\mathfrak{o}_K$ has a basis, as a module over $\mathbb{Z}$, equal to $1, \frac{1}{2}(1+\sqrt{D})$ if $D \equiv 1 \mod 4$ or $1, \sqrt{D}$ otherwise. If $D = m^2D_0$, where D_0 is square-free, then $\text{End}(E)$ is an order in K. It is equal to $\mathbb{Z} + m\mathfrak{o}_K$ (see [Borevich-Shafarevich. Number Theory]). In any case, $\text{End}(E)_{\mathbb{Q}} \cong K$, so we are in case IV of classification of endomorphism rings of abelian varieties. Also, we see that $\text{End}(A)$ is an order $\mathfrak{o}$ in K. The lattice Λ must be a module over $\mathfrak{o}$, in fcat, one can show that it is a projective module of rank 1. Conversely, if we tale Λ to be such a module over an order $\mathfrak{o}$ in K, we obtain an elliptic curve $A = \mathbb{C}/\Lambda$ with $\text{End}(A) \cong \mathfrak{o}$. In this way one can show that there is a bijective correspondence between isomorphism classes of elliptic curves with $\text{End}(A) = \mathfrak{o}_K$ and the class group of K (i.e. the group of classes of ideals in $\mathfrak{o}_K$ modulo principal ideals, or, in a scheme-theoretical language, the Picard group of Spec $\mathfrak{o}_K$. The number of such classes if called the *class number* of K.

Note that $\text{Aut}(E) = \text{End}(E)^*$ can be larger than $\{\pm 1\}$ only if E admits complex multiplication with Gaussian integers (i.e. $D = -1$) or Eisenstein integers (i.e. $D = -3$). In fact, if $D \equiv 1 \mod 4$, an invertible algebraic integer $a + \frac{1}{2}b(1+\sqrt{D}), a, b \in \mathbb{Z}$ must satisfy $\text{Nm}(\frac{1+\sqrt{D}}{2}) = \pm 1$. This implies $D = -3$. Similarly, if $D \not\equiv 1 \mod 4$, we obtain $a^2 - Db^2 = \pm 1$ implies $D = -1$.

Remark 3. Let E be an elliptic curve with complex multiplication $\text{End}(E)_{\mathbb{Q}} = K$. Recall that E admits a Weierstrass equation

$$y^2 = x^3 + a_4x + a_6,$$

and the isomorphism class of E is determined by the value of the *absolute invariant*

$$j(E) = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

According to the *Theorem of Weber and Fuerter*, the j-invariant $j(E)$ is an algebraic integer such that $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$ and the field $K(j(E))$is a maximal unramified extension of K (see [Silverman, Arithmetic of elliptic curves], Appendix C). Assume that $j(E) \in \mathbb{Q}$, by the class fields theory this implies that the class number of K is equal to 1. Also, it is known that $j(E) \in \mathbb{Q}$ if and only if E can be defined over $\mathbb{Q}$. There are exactly nine imaginary quadratic fields K with class number 1. They are the fields $\mathbb{Q}(\sqrt{-d})$, where

$$d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

The corresponding values of the absolute invariants are

$$2^6 \cdot 3^3, \quad 2^6 \cdot 5^3, \quad 0, \quad -3^3 \cdot 5^3, \quad -2^{15}, \quad -2^{15} \cdot 3^3, \quad -2^{18} \cdot 3^3 \cdot 5^3, \; -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3,$$

$$-2^18 \cdot 3^3 \cdot 5^3 \cdot 23^3, \quad 2^3 \cdot 3^3 \cdot 11^3, \quad 2^4 \cdot 3^3 \cdot 5^3, \quad 3^3 \cdot 5^3 \cdot 17^3, \; -3 \cdot 2^{15} \cdot 5^3.$$

Let $f : E \to E$ be an endomorphism of E of finite degree $n > 0$. By Hurwitz' formula, the map f is an unramified finite cover of degree n. Its kernel is a finite subgroup T of order n of E. The group $E[n]$ of n-torsion elements of $E = \mathbb{C}/\Lambda$ is isomorphic to $\frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$. Assume that f_r is defined by a matrix N whose entries are mutually coprime (otherwise the endomorphism a composition of an endomorphism g with g_r satisfying this property and multiplication by an integer). The theory of elementary divisors allows us to find two bases (γ_1, γ_2) and (γ_1', γ_2') in Λ such that $(f_r(\gamma_1), f(\gamma_2)) = (n\gamma_1', \gamma_2')$. Since $j(\tau)$ depends only on Λ, we obtain that $j(tau) = j(n\tau)$. It is known that there exists a polynomial $\Phi_n(X, Y)$ with integer coefficients such that $\Phi(j(\tau), j(n\tau)) \equiv 0$ for any $\tau \in \mathbb{H}$. The equation $\Phi_n(X, Y) = 0$ is called the *modular equation* of level n. Thus the number of elliptic curves admitting an endomorphism of degree n is equal to the number of solutions of the equation $\Phi_n(x, x) = 0$. It is a finite set of points, hence an algebraic subvariety of $\mathcal{A}_1 \cong \mathbb{A}^1$. It is a 0-dimensional *Shimura variety*. It has been computed by R. Fricke and it is equal to $h_0(-n) + h_0(-4n)$ if $n \equiv 2, 3 \mod 4$, and $h_0(-4n)$ if $n \equiv 1 \mod 4$. Here $h_0(-d)$ is the class number of primitive quadratic integral positive definite forms with discriminant equal to $-d$.

Let $f : E \to E'$ be an *isogeny* of elliptic curves and $g : E' \to E$ be its inverse, i.e. $g \circ f = [n]$, where n is the degree of f. Let f_a be given by a complex number z and g be given by a complex number z'. Then $zz' = d$. Also we know that $|z|^2 = \det f_r = d$. Thus, we obtain that $z' = \bar{z}$ is the complex conjugate of z.

Let $A = E_1 \times \cdots \times E_g$ be the product of g isogenous elliptic curves. We assume that $\mathrm{End}(E_i) = \mathbb{Z}$. Let α_{ij} be an isogeny $E_i \to E_j$ of minimal degree so that any isogeny $E_i \to E_j$ can be written in form $[d_{ij}] \circ \alpha_{ij}$ (which we denote, for brevity, by $d_{ij}\alpha_{ij}$) for some integer d_{ij} and a complex number α_{ij}. Obviously $\alpha_{ii} = 1$.

The analytic representation of an endomorphism $f : A \to A$ is given by a matrix

$$M = \begin{pmatrix} d_{11} & d_{12}\alpha_{12} & \dots & d_{1g}\alpha_{ig} \\ d_{21}\overline{\alpha_{12}} & d_{22} & \dots & d_{2g}\alpha_{2g} \\ \vdots & \vdots & \vdots & \vdots \\ d_{g1}\overline{\alpha_{1g}} & d_{g2}\overline{\alpha_{2g}} & \dots & d_{gg} \end{pmatrix}.$$

We may choose the period matrix of A to be equal to the diagonal matrix $\mathrm{diag}[\tau_1, \dots, \tau_g]$, where $\tau_i = x_i + \sqrt{-1}y_i$ is the period of E_i. Let us choose a principal polarization L_0 on A to be the reducible one coming from the principal polarizations on the curves E_i. Its Hermitian form is given by the diagonal matrix $\mathrm{diag}[y_1^{-1}, \dots, y_g^{-1}]$. Assume that A has another principal polarization L and M is a symmetric endomorphism corresponding to L. By (2.1), the matrix of the Hermitian form H corresponding to L is equal to the matrix

$$M' = \mathrm{diag}[y_1^{-1}, \dots, y_g^{-1}] \cdot M \tag{3.3}$$

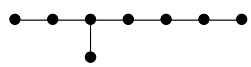
In particular, this implies that $y_i d_{ij} = y_j d_{ji}$.

Assume now that $E_1 = \ldots = E_g = E$ and $\mathrm{End}(E) = \mathbb{Z}$. Since E has no complex multiplications, $\alpha_{ij} = 1$, hence M is a symmetric integral matrix. It follows from (2.2) that f_r is given by the matrix $N = \left(\begin{smallmatrix} M & 0 \\ 0 & M \end{smallmatrix}\right)$. Since we are looking for f defined by a principal polarization, f must be an isomorphism, hence $\det M = 1$. We know also that the coefficients of its characteristic polynomial are positive rational numbers. This implies that M is positive definite. Let $(\gamma_1, \dots, \gamma_{2g}) = (\tau e_1, \dots, \tau e_g, e_1, \dots, e_g)$ be a basis of $\Lambda_{\mathbb{R}}$. It follows from (3.3) that the matrix of the symplectic form corresponding to H in this basis is equal to (a_{ij}), where $a_{ij} = y^{-1}\mathrm{Im}(H(\gamma_i, \gamma_j))$. We get for $1 \le i < j \le g$

$$a_{ij} = y^{-1}\mathrm{Im}(H(e_i, e_j)|\tau|^2) = 0,\ a_{i,j+g} = y^{-1}\mathrm{Im}(H(e_i, e_j)\tau) = d_{ij}.$$

This implies that the type D of the polarization L is equal to the matrix (d_{ij}) (reduced to the diagonal form).

It is known that a unimodular positive definite matrix of rank $g \le 7$ is isomorphic to the odd lattice I^r defined by the quadratic form $x_1^2 + \ldots + x_g^2$. By above this implies that the only principal polarization on an abelian variety $A = E^g$ is of the form $\sum_{i=1}^g p_i^*(\text{point})$, where p_i is the projection to the i-th factor. In particular, A cannot be isomorphic to the Jacobian variety of a curve of genus g. However, if $g = 8$, there is one more positive definite unimodular quadratic lattice defined by the matrix $2I_8 - P_{E_8}$, where P_{E_8} incidence matrix of the Dynkin diagram of type E_8

E_8 

Remark 4. It is known that the rank of any positive definite unimodular quadratic lattice is divisible by 8 [J.-P. Serre, Cours de Arithmetique], 2.3. Thus, if E has no complex multiplication, the product of r copies of E does not admit a principal polarization unless r is divisible by 8. Note that there is only positive definite unimodular quadratic lattices of rank 16 not isomorphic to $E_8 \oplus E_8$ and there are 24 non-isomorphic such lattices of rank 24, the Leech lattice is among them. So we have 2 (resp. 24) principally polarized abelian varieties isomorphic to E^8 (resp. E^{12}), where E is an elliptic curve. Do they have any geometric meaning, e.g. being the Prym or Jacobian varieties?

Example 5. Let M be a *quadratic lattice*, i.e. a free abelian group of finite rank equipped with a symmetric bilinear form $B : M \times M \to \mathbb{Z}$. Assume that the rank of M is an even number $2k$ and the bilinear from is positive definite (when tensored with $\mathbb{R}$). Assume also that the orthogonal group of M (i.e. the subgroup of $\mathrm{Aut}(M)$ that preserves the symmetric form) contains an element ι such that $\iota^2 = -\mathrm{id}_M$. Then we can use ι to define a complex structure on $W = M_{\mathbb{R}}$ and define a hermitian form H by taking $E(x, y) := -B(\iota(x), y)$ so that $E(\iota(x), y) = B(x, y)$ is symmetric and positive definite, and

$$E(y, x) = -B(\iota(y), x) = -B(x, \iota(y)) = -B(\iota(x), \iota^2(y)) = B(\iota(x), y) = -E(x, y)$$

is skew-symmetric, obviously non-degenerate.

Let us consider M as a module over $\mathbb{Z}[i]$ by letting i act on M as the isometry ι. Since $\mathbb{Z}[i]$ is a principal ideal domain, we get $M \cong \mathbb{Z}[i]^k$ and we have an isomorphism $(M_{\mathbb{R}}, \iota) \cong \mathbb{C}^k$, so that M can be identified with the lattice Λ with a basis equal to the union of k copies of the basis $(i, 1)$. Obviously, the abelian variety $A = \mathbb{C}^k/M$ becomes isomorphic to the product $E_{\sqrt{-1}}^k$, where $E_{\sqrt{-1}}$ is the elliptic curve with complex multiplication by $\mathbb{Z}[i]$. On the other hand, if we take M to be an even unimodular lattice of rank $2k$, then our Hermitian form H defines an indecomposable principal polarization. As we remarked before such lattices M exist only in dimension divisible by 8. So, k is divisible by 4.

If $k = 4$, there exists a unique such lattice, the E_8-lattice M. The abelian 4-fold $A = \mathbb{C}^4/M$ is remarkable for many reasons. For example, it is isomorphic to the intermediate Jacobian of a Weddle quartic double solid, i.e. a nonsingular model of the double cover of $\mathbb{P}^3$ branched along a Weddle quartic surface with 6 nodes (see [R. Varley, Amer. J. Math. 108 (1986), no. 4]). Another remarkable property of A is that the theta function corresponding to its indecomposable principal polarization has maximal value of critical points (equal to 10 in dimension 4 for simple abelian varieties which are not isomorphic to the Jacobian variety of a hyperelliptic curve) (see [O. Debarre, C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), no. 20]).

Recall that the *Jacobian variety* $\mathrm{Jac}(C)$ of a compact Riemann surface C of genus g (or, equivalently, nonsingular complex projective curve of genus g) is an abelian variety whose period matrix is equal to

$$\Pi = (\int_{\gamma_i} \omega_j),$$

where $\omega_1, \ldots, \omega_g$ is a basis of holomorphic 1-forms on C and $\gamma_1, \ldots, \gamma_{2g}$ is a basis of $H_1(C, \mathbb{Z})$. One can always choose a basis of $H_1(C, \mathbb{Z})$ and a basis in $\Omega^1(C)$ such that the period matrix $\Pi = [\tau I_g]$, where $\tau \in \mathcal{Z}_g$. In particular, $\mathrm{Jac}(C)$ has always a principal polarization L_0. The unique nonzero section of L_0 has the divisor of zeros equal to the image of the symmetric product $C^{(g-1)} = C^g/\mathfrak{S}_{g-1}$ under the *Abel-Jacobi map*

$$C^{(g-1)} \to \mathrm{Jac}(C), \quad \sum_{k=1}^{g-1} c_k \mapsto \sum_{k=1}^{g-1} (\int_{p_1}^{c_k} \omega_1, \ldots, \int_{p_{g-1}}^{c_k} \omega_g) \mod \Pi\mathbb{Z}^{2g},$$

where $p_1, \ldots, p_{g-1}$ are fixed points on C.

Example 6. Following [T. Hayashida, M. Nishi, J. Math. Soc. Japan **17** (1965)] let us give an example of the Jacobian of a curve of genus 2 isomorphic to the product of two isomorphic elliptic curves. Let $K = \mathbb{Q}(-m)$ be an imaginary quadratic field and $\mathfrak{o}$ be its ring of integers. We assume that the class number of K is greater than 1 and choose a non-principal ideal $\mathfrak{a}$ on $\mathfrak{o}$. For example, we can take $m = 5$. Since $-5 \equiv 3 \mod 4$, the ring $\mathfrak{o}$ is generated over $\mathbb{Z}$ by 1 and $\omega = \sqrt{-5}$. We may take for $\mathfrak{a}$ the ideal generated by $(2, 1+\omega)$. In fact, $\mathrm{Nm}(\mathfrak{a}) = (\mathrm{Nm}(2), \mathrm{Nm}(1+\omega)) = (4, 6) = (2)$ and since the equation $\mathrm{Nm}(x + y\omega) = x^2 + 5b^2 = 2$ has no integer solutions, we obtain that the ideal $\mathfrak{a}$ is not principal. Let

$$E = \mathbb{C}/\mathfrak{o} = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\omega.$$

Consider a homomorphism $\phi : E \to E \times E$ defined by $x \mapsto (2x, (1+w)x)$. Let E' be the image of this homomorphism. Let $E_1 = E \times \{0\}$, $E_2 = \{0\} \times E$, and Δ be the diagonal. Let us compute the intersection indices of E' with these three curves.

Suppose $\phi(x) \in E_1$, then $x(1+\omega) \in \mathfrak{o}$, hence there exists $m, n \in \mathbb{Z}$ such that

$$x = \frac{m + n\omega}{1+\omega} = \frac{1}{6}(m + 5 + (m-n)\omega) \in \mathbb{Z}\frac{1+\omega}{6} + \mathbb{Z}.$$

This shows that there are 3 intersection points $(0,0), (\frac{1+\omega}{3}, 0), (\frac{2(1+\omega)}{3}, 0)$.

Suppose $\phi(x) = (0, (\omega+1)x) \in E_2$, then $2x \in \mathfrak{o}$, hence there are two intersection points $(0,0), (0, \frac{1}{2}(1+\omega))$.

Suppose $\phi(x) = (2x, (1+\omega)x) \in \Delta$, then $(1-\omega)x = 2x - (1+w)x \in \mathfrak{o}$. This implies that $x \in \frac{1+\omega}{6}\mathbb{Z} + \mathbb{Z}$, hence there are 3 intersection points $(0,0), (\frac{1+\omega}{3}, \frac{1+\omega}{3}), (\frac{2(1+\omega)}{3}, \frac{2(1+\omega)}{3})$.

Now we consider the divisor

$$C = 2\Delta + E' + E_1 - 2E_2.$$

We have $C \cdot \Delta = 2, C \cdot E' = 5, C \cdot E_1 = 3, C \cdot E_2 = 5, C^2 = 2$. By Riemann-Roch, C is an effective divisor class, so we may assume that C is a curve of arithmetic genus 2. If C is reducible, then $C = C_1 + C_2$ is the sum of two elliptic curves with $C_1 \cdot C_2 = 1$, and we may assume that one of its components, say C_1, intersects Δ and E_1 with multiplicity 1. We have $C_2 = C - C_1 \sim 2\Delta + E' + E_1 - 2E_2 - C_1$. Intersecting with C_1, we get $1 = 4 - 2(E_2 \cdot C_1)$, a contradiction. Thus C is an irreducible curve of arithmetic genus 2. It is known that this implies that C is a smooth curve of genus 2 and $A \cong \text{Jac}(D)$ (see [A. Weil, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957** (1957)]).[1] and as we remarked before, it must be a nonsingular curve of genus 2, and $A = E \times E$ is isomorphic to $\text{Jac}(C)$.

[1] To see this use one considers the normalization map $\bar{D} \to A$ and the dual map $\hat{A} \to \text{Jac}(\bar{D})$ and proves that it is injective, hence the geometric genus coincides with the arithmetic genus.

Lecture 4

Abelian surfaces with real multiplication

Let A be an abelian variety of dimension 2, i.e. an abelian surface. The Poincaré duality equips the group $H^2(A,\mathbb{Z}) = \mathbb{Z}^6$ with a structure of a unimodular quadratic lattice of signature $(3,3)$. It is an even lattice, i.e. its values are even integers. By Milnor's theorem, $H^2(A,\mathbb{Z}) \cong U \oplus U \oplus U$, where U is a hyperbolic plane over $\mathbb{Z}$, i.e. its quadratic form could be defined by a matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and the direct sum is the orthogonal direct sum. Let T_A be the orthogonal complement of $\mathrm{NS}(A)$ in $H^2(A,\mathbb{Z})$. It is a quadratic lattice of signature $(2, 4-\rho)$, and we have an orthogonal decomposition of quadratic lattices

$$H^2(A,\mathbb{Z}) = \mathrm{NS}(A) \oplus T_A.$$

The quadratic form on $\mathrm{NS}(A)$ is defined by the intersection theory of curves on an algebraic surface. For any irreducible curve C on A, the adjunction formula $C^2 + C \cdot K_A = C^2 = -2\chi(\mathcal{O}_C)$, together with the fact that A has no rational curves, gives $C^2 \geq 0$ and $C^2 = 0$ if and only if C is a smooth elliptic curve. By writing any effective divisor as a sum of irreducible curves, we obtain that $D^2 \geq 0$ on the cone $\mathrm{Eff}(A)$ in $\mathrm{NS}(A)_{\mathbb{R}}$ of classes of effective divisors modulo homological equivalence. By Hodge's Index Theorem, we have $D \cdot C \geq 0$ for any effective divisors D and C. This implies that $\mathrm{Eff}(A)$ coincides with the cone $\mathrm{Nef}(A)$ of nef divisor classes. The latter is known to be the closure of the cone $\mathrm{Amp}(A)$ of ample divisor classes. By Riemann-Roch and the vanishing Theorem, $h^0(D) = D^2/2$ for any ample divisor D. Thus the restriction of the trace quadratic form on $\mathrm{End}(A)$ to $\mathrm{Amp}(A)$ is equal to twice of the restriction of the intersection form to $\mathrm{Amp}(A)$.

Suppose A is a simple abelian surface with $\mathrm{End}(A) \neq \mathbb{Z}$. According to the classification of possible endomorphism algebras, we have four possible types:

(i) $\mathrm{End}(A)_{\mathbb{Q}}$ is a totally real quadratic field K and $\rho = 2$;

(ii) $\mathrm{End}(A)_{\mathbb{Q}}$ is a totally indefinite quaternion algebra over $K = \mathbb{Q}$ and $\rho = 3$;

(iii) $\mathrm{End}(A)_{\mathbb{Q}}$ is a totally imaginary quadratic extension K of a real quadratic field K_0 and $\rho = 2$;

Observe that we have intentionally omitted the cases when $\mathrm{End}(A)_{\mathbb{Q}}$ is a definite quaternion algebra and when $\mathrm{End}(A)_{\mathbb{Q}}$ is a totally imaginary quadratic extension of $\mathbb{Q}$. These types of algebras occur for a non-simple abelian surface. In the former case it must be the product of two elliptic curves with complex multiplication by $\sqrt{-1}$ (see [CAV], Chapter 9, Example 9.5.5 and Exercises

1). In the latter case, $\mathrm{End}(A)_{\mathbb{Q}}$ must be isomorphic to an indefinite quaternion algebra (loc.cit. Exercise 4 in Chapter 4).

Let us first discuss abelian surfaces with type (i) endomorphism ring. First observe that the Rosati involution acts identically on the totally real field $K \subset \mathrm{End}(A)$, hence all endomorphisms come from $\mathrm{NS}(A)$. Let

$$\tau = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix}$$

be the period matrix of A. We assume that $A = \mathbb{C}^2/\mathbb{Z}^2 + \mathsf{D}\mathbb{Z}^2$ has a primitive polarization of degree n. Its type is defined by the diagonal matrix $\mathsf{D} = \mathrm{diag}[1, n]$. Let $f \in \mathrm{End}^s(A)$, where f_a is defined by a matrix M and f_r is defined by a matrix N as in (2.2). Since f is symmetric, N satisfies (2.4). We easily obtain that

$$\begin{pmatrix} A_1 & A_3 \\ A_2 & A_4 \end{pmatrix} = \begin{pmatrix} a_1 & na_2 & 0 & nb \\ a_3 & a_4 & -b & 0 \\ 0 & nc & a_1 & na_3 \\ -c & 0 & a_2 & a_4 \end{pmatrix}.$$

By (2.2) and (2.3), we have

$$M = (\tau A_3 + \mathsf{D}A_4)\mathsf{D}^{-1}, \quad M\tau = \tau A_1 + \mathsf{D}A_2,$$

and

$$(\tau A_3 + \mathsf{D}A_4)\mathsf{D}^{-1}\tau = \tau A_1 + \mathsf{D}A_2.$$

The left-hand side in the secon equality is equal to

$$\begin{pmatrix} 0 & b(-z_2^2 + z_1z_3) \\ b(z_2^2 - z_1z_3) & 0 \end{pmatrix} + \begin{pmatrix} a_1z_1 + a_3z_2 & a_1z_2 + a_3z_3 \\ na_2z_1 + a_4z_2 & na_2z_2 + a_4z_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1z_1 + a_3z_2 & b(-z_2^2 + z_1z_3) + a_1z_2 + a_3z_3 \\ b(z_2^2 - z_1z_3) + na_2z_1 + a_4z_2 & +na_2z_2 + a_4z_3 \end{pmatrix}.$$

The right-hand side is equal to

$$\begin{pmatrix} a_1z_1 + a_3z_2 & na_2z_1 + a_4z_2 + nc \\ a_1z_2 + a_3z_3 - nc & na_2z_2 + a_4z_3 \end{pmatrix}.$$

Comparing the entries of the matrices in each side, we find a relation

$$b(z_2^2 - z_1z_3) + a_2nz_1 + (a_4 - a_1)z_2 - a_3z_3 + nc = 0.$$

We rename the coefficients to write it in the classical form to obtain what G. Humbert called the *singular equation* for the period matrix τ:

$$naz_1 + bz_2 + cz_3 + d(z_2^2 - z_1z_3) + ne = 0. \tag{4.1}$$

We also assume that $(a, b, c, d, e) = 1$. In this new notations, the matrix $N_0 = N - a_1I_4$ representing $(f_0)_r = (f - a_1\mathrm{id})_r$ can be rewritten in the form

$$N_0 = -a_1I_4 + N = \begin{pmatrix} 0 & na & 0 & nd \\ -c & b & -d & 0 \\ 0 & ne & 0 & -nc \\ -e & 0 & a & b \end{pmatrix}. \tag{4.2}$$

and $(f_0)_a$ is represented by the matrix

$$M_0 = \begin{pmatrix} -nz_2 & nz_1 - c \\ -nz_3 + na & nz_2 + b \end{pmatrix}. \tag{4.3}$$

We have

$$\mathrm{Tr}(N_0) = 2\mathrm{Tr}(M_0) = 2b,\ \det(N_0) = \det(M_0)^2 = n^2(ac+ed)^2.$$

Thus f_0 satisfies a quadratic equation

$$t^2 - bt + n(ac+ed) = 0, \tag{4.4}$$

so that $1, f_0$ generate a subalgebra $\mathfrak{A}$ of rank 2 of $\mathrm{End}^s(A)$ isomorphic to

$$\mathfrak{A} \cong \mathbb{Z}[t]/(t^2 - bt + n(ac+ed)).$$

The discriminant Δ of the equation (4.4) is equal to

$$\Delta = b^2 - 4n(ac+ed). \tag{4.5}$$

It is called the *discriminant* of the singular equation. Note that, if b is even, $D \equiv 0 \mod 4$, otherwise $D \equiv 1 \mod 4$.

Since we know that the eigenvalues of M are real numbers,

$$\Delta > 0. \tag{4.6}$$

Thus if Δ is not a square, the algebra $\mathfrak{A}$ is an order in the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$. On the other hand, if Δ is a square, then the algebra $\mathfrak{A}$ has zero divisors defined by the integer roots $\frac{1}{2}(b \pm \sqrt{\Delta})$ of equation (4.4).

Let L_Δ be the line bundle that is mapped to f_0 inder $\alpha : \mathrm{NS}(A) \to \mathrm{End}^s(A)$. Applying (2.6), we obtain that

$$(L_0, L_\Delta) = nb = \tfrac{1}{2}(L_0^2)b, \quad (L_\Delta^2) = \tfrac{1}{2}n(b^2 - \Delta). \tag{4.7}$$

Thus the sublattice of $\mathrm{NS}(A)$ generated by L_0, L has discriminant equal to $(L_0)^2(L^2) - (L_0, L)^2 = -n^2\Delta$.

When L_Δ is ample, we can also determine the type of the polarization defined by L_Δ. It is equal to the type of the alternating form given by the matrix

$${}^tN_0 J_D N_0 = \begin{pmatrix} 0 & na & 1 & nd \\ -c & b & -d & n \\ -1 & ne & 0 & -nc \\ -e & -n & a & b \end{pmatrix}. \tag{4.8}$$

Let $\mathcal{A}_{2,n} = \mathcal{Z}_2/\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ be the coarse moduli space of principally polarized abelian surfaces. We denote by $\mathcal{H}_\Delta$ the set of period matrices $\tau \in \mathcal{Z}_2$ satisfying a singular modular equation with discriminant Δ. Let

$$\mathrm{Hum}_n(\Delta) = \mathcal{H}_\Delta/\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$$

be the image of $\mathcal{H}_\Delta$ in $\mathcal{A}_{2,n} := \mathcal{A}_{2,\mathsf{D}}$. This is the locus of isomorphism classes of abelian surfaces with primitive polarization of degree n that admit an embedding of a quadratic algebra $\mathbb{Z}[t]/(t^2 +$

$\alpha t + \beta)$ with discriminant $\Delta = \alpha^2 - 4\beta$ in End(A). We call it the *Humbert surface* of discriminant Δ.

Suppose $\tau \in \mathcal{H}_\Delta$ and let $\tau' = M \cdot \tau$ for some $M \in \mathrm{Sp}(4, \mathbb{Z})$. If τ satisfies a singular equation (4.1), then the matrix N_0 defining an endomorphism of $\mathbb{C}^2/\Lambda_\tau$ changes to ${}^tM^{-1} \cdot N_0 \cdot M$ ([CAV], 8.1). Thus τ' satisfies another singular equation although with the same discriminant.

We will prove later the following theorem, which is in the case $n = 1$ due to G. Humbert.

Theorem 7. *Every irreducible component of the Humbert surface* $\mathrm{Hum}_n(\Delta)$ *is equal to the image in* $\mathcal{Z}_2/\mathrm{Sp}(J_D, \mathbb{Z})$ *of the surface given by the equation*

$$z_1 + bz_2 + cnz_3 = 0, \tag{4.9}$$

where $\Delta = b^2 - 4nc, 0 \le b < 2n$. *The number of irreducible components is equal to*

$$\#\{b \mod 2n : b^2 \equiv \Delta \mod 4t\}.$$

Assume Δ is not a square. Then $\mathrm{End}^s(A)_\mathbb{Q}$ contains the field $K = \mathbb{Q}(\sqrt{D})$. Let $\mathfrak{o}_K$ be its ring of integers defined by equation (4.4). The lattice Λ aquires a structure of a rank 1 module over $\mathfrak{o}_K$ via action of f_r. It is known that any such module is isomorphic to $\mathfrak{o}_K \oplus \mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $\mathfrak{o}_K$. Let $\Gamma = \mathrm{SL}(\mathfrak{o}_K \oplus \mathfrak{a})$ be the group of automorphisms of this module represented by matrices with unimodular matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with coefficients in $\mathfrak{o}_K$ such that, for any $x \in \mathfrak{o}_K, y \in \mathfrak{a}$, we have $\alpha x + \beta y \in \mathfrak{o}_K, \gamma x + \delta y \in \mathfrak{a}$. It is called the *Hilbert modular group*.The group Γ acts on $\mathbb{H} \times \mathbb{H}$ by

$$(z_1, z_2) \mapsto (\frac{\alpha z_1 + \gamma}{\beta z_1 + \delta}, \frac{\alpha z_1 + \gamma}{\beta z_1 + \delta}).$$

We also consider a little larger group $\tilde{\Gamma}$ acting on $\mathbb{H} \times \mathbb{H}$ by adding to Γ an automorphism $\sigma : (z_1, z_2) \mapsto (z_2, z_1)$.

Corollary 8. *Assume that* Δ *is not a square. Then the irreducible component defined by* (4.9) *is the image of a degree 1 map* $\mathbb{H} \times \mathbb{H}/\Gamma \to \mathcal{A}_{2,n} = \mathcal{Z}_2/\mathrm{Sp}(J_D, \mathbb{Z})$ *if* $b \not\equiv 0 \mod n$ *and it is the image of* $\mathbb{H} \times \mathbb{H}/\tilde{\Gamma} \to \mathcal{A}_{2,n}$ *if* $b \equiv 0 \mod n$.

Proof. (see [G. van der Geer, Hilbert modular surfaces], iX, Proposition 2.6). Let $S = \begin{pmatrix} 1 & \frac{1}{2}(b+\sqrt{\Delta} \\ 1 & \frac{1}{2}(b-\sqrt{\Delta}) \end{pmatrix}$. Write Δ in the form $\Delta = b^2 - 4nc$. Consider the map

$$\mathbb{H} \times \mathbb{H} \to \mathcal{Z}_2, \ (z_1, z_2) \mapsto S^{-1} \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} {}^tS^{-1}.$$

One checks immediately that the image is equal to the subset of matrices $\tau = \begin{pmatrix} -bx_2 - cnx_3 & x_2 \\ x_2 & x_3 \end{pmatrix}$. Next, we compute the subgroup of $\mathrm{Sp}(J_D, \mathbb{Z})$ that leaves invariant the image of the map. It turns oyt to be the group Γ or $\tilde{\Gamma}$. $\square$

Lecture 5

$\triangle$ is a square

.

Let $i : B \hookrightarrow A$ be an abelian subvariety of an abelian variety A with primitive polarization L_0 of degree n. Let $L_0' = i^*(L_0)$ be the induced polarization of B and $\phi_B : B \to \hat{B}$ be the isogeny defined by L_0'. Consider the composition

$$\mathrm{Nm}_B := \phi_{L_0'}^{-1} \circ i^* \circ \phi_{L_0} \circ i : A \to \hat{A} \to \hat{B} \to B \to A.$$

It is called the *norm-endomorphism* associated to B. It is a symmetric endomorphism corresponding to the Hermitian form obtained by restricting the Hermitian form of L_0 to $H_1(B, \mathbb{C}) \subset H_1(A, \mathbb{C})$ and then extending it to $H_1(A, \mathbb{C})$ by zero. Also it is easy to see that $\mathrm{Nm}_B^2 = e(L_0')\mathrm{Nm}_B$. Taking $f = \mathrm{Nm}_B$ and $d = e(L_0')$, we obtain that f satisfies the equation $f^2 - df = 0$.

Let us go back to abelian surfaces and assume that $\Delta = k^2$ is a square. Then the minimal polynomial defining the corresponding endomorphism has roots $\alpha_\pm = \frac{1}{2}(b \pm k)$. Since $\Delta \equiv b^2 \mod 4n$, $\alpha_\pm \in \mathbb{Z}$. The equation

$$0 = (f - \alpha_+ \mathrm{id}_A)(f + \alpha_- \mathrm{id}_A) = 0$$

shows that the endomorphisms $g_\pm = f - \alpha_\pm \mathrm{id}_A$ satisfy the equations

$$g_\pm^2 = \pm k g_\pm, \quad g_+ \circ g_- = 0. \tag{5.1}$$

Let $E_\pm = g_\pm(A) \subset A$. These are elliptic curves on A, and we have exact sequences of homomorphisms of abelian varieties:

$$0 \to E_+ \longrightarrow A \xrightarrow{g_-} E_- \to 0, \quad 0 \to E_- \longrightarrow A \xrightarrow{g_+} E_+ \to 0$$

Note that $g_\pm | E_\pm = [\pm k]$, hence $E_+ \cdot E_- = \#\mathrm{Ker}([k]) = k^2$. Since the kernel of the isogeny

$$E_+ \times E_- \to A, (x, y) \mapsto x + y$$

is the group $E_+ \cap E_-$, we obtain that its degree is equal to k^2.

Suppose $A = \mathrm{Jac}(C)$ for some curve C of genus 2 and the polarization $L_0 \cong \mathcal{O}_A(C)$ is the principal polarization defined by C embedded in $\mathrm{Jac}(C)$ via the Abel-Jacobi map. Since k is equal to the trace of the characteristic equation fro g_+, formula (2.8) and the projection formula imply that

$$\mathrm{Tr}(g_+^2) = \mathrm{Tr}(k g_+) = k\mathrm{Tr}(g_+) = k^2 = (g_+^*(C), C) = (C, (g_+)_*(C)) = d_+ C \cdot E_+ = d_+ d_-,$$

where $d_\pm$ is the degree of the projection $g_\pm|C : C \to E_\pm$. Since $d_+, d_- \le k$, we get $d_+ = d_- = k$. Obviously, $k > 1$ since C is not isomorphic to an elliptic curve.

Thus we obtain the following.

Theorem 9. *Suppose a period τ of $\mathrm{Jac}(C)$ satisfies a singular equation with discriminant $\Delta = k^2 > 1$, then C is a degree k cover of an elliptic curve.*

Conversely, assume that there exists a degree k cover $q : C \to E$, where E is an elliptic curve. Then the cover is ramified, hence the canonical map $q^* : E = \mathrm{Jac}(E) \to A = \mathrm{Jac}(C)$ is injective. We identify its image with E. Let $N : \mathrm{Jac}(C) \to \mathrm{Jac}(E) = E$ be the norm map (defined on divisors by taking q_*). Then $N \cdot q^* : E \to E$ is the map $[k]$. Let $g = \mathrm{Nm}_E : A \to A$. Then, it follows from the definition of the norm-endomorphism that $g^2 = kg$. Arguing as above, we find that the symmetric endomorphism Nm_E defines a singular equation for a period of $\mathrm{Jac}(C)$ whose discriminant is equal to k^2.

Example 10. Assume that a period of $A = \mathrm{Jac}(C)$ satisfies a singular equation with $\Delta = 4$, so that C is a bielliptic curve, i.e. there exists a degree 2 cover $\alpha : C \to E$. Let $\iota : C \to C$ be the deck transformation of this cover. If C is given by the equations

$$y^2 - f_6(x) = 0 \tag{5.2}$$

then, we may choose (x, y) in such a way that ι is given by $(x, y) \mapsto (y, -x)$ and $f_6(x) = g_3(x^2)$. Let

$$v^2 - g_3(u) = 0$$

be the equation of an elliptic curve E. The map $(x, y) \to (x^2, v)$ defines the degree 2 cover $\alpha : C \to E$. Let du/v be a holomorphic 1-form on E, then $\alpha^*(du/v) = xdx/y$ is a holomorphic 1-form on C. The involution ι^* acts on the space of holomorphic 1-forms on C spanned by dx/y and xdx/y, and decomposes it into two eigensubspaces with eigenvalues $+1$ and -1. Consider the involution $\iota' : (x, y) \mapsto (-y, -x)$. The field of invariants is generated by y^2, xy, x^2. Again $f_6 = g_3(x^2)$ and we get the equation $(xy)^2 = x^2 g_3(x^2)$. Thus the quotient $C/(\iota')$ is another elliptic curve with equation

$$v^2 - ug_3(u) = 0.$$

The map $\alpha' : C \to E'$ is given by $(u, v) \mapsto (x^2, xy)$. We have $\alpha'^*(du/v) = 2dx/y$. Thus any hyperelliptic integral $\int \frac{a+bdx}{y}$ can be written as a linear combination of elliptic integrals. This was one of the motivation for the work of G. Humbert.

One may ask how to find whether a hyperelliptic curve given by equation (5.2) admits a degree 2 map onto an elliptic curve in terms of the coefficients of the polynomial f_6. The answer was known in the 19th century. Let us explain it. First let us put a *level* on the curve by ordering the the Weierstrass points $(0, x_i), f_6(x_i) = 0, i = 1, \ldots, 6$. By considering the Veronese map $\nu : \mathbb{P}^1 \to \mathbb{P}^2$ we put these 6 points $(x_i, 1)$ on a conic K in $\mathbb{P}^2$. Let $p_i = \nu(x_i)$. Applying Proposition 9.4.9 from [CAG], we obtain that the following is equivalent:

- there exists an involution τ of $\mathbb{P}^1$ with orbits $(x_1, x_2), (x_3, x_4), (x_5, x_6)$;
- the lines $\overline{p_1, p_2}, \overline{p_3, p_4}, \overline{p_5, p_6}$ intersect;
- the three quadratic polynomial $(x - x_1)(x - x_2), (x - x_3)(x - x_4), (x - x_5)(x - x_6$ are linearly dependent;

- if $a_it_0 + E_it_1 + c_it_2 = 0$ are the equations of the three lines, then

$$D_{12,34,56} = \det \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & E_2 & c_2 \\ a_3 & E_3 & c_3 \end{pmatrix} = \det \begin{pmatrix} 1 & x_1+x_2 & x_1x_2 \\ 1 & x_3+x_4 & x_3x_4 \\ 1 & x_5+x_6 & x_5x_6 \end{pmatrix} 0.$$

(see [**?**], p. 468). Let

$$I = \prod_{\sigma\in\mathfrak{S}_6} D_{\sigma(1)\sigma(2),\sigma(3)\sigma(4),\sigma(5)\sigma(6)}.$$

The stabilizer subgroup of $D_{12,34,56})^2$ in $\mathfrak{S}_6$ is generated by the transpositions $(12),(34),(56)$ and permutations of three pairs $(12),(34),(56)$. It is a subgroup of order 48. Thus, after symmetrization, I defines the Clebsch-Gordan invariant I_{15} of degree $6!/48 = 15$ in coefficients of the binary form. [1]

Remark 11. Note that, if one does not assume that the 6 points $p_1,\ldots,p_6$ are on a conic, the last two conditions define an irreducible component of the moduli space of marked cubic surfaces with an Eckardt point (see [CAG], 9.4.5).

Remark 12. Explicitly, suppose the characteristic equation of f_0 and N_0 is equal to $t^2 - bt + (ac + ed) = 0$. Suppose that $\Delta = b^2 - 4((ac+ed) = k^2$. The matrix N_0 in its action on Λ has two eigensublattices $\Lambda_\pm$ of Λ with eigenvalues $\alpha_\pm$. They are generated by

$$v_1^\pm = (d, 0, -c, \alpha_\pm), \quad v_2^\pm = (0, d, b-\alpha_\pm, -a),$$

where the coordinates are taken with respect to the basis $(\gamma_1,\gamma_2,e_1,e_2)$ of $\Lambda = \tau\mathbb{Z}^2 + \mathbb{Z}^2$. So, we can write

$$v_1^\pm = (dz_1 - c, dz_2 + \alpha_\pm),\ v_2^\pm = (dz_2 + b - \alpha_\pm, dz_3 - a).$$

The endomorphism f_0 represented by the matrix M_0 has the eigenvalues $\alpha_\pm$ with one-dimensional eigensubspaces $V_\pm$ generated by the vectors $w_\pm = v_1^\pm$, the vectors $v_1^\pm, v_2^\pm$ are proportional over $\mathbb{C}$ with the coefficient proportionality equal to

$$\tau_\pm = \frac{dz_2 + \alpha_\pm}{dz_3 - a} = \frac{dz_1 - c}{dz_2 + b - \alpha_\pm}.$$

Let

$$E_\pm = V_\pm/\Lambda_\pm \cong \mathbb{C}/\mathbb{Z}\tau_\pm + \mathbb{Z}.$$

The embedding $\Lambda_\pm \hookrightarrow \Lambda$ define a homomorphism $E_\pm \to A$. Its kernel is equal to the torsion of the group $\Lambda/\Lambda_\pm$. We have

$$v_1^\pm \wedge v_2^\pm = (d^2, d(b-\alpha_\pm), -ad, cd, d\alpha_\pm, ed)$$

is equal to d times a vector with mutually coprime coordinates. More precisely,

$$av_1^\pm + \alpha_\pm v_2^\pm = (da, d\alpha_\pm, -ac + \alpha_\pm(b-\alpha_\pm), 0) = d(a, \alpha_\pm, e, 0) = dg_\pm.$$

This shows that the torsion is of degree d.

[1] Its explicit formula occupies 15 pages of Salmon's book [G. Salmon, Lessons introductory to the modern higher algebra, Appendix.

Let $\Lambda'_\pm = \Lambda_\pm + \mathbb{Z}g_\pm$. Then $E'_\pm = V_\pm/\Lambda'_\pm$ embeds in A. We have $E(v_1^\pm, g_\pm) = (b - 2\alpha_\pm) = k$, where $k^2 = \Delta$.

Then we have homomorphism of the complex tori:

$$E_+ \times E_- = V_+ \oplus V_-/\Lambda'_+ \oplus \Lambda'_- \to A = V_+ \oplus V_-/\Lambda.$$

Its kernel is a finite group $\Lambda/\Lambda'_+ \oplus \Lambda'_-$ of order equal to the determinant of the 4×4-matrix with columns $v_1^+, v_1^-, v_2^+, v_2^-$ divided by d^2. Computing the determinant, we find that it is equal to $d^2\Delta$. Thus we obtain

Remark 13. We know from Example 6 that the Jacobian variety $\text{Jac}(C)$ of a curve of genus 2 could be isomorphic to the product of two isogenous elliptic curves $E_1 \times E_2$. Let k_1, k_2 be the degrees of the projections of $C \to E_i$. Fix an embedding $E_i \hookrightarrow E_1 \times E_2$ and consider the corresponding norm-endomorphisms g_i. Then, we obtain that the period matrix of A satisfies two singular equations with discriminants k_1^2 and k_2^2. We have two isogenies

$$E_1 \times E'_1 \to E_1 \times E_2, \quad E_2 \times E'_2 \to E_1 \times E_2$$

of degrees k_1^2 and k_2^2.

Remark 14. (see [N. Murabayashi, Manuscripta Math. **84** (1994)). Consider the abelian variety A defined by the period matrix

$$\tau = \begin{pmatrix} z_1 & 1/k \\ 1/k & z_3 \end{pmatrix} \tag{5.3}$$

Let $p : \mathbb{C}^2 \to \mathbb{C}^2$ be the linear map $(a, b) \mapsto (0, kb)$. Then $p(\gamma_1) = e_2, p(\gamma_2) = k\gamma_2 - e_1, p(e_1) = 0, p(e_2) = ke_2$. Thus p defines an endomorphism of A with

$$f_a = \begin{pmatrix} 0 & 0 \\ 0 & k \end{pmatrix}, \; f_r = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & k & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & k \end{pmatrix}$$

We have $p(\Lambda) = \mathbb{Z}1 + \mathbb{Z}kz_3 = \mathbb{C}/\Lambda_1$ and $\text{Ker}(p) \cap \Lambda = \mathbb{Z}(k\gamma_1 - e_2) + \mathbb{Z}e_1$. We see that the matrix is a special case of the matrix N_0 from (4.2). We get $a = c = d = 0, b = k, e = -1$. Thus τ satisfies the singular equation $kz_2 = 1$, of course, this was obvious from the beginning. The discriminant of this equation is equal to k^2. This shows that p defines a surjective homomorphism to the complex 1-torus $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}kz_3$ and its kernel is the complex torus $E' = \mathbb{C}/\mathbb{Z} + \mathbb{Z}kz_1 = \mathbb{C}/\Lambda_2$ embedded in A by the map $z \mapsto (z, 0)$ that sends 1 to e_1 and kz_1 to $k\gamma_1 - e_2$. We also can embed E' in A by the map $\mathbb{C} \to \mathbb{C}^2$ that sends 1 to e_2 and kz_3 to $k\gamma_2$. The determinant of the matrix of the map $\Lambda_1 \oplus \Lambda_2 \to \Lambda$ is equal to k^2, thus we have an isogeny $E \times E' \to A$ of degree k^2.

Example 15. Assume $k = 3$. Let $f : C \to E$ be a degree 3 map onto an elliptic curve E. Assume that $\text{Jac}(C)$ contains only one pair of one-dimensional subgroups E, E' with $E \cdot E' = k^2$ and that E is not isomorphic to E'. Let σ be the hyperelliptic involution of C and $\phi : C \to C/(\sigma) = \mathbb{P}^1$ be the canonical degree 2 cover. By our assumption, the subfield of the field of rational functions on C contains a unique subfield isomorphic to the field of rational functions on E. This shows that σ leaves this field invariant and hence induces an involution $\bar{\sigma}$ on E such that we have a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\sigma} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ E & \xrightarrow{\bar{\sigma}} & E \end{array} .$$

We assume that the map $f : C \to E$ ramifies at two distinct points. This is a non-degenerate case, in another case we may have one ramification point of index 3. Let x be one of the Weierstrass points, a fixed point of σ. We have $f(x) = f(\sigma(x)) = \bar{\sigma}(f(x))$. Thus, by taking $f(x)$ to be the origin of a group law on E, we may assume that $\bar{\sigma}$ is an order 2 automorphism of E. Obviously, it has four fixed points, the 2-torsion points on E. This shows that f defines a map of a set of 6 Weierstrass points W to the set $F = E^{\bar{\sigma}}$ of 4 fixed points $a_1, \ldots, a_4$ of $\bar{\sigma}$. If a is one of these fixed points and $f(x) = a$, then $f(\sigma(x)) = a$, hence σ preserves the fiber $f^{-1}(a)$ (considered as an effective divisor of degree 3 on C. Since σ is of order 2, it must fix one of the points or the whole fiber. The latter case happens if f has a ramification point over a. Thus the fibers of the map $W \to F$ have cardinalities $(3, 1, 1, 1)$ or $(2, 2, 1, 1)$. To exclude the latter possibility, we consider the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\phi} & \mathbb{P}^1 \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \bar{f}} \\ E & \xrightarrow{\bar{\phi}} & \mathbb{P}^1 \end{array} ,$$

Comparing the ramification schemes for the degree 6 maps $\bar{\phi} \circ f : C \to \mathbb{P}^1$ and $\bar{f} \circ \phi$ one can see that the second possibility does not occur. Let us consider the case $(3, 1, 1, 1)$. We assume that $f^{-1}(a_1)$ consists of three points in W. Let $y_i = \bar{\phi}(a_i)$. The the map $\bar{\phi} \circ f : C \to \mathbb{P}^1$ ramifies the 3 preimage of each point $y_i \in \bar{\phi}(F)$ with index ramification equal to 2, and ramifies at 2 points over the image b in $\mathbb{P}^1$ of the two branch points of $C \to E$.

Using the commutative diagram we see that the branch points of the map $\bar{f} : \mathbb{P}^1 \to \mathbb{P}^1$ are three points $y_2, y_3, y_4 \in \bar{\phi}(F)$. The fiber $\bar{f}^{-1}(y_i)$ contains one point from $\phi(W)$, the other point in the this fiber is a ramification point.

Now, we see that the set of Weierstrass points W is split into a disjoint set of triples of points $A+B$, where $f(A) = a \in F$ and $f(B) = F \setminus \{a\}$. We choose a group law on E to assume that $a_1 = \{0\}$. We know that Ker(Jac$(C) \to E$) = Ker(Nm : Jac$(C) \to E$). Since Nm$(x + y + z) = 0$, hence $\{x + y + z\} \subset E'$. The image $\phi(A)$ of A in $\mathbb{P}^1$ is a fiber of the map $\bar{f} : \mathbb{P}^1 \to \mathbb{P}^1$ over $y_1 = \bar{\phi}(0)$. The image of each point in B under ϕ is contained in a fiber over a point y_2, y_3, y_4 complementary to the ramification point over y_2, y_3, y_4.

Thus we come to the following problem. Let $C : y^2 - F_6(x) = 0$. The polynomial F_6 should be written as the product $\Phi_3\Psi_3$ of two cubic polynomials such that there exists a degree 3 map $\mathbb{P}^1 \to \mathbb{P}^1$ such that the zeros of Φ_3 form one fiber, and the zeros of Ψ_3 are in the same fiber containing 3 ramification points.

We follow the argument of E. Goursat [E. Goursat, Bull. Soc. Math. France, **13** (1885)], and H. Burhardt [H. Burhardt, Math. Ann. **36** (1869)] in a nice exposition due to T. Shaska [T. Shaska, Forum Math. **16** (2004)].

Let $F(u, v) = 0$ be the binary form of degree 6 defining the ramification points of $\phi : C \to \mathbb{P}^1$. We seek for a condition that $F(u, v) = \Phi(u, v)\Psi(u, v)$, where the cubic binary forms satisfy the following conditions.

Let $G(u,v)$ be a binary cubic and

$$J(u,v) = J(G,\Phi) = \det \begin{pmatrix} G'_u & G'_v \\ \Phi'_u & \Phi'_v \end{pmatrix}$$

be the jacobian of G, Φ. Its zeroes are the four ramification points of the map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ given by (G, Φ). Let

$$K = K(u,v;u'v') = \det \begin{pmatrix} G(u,v) & \Phi(u,v) \\ G(u',v') & \Phi(u',v') \end{pmatrix} /(uv' - u'v)$$

be the anti-symmetric bi -homogeneous form of bidegree $(2,2)$ on $\mathbb{C}^2 \times \mathbb{C}^2$ expressing the condition that two points (u,v) and (u',v') are in the same fiber of ϕ. Its set of zeros $(u:v) = (u':v')$ consists of 4 ramification points of ϕ. In other words,

$$K(u,v;u',v') = J(G,\Phi).$$

Consider K as a polynomial in u', v' with coefficients in $\mathbb{C}[u,v]$. Let

$$R(u,v) = R(K(u,v;u',v'), J(u',v'))$$

be the resultant. Its vanishing expresses the condition that K and J have a common zero. It is a binary form of degree 4 in u, v. Let $\Psi(u,v)$ be a cubic binary form dividing $R(u,v)$. Then the hyperelliptic curve $y^2 - \Phi(u,v)\Psi(u,v) = 0$[2] admits a map of degree 3 to C. The equation of C is $y^2 - \psi(x) = 0$, where $v^2\psi(u/v) = \Psi(u,v)$.

Using the projective transformations of (u,v) and a linear transformation of G, Φ, one may assume that $G(u,v) = u^2v$. We can also assume that $\Phi(u,v) = u^3 + au^2v + buv^2 + v^3$. Then we find that

$$F(u,v) = (u^3 + au^2v + buv^2 + v^3)(4u^3 + b^2 + 2bx + 1),$$

so that a, b are two parameters on which our hyperelliptic curves depend.

Finally, we refer to [Burhardt] and [T. Shaska, Forum Math. **16** (2004)] for an explicit invariant of binary sextics defining the locus Hum(9). In [K. Magaard, T. Shaska, H. Völklein, Forum Math. **21** (2009)], one can find a treatment of the case $k = 5$.

A generalization of a problem of finding the conditions that a map $C \to E$ of degree k exists is the following problem.

A principally polarized abelian variety P is called a *Prym-Tyurin variety of exponent* e if there exists a curve C and an embedding $P \hookrightarrow \mathrm{Jac}(C)$ such that the principal polarization of C induces the polarization of type $(e, \ldots, e)$. Prym-Tyurin varieties of index 2 are the Prymians of covers $C \to D$ of degree 2 with at most 2 branch points. A generalization of the Prym constructions is a symmetric correspondence T on C such that $(T-1)(T+e-1) = 0$ in the ring of correspondences. The associated Prym variety of index e is the image of $T - 1$.

For example, the existence of a degree k cover $C \to E$ gives a realization of E as a Prym-Tyurin variety of exponent k. So, the problem is the following. Fix a ppav P of dimension p and a positive number e. Find all curves C of fixed genus g such that $P \subset \mathrm{Jac}(C)$ and the principal polarization induces a polarization of type $(e, \ldots, e)$ on P.

For example, assume that $p = 2$ and $g = 3$. Then $\mathrm{Jac}(C)$ should be isogenous to the product $P \times E$, where E is an elliptic curve.

[2] One views this equation as a curve in $\mathbb{P}(1,1,2)$.

Lecture 6

$\triangle$ is not a square

Let us study the Humbert surface $\mathrm{Hum}(\Delta) := \mathrm{Hum}_1(\Delta)$, where Δ is not a square. We will see the speciality of abelian surfaces belonging to the Humbert surface $\mathrm{Hum}(\Delta)$ in terms of the associated Kummer surface. Let A be a principally polarized abelian surface and $\mathrm{Kum}(A)$ be the quotient of A by the cyclic group of order 2 generated by the involution $\iota = [-1]$. Let L be a principal polarization of A. The involution ι is a symmetric endomorphism corresponding to L^{-1}. Then ι^* acts on $H^1(A, \mathbb{Z})$ as the multiplication by -1, hence its acts on $H^2(A, \mathbb{Z})$ identically. This shows that $c_1(L) = c_1(\iota^*(L))$, hence $M = \iota^*(L) \otimes L$ satisfies $\iota^*(M) = M$ (such line bundles are called *symmetric*) and $c_1(M) = 2c_1(L)$, or, equivalently, M defines a polarization of type $(2,2)$ with $(M, M) = 4(L, L) = 8$. By Riemann-Roch, $\dim H^0(A, M) = 4$, and the linear system $|M|$ defines a regular map $f : A \to \mathbb{P}^3$ that factors through a degree 2 quotient map

$$\phi : A \to A/(\iota)$$

and an isomorphism $A/(\iota) \to X$, where X is a quartic surface in $\mathbb{P}^3$. The quotient $A/(\iota)$ is denoted by $\mathrm{Kum}(A)$ and is called the *Kummer surface* associated to A. The 16 fixed points of the involution ι are the 2-torsion points $e \in A$. Their images p_e on X are ordinary double points. Assume that the polarization L is irreducible. Then $A \cong \mathrm{Jac}(C)$ for some smooth genus 2 curve $C \subset A$ and A can be identified with the subgroup $\mathrm{Pic}^0(C)$ of divisor classes of degree 0. By translating C by a point in A, we may assume that C is the divisor of zeros of a section of L. For any 2-torsion point $e \in A$, let C_e denote the translation of C by the point e. We have $2(C_e) \in |L^{\otimes 2}|$. Let us identify $\mathrm{Kum}(A)$ with the quartic surface X and let T_e be the image $f(C_e)$ in X. Then $f^{-1}(2T_e) = 2(C_e)$, hence $2T_e$ is equal to $X \cap H_e$ for some plane H_e in $\mathbb{P}^3$. Since plane sections of X are plane curves of degree 4, we see that T_e must be a conic. The plane H_e (or the conic C_e) is called a *trope*.

Note that the map $C_e \to T_e$ is given by the linear system $|L^{\otimes 2}|C_e|$ of degree 2 on $C_e \cong C$. It defines a degree 2 map $C_e \to T_e$, so T_e is a smooth conic. Thus we have 16 nodes $p_e \in X$ and 16 tropes T_e. The 6 ramification points of the map $C_e \to T_e$ are fixed points of ι. Hence, they are 2-torsion points lying on C_e. Thus each trope passes through 6 nodes. It is clear that the number of tropes containing a given node does not depend on the node (use that nodes differ by translation automorphism of A descent to X). By looking at the incidence relation $\{(C_e, e') : e' \in C_e\}$, we obtain that each node is contained in 6 tropes. Thus we get a combinatorial configuration (16_6) expressing the incidence relation between two finite sets. This is the famous *Kummer configuration*.

To obtain a minimal resolution of $\mathrm{Kum}(A)$, we lift the involution $\iota = [-1]_A$ to an involution $\tilde{\iota}$ of the blow-up $\tilde{A} \to A$ of the set $A[2]$. The quotient $\tilde{X} = \tilde{A}/(\tilde{\iota})$ has the projection to $A/(\iota) =$

Kum(A) which is a minimal resolution of the 16 nodes of Kum(X).

$$\begin{array}{ccc} \tilde{A} & \xrightarrow{\tilde{\phi}} & \tilde{X} \\ \downarrow{\scriptstyle \tilde{\sigma}} & & \downarrow{\scriptstyle \sigma} \\ A & \xrightarrow{\phi} & X \end{array}$$

Since ι acts as -1 on the tangent space $T_0(A)$, it acts identically on the exceptional curves R_i' of $\tilde{\sigma}$. Thus the quotient $\tilde{A}/\tilde{\iota}$ is nonsingular and the proejction $\tilde{p}$ is a degree 2 cover of nonsingular surfaces ramified over 16 curves R_i' isomorphic to $\mathbb{P}^1$. Using the known behaviour of the canonical class under a blow-up, we obtain $K_{\tilde{A}} = \sum R_i'$. The Hurwitz formula $K_{\tilde{A}} = \tilde{p}^*(K_{\tilde{X}}) + \sum R_i'$ implies that $K_{\tilde{X}} = 0$. Since $\tilde{\iota}$ acts on $H^1(\tilde{A}, \mathbb{Q})$ as -1, we obtain that $H^1(\tilde{X}, \mathbb{Q}) \subset H^1(\tilde{A}, \mathbb{Q})^{\tilde{p}} = \{0\}$ must be trivial. Thus $b_1(\tilde{X}) = 0$, and we obtain that $\tilde{X}$ is a K3 usrace.[1].

Let p be one of the 16 nodes of X. Projecting from this point, we get a morphism $X \setminus \{p\} \to \mathbb{P}^2$ of degree 2. Let us choose coordinates in $\mathbb{P}^3$ such that $p = [1, 0, 0, 0]$. Then the equation of X can be written in the form

$$t_0^2 F_2(t_1, t_2, t_3) + 2t_0 F_3(t_1, t_2, t_3) + F_4(t_1, t_2, t_3) = 0,$$

where $F_k(t_1, t_2, t_3)$ is a homogeneous form of degree indicated by the subscript. It is clear that the pre-image of a point $[x_1, x_2, x_3]$ on the plane consists of two points which coincide when

$$F = F_3(t_1, t_2, t_3)^2 - F_2(t_1, t_2, t_3)F_4(t_1, t_2, t_3) = 0.$$

We say that X is birationally isomorphic to the double plane with branch curve $B : F = 0$ of degree 6. Note that the conic $F_2 = 0$ is the image of the tangent cone at p and it is tangent to B at all its intersection points with it. Of course, this is true for any irreducible quartic surface with a node p. In our case we get more information about the branch curve B. Let $C_1, \ldots, C_6$ be the six tropes containing p. Then any line in the plane T_i spanned by C_i intersects the surface at one points besides p. This implies that the projection of C_i, which is a line ℓ_i in the plane, must be contained in B. Thus, we obtain that B is the union of 6 lines $\ell_1, \ldots, \ell_6$. Obviously, they intersect at $15 = \binom{6}{2}$ points, the images of the remaining 15 nodes on X. So, we obtain that X is birationally isomorphic to a surface in $\mathbb{P}(3, 1, 1, 1)$ given by the equation

$$x_0^2 = l_1 \cdots l_6,$$

where $l_1, \ldots, l_6$ are linear forms in variables x_1, x_2, x_3. The corresponding lines $\ell_1, \ldots, \ell_6$ are in general linear position. However, they are not general 6 lines in the plane since they satisfy an additional condition that there exists a smooth conic K that tangent each line.

Conversely, one can show that such equation defines a surface birationally isomorphic to the Kummer surface corresponding to the hyperelliptic curve of genus 2 isomorphic to the double cover of K branched at the tangency points. One uses that the pre-image of K under the cover splits into the sum of two smooth rational curves $K_1 + K_2$ intersecting at 6 points. Let h be the pre-image of a general line in the plane. Then $h \cdot K_1 = h \cdot K_2 = 2$ and $(h + K_1)^2 = 2 + 4 - 2 = 4$. The linear system $|h + K_1|$ maps the double plane to a quartic surface in $\mathbb{P}^3$ with 16 nodes, fifteen of them are the images of the intersection points of the lines, and the sixteenth is the image of K_2.

[1]By definition, a K3 surface is a smooth algebraic surface with trivial canonical class and the first Betti number equal to 0

In the following we will follow the paper [C. Birkenhake, H. Wilhelm, Trans. Amer. Math. Soc. **355** (2003)]. Applying Lemma 7, we may assume that $b = 0, 1$ and $\Delta = b + 4m$. Recall from (4.7) that $A \in \mathrm{Hum}(\Delta)$ contains a line bundle L_Δ such that

$$(L_\Delta^2) = \tfrac{1}{2}(b^2 - \Delta) = -2m, \quad (L_0, L_\Delta) = b.$$

Suppose

$$\Delta = 8d^2 + 9 - 2k,$$

where $k \in \{4, 6, 8, 10, 12\}$ and $d \geq 1$. We have $(L_\Delta^2) = -(4d^2 + 4 - k)$. Let $L = L_0^{\otimes d} \otimes L_\Delta$. We easily compute

$$(L^2) = 4d(d+1) + k - 4, \quad (L, L_0) = 4d + 1.$$

Using the formula (4.8), we find that the type of the polarization defined by L is equal to $(1, 2d(d+1) + \frac{k}{2} - 2)$. After tensoring L with some line bundle from $\mathrm{Pic}^0(A)$, we may assume that L is symmetric, i.e. $[-1]^*(L) = L$.[2] For any symmetric line bundle L defining a polarization of type (d_1, d_2), $[-1]_A$ acts on $H^0(L)$ decomposing it into the direct sum of linear subspaces $H^0(L)^\pm$ of eigensubspaces of dimensions $\frac{1}{4}((L^2) - \#X_2^\mp(L)) + 2$, where

$$X_2^\pm(L) = \{x \in A[2] : [-1]_A | L(x) = \pm 1\}.$$

It is known that

$$X_2^+(L) \in \begin{cases} \{8, 16\} & \text{if } d_1 \text{is even,} \\ \{4, 8, 12\} & \text{if } d_1 \text{is odd and } d_2 \text{is even,} \\ \{6, 10\} & \text{if } d_2 \text{ is odd.} \end{cases}$$

(see [CAV], 4.7.7 and 4.14). Since in our case $d_1 = 1$, we can choose L such that $k = \#X_2(L)^+$ and $\dim H^0(L)^- = d(d+1) + 1$. By counting constants, we can choose a divisor $D \in |L|$ such that $\mathrm{mult}_0 D \geq 2d + 1$ (the number of conditions is $d(d+1)$). The geometric genus $g(D)$ of D is equal to $1 + \frac{1}{2}D^2 - d(2d+1) = d + \frac{k-2}{2}$. Let

$$\phi : A \to \mathrm{Kum}(A) = A/([-1]_A) \subset \mathbb{P}^3$$

be the map from A to the Kummer surface given by the linear system $|L_0^{\otimes 2}|$. It extends to a map $\tilde{A} \to X$ from the blow-up of 16 2-torsion points of A to a minimal nonsingular model of $\mathrm{Kum}(A)$. The divisor D is invariant with respect to the involution $[-1]_A$. The normalization $\bar{D}$ of D is mapped $(2:1)$ onto the normalization $\bar{C}$ of $C = \phi(D)$ and ramifies at $k - 1$ points and some point in the pre-image of 0. The Hurwitz Formula applied to the map $\bar{D} \to \bar{C}$ gives

$$g(\bar{D}) = d + \frac{k-2}{2} = -1 + 2g(\bar{C}) + \frac{k-1+r}{2}, \tag{6.1}$$

where r is the number of ramification points over 0(one can show that C is smooth outside $\phi(0)$, see [BirkenkakeWilhelm], Proposition 6.3]). We may obtain $\bar{D}$ by blowing up 0 and taking the proper inverse transform of D. The preimage of 0 consists of $2d + 1$ points that are fixed under the involution $[-1]_A$ extended to $\tilde{A}$. This shows that $r = 2d + 1$ and (6.1) gives $g(\bar{C}) = 0$. Thus C is a rational curve and the proper transform of $\phi(C)$ in the blow-up of $\phi(0)$ intersects the exceptional curve with multiplicity $2d + 1$. Since $(L_0, L) = 4d + 1$, the image C' of C under the proejction $\pi : X \dashrightarrow \mathbb{P}^2$ from $\phi(0)$ is a plane curve of degree $4d + 1 - (2d + 1) = 2d$ that passes through $k - 1$

[2] We use that $[-1]_A$ acts as $[-1]$ on $\mathrm{Pic}^0(A)$, since $M = [-1]^*(L) \otimes L^{\otimes -1} \in \mathrm{Pic}^0(A)$, we write $M = N^{\otimes 2}$ and check that $[-1]^*(L \otimes N) \cong L \otimes N$.

intersection points $\ell_i \cap \ell_j$. Also note that, if C intersects one of the six tropes T_i corresponding to the lines ℓ_i at a point q with multiplicity m, then C' intersect ℓ_i at $\bar{q} = \pi(q)$ with multiplicity $2m$. This follows from the projection formula $(\pi(C), \ell_i)_{\bar{q}} = (C, \pi^*(\ell_i))_q = 2(C, T_i)_q$.

So, we obtain the following theorem from [BirkenhakeWilhelm].[3]

Theorem 16. *Suppose $\Delta = 8d^2 + 9 - 2k$, where $d \geq 1$ and $k \in \{4, 6, 8, 10, 12\}$. If (A, L_0) is an abelian surface with an irreducible principal polarization L_0 belonging to* Hum(Δ)*, then the double plane model of* Kum(A) *defined by 6 lines $\ell_1, \ldots, \ell_6$ has the property that there exists a rational curve C of degree $2d$ with nonsingular points at $k - 1$ intersection points $\ell_i \cap \ell_j$ and intersecting the lines at the remaining intersection points with even multiplicity.*

Similarly, Birkenhake and Wilhelm prove the following.

Theorem 17. *Suppose $\Delta = 8d(d+1) + 9 - 2k$, where $d \geq 1$ and $k \in \{4, 6, 8, 10, 12\}$. If (A, L_0) is an abelian surface with an irreducible principal polarization L_0 belonging to* Hum(Δ)*, then the double plane model of* Kum(A) *defined by 6 lines $\ell_1, \ldots, \ell_6$ has the property that there exists a rational curve C of degree $2d + 1$ with nonsingular points at k intersection points $\ell_i \cap \ell_j$ and intersecting the lines at the remaining intersection points with even multiplicity.*

The following is the special case considered by G. Humbert.

Example 18. Take $\Delta = 5, d = 1, k = 6$. Then C is a conic passing through 5 intersection points $p_i = \ell_i \cap \ell_{i+1}, i = 1, \ldots, 4$ and $p_5 = \ell_1 \cap \ell_5$ forming the set of 5 vertices of a 5-sided polygon Π with sides $\ell_1, \ldots, \ell_5$ and touching the sixth line ℓ_6.

Together with the conic K touching all 6 lines, the pentagon is the *Poncelet pentagon* for the pair of conics K, C (i.e. K is inscribed in Π and C is circumscribed around Π).

Example 19. Take $\Delta = 13, d = 1, k = 6$. The only possibility is the following. Let $p_1 = \ell_1 \cap \ell_2, p_2 = \ell_2 \cap \ell_3, p_3 = \ell_1 \cap \ell_3$. Take $p_4 = \ell_1 \cap \ell_4, p_5 = \ell_2 \cap \ell_5, p_6 = \ell_3 \cap \ell_6$. Then there must be a plane cubic passing through $p_1, \ldots, p_6$ and touching ℓ_4, ℓ_5, ℓ_6.

These two theorems deals with the case when $\Delta \equiv 1 \mod 4$ (although they do not cover all possible Δ's. The next theorem treats the cases with $\Delta \equiv 0 \mod 4$

Theorem 20. *Suppose $\Delta = 8d^2 + 8 - 2k$ (resp. $8d(d+1) + 8 - 2k$, where $d \geq 1$ and $k \in \{4, 6, 8, 10, 12\}$. If (A, L_0) is an abelian surface with an irreducible principal polarization L_0 belonging to* Hum(Δ)*, then the double plane model of* Kum(A) *defined by 6 lines $\ell_1, \ldots, \ell_6$ has the property that there exists a rational curve C of degree $2d$ (resp. $2d + 1$) with nonsingular points at k (resp. $k - 1$) intersection points $\ell_i \cap \ell_j$ and intersecting the lines at the remaining intersection points with even multiplicity.*

Example 21. Take $d = 1, k = 4, \Delta = 8$. Then we get two 4-Poncelet related conics C and K circumscribed and inscribed in a quadrangle of lines. Note that Hum(8) is the locus in $\mathcal{A}_2$ of surfaces with real multiplication by $\mathbb{Q}(\sqrt{2})$. One can see in the following way (see [Terasoma]). Consider the following subgroups of Sp$(4, \mathbb{Z})$"

$$\Gamma_1(2) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(4, \mathbb{Z}) : A - I_2 \equiv D - I_2 \equiv C \equiv 0 \mod 2\}, \tag{6.2}$$

$$\Gamma_0(2) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(4, \mathbb{Z}) : C \equiv 0 \mod 2\}, \tag{6.3}$$

$$\Gamma(2) = \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(4, \mathbb{Z}) : A - I_2 \equiv D - I_2 \equiv C \equiv B \equiv 0 \mod 2\}. \tag{6.4}$$

[3] We omitted some details justifying, for example, why C can be chosen irreducible or why its singular point at 0 is an ordinary point of multiplicity $2d + 1$.

One can show that $\mathcal{Z}_2/\Gamma_1(2)$ is the fine moduli space $\mathcal{A}_{2,1}(2)$ of pairs (A,ϕ), where A is a ppas (principally polarized abelian surface) and $\phi : (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow A[2]$ is a homomorphism of groups with the image a totally isotropic subgroup of $A[2]$ with respect to the symplectic form on $H_1(A,\mathbb{Z})/2H^1(A,\mathbb{Z}) \cong A[2]$ induced by the symplectic form on $H_1(A,\mathbb{Z})$ defined by the polarization.

The quotient $\mathcal{Z}_2/\Gamma_0(2)$ is the fine moduli space $\mathcal{A}_{2,0}(2)$ of pairs (A,ϕ), where A is a ppas (principally polarized abelian surface) and $V \subset A[2]$, where V is a totally isotropic subgroup of $A[2]$.

Finally, the quotient $\mathcal{Z}_2/\Gamma(2)$ is the fine moduli space $\mathcal{A}_2(2)$ of pairs (A,ϕ), where A is a ppas (principally polarized abelian surface) and $\phi : \mathbb{F}_2^4 \hookrightarrow A[2]$ is an isomorphism of 4-dimensional symplectic linear spaces over $\mathbb{F}_2$, where the symplectic form on $\mathbb{F}_2^4$ is defined by the matrix J.

We have a sequence of finite maps

$$\mathcal{A}_2(2) \to \mathcal{A}_{2,1}(2) \to \mathcal{A}_{2,0}(2) \to \mathcal{A}_2$$

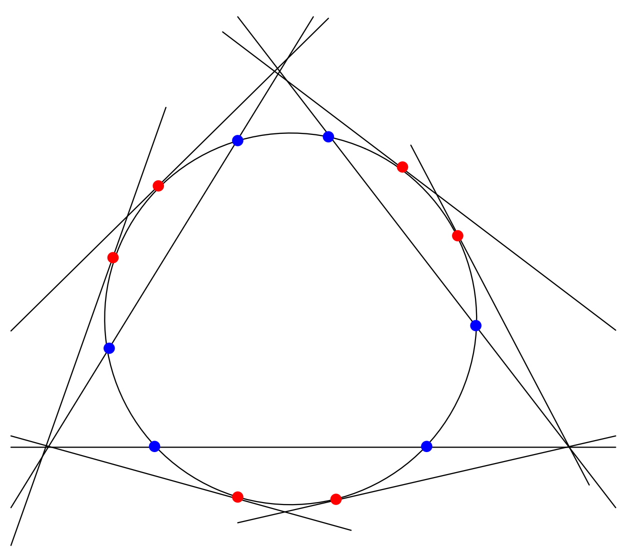
corresponding to inclusions of groups

$$\Gamma(2) \subset \Gamma_1(2) \subset \Gamma_0(2) \subset \mathrm{Sp}(4,\mathbb{Z})$$

with corresponding indices $15, 8, 6$. Note that $\Gamma(2)$ is a normal subgroup of $\mathrm{Sp}(4,\mathbb{Z})$ with the quotient isomorphic to $\mathrm{Sp}(4,\mathbb{F}_2) \cong \mathfrak{S}_6$. It is known that the moduli space $\mathcal{A}_2(2)$ is isomorphic to a locally closed subset of the GIT-quotient $(\mathbb{P}^2)//\mathrm{SL}(3)$ parameterizing orbits of 6 distinct points on a conic. The group $\mathfrak{S}_6$ acts on this space by permuting the points. Let

$$\mathfrak{f}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{R}).$$

It is an element of order 2, called the *Fricke involution*. It normalizes both $\Gamma_0(2)$ and $\Gamma_1(2)$ and acts as an involution on the spaces $\mathcal{A}_{2,0}(2)$ and $\mathcal{A}_{2,1}(2)$. The fixed locus of $\mathfrak{f}_2$ in $\mathcal{A}_{2,1}(2)$ is mapped to $\mathrm{Hum}(8)$.



A point in $\mathcal{A}_{2,1}(2)$ is represented by an ordered triple of pairs of points in fixed conic modulo projective transformations leaving the conic invariant. These are painted in blues and joined by three lines. The new 3 pairs pinted in red is the image of the point under the Fricke involution.

Remark 22. It follows from the Teichmüller theory any holomorphic differential on a Riemann surface X of genus g defines an immersion of $\mathbb{H}$ in $\mathcal{M}_g$ such the image is a complex geodesic with respect to the Techmüller metric. According to C. McMullen [**?**], the closure of the image of $\mathbb{H}$ in $\mathcal{M}_2$ is either a curve, or a Humbert surface $\mathrm{Hum}(\Delta)$, where Δ is not a square, or the whole $\mathcal{M}_2$.

Lecture 7

Fake elliptic curves

We will discuss abelian surfaces with the endomorphism ring of the third type, i.e. imaginary quadratic extensios of a real quadratic field later. They are examples of abelian varieties of CM-type. In this lecture we will consider *fake abelian surfaces*, i.e. abelian surfaces with the ring $\mathrm{End}(A)_{\mathbb{Q}}$ isomorphic to an order in an indefinite quaternion algebra. Fake elliptic curves are parameterized by a complete algebraic curve (a *Shimura curve*), the quotient of $\mathbb{H}$ by a cocompact Fuchsian group isomorphic to the group of units of a quaternion algebra over $\mathbb{Q}$. A construction of the moduli space is as follows. Let $B = \mathbb{Q}(a, b)$ be an indefinite quaternion algebra over $\mathbb{Q}$ and $\mathfrak{o}$ be an order in B. Recall that this means that $\mathfrak{o}$ is an algebra over $\mathbb{Z}$ containing 1 such that $\mathfrak{o} \otimes \mathbb{Q} \cong B$. Note that each order is contained in a unique maximal order. Let us identify $B_{\mathbb{R}}$ with $\mathrm{Mat}_2(\mathbb{R})$ and consider a linear $\mathbb{R}$-isomorphism

$$\phi : B_{\mathbb{R}} \to \mathbb{C}^2, \quad X \mapsto X \cdot z,$$

where $z \in \mathbb{P}^1 \setminus \mathbb{P}^1(\mathbb{R})$. Let $\Lambda_z = \phi(\mathfrak{o})$. The complex torus $\mathbb{C}^2/\Lambda_z$ is an abelian variety. In fact, we define the alternating form E_z on Λ_z by $E_z(\phi(x), \phi(y)) = -\mathrm{Tr}(ix\bar{y})$. The real part of the associated Hermitian form is equal to the positive definite symmetric matrix $\mathrm{Tr}(x\bar{y})$. This gives us an abelian surface $A_z = \mathbb{C}^2/\Lambda_z$. Note that $A_z \cong A_{z'}$ if and only if there exists a unit u from $\mathfrak{o}$ such that $\phi(u)(z) = z'$. We can find u with $\mathrm{Nm}(u) = -1$ such that $\mathrm{Im}(z') > 0$, and then obtain that z is defined uniquely up to the action of the group $\Gamma = \phi(\mathfrak{o}_1^*)/\{\pm\} \subset \mathrm{PSL}_2(\mathbb{R})$, where $\mathfrak{o}_1^*$ is the group of elements in $\mathfrak{o}$ with $\mathrm{Nm}(u) = 1$. The group Γ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, a *Fuchsian group of the first kind* (a discrete subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$ such that the quotient $\mathbb{H}/\Gamma$ is isomorphic to the complement of finitely many points on a compact Riemann surface). It is known that Γ is a cocompact, i.e. the quotient $\mathbb{H}/\Gamma$ is a compact Riemann surface. It is also an arithmetic group [1] Such quotients are called the *Shimura curves*. Conversely, any point on the curve $\mathbb{H}/\Gamma$ defines a polarized abelian surface with endomorphism algebra containing $\mathbb{O}$ for some order in a B. The curve $\mathbb{H}/\Gamma$ is the coarse moduli space of such abelian surfaces.

Let us give an example of a fake elliptic curve from [K. Hashimoto, N. Murabayashi, Tohoku Math. J. (2) **47** (1995)]. Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and $\mathfrak{o}_B$ be the maximal order in B. By definition, $B_{\mathbb{R}} \cong \mathrm{Mat}_2(\mathbb{R})$. Let $x \mapsto x^*$ be the involution in B induced by the transpose involution of $\mathrm{Mat}_2(\mathbb{R})$. The trace bilinear form $\mathrm{Tr}(xy^*)$ restricted to the symmetric part $B^s = \{x \in B : x = x^*\}$ of B defines a structure of a positive definite lattice on $\mathfrak{o}_B^s := B^s \cap \mathfrak{o}_B$ of rank 3. The discriminant of B is equal to the discriminant of the lattice $\mathfrak{o}_B^s$.

[1]This means that its preimage in $\mathrm{SL}_2(\mathbb{R})$ contains a subgroup of finite index whose elements are matrices with entries in an algebraic number field.

Let us choose

$$B = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}, \quad \mathbf{i}^2 = -6,\ \mathbf{j}^2 = 2,\ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

The maximal order $\mathfrak{o}_B$ has a basis

$$(\alpha_1, \dots, \alpha_4) = (1, \tfrac{1}{2}(\mathbf{i}+\mathbf{j}), \tfrac{1}{2}(\mathbf{i}-\mathbf{j}), \frac{1}{4}(2+2\mathbf{j}+\mathbf{k})).$$

Note that $\mathbf{i}, \mathbf{j}, \mathbf{k}/2 = (\mathbf{i}-\mathbf{j})(\mathbf{i}+\mathbf{j})/4 - 1 \in \mathfrak{o}_B$. The discriminant is equal to the determinant of the matrix $(\mathrm{Tr}(\alpha_i\bar{\alpha}_j))$. One finds that the discriminant of this matrix is equal to -6. The embedding of $\mathbb{E}_{\mathbb{R}}$ in $\mathrm{Mat}_2(\mathbb{R})$ is given by

$$\mathbf{i} \mapsto \begin{pmatrix} 0 & -1 \\ 6 & 0 \end{pmatrix}, \quad \mathbf{j} \mapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}.$$

We consider the isomorphism $\phi_z : B_{\mathbb{R}} \to \mathbb{C}^2$ given by $X \mapsto X \cdot \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)$, where $z \in \mathbb{C}$ and consider the abelian surface A_z. Let $\omega_i = \phi_z(\alpha_j) \in \mathbb{C}^2$. One computes the matrix of the alternating form E_z in this basis to obtain that it is equal to

$$\begin{pmatrix} 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

If we put $\omega_1' = -\omega_3, \omega_2' = \omega_4, \omega_3' = -\omega_1, \omega_4' = \omega_3 - \omega_2$, we obtain a standard symplectic basis defined by the matix J. We easily compute the period matrix

$$\tau_z = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} = \begin{pmatrix} \frac{3z}{2} - \frac{1}{4z} & -\frac{3\sqrt{2}z}{4} - \frac{1}{2} - \frac{\sqrt{2}}{8z} \\ -\frac{3\sqrt{2}z}{4} - \frac{1}{2} - \frac{\sqrt{2}}{8z} & \frac{3z}{4} - \frac{1}{2} - \frac{1}{8z} \end{pmatrix}.$$

One finds that the period matrix τ_z satisfies the following 2-parametrical family of singular equations:

$$-(\lambda+\mu)z_1 + \lambda z_2 + (\lambda + 2\mu)z_3 + \lambda(z_2^2 - z_1 z_3) + \mu = 0.$$

Its discriminant is equal to

$$\Delta = \lambda^2 + 4(\lambda+\mu)(\lambda+2\mu) - 4\lambda\mu = 5\lambda^2 + 8\mu(\lambda+\mu).$$

Taking $(\lambda, \mu) = (1, 0)$ and $(0, 1)$, we obtain that the image of τ lies in the intersection of two Humbert surfaces $\mathrm{Hum}(5)$ and $\mathrm{Hum}(8)$ which we discussed in the previous lecture. It will turn out that the family of genus 2 curves whose endomorphism rings contains B is given by the following formula.

$$y^2 = x(x^4 - px^3 + qx^2 - rx + 1),$$

where

$$p = -2(s+t), r = -2(s-t), q = \frac{(1+2t^2)(11 - 28t^2 + 8t^4)}{3(1-t^2)(1-4t^2)},$$

and $g(s,t) = 4s^2t^2 - s^2 + t^2 + 2 = 0$.

The base is the elliptic curve given by the affine equation $g(s,t) = 0$. The Shimura curve is of genus 0, the quotient of the base by the subgroup generated by the involutions $(t,s) \mapsto (-t, \pm s), (x,y) \mapsto (-x, iy), (x^{-1}, yx^{-3})$.

Lecture 8

Periods of K3 surfaces

A K3 surface was defined as a complex algebraic surface with $K_X = 0$ and $b_1(X) = 0$. The *Noether formula*

$$12\chi(X, \mathcal{O}_X) = K_X^2 + c_2,$$

where $\chi(X, \mathcal{O}_X) = 1 - q(X) + p_g(X) := 1 - \dim H^0(X, \Omega_X^1) + \dim H^0(X, \Omega_X^2)$ and c_2 is the second Chern class of X equal to the Euler-Poincaré characteristic of X, gives us that $c_2(X) = 24$ and $b_2(X) = 22$. The cohomology $H^2(X, \mathbb{Z}) \cong \mathbb{Z}^{22}$[1] and the Poincaré duality equips it with a structure of a unimodular indefinite quadratic lattice. Its signature is equal to $(3, 19)$. The lattice $H^2(X, \mathbb{Z})$ is an even unimodular lattice, and as such, by a theorem of J. Milnor, must be unique, up to isomorphism. We can choose a representative of the isomorphism class to be the lattice

$$L_{K3} := U \oplus U \oplus U \oplus E_8 \oplus E_8.$$

(sometimes referred to as the *K3-lattice*). Here the direct sum is the orthogonal direct sum, U is an integral hyperbolic plane that has a basis (f, g) with $f^2 = g^2 = 0, f \cdot g = 1$(called a *canonical basis*) and E_8 is the negative definite unimodular lattice of rank 8 that we saw before in Lecture 3.

The first Chern class map $c_1 : \text{Pic}(X) \to H^2(X, \mathbb{Z})$ is injective, and its image is a sublattice S_X of $H^2(X, \mathbb{Z})$ which is, by Hodge Index Theorem is of signature $(1, \rho)$, where $\text{Pic}(X) \cong \mathbb{Z}^\rho$. Note that the Poincaré duality allows us to identify $H^2(X, \mathbb{Z})$ with $H_2(X, \mathbb{Z})$. Applying this to S_X, gives the identification between cohomology classes defined by line bundles via the first Chern class and divisor classes of defined by their meromorphic sections. So we will identify S_X with the subgroup of algebraic cycles $H_2(X, \mathbb{Z})_{\text{alg}}$ of $H_2(X, \mathbb{Z})$.

Let $T_X = (S_X)^\perp$ be the *transcendental lattice*. We have the *Hodge decomposition*

$$H^2(X, \mathbb{C}) = H^{2,0} \oplus H^{1,1} \oplus H^{0,2} \cong \mathbb{C} \oplus \mathbb{C}^{20} \oplus \mathbb{C},$$

and $(S_X)_\mathbb{C} \subset H^{1,1}$. Thus $(T_X)_\mathbb{C}$ has a decomposition

$$(T_X)_\mathbb{C} = H^{2,0} \oplus H_0^{1,1} \oplus H^{0,2} \cong \mathbb{C}^{22-\rho},$$

[1] The assumption that $b_1(X) = 0$ implies that the group $H_1(X, \mathbb{Z})$ is finite. Any its nonzero element defines a finite unramified cover $f : X' \to X$ of some degree $d > 1$ with $K_{X'} = f^*(K_X) = 0$, hence $p_g(X') = 1$ and $c_2(X') = dc_2(X) = 24d$ giving a contradiction to the Noether formula. This shows that $H^2(X, \mathbb{Z})$ has no torsion. A much more difficult fact is that $\pi_1(X) = 0$.

where $H_0^{1,1} = (T_X)_{\mathbb{C}} \cap H^{1,1}$. The complex line $\mathfrak{p}(X) := (H^{2,0} \subset (T_X)_{\mathbb{C}})$, viewed as a point on the projective space $|(T_X)_{\mathbb{C}}|$ of lines in $(T_X)_{\mathbb{C}}$ is called the *period* of X. If we choose a basis ω in $H^{2,0}(X) = \Omega^2(X)$, then we have a complex valued linear function on $H_2(X, \mathbb{Z})$ defined by $\gamma \mapsto \int_\gamma \omega$. Integrating over an algebraic cycle coming from S_X, we get zero (because our form is of type $(2,0)$ and an analytic cycle has one complex coordinate z), so the function can be considered as a linea function on $(H_2(X,\mathbb{C})/S_X)$, i.e. an element from $(T_X)_{\mathbb{C}}$. This explains the name *period*.

The Poincaré Duality on $H^2(X, \mathbb{C})$ corresponds via the de Rham Theorem, to the exterior product of 2-forms. Since ω is a form of type $(2,0)$, we get $w \wedge w = 0$. Thus $\mathfrak{p}(X)$ belongs to a quadric Q_T in $|(T_X)_{\mathbb{C}}|$ defined by the quadratic form defining the quadratic lattice $H^2(X, \mathbb{Z})$ restricted to T_X. Also, $\omega \wedge \bar{\omega}$ is a form of type $(2,2)$ which is proportional to the volume form generating $H^4(X, \mathbb{R})$. Since its sign does not depend on a scalar multiple of ω, we may choose an orientation on the 4-manifold X to assume that it is positive. Thus we get a second condition $\omega \wedge \bar{\omega} > 0$. This defines an open (in the usual topology) subset Q^0 of Q. So, we see that the period $\mathfrak{p}(X)$ defines a point on the manifold Q^0 of dimension $20 - \rho(X)$. We would like to introduce a space, where the periods lie. However, our our manifold Q^0 obviously depends on X, so we have to find some common target fro the map $X \mapsto \mathfrak{p}(X)$.

We fix an even quadratic lattice S of signature $(1, r)$ and a primitive embedding $S \hookrightarrow L_{K3}$ (primitive means that the quotient group has no torsion). Then we repeat everything from above, replacing S_X with S, and denoting by T its orthogonal complement in L_{K3}. Its signature is $(2, 19 - r)$. Then we obtain a quadric Q_T in the projective space $|T_{\mathbb{C}}| \cong \mathbb{P}^{20-r}$ defined by the quadratic form of T. We also obtain its open subset Q_T^0 defined by the condition $x \cdot \bar{x} > 0$. Now we fix a manifold $\mathcal{D}_T := Q_T$ which is called the *period domain* defined by the lattice T. Of course, as a manifold it depends only on its dimension $19 - r$. When, its dimension is positive, it consists of two connected components, each is a Hermitian symmetric domain of orthogonal type of type IV in Cartan's classification of such spaces. We have

$$\mathcal{D}_T \cong \emptyset(2, 19-r)/\mathrm{SO}(2) \times O(19-r), \quad \mathcal{D}_T^0 \cong \mathrm{SO}(2, 19-r)/\mathrm{SO}(2) \times \mathrm{SO}(19-r),$$

where $\mathcal{D}_T^0$ denotes one of the connected components.

A choice of an isomorphism of quadratic lattices $\phi : H^2(X, \mathbb{A}) \to L_{K3}$ (called a *marking*) and a primitive embedding $j : S \hookrightarrow S_X$ such that $\phi \circ j : S \hookrightarrow L_{K3}$ coincides with a fixed embedding $S \hookrightarrow L_{K3}$ (called a *lattice S polarization*) defines a point $\phi(\mathfrak{p}(X)) \in \mathcal{D}_T$. For some technical reasons one has additionally assume that the image of S in S_X contains a semi-ample divisor class, i.e. the class D such that $D^2 > 0$ and $D \cdot R \geq 0$ for every irreducible curve on X. A different choice of (ϕ, j) with the above properties replaces the point $\phi(\mathfrak{p}(X))$ by the point $g \cdot \phi(\mathfrak{p}(X))$, where g belongs to the group

$$\Gamma_S := \{g \in \mathrm{O}(L_{K3}) : g|S = \mathrm{id}_S\}.$$

Let $A_T = T^\vee/T$ be the *discriminant group*, where T embeds in its dual group $T^\vee = \mathrm{Hom}(T, \mathbb{Z})$ via viewing the symmetric bilinear form on T as a homomorphism $\iota : S \to \mathrm{Hom}(S, \mathbb{Z})$ such that $\iota(s)(s') = s \cdot s'$. It is a finite abelian defined by a symmetric matrix representing the quadratic form on T in some basis of T. Its order is equal to the discriminant of the quadratic form. The discriminant group is equipped with a quadratic map

$$q_T : A_T \to \mathbb{Q}/2\mathbb{Z}, \quad x^* \mapsto x^{*2} \mod 2,$$

where $x^* \in T^\vee$ is a representative of a coset in A_T, and we extend the quadratic form q of T to $T^\vee \subset T_{\mathbb{Q}}$ and then check that the definition is well defined on cosets.

We have a natural homomorphism of

$$\rho : \mathrm{O}(T) \to \mathrm{O}(A_T, q_T).$$

Its kernel consists of orthogonal transformations of T that can be lifted to an orthogonal transformation σ of L_{K3} such that $\sigma|S = \mathrm{id}_S$. Thus we obtain that

$$\Gamma_T \cong \mathrm{Ker}(\rho).$$

Now we can consider the quotient space $\mathcal{D}_T/\Gamma_T$. It is a quasi-projective algebraic variety of dimension $20 - \rho$. The *Global Torelli Theorem* of I. Pyatetsky-Shapiro and I. Shafarevich asserts that assigning to X its period point $\mathfrak{p}$ defined a point in $\mathcal{D}_T$ that does not depend on marking ϕ and two S-poilarzed surfaces are isomorphic preserving the polarization if and only if the images are the same. One can use this to identify the quotient with the coarse moduli space $\mathcal{M}_{K3,S}$E of S-polarized K3 surfaces.

For any vector $\delta \in T$, let $\delta^\perp$ denote the orthogonal complement of $\mathbb{C}\delta$ in $T_\mathbb{C}$. This is a hyperplane in the projective space $|T_\mathbb{C}|$ defined by a linear function with rational coefficients. Let $H_\delta = \mathcal{D}_T \cap \delta^\perp$ be the subset of the period domain $\mathcal{D}_T$. If $\delta^2 < 0$, then the signature of the lattice $(\mathbb{R}\delta)^\perp \subset T_\mathbb{R}$ is equal to $(2, 18 - r)$, so H_δ is the same type domain. For any positive integer N consider

$$\mathcal{H}(N) = \bigcup_{\delta, \delta^2 = -N} H_\delta.$$

The group Γ_T acts on the set of δ's with $\delta^2 = -N$ and we denote by $\mathrm{Heeg}(N)$ the image of $\mathcal{H}(N)$ in the quotient space $\mathcal{M}_{K3,S}$. It is empty or a hypersurface in $\mathcal{M}_{K3,S}$. It is denoted by $\mathrm{Heeg}(N)$ and is called the *Heegner divisor* in the moduli space of lattice S polarized K3 surfaces.

In the next lecture we will compare it with the Humbert surface $\mathrm{Hum}(\Delta)$.