Endomorphisms of Complex Abelian Varieties

Igor Dolgachev and Yuri G. Zarhin

July 31, 2024

Contents

Introduction

This book is an extended version of lecture notes of the first-named author for a short course lectures at the University of Milan in February, 2014. The goal was to provide an introduction to the theory of endomorphisms of complex abelian varieties with an emphasis on the geometric aspects of theory related to classical algebraic geometry and the theory of K3 surfaces. The fruitful collaboration with the second-named author allowed us to clean the notes of numerous inaccuracies, add more factual material add some arithmetical aspects of the theory.

There are numerous expositions of the theory of abelian varieties, a book of Mumford [126] being the best example. Most of them include the theory of abelian varieties as a separate chapter. The novelty of our exposition is to provide an elementary self-contained and more detailed introduction to this subject as well as to provide some new results and many examples relating this theory to other objects of study in algebraic geometry like K3 surfaces, curves of low genus, and del Pezzo surface.

The following is the contents of the book. In Chapter 1, we give the basic facts about complex tori and complex abelian varieties and discuss the question of the fields of the definition for them,

In Chapter 2, we discuss the algebras of endomorphisms of a complex abelian varieties and their linear representations on the subgroup of l-torsion points. We also give an introduction to the theory of central simple finite-dimensional algebras.

In Chapter 3, we specialize in the case of one-dimensional abelian varieties, elliptic curves. In particular, we discuss elliptic curves with complex multiplication and the conditions for the non-existence of an isogeny between them. We also discuss the conditions for an abelian variety to be isogenous to the product of elliptic curves.

In Chapter 4, we discuss Humbert's condition on the period matrix of an abelian surface for its endomorphism algebra containing a real quadratic algebra over $\mathbb{Q}$. Such abelian varieties can be parameterized by a complex surface known as a Humbert surface. We discuss two types of such surfaces corresponding to whether the discriminant of the Humbert singular equation is square or not.

In Chapter 5, we discuss abelian surfaces whose algebra of endomorphisms contains an indefinite quaternion algebra. They are also known as fake elliptic curves because their moduli space is isomorphic to the quotient of the upper half-plane by a discrete group. We give several explicit examples of such abelian surfaces.

In Chapter 6, we relate the theory of abelian surfaces and K3 surfaces. The simplest example of the relationship is the fact that quotient of an abelian surface by its negation involution is birationally isomorphic to a K3 surface. We give a brief introduction to the theory of periods that is used to construct the moduli space of K3 surfaces with a given structure of their Picard lattice. We explain the isomorphism between the moduli space of abelian surfaces with polarization of degree n and the moduli space of K3 surfaces with the lattice polarization of a certain type depending on n. In particular, we discuss some explicit examples of moduli spaces of lattice polarized K3 surfaces that are isomorphic to Humbert surfaces.

In Chapter 7, we discuss the moduli space of principally polarized abelian surfaces with level two structures. By a theorem of Igusa, this moduli space admits a compaticfication isomorphic to a hypersurface of degree four in $\mathbb{P}^4$ with an explicit $\mathfrak{S}_6$-invariant equation. The hypersurface was known classically as the Castelnuovo quartic three-fold and its projectively dial hypersurface is the famous Segre cubic hypersurface with the maximal number of ordinary singular points. We discuss some surfaces related to Humbert surfaces.

In Chapter 8, we discuss abelian varieties isomorphic to the Jacobian variety of a smooth projective algebraic curve of genus three. The canonical model of such a curve is a plane quartic curve. We discuss the geometry of such curves that admit a biregular involution. The cyclic cover of the projective plane of degree four ramified along a a smooth quartic curve is a quartic K3 surface. We discuss the geometry of quartic curves with some On the other hand, the double cover of the projective plane ramified along a quartic curves is a rational del Pezzo surface of degree 2. We give a brief introduction to the theory of del Pezzo surfaces and find the explicit condition on the del Pezzo surface in order the endomorphism ring of the Jacobian is isomorphic to $\mathbb{Z}$.

In Chapter 9, we give a brief introduction to the theory of Shimura varieties that serve as the moduli spaces of abelian varieties with the given structure of its algebra of automorphisms. In particular, we discuss the Mumford-Tate groups and abelian varieties with complex multiplication.

In Chapter 10, we discuss abelian varieties which are isomorphic to the Jacobian varieties of genus g curves. The algebra endomorphisms of such an abelian varieties can be described in terms of the algebra of correspondences on the curve. We find a condition on the curve for the algebra of endomorphisms of its Jacobian variety to be isomorphic to $\mathbb{Z}$.

Finally, in the last Chapter 11, we discuss the subvarieties of the moduli space of abelian varieties with fixed polarization that contain a Zariski dense subset parametrizing abelian varieties with complex multiplication.

We do not discuss results of Faltings [50,51,53] related to the Tate conjecture on homomorphisms of abelian varieties in characteristic zero - there are several excellent books that discuss this topic in details [31,52,163] as well as a survey article [177]. (See also [36, Sect. 4.4] and [14,49,186,187, 192].)

The first-named author expresses his gratitude to Professor Bert van Geemen for giving him the opportunity to give the course of lectures on endomorphisms of abelian varieties at the University of Milan. He also thanks the audience for their active involvement with the lectures by correcting inaccuracies and asking challenging questions.

The second named author was partially supported by the Simons Foundation Collaboration grant #

585711. Part of this work was done in January–May 2022 and December 2023 during his stay at the Max-Planck Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

Chapter 1

Complex Abelian Varieties

The main references here are to the book [106], [34], [88], [126]. For convenience for a reader, we will briefly remind the basic facts and fix the notations.

1.1 Compact Complex Tori

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 tangent bundle of A is trivial; it is naturally isomorphic to $A \times V$. Thus, the complex space V is naturally isomorphic to the tangent space of A at the origin, or to the linear space of holomorphic vector fields $\Theta(A)$ on A. It is also isomorphic to the universal cover of A. The group Λ can be identified with the fundamental group of A that coincides with $\mathrm{H}_1(A, \mathbb{Z})$. The dual linear space $V^\vee$ is naturally isomorphic to the linear space $\Omega^1(A)$ of holomorphic differential 1-forms on A. The map:

$$\alpha : \Lambda = \mathrm{H}_1(A, \mathbb{Z}) \to \Omega^1(A)^* = V, \quad \alpha(\gamma) : \omega \mapsto \int_\gamma \omega,$$

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 $V^\vee$. The map $\mathrm{H}_1(A, \mathbb{Z}) \to V$ 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 $\mathrm{H}^1(A, \mathbb{C})$.

[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.

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

Since a complex torus of dimension g is diffeomorphic to the product of $2g$ circles, for any abelian group G of coefficients, we have an isomorphism

$$H^n(A, G) \cong \bigwedge^n H^1(A, G).$$

In particularly, we have an isomorphism

$$H^n(A, \mathbb{Z}) \cong \bigwedge^n H^1(A, \mathbb{Z}) = \bigwedge^n \Lambda^\vee.$$

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

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

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

The complex cohomology group $H^n(A, \mathbb{C})$ admits the *Hodge decomposition*:

$$H^n(A, \mathbb{C}) \cong \bigoplus_{p+q} H^q(A, \Omega^p_A), \tag{1.3}$$

where Ω^q_A is the head of holomorphic p-forms, and

$$H^q(A, \Omega^p_A) \cong \bigwedge^p V \otimes \bigwedge^q V^\vee. \tag{1.4}$$

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 $z_1, \dots, z_g$ on V, the Kähler metric is given 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 $\mathrm{H}^2(A, \mathbb{R})$.

Let $\mathrm{Pic}(A)$ be the group of isomorphisms of holomorphic line bundles on A. One can describe it by means of the *Appel-Humbert data* attached to (V, Λ). It is a pair (H, χ) that consists of an *Hermitian form* $H : V \times V \to \mathbb{C}$ such that

$$\mathrm{Im}(H)(\Lambda, \Lambda) \subset \mathbb{Z} \tag{1.5}$$

and a *semi-character* $\chi : \Lambda \to \mathbb{U}(1)$ of Λ, i.e. a map

$$\chi : \Lambda \to \mathrm{U}(1) := \{z \in \mathbb{C}, |z| = 1\}$$

satisfying

$$\chi(\lambda\lambda') = \chi(\lambda)\chi(\lambda')e^{\pi i \mathrm{Im}(H(\lambda,\lambda'))}. \tag{1.6}$$

Combining (1.5) and (1.6), we obtain that, for all $\lambda, \lambda' \in \Lambda$,

$$\chi(\lambda\lambda') = \pm\chi(\lambda)\chi(\lambda'). \tag{1.7}$$

(Notice that if $H \equiv 0$, a semi-character $\chi : \Lambda \to \mathrm{U}(1)$ is a group homomorphism, i.e., a character of Λ.)

If H is a Hermitian form on V that enjoys property (1.5), then there exists a semi-character $\chi : \Lambda \to \mathrm{U}(1)$ such that (H, χ) is an A.-H. data. If (H', χ') is another A.-H. data for V, then both $(H + H', \chi\chi')$ and $(H - H', \chi/\chi')$ are also A.-H. datas. In other words, the set of all A.-H. datas attached to (V, Λ) carries the natural structure of a commutative group where the identity element is the pair $(0, \mathbf{1})$ where $\mathbf{1} : \Lambda \to \{1\} \subset \mathrm{U}(1)$ is the constant map.

If H is an Hermitian form on V that enjoys property (1.5), then there exists a semi-character $\chi : \Lambda \to \mathrm{U}(1)$ such that the pair (H, χ) is an A.H. data. The set of of such χ (for given H) is obviously a torsor over the group $\mathrm{Hom}(\Lambda, \mathrm{U}(1)) \cong \mathrm{Hom}(\Lambda, \mathrm{U}(1))^{2g}$.

Each A.-H. data (H, χ) defines a holomorphic line bundle $L = \mathcal{L}(H, \chi)$. It is defined to be the quotient of the trivial holomorphic line bundle $V \times \mathbb{C}$ by the free action of Λ:

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

The projection map $V \times \mathbb{C} \to V$ is Λ-equivariant (here the subgroup Λ acts on V by translations) and induces the structure of a holomorphic line bundle over $V/\Lambda = A$ on $L = L(H, \chi)$.

Conversely, every holomorphic line bundle L on $A = V/\Lambda$ becomes trivial (isomorphic to $V \times \mathbb{C}$) after pulling back to V and is isomorphic to $\mathcal{L}(H, \chi)$ for precisely one A.H. data (H, χ) attached to (V, Λ) (Theorem of Appel-Humbert). In order to find H, one should consider the first Chern class of L, i.e., the corresponding alternating bilinear form

$$c_1(L) \in \mathrm{H}^2(A, \mathbb{Z}) = \mathrm{Hom}(\bigwedge^2 \Lambda, \mathbb{Z}).$$

Extending this bilinear form by $\mathbb{R}$-linearity to $\Lambda_{\mathbb{R}} = V$, we get an alternating $\mathbb{R}$-bilinear form

$$E : V \times V \to \mathbb{R}.$$

It turns out that E coincides with the imaginary part of H.

It follows that

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

Notice that, for all $u, v \in V$,

$$H(u, v) = \mathcal{R}(u, v) + \mathbf{i}E(u, v)$$

and, therefore (multiplying it by $\mathbf{i}$),

$$-E(u, v) + \mathbf{i}\mathcal{R}(u, v) = \mathbf{i}\big(\mathcal{R}(u, v) + \mathbf{i}E(u, v)\big) =$$

$$\mathbf{i}H(u, v) = H(\mathbf{i}u, v) = \mathcal{R}(\mathbf{i}u, v) + \mathbf{i}E(\mathbf{i}u, v).$$

Comparing the real and imaginary parts, we obtain the real part of H:

$$\mathcal{R}(u, v) = E(\mathbf{i}u, v),\ H(u, v) = E(\mathbf{i}u, v) + \mathbf{i}E(u, v), \quad \forall u, v \in V. \tag{1.8}$$

On the other hand, since H is Hermitian, $H(\mathbf{i}u, \mathbf{i}v) = H(u, v)$, i.e.,

$$\mathcal{R}(\mathbf{i}u, \mathbf{i}v) = \mathcal{R}(u, v),\ E(\mathbf{i}u, \mathbf{i}v) = E(u, v), \quad \forall u, v \in V. \tag{1.9}$$

Remark 1.1. Suppose that $H \equiv 0$ and $(0, \chi)$ is an A.H. data. Then, $\chi : \Lambda \to \mathrm{U}(1)$ is a group homomorphism and $\mathcal{L}(H, \chi)$ is the quotient of $V \times \mathbb{C}$ modulo the following action of Λ:

$$(v, z) \mapsto (v + \lambda, \chi(\lambda)z)\ \forall v \in V, z \in \mathbb{C}, \lambda \in \Lambda. \tag{1.10}$$

Let us consider the principal $\mathbb{C}^*$-bundle $\mathcal{L}(0, \chi)^*$ obtained from $\mathcal{L}(H, \chi)$ by deleting the zero section. Then, $\mathcal{L}(0, \chi)^*$ may be viewed as the quotient of the commutative complex Lie group $V \times \mathbb{C}^*$ by its discrete subgroup

$$\tilde{\Lambda} = \{(\lambda, \chi(\lambda)) \mid \lambda \in \Lambda\} \subset V \times \mathbb{C}^*.$$

It carries the natural structure of the commutative complex Lie group that fits in the short exact sequence:

$$1 \to \mathbb{C}^* \to \mathcal{L}(0, \chi)^* \to A \to 0$$

(see [188, Sect. 11]).

We say that A.H. data (H, χ) is a *polarization* of A if H is a positive-definite Hermitian form on V. Two polarizations with the same Hermitian form are called *equivalent*. (Sometimes one calls a polarization just a positive-definite Hermitian form H on V that enjoys property (1.5).)

The following conditions are obviously equivalent.

1. (H, χ) is a polarization.
2. The symmetric $\mathbb{R}$-bilinear form $\mathcal{R} = \mathrm{Re}(H) : V \times V \to \mathbb{R}$ is positive-definite.
3. If $E = \mathrm{Im}(H)$, then, for any nonzero $v \in V$,

$$E(\mathbf{i}u, u) > 0.$$

1.2 Abelian Varieties

A complex torus A is called an *abelian variety* if it admits a polarization. A holomorphic line bundle L on A is called *ample* if $L \cong \mathcal{L}(H, \chi)$ where H is a polarization. It is known that L is ample if and only if the holomorphic sections of some positive tensor power of L embed A in a complex projective space. More precisely, L is ample if and only if the holomorphic sections of $L^{\otimes 3}$ embed A in a projective space (a theorem of Lefschetz) [127, p. 28].

Note that the Hermitian form H on can be uniquely reconstructed from the restriction of $\mathrm{Im}(H)$ to $\Lambda \times \Lambda$, first one extends it, by $\mathbb{R}$-linearity, to a $\mathbb{R}$-bilinear and R-valued symplectic form E on W, and then checks that

$$H(x, y) = E(\mathbf{i}x, y) + \mathbf{i}E(x, y). \tag{1.11}$$

In fact,

$$H(x, y) = \mathcal{R}(x, y) + \mathbf{i}E(x, y);\ \mathcal{R}(x, y) = \mathrm{Re}(H(x, y)), E(x, y) = \mathrm{Im}(H(x, y))$$

implies

$$H(\mathbf{i}x, y) = \mathcal{R}(\mathbf{i}x, y) + \mathbf{i}E(\mathbf{i}x, y) = \mathbf{i}H(x, y) = \mathbf{i}\mathcal{R}(x, y) - E(x, y).$$

Hence, comparing the real and imaginary parts, we get $\mathcal{R}(x, y) = E(\mathbf{i}x, y)$. Since $H(x, y) = H(\mathbf{i}x, \mathbf{i}y)$ and its real part is a positive definite symmetric bilinear form, we immediately obtain that E satisfies

$$E(\mathbf{i}x, \mathbf{i}y) = E(x, y), \quad E(\mathbf{i}x, y) = E(\mathbf{i}y, x), \quad E(\mathbf{i}x, x) > 0,\ x \neq 0. \tag{1.12}$$

We say that a complex structure (W, I) on the real vector space W is *polarized* with respect to a symplectic form E on W if E satisfies (1.12) (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

$$H_{\mathbb{C}}(x, y) = \tfrac{1}{2}\mathbf{i}E_{\mathbb{C}}(x, \bar{y}). \tag{1.13}$$

Let $x = a + \mathbf{i}b, y = a' + \mathbf{i}b' \in W_{\mathbb{C}}$ with $a, b, a', b' \in W$.

We have

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

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

Now, if $x = w - \mathbf{i}I(w), x' = w' - \mathbf{i}I(w') \in V$,

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

and

$$E_{\mathbb{C}}(x, x') = E_{\mathbb{C}}(w - \mathbf{i}I(w), w' - \mathbf{i}I(w'))$$

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

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

$$\mathsf{G}(g,W_{\mathbb{C}})_E := \{V \in \mathsf{G}(g,W_{\mathbb{C}}) : H_{\mathbb{C}}|_V > 0, E_{\mathbb{C}}|_V = 0\}. \tag{1.14}$$

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

Conversely, let us fix a real vector space W of dimension $2g$ that contains a discrete lattice Λ of rank $2g$, so that W/Λ is a real torus of dimension $2g$. Suppose we are given a symplectic form $E \in \bigwedge^2 W^\vee$ 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 (1.13).

Suppose $V = (W,I) \in \mathsf{G}(g,W_{\mathbb{C}})_E$. It is immediate to check that $E_{\mathbb{C}}(\bar{x},y) = \overline{E_{\mathbb{C}}(x,\bar{y})}$. Thus, $H(\bar{x},\bar{x}) = -H(x,x) < 0$. 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 $I(w) = \mathbf{i}(v-\bar{v})$ is isomorphic to the complex structure on V via the projection $W \to V, v+\bar{v} \to v$. 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 (1.14).

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

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

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

Remark 1.2. According to Elie Cartan's classification of Hermitian symmetric spaces there are four classical types I,II, III and IV and two exceptional types E_6 and E_7. We will see type IV spaces later while discussing K3 surfaces, and we will see other classical types while discussing special subvarieties of the moduli spaces of abelian varieties. It is not known whether the exceptional types admit realizations as the moduli spaces of some geometric objects.

So far, we have forgotten about the lattice Λ in the real vector space W. The space $\mathsf{G}(g,W_{\mathbb{C}})_E$ 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 Kähler 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 $\mathrm{diag}[d_1,\dots,d_g]$ where all d_i are positive integers with $d_i|d_{i+1}, i = 1,\dots,g-1$. The sequence $(d_1,\dots,d_g)$ 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 $d = d_1 \cdots d_g$ is equal to the determinant of any skew-symmetric matrix representing the form. It is called the *degree* of the polarization.

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*.

The number d_g is equal to the exponent of the abelian group $\Lambda/\iota(\Lambda)$, where $\iota : \Lambda \to \Lambda$ is defined by the non-degenerate bilinear form $\Im(H)$. It is denoted by $e(L)$ and is called the *exponent* of the polarization defined by an ample line bundle L.

A polarization is called *primitive* if $\gcd(d_1, \ldots, d_g) = 1$. It is called *principal* if its degree is equal to 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 $(Z\ \mathsf{D})$. Write $Z = X + \mathbf{i}Y$, where $X = \mathrm{Re}(\tau)$ and $Y = \mathrm{Im}(\tau)$ are real matrices. Then $\gamma_k = \sum_{s=1}^{g} x_{ks}e_s + \sum y_{ks}ie_s, k = 1, \ldots, g$, and 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

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

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

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

We have proved one direction of the following theorem.

Theorem 1.3 (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*

$$
{}^tZ = Z, \quad \mathrm{Im}(Z) > 0.
$$

We leave the proof of the converse to the reader.

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

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

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

we obtain that

$$S = \mathrm{Im}(\tau)^{-1}. \tag{1.15}$$

So, we see that we can choose a special basis $(\gamma_1, \ldots, \gamma_{2g})$ 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

$$\mathfrak{H}_g := \{Z \in \mathrm{Mat}_n(\mathbb{C}) : {}^t Z = Z, \mathrm{Im}(Z) > 0\}.$$

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

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

Note that $\mathfrak{H}_g \cong \mathsf{G}(g, \mathbb{C}^g)_E$, where $E : \mathbb{R}^{2g} \times \mathbb{R}^{2g} \to \mathbb{R}$ is a symplectic form defined by the matrix D. However, the isomorphism depends on a choice of a special basis in $\mathbb{R}^{2g}$. One must view $\mathfrak{H}_g$ as the moduli space of polarized 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

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

If $X = \begin{pmatrix} N_1 & N_2 \\ N_3 & N_4 \end{pmatrix}$, where N_1, N_2, N_3, N_4 are square integer matrices of size g, then $X \in \mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ if and only if

$$N_1 \cdot \mathsf{D} \cdot {}^t N_2 = N_2 \cdot \mathsf{D}^t \cdot N_1, \quad N_3 \cdot \mathsf{D} \cdot {}^t N_4 = N_4 \cdot \mathsf{D} \cdot {}^t N_3, \quad N_1 \cdot \mathsf{D} \cdot {}^t N_4 - N_2 \cdot \mathsf{D} \cdot {}^t N_3 = \mathsf{D}.$$

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

$$\mathcal{A}_{g,\mathsf{D}} = \mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z}) \backslash \mathfrak{H}_g.$$

The group $\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ acts on $\mathfrak{H}_g$ by

$$Z \mapsto (ZN_1 + N_2)(N_3 Z + N_4)^{-1} \mathsf{D}.$$

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

$$\mathcal{A}_g = \mathrm{Sp}(2g, \mathbb{Z}) \backslash \mathfrak{H}_g.$$

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 holomorphic 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 $c_1(L_i) = \alpha_i \in \bigwedge^2 \Lambda^\vee$ and

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

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

$$L^g = g! d_1 \cdots d_g.$$

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

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

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

$$\chi(L) = \sum_{i=0}^{g} (-1)^i \dim H^i(A, L) = \frac{L^g}{g!}.$$

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 linear space $H^{1,0}(A)$ with the dual linear space $V^\vee$. Using the Dolbeault's Theorem, one can identify $H^{0,1}(A)$ with the cohomology group $\mathrm{H}^1(A, \mathcal{O}_A)$. The group $\mathrm{H}^1(A, \mathbb{Z}) = \Lambda^\vee$ embeds in $\mathrm{H}^1(A, \mathbb{C})$, and its projection to $H^{0,1}$ is a discreet subgroup Λ' of rank $2g$ in $H^{0,1}$. The inclusion $\mathrm{H}^1(A, \mathbb{Z}) \to \mathrm{H}^1(A, \mathcal{O}_A)$ corresponds to the homomorphism derived from the exponential exact sequence

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

by passing to cohomology. It also gives an exact sequence

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

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

Remark 1.4. Note that one can define the group $\mathrm{Pic}^0(X)$ for any irreducible projective algebraic variety X over an algebraically closed field (in fact, in much more general situation) as the group of classes of divisors algebraically equivalent to zero modulo linear equivalence. It can be equipped with a structure of an algebraic connected commutative group variety. It X is nonsingular, it has a structure of an abelian variety defined as a complete connected algebraic group. It is called the *Picard variety* of X.

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 linear space V to the linear space $\bar{V}^\vee$ of $\mathbb{C}$-antilinear functions on V (where $\bar{V}$ is equal to V with the complex structure $I(v) = -iv$).[2] Considered as a vector space over $\mathbb{R}$, it is isomorphic to the real vector space $W^\vee = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ by means of the isomorphism

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

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

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

so that

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

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

$$\phi_L : A \to \hat{A} \tag{1.16}$$

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

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

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 holomorphic line bundle L defines a map (1.16) 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 $(d, \dots, d)$ can be identified with the multiplication map $[d] : x \to dx$. Its kernel is the subgroup $A[d]$ of d-torsion points in A. Clearly, d_g coincides with the exponent e_L of the group $K(L)$, which is 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, $\phi_L^{-1} \circ \phi_L = [e_L]$.

1.3 Questions of Rationality

In this section, we will view abelian varieties as algebraic varieties and discuss the fields of definition of these varieties, their torsion points and endomorphisms.

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

Definition 1.1 (Definition-Construction)**.** Let us fix a holomorphic embedding of an abelian variety A into a complex projective space $\mathbb{P}^N(\mathbb{C})$. In what follows, we will identify A with its image in $\mathbb{P}^N(\mathbb{C})$. Then, A is complex projective manifold, hence by the Chow theorem, it is a complex projective *algebraic* variety, i.e., is the set of common zeros of finitely many homogenous polynomials in homogeneous coordinates $(T_0 : \dots T_n)$ in $\mathbb{P}^N$. (Its irreducibility follows readily.) All the coefficients of these polynomials lie in $\mathbb{C}$. However, there are only finitely many such coefficients that generate a certain finitely generated subfield K of $\mathbb{C}$ over $\mathbb{Q}$. Extending this subfield, in order to make "rational" the zero 0_A of group law on A, we may assume that $0_A \in A(K)$. Applying the Chow theorem to the graph in $\mathbb{P}^N(\mathbb{C}) \times \mathbb{P}^N(\mathbb{C}) \times \mathbb{P}^N(\mathbb{C}) \subset \mathbb{P}^{(N+1)^3-1}(\mathbb{C})$ of the holomorphic addition map $A \times A \to A, (x, y) \mapsto x + y$, we obtain that the addition map is a regular map of projective algebraic varieties that is defined over a certain finitely generated extension of K. So, further extending K, we may and will assume that the addition map is defined over a certain subfield K of $\mathbb{C}$ that is finitely generated over $\mathbb{Q}$. In a similar way, considering the inversion map $A \to A, a \mapsto -a$ and enlarging the field, we may and will assume that there is a subfield $K \subset \mathbb{C}$ that is finitely generated over $\mathbb{Q}$ and such that A is a projective algebraic K-subvariety of $\mathbb{P}^N$ such that $0_A \in A(K)$, and the group law and the inversion map on A are defined over K. If K enjoys all these properties, we say that *the abelian variety A is defined over K*. If this is the case and L is a subfield of $\mathbb{C}$ that contains K, we set

$$A(L) := A \bigcap \mathbb{P}^N(L),$$

which is a *subgroup* of A.

If L is finitely generated over $\mathbb{Q}$, then a theorem of Mordell-Weil-Néron-Lang asserts that $A(L)$ is a finitely generated commutative group [104, 111].

In what follows, we will use the following elementary observation:

Lemma 1.5. *Let K be a subfield of $\mathbb{C}$ that is finitely generated over $\mathbb{Q}$, and $\bar{K}$ be its algebraic closure in $\mathbb{C}$. Let $\mathrm{Aut}(\mathbb{C}/\bar{K})$ be the group of all field automorphisms of $\mathbb{C}$ that leave invariant every element of $\bar{K}$. Let N be be a positive integer. Let us consider the natural action of $\mathrm{Aut}(\mathbb{C}/\bar{K})$ on $\mathbb{P}^N(\mathbb{C})$.*

Then, the set of fixed points coincides with $\mathbb{P}^N(\bar{K})$. Every $\mathrm{Aut}(\mathbb{C}/\bar{K})$-orbit that is not a fixed point is infinite.

Theorem 1.6. *Let K be a subfield of $\mathbb{C}$ that is finitely generated over $\mathbb{Q}$, and $\bar{K}$ its algebraic closure in $\mathbb{C}$. Suppose that A is an abelian variety that is defined over K. Then*

(i) All points of finite order on A are defined over $\bar{K}$.

(ii) Let f be a holomorphic endomorphism of the commutative complex Lie group A. Then, f is a regular self-map of the projective algebraic variety A that is defined over $\bar{K}$.

Proof. Since A is defined over K, it is a $\mathrm{Aut}(\mathbb{C}/\bar{K})$-invariant subset of $\mathbb{P}^N(\mathbb{C})$; the set of fixed points on A coincides with $A(\bar{K})$.

If n is a positive integer then let us consider the subgroup

$$A[n] = \{x \in A \mid nx = 0_A\}$$

of A. For the future use we denote the subgroup $\mathrm{Tors}(A)$ of torsion elements of A by $A[\infty]$, and, for any prime l, denote its l-primary component by $A[l^\infty]$.

Since $A = V/\Lambda$, the group

$$A[n] = \frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$$

is finite. Since A, together with its group structure, is defined over K, each $\sigma \in \mathrm{Aut}(\mathbb{C}/\bar{K})$ sends $A[n]$ to $A[n]$. This implies that the $\mathrm{Aut}(\mathbb{C}/\bar{K})$-orbit of every $x \in A[n]$ lies in $A[n]$ and therefore is a finite set. By Lemma 1.5, $x \in \mathbb{P}^N(\bar{K})$, i.e.,

$$x \in A \bigcap \mathbb{P}^N(\bar{K}) = A(\bar{K}).$$

This means that $A[n] \subset A(\bar{K})$, which proves (i).

In order to prove (ii), observe that the set

$$A[\infty] = \bigcup_{n=1}^{\infty} A[n] = \bigcup_{n=1}^{\infty} \frac{1}{n}\Lambda/\Lambda$$

is everywhere dense in $A = V/\Lambda$ in classical complex topology and, therefore, in Zariski topology as well. Since f is a group endomorphism, $A[\infty]$ is f-invariant; moreover, f is uniquely determined by its restriction to $A[\infty]$. Applying Chow's theorem to the graph of f in the projective algebraic variety $A \times A$, we conclude that f is a regular self-map of A. Since A is defined over K, every $\sigma \in \mathrm{Aut}(\mathbb{C}/\bar{K})$ gives rise to the regular self-map ${}^\sigma f$ of A characterized by

$$f {}^\sigma f(\sigma^{-1}x) = \sigma(u(x)) \; \forall x \in A \subset \mathbb{P}^n(\mathbb{C}). \tag{1.17}$$

In particular,

$${}^\sigma f(x) = f(x) \; \forall x \in A(\bar{K}). \tag{1.18}$$

By already proven (i), $A[\infty] \subset A(\bar{K})$. Combining this with (1.18), we conclude that ${}^\sigma f$ coincides with f on $A[\infty]$ and therefore ${}^\sigma f = f$ for all $\sigma \in \mathrm{Aut}(\mathbb{C}/\bar{K})$. This means that f is defined over $\bar{K}$. □

Let $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ be the *absolute Galois group* of K, i.e. the Galois group $\mathrm{Gal}(K^s/K)$ of the separable algebraic closure of K. There is the natural action of $\mathrm{Gal}(K)$ on the commutative group $A(\bar{K})$. Clearly, $A[n]$ is a $\mathrm{Gal}(K)$-stable subgroup of $A(\bar{K})$ for all positive integers n. This gives rise to the continuous group homomorphism

$$\rho_{n,A,K} : \mathrm{Gal}(K) \to \mathrm{Aut}(A[n]) = \mathrm{Aut}_{\mathbb{Z}/n}(A[n]). \tag{1.19}$$

We write

$$\tilde{G}_{n,A,K} \subset \mathrm{Aut}(A[n]) = \mathrm{Aut}_{\mathbb{Z}/n}(A[n])$$

for the image of $\rho_{n,A,K}$ in $\mathrm{Aut}_{\mathbb{Z}/n}(A[n])$. Then, $G(n) := \ker(\rho_{n,A,K})$ is a closed normal subgroup in $\mathrm{Gal}(K)$ of finite index and therefore is an open subgroup of $\mathrm{Gal}(K)$. We write $K(A[n])$ for the subfield of $\ker(\rho_{n,A,K})$-invariants in $\bar{K}$. We call $K(A[n])$ the field of definition of all points of order dividing n on A, because $K(A[n])$ is the smallest overfield L of K such that $A[n] \subset A(L)$. By definition, $K(A[n])$ is a finite Galois extension of K and its Galois group

$$\mathrm{Gal}(K(A[n])/K) = \tilde{G}_{n,A,K} \subset \mathrm{Aut}(A[n]) = \mathrm{Aut}_{\mathbb{Z}/n}(A[n]).$$

If m is any positive integer, then

$$A[n] = \frac{1}{n}\Lambda/\Lambda = m\left(\frac{1}{nm}\Lambda/\Lambda\right) = mA[mn] \subset A[mn],$$

i.e.,

$$A[n] = mA[mn] \subset A[mn].$$

This implies that every automorphism of the commutative group $A[nm]$ leaves invariant the subgroup $A[n]$, and gives rise to the natural homomorphism

$$\pi_{nm,n} : \mathrm{Aut}(A[mn]) \to \mathrm{Aut}(A[n]),\ \pi_{nm,n}(u)(x) = u(x)\ \forall u \in \mathrm{Aut}(A[mn]),\ x \in A[n] \subset A[mn].$$

This implies that

$$\rho_{n,A,K} = \pi_{mn,n} \circ \rho_{mn,A,K} : \mathrm{Gal}(K) \to \mathrm{Aut}(A[mn]) \to \mathrm{Aut}(A[n]),$$

and

$$K \subset K(A[n]) \subset K(A[mn]). \tag{1.20}$$

The following observation that deals with $m = 2$ (and $n = 2$) will be used in Chapter **??**.

Claim 1.7. Let n be an even positive integer.

If $K(A[2n]) \neq K(A[n])$, then $K(A[2n])/K(A[n])$ is an abelian field extension, whose Galois group $\mathrm{Gal}(K(A[2n])/K(A[n])$ is a finite abelian group of exponent 2.

Proof. Let

$$\sigma \in \mathrm{Gal}(K(A[2n]/K(A[n])) \subset \tilde{G}_{2n,A,K} \subset \mathrm{Aut}(A[2n]).$$

Then, for any $x \in A[2n]$, we have $2x \in A[n]$, and therefore, $\sigma(2x) = 2x$. This implies that

$$2(\sigma(x) - x) = \sigma(2x) - 2x = 0,$$

i.e., $y = \sigma(x) - x \in A[2]$, and

$$\sigma(x) = x + y.$$

Notice that $\sigma(y) = y$, because $A[2] \subset A[n]$ (recall that n is even). Thus,

$$\sigma^2(x) = \sigma(x + y) = \sigma(x) + \sigma(y) = \sigma(x) + y = (x + y) + y = x + 2y = x.$$

This proves that each $\sigma \in \mathrm{Gal}(K(A[2n]/K(A[n])$ has order dividing 2, and therefore, $\mathrm{Gal}(K(A[2n]/K(A[n]))$ is a finite abelian group either of exponent 1 (i.e., $K(A[2n]) = K(A[n])$), or of exponent 2. □

Chapter 2

Endomorphisms of Abelian Varieties

In this chapter, we will discuss general facts about endomorphisms of abelian varieties.

2.1 Generalities on Endomorphisms of Abelian Varieties

A holomorphic map $f : A = V/\Lambda \to A' = V'/\Lambda'$ of complex tori that sends zero to zero is called a *homomorphism* of complex tori. One can show that this is equivalent to that f is a homomorphism of complex Lie groups, i.e.,

$$f(x+y) = f(x) + f(y), \quad \forall x, y \in A.$$

Obviously, it is defined by a unique linear $\mathbb{C}$-map $f_a : V \to V'$ (called an *analytic representation* of f) and a unique $\mathbb{Z}$-linear map $f_r : \Lambda \to \Lambda'$ (called a *rational representation* of f) such that the restriction of f_a to Λ coincides with f_r. Namely,

$$f(v + \Lambda) = f_a(v) + \Lambda', \quad \forall v \in V. \tag{2.1}$$

If $A'' = V''/|\Lambda''$ a complex torus and $h : A' \to A''$ a homomorphism of complex tori then the composition $h \circ f : A \to A''$ is also a homomorphism of complex tori and the corresponding $(h \circ f)_a : V \to V''$, $(h \circ f)_r : \Lambda \to \Lambda A''$ enjoy the following properties:

$$(h \circ f)_a = h_a \circ f_a, \ (h \circ f)_r = h_r \circ f_r. \tag{2.2}$$

Example 2.1. Suppose that $V = V'$ and Λ is a subgroup of finite index in Λ'. Then,

$$f : A = V/\Lambda \to A' = V/\Lambda', \ f(v + \Lambda) = v + \Lambda' \ \forall v \in V$$

is a homomorphism of complex tori such that $f_a : V \to V$ is the *identity map*, and $f_r : \Lambda \to \Lambda'$ is the *inclusion map*.

Remark 2.2. Since f is a group homomorphism, $f(A[n]) \subset A'[n])$ for all positive integers n.

Lemma 2.3. *Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be abelian varieties, and $f : A \to A'$ be a homomorphism of abelian varieties.*

(i) The kernel $\ker(f) \subset A$ *of* f *is finite if and only if the corresponding homomorphism* $f_r : \Lambda \to \Lambda'$ *of lattices is injective. If this is the case and* $\dim(A) = \dim(A'$*, then* f *is surjective, the image* $f_r(\Lambda)$ *of* Λ *is a subgroup of finite index in* Λ'*, and this index equals the order of* $\ker(f)$.

(ii) f *is an isomorphism of abelian varieties if and only if* $\dim(A) = \dim(A')$*, and* $f_r(\Lambda) = \Lambda'$.

Proof. Recall that there is a $\mathbb{C}$-linear map $f_a : V \to V'$ such that

$$f_a(\lambda) = f_r(\lambda), \quad \forall \lambda \in \Lambda,$$

$$f(v + \Lambda) = f_r(v) + \Lambda' \in V'/\Lambda' = A' \; \forall v + \Lambda \in V/\Lambda = A.$$

If f_r is not injective then there is a *nonzero* $\lambda \in \Lambda$ such that $f_r(\lambda) = 0 \in V'$. This implies that $f_a(\lambda) = 0 \in V'$. By $\mathbb{C}$-linearity of f_a, the line $\mathbb{C} \cdot \lambda \subset V$ goes to $0 \in V'$. This implies that the image of the *uncountable* set $\mathbb{C} \cdot \lambda$ in $V/\Lambda = A$ lies in the kernel of f. Since Λ is countable, this image is also uncountable, and we obtaint that $\ker(f)$ is an uncountable set. In particular, it is infinite, so f is *not* an isogeny. Assume now that f_r is *injective*. It follows that f_a is also injective, because the natural map

$$\Lambda \otimes \mathbb{R} \to V, \; \lambda \otimes c \mapsto c\lambda$$

is an isomorphism of real vector spaces, and, for any $c \in \mathbb{R}, \; \lambda \in \Lambda$,

$$f_a(c\lambda) = cf_a(\lambda) = cf_r(\lambda).$$

Since A and A' are of the the same dimension, the lattices Λ and Λ' have the same rank. Hence, the image $f_r(\Lambda)$ is a subgroup of finite index in Λ'. Let us denote this index by d. Then, $\Lambda_0 := f_a^{-1}(\Lambda') \subset V$ contains the sublattice

$$f_a^{-1}(f_r(\Lambda) = f_r^{-1}(f_r(\Lambda)) = \Lambda$$

as a subgroup of index d. It follows that the kernel of f is Λ_0/Λ, which is a group of order d. This ends the proof of (i). Assertion (ii) follows readily from (i). □

Clearly, the set $\mathrm{Hom}(A, A')$ of all homomorphisms $f : A$ to A' carries the natural structure of an abelian group and the map

$$\mathrm{Hom}(A, A') \to \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda'), \; f \mapsto f_r,$$

is an *injective* homomorphism of abelian groups. Since the group $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$ is isomorphic (non-canonically) to

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{2\dim(A)}, \mathbb{Z}^{2\dim(A')}) = \mathbb{Z}^{4\dim(A)\dim(A')},$$

$\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda')$ is a free abelian group of rank $\leq 4\dim(A)\dim(A')$ (actually, this bound can be improved to $2\dim(A)\dim(A')$, which is sharp).

Let $\mathrm{End}(A)$ be the set of *endomorphisms* of a complex torus $A = V/\Lambda$, i.e. homomorphisms of A to itself. As usual, the set of endomorphisms of an abelian group is equipped with the structure of an associative unitary ring with multiplication defined 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

$$\rho_a : \mathrm{End}(A) \hookrightarrow \mathrm{End}_{\mathbb{C}}(V) \cong \mathbf{Mat}_g(\mathbb{C}),\ f \mapsto f_a; \quad \rho_r : \mathrm{End}(A) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda) \cong \mathbf{Mat}_{2g}(\mathbb{Z}),\ f \mapsto f_r.$$

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

Instead of the endomorphism ring $\mathrm{End}(A)$, it is often more convenient to work with the endomorphism $\mathbb{Q}$-algebra of endomorphisms of A defined as

$$\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q} \tag{2.3}$$

(often denoted by $\mathrm{End}^0(A)$). By definition, $\mathrm{End}_{\mathbb{Q}}(A)$ is a finite-dimensional $\mathbb{Q}$-algebra and the natural map

$$\mathrm{End}(A) \to \mathrm{End}_{\mathbb{Q}}(A),\ u \mapsto u \otimes 1$$

is a ring embedding. Extending ρ_r by $\mathbb{Q}$-linearity, we get the embedding of $\mathbb{Q}$-algebras

$$\mathrm{End}_{\mathbb{Q}}(A) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda) \otimes \mathbb{Q} = \mathrm{End}_{\mathbb{Q}}(\Lambda_{\mathbb{Q}}), f \otimes s \mapsto f_r \otimes s \quad \forall f \in \mathrm{End}(A), s \in \mathbb{Q}$$

which we continue to denote by ρ_r. Here

$$\Lambda_{\mathbb{Q}} := \Lambda \otimes \mathbb{Q}$$

is the $\mathbb{Q}$-vector space of dimension $2\dim(A)$, which may be viewed as the following $\mathbb{Q}$-vector subspace of $\Lambda_{\mathbb{R}} := \Lambda \otimes \mathbb{R} = V$.

$$\Lambda_{\mathbb{Q}} = \{v \in V \mid \exists \text{ a positive integer } N \text{such that } Nv \in \Lambda\} \subset V.$$

Similarly, we may extend ρ_a by $\mathbb{Q}$-linearity to the embedding of $\mathbb{Q}$-algebras

$$\mathrm{End}_{\mathbb{Q}}(A) \hookrightarrow \mathrm{End}_{\mathbb{C}}(V), \quad \otimes s \mapsto s f_a \quad \forall f \in \mathrm{End}(A), s \in \mathbb{Q}.$$

Taking unto account that $f_r = \rho_r$ coincides with the restriction of $\rho_a(f) = f_a$ to Λ for all $f \in \mathrm{End}(A)$, we conclude that the homomorphism

$$\rho_r(f) : \Lambda_{\mathbb{Q}} \to \Lambda_{\mathbb{Q}} \subset V$$

coincides with the restriction of $\rho_r(f) : V \to V$ to $\Lambda_{\mathbb{Q}}$ for all $f \in \mathrm{End}_{\mathbb{Q}}(A)$.

Example 2.4. Let $A' = V'/\Lambda'$ be a complex torus of positive dimension with $\mathrm{End}(A') \cong \mathbb{Z}$. Let us consider the set $\mathrm{Sub}(\Lambda')$ of all subgroups Λ of finite index in Λ' that enjoy the following property:

$$\Lambda \not\subset m\Lambda', \quad \text{for any integer } m > 1. \tag{2.4}$$

Clearly, $\mathrm{Sub}(\Lambda')$ is an infinite countable set containing Λ'. If $\Lambda_1, \Lambda_2 \in \mathrm{Sub}(\Lambda')$, then let us consider the infinite subgroup of $\mathbb{Z}$ defined by:

$$(\Lambda_2 : \Lambda_1) = \{k \in \mathbb{Z} \mid k \cdot \Lambda_1 \subset \Lambda_2\} \subset \mathbb{Z}. \tag{2.5}$$

Clearly, $(\Lambda_2 : \Lambda_1) = \mathbb{Z}$ if and only if $\Lambda_2 \supset \Lambda_1$. In particular, for any $\Lambda \in \mathrm{Sub}(\Lambda')$,

$$(\Lambda : \Lambda) = \mathbb{Z}.$$

If $\Lambda_1, \Lambda_2, \Lambda_3 \in \mathrm{Sub}(\Lambda')$, then there is a natural biadditive map:

$$(\Lambda_3 : \Lambda_2) \times (\Lambda_2 : \Lambda_1) \to (\Lambda_3 : \Lambda_1), \quad (k_{32}, k_{21}) \mapsto k_{32}k_{21}. \tag{2.6}$$

For each $\Lambda \in \Lambda'$, let us consider the complex torus

$$A_\Lambda := V'/\Lambda.$$

If $\Lambda_1, \Lambda_2 \in \mathrm{Sub}(\Lambda')$, then to each $k \in (\Lambda_2 : \Lambda_1) \subset \mathbb{Z}$ corresponds a homomorphism of complex tori

$$[k] : A_{\Lambda_1} :\to V'/\Lambda_2 = A_{\Lambda_2}, \quad v + \Lambda_1 \mapsto kv + \Lambda_2 \ \forall v \in= V'. \tag{2.7}$$

such that the corresponding maps $[k]_a : V' \to V'$ and $[k]_r : \Lambda_1 \to \Lambda_2$ are as follows:

$$[k]_a(v) = kv, \quad \forall v \in V', \ [k](r)(\lambda) = k\lambda \in \Lambda_2 \ \forall \lambda \in \Lambda_1. \tag{2.8}$$

Clearly, the map $k \mapsto [k]$ defines an embedding of groups:

$$(\Lambda_2 : \Lambda_1) \to \mathrm{Hom}(A_{\Lambda_1}, A_{\Lambda_2}), \ k \mapsto [k]. \tag{2.9}$$

In what follows, we will identify $(\Lambda_2 : \Lambda_1)$ with its image in $\mathrm{Hom}(A_{\Lambda_1}, A_{\Lambda_2})$.

If $\Lambda_1, \Lambda_2, \Lambda_3 \in \mathrm{Sub}(\Lambda')$, then, for each

$$k_{21} \in (\Lambda_2 : \Lambda_1) \subset \mathrm{Hom}(A_{\Lambda_3}, A_{\Lambda_2}) k_{32} \in (\Lambda_3 : \Lambda_1) \subset \mathrm{Hom}(A_{\Lambda_3}, A_{\Lambda_2}),$$

the composition $k_{32} \circ k_{21} \in \mathrm{Hom}(A_{\Lambda_3}, A_{\Lambda_1})$ coincides with the product (2.6)

$$k_{32}k_{21} \in (\Lambda_3 : \Lambda_1) \subset \mathrm{Hom}(A_{\Lambda_3}, A_{\Lambda_1}).$$

Remark 2.5. If $A' = V'/\Lambda'$ is a abelian variety then all $A_\Lambda := V'/\Lambda$ are also abelian varieties. Indeed, if H is a positive-definite Hermitian form on V', whose imaginary part takes on only integer values on Λ', then the same is true for any $\Lambda \subset \Lambda'$.

Theorem 2.6. *Suppose that*

$$\mathrm{End}(A') = \mathbb{Z} = (\Lambda' : \Lambda').$$

Then, the complex tori A_Λ enjoy the following properties:

(i)

$$\mathrm{Hom}(A_{\Lambda_1}, A_{\Lambda_2}) = (\Lambda_2 : \Lambda_1) \ \forall \Lambda_1, \Lambda_2 \in \mathrm{Sub}(\Lambda').$$

(ii)

$$\mathrm{End}(A_\Lambda) = (\Lambda : \Lambda) = \mathbb{Z} \ \forall \Lambda \in \mathrm{Sub}(\Lambda').$$

(iii) If $\Lambda_1, \Lambda_2 \in \mathrm{Sub}(\Lambda')$ then the complex tori A_{Λ_1} and A_{Λ_2} are isomorphic if and only if $\Lambda_1 = \Lambda_2$.

Proof. Let $f : A_{\Lambda_1} \to A_{\Lambda_2}$ be a homomorphism of complex tori with the corresponding analytic and rational representations

$$f_a \in \mathrm{End}_{\mathbb{C}}(V'),\ f_r \in \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2)$$

such that the restriction of f_a to Λ_1 coincides with

$$\Lambda_1 \to \Lambda_2 \stackrel{f_r}{\to} V',$$

and

$$f(v + \Lambda_1) = f_a(v) + \Lambda_2\ \forall v \in V'.$$

Let us consider the index $d = [\Lambda' : \Lambda_1]$, which is a positive integer. Then,

$$df_a(\Lambda') = df_r(\Lambda') = f_r(d(\Lambda') \subset f_r(\Lambda_1) \subset \Lambda_2 \subset \Lambda',$$

and, therefore, the map

$$A' = V/\Lambda' \to V/\Lambda' = A',\ v + \Lambda' \mapsto df_a(v) + \Lambda'\ \forall v \in V' \tag{2.10}$$

defines an endomorphism of the complex torus A'. Since $\mathrm{End}(A') = \mathbb{Z}$, there is an integer m such that

$$mv + \Lambda' = df_a(v) + \Lambda'\ \forall v \in V',$$

i.e.,

$$df_a(v) = mv\ \forall v \in V'.$$

This implies that

$$f_a(v) = \frac{m}{d}v.$$

It follows that

$$\Lambda_2 \subset f_r(\Lambda_1) = f_a(\Lambda_1) = \frac{m}{d}\Lambda_1,$$

and therefore,

$$\frac{m}{d}\Lambda_1 \subset \Lambda_2 \subset \Lambda'. \tag{2.11}$$

We claim that m/d is an *integer*. Indeed, there is a basis $\lambda_1, \ldots, \lambda_{2g}$ (with $g = \dim_{\mathbb{C}}(V')$) of the $\mathbb{Z}$-module Λ' and positive integers $d_1, \ldots, d_{2d}$ such that $d_i \mid d_{i+1}$, and

$$\Lambda_1 = \bigoplus_{i=1}^{2g} \mathbb{Z} \cdot d_i\lambda_i \subset \bigoplus_{i=1}^{2g} \mathbb{Z} \cdot \lambda_i = \Lambda'.$$

It follows from (2.4), that $d_1 = 1$, and, therefore, $\lambda_1 \in \Lambda_1$. Applying (2.11), we conclude that $\frac{m}{d}\lambda_1 \in \Lambda_1$.

Since λ_1 is an element of a basis of the free $\mathbb{Z}$-module Λ', we obtain that $k := m/d \in \mathbb{Z}$. This means that $f_a = [k]_a$ and therefore $f = [k]$, which proves (ii).

(i) follows from (ii) applied to $\Lambda_1 = \Lambda_2 = \Lambda$. In order to prove (iii), suppose that $f : A_{\Lambda_1} \to A_{\Lambda_2}$ is an isomorphism. It follows from (ii) that there is an integer k such that $k\Lambda_1 \subset \Lambda_2$ and $f = [k]$. By Lemma 2.3(2), $[k]_r(\Lambda_1) = \Lambda_2$. In light of (2.8), $k\Lambda_1 = \Lambda_2$. Now it follows from condition (2.4) that $k = \pm 1$, i.e., $\Lambda_2 = \Lambda_1$. □

We will need the following elementary assertion:

Claim 2.7. Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be complex tori, n a positive integer, and $f : A \to A'$ a homomorphism of complex tori. Then,

$$f \in n \cdot \mathrm{Hom}(A, A') \Longleftrightarrow f(A[n]) = \{0\}.$$

In other words, the natural group homomorphism

$$\mathrm{Hom}(A, A')/n \to \mathrm{Hom}_{\mathbb{Z}/n}(A[n], A'[n]),$$

defined by $f + n\mathrm{Hom}(A, A')/ \mapsto f|_{A[n]} : A[n] \to A'[n],\ x \mapsto f(x)$. is injective.

Proof. Both conditions are equivalent to the inclusion

$$f_r(\Lambda) \subset n \cdot \Lambda'.$$

□

Theorem 2.8. *Let $A = V/\Lambda$ and $A' = V'/\Lambda'$ be abelian varieties that are defined over a finitely generated subfield K of $\mathbb{C}$. Then, every homomorphism $f : A \to A'$ is a regular map of projective algebraic varieties that is defined over $\bar{K}$.*

Proof. The graph $\Gamma_f \subset A \times A'$ is a compact smooth complex submanifold of the projective variety $A \times A'$. By Chow's Theorem, Γ_f is a projective variety itself. It follows readily that f is a regular map.

Recall (Remark 2.2) that, for all positive integers n,

$$f(A[n]) \subset A'[n].$$

Since both A and A' are defined over K, every $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ gives rise to the homomorphism of abelian varieties

$$^{\sigma}f : A \to A', \quad x \mapsto \sigma(f(\sigma^{-1}(x)) \ \forall x \in A.$$

Assume now that $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$. Notice that the subfield $\mathbb{C}^{\mathrm{Aut}(\mathbb{C}/K)}$ of all $\mathrm{Aut}(\mathbb{C}/K)$-invariants in $\mathbb{C}$ coincides with K.

Since, for all n,

$$A[n] \subset A(\bar{K}), \quad A'[n] \subset A'(\bar{K}),$$

the homomorphisms f and $^{\sigma}f$ coincide on $A[n]$. Taking into account that $\cup_{n=1}^{\infty} A[n]$ is dense in A, we conclude that

$$^{\sigma}f = f, \quad \forall \sigma \in \mathrm{Aut}(\mathbb{C}/\bar{K}).$$

This means that

$$\sigma(\Gamma_f) = \Gamma_f, \quad \forall \sigma \in \mathrm{Aut}(\mathbb{C}/\bar{K}).$$

It follows that the projective subvariety Γ_f is defined over $\bar{K}$ and therefore f is also defined over $\bar{K}$. □

Remark 2.9. Actually, the same arguments prove that every homomorphism f is defined over the compositum of the fields

$$K(A[\infty]) = \cup_{n=1}^{\infty} K(A[n]) \text{ and } K(A'[\infty]) = \cup_{n=1}^{\infty} K(A'[n]).$$

Clearly, every f is defined over a certain finite algebraic extension of K, and therefore, it is defined over the compositum of $K(A[n])$ and $K(A'[n])$ for some n, in light of the inclusions (1.20). Since $\mathrm{Hom}(A, A')$ is a finitely generated group, there is a positive integer n such that all the homomorphisms $f : A \to A'$ are defined over the compositum of $K(A[n])$ and $K(A'[n])$.

The following useful theorem of A. Silverberg [157], which is based on Minkowski's Lemma [150, Lemma1]), gives a refinement of this statement.

Theorem 2.10. *Let $n \geq 3$ be an integer. Let K be a subfield of $\mathbb{C}$ that is finitely generated over $\mathbb{Q}$. Suppose that A and A' are abelian varieties that are defined over K. If $A[n] \subset A(K)$ and $A'[n] \subset A'(K)$ then all homomorphisms from A to A' are defined over K.*

Proof. Since the group $\mathrm{Hom}(A, A')$ is finitely generated, there is a finite Galois field extension L/K (with $L \subset \bar{K}$) such that all homomorphisms from A to A' are defined over L. It follows that

$$f(A(L)) \subset A'(L), \quad \forall f \in \mathrm{Hom}(A, A').$$

Let $G = \mathrm{Gal}(L/K)$ be the (finite) Galois group of L/K. Then, there is a natural group homomorphism

$$G \to \mathrm{Aut}(\mathrm{Hom}(A, A')), \quad \sigma \mapsto \{f \mapsto \sigma(f)\}. \tag{2.12}$$

It is defined as follows: for any $\sigma \in \mathrm{Gal}(K)$, whose image in $\mathrm{Gal}(L/K) = G$ is σ,

$$\sigma(f) = {}^{\sigma} f$$

(since f is defined over L, $g(f)$ does *not* depend on the choice of σ). We have

$$g(f)(g(x)) = g(f(x)), \quad \forall x \in A(L).$$

In particular,

$$\sigma(f)(x) = f(x), \quad \forall x \in A[n] \subset A(K) = A(L)^G.$$

It follows from Claim 2.7 that

$$\sigma(f) - f \in n \cdot \mathrm{Hom}(A, A') \; \forall \sigma \in G, f \in \mathrm{Hom}(A, A'). \tag{2.13}$$

Let $\tilde{G} \subset \mathrm{Aut}(\mathrm{Hom}(A, A'))$ be the image of G under the homomorphism (2.12). Since G is finite, its image $\tilde{G}$ is also a finite group. It follows from (2.13) that every

$$\tilde{\sigma} \in \tilde{G} \subset \mathrm{Aut}(\mathrm{Hom}(A, A'))$$

is congruent to the identity automorphism of the group $\mathrm{Hom}(A, A')$ modulo n. Since $n \geq 3$ and $\mathrm{Hom}(A, A')$ is a free abelian group of finite rank, it follows from Minkowski Lemma that $\tilde{G}$ boils down to the identity map. This means that

$$\sigma(f) = f, \quad \forall \sigma \in G = \mathrm{Gal}(L/K), f \in \mathrm{Hom}(A, A'),$$

which, in turn, means that all the f are defined over K. □

Remark 2.11. Suppose that $\dim(A) > 0$ and $n > 1$. It what follows, we identify $\mathrm{End}(A)/n$ with its (isomorphic) image in $\mathrm{End}_{\mathbb{Z}/n}(A[n]$. It is not necessarily true that all elements of $\mathrm{End}(A)/n$ are endomorphisms of the Galois module $A[n]$, because we do not assume that all endomorphisms of A are defined over K. However, we know that all of them are defined over $\bar{K}$. for all $f \in \mathrm{End}(A)$ It follows from (1.17) and (1.19) that, for any $\sigma \in \mathrm{Gal}(K)$,

$$\rho_{n,A,K}(\sigma)\mathrm{End}(A)/n\rho_{n,A,K}(\sigma)^{-1} \subset \mathrm{End}(A)/n. \tag{2.14}$$

This implies

$$\rho_{n,A,K}(f + n \cdot \mathrm{End}(A)) =^{\sigma} f + n \cdot \mathrm{End}(A).$$

We will mainly be interested in the case when $n = \ell$ is a prime number, i.e., when $\mathbb{Z}/n = \mathbb{F}_\ell$ is a field.

2.2 Very Simple Linear Representations and Endomorphisms of Abelian Varieties

Property (2.14) inspires the following definition, see [183, Defn. 1.1].

Definition 2.1. Let $\mathcal{V} \neq \{0\}$ be a vector space over a field k, let G be a group and $\rho : G \to \mathrm{Aut}_k(\mathcal{V})$ be a linear representation of G in $\mathcal{V}$. Suppose that $R \subset \mathrm{End}_k(\mathcal{V})$ is a k-subalgebra containing the identity operator $\mathrm{Id} : \mathcal{V} \to \mathcal{V}$. We say that R is G-normal (or just normal) if

$$\rho(s)R\rho(s)^{-1} \subset R, \quad \forall s \in G.$$

Remark 2.12. If R is a subalgebra of $\mathrm{End}_k(\mathcal{V})$ then both R and $\rho(s)R\rho(s)^{-1}$ have the same dimension over k. It follows that R is normal if and only if

$$\rho(s)R\rho(s)^{-1} = R, \quad \forall s \in G.$$

Examples 2.13.

1. Obviously, $\mathrm{End}_k(\mathcal{V})$ and $k\cdot\mathrm{Id}$ are normal subalgebras. We call them *obvious normal subalgebras.*
2. Let A be an abelian variety of positive dimension that is defined over a field K. Let ℓ be a prime number, $\mathcal{V} = A[\ell]$, $G = \mathrm{Gal}(K)$, $\rho = \rho_{A,\ell,K}$. It follows from (2.14) that $\mathrm{End}(A)/\ell$ is a normal subalgebra of $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$.

The following definition was introduced in [180] (see also [183]).

Definition 2.2. Let $\mathcal{V} \neq \{0\}$ be a vector space over a field k, let G be a group and $\rho : G \to \mathrm{Aut}_k(\mathcal{V})$ be a linear representation of G in $\mathcal{V}$. We say that the G-module $\mathcal{V}$ is *very simple* if every normal subalgebra of $\mathrm{End}_k(\mathcal{V})$ is obvious.

Remark 2.14. Very simple modules enjoy the following properties [180, 183]:

(0) Let $\rho(G) \subset \mathrm{Aut}_k(\mathcal{V})$ be the image of ρ. Then, the G-module $\mathcal{V}$ is very simple if the $\rho(G)$-module $\mathcal{V}$ is very simple (because a subalgebra of $\mathrm{End}_k(\mathcal{V})$ is G-normal if and if it is $\rho(G)$-normal).

(1) If $\dim_k(\mathcal{V}) = 1$, then the G-module $\mathcal{V}$ is very simple (because in this case any subalgebra of $\mathrm{End}_k(\mathcal{V})$ coincides with $\mathrm{End}_k(\mathcal{V}) = k \cdot \mathrm{Id}$).

(2) Let $k[G]$ be the group k-algebra of G. Then, every very simple G-module $\mathcal{V}$ is absolutely simple, i.e., the k-algebra homomorphism $k[G] \to \mathrm{End}_k(\mathcal{V})$ induced by ρ is surjective. (It follows follows readily from the G-normality of the image of $k[G] \to \mathrm{End}_k(\mathcal{V})$.

(3) Let G' be a subgroup of G such that the G'-module $\mathcal{V}$ is very simple. Then, the G-module V is also very simple (because every G-normal algebra of $\mathrm{End}_k(V)$ is also G'-normal).

(4) If the G-module $\mathcal{V}$ is very simple, $\dim_k(\mathcal{V}) > 1$, and G' is a *non-central* normal subgroup of G, then the G'-module $\mathcal{V}$ is absolutely simple. In particular, G' is *non-abelian*.

(5) If $k = \mathbb{F}_2$ and $\dim_k(\mathcal{V}) = 2$, then every G-module $\mathcal{V}$ is *not* very simple.

The following assertion was proven in [183, Th. 6.4] for $\ell = 2$.

Theorem 2.15. *Let A be an abelian variety of positive dimension defined over a field K. Let ℓ be a prime,*

$$k = \mathbb{F}_\ell,\ \mathcal{V} = A[\ell],\ G = \mathrm{Gal}(K),\ \rho = \rho_{A,\ell,K}.$$

If the G-module $A[\ell]$ is very simple, then $\mathrm{End}(A) = \mathbb{Z}$. In particular, A is a simple abelian variety.

Proof. Combining Example 2.13 with the definition of very simplicity, we conclude that $\mathrm{End}(A)/\ell$ is either $\mathbb{F}_\ell \cdot \mathrm{Id}$, or $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$. This implies that the $\mathbb{F}_\ell$-dimension of $\mathrm{End}(A)/\ell$ is either 1, or $4\dim(A)^2$. Since $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module, its rank is either 1 or $4\dim(A)^2$. In the former case, $\mathrm{End}(A) = \mathbb{Z}$ and we are done. In the latter case, the rank of $\mathrm{End}(A)$ is strictly greater than $2\dim(A)^2$, that contradicts Theorem 2.29 below. This ends the proof. □

Remark 2.16. Recall that $\dim_{\mathbb{F}_\ell}(A[\ell]) = 2\dim(A)$. In particular, if $\dim(A) = 1$ (i.e., A is an elliptic curve) then $\dim_{\mathbb{F}_\ell}(A[\ell]) = 2$. In light of Remark 2.14(5), the conditions of Theorem 2.15 are *not* fulfilled if $\dim(A) = 1$ and $\ell = 2$.

We will use this theorem for $\ell = 2$ in Chapter 10, in order to give an explicit construction of hyperelliptic jacobians without nontrivial endomorphisms. This would require an analysis of the following class of representations naturally related to permutation groups, see [183]. We discuss this topic in the next section.

Let ℓ be an odd prime and δ be an automorphism of a positive-dimensional abelian variety $A = V/\Lambda$ that satisfies the ℓth cyclotomic equation

$$\Phi_\ell(\delta) = \sum_{j=0}^{\ell-1} \delta^j = 0$$

in $\mathrm{End}(A)$. Clearly δ^ℓ is the identity automorphism of A and the subgroup of fixed points of δ

$$A^\delta = \{x \in A \mid \delta(x) = x\}$$

is contained in $A[\ell]$, and therefore, may be viewed as a finite-dimensional $\mathbb{F}_\ell$-vector space. In order to find its dimension, notice that the subring $\mathbb{Z}[\delta]$ of $\mathrm{End}(A)$ is isomorphic to the ℓth cyclotomic ring $\mathbb{Z}[\zeta_\ell]$ (a primitive ℓth root of unity ζ_ℓ goes to δ). Indeed, recall that the ℓth cyclotomic polynomial

$$\Phi_\ell(t) = \sum_{j=0}^{\ell-1} \in \mathbb{Z}[t] \subset \mathbb{Q}[t]$$

is irreducible over $\mathbb{Q}$ and the ring $\mathbb{Z}[\zeta_\ell]$ is isomorphic to the quotient $\mathbb{Z}[t]/(\Phi_\ell(t))$ of the polynomial ring $\mathbb{Z}[t]$ by the ideal generated by $\Phi_\ell(t)$ where under this isomorphism the coset of x goes to ζ_ℓ. (The latter assertion follows from the fact that $\{1, \zeta_\ell, \dots \zeta_\ell^{\ell-2}\}$ is a basis of the free $\mathbb{Z}$-module $\mathbb{Z}[\zeta_\ell]$ of rank $\ell - 1$.) Let us consider the surjective ring homomorphism

$$\mathbb{Z}[t]/(\Phi_\ell(t)) \to \mathbb{Z}[\delta],\ P(t) + \Phi_\ell(t)\mathbb{Z}[t] \mapsto P(\delta) \in \mathbb{Z}[\delta]\ \forall P(t) \in \mathbb{Z}[t]. \tag{2.15}$$

Suppose that the map (2.15) is *not* injective. This means that there is a polynomial $\mathcal{P}(t) \in \mathbb{Z}[t]$ *not* divisible by $(\Phi_\ell(t)$ such that $\mathcal{P}(\delta) = 0$. Replacing $\mathcal{P}(t)$ by its remainder with respect to division by the (monic) $\Phi_\ell(t)$, we may and will assume that $\deg(\mathcal{P}) < \ell - 1$. Since $\Phi_\ell(t)$ is irreducible over $\mathbb{Q}$ and

$$\deg(\Phi_\ell) = \ell - 1 > \deg(\mathcal{P}),$$

the polynomials $\mathcal{P}(t)$ and $\Phi_\ell(t)$ have no common roots, i.e., their *resultant* $D \neq 0$. Since both $\mathcal{P}(t)$ and $\Phi_\ell(t)$ have integer coefficients, there are polynomials $h(t), s(t) \in \mathbb{Z}[t]$ such that

$$D = h(t)\Phi_\ell(t) + s(t)\mathcal{P}(t).$$

This implies that $D \in \mathbb{Z}$, and in the ring $\mathbb{Z}[\delta]$,

$$D = h(\delta)\Phi_\ell(\delta) + s(\delta)\mathcal{P}(\delta) = h(\delta) \cdot 0 + s(\delta) \cdot 0 = 0,$$

i.e., the multiplication by D in A is the zero map, which is absurd. The obtained contradiction proves that the map (2.15) is injective, and therefore, is a ring isomorphism. It follows that the composition of ring isomorphisms

$$\mathbb{Z}[\zeta_\ell] \to \mathbb{Z}[t]/(\Phi_\ell(t)) \to \mathbb{Z}[\delta],\ \sum_{j=0}^{\ell-2} c_i\zeta_\ell^j \mapsto \left(\sum_{j=0}^{\ell-2} c_j t^j\right) + \Phi_\ell(t)\mathbb{Z}[t] \mapsto \sum_{j=0}^{\ell-2} c_i\delta_\ell^j \tag{2.16}$$

is also a *ring isomorphism*. Thus, the ring $\mathbb{Z}[\delta]$ is a Dedekind ring, and there is an isomorphism:

$$\mathbb{Z}[\delta]/(1-\delta) \cong \mathbb{Z}[\zeta_\ell]/(1-\zeta_\ell) = \mathbb{F}_\ell.$$

In addition, the $\mathbb{Q}$-subalgebra

$$\mathbb{Q}[\delta] := \mathbb{Z}[\delta] \otimes \mathbb{Q} \subset \mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q}$$

is isomorphic to the ℓth cyclotomic field $\mathbb{Q}(\zeta_\ell)$ (as above ζ_ℓ goes to δ). Since Λ is a free $\mathbb{Z}$-module of finite rank, the corresponding $\mathbb{Z}[\delta]$-module Λ is torsion-free and finitely generated. Since the ring $\mathbb{Z}[\zeta_\ell]$ is Dedekind, Λ is a direct sum $\oplus_{j=1}^r P_j$ of r *invertible* (i.e., rank 1 locally free) $\mathbb{Z}[\delta]$-modules,

for some positive integer r. The $\mathbb{Z}$-rank arguments imply that $2\dim(A) = r(\ell-1)$. Thus, since $\mathbb{Z}[\zeta_\ell]$ is a free $\mathbb{Z}$-module of rank $\ell-1$,

$$r = \frac{2\dim(A)}{\ell-1},$$

and, therefore,

$$A^\delta = (1-\delta)^{-1}\Lambda/\Lambda \cong \Lambda/(1-\delta)\Lambda \cong \mathbb{Z}[\zeta_\ell]^r/(1-\zeta_\ell)\mathbb{Z}[\zeta_\ell]^r = \mathbb{F}_\ell^r.$$

This implies that

$$\dim_{\mathbb{F}_\ell}(A^\delta) = r = \frac{2\dim(A)}{\ell-1}.$$

Since $\Lambda = \oplus_{j=1}^r P_j$, its endomorphism ring $\mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda)$ is a $\mathbb{Z}[\delta]$-algebra that (if viewed as the $\mathbb{Z}[\delta]$-module) is a direct sum $\oplus_{i,j=1}^r \mathrm{Hom}(P_i, P_j)$ of r^2 invertible $\mathbb{Z}[\delta]$-modules $\mathrm{Hom}(P_i, P_j)$. In particular, $\mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda)$ is a free $\mathbb{Z}$-module of rank $r^2(\ell-1)$.

Let $\mathrm{End}_\delta(A)$ be the centralizer of δ in $\mathrm{End}(A)$. It is a subring of $\mathrm{End}(A)$, and the center of $\mathrm{End}_\delta(A)$ contains $\mathbb{Z}[\delta]$. So, one may view $\mathrm{End}(A)$ as a $\mathbb{Z}[\delta]$-algebra. As above, $\mathrm{End}_\delta(A)$ is a direct sum of d projective $\mathbb{Z}[\delta]$-modules of rank 1 for some positive integer d. The rational representation of elements of $\mathrm{End}_\delta(A)$ gives us the ring embedding $\mathrm{End}_\delta(A) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda)$.Its image lies in $\mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda)$, which gives us an embedding of $\mathbb{Z}[\delta]$-algebras

$$\iota_r : \mathrm{End}_\delta(A) \hookrightarrow \mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda),\ f \mapsto f_r. \tag{2.17}$$

Remark 2.17. Comparing the ranks in (2.17), we obtain the inequality $d \le r^2$. What will happen if the equality holds? It follows immediately that there is a positive integer N such that

$$N \cdot \mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda) \subset \iota_r(\mathrm{End}_\delta(A)).$$

We claim that in this case the embedding (2.17) is bijective (and an isomorphism of $\mathbb{Z}[\delta]$-algebras), i.e.,

$$\iota_r(\mathrm{End}_\delta(A)) = \mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda). \tag{2.18}$$

In the course of the proof, it is convenient to identify (via the rational representation) $\mathrm{End}(A)$ with its image in $\mathrm{End}_{\mathbb{Z}}(\Lambda)$ and consider ι_r as the *inclusion map*. Let $u \in \mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda)$. Then, $Nu \in \mathrm{End}_\delta(A))$. This implies that, if we extend $Nu : \Lambda \to \Lambda$ by $\mathbb{R}$-linearity to the $\mathbb{R}$-linear map

$$(Nu)_{\mathbb{R}} : V = \Lambda \otimes \mathbb{R} \to \Lambda \otimes \mathbb{R} = V,$$

then $u_{\mathbb{R}}$ is a $\mathbb{C}$-linear self-map of V. Thus, $\frac{1}{N}(Nu)_{\mathbb{R}}$ is also a $\mathbb{C}$-linear self-map of V. Taking into account that the restriction of $\frac{1}{N}(Nu)_{\mathbb{R}}$ to Λ coincides with u and, in particular, sends Λ to Λ, we conclude that $u \in \mathrm{End}(A)$. Since Nu commutes with δ in $\mathrm{End}(A)$, we conclude that

$$N(u\delta - \delta u) = (Nu)\delta - \delta(Nu) = 0$$

in $\mathrm{End}(A)$. Therefore, the image $(u\delta - \delta u)(A)$ lies in the finite set $A[N]$. Since $\dim(A) > 1$, $u\delta - \delta u$ is a constant map. Since this map sends the zero of A into itself, i.e.,

$$u\delta - \delta u = 0 \in \mathrm{End}(A),$$

we obtain that $u \in \mathrm{End}_\delta(A)$.

Let K be a finitely generated subfield of $\mathbb{C}$ such that A and its endomorphism δ are defined over K. It follows that

$$A^\delta \subset A[\ell] \subset A(\bar{K}),$$

and A^δ is a $\mathrm{Gal}(K)$-invariant $\mathbb{F}_\ell$-vector subspace of $A[\ell]$. The following assertion may be viewed as a natural extension of Theorem 2.15.

Theorem 2.18. *Let* $\mathrm{End}(A)_\delta$ *be the centralizer of* $\delta \in \mathrm{End}(A)$ *and*

$$\mathrm{End}_{\mathbb{Q}}(A)_\delta = \mathrm{End}(A)_\delta \otimes \mathbb{Q} \subset \mathrm{End}_{\mathbb{Q}}(A)$$

be the corresponding $\mathbb{Q}$*-subalgebra of* $\mathrm{End}_{\mathbb{Q}}(A)$*. Suppose that the* $\mathrm{Gal}(K)$*-module* A^δ *is very simple. Then, either* $\mathrm{End}(A)_\delta = \mathbb{Z}[\delta]$*, or* $\mathrm{End}_{\mathbb{Q}}(A)_\delta$ *is isomorphic to the matrix algebra of size* r *over the field* $\mathbb{Q}[\delta]$*. In the latter case,* A *is isogenous to a self-product* B^r *of a* $(ell-1)/2$*-dimensional abelian variety* B *with* $\mathrm{End}_{\mathbb{Q}}(B) \cong \mathbb{Q}(\zeta_\ell)$*.*

Proof. First, notice that $\mathrm{End}_\delta(A)$ is a torsion free finitely generated $\mathbb{Z}[\delta]$-algebra, hence, is a projective $\mathbb{Z}[\delta]$-module of finite rank, say d. Hence, the quotient $\mathrm{End}_\delta(A)/(1-\delta)\mathrm{End}_\delta(A)$ is a d-dimensional $\mathbb{Z}[\delta]/(1-\delta) = \mathbb{F}_\ell$-algebra.

Lemma 2.19. *Let* $u \in \mathrm{End}(A)_\delta \subset \mathrm{End}(A)$*. Then:*

(i) $u(A^\delta) \subset A^\delta$;

(ii) $u(A^\delta) = \{0\}$ *if and only if* $u \in (1-\delta)\mathrm{End}_(A)_\delta$.

□

End of Proof of Theorem 2.18 (modulo Lemma 2.19). It follows from Lemma 2.19 that the action of $\mathrm{End}_\delta(A)$ on A^δ induces the $\mathbb{F}_\ell$-algebra embedding

$$\mathrm{End}_\delta(A)/(1-\delta)\mathrm{End}_\delta(A) \hookrightarrow \mathrm{End}_{\mathbb{F}_\ell}(A^\delta),\ u+(1-\delta)\mathrm{End}_\delta(A) \mapsto \{x \mapsto u(x)\ \forall x \in A^\delta\}. \quad (2.19)$$

Since A and δ are defined over K, the image R of the embedding (2.19) is a normal $\mathrm{Gal}(K)$-subalgebra of $\mathrm{End}_{\mathbb{F}_\ell}(A^\delta)$. Hence,

$$\dim_{\mathbb{F}_\ell}(R) = \dim_{\mathbb{F}_\ell}(\mathrm{End}_\delta(A)/(1-\delta)\mathrm{End}_\delta(A)) = d.$$

Since the Galois module A^δ is very simple, either $d = 1$ or

$$d = \dim_{\mathbb{F}_\ell}(\mathrm{End}_{\mathbb{F}_\ell}(A^\delta) = \left(\dim_{\mathbb{F}_\ell}(A^\delta\right)^2 = r^2.$$

If $d = 1$, $\mathrm{End}_\delta(A)$ is a projective $\mathbb{Z}[\delta]$-module of rank 1, which implies easily that

$$\mathbb{Z}[\delta] \subset \mathrm{End}_\delta(A) \subset \mathbb{Z}[\delta] \otimes \mathbb{Q};$$

the latter is isomorphic to the ℓth cyclotomic field $\mathbb{Q}(\zeta_\ell)$. Since $\mathrm{End}_\delta(A)$ is a free $\mathbb{Z}$-module of finite rank, it is integral over $\mathbb{Z}[\delta]$. Taking into account that $\mathbb{Z}[\delta] = \mathbb{Z}[\zeta_\ell]$ is integrally closed, we conclude that $\mathbb{Z}[\delta] = \mathrm{End}_\delta(A)$ and we are done.

Let us assume that $d = r^2$. By Remark 2.17,

$$\mathrm{End}_\delta(A) = \mathrm{End}_{\mathbb{Z}[\delta]}(\Lambda).$$

Proof of Lemma 2.19. (i) is obvious. Notice that *if* part in (ii) is obvious. In order to prove the *only if*, part recall that there is $\lambda \in \mathbb{Z}[\zeta_\ell]$ such that $\lambda(1-\zeta_\ell) = \ell$. This shows the existence of $v \in \mathbb{Z}[\delta]$ such that $v(1-\delta) = (1-\delta)v = \ell$ in $\mathrm{End}_\delta(A)$. This implies that

$$v(A[\ell]) \subset A^\delta.$$

It follows that $u(A^\delta) = \{0\}$, hence $uv(A[\ell]) = \{0\}$ and, therefore, there is $w \in \mathrm{End}(A)$ such that

$$vu = uv = \ell w = v(1-\delta)w$$

and, hence, $u = (1-\delta)w$. Clearly, $w \in \mathrm{End}_\delta(A)$.

□

2.3 Permutational Representations

Let ℓ be a prime number and $\mathbb{F}_\ell$ be the finite field of ℓ elements. Let $n \geq 3$ be a positive integer that is not divisible by ℓ, and $\mathfrak{R}$ be a set of cardinality n. We write $\mathrm{Perm}(\mathfrak{R})$ for the group of all permutations of $\mathfrak{R}$ and $\mathrm{Alt}(\mathfrak{R})$ for its unique subgroup of index 2. A choice of ordering on $\mathfrak{R}$ defines a group isomorphism $\mathrm{Perm}(\mathfrak{R}) \cong \mathfrak{S}_n$; the image of $\mathrm{Alt}(\mathfrak{R})$ under this isomorphism coincides with the *alternating group* $\mathfrak{A}_n$. Sometimes, slightly abusing notation, we denote $\mathrm{Perm}(\mathfrak{R})$ by $\mathfrak{S}_n$ and $\mathrm{Alt}(\mathfrak{R})$ by $\mathfrak{A}_n$. Let $\mathbb{F}_\ell^{\mathfrak{R}}$ be the n-dimensional $\mathbb{F}_\ell$-vector space of $\mathbb{F}_\ell$-valued functions $\phi : \mathfrak{R} \to \mathbb{F}_\ell$. The vector space $\mathbb{F}_\ell^{\mathfrak{R}}$ is provided with the natural action of $\mathrm{Perm}(\mathfrak{R})$ that is defined as follows. Each permutation $s \in \mathrm{Perm}(\mathfrak{R})$ sends a function $\phi : \mathfrak{R} \to \mathbb{F}_\ell$ to the function

$$s(\phi) : b \mapsto \phi(s^{-1}(b), b \in \mathfrak{R}.$$

This action provides $\mathbb{F}_\ell^{\mathfrak{R}}$ with the structure of a faithful $\mathrm{Perm}(\mathfrak{R})$-module. The *permutation module* $\mathbb{F}_\ell^{\mathfrak{R}}$ contains the $\mathrm{Perm}(\mathfrak{R})$-invariant $(n-1)$-dimensional hyperplane

$$\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0 = \{\phi : \mathfrak{R} \to \mathbb{F}_\ell \mid \sum_{b \in \mathfrak{R}} \phi(b) = 0\} \tag{2.20}$$

and the $\mathrm{Perm}(\mathfrak{R})$-invariant line $\mathbb{F}_\ell \cdot \mathbf{1}_{\mathfrak{R}}$ where $\mathbf{1}_{\mathfrak{R}}$ is the *constant* function 1. Since $n = \#(\mathfrak{R})$ is *not* divisible by ℓ, these subspaces meet each other only at 0. This implies that the *permutation module* $\mathbb{F}_\ell^{\mathfrak{R}}$ splits into a direct sum

$$\mathbb{F}_\ell^{\mathfrak{R}} = \left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0 \oplus \mathbb{F}_\ell \cdot \mathbf{1}_{\mathfrak{R}}. \tag{2.21}$$

Since $\mathrm{Perm}(\mathfrak{R})$ acts faithfully on $\mathbb{F}_\ell^{\mathfrak{R}}$ and identically on $\mathbb{F}_\ell \cdot \mathbf{1}_{\mathfrak{R}}$, it follows from the splitting (2.21) that the $\mathrm{Perm}(\mathfrak{R})$-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is *faithful*. It is well known [124] that the $\mathrm{Perm}(\mathfrak{R})$-module (and even the $\mathrm{Alt}(\mathfrak{R})$-module) $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is *absolutely simple* if $n \geq 5$.[1]

Let $G \subset \mathrm{Perm}(\mathfrak{R})$ be a permutation group of $\mathfrak{R}$. Then, $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ carries the natural structure of a faithful G-module. It is reasonable to ask when this module is very simple? This question was studied in ([180], [179, Sect. 4], [183, Th. 5.5 and 5.7], [193, Th. 4.7]). Let us quote some of the results that were obtained there.

[1] Absolutely simple means that, after any extension of scalars, the module does not have any non-trivial invariant subspaces.

Lemma 2.20. *Suppose that $\ell = 2$ and the G-module $\left(\mathbb{F}_2^{\mathfrak{R}}\right)^0$ is very simple. Then, $n = \#(\mathfrak{R}) \geq 5$ and G is a doubly transitive permutation group.*

Theorem 2.21. *Suppose that $n \geq 5$ and $G = \mathfrak{S}_n$ or $\mathfrak{A}_n$. Then, the G-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is very simple for all prime ℓ except the case where $n = 5$ and $\ell \equiv \pm 1 \bmod 5$.*

Remark 2.22. In light of Remark 2.14(3), the very simplicity of the $\mathfrak{S}_n$-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ follows readily from the very simplicity of the $\mathfrak{A}_n$-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$

Remark 2.23. We will use the case $\ell = 2$ of Theorem 2.21 in Chapter 10 and Section 8.3, in order to construct jacobians without nontrivial endomorphisms.

Proof of Theorem 2.21. Using Remark 2.22, it suffices to check the case $G = \mathfrak{A}_n = \mathrm{Alt}(\mathfrak{R})$. We have already seen that the faithful $G = \mathrm{Alt}(\mathfrak{R})$-module $\mathcal{V} = \left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is absolutely simple.

Let $R \subset \mathrm{End}_{\mathbb{F}_\ell}(\mathcal{V})$ be a G-normal subalgebra. Clearly, $\mathcal{V}$ is a faithful R-module.

Step 1. $\mathcal{V}$ is a *semisimple* R-module. Indeed, let $U \subset V$ be a simple R-submodule. Then $U' = \sum_{s \in G} sU$ is a non-zero G-stable subspace in $\mathcal{V}$ and therefore must coincide with $\mathcal{V}$. On the other hand, each sU is also a R-submodule in $\mathcal{V}$, because $s^{-1}Rs = R$. Moreover, since

$$Rs^{-1}W = s^{-1}sRs^{-1}W = s^{-1}RW = s^{-1}W,$$

if $W \subset sU$ is an R-submodule, then $s^{-1}W$ is an R-submodule in U, because

Since U is simple, $s^{-1}W = \{0\}$ or U. This implies that sU is also simple. Hence $V = U'$ is a sum of simple R-modules and therefore is a semisimple R-module.

Step 2. The R-module $\mathcal{V}$ is *isotypic*. Indeed, let us split the semisimple R-module V into the direct sum

$$\mathcal{V} = \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_r$$

of its isotypic components. Dimension arguments imply that $r \leq \dim(\mathcal{V}) = n - 1$. It follows easily from the arguments of the previous step that for each isotypic component $\mathcal{V}_i$, for each $s \in G$, its image $s\mathcal{V}_i$ is an isotypic R-submodule. Therefore, it is contained in some $\mathcal{V}_j$. Similarly, $s^{-1}\mathcal{V}_j$ is an isotypic submodule obviously containing $\mathcal{V}_i$. Since $\mathcal{V}_i$ is the isotypic component, $s^{-1}\mathcal{V}_j = \mathcal{V}_i$, and therefore, $s\mathcal{V}_i = \mathcal{V}_j$. This means that s permutes the $\mathcal{V}_i$; since $\mathcal{V}$ is simple G-module, G permutes them transitively. This gives rise to the homomorphism $G \to \mathbf{S}_r$. Since G is a simple group, whose order ($= n!/2$) is greater than $(n-1)! \geq r! =$ order of $\mathbf{S}_r$, this homomorphism must be trivial. This means that $s\mathcal{V}_i = \mathcal{V}_i$ for all $s \in G$, and $\mathcal{V} = \mathcal{V}_i$ is isotypic.

Step 3. Since $\mathcal{V}$ is isotypic, there exist a simple R-module W and a positive integer d such that the R-modules $\mathcal{V}$ and W^d are isomorphic. It follows that

$$d \cdot \dim(W) = \dim(\mathcal{V}) = n - 1$$

and the centralizer $\mathrm{End}_R(\mathcal{V})$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathrm{End}_R(W))$ of size d over $\mathrm{End}_R(W)$.

Let us put

$$F = \mathrm{End}_R(W).$$

Since W is simple, F is a finite division algebra of characteristic ℓ. Therefore F is a finite field of characteristic ℓ and $[F : \mathbb{F}_\ell]$ divides $n-1$. We have $\mathrm{End}_R(V) \cong \mathrm{Mat}_d(F)$. Clearly, $\mathrm{End}_R(V) \subset \mathrm{End}_{\mathbb{F}_\ell}(\mathcal{V})$ is stable under the adjoint action of $\mathfrak{A}_n$. This induces a group homomorphism

$$\alpha : \mathfrak{A}_n \to \mathrm{Aut}(\mathrm{End}_R(\mathcal{V})) = \mathrm{Aut}(\mathrm{Mat}_d(F)).$$

Since F is the center of $\mathrm{Mat}_d(F)$, it is stable under the action of $\mathfrak{A}_n$, i.e., we get a homomorphism $\mathfrak{A}_n \to \mathrm{Aut}(F)$, which must be trivial, since $\mathfrak{A}_n$ is a simple non-abelian group, and $\mathrm{Aut}(F) = \mathrm{Gal}(F/\mathbb{F}_\ell)$ is abelian. This implies that the center F of $\mathrm{End}_R(\mathcal{V})$ commutes with $\mathfrak{A}_n$. Since $\mathrm{End}_G(\mathcal{V}) = \mathbb{F}_\ell$ (recall that the $\mathfrak{A}_n$-module $\mathcal{V}$ is absolutely simple), we have $k = \mathbb{F}_\ell$. This implies that $\mathrm{End}_R(\mathcal{V}) \cong \mathrm{Mat}_d(\mathbb{F}_\ell)$, and

$$\alpha : \mathfrak{A}_n \to \mathrm{Aut}(\mathrm{End}_R(\mathcal{V})) = (\mathrm{End}_R(\mathcal{V}))^*/\mathbb{F}_\ell^* \cong \mathrm{GL}(d, \mathbb{F}_\ell)/\mathbb{F}_\ell^* = \mathrm{PGL}(d, \mathbb{F}_\ell)$$

is trivial if and only if $\mathrm{End}_R(\mathcal{V}) \subset \mathrm{End}_{\mathfrak{A}_n}(V) = \mathbb{F}_\ell \cdot \mathrm{Id}$. Since $\mathrm{End}_R(\mathcal{V}) \cong \mathrm{Mat}_d(\mathbb{F}_\ell)$, α is trivial if and only if $d = 1$, i.e. $\mathcal{V}$ is an absolutely simple R-module. It follows from the Jacobson density theorem (see [18, §5] or [101, Chapter 4,§11]) that $R \cong \mathrm{Mat}_m(\mathbb{F}_\ell)$ with $dm = n-1$. This implies that α is trivial if and only if $R \cong \mathrm{Mat}_{n-1}(\mathbb{F}_\ell)$, i.e., $R = \mathrm{End}(\mathcal{V})$.

The adjoint action of $\mathfrak{A}_n$ on R gives rise to a homomorphism

$$\beta : \mathfrak{A}_n \to \mathrm{Aut}(R) = R^*/\mathbb{F}_\ell^* \cong \mathrm{PGL}(m, \mathbb{F}_\ell).$$

Clearly, β is trivial if and only if R commutes with $\mathfrak{A}_n$, i.e., $R = \mathbb{F}_\ell \cdot \mathrm{Id}$. This implies that we are done if either α, or β is trivial.

Step 4. Recall that $md = n-1$. Let us put

$$c := \min(d, m).$$

Then

$$c^2 \le n-1$$

and either $c = d$, or $c = m$. Thus, it suffices to check that every group homomorphism $\mathfrak{A}_n \to \mathrm{PGL}(c, \mathbb{F}_\ell)$ is trivial. Let us consider the following cases:

(0) If $c = 1$ then the group $\mathrm{PGL}(1, \mathbb{F}_\ell)$ is the one-element group, hence every homomorphism to $\mathrm{PGL}(1, \mathbb{F}_\ell)$ is trivial, and we are done.

(i) If $(n-1)$ is a *prime* number, then $c = 1$ and, in light of case (i), we are done. So, in what follows, we may and will assume that $c > 1$ (i.e., both $m, d > 1$) and $n-1$ is *not* prime. In particular, $n \ne 6, 8$.

(ii) Suppose that

$$\frac{\ell^{n-1}}{\ell - 1} < \frac{n!}{2}.$$

Since $c^2 \le n-1$, the order of $\mathrm{PGL}(c, \mathbb{F}_\ell))$ is strictly less than the ratio

$$\frac{\ell^{c^2}}{\ell - 1} \le \frac{\ell^{n-1}}{\ell - 1} < \frac{n!}{2}.$$

Since the order of $\mathfrak{A}_n$ is $n!/2$, every homomorphism from $\mathfrak{A}_n$ to $\mathrm{PGL}(c, \mathbb{F}_\ell)$ is trivial, so we are done.

(iii) Suppose that $\ell \in \{2, 3\}$. We claim that in this case

$$\frac{\ell^{N-1}}{\ell - 1} < \frac{N!}{2}$$

for all integers $N \geq 5$. Indeed, after we replace N by $N + 1$, the left-hand side of the desired inequality is multiplied by $\ell < 5 < N$, while the right-hand side is multiplied by $N > \ell$. Hence, it suffices to check the validity of the inequality for $N = 5$ and $\ell = 2, 3$. In this case, we get

$$\frac{\ell^{5-1}}{\ell - 1} = \frac{\ell^4}{\ell - 1} < 60 = \frac{5!}{2},$$

that proves the desired inequality. In light of case (ii), we are done if $\ell \in \{2, 3\}$.

It follows from Case (iii), that we may assume that $\ell \geq 5$.

(iv) Suppose that $n \geq 9$. Then,

$$c - 1 \leq [\sqrt{n-1}] - 1 < [n/3].$$

Let

$$\gamma : \mathfrak{A}_n \to \mathrm{PGL}_c(\mathbb{F}_\ell)$$

be a group homomorphism. We need to prove that γ is trivial. Let $\bar{\mathbb{F}}_\ell$ be the algebraic closure of $\mathbb{F}_\ell$. Since $\mathrm{PGL}(c, \mathbb{F}_\ell) \subset \mathrm{PGL}_(\bar{\mathbb{F}}_\ell)$, it suffices to check that the composition

$$\mathfrak{A}_n \to \mathrm{PGL}(c, \mathbb{F}_\ell) \subset \mathrm{PGL}(c, \bar{\mathbb{F}}_\ell),$$

which we continue denote by γ, is trivial.

Let

$$\pi : \widetilde{\mathfrak{A}}_n \twoheadrightarrow \mathfrak{A}_n$$

be the universal central extension of the perfect group $\mathfrak{A}_n$. It is well known that, for $n \geq 5$, $\widetilde{\mathrm{A}}_n$ is also perfect and the kernel (the *Schur's multiplier*) of π is a cyclic group of order 2. One could *lift* γ to the group homomorphism

$$\gamma' : \widetilde{\mathfrak{A}}_n \to \mathrm{GL}(c, \bar{\mathbb{F}}_\ell).$$

Clearly, γ is trivial if and only if γ' is trivial. In order to prove the triviality of γ'. Let $r := [n/3]$, and notice that $\mathfrak{A}_n$ contains a subgroup D isomorphic to $(\mathbb{Z}/3\mathbb{Z})^r$ (generated by disjoint 3-cycles). Let D' be a Sylow 3-subgroup in $\pi^{-1}(D)$. Clearly, π maps D' isomorphically onto D. Therefore, D' is a subgroup of $\widetilde{\mathfrak{A}}_n$ that is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^m$. Now, let us discuss the image and the kernel of γ'.

First, since $\widetilde{\mathfrak{A}}_n$ is perfect, its image lies in $\mathrm{SL}(c, \bar{\mathbb{F}}_\ell)$, i.e., one may view γ' as a homomorphism from $\widetilde{\mathfrak{A}}_n$ to $\mathrm{SL}(c, \bar{\mathbb{F}}_\ell)$. Second, the only proper normal subgroup in $\widetilde{\mathfrak{A}}_n$ is the kernel of π. This implies that if γ' is nontrivial, then its kernel meets D' only at the identity element. Therefore, $\mathrm{SL}(c, \bar{\mathbb{F}}_\ell)$ contains the subgroup $\gamma'(D')$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^r$. Since $\ell > 3$, the subgroup

$\gamma'(D')$ is conjugate to an elementary 3-group of diagonal matrices in $\mathrm{SL}(c, \bar{\mathbb{F}}_\ell)$. This implies that

$$r \le c - 1.$$

Since $r = [n/3]$, we get a contradiction implying that our assumption of the nontriviality of γ' was wrong. Hence, γ' is trivial and therefore γ is also trivial.

By Case (iv), we may assume that $n \in \{5, 7\}$.

(v) Suppose that $n = 7$. Then, $\ell \neq 7$, and $n - 1 = 2 \times 3$. Since both integers 2 and 3 are prime, $c = 2$. Let $\gamma : \mathfrak{A}_7 \to \mathrm{PGL}(2, \mathbb{F}_\ell)$ be a nontrivial group homomorphism. Since $\mathfrak{A}_n$ is simple and perfect, γ is injective. Moreover, its image $H := \gamma(\mathfrak{A}_7)$ lies in $\mathrm{PSL}(2, \mathbb{F}_\ell)$ and is isomorphic to the group $\mathfrak{A}_7$ of order is $7!/2$. Suppose that $H = \mathrm{PSL}(2, \mathbb{F}_\ell)$. Since ℓ divides the order of $\mathrm{PSL}(2, \mathbb{F}_\ell)$, we conclude that $\ell \le 7$. This implies that $\ell = 5$, and therefore, the order of $\mathrm{PSL}(2, \mathbb{F}_\ell)$ is equal to $60 < 7!/2$. Recall that $7!/2$ is the order of H. Since H is a subgroup of $\mathrm{PSL}(2, \mathbb{F}_\ell)$, we get a contradiction. Thist implies that $H \neq \mathrm{PSL}(2, \mathbb{F}_\ell)$. It follows that H is a *proper* simple non-abelian subgroup of $\mathrm{PSL}(2, \mathbb{F}_\ell)$. It is known ([162, Theorems 6.25 and 6.26]) that each *proper* simple non-abelian subgroup of $\mathrm{PSL}(2, \mathbb{F}_\ell)$ is isomorphic to $\mathfrak{A}_5$; in particular, its order is equal to 60. However, the order of H is $\frac{7!}{2} \neq 60$. The obtained contradiction implies that if $n = 7$, then every homomorphism from $\mathfrak{A}_7$ to $\mathrm{PGL}(2, \mathbb{F}_\ell)$ is trivial, so we are done.

(vi) The only remaining case is $n = 5$. Since $n - 1 = 2 \times 2$ and 2 is a prime, $c = d = m = 2$. Since $\mathfrak{A}_5$ is simple perfect,

$$\alpha(\mathfrak{A}_5) \subset \mathrm{PSL}(2, \mathbb{F}_\ell),\ \beta(\mathfrak{A}_5) \subset \mathrm{PSL}(2, \mathbb{F}_\ell)$$

and we may view α and β as *injective group* homomorphisms from $\mathfrak{A}_5$ to $\mathrm{PSL}(2, \mathbb{F}_\ell)$. It follows that the order $(\ell^2 - 1)\ell/2$ of $\mathrm{PSL}(2, \mathbb{F}_\ell)$ is divisible by 60, which is the order of $\mathfrak{A}_5$. In particular, $(\ell^2 - 1)\ell/2$ is divisible by 5. Since the prime $\ell \neq 5$, we conclude that $\ell \equiv \pm 1 \bmod 5$. This ends the proof.

Remark 2.24.

1. It is known ([162, loc.cit.]) that, if $\ell \equiv \pm 1 \bmod 5$, then $\mathrm{PSL}(2, \mathbb{F}_\ell)$ contains a subgroup isomorphic to $\mathfrak{A}_5$.

2. If $\ell \equiv \pm 1 \bmod 5$, then the $\mathfrak{A}_5$-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is *not* very simple [193, Theorem 4.7]. (This *exceptional* case was overlooked in [179], see [193]).

3. The $\mathfrak{S}_5$-module $\left(\mathbb{F}_\ell^{\mathfrak{R}}\right)^0$ is very simple for all prime ℓ [193, Theorem 4.7].

2.4 The Rosati Involution

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 allows us to define the involutions of the rings

$\mathrm{End}_{\mathbb{C}}(V)$ (resp. $\mathrm{End}_{\mathbb{Q}}(\Lambda_{\mathbb{Q}})$) by taking the adjoint operator with respect to H_0 (resp. $\mathrm{Im}(H_0)$).[2] Using the representations ρ_a and ρ_r, we transfer this involution to the endomorphism algebra

$$\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes \mathbb{Q}$$

of A.

It is called the *Rosati involution* and, following classical notation, we denote it by $f \mapsto f'$. The Rosati involution can be defined as

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

If we view $\hat{A}$ as the Picard variety of A, then f^* is the usual pull-back map of isomorphism classes of holomorphic line bundles on A. Note that $\phi_{L_0}^{-1}$ is defined only after we tensor $\mathrm{End}(A)$ with $\mathbb{Q}$, so the Rosati involution is defined only on $\mathrm{End}_{\mathbb{Q}}(A)$. However, if L_0 is a principal polarization, then ϕ_{L_0} is an isomorphism, and the Rosati involution is an involution of $\mathrm{End}(A)$.

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

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

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 [106]). 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 $P_r(f) = P_a(f)^2$.

[2] 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 $T^* : V \to V$ such that $H(T(x), y) = H(x, T^*(y))$ for all $x, y \in V$.

Let $\mathrm{Pic}(A)$ be the group of isomorphism classes of holomorphic line bundles on a complex abelian variety A and $c_1 : \mathrm{Pic}(A) \to H^2(A, \mathbb{Z})$ be the Chern class homomorphism. Its image is denoted by $\mathrm{NS}(A)$ and is called the *Néron-Severi group*. By definition

$$\mathrm{NS}(A) \cong \mathrm{Pic}(A)/\mathrm{Pic}^0(A).$$

We define a homomorphism of abelian groups

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

It induces a homomorphism of linear spaces over $\mathbb{Q}$

$$\alpha_{\mathbb{Q}} : \mathrm{NS}(A)_{\mathbb{Q}} := \mathrm{NS}(A) \otimes \mathbb{Q} \to \mathrm{End}_{\mathbb{Q}}(A).$$

If $f \in \mathrm{End}(A)$ lies in $\alpha(\mathrm{NS}(A))$, then $\phi_L = \phi_{L_0} \circ f$ for some $L_0 \in \mathrm{NS}(A)$. This means that $H_0(f_a(z), z') = H(z, z')$ for some Hermitian form H such that

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

Since $H(z, z') = \overline{H(z', z)}$, this means that the operator f_a is self-adjoint, hence f is symmetric. This implies easily that α defines an isomorphism of $\mathbb{Q}$-linear spaces

$$\alpha : \mathrm{NS}(A)_{\mathbb{Q}} \stackrel{\cong}{\to} \mathrm{End}^s_{\mathbb{Q}}(A) := \mathrm{End}^s(A) \otimes \mathbb{Q}. \tag{2.22}$$

If L_0 is a principal polarization, this defines an isomorphism

$$\alpha : \mathrm{NS}(A) \stackrel{\cong}{\to} \mathrm{End}^s(A) \tag{2.23}$$

[106, 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 that if L is a principal polarization then $\alpha(L)$ is an automorphism of A. The converse is not true.

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

$$H = H_0(f_a(z), z'). \tag{2.24}$$

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

$$M \cdot (Z|\mathsf{D}) = (Z|\mathsf{D}) \cdot N, \tag{2.25}$$

where the matrix

$$N = \begin{pmatrix} N_1 & N_3 \\ N_2 & N_4 \end{pmatrix} \in \mathrm{Mat}_{2g}(\mathbb{Z})$$

defines f_r. Thus, we get

$$M = (Z \cdot N_3 + \mathsf{D}N_4)\mathsf{D}^{-1},$$

hence,

$$M\tau = (Z \cdot N_3 + \mathsf{D}N_4)\mathsf{D}^{-1}Z = \tau N_1 + \mathsf{D}N_2. \tag{2.26}$$

This shows that the period matrix Z must satisfies 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}. This implies that the matrix N satisfies ${}^tN \cdot J_{\mathsf{D}} = -J_{\mathsf{D}}{}^t \cdot N$. This gives

$${}^tN_1\mathsf{D} = \mathsf{D}N_4, \quad {}^tN_2\mathsf{D} = -\mathsf{D}N_2, \quad {}^tN_3\mathsf{D} = -\mathsf{D}N_3. \tag{2.27}$$

If $\mathsf{D} = I_g$ (i.e., in the case of principal polarization), then

$$N = \begin{pmatrix} N_1 & N_2 \\ N_3 & {}^tN_1 \end{pmatrix}, \tag{2.28}$$

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

The coefficients of the characteristic polynomial have the following geometric meaning in terms of the intersection theory on $\mathrm{Pic}(A)$ (induced by the intersection theory on $H^*(A, \mathbb{Z})$).

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

$$dc_i^a = \frac{(L_0^{g-i}, L^i)}{(g-i)!i!}, \quad i = 0, \dots, g, \tag{2.29}$$

where $d = d_1 \cdots d_g$ [106], (5.2.1). In particular, L is ample if and only if all eigenvalues of f_a are positive.[3] 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 $i = 0, \dots, g$.

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 a holomorphic ample line bundle. The "almost" *inverse isogeny* of f is the holomorphic homomorphism $g : A' \to A$ such that $g \circ f = [e]$, where e is the exponent of the kernel of f. (Such a g always exists and unique. In addition, g is also an isogeny.) For example, $e \cdot \phi_L^{-1}$ is the almost inverse isogeny of ϕ_L. One may easily check that the existence of an isogeny between abelian varieties is an equivalence relation on the set of isomorphism classes of abelian varieties.

Suppose that $\alpha(L) = f \in \mathrm{End}^s(A)$ 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 (2.29) with $i = g$, we obtain

$$c_g^a = \frac{d'g!}{g!d} = \deg(f). \tag{2.30}$$

[3] 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.

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

$$c_i = \binom{g}{i}\frac{(f^*(L_0)^i, L_0^{g-i})}{(L_0^g)} \tag{2.31}$$

(see [106], (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

$$\mathrm{Tr}(f\circ f') = \frac{2}{(g-1)!}\frac{(f^*(L_0), L_0^{g-1})}{(L_0^g)},\quad \mathrm{Nm}(f\circ f') = \frac{(f^*(L_0)^g)}{(L_0^g)}. \tag{2.32}$$

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

2.5 Semi-simple Finite-dimensional Algebras

We know that $\mathrm{End}_{\mathbb{Q}}(A)$ is isomorphic to a subalgebra of the matrix algebra $\mathrm{Mat}_{2g}(\mathbb{Q})$, and hence, is a finite-dimensional algebra over $\mathbb{Q}$. Recall that a finite-dimensional associative algebra D over a field F is called a *simple algebra* if it has no nonzero two-sided ideals. An algebra over F is called *semi-simple* if it is isomorphic to the direct product of simple F-algebras. The center of a simple algebra is a field containing F. If the center coincides with F, the algebra is called a *central simple algebra*.

If D is a skew field and K is the center of D then K is an overfield of F and the K-dimension of D is always a square. This is proved by showing that, over some finite extension L of K, the algebra $D_L = D\otimes_K L$ *splits*, i.e., becomes isomorphic to a matrix algebra over L.

An example of a central simple algebra is the matrix algebra $\mathrm{Mat}_n(F)$. Another example of a simple algebra is a field, or a *division algebra*, also called a *skew field*, an algebra (often assumed to be non-commutative), where every nonzero element is invertible.

By a *Theorem of Wedderburn* (see [18, Chapter 8,§8] or [101, Chapter 1,§3]), a semi-simple algebra over a field F is isomorphic to the direct product of matrix algebras over division algebras.

An example of a non-commutative central simple F-algebra (if $\mathrm{char}(F)\neq 2$) is a 4-dimensional *quaternion algebra*

$$H = \left(\frac{a,b}{F}\right) = F + F\mathbf{I} + F\mathbf{J} + F\mathbf{K},$$

where $\mathbf{I}^2 = a\neq 0, \mathbf{J}^2 = b\neq 0, \mathbf{K} = \mathbf{I}\cdot\mathbf{J} = -\mathbf{J}\cdot\mathbf{I}$ [58, Chapter 1], [170, Chapter 2]. Note that, multiplying a or b by a non-zero square in the field does not change the isomorphism class of the algebra. Also $\left(\frac{a,b}{F}\right)\cong\left(\frac{b,a}{F}\right)$. The algebra H is a division algebra if and only if the only solution in F^3 of the equation $x_0^2 = ax_1^2 + bx_2$ is the triple $(x_0,x_1,x_2) = (0,0,0)$ [58, 1.3], [136, 1.6]. Also, note, for later computations, that

$$\mathbf{I}\cdot\mathbf{K} = -\mathbf{I}\cdot\mathbf{K} = \mathbf{I}\cdot\mathbf{I}\cdot\mathbf{J} = a\mathbf{J},\quad \mathbf{J}\cdot\mathbf{K} = -\mathbf{K}\cdot\mathbf{J} = \mathbf{J}\cdot\mathbf{I}\cdot\mathbf{J} = -\mathbf{J}^2\cdot\mathbf{I} = -b. \tag{2.33}$$

The quaternion algebra H is equipped with an anti-involution

$$x = \alpha + \beta\mathbf{I} + \gamma\mathbf{J} + \delta\mathbf{K} \mapsto \bar{x} = \alpha - \beta\mathbf{I} - \gamma\mathbf{J} - \delta\mathbf{K}$$

such that

$$\mathrm{Nm}(x) = \mathrm{Nm}_H(x) := x\bar{x} = \bar{x}x = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \in F. \tag{2.34}$$

If we put

$$\mathrm{tr}(x) = \mathrm{tr}_H(x) := x + \bar{x} = 2\alpha \in F. \tag{2.35}$$

then direct calculations show that

$$\mathrm{tr}(\bar{x}) = \mathrm{tr}(x), \quad x^2 - \mathrm{tr}(x)x + \mathrm{Nm}(x) = 0, \quad \forall x \in H. \tag{2.36}$$

Clearly,

$$\mathrm{tr}(1) = 2, \mathrm{tr}(\mathbf{I}) = \mathrm{tr}(\mathbf{J}) = \mathrm{tr}(\mathbf{K}) = 0. \tag{2.37}$$

Notice that

$$\mathrm{tr}(xy) = \mathrm{tr}(yx)\ \forall x, y \in H; \quad \mathrm{tr}(yxx^{-1}) = \mathrm{tr}(x), \quad \overline{yxy^{-1}} = y\bar{x}y^{-1}, \quad \forall x \in H, y \in H^*. \tag{2.38}$$

Indeed, let us consider the F-algebra $\mathrm{End}_F(H)$ of all F-linear operators in the F-vector space H and the corresponding faithful *left regular representation* of H

$$\mathrm{mult}_H : H \to \mathrm{End}_F(H),\ y \mapsto \mathrm{mult}_H(y) : H \to H,\ x \mapsto yx, \quad \forall x \in F, \tag{2.39}$$

which is an injective homomorphism of F-algebras that sends 1 to 1. Let

$$\mathrm{Tr}_H : \mathrm{End}_F(H) \to F$$

be the corresponding F-linear *trace map* such that

$$\mathrm{Tr}_H(uwu^{-1}) = \mathrm{Tr}_H(w), \tag{2.40}$$

for all $w \in \mathrm{End}_F(H)$ and F-linear automorphisms u of the F-vector space H.

$$\mathrm{Tr}_H\left(\mathrm{mult}_H(yx)\right) = \mathrm{Tr}_H\left(\mathrm{mult}_H(x)\mathrm{mult}_H(y)\right) = \mathrm{Tr}_H\left(\mathrm{mult}_H(y)\mathrm{mult}_H(x)\right) = \mathrm{Tr}_H\left(\mathrm{mult}_H(xy)\right) \tag{2.41}$$

for all $x, y \in H$. It follows that, for any $x \in H, y \in H^*$,

$$\mathrm{Tr}_H\left(\mathrm{mult}_H(yxy^{-1})\right) = \mathrm{Tr}_H(\mathrm{mult}_H(y)\mathrm{mult}_H(x)\mathrm{mult}_H(y)^{-1}) = \mathrm{Tr}_H(x).$$

Using (2.33), we get

$$\mathrm{Tr}_H(\mathbf{I}) = \mathrm{Tr}_H(\mathbf{J}) = \mathrm{Tr}_H(\mathbf{K}) = 0, \text{ and } \mathrm{Tr}_H(1) = 4. \tag{2.42}$$

Combining the F-linearity of both tr and Tr_H with (2.37) and (2.42), we conclude that, for any $x \in H$,

$$\mathrm{Tr}_H(\mathrm{mult}(x)) = 2\mathrm{tr}(x) = 2\mathrm{tr}_H(x).$$

It follows from (2.40) that $\mathrm{tr}(yxx^{-1}) = \mathrm{tr}(x)$, which proves the first formula of (2.38). The second formula of (2.38) follows from (2.35).

Remark 2.25. The trace map on H gives rise to the symmetric non-degenerate F-bilinear *trace form*

$$H \times H \to F, \quad x, y \mapsto \mathrm{tr}(xy).$$

Indeed, the non-degeneracy follows from the explicit formula:

$$\mathrm{tr}\left((\alpha_1 + \beta_1\mathbf{I} + \gamma_1\mathbf{J} + \delta_1\mathbf{K})(\alpha_2 + \beta_2\mathbf{I} + \gamma_2\mathbf{J} + \delta_2\mathbf{K})\right) = \alpha_1\alpha_2 + a\beta_1\beta_2 + b\gamma_1\gamma_2 - ab\delta_1\delta_2, \quad \forall \alpha_i, \beta_i, \gamma_i, \delta_i \in F.$$

Later we will use a closely related to the trace form the non-degenerate F-bilinear form

$$\mathrm{B}_{\mathrm{tr}} : H \times H \to F, \quad x, y \mapsto \mathrm{tr}(x\bar{y}). \tag{2.43}$$

It is symmetric, because

$$\mathrm{B}_{\mathrm{tr}}(y, x) = \mathrm{tr}(y\bar{x}) = \mathrm{tr}(\overline{y\bar{x}}) = \mathrm{tr}(x\bar{y}) = \mathrm{B}_{\mathrm{tr}}(x, y).$$

Again, direct computations tell us that $\{1, \mathbf{I}, \mathbf{J}, \mathbf{K}\}$ is an orthogonal basis of the F-vector space H with respect to B_{tr}, while

$$\mathrm{B}_{\mathrm{tr}}(1,1) = 2,\ \mathrm{B}_{\mathrm{tr}}(\mathbf{I},\mathbf{I}) = -2\alpha,\ \mathrm{B}_{\mathrm{tr}}(\mathbf{J},\mathbf{J}) = -2\beta,\ \mathrm{B}_{\mathrm{tr}}(\mathbf{K},\mathbf{K}) = 2\alpha\beta.$$

It follows that the determinant of the matrix of the form B_{tr} with respect to the basis $\{1, \mathbf{I}, \mathbf{J}, \mathbf{K}\}$ is equal to

$$2 \cdot (-2\alpha) \cdot (-2\beta) \cdot (2\alpha\beta) = (4\alpha\beta)^2,$$

which is a (nonzero) *square* in F. Hence, the determinant of the form B_{tr} with respect to any basis of the F-vector space H is also a *square*.

The following assertion will be used in Chapter 5.

Proposition 2.26. *If $\rho \in H \setminus F$ and $\rho^2 \in F^*$, then:*

(i) $\mathrm{tr}(\rho) = 0 = \mathrm{tr}\left(\rho^{-1}\right)$, *that is,*

$$\bar{\rho} = -\rho \in F\mathbf{I} + F\mathbf{J} + F\mathbf{K}, \quad \overline{\rho^{-1}} = -\rho^{-1} \in F\mathbf{I} + F\mathbf{J} + F\mathbf{K}.$$

(ii) The F-bilinear form

$$E = E_\rho : H \times H \to F, \quad E(x, y) = \mathrm{tr}(\rho x\bar{y}) \tag{2.44}$$

is an alternating nondegenerate F-bilinear form such that

$$E(x\eta, y\eta) = E(x, y) \quad \forall x, y \in H \text{ and } \forall \eta \in H \setminus F \text{ with } \eta^2 = -1. \tag{2.45}$$

(iii) The map

$$H \to H, \quad x \mapsto x^* := \rho\bar{x}\rho^{-1}$$

is an anti-involution of the F-algebra H.

(iv) Suppose that $c = \rho^2 \in F$ is not as square in F. Let $\eta \in H$ and $s \in F^*$ satisfy the equality

$$\eta^2 = s^2\rho^2 = s^2 c \in F^*.$$

Then, there exists $\delta \in H^*$ such that $\eta = s \cdot \delta\rho\delta^{-1}$ and

$$E(x\eta, x) = s \cdot c \cdot \mathrm{Nm}(\delta)^{-1} \cdot \mathrm{tr}\left((x\delta)(x\delta)^*\right), \quad \forall x \in H.$$

(v) Let $F = \mathbb{R}$ and $c = \rho^2 \in \mathbb{R}, c < 0$. Suppose that

$$\mathrm{tr}(xx^*) > 0, \quad \forall x \in H \setminus \{0\}.$$

Let $\mathcal{X}(H) := \{\eta \in H \mid \eta^2 = -1\}$. Then, either, for all $\eta \in \mathcal{X}(H)$,

$$E(x\eta, x) = \mathrm{tr}(\rho x\eta\bar{x}) > 0, \quad \forall x \in H \setminus \{0\}, \tag{2.46}$$

or, for all $\eta \in \mathcal{X}(H)$,

$$E(x\eta, x) < 0 \quad \forall x \in H \setminus \{0\}.$$

Proof. Indeed, ρ is obviously invertible in H. It follows from the second formula of (2.36) that $\mathrm{tr}(\rho)x = \rho^2 + \mathrm{Nm}(\rho) \in F$. Since $\rho \notin F$, we get $\mathrm{tr}(\rho)\rho = 0$ and $\rho \neq 0$, which imply that $\mathrm{tr}(\rho) = 0$, i.e., $\bar{\rho} = -\rho$. Now, we have

$$\rho \cdot \rho^{-1} = \rho^{-1} \cdot \rho = 1 = \bar{1} = \overline{\rho^{-1}\rho} = \bar{\rho}\overline{\rho^{-1}} = -\rho\overline{\rho^{-1}}.$$

This implies that $\overline{\rho^{-1}} = -\rho^{-1}$, i.e., $\mathrm{tr}(\rho^{-1}) = 0$. This ends the proof of (i).

Let us prove (ii). The F-bilinearity of E is obvious while its non-degeneracy follows from the non-degeneracy of the trace form (see Remark 2.25). Now, using the first equality of (2.36), (2.38) and the already proven assertion (i), we have

$$E(x,y) = \mathrm{tr}(\rho x\bar{y}) = \mathrm{tr}\big(\overline{\rho x\bar{y}}\big) = \mathrm{tr}(y\bar{x}\bar{\rho}) = \mathrm{tr}\left(y\bar{x}(-\rho)\right) = -\mathrm{tr}(y\bar{x}\rho) = -\mathrm{tr}\left(\rho(y\bar{x}\rho)\rho^{-1}\right) = -\mathrm{tr}(\rho y\bar{x}) = -E(y,x).$$

This proves that E is alternating. In order to finish the proof of (ii), notice that in light of (i), $\bar{\eta} = -\bar{\eta}$, hence

$$E(x\eta, y\eta) = \mathrm{tr}(\rho x\eta\overline{y\eta}) = \mathrm{tr}(\rho x\eta\bar{\eta}\bar{y}) = -\mathrm{tr}(\rho x\eta^2 y) = -\big(-\mathrm{tr}(\rho x\bar{y})\big) = \mathrm{tr}(\rho x\bar{y}) = E(x,y).$$

Now, let us prove (iii), loosely following [102, Ch. IX, proof of Th. 4.3]. Since the map $x \mapsto x^*$ is a composition of an anti-automorphism and an automorphism, it is an anti-automorphism. In order to check that this is an involution, it suffices to observe that

$$(x^*)^* = \left(\rho\bar{x}\rho^{-1})\right)^* = \rho \cdot \overline{\rho\bar{x}\rho^{-1}} \cdot \rho^{-1} = \rho \cdot \overline{\rho^{-1}}x\bar{\rho} \cdot \rho^{-1} = (-\rho\rho^{-1})x(-\rho\rho^{-1}) = x.$$

In order to prove (iv), first notice that $\eta \notin F$, because η^2 is *not* a square in F. Further, replacing η by $s^{-1}\eta$, we may and will assume that

$$s = 1, \quad \rho^2 = \eta^2 = c \in F^*.$$

Since c is *not* a square in F, both F-subalgebras $F + F\rho$ and $F + F \cdot \eta$ are isomorphic to the quadratic field extension $F(\sqrt{c})$ of F. In other words, the map

$$F + F \cdot \rho \to F + F \cdot \eta, \quad \alpha + \beta\rho \mapsto \alpha + \beta\eta \; \forall \alpha, \beta \in F$$

is a F-linear field isomorphism that sends ρ to η. It follows from the theorem of Skolem-Noether (see [18, §11]) that there is $\delta \in H^*$ such that

$$\eta = \delta\rho\delta^{-1}.$$

Then,

$$\begin{aligned} &E(x\eta, x) = \mathrm{tr}(\rho x \eta \bar{x}) = \mathrm{tr}(x\bar{\eta}\bar{x}\bar{\rho}) = \mathrm{tr}\left(x(-\eta)\bar{x}(-\rho)\right) = \mathrm{tr}(x\eta\bar{x}\rho) \\ &= \mathrm{tr}(x\delta\rho\delta^{-1}\bar{x}\rho) = \mathrm{tr}(x\delta\rho\delta^{-1}\bar{x}\rho) = \mathrm{tr}((x\delta)(\rho\delta^{-1}\bar{x}\rho^{-1}\rho^2)) \\ &= \mathrm{tr}((x\delta)(\rho\delta^{-1}\bar{x}\rho^{-1})c)c \cdot \mathrm{tr}((x\delta)(\rho\overline{(x\bar{\delta}^{-1})}\rho^{-1})) \\ &= c \cdot \mathrm{tr}((x\delta)(x\bar{\delta}^{-1})^*)) = c \cdot \mathrm{tr}((x\delta)(x\delta\delta^{-1}\bar{\delta}^{-1})^*)) \\ &= c \cdot \mathrm{tr}((x\delta)(x\delta\mathrm{Nm}(\delta)^{-1})^*)) = c \cdot \mathrm{Nm}(\delta)^{-1} \cdot \mathrm{tr}((x\delta)(x\delta)^*)). \end{aligned} \tag{2.47}$$

(v) follows readily from (iv) applied to $F = \mathbb{R}$. □

Remark 2.27. Let $\tilde{F}$ be an overfield of F. Then, $\tilde{H} = H \otimes_F \tilde{F}$ is the quaternion algebra $\left(\frac{a,b}{\tilde{F}}\right)$. Identifying H with

$$H \otimes 1 \subset H \otimes_F \tilde{F} \subset \tilde{H},$$

we may view H as the certain F-subalgebra of $\tilde{H}$, and $1, \mathbf{I}, \mathbf{J}, \mathbf{K}$ as a basis of the $\tilde{F}$-vector space $\tilde{H}$. Now, the explicit formula (2.35) implies that

$$\mathrm{tr}_{\tilde{H}}(x) = \mathrm{tr}_H(x) \in F, \quad \forall x \in H \subset \tilde{H}. \tag{2.48}$$

This implies that the restriction of the canonical involution

$$\tilde{H} \to \tilde{H}, \quad x \mapsto x' = \mathrm{tr}_{\tilde{H}}(x) - x$$

to H coincides with the canonical involution

$$H \to H, \quad x \mapsto x' = \mathrm{tr}_H(x) - x.$$

Combining this with (2.34), we obtain that

$$\mathrm{Nm}_{\tilde{H}}(x) = \mathrm{Nm}_H(x) \in F \quad \forall x \in H \subset \tilde{H}.$$

Remark 2.28. The characteristic polynomial $\mathcal{P}_x(t) \in F[t]$ of $\mathrm{mult}_H(x) : H \to H$ coincides with $\left(t^2 - \mathrm{tr}(x)t + \mathrm{Nm}(x)\right)^2$. Indeed, if $H \cong \mathrm{Mat}_2(F)$ then our assertion follows readily from the fact that the left $\mathrm{Mat}_2(F)$-module $\mathrm{Mat}_2(F)$ is isomorphic to a direct sum of two copies of the $\mathrm{Mat}_2(F)$-moduleF^2. In order to do the general case, it suffices to recall that there is an overfield $\tilde{F}$ of F such that $H_{\tilde{F}} = H \otimes_F \tilde{F}$ is isomorphic to $\mathrm{Mat}_2(\tilde{F})$ and apply Remark 2.27.

If, for any $x \neq 0$, $\mathrm{Nm}(x) \neq 0$, then

$$x^{-1} = \frac{1}{\mathrm{Nm}(x)} x',$$

hence, H is a skew field. A quaternion algebra H over a totally real number field K is called *totally definite* if for every (real) field embedding $\sigma : K \hookrightarrow \mathbb{R}$, the $\mathbb{R}$-algebra $H_\sigma = H \otimes_{K,\sigma} \mathbb{R}$ obtained by the change of scalars H_σ is a skew field. If, for any σ as above, the algebra H_σ acquires zero divisors, hence become isomorphic to $\mathrm{Mat}_2(\mathbb{R})$, it is called *totally indefinite*.

For example, for the quaternion algebra $H = \left(\frac{a,b}{\mathbb{Q}}\right)$, a splitting field is $L = \mathbb{Q} + \mathbb{Q}\mathbf{I} \cong \mathbb{Q}(\sqrt{a})$, so that $H \otimes L = L + L\mathbf{J}$. One can write any element in H as $x = m + n\mathbf{J}$, where $m = \alpha + \beta\mathbf{I}, n = \gamma + \delta\mathbf{K} \in K$. The multiplication rule becomes

$$(m + n\mathbf{J})(m' + n'\mathbf{J}) = mm' + n\bar{n}'b + (mn' + n\bar{m}')\mathbf{J};$$

in particular, for any $m \in L$, we have $m\mathbf{J} = \mathbf{J}\bar{m}$. The map

$$m + n\mathbf{j} \mapsto \begin{pmatrix} m & n \\ b\bar{n} & \bar{m} \end{pmatrix} \tag{2.49}$$

defines an isomorphism $f : H_L \to \mathrm{Mat}_2(L)$. Observe that $\overline{m + n\mathbf{J}} = \bar{m} - n\mathbf{J}$ and $\overline{xy} = \bar{y}\bar{x}$. We see that, under this isomorphism, the trace $\mathrm{tr}(x)$ (resp. the norm $\mathrm{Nm}(x)$) corresponds to the usual trace (resp. the determinant) of a matrix. Also, observe that $f(\bar{x}) = J \cdot {}^t f(x) \cdot J^{-1}$, where $J = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Let R be a finite-dimensional simple algebra over a field F of characteristic 0. Then, its center K is an extension of finite degree of F. In addition, there is an isomorphism of K-algebras $R \cong \mathrm{Mat}_r(D)$, where D is a finite-dimensional central division algebra over K, and r is a certain positive integer. Taking into account that $\dim_K(D)$ is a complete square, we may define the *reduced degree* of R (over K), denoted by $[R : K]_{\mathrm{red}}$, to be the positive integer $r\sqrt{\dim_K(D)}$, whose square is $\dim_K(R) = r^2 \dim_K(D)$. We also define the *reduced degree* $[R : F]_{\mathrm{red}}$ of R over F as the product $[R : K]_{\mathrm{red}}[K : F]$. Clearly,

$$[R : K]_{\mathrm{red}} \mid [R : K], \quad [R : F]_{\mathrm{red}} \mid [R : F] \tag{2.50}$$

if R is a *simple* F-algebra.

The reduced degrees admits a natural interpretation as the rank of R equipped with a Lie K-algebra structure defined by the bracket operation

$$[u, v] = uv - vu, \ \forall u, v \in R. \tag{2.51}$$

It is known ([81, Ch. X, Sect. 3], [190, p. 66, Step 3]) that the Lie algebra R splits into a direct sum

$$R = K \oplus \mathrm{sl}(R)$$

of its center K and its derived algebra $\mathrm{sl}(R)$, which is a simple K-Lie algebra of rank

$$\sqrt{\dim_K(R)} - 1 = r\sqrt{\dim_K(D)} - 1 = [R : K]_{\mathrm{red}} - 1.$$

This implies that R is a reductive K-Lie algebra of rank

$$([R:K]_{\text{red}} - 1) + 1 = [R:K]_{\text{red}},$$

and also R is a reductive F-Lie algebra of rank

$$[R:K]_{\text{red}}[K:F] = [R:F]_{\text{red}}.$$

Now, let R be an arbitrary finite-dimensional semi-simple F- algebra. It follows that, if we define the structure of a F-Lie algebra on R by (2.51), then R becomes a reductive Lie algebra over F. Let us define the reduced degree $[R:F]_{\text{red}}$ over F as the sum of the reduced degrees of its simple factors over F. The additivity of ranks of reductive Lie algebras (wrt direct sums) implies that $[R:F]_{\text{red}}$ coincides with the rank of of the$F$-Lie algebra R. (Notice that each *Cartan subalgebra* of R is either an overfield of F or a direct sum of finitely many overfields of F.)

A semi-simple finite-dimensional algebra F-algebra R comes equipped with the *trace* F-bilinear map $R \times R \to F$ defined by $(x,y) \mapsto \text{Tr}(xy)$, where $\text{Tr}(a)$ is the trace of the F-linear linear operator $R \to R, x \mapsto xa$. We can also define the *reduced trace* and the *reduced norm* of a *central simple* K-algebra R by embedding R into the matrix algebra $\text{Mat}_r(L)$ over a splitting field L of R, and taking the usual trace and norm of a matrix. Note that this does not depend on the choice of L and the values of the reduced trace and the reduced norm belong to K.

The possible structure of the $\mathbb{Q}$-algebra $\text{End}_{\mathbb{Q}}(A)$ is known. It is a finite-dimensional associative algebra R admitting an anti-involution[4] $x \to x^*$ and a symmetric bilinear form $\text{Tr} : R \times R \to \mathbb{Q}$ such that the quadratic form $x \mapsto \text{Tr}(xx^*)$ 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 A. Albert and G. Scorza in the beginning of the last century.

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 σ-invariants. Then, K_0 is a totally real algebraic number field. If $K \neq K_0$, then it is a purely imaginary quadratic extension of K_0. Since R is central simple over K, its K-dimension is equal to n^2 for some positive integer n.

Let

$$e = [K:\mathbb{Q}], \quad e_0 = [K_0:\mathbb{Q}].$$

Then, $[K:K_0] = 1$ or 2, and

$$\dim_{\mathbb{Q}}(R) = en^2 = [K:K_0]e_0n^2.$$

If R is not simple, then it is isomorphic to the finite product of such simple $\mathbb{Q}$-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's Reducibility Theorem* and asserts that

[4] 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 $x \cdot y := y \cdot x$.

an abelian variety is simple if and only if it does not contain a k-dimensional abelian subvariety of dimension $k \neq 0, g$. The endomorphism algebra $R = \mathrm{End}_{\mathbb{Q}}(A)$ of a simple abelian variety A is a skew-field.

Let

$$\rho := \dim_{\mathbb{Q}} \mathrm{NS}_{\mathbb{Q}}(A)$$

be the *Picard number* of A. It follows from (2.22) that it coincides with $\dim_{\mathbb{Q}} \mathrm{End}^s_{\mathbb{Q}}(A)$.

The following table gives four possible cases for a simple algebra R.

Type	n	e	ρ	Restriction
I	1	e_0	e_0	$e \mid g$
II	2	e_0	$3e$	$2e \mid g$
III	2	e_0	e_0	$2e \mid g$
IV	n	$2e_0$	$e_0 n^2$	$e_0 n \mid g$

Table 2.1: Endomorphisms algebras of simple abelian varieties

It is known that any finite-dimensional simple algebra R over $\mathbb{R}$ is isomorphic to either $\mathrm{Mat}_r(\mathbb{R})$, or $\mathrm{Mat}_r(\mathbb{C})$, or $\mathrm{Mat}(\mathbb{H})$, where $\mathbb{H}$ is the usual quaternion algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$. By embedding R into $R_{\mathbb{R}}$, we can identify the anti-involution $x \mapsto x^*$ with taking the transpose ${}^t x$ of the matrix x in the first case, and with taking the adjoint ${}^t\bar{x}$ of the matrix $\bar{x}$ in the remaining two cases. Since the $\mathbb{Q}$-subalgebra of symmetric elements in $\mathrm{End}_{\mathbb{Q}}(A)$ is isomorphic to the subalgebra of R of elements x such that $x = x^*$, this gives the information about the possible Picard number ρ of A.

If A is not simple, its endomorphism algebra is not a skew field, i.e., it has zero divisors.

Note that

$$[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2g. \tag{2.52}$$

Indeed, $\mathrm{End}_{\mathbb{Q}}(A)$ embeds in $\mathrm{Mat}_{2g}(\mathbb{Q})$ via its rational representation. Hence, the reductive $\mathbb{Q}$-Lie algebra $\mathrm{End}_{\mathbb{Q}}(A)$ is isomorphic to a $\mathbb{Q}$-Lie subalgebra of the reductive $\mathbb{Q}$-Lie algebra $\mathrm{Mat}_{2g}(\mathbb{Q})$ of rank $2g$. This implies that $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}}$ does not exceed $2g$.

If A is a simple abelian variety, then $\mathrm{End}_{\mathbb{Q}}(A)$ is a skew-field that acts faithfully on the $2g$-dimensional $\mathbb{Q}$-vector space $\Lambda_{\mathbb{Q}}$. This implies that $\dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}}(A))$ divides $2g$. In particular, for any simple abelian variety A,

$$\dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}}(A)) \leq 2 \dim(A). \tag{2.53}$$

It follows from (2.50) that $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} | 2g$. More precisely, $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}}$ divides g if A is of types I-III, and $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}}$ divides $2g$ if A is of type IV. In the latter case, the equality in (2.52) occurs if and only if A is of type IV with $e_0 = g$. If A is not necessarily simple, the equality occurs if and only if A is isogenous to the product of simple abelian varieties A_i with $[\mathrm{End}^0(A_i) : \mathbb{Q}]_{\mathrm{red}} = 2 \dim A_i$.

We say in this case that A is of CM-*type*. We will study such varieties in details in Chapter 9.

Theorem 2.29. *Let A and B be abelian varieties. Then, the rank of the free abelian group* $\mathrm{Hom}(A,B)$ *does not exceed* $2\dim(A)\dim(B)$. *In particular, for any abelian variety A,*

$$\dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}}(A)) \le 2\dim(A)^2. \tag{2.54}$$

Proof. We may assume that $A \neq \{0\}, B \neq \{0\}$. Replacing A and B by abelian varieties isogenous to them, we may and will assume that

$$A = \prod_{i=1}^{r} A_i,\ B = \prod_{j=1}^{s} B_j,$$

where all A_i and B_j are simple abelian varieties. Then

$$\mathrm{Hom}(A,B) = \prod_{i=1}^{r}\prod_{j=1}^{s} \mathrm{Hom}(A_i,B_j).$$

Since

$$\dim(A) = \sum_{i=1}^{r} \dim(A_i),\ \dim(B) = \sum_{j=1}^{r} \dim(B_j),$$

it suffices to check that the rank of each $\mathrm{Hom}(A_i,B_j)$ does not exceed $2\dim(A_i)\dim(B_j)$. In other words, it suffices to prove the theorem in the case of *simple* abelian varieties A and B. So, assume that both A and B are simple. If A and B are not isogenous, then the group $\mathrm{Hom}(A,B) = \{0\}$ and its rank is 0, which does not exceed $2\dim(A)\dim(B)$. On the other hand, if A and B are isogenous, the rank of $\mathrm{Hom}(A,B)$ equals the rank of $\mathrm{End}(A)$. As we have already seen in (2.53), it does not exceed $2\dim(A)$. In its turn, since $B \neq \{0\}$, it does not exceed $2\dim(A)\dim(B)$. This ends the proof. □

It follows from the Hodge decomposition (1.3) of complex cohomology of A of dimension g that

$$H^{1,1}(A,\mathbb{C}) = H^1(A,\Omega^1_A) \cong V \otimes V^{\vee} \cong \mathbb{C}^{g^2}.$$

Since the first Chern class homomorphism defines an invective homomorphism

$$c_1 : \mathrm{NS}_{\mathbb{Q}}(A) \to H^{1,1}(A,\mathbb{C}) \cap H^2(A,\mathbb{Z}),$$

we obtain that

$$\dim_{\mathbb{Q}} \mathrm{NS}_{\mathbb{Q}}(A) \le g^2.$$

Definition 2.3. An abelian variety A of dimension $g > 1$ is called *singular* if $\dim_{\mathbb{Q}} \mathrm{End}^s_{\mathbb{Q}}(A) = g^2$. In view of(2.22), this is equivalent to that $\dim_{\mathbb{Q}} \mathrm{NS}(A)_{\mathbb{Q}}$ is maximal possible and equal to g^2.

Theorem 2.30. *[127] The following properties are equivalent:*

- *A is a singular abelian variety of dimension g;*
- *A is isogenous to the product of g elliptic curves E_i with complex multiplication.*

Proof. The second property obviously implies the first. Indeed, it is obvious that the *Picard number* of A

$$\rho(A) := \dim_{\mathbb{Q}} \mathrm{NS}_{\mathbb{Q}}(A)$$

does not change under an isogeny. So, we may assume that A is isomorphic to the product of elliptic curves. Since there is only one isogeny class of an elliptic curve E with complex multiplication,

$$\rho(E \times E) = 2 + \dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}}(E)) = 4.$$

By induction, we get $\rho(E^g) = g^2$.

Conversely, if A is singular, then the classification of possible endomorphism algebras shows that A is as in Case IV. The algebra $\mathrm{End}_{\mathbb{Q}}(A)$ is a purely imaginary quadratic extension K of a totally real field K_0 with $[K_0 : \mathbb{Q}] = g$. Thus, $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} = 2g$, and therefore, A is isogeneour to the product of simple abelian varieties A_i with $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} = 2\dim(A_i)$. It is immediate to see that $\dim(A_i) = 1$. □

In fact, we have a stronger result proven in [156] (see also [106, Chapter 10, Corollary (6.3)]) in dimension 2 and in [86] for arbitrary dimension.

Theorem 2.31. *A is a singular abelian variety if and only if it is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.*

Chapter 3

Elliptic Curves

An *elliptic curve* is a one-dimensional abelian variety. Here we recall some basic facts about elliptic curves and discuss abelian varieties that are isogenous to the product of elliptic curves. There is an enormous literature about elliptic curves, for example, we may refer the reader to [119], [158].

3.1 Weierstrass Equation

Let

$$\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\} \subset \mathbb{C}$$

be the *upper half-plane*.

An *elliptic curve* is a one-dimensional abelian variety $E = \mathbb{C}/\Lambda$. We can find a special symplectic basis in Λ of the form $(\tau, 1)$, where $\tau = x + \mathbf{i}y \in \mathfrak{H}$. The matrix of the symplectic form $\mathrm{Im}(H)$ on Λ with respect to this basis is the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since $\mathbf{i} = -\frac{x}{y} + \frac{1}{y}\tau$, we get $\mathrm{Im}(H)(\mathbf{i}, 1) = \frac{1}{y}$. By (1.15), $H = \frac{1}{y} z\bar{z}'$ in agreement with (1.15). The Hermitian form H defines a principal polarization on E. It corresponds to a line bundle L_0 of degree 1. We will always consider E as a one-dimensional principally polarized abelian variety.

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

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

The orbit space is known to be isomorphic to $\mathbb{C}$, the isomorphism is defined by a certain holomorphic unction $j : \mathfrak{H} \to \mathbb{C}$, 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) textbook on functions of one complex variable.

One may also find there the definition of the Weierstrass function $\wp(z)$ attached to Λ. It is an even Λ-periodic meromorphic function on $\mathbb{C}$, whose set of poles coincides with Λ (and all those poles are double). The holomorphic map

$$\mathbb{C}/\Lambda \setminus \{0 + \Lambda\} \to \mathbb{P}^2(\mathbb{C}), \quad z + \Lambda \mapsto (X : Y : Z) = (\wp(z) : \wp'(z) : 1)$$

extends to a holomorphic *embedding*

$$\phi_\Lambda : E \hookrightarrow \mathbb{P}^2(\mathbb{C}),$$

whose image $\phi_\Lambda(E)$ is the nonsingular cubic curve (the *Weierstrass model* of E)

$$\mathcal{C}_\Lambda : Y^2Z = 4X^3 - g_2X^2Z - g_3Z^3, \tag{3.1}$$

with

$$g_2 = g_2(\Lambda) = 60 \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^4}, \quad g_3 = g_3(\Lambda) = 140 \sum_{\lambda\in\Lambda\setminus\{0\}} \frac{1}{\lambda^6}. \tag{3.2}$$

The cubic polynomial

$$P_\Lambda(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \tag{3.3}$$

has no multiple roots, i.e.,

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0. \tag{3.4}$$

In addition,

$$j(E) = j(\mathbb{C}/\Lambda) = 1728\frac{g_2(\Lambda)}{\Delta(\Lambda)} = 1728\frac{g_2(\Lambda)}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}. \tag{3.5}$$

In the following, we will identify E with its image in $\mathbb{P}^2(\mathbb{C})$, i.e., with the plane cubic curve $\mathcal{C}_\Lambda$ (3.1). Then, the zero 0_E of the group law on E is the point $\infty := (0 : 1 : 0)$. The inversion map $[-1]$ is $(X : Y : Z) \to (X : -Y : Z)$ in light of evenness of $\wp(z)$ and oddness of its derivative. All three points of order 2 on E (i.e., the elements of $E[2] \setminus \{0_E\}$ are

$$W_1 = (\alpha_1 : 0 : 1),\ W_2 = (\alpha_2 : 0 : 1),\ W_3 = (\alpha_3 : 0 : 1), \tag{3.6}$$

where $\alpha_1, \alpha_2, \alpha_3$ are all three roots of the cubic polynomial $P_\Lambda(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, i.e.,

$$P_\Lambda(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) = 4(x - \alpha_1)(x - \alpha_2)(x - \alpha_3). \tag{3.7}$$

Remark 3.1. If $p, q \in \mathbb{C}$ are complex numbers such that $p^3 - 27q^2 \neq 0$, then there exists precisely one lattice Λ in $\mathbb{C}$ such that

$$p = g_2(\Lambda),\ q = g_3(\Lambda),\ j(\mathbb{C}/\Lambda) = 1728\frac{p^3}{p^3 - 27q^2}.$$

One can also arrive at the Weierstrass equation by embedding E into a $\mathbb{P}^2$ using sections of a line bundle $L = L_0^3$, where $\deg(L_0) = 1$. Its image in the plane is a nonsingular plane curve with an inflection point equal to the image of 0_E. In appropriate projective coordinates, the equation becomes

$$y^2z - x^3 - Axz^2 - Bz^3 = 0, \tag{3.8}$$

where $4A^3 + 27B^2 \neq 0$. The Weierstrass equation is the equation of its affine part that consists of points $(x : y; z)$ with $z \neq 0$. In fact, any nonsingular projective curve of genus 1 over a field K of characteristic $\neq 2, 3$ that admits a rational K-point is isomorphic to a plane curve given by equation (3.8). For this reason, any complex nonsingular curve of genus 1 is often called an elliptic curve.

Remark 3.2. Let K be a finitely generated subfield of $\mathbb{C}$ that contains $g_2(\Lambda)$ and $g_3(\Lambda)$ over $\mathbb{Q}$. (E.g., $K = \mathbb{Q}(g_2(\Lambda), g_3(\Lambda))$.) Then, the group operations on $E = C_\Lambda$ are regular maps of algebraic varieties that are defined over K. In addition,

$$K(E[2]) = K(\alpha_1, \alpha_2, \alpha_3),\ K(E[4]) = K(\alpha_1, \alpha_2, \alpha_3, \sqrt{-1}, \sqrt{\alpha_1 - \alpha_2}, \sqrt{\alpha_2 - \alpha_3}, \sqrt{\alpha_3 - \alpha_1}). \tag{3.9}$$

In particular, in the notation of Section 1.3, $K(E[2])$ coincides with the splitting field of the cubic polynomial $P_\Lambda(x)$ over K. This implies readily that one of the following three conditions holds:

(i) $P_\Lambda(x)$ splits completely over K and $K(E[2]) = K$.

(ii) $P_\Lambda(x)$ has precisely one root in K and $K(E[2])$ is a quadratic extension of K.

(iii) $P_\Lambda(x)$ is irreducible and $K(E[2])/K$ is a Galois extension, whose Galois group is either a cyclic group of order 3 or the noncommutative full symmetric group $\mathbf{S}_3$ of order 6.

Claim 3.3. The $\mathrm{Gal}(K)$-module $E[2]$ is *simple* if and only if the polynomial $P_\Lambda(x)$ is *irreducible* over K. Moreover, the $\mathrm{Gal}(K)$-module $E[2]$ is *absolutely simple* if and only if the Galois group $\mathrm{Gal}(P_\Lambda/K)$ of the irreducible polynomial $P_\Lambda(x)$ over K is the full symmetric group $\mathbf{S}_3$.

Proof. If $P_\Lambda(x)$ if reducible, then at least one of its roots, say α_j lies in K. This means that $W_j = (\alpha_j : 0 : 1) \in E(K)$ and therefore $E[2]$ contains a proper $\mathrm{Gal}(K)$-submodule $\{0_E, W_j\}$. In particular, $E[2]$ is not simple.

On the other hand, if $P_\Lambda(x)$ is irreducible, then $\mathrm{Gal}(K)$ acts transitively on the set $\{\alpha_1, \alpha_2, \alpha_3\}$ of roots of $P_\Lambda(x)$. This implies that $\mathrm{Gal}(K)$ acts *transitively* on the set $\{W_1 = (\alpha_1 : 0 : 1),\ W_2 = (\alpha_2 : 0 : 1), W_3 = (\alpha_3 : 0 : 1)\}$ of all nonzero elements of $E[2]$. Hence, the $\mathrm{Gal}(K)$-module $E[2]$ is simple.

In order to prove the second assertion of the claim, recall that the absolute irreducibility (simplicity) of an irreducible representation (simple module) over $\mathbb{F}_2$) means that its every nonzero endomorphism is the identity map. Let u be a nonzero endomorphism of the simple Galois module $E[2]$. By Schur's Lemma, the simplicity implies that u is an automorphism of $E[2]$. This means that u acts as a certain permutation of the set $\{W_1, W_2, W_3\}$ of all nonzero elements of $E[2]$. In other words, there is a permutation $\sigma \in \mathbb{S}_3$ such that

$$u(W_i) = W_{\sigma(i)}, \quad \forall i = 1, 2, 3. \tag{3.10}$$

Since u commutes with the Galois action on $E[2]$, σ commutes with

$$\mathrm{Gal}(P_\Lambda/K) \subset \mathbf{S}_3.$$

The irreducibility of $P_\Lambda(x)$ means that $\mathrm{Gal}(P_\Lambda/K)$ is either $\mathbf{S}_3$ or the alternating group $\mathbf{A}_3$, which is a cyclic group of order 3. In the former case, σ is the identity permutation, which means that u is the identity automorphism of $E[2]$. This implies that the Galois module $E[2]$ is absolutely simple. In the latter case, every even nontrivial even permutation σ is defined by (3.10) a non-trivial automorphism of the Galois module $E[2]$ that implies that $E[2]$ is not absolutely simple.

□

3.2 Elliptic Curves with Complex Multiplication

Let f be an endomorphism of E, then its analytic representation f_a is defined by a complex number z, and its rational representation $f_r : \Lambda \to \Lambda$ is the map $\lambda \mapsto z\lambda$. Following the classical tradition, we denote the period $Z \in \mathfrak{H}_1$ by τ. In the basis $(\tau, 1)$ of Λ, f_r is given by an integral matrix $N = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$, so that we have $(z\tau, z) = (a_{11}\tau + a_{12}, a_{21}\tau + a_{22})$. This gives $z = a_{21}\tau + a_{22}$ and $(a_{21}\tau + a_{22})\tau = a_{11}\tau + a_{12}$, and hence a quadratic equations for τ

$$a_{21}\tau^2 + (a_{22} - a_{11})\tau - a_{12} = 0. \tag{3.11}$$

It agrees with (2.25). The discriminant of the quadratic equation (2.25) is equal to

$$D = (a_{22} - a_{11})^2 + 4a_{12}a_{21} = (a_{11} + a_{22})^2 - 4(a_{11}a_{22} - a_{12}a_{21}) = \mathrm{Tr}(N)^2 - 4\det(N). \tag{3.12}$$

Since $\mathrm{Im}(\tau) > 0$, we must have $a_{21} \neq 0, D < 0$, or $a_{21} = a_{22} - a_{11} = a_{12} = 0$. 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,

$$\tau = \frac{a_{11} - a_4 + \mathbf{i}\sqrt{-D}}{2a_{21}}.$$

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

$$z = a_{21}\tau + a_{22} = \tfrac{1}{2}(a_{11} + a_{22} + \mathbf{i}\sqrt{-D})$$

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

Multiplying (3.11) by a_3, we obtain that $a_{21}\tau$ 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 (3.12) shows that, D is divisible by 4 if $\mathrm{Tr}(N) = a_{11} + a_{22}$ 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 $D = m^2 D_0$, where D_0 is square-free, then $\mathrm{End}(E)$ is an order in K and D is its *discriminant*. The order is equal to $\mathbb{Z} + m\mathfrak{o}_K$ (see [16]). In any case, $\mathrm{End}_{\mathbb{Q}}(E) \cong K$, so we are in case IV of classification of endomorphism rings of abelian varieties. Also, we see that $\mathrm{End}(E)$ is an order $\mathfrak{o}$ in K. The lattice Λ must be a module over $\mathfrak{o}$, in fact, one can show that it is a projective module of rank 1. Conversely, if we take Λ to be such a module over an order $\mathfrak{o}$ in K, we obtain an elliptic curve $E = \mathbb{C}/\Lambda$ with $\mathrm{End}(E) \cong \mathfrak{o}$.

In this way, one can show that there is a bijective correspondence between isomorphism classes of elliptic curves E with $\mathrm{End}(E) = \mathfrak{o}_K$ 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 is called the *class number* of K.

Note that $\mathrm{Aut}(E)$, which is equal to the group $\mathrm{End}(E)^*$ of invertible elements in $\mathrm{End}(A)$, 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 $\mathrm{Nm}(\frac{1+\sqrt{D}}{2}) = \pm 1$. This implies $D = -3$. Similarly, if

$D \not\equiv 1 \mod 4$, we obtain $a^2 - Db^2 = \pm 1$ implies $D = -1$. If C is a birational model of E as a nonsingular plane cubic, then C is a harmonic cubic if $D = -1$ and equianharmonic cubic otherwise.

Remark 3.4. Let E be an elliptic curve with complex multiplication and $\mathrm{End}_{\mathbb{Q}}(E) = K$. Recall that E admits a Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3,$$

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

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

The curve E has complex multiplication by Gaussian numbers (resp. Eisenstein number) if and only if $g_3 = 0$ (resp. $g_2 = 0$).

According to the *Theorem of Weber and Fuerter*, the j-invariant $j(E)$ of an elliptic curve with complex multiplication is an algebraic integer; in addition, if $\mathrm{End}(E)$ is the whole ring of integers $\mathfrak{o}_K$ in K, then $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$. The field $K(j(E))$ is the *class field* of K, i.e. the maximal unramified extension of K (see [159], Chapter 2, Th. 6.1 and 4.3).

Assume that $j(E) \in \mathbb{Q}$, by the class field 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 $j(E)$ are

$$2^6 \cdot 3^3, 2^3 \cdot 3^3 \cdot 11^3 \ (d = 1); \quad 2^6 \cdot 5^3 \ (d = 2); \quad 0, 2^4 \cdot 3^3 \cdot 5^3, -2^{15} \cdot 3 \cdot 5^3 \ (d = 3); \quad -3^3 \cdot 5^3, 3^3 \cdot 5^3 \cdot 17^3 \ (d = 7);$$

$$2^6 \cdot 5^3 \ (d = 2); \quad -2^{15} \ (d = 11); \quad -2^{15} \cdot 3^3 \ (d = 19); \quad -2^{18} \cdot 3^3 \cdot 5^3 \ (d = 43); \quad -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3 \ (d = 67);$$

$$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3 \ (d = 163)$$

(see [159, Appendix A, Sect. 3])

Note that the classification of endomorphisms algebras in Table 2.1 shows that $\mathrm{End}(E)$ is either isomorphic to $\mathbb{Z}$, or it is an order in a totally imaginary quadratic extension K of $\mathbb{Q}$.

3.3 Isogenies of Elliptic Curves

Let $f : E \to E$ be an endomorphism of E of finite degree $n > 0$. By Riemann-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 $\frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$.

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 > 1).

In other words, we assume that the kernel of f is a cyclic group of order n. In this case, f is called a *cyclic isogeny*).

The theory of elementary divisors allows us to find two bases (γ_1, γ_2) and (γ_1', γ_2') in Λ such that $(f_r(\gamma_1), f_r(\gamma_2)) = (n\gamma_1', \gamma_2')$.

In particular, the kernel of f is the cyclic order n subgroup generated by $\frac{1}{n}\gamma_1 \mod \Lambda$.

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 $\tau \in \mathfrak{H}$.

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 with cyclic kernel is equal to the number of solutions of the equation $\Phi_n(x, x) = 0$. This number was 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 $n \equiv 1 \mod 4$ [55]. 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 an isogeny that is an "almost" inverse of f, i.e., $g \circ f = [n]$, where a positive integer 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, $zz' = n$. Also we know that $|z|^2 = \det f_r = n$. Thus, we obtain that $z' = \bar{z}$ is the complex conjugate of z.

The following two assertions allow us, in many cases, to check easily that given elliptic curves are not isogenous [191].

Theorem 3.5. *Let $E = \mathbb{C}/\Lambda$ and $E' = \mathbb{C}/\Lambda'$ be elliptic curves, and let K be a finitely generated subfield of $\mathbb{C}$ such that*

$$g_2(\Lambda), g_3(\Lambda), g_2(\Lambda'), g_3(\Lambda') \in K,$$

i.e., the cubic polynomials

$$P_\Lambda(x), P_{\Lambda'}(x) \in K[x].$$

Suppose that $P_\Lambda(x)$ is irreducible over K while $P_{\Lambda'}(x)$ is reducible over K.

If E and E' are isogenous, then they both are isogenous to the elliptic curve with absolute invariant 0 and endomorphism ring $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$.

Proof. It follows from Remark 3.2(iii) that replacing, if necessary, K with its quadratic extension, we may assume that $K(E[2])/K$ is a cyclic extension of degree 3.

Since $P_{\Lambda'}(x)$ is reducible, it follows from (3.9) that the field $K(E'[2])$ either coincides with K, or with its quadratic extension. Moreover, $K(E'[4])/K(E'[2])$ is a finite abelian extension, whose degree is a power of 2 (see (3.9) or Claim 1.7 applied to $n = 2$). This implies that $K(E'[4])/K$ is a Galois extension of degree equal to a power of 2. Since $[K(E[2]) : K] = 3$, the fields $K(E[2])$ and $K(E'[4])$ are linearly disjoint over K. Replacing now K by $K(E'[4])$, we may assume that $K(E'[4]) = K$ and $K(E[2])/K$ is a cyclic extension of degree 3. By Theorem 2.10, all endomorphisms of E' are defined over K. BY Claim 3.3, the $\mathrm{Gal}(K)$-module $E[2]$ is simple while the $\mathrm{Gal}(K)$-module $E'[2]$ is not simple.

Let $G = \tilde{G}_{4,E,K}$ be the Galois Group of the field extension $K(E[4])/K$. We know (see (3.9) or Claim 1.7 applied to $n = 2$) that its normal subgroup

$$H = \mathrm{Gal}(K(E[4])/K(E[2]))$$

is a finite abelian 2-group. By the Galois theory, the quotient

$$G/H = \mathrm{Gal}(K(E[4])/K)/\mathrm{Gal}(K(E[4])/K(E[2])) = \mathrm{Gal}(K(E[2])/K).$$

It is a cyclic group of order 3. This implies that $\frac{1}{3}[K(E[4]) : K]$ is a power of 2; in particular, it is prime to 3.

Let C be a Sylow-3-subgroup of G that is a cyclic group of order 3. Clearly, the restriction to C of the surjection

$$G \twoheadrightarrow G/H = \mathrm{Gal}(K(E[2])/K)$$

is a group isomorphism of cyclic groups of order 3. Let us consider the subfield

$$L := K(E[4])^C$$

of C-invariants in $K(E[4])$. By definition of L, its degree

$$[L : K] = \frac{1}{3}[K(E[4]) : K],$$

as we know, is prime to 3. In addition,

$$L(E[4]) = K(E[4]),\ \tilde{G}_{4,E,L} = \mathrm{Gal}(L(E[4])/L) = C.$$

We claim that

$$L(E[2]) = K(E[4]) = L(E[4]). \tag{3.13}$$

Indeed, $L(E[2])$ is the compositum of L and $K(E[2])$. Since $K(E[2])/K$ is Galois of prime degree 3, and $[L : K]$ is prime to 3, the field extensions $K(E[2])/K$ and L/K are linearly disjoint, i.e., their compositum $L(E[2])$ has degree

$$3 \cdot [L : K] = 3 \cdot \frac{[K(E[4]) : K]}{3} = [K(E[4]) : K].$$

This implies that the fields $L(E[2])$ and $K(E[4])$ have the same degree over K. Since $L(E[2])$ is obviously a subfield of $K(E[4])$, we get the desired equality (3.13).

Taking into account that $L(E[2])$ is the splitting field of the polynomial $P_\Lambda(x)$, we conclude that this polynomial remains irreducible over L and its Galois group over L is the cyclic group C of order 3. It follows from Theorem 2.10 that all homomorphisms from E to E' are defined over $L(E[4]) = L(E[2])$. Of course, $P_{\Lambda'}(x)$ remains reducible and (even splits) over the overfield L of K.

It follows from Claim 3.3 that the $\mathrm{Gal}(K)$-module $E[2]$ is simple while the $\mathrm{Gal}(K)$-module $E'[2]$ is not simple. This implies that every homomorphism of the Galois module $E[2] \to E'[2]$ is **zero**.

Suppose that E are E' are isogenous and let $f : E \to E'$ be an isogeny. Since $\mathrm{Hom}(E, E')$ is a free abelian group of finite rank, we may assume (dividing f by a suitable power of 2 if necessary) that

$$f \notin 2 \cdot \mathrm{Hom}(E, E').$$

This means that $f(E[2]) \neq \{0\}$. It follows that f is *not* defined over L, since otherwise, it induces a non-identity homomorphism of the Galois modules $E[2] \to E'[2]$, which (as we have already seen) does not exist. However, f is defined over $L(E(4]) = L(E(2])$.

Let σ be any element of the cyclic group $C = \mathrm{Gal}(L(E(4])/L)$. Then, $\sigma(f) : E \to E'$ is an isogeny that does not coincide with f, unless σ is the identity element of C. This implies that there exists a unique $c_\sigma \in \mathrm{End}_{\mathbb{Q}}(E')^*$ such that

$$\sigma(f) = c_\sigma f \ \text{ in } \ \mathrm{Hom}(E, E') \otimes \mathbb{Q}.$$

In addition, if $\tau \in C$, then

$$c_{\sigma\tau}(f) = \sigma\tau(f) = \sigma(\tau(f)) = \sigma(a_\tau f) = \sigma(c_\tau)\sigma(f).$$

Since all the endomorphisms of E' are defined over K, and therefore, over L, we have $\sigma(c_\tau) = c_\tau$. Thus,

$$c_{\sigma\tau} f = c_\tau \sigma(f) = c_\tau c_\sigma f.$$

Since C is commutative, $\sigma\tau = \tau\sigma$ and

$$c_{\tau\sigma}(f) = c_{\sigma\tau}(f) = c_\tau c_\sigma f,$$

i.e.,

$$c_{\tau\sigma} = c_\tau c_\sigma, \quad \forall \tau, \sigma \in C.$$

In other words, the map

$$C \to \mathrm{End}_{\mathbb{Q}}(E')^*, \quad \sigma \mapsto c_\sigma$$

is a group homomorphism. Take any non-identity element σ of C. Then, $a := c_\sigma$ is a non-identity element of $\mathrm{End}_{\mathbb{Q}}(E')$, whose cube is the identity automorphism of E. Hence $\mathbb{Q}[a]$ is a $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}(E')$ that contains a nontrivial cube root of unity. Since $\mathrm{End}_{\mathbb{Q}}(E')$ is either $\mathbb{Q}$, or an imaginary quadratic field, we conclude that $\mathrm{End}_{\mathbb{Q}}(E')$ is isomorphic to $\mathbb{Q}(\sqrt{-3})$. Since E are E' are isogenous, the endomorphism algebra of E is also isomorphic to $\mathbb{Q}(\sqrt{-3})$. □

Theorem 3.6 (See [181, 191])**.** *Let $E = \mathbb{C}/\Lambda$ and $E' = \mathbb{C}/\Lambda'$ be elliptic curves, and let K be a finitely generated subfield of $\mathbb{C}$ such that*

$$g_2(\Lambda), g_3(\Lambda), g_2(\Lambda'), g_3(\Lambda') \in K.$$

Suppose that both polynomials $P_\Lambda(x)$ and $P_{\Lambda'}(x)$ are irreducible over K. Assume additionally that

(i) The Galois group $\mathrm{Gal}(P_\Lambda/K)$ *is* $\mathbf{A}_3$*;*

(i) The Galois group $\mathrm{Gal}(P_{\Lambda'}/K)$ *is* $\mathbf{S}_3$*.*

Then, E and E' are not isogenous.

Proof. First, notice that the splitting fields $K(E[2])$ and $K(E'[2])$ are *linearly disjoint* over K. Indeed, the Galois groups $\mathrm{Gal}(K(E[2])/K) = \mathbf{A}_3$ and $\mathrm{Gal}(K(E'[2])/K) = \mathbf{S}_3$ have no nontrivial isomorphic quotients. This implies that the intersection $K(E[2]) \cap K(E'[2]) = K$, and therefore, $K(E[2])$ and $K(E'[2])$ are linearly disjoint over K.

Claim 3.7. The natural action of $\mathrm{Gal}(K)$ on the $\mathbb{F}_2$-vector space $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$ is irreducible.

Let us continue with the proof and prove the claim later. Recall that there is the natural Galois-equivariant embedding of $\mathbb{F}_2$-vector spaces

$$\mathrm{Hom}(E, E')/2 \hookrightarrow \mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2]).$$

The irreducibility of $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$ implies that either $\mathrm{Hom}(E, E')/2 = \{0\}$, or the $\mathbb{F}_2$-vector spaces $\mathrm{Hom}(E, E')/2$ and $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$ are isomorphic. In the former case, $\mathrm{Hom}(E, E') = \{0\}$ and we are done. In the latter case, $\mathrm{Hom}(E, E')$ is a free $\mathbb{Z}$-module of rank 4 that contradicts the inequality from Theorem 2.29. This ends the proof. □

Proof of Claim 3.7. Let L be the compositum of the fields $K(E[2])$ and $K(E'[2])$ in $\bar{K}$. The *linear disjointness* of these fields means that the Galois group

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(K(E[2])/K) \times \mathrm{Gal}(K(E'[2])/K) = \mathbf{A}_3 \times \mathbf{S}_3.$$

It follows that the irreducibility of the representation of $\mathrm{Gal}(K)$ in $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$ is equivalent to the irreducibility of the representation of $\mathrm{Gal}(L/K)$ in $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$. In light of Claim 3.3, the $\mathrm{Gal}(K(E[2])/K)$-module $E[2]$ is simple and the $\mathrm{Gal}(K(E'[2])/K)$-module $E'[2]$ is absolutely simple. Now the irreducibility of the representation of $\mathrm{Gal}(L/K) = \mathrm{Gal}(K(E[2])/K) \times \mathrm{Gal}(K(E'[2])/K)$ in $\mathrm{Hom}_{\mathbb{F}_2}(E[2], E'[2])$ is a special case of the following elementary Lemma [181, Lemma 3.1] applied to

$$F = \mathbb{F}_2,\ H_1 = \mathrm{Gal}(K(E[2])/K),\ W_1 = E[2],\ H_2 = \mathrm{Gal}(K(E'[2])/K),\ W_2 = E'[2].$$

Lemma 3.8. *Let F be a field. Let $\tau_1 : H_1 \to \mathrm{Aut}_F(W_1)$ be an irreducible finite-dimensional representation of a group H_1 over F, and $\tau_2 : H_2 \to \mathrm{Aut}_F(W_2)$ be an absolutely irreducible finite-dimensional representation of a group H_2 over F. Then, the natural linear representation*

$$\tau_1^* \otimes \tau_2 : H_1 \times H_2 \to \mathrm{Aut}_F(\mathrm{Hom}_F(W_1, W_2))$$

of the group $H_1 \times H_2$ in the F-vector space $\mathrm{Hom}_F(W_1, W_2)$ is irreducible.

□

We already know from Theorem 2.31 the description of $\mathrm{End}_{\mathbb{Q}}(A)$ if A is isogenous to the product of elliptic curves with complex multiplication.

Let us assume now that $A = E_1 \times \cdots \times E_g$ is the product of g isogenous elliptic curves E_i with $\mathrm{End}(E_i) \cong \mathbb{Z}$..

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 the form $[d_{ij}] \circ \alpha_{ij}$ (which we denote, for brevity, by $d_{ij}\alpha_{ij}$) for some nonzero integer d_{ij} and a complex number α_{ij}.

We may assume that $\alpha_{ii} = 1$ and $\alpha_{ji} = \overline{\alpha_{ij}}$ for all $i, j = 1, \dots g$.

The analytic representation of an endomorphism $f : A \to A$ is given by a Hermitian 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 (2.24), the matrix of the Hermitian form H corresponding to L is equal to the matrix

$$M' = \mathrm{diag}[y_1^{-1}, \dots, y_g^{-1}] \cdot M \tag{3.14}$$

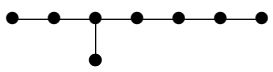
In particular, this implies that $y_i d_{ij} = y_j d_{ji}$.

Assume now that $E_1 = \dots = E_g = E$ 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 (2.25) 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 (3.14) that the matrix of the symplectic form corresponding to H in this basis is equal to (a_{ij}), where $a_{ij} = y^{-1}\mathrm{Im}(H(\gamma_i, \gamma_j))$. This gives

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

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

A classical result that goes back to Hermite asserts that a positive definite integral symmetric matrix of rank $g \le 7$ with determinant 1 can be reduced over $\mathbb{Z}$ to the identity matrix (see [91, p. 243–244]). By above, this implies that (up to an automorphism of A) 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 a positive definite symmetric matrix with determinant 1 that cannot be reduced to the identity matrix. This matrix is equal to $2I_8 - P_{\mathsf{E}_8}$, where P_{E_8} incidence matrix of the Dynkin diagram of type E_8:

E_8  (3.15)

Recall that this diagram describes the matrix by the following rule: all diagonal elements are equal to 2, and, after we order the set of vertices, the off-diagonal elements are equal to 0 or -1 according to whether two vertices are disjoint or incident.

Remark 3.9. It is known that the rank of any positive definite integral symmetric matrix with determinant 1 and even diagonal entries is divisible by 8 (see [148, 2.3]).

Thus, if E has no complex multiplication and a positive integer r is not divisible by 8, then the product of r copies of E does not admit a principal polarization such that the diagonal entries of the corresponding unimodular symmetric matrix are even.

Note that there is only one isomorphism class of even positive definite unimodular quadratic lattices of rank 16 not isomorphic to $\mathsf{E}_8 \oplus \mathsf{E}_8$ and there are 24 non-isomorphic such lattices of rank 24. One of them is the notorious *Leech lattice*. It is distinguished from the other even unimodular positive definite lattices of rank 24 by the property that the minimal value of its quadratic form is equal to 4. So we have 2 (resp. 24) distinguished principally polarized abelian varieties isomorphic to E^8 (resp. E^{12}), where E is an elliptic curve without complex multiplication.

Do they have any geometric meaning, for example, are they Prym varieties or Jacobian varieties?

Example 3.10. 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 form 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 the 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 $\mathbb{Z}[\mathbf{i}]$ by letting $\mathbf{i}$ act on M as the isometry ι. Since $\mathbb{Z}[\mathbf{i}]$ is a principal ideal domain, we get $M \cong \mathbb{Z}[\mathbf{i}]^k$ 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 $(\mathbf{i}, 1)$. Obviously, the abelian variety $A = \mathbb{C}^k/M$ becomes isomorphic to the product $E_{\mathbf{i}}^k$, where $E_{\mathbf{i}}$ is the elliptic curve with complex multiplication by $\mathbb{Z}[\mathbf{i}]$. On the other hand, if we take M to be an even unimodular[1] lattice of rank $2k$, then our Hermitian form H defines an indecomposable principal polarization. As we remarked earlier, such a lattice M exists 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 six ordinary nodes birationally isomorphic to the Kummer surface of the Jacobian of a curve of genus 2 (see [168]). Another remarkable property of A is that its

[1] A quadratic lattice is called *unimodular* if the natural homomorphism $M \to M^\vee$ defined by the associated symmetric bilinear form is bijective. Equivalently, the determinant of the symmetric matrix of the bilinear form in any basis is equal to ± 1.

indecomposable principal polarization, considered as an irreducible divisor in A, has the maximal possible number of singular points (equal to 10) for a simple abelian variety of dimension 4, which is not isomorphic to the Jacobian variety of a hyperelliptic curve (see [34]).

The automorphism group $\mathrm{Aut}(A) = \mathrm{End}(A)^\times$ of the abelian variety A, which can be called the *E_8-abelian variety* was computed by J.-P. Serre (in a letter of September 16 1986 to R. Valley). It is isomorphic to the group $G = 2^6 \rtimes \mathfrak{S}_6$, the semi-direct product of the elementary abelian group 2^6 of rank 6 and the symmetric group $\mathfrak{S}_6$ that acts in 2^6 via its permutation representation on the set of subsets of $\{1, \dots, 6\}$ of even cardinality modulo taking the complementary subset. We leave it to the reader to prove that this group is naturally isomorphic to the group $\mathrm{Sp}(4, \mathbb{F}_2)$ of automorphisms of the symplectic linear space $\mathbb{F}_2^4$ equipped with the standard symplectic form $\sum x_i y_i$.

It is known that the group G can be realized as a group of automorphisms of the three-dimensional variety X isomorphic to the double cover of $\mathbb{P}^3$ ramified over the Weddle quartic surface. It admits a nonsingular birational model, which is a Fano variety with the intermediate Jacobian isomorphic, as a polarized abelian variety, to the E_8-abelian variety [**?**].

This follows from the classical fact that the index two subgroup G' of G isomorphic to $2^5 \rtimes \mathfrak{S}_6$ (isomorphic to the Weyl group $W(D_6)$ of the root system of type D_6) acts by projective transformations in $\mathbb{P}^3$ leaving invariant the Weddle quartic surface [24, p. 117] (see [44, p. 128], or [43] for a modern exposition).

3.4 Intersection Theory on an Abelian Surface

In what follows, we will freely use the following results about the intersection numbers $X \cdot Y$ of divisors X and Y on a two-dimensional abelian variety, (an *abelian surface* A. We will prove them at the end of this section.

Claim 3.11. Let A be an abelian surface.

(i) The local intersection index of two distinct elliptic curves in A at any common point is 1. So, their (global) intersection number is just the number of common points, each of which is counted with multiplicity one.

(ii) The intersection number of two effective divisors on A is always a nonnegative integer.

(iii) If the intersection number of two irreducible curves on A is 0, then they both are elliptic curves and one of them is obtained from another one by a translation.

(iv) Let X be an irreducible curve on A and E is an elliptic curve on A. If their intersection number $X \cdot E = 1$ then X is an elliptic curve, and A is biregular to the product $X \times E$ [174].

(v) Let C be an effective divisor on A that is a sum of two elliptic curves E_1 and E_2 with $E_1 \cdot E_2 = 1$. Suppose that E is an elliptic curve on A such that $C \cdot E > 1$.

Then,

$$E_1 \cdot E \geq 1, \; E_2 \cdot E \geq 1.$$

Example 3.12. Following [69], let us give an example of the Jacobian of a curve of genus 2 isomorphic to the product of two isomorphic elliptic curves. Let d be a square-free positive integer and $K = \mathbb{Q}(\sqrt{-d})$ be the corresponding 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 $\mathfrak{a}$ in $\mathfrak{o}$. For example, we can take $d = 5$. 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 $(2, 1+\omega)$. In fact, the norm ideal $\mathrm{Nm}(\mathfrak{a}) \neq \mathbb{Z}$ of $\mathbb{Z}$ is generated by all integers $\mathrm{Nm}((a + b(1+\omega))$ (with $a, b \in \mathbb{Z}$). In particular, $\mathrm{Nm}(\mathfrak{a})$ contains $\mathrm{Nm}(2) = 4$ and $\mathrm{Nm}(1+\omega) = 6$ and therefore contains $2\mathbb{Z}$.

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 ϕ, which is also an elliptic curve in the *abelian surface*

$$A := E \times E.$$

Let $E_1 = E \times \{0\}, E_2 = \{0\} \times E$, and Δ be the diagonal in the abelian surface A - all three of them are elliptic curves isomorphic to E. Let us compute the intersection numbers $E' \cdot E_i, i = 1, 2, 3$.

Let $x + \mathfrak{o} \in E$ with $x \in \mathbb{C}$. If $\phi(x + \mathfrak{o}) \in E_1$, then $x(1+\omega) \in \mathfrak{o}$, hence there exists $m, n \in \mathbb{Z}$ such that

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

This shows that there are three intersection points $(0,0), \left(\frac{1-\omega}{3}, 0\right), \left(\frac{2(1-\omega)}{3}, 0\right)$. This implies that

$$E' \cdot E_1 = 3.$$

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

$$E' \cdot E_2 = 2.$$

If $\phi(x + \mathfrak{o}) = (2x + \mathfrak{o}, (1+\omega)x + \mathfrak{o}) \in \Delta$, 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 three intersection points $(0,0), \left(\frac{1+\omega}{3}, \frac{1+\omega}{3}\right), \left(\frac{2(1+\omega)}{3}, \frac{2(1+\omega)}{3}\right)$, and

$$E' \cdot \Delta = 3.$$

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 the Riemann-Roch theorem for abelian varieties [127, Sect. 16] applied to the abelian surface A, the *Euler characteristic* of the invertible sheaf $\mathcal{O}_A(C)$ is given by the formula

$$1 = \frac{1}{2!}C^2 = \dim_{\mathbb{C}} \mathrm{H}^0(A, \mathcal{O}_A(C)) - \dim_{\mathbb{C}} \mathrm{H}^1(A, \mathcal{O}_A(C)) + \dim_{\mathbb{C}} \mathrm{H}^2(A, \mathcal{O}_A(C)). \qquad (3.16)$$

Since the canonical class of the abelian variety A is trivial, it follows from Serre's Duality that $\dim_{\mathbb{C}} \mathrm{H}^2(A, \mathcal{O}_A(C)) = \dim_{\mathbb{C}} \mathrm{H}^0(A, \mathcal{O}_A(-C))$. Now (3.16) implies that

$$1 = \dim_{\mathbb{C}} \mathrm{H}^0(A, \mathcal{O}_A(C)) - \dim_{\mathbb{C}} \mathrm{H}^1(A, \mathcal{O}_A(C)) + \dim_{\mathbb{C}} \mathrm{H}^0(A, \mathcal{O}_A(-C)) \leq$$

$$\dim_{\mathbb{C}} \mathrm{H}^0(A, \mathcal{O}_A(C)) + \dim_{\mathbb{C}} \mathrm{H}^2(A, \mathcal{O}_A(C)),$$

and therefore, either $\mathrm{H}^0(A, \mathcal{O}_A(C)) \neq \{0\}$, and hence, the linear equivalence class of C is effective, or $\mathrm{H}^0(A, \mathcal{O}_A(-C)) \neq \{0\}$, and hence the linear equivalence class of $-C$ is *effective*. Taking into account that $C \cdot \Delta = 2$ is a positive integer and Δ is an effective divisor; we conclude that the class of $-C$ is *not* effective. Hence, the class of C is effective. Let D be an effective divisor on A that is linearly equivalent to C. Since $D^2 = C^2 = 2$, the theorem of Riemann-Roch [127, Sect. 16] implies that the invertible sheaf $L = \mathcal{O}_A(D)$ satisfies the conditions

$$\chi(L) = 1,\ \mathrm{H}^0(A, L) \neq 0,\ \deg(\phi_L) = \chi(L)^2 = 1.$$

Since $\deg(\phi_L) = 1$, ϕ_L is an isomorphism. Since $\mathrm{H}^0(A, L) \neq \{0\}$, it follows from the vanishing theorem of [127, Sect. 16] that the index $i(L) = 0$. By Corollary from [127, Sect. 16], the Hermitian form attached to L is positive-definite, i.e., the class of D is a principal polarization on A. Since $D^2 = 2$, it follows that D is a curve of arithmetic genus 2, by the adjunction formula (recall that the canonical class of A is zero). If D is irreducible, then it is a nonsingular curve of genus 2 [2] and $A \cong \mathrm{J}(D)$ [174, Satz 2].

If the divisor D is reducible, then it follows from Claim 3.11 that D is a sum $C_1 + C_2$ of two elliptic curves C_1 and C_2m and $A = C_1 \times C_2$, where we identify C_1 with $C_1 \times \{0\}$ and C_2 with $\{0\} \times C_2$ [174, Satz 2]. Then,

$$C_1 \cdot C_2 = 1.$$

Recall that

$$C \cdot \Delta = 2 > 1,\ C \cdot E_1 = 3 > 1.$$

In light of Claim 3.11(vi),

$$C_1 \cdot \Delta \geq 1, C_2 \cdot \Delta \geq 1;\ C_1 \cdot E_1 \geq 1, C_2 \cdot E_1 \geq 1.$$

This implies that

$$C_1 \cdot \Delta = 1,\ C_2 \cdot \Delta = 1$$

and the sum

$$3 = C \cdot E_1 = C_1 \cdot E_1 + C_2 \cdot E_1$$

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

of two positive integers $C_1 \cdot E_1$ and $C_2 \cdot E_1$ is 3. Hence, precisely one of those summands is 1. We may assume that $C_1 \cdot E_1 = 1$.

So, C_1, intersects Δ and E_1 with multiplicity 1. We have $C_2 = D - C_1 \sim 2\Delta + E' + E_1 - 2E_2 - C_1$. Intersecting with C_1, we get $1 = 4 - 2(E_2 \cdot C_1)$, a contradiction.

Proof of Claim 3.11. We write $[-1]$ for the negation map

$$[-1] : A \to A,\ a \mapsto -a$$

on A. For each $b \in A$, we write t_b for the corresponding translation map

$$t_b : A \to A,\ a \mapsto a + b$$

on A.

(i) Using translations in A, we may assume that two distinct elliptic curves $E_1, E_2 \subset A$ meet at 0_A. We need to check that they meet there transversally. Let $A = \mathbb{C}^2/\Gamma$ where Γ is a discrete lattice in $\mathbb{C}^2$ of rank 4. Then

$$E_1 = W_1/(\Gamma \cap W_1),\ E_2 = W_2/(\Gamma \cap W_2)$$

where W_1 and W_2 are *distinct* one-dimensional complex vector subspaces in $\mathbb{C}^2$ such that $\Gamma \cap W_j$ is a discrete lattice of rank 2 in W_j for $j = 1, 2$. Since W_1 and W_2 meet transversally at $(0, 0) \in \mathbb{C}^2$, the curves E_1 and E_2 meet tranversally at $(0, 0) + \Gamma = 0_A$.

(ii) It suffices to check that if C_1, C_2 are irreducible curves in A, then $C_1 \cdot C_2 \geq 0$. Using a suitable translation in A, we may assume that $C_1 \neq C_2$, and therefore, C_1 meets C_2 only at finitely many points (if any). This implies that $C_1 \cdot C_2 \geq 0$.

(iii) If $C_1 \cdot C_2 = 0$, then $C_1 = C_2 = C$. We may also assume that C contains 0_A. If $P \in C$, then $(C + P) \cdot C = C \cdot C = 0$ and therefore C is invariant under translation by every $c \in C$. Similarly, $(C - c) \cdot C = C \cdot C = 0$ and therefore C is invariant under translation by $-c$ for every $c \in C$. So, if G is a closed connected algebraic subgroup of A generated by C, then G acts transitively on C by translations. This implies that either $G = A$ or G is an elliptic curve that contains C. Since C is a curve, $G \neq A$, and therefore, C is a curve in the elliptic curve G. By dimension arguments, $C = G$.

(iv) Using translations in A, we may assume that 0_A is the only common point of X and E. This implies that every point x of X is the only common point of the curves X and $t_x(E)$. Notice also that

$$[-1]E = E.$$

Since

$$1 = E \cdot X = t_x(E) \cdot X,$$

x is a nonsingular point of X, and hence, the curve X is smooth. Since X lies on the abelian surface A, it is not rational. [3] Since the canonical class K_A is equal too ero, the adjunction formula implies that $C^2 \geq 0$, and $C^2 = 0$ if and only if C is a smooth elliptic curve.

[3] A morphism of a rational curve C to a complex torus $T = \mathbb{C}^g/\Lambda$ can be composed with the normalization morphism $\tilde{C} \to C$, and then lifted to a holomorphic map of the universal covers $\mathbb{P}^1(\mathbb{C}) \to \mathbb{C}^g$. The latter map is obviously a constant map.

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 the restriction of the intersection form to $\mathrm{Amp}(A)$.

Let us consider the regular map:

$$s : X \times E \to A,\ (x, e) \mapsto x + e$$

defined by the group law on A. Since both X and E are projective irreducible, the image $s(X)$ is an irreducible closed subset of the surface A that contains two distinct irreducible curves X and A. Hence, the image is of dimension two, hence it coincides with A. This means that s is surjective, i.e., for each $a \in A$ there are exist $x \in X$ and $e \in E$ such that

$$a = x + e.$$

This innocently looking equality actually means that for each $a \in A$ there exist $x \in X$ and $e \in E$ such that

$$t_a([-1]X) \ni a - x = e \in E \cap t_a([-1]X);\ t_a([-1]E) \ni a - e = x \in t_a([-1]E) \cap X.$$

Taking into account that

$$t_a([-1]X) = [-1]X \cdot E = X \cdot [-1]E = X \cdot E = 1;$$

$$t_a([-1]E) \cdot X = [-1]E \cdot X = E \cdot X = 1,$$

we conclude that such a pair (x, e) is *unique* for any given $a \in A$.

This implies that $s : X \times E \to A$ is a birational regular map of smooth projective varieties. Therefore, the dimensions of the linear spaces of regular 1-forms (differentials of the first kind) on A and $X \times E$ coincide, i.e.,

$$2 = \dim(A) = 1 + g,$$

which means that $g = 1$, i.e., X is an elliptic curve. Take $0_A \in X$ as the zero of group law on X. Then, the surjective regular map $s : X \times E \to A$ sends the zero $(0_X, 0_E)$ of $X \times E$ to the zero of A, hence it is an isogeny of abelian surfaces that is *bijective*, i.e., $\deg(S) = 1$. This implies that s is a biregular isomorphism. Hence, A is biregular to $X \times E$. This ends the proof.

(v) Suppose that, say, $E_1 \cdot E = 0$. This means that E is a translation of E_1, and therefore,

$$1 < C \cdot E = C \cdot E_1,$$

i.e.,

$$C \cdot E_1 > 1.$$

However,

$$C \cdot E_1 = (E_1 + E_2) \cdot E_1 = E_1^2 + E_1 \cdot E_2 = 0 + 1 = 1,$$

which contradicts the previous inequality. This contradiction proves that

$$E_1 \cdot E \geq 1.$$

□

Chapter 4

Humbert surfaces

In this chapter, we will study polarized abelian surfaces such that $\mathrm{End}_{\mathbb{Q}}(A)$ contains a real quadratic number field K such that all its elements of K are invariant under the corresponding Rosati involution. We also assume that $\mathrm{End}(A)$ contains a fixed order of K with discriminant Δ. . They form a closed subvariety of codimension one in the moduli space of polarized abelian surfaces which is called a *Humbert surface*.

4.1 The Singular Equation

Let A be an *abelian surface*. The Poincaré duality equips the group $\mathrm{H}^2(A,\mathbb{Z}) = \mathbb{Z}^6$ with a structure of a unimodular even quadratic lattice of signature $(3,3)$. By Milnor's theorem, $\mathrm{H}^2(A,\mathbb{Z}) \cong U \oplus U \oplus U$, 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 [120, Chapter 2], [148, Chapter 5]. Let $T(A)$ be the orthogonal complement of $\mathrm{NS}(A)$ in $\mathrm{H}^2(A,\mathbb{Z})$. By Hodge's Index Theorem, the signature of $\mathrm{NS}(A)$ is equal to $(1,\rho-1)$, where ρ is the Picard number of A. Since the signature of $H^2(A,\mathbb{Z})$ is equal to $(3,3)$, the signature of $T(A)$ is equal to $(2,4-\rho)$. Tensoring by $\mathbb{Q}$, we get an orthogonal decomposition of quadratic lattices

$$\mathrm{H}^2(A,\mathbb{Q}) = \mathrm{NS}(A)_{\mathbb{Q}} \oplus T(A)_{\mathbb{Q}}.$$

The quadratic form on $\mathrm{NS}(A)$ is defined by the intersection theory of curves on an algebraic surface.

It follows from the Hodge decomposition (1.3) that

$$1 \leq \rho(A) \leq 4.$$

Using Table 2.1, we describe possible type of the endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(A)$.

1. A is simple.

   (i) $\rho(A) = 1$: $n = e = e_0 = 1$ and $\mathrm{End}(A) \cong \mathbb{Z}$.

(ii) $\rho(A) = 2$: $n = 1, e = e_0 = 2$, and $\mathrm{End}_{\mathbb{Q}}(A)$ is a real quadratic field.

(iii) $\rho(A) = 2$: $n = 1, e_0 = 2, e = 4$, and A has a complex multiplication.

(iv) $\rho(A) = 3$: $n = 2, e = e_0 = 1$, and A is totally indefinite quaternion algebra over $\mathbb{Q}$.

2. A is not simple and hence isogenous to the product $E_1 \times E_2$ of two elliptic curves.

(i) $\rho(A) = 2$: E_1 is not isogenous to E_2.

(ii) $\rho(A) = 3$: E_1 is isogenous to E_2, $\mathrm{End}(E_1) \cong \mathrm{End}(E_2) \cong \mathbb{Z}$.

(iii) $\rho(A) = 4$: $A \cong E \times E$, $\mathrm{End}_{\mathbb{Q}}(E)$ is a totally imaginary quadratic field.

Let

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

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 (2.25). Since f is symmetric, N satisfies (2.27). We easily obtain that

$$\begin{pmatrix} N_1 & N_3 \\ N_2 & N_4 \end{pmatrix} = \begin{pmatrix} a_1 & na_2 & 0 & nb \\ a_3 & a_4 & -b & 0 \\ 0 & nc & a_1 & na_3 \\ -c & 0 & a_2 & a_4 \end{pmatrix}.$$

By (2.25) and (2.26), we have

$$M = (Z \cdot N_3 + \mathsf{D}N_4)\mathsf{D}^{-1}, \quad M \cdot Z = Z \cdot N_1 + \mathsf{D} \cdot N_2,$$

and

$$(Z \cdot N_3 + \mathsf{D} \cdot N_4) \cdot \mathsf{D}^{-1} \cdot Z = \tau N_1 + \mathsf{D} \cdot N_2.$$

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

$$\begin{pmatrix} 0 & b(-z_2^2 + z_1 z_3) \\ b(z_2^2 - z_1 z_3) & 0 \end{pmatrix} + \begin{pmatrix} a_1 z_1 + a_3 z_2 & a_1 z_2 + a_3 z_3 \\ na_2 z_1 + a_4 z_2 & na_2 z_2 + a_4 z_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 z_1 + a_3 z_2 & b(-z_2^2 + z_1 z_3) + a_1 z_2 + a_3 z_3 \\ b(z_2^2 - z_1 z_3) + na_2 z_1 + a_4 z_2 & +na_2 z_2 + a_4 z_3 \end{pmatrix}.$$

The right-hand side is equal to

$$\begin{pmatrix} a_1 z_1 + a_3 z_2 & na_2 z_1 + a_4 z_2 + nc \\ a_1 z_2 + a_3 z_3 - nc & na_2 z_2 + a_4 z_3 \end{pmatrix}.$$

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

$$b(z_2^2 - z_1 z_3) + a_2 n z_1 + (a_4 - a_1) z_2 - a_3 z_3 + nc = 0.$$

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

$$naz_1 + bz_2 + cz_3 + d(z_2^2 - z_1 z_3) + ne = 0. \tag{4.1}$$

We also assume that $(a, b, c, d, e) = 1$. In this new notations, the matrix $N_0 = N - a_1 I_4$ representing $(f_0)_r = (f - a_1 \mathrm{id})_r$ can be rewritten in the form

$$N_0 = -a_1 I_4 + N = \begin{pmatrix} 0 & na & 0 & nd \\ -c & b & -d & 0 \\ 0 & ne & 0 & -nc \\ -e & 0 & a & b \end{pmatrix}. \tag{4.2}$$

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

$$M_0 = \begin{pmatrix} -dz_2 & dz_1 - c \\ -dz_3 + na & dz_2 + b \end{pmatrix}. \tag{4.3}$$

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 and f_0 generate a subalgebra $\mathfrak{o}$ of rank 2 of $\mathrm{End}^s(A)$ isomorphic to

$$\mathfrak{o} \cong \mathbb{Z}[t]/(t^2 - bt + n(ac + ed)). \tag{4.5}$$

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

$$\Delta = b^2 - 4n(ac + ed). \tag{4.6}$$

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

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

$$\Delta > 0. \tag{4.7}$$

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

Note that, replacing t with $t + \alpha$, we may assume that $b = 0$ if b is even, or $b = 1$, otherwise. Suppose that there is a holomorphic line bundle L_Δ, whose algebraic equivalence class is mapped to f_0 inder $\alpha : \mathrm{NS}(A) \to \mathrm{End}^s(A)_{\mathbb{Q}}$. (Such a bundle exists for all $f_0 \in n\mathrm{End}^s(A)$.)

Applying (2.29), we obtain that

$$(L_0, L_\Delta) = nb = \tfrac{1}{2}(L_0^2)b, \quad (L_\Delta^2) = \tfrac{1}{2}n(b^2 - \Delta). \tag{4.8}$$

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

Recall that a finite algebra R over $\mathbb{Z}$ of degree n can be considered as a quadratic lattice with associated symmetric bilinear form defined by

$$(x, y) = \mathrm{Tr}(xy), \tag{4.9}$$

where $\mathrm{Tr} : R \to \mathbb{Z}$ is the $\mathbb{Z}$-linear function whose value on an element $x \in R$ is equal to the trace of the endomorphism $\alpha_x : r \mapsto xr$ (the coefficient at $(-\lambda)^{n-1}$ in the characteristic polynomial). The discriminant of the corresponding quadratic form is called the *discriminant* of R (the last coefficient of the characteristic polynomial of α_x).

In our case, when $R = \mathfrak{o}$ from (4.5), we take the basis $(1, \bar{t})$ of $\mathfrak{o}$, where $\bar{t}$ is the coset of t, and obtain that the matrix of the bilinear form (4.9) is equal to

$$\begin{pmatrix} 2 & -b \\ -b & b^2 - n(ac + ed) \end{pmatrix} = \begin{pmatrix} 2 & -b \\ -b & \frac{1}{2}(b^2 - \Delta) \end{pmatrix}.$$

Comparing this with the sublattice $\langle L_0, L_\Delta \rangle$ of $\mathrm{NS}(A)$, we obtain that there is an isomorphism of quadratic lattices

$$\langle L_0, L_\Delta \rangle \cong \mathfrak{o}(n), \tag{4.10}$$

where (n) means that we multiply the values of the quadratic form by n.

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

$${}^t N_0 \cdot J_D = \begin{pmatrix} 0 & na & 1 & nd \\ -c & b & -d & n \\ -1 & ne & 0 & -nc \\ -e & -n & a & b \end{pmatrix}. \tag{4.11}$$

Let $\mathcal{A}_{2,n} = \mathfrak{H}_2/\mathrm{Sp}(J_\mathsf{D}, \mathbb{Z})$ be the coarse moduli space of abelian surfaces with polarization of type $(1, n)$. We denote by $\mathcal{H}_\Delta$ the set of period matrices $Z \in \mathfrak{H}_2$ satisfying a singular modular equation with discriminant Δ. Let

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

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 $\mathrm{End}(A)$. It is called the *Humbert surface* of discriminant Δ.

Suppose $Z \in \mathcal{H}_\Delta$ and let $Z' = M \cdot Z$ for some $M \in \mathrm{Sp}(4, \mathbb{Z})$. If Z satisfies a singular equation (4.1), then the matrix N_0 defining an endomorphism of $\mathbb{C}^2/\Lambda_\tau$ changes to ${}^t M^{-1} \cdot N_0 \cdot M$ ([106], 8.1). Thus, Z' 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 4.1. *Every irreducible component of the Humbert surface* $\mathrm{Hum}_n(\Delta)$ *is equal to the image in* $\mathfrak{H}_2/\mathrm{Sp}(J_D, \mathbb{Z})$ *of the surface given by the equation*

$$nz_1 + bz_2 + cz_3 = 0, \tag{4.12}$$

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

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

Consider the quadratic $\mathbb{Z}$-algebra $\mathfrak{o}$ from (4.5). Let $K = \mathfrak{o} \otimes \mathbb{Q}$. If Δ is not a square, then K is a real quadratic extension of $\mathbb{Q}$. Let $\Delta = m^2\Delta_0$, where Δ_0 is square-free. Then, $K = \mathbb{Q}(\sqrt{\Delta_0})$. If m is odd, then the order $\mathfrak{o}$ is generated by 1 and $\frac{1}{2}m(1+\sqrt{\Delta_0})$. If m is even, then $\mathfrak{o}$ is generated by 1 and $m\sqrt{\Delta_0}$ if $\Delta_0 \equiv 2, 3 \mod 4$, and by 1 and $\frac{1}{2}m(1+\sqrt{\Delta_0})$ otherwise. Note that the *discriminant* of the order $\mathfrak{o}$ is equal to Δ.

Let $\sigma_1, \sigma_2 : K \to \mathbb{R}$ be two distinct embeddings of K into the field $\mathbb{R}$ of real numbers.

If $\Delta = k^2$ is a square, then $\mathfrak{o} = \mathbb{Z}[\omega]$ is just an order in $K = \mathfrak{o} \otimes \mathbb{Q} = \mathbb{Q} \oplus \mathbb{Q}$. Under the isomorphism

$$\mathfrak{o}_{\mathbb{Q}} \to \mathbb{Q} \oplus \mathbb{Q},\ x + y\omega \mapsto (x + y\alpha_+, x + y\alpha_-),$$

where $\alpha_\pm = \frac{1}{2}(b \pm k)$, the order $\mathfrak{o}$ becomes isomorphic to an order in $\mathbb{Z} \oplus \mathbb{Z}$. We denote by σ_1, σ_2 be the projections from $K \otimes \mathbb{R} \cong \mathbb{R} \oplus \mathbb{R} \to \mathbb{R}$.

Let $\mathrm{SL}_2(\mathfrak{o})$ be the group of 2×2 matrices with determinant 1 and entries in $\mathfrak{o}$. Consider its action on the product $\mathfrak{H} \times \mathfrak{H}$ of the upper-half planes

$$(z_1, z_2) \mapsto \left(\frac{\sigma_1(\alpha)z_1 + \sigma_1(\gamma)}{\sigma_1(\beta)z_1 + \sigma_1(\delta)}, \frac{\sigma_2(\alpha)z_1 + \sigma_2(\gamma)}{\sigma_2(\beta)z_1 + \sigma_2(\delta)}\right).$$

Let $R = \begin{pmatrix} 1 & -\frac{1}{2}(b-\sqrt{\Delta}) \\ -1 & \frac{1}{2}(b+\sqrt{\Delta}) \end{pmatrix}$. Write Δ in the form $\Delta = b^2 - 4nc$. Consider the map

$$\mathfrak{H} \times \mathfrak{H} \to \mathfrak{H}_2,\ (z_1, z_2) \mapsto {}^tR \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} R.$$

Then, the image of the map is equal to the set of matrices $\left(\begin{smallmatrix} w_1 & w_2 \\ w_2 & w_3 \end{smallmatrix}\right) \in \mathfrak{H}_2$ satisfying equation (4.12).

Let $\Phi : \mathrm{SL}_2(\mathfrak{o}) \mapsto \mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ be the homomorphism of groups defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} {}^tR & 0 \\ 0 & R^{-1} \end{pmatrix} \cdot \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix} \cdot \begin{pmatrix} {}^tR^{-1} & 0 \\ 0 & R \end{pmatrix}.$$

One checks that the map $\mathfrak{H}^2 \to \mathfrak{H}_2$ is equivariant with respect to the action of $\mathrm{SL}_2(\mathfrak{o})$ on $\mathfrak{H}^2$, and the action of $\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ on $\mathfrak{H}_2$. This defines a morphism

$$\Phi : \mathrm{SL}_2(\mathfrak{o})\backslash\mathfrak{H}^2 \to \mathrm{Hum}_n(\Delta).$$

If $b \not\equiv 0 \mod n$, then the morphism Φ is of degree 1. Otherwise, Φ is of degree 2 and factors through the involution σ that switches the factors in $\mathfrak{H}^2$ (see [167], IX, Proposition 2.5).

The quotient $\mathrm{SL}_2(\mathfrak{o})\backslash\mathfrak{H}^2$ (resp. $(\mathrm{SL}_2(\mathfrak{o}), \sigma)\backslash\mathfrak{H}^2$) is a special case of a *Hilbert modular surface* (resp. *symmetric Hilbert modular surface*).

4.2 Δ 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 let $e(L_0')$ be the exponent of the (finite) kernel $\ker(\phi_{L_0'})$ of the isogeny $\phi_{L_0'} : B \to \hat{B}$. Then, there is an isogeny

$$\psi_{L_0'} = e(L_0')\phi_{L_0'}^{-1} : \hat{B} \to B$$

such that the composition

$$\psi_{L_0'} \circ \phi_{L_0'} : B \to \hat{B} \to B$$

is the multiplication by $e(L_0')$ in B.

Consider the composition

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

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 $\mathrm{H}_1(B, \mathbb{C}) \subset \mathrm{H}_1(A, \mathbb{C})$, and then, extending it to $\mathrm{H}_1(A, \mathbb{C})$ 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

$$g_\pm^2 = \pm k g_\pm, \quad g_+ \circ g_- = 0. \tag{4.13}$$

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

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

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 $A = \mathrm{J}(C)$ 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 $\mathrm{J}(C)$ via the Abel-Jacobi map. Since k is equal to the trace of the characteristic equation for g_+, formula (2.31) and the projection formula imply that

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

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

Thus, we obtain the following:

Theorem 4.2. *Suppose a period Z of $\mathrm{J}(C)$ 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 $q^* : E = \mathrm{J}(E) \to A = \mathrm{J}(C)$ is injective. We identify its image with E. Let $N : \mathrm{J}(C) \to \mathrm{J}(E) = E$ be the norm map (defined on divisors by taking q_*). Then, $N \cdot q^* : E \to E$ is the map $[k]$. Let $g = \mathrm{Nm}_E : A \to A$. 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 $\mathrm{J}(C)$ whose discriminant is equal to k^2.

Example 4.3. Assume that a period of $A = \mathrm{J}(C)$ 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

$$y^2 - f_6(x) = 0, \tag{4.14}$$

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 linear 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 motivations for the work of G. Humbert.

One may ask how to find whether a hyperelliptic curve given by equation (4.14) admits a degree two map onto an elliptic curve in terms of the coefficients of the polynomial f_6. The answer has been known since the 19th century. Let us explain it. First, let us put a 2-*level* on the curve by ordering 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 [41], we obtain that the following properties are equivalent:

- there exists an involution σ of $\mathbb{P}^1$ with orbits $(x_1, x_2), (x_3, x_4), (x_5, x_6)$;
- the lines $\overline{p_1, p_2}, \overline{p_3, p_4}, \overline{p_5, p_6}$ are concurrent;
- 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 $a_it_0 + b_it_1 + c_it_2 = 0$ are the equations of the three lines, then

$$D_{12,34,56} = \det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = \det \begin{pmatrix} 1 & x_1 + x_2 & x_1x_2 \\ 1 & x_3 + x_4 & x_3x_4 \\ 1 & x_5 + x_6 & x_5x_6 \end{pmatrix} = 0.$$

(see [41], 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 skew invariant* I_{15} of degree $6!/48 = 15$ in coefficients of the binary form.[1] Recall that the algebra of SL_2-invariants of binary forms of degree 6 is generated by *Clebsch invariants* $I_2, I_4, I_6, I_{10}, I_{15}$ (in Salmon's notation they are A, B, C, D, E) of degrees indicated in the subscript. These invariants satisfy a basic relation

$$I_{15}^2 = P(I_2, I_4, I_6, I_{10}), \tag{4.15}$$

where P is a weighted homogenous polynomial of degrees 15 explicitly given by the expression

$$P = \det \begin{pmatrix} \frac{1}{2}(I_2A_4 + 18A_6) & 4(A_2^2 + 3I_2A_6) & 2A_{10} \\ 4(2A_4^3 + 3I_2A_6) & 2A_{10} & 288(A_4^3 + 2I_2A_4A_6 + 9A_4^2) \\ 2A_{10} & 288(A_4^3 + 2I_2A_4A_6 + 9A_4^2) & 72(A_4A_{10} + 48A_4^2I_6 + 72I_2I_6^2) \end{pmatrix},$$

where

$$\begin{aligned} 12A_2 &= I_2^2 - 36A_4, \\ 216A_6 &= 108I_2I_4 + 54I_6, \\ 3125A_{10} &= 9D - 384I_2^5 + 12000I_2^2(I_2A_4 + 5A_6) - 75000A_4(I_2A_4 + 6A_6). \end{aligned}$$

Here D is the *discriminant* of a binary form of degree 6 . We have

$$-\frac{1}{2 \cdot 3^4} D = 3 \cdot 2^7 I_2^5 - 3 \cdot 2^4 \cdot 5^3 I_2^3 I_4 - 2^4 \cdot 5^4 I_2^2 I_6 + 150(I_2I_4^2 + I_4I_6) + 3^2 \cdot 5^5 I_{10}.$$

Remark 4.4. 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 [41], 9.4.5).

Remark 4.5. 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

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

[1] Its explicit formula occupies 14 pages of Salmon's book [144], Appendix.

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 $\Lambda_\pm \hookrightarrow \Lambda$ defines a homomorphism $E_\pm \to A$. Its kernel is equal to the torsion subgroup 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 order of the torsion subgroup is equal to d.

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 $k^2 = \Delta$.

There is a 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 $d^2\Delta$.

Remark 4.6. We know from Example 3.12 that the Jacobian variety $\mathrm{J}(C)$ 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. We obtain that the period matrix of A satisfies two singular equations with discriminants k_1^2 and k_2^2. There are 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 4.7. (see [129]). Consider the abelian variety A defined by the period matrix

$$\tau = \begin{pmatrix} z_1 & 1/k \\ 1/k & z_3 \end{pmatrix}. \tag{4.16}$$

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 $\mathrm{Ker}(p) \cap \Lambda = \mathbb{Z}(k\gamma_1 - e_2) + \mathbb{Z}e_1$. 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 $k\gamma_1 - e_2$. Also, one can embed E' in A via 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, this defines an isogeny $E \times E' \to A$ of degree k^2.

Example 4.8. Assume $k = 3$. Let $f : C \to E$ be a degree 3 map onto an elliptic curve E. Assume that $\mathrm{J}(C)$ 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 γ 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 induces an involution $\bar{\sigma}$ on E such that there is 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 general case; in a special case, we may have one ramification point of ramification index 3. Let x be one of the Weierstrass points, a fixed point of γ. We have $f(x) = f(\gamma(x)) = \bar{\gamma}(f(x))$. Thus, by taking $f(x)$ to be the origin of a group law on E, we may assume that $\bar{\gamma}$ 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 W of 6 Weierstrass points to the set $F = E^{\bar{\gamma}}$ of four fixed points $a_1, \dots, a_4$ of $\bar{\sigma}$. If a is one of the fixed points ,and $f(x) = a$, then $f(\gamma(x)) = a$, hence γ preserves the fiber $f^{-1}(a)$ (considered as an effective divisor of degree 3 on C). Since γ is of order 2, it must fix one of the points or the whole fiber. The latter case happens if one of the points of the fiber is a ramification point of f. Thus, the fibers of the map $W \to F$ have cardinalities $(3, 1, 1, 1)$, or $(2, 2, 1, 1)$. In the latter case, both ramification points of f are over four points from F. Let us consider the commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\phi} & \mathbb{P}^1 \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \bar{f}} \\ E & \xrightarrow{\bar{\phi}} & \mathbb{P}^1. \end{array} \tag{4.17}$$

In the case $(2, 2, 1, 1)$, the composition $\bar{\phi} \circ f : C \to \mathbb{P}^1$ has four branch points. On the other hand, the equal composition $f \circ \phi : C \to \mathbb{P}^1$ has at least six branch points because ϕ has 6 branch points. Therefore, the case $(2, 2, 1, 1)$ is not realized. Let us consider the case $(3, 1, 1, 1)$. Let us assume that $f^{-1}(a_1)$ consists of three points in W. Let $y_i = \bar{\phi}(a_i)$. The map $\bar{\phi} \circ f : C \to \mathbb{P}^1$ ramifies at each of the three pre-images of any point $y_i \in \bar{\phi}(F)$ with the ramification index equal to 2, and ramifies at two points over the image b in $\mathbb{P}^1$ of the two branch points of $C \to E$.

It follows from the commutative diagram (4.17) 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 this fiber is a ramification point.

Now, we see that the set of Weierstrass points W is the union of two disjoint 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 $a_1 = \{0\}$. Since $\mathrm{Ker}(\mathrm{J}(C) \to E) = \mathrm{Ker}(\mathrm{Nm} : \mathrm{J}(C) \to E)$ and $\mathrm{Nm}(x + y + z) = 0$, we obtain that $\{x + y + z\}$ is contained in 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.

So, we arrive at 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 [59] and H. Burhardt [20], a nice exposition of this can be found in [154].

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 a condition for a factorization $F(u, v) = \Phi(u, v)\Psi(u, v)$, 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 the pair of functions G, Φ. Its zeros 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 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 quartic binary form 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 $v^2\psi(u/v) = \Psi(u, v)$.

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

Using the projective transformations of (u, v), and a linear transformation of the linear space generated by G and 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.

One may ask about the description of the set of degree N covers $f : C \to E$ of a fixed elliptic curve E. To describe this set, one introduces a functor (the *Hurwitz functor*) that assigns to a scheme T the family of normalized T-covers $f : \mathcal{C}/T \to (E \times T)/T$ such that, for each $t \in T$, the cover $\mathcal{C}_t \to E \times \{t\}$ is a normalized degree N cover of a genus two curve.[3] By a result of E. Kani [84] this functor is represented by an open subscheme of the modular curve $X(N)$ of level N.

Finally, we refer to [20] and [154] for an explicit invariant of binary sextics defining the locus $\mathrm{Hum}(9)$. In [110], one can find a treatment of the case $k = 5$.

Remark 4.9. 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 of $P \hookrightarrow \mathrm{J}(C)$ such that the principal polarization of C induces a polarization of type $(e, \dots, e)$ on P. Prym-Tyurin varieties of exponent 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 (see Section 10.1). The associated Prym variety of exponent 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 $P \subset \mathrm{J}(C)$ and the principal polarization induces a polarization of type $(e, \dots, e)$ on P.

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

Let k be a positive integer and $X(k)$ be the compactification of $\Gamma(k)\backslash\mathfrak{H}$, where $\Gamma(k)$ is the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ i.e., $\Gamma(k)$ is the kernel of the natural *surjective* group homomorphism (the entry-wise reduction map modulo k)

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z}).$$

(See [170, Th. 28.2.6] for a proof of the surjectiveness). Then, $X(k)$ is called a *modular curve* of principal level k. Let

$$G_k = \mathrm{SL}_2(\mathbb{Z})/\Gamma(k) = \mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$$

be the quotient group. For $\epsilon \in (\mathbb{Z}/k\mathbb{Z})^*$ denote by α_ϵ the automorphism of G_k induced by the conjugation with the matrix $\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$. It sends the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$ to the matrix $\left(\begin{smallmatrix} a & \epsilon b \\ \epsilon^{-1}c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$. We define the diagonal modular surface

$$Z(k; \epsilon) := X(k) \times X(k)/G_k,$$

[3] A cover is normalized if it is not a composition of a cover $C \to E$ and an isogeny $E \to E$.

where G_k acts by $g \cdot (x, y) = (g(x), \alpha_\epsilon(g)(y))$.

The following theorem was proved by E. Kani [83].

Theorem 4.10. *Let $\tilde{Z}(k;\epsilon)$ be a minimal desingularization of $Z(k;\epsilon)$. It is a regular surface with Kodaira dimension $\min(2, p_{g,\epsilon})$, where $p_{g,\epsilon}$ is the geometric genus of the surface. We have*

(a) $\tilde{Z}(k;\epsilon)$ is a rational surface if and only if $k \leq 5$, or

$$(k, \epsilon) = (6, 1), (7, 1), (8, 1).$$

(b) $\tilde{Z}(k;\epsilon)$ is birationally elliptic K3 if and only if

$$(k, \epsilon) = (6, 5), (7, 3), (8, 3), (8, 5), (9, 1), (12, 1).$$

(c) $\tilde{Z}(k;\epsilon)$ is of Kodaira dimension 1 with $p_g = 2$ if and only if

$$(k, \epsilon) = (8, 7), (9, 2), (10, 1), (10, 3), (9, 1), (11, 1).$$

(d) $\tilde{Z}(k;\epsilon)$ is of general type with $p_g \geq 3$ if and only if $k \geq 13$, or

$$(k, \epsilon) = (11, 2), (12, 5), (12, 7), (12, 11).$$

Let $\mathcal{M}_g^{\text{ell}}(k)$ be the moduli space of curves of genus g that admit a finite map of degree k onto an elliptic curve. If $g = 2$, then any such curve admits two maps onto an elliptic curve, hence $\mathcal{M}_2^{\text{ell}}(k)$ is a double cover of the Humbert surface $\text{Hum}(k^2)$.

The following nice observation is due to E. Kani.

Theorem 4.11. *$\mathcal{M}_2^{\text{ell}}(k)$ is an open subvariety of of $Z(k, -1)$. In particular, it is rational if and only if $k \leq 5$, K3 if and only if $k = 6, 7$, elliptic if and only if $k = 8, 9, 10$, and it is of general type otherwise.*

Proof. Recall that a principally polarized abelian surface A defines a point in $\text{Hum}(k^2)$ if and only if there exists a pair of elliptic curves (E, E') on A such that $E \times E' \to A$ is an isogeny of degree k^2. Let U be an open subset of $\text{Hum}(k^2)$ of abelian surfaces for which such a pair of curves is unique. Let U' be its pre-image under the natural map $\mathcal{M}_2^{\text{ell}}(k) \to \text{Hum}(k^2)$. The canonical inclusions $\phi : E \cap E' \hookrightarrow E$ and $\phi' : E \cap E' \hookrightarrow E'$ define an isomorphism $\phi^{-1} \circ \phi' : E'[k] \to E[k]$. One can show that this isomorphism is compatible with the Weil pairing on E', and the Weil pairing multiplied by -1 on $E[k]$. If we fix a full k-level structure on E', i.e. an isomorphism of the standard symplectic group $(\mathbb{Z}/k\mathbb{Z})^2$ to $E'[k]$, then the composition with $\phi' \circ \phi^{-1}$ defines a full k-level structure on E. This defines a point in $X(k) \times X(k)$. To get rid of the levels, we have to consider the quotient of $X(k) \times X(k)$ by the group $G_k(-1)$. □

Corollary 4.12. *The Humbert surfaces $\text{Hum}(k^2)$ are rational for $k \leq 10$.*

Proof. If $Z(k;-1)$ is rational, then the quotient is rational. Suppose $Z(k;\epsilon)$ is birationally isomorphic to a K3 surface. The fixed locus of the rational cover involution $Z(k;-1) \to \mathrm{Hum}(k^2)$ consists of $G_k(-1)$-orbits of pairs $((E,\alpha),(E,\alpha^{-1}))$, where α is the full k-level. It is a curve R isomorphic to $X(k)$.

Let $\tilde{Z}(k;-1)$ be a resolution of singularities of $Z(k;-1)$. Suppose that there is a birational morphism from $\tilde{Z}(k;-1) \to Y$, where Y is a K3 surface Y or a relatively minimal elliptic surface of Kodaira dimensions one. The involution of Z(k;-1)$lifts to a birational involution of \tilde{Z}(k;-1)$. Since Y is a minimal surface of non-negative Kodaira dimension, it descends to a biregular involution of Y. It is known that a biregular involution of a K3 surface Y, which fixes point-wise a curve acts non-trivially on the one-dimensional space $\Omega^2(A)$ of regular differential 2-forms. It is easy to see that the quotient by such an involution must be a rational surface. If Y is of Kodaira dimension one, then the involution preserves the elliptic fibration, and, since $X(k)$ is not isomorphic to an elliptic curve, we obtain that it intersects the general fiber at 4 points. Since Y is nonsingular, the quotient is birationally isomorphic to a rational ruled surface. □

Remark 4.13. One should compare the previous result with known results about the rationality of Humbert surfaces $\mathrm{Hum}_n(\Delta)$, where D is square-free. For example, when $D = p \equiv 1 \mod 4$, it is known that the corresponding Hilbert modular surface is rational for $p = 5, 13, 17$, a K3 surface if $p = 29, 37, 41$ and an elliptic surface for $p = 53, 61, 73$ [72]. As before, one proves that the quotient by $\mathfrak{S}_2$ is rational for these primes.

Corollary 4.14. *Let* $\mathrm{Hum}(k^2)'$ *be the closed subvariety of* $\mathrm{Hum}(k^2)$ *parameterizing principally polarized abelian surfaces* A *for which there exists an isogeny* $E \times E \to A$ *of degree* k^2*. Then,* $\mathrm{Hum}(k^2)'$ *is a rational curve.*

Proof. It follows from the proof of the previous corollary that $\mathrm{Hum}(k^2)'$ is isomorphic to the quotient $X(k)/G_k \cong \mathbb{P}^1$. □

Remark 4.15. A recent thesis of Robert Auffarth [4] gives some conditions, in terms of the Néron-Severi group, for the existence of an elliptic curve on an abelian variety of arbitrary dimension.

We will see more examples of Humbert surfaces with square discriminant in Chapter 10.

4.3 Δ 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.

For any abelian variety A, the quotient space by the cyclic group generated by the involution $\iota = [-1]_A$ is denoted by $\mathrm{Kum}(A)$ and is called the *Kummer variety* associated to A. The fixed points of the involution ι are 2-torsion points of A. In local coordinates $z_1, \ldots, z_g$ at such a point, the involution acts as $z_i \mapsto -z_i$. Thus, the image of a 2-torsion point in $\mathrm{Kum}(A)$ is a singular point whose local ring is isomorphic to the local ring of the vertex of the affine cone over the second

Veronese variety V_2^{g-1}, the image of $\mathbb{P}^{g-1}$ in $\mathbb{P}^{\frac{1}{2}g(g+1)-1}$ under the Veronese map given by quadratic forms in $z_1, \ldots, z_g$.

Let A be a principally polarized abelian surface and let $\mathrm{Kum}(A)$ be the associated Kummer surface. Let L be a principal polarization of A. The involution ι is a symmetric endomorphism corresponding to L^{-1}. Then, ι^* acts on $\mathrm{H}^1(A, \mathbb{Z})$ as the multiplication by -1, hence its acts on $\mathrm{H}^2(A, \mathbb{Z})$ 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

$$\phi : A \to \mathrm{Kum}(A)$$

and a map $\psi : \mathrm{Kum}(A) \to X \subset \mathbb{P}^3$. If the polarization is irreducible, ψ is an isomorphism onto a quartic surface X. Otherwise, the map ψ is a degree 2 map onto a nonsingular quadric Q, with the branch divisor equal to the union of 8 lines, four from each ruling. Assume that the polarization L is irreducible. It follows from above that X has 16 singular points which are locally isomorphic to the singular point of a quadratic cone in $\mathbb{C}^3$, i.e. an ordinary double point. Then, $A \cong \mathrm{J}(C)$ 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 ι 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 $A/(\iota) = \mathrm{Kum}(A)$ which is a minimal resolution of the 16 nodes of $\mathrm{Kum}(X)$.

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

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 projection $\tilde{p}$ 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 Riemann-Hurwitz formula $K_{\tilde{A}} = \tilde{p}^*(K_{\tilde{X}}) + \sum R_i'$ implies that $K_{\tilde{X}} = 0$. Since $\tilde{\iota}$ acts on $\mathrm{H}^1(\tilde{A}, \mathbb{Q})$ as -1, we obtain that $\mathrm{H}^1(\tilde{X}, \mathbb{Q}) \subset \mathrm{H}^1(\tilde{A}, \mathbb{Q})^{\tilde{p}} = \{0\}$ must be trivial. Thus, $b_1(\tilde{X}) = 0$, and we obtain that $\tilde{X}$ is a K3 usrace (see more about K3 surfaces in Lecture 9).

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

$$t_0^2 F_2(t_1, t_2, t_3) + 2t_0 F_3(t_1, t_2, t_3) + F_4(t_1, t_2, t_3) = 0, \tag{4.18}$$

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 see that X is birationally isomorphic to the double cover of $\mathbb{P}^2$ 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 $C_1, \dots, C_6$ 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 $\ell_1, \dots, \ell_6$. 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 $l_1, \dots, l_6$ are linear forms in variables x_1, x_2, x_3. The corresponding lines $\ell_1, \dots, \ell_6$ 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 touches each line.

Conversely, one can show that equation (4.18) 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.

In the following we will follow the paper of C. Birkenhake and H. Wilhelm [13]. Applying Lemma 4.1, we may assume that $b = 0, 1$ and $\Delta = b + 4m$. Recall from (4.8) 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

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

Applying (4.11), 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. $[-1]^*(L) = L$.[4] 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 [106], 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 sixteen 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 Riemann-Hurwitz formula applied to the map $\bar{D} \to \bar{C}$ gives

$$g(\bar{D}) = d + \frac{k-2}{2} = -1 + 2g(\bar{C}) + \frac{k-1+r}{2}, \tag{4.19}$$

where r is the number of ramification points over 0 (one can show that C is smooth outside $\phi(0)$, see [13], Proposition 6.3). We can obtain $\bar{D}$ by blowing up 0 and taking the proper inverse transform of D. The pre-image 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 (4.19) 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 $k - 1$ 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.[5]

[4] 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 $[-1]^*(L \otimes N) \cong L \otimes N$.

[5] 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 $2d + 1$.

Theorem 4.16. *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 4.17. *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 example is a special case considered by G. Humbert.

Example 4.18. 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).

It is easy to see that an abelian surface with real multiplication by $\mathbb{Q}(\sqrt{5})$ admits a principal polarization. A general such surface is the Jacobian of a curve C of genus 2. We may assume that its period τ satisfies a singular equation with $b = 1$. It follows from (4.7) that A admits a divisor class D with $D^2 = -2$ and $C \cdot D = 1$. Let $C' = C + D$ so that $C'^2 = 2$ and $C \cdot C' = 3$. The linear system $|C + C'|$ defines a map $A \to \mathbb{P}^4$ onto a surface of degree 10. An abelian surface of degree 10 in $\mathbb{P}^4$ was first studied by A. Comessatti [30]. We refer to [105] for a modern account of Comessatti's paper. There is a huge literature devoted to these surfaces, for example, exploring the relationship between such surfaces and the geometry of the *Horrocks-Mumford rank 2 vector bundle* over $\mathbb{P}^4$ whose sections vanish on Comessatti surfaces (see [75]).

Example 4.19. 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 rational 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 4.20. *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.*

Remark 4.21. It follows from the Teichmüller theory that any holomorphic differential on a Riemann surface X of genus g defines an immersion of $\mathfrak{H}$ in $\mathcal{M}_g$ such the image is a complex geodesic with respect to the Techmüller metric. According to C. McMullen [113], the closure of the image of $\mathfrak{H}$ in $\mathcal{M}_2$ is either a curve, or a Humbert surface $\mathrm{Hum}(\Delta)$, where Δ is not a square, or the whole $\mathcal{M}_2$.

Chapter 5

Fake Elliptic Curves

In this chapter, we will discuss *abelian surfaces of quaternion type*, also called abelian surfaces with *quaternion multiplication,* or QM-surfaces for short, and also called *fake elliptic curves* . These are simple abelian surfaces A with the ring $\mathrm{End}(A)$ isomorphic to an order in an indefinite quaternion algebra over $\mathbb{Q}$ (Type II in Table 2.1). We refer to some details to [103, Chapter IX] and some general properties of quaternion algebras to [58] or [170]. In what follows we will freely use the notation and results of Section 2.5.

5.1 Indefinite Quaternion Algebras

Let F be a subfield of $\mathbb{R}$. (We are mainly interested in the case when $F = \mathbb{Q}$ or $\mathbb{R}$.) Let $H = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over F. Throughout this chapter, we assume that it is totally indefinite. This is equivalent to that H splits over a real quadratic extension L/F with $L \subset \mathbb{R}$) and

$$\Phi_{\mathbb{R}} : H_{\mathbb{R}} := H \otimes_R \mathbb{R} \cong \mathrm{Mat}_2(\mathbb{R}).$$

We fix this isomorphism and get the corresponding F-algebra *embedding*

$$\Phi : H \hookrightarrow \mathrm{Mat}_2(\mathbb{R}),$$

which is the restriction of our isomorphism to $H = H \otimes 1 \subset H_{\mathbb{R}}$. Clearly, Φ uniquely determines $\Phi_{\mathbb{R}}$, namely

$$\Phi_{\mathbb{R}}(u \otimes r) = r \cdot \Phi(u) \; \forall u \in H, r \in \mathbb{R}.$$

Explicitly, H is totally indefinite if and only if only one of the numbers $a, b, -ab = \mathbf{K}^2$ is positive. By permuting $\mathbf{I}, \mathbf{J}, \mathbf{K}$, we may assume that $a > 0$. Then, H splits over $L = F(\sqrt{a})$, and we can write any $x \in H$ in the form

$$x = m + n\mathbf{J},$$

where $m = \alpha + \beta\mathbf{I},\ n = \gamma + \delta\mathbf{I}$ belong to L i.e., $\alpha, \beta, \gamma, \delta \in F$. One can choose the embedding Φ by

$$x \mapsto \begin{pmatrix} m & n \\ b\bar{n} & \bar{m} \end{pmatrix}.$$

It is determined by

$$\Phi(\mathbf{I}) = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad \Phi(\mathbf{J}) = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}.$$

We have

$$\mathrm{Nm}(x) := x\bar{x} = \det(\Phi_{\mathbb{R}}(x)) = m\bar{m} - bn\bar{n} = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2. \tag{5.1}$$

This shows that the anti-involution (called the *canonical involution*) $x \mapsto \bar{x}$ is not positive. To replace it with a positive anti-involution, we use the following:

Lemma 5.1. *Let $\rho \in H^* \setminus F$ with $\rho^2 \in F \setminus \{0\}$. Then, $x \mapsto x^* := \rho^{-1}\bar{x}\rho$ is an anti-involution of H. Every anti-involution of H is obtained in this way. Moreover, it is* positive, *i.e.,* $\mathrm{tr}(xx^*) > 0$, *for any $x \neq 0$, if and only if $\rho^2 < 0$.*

Proof. (see [103, Chapter IX, Theorem 1.4 and Theorem 2.3]). We have already checked in Prop. 2.26 that $x \mapsto x^*$ is an anti-involution.

To prove the second assertion, we use that the composition of two anti-involutions is an automorphism of H. According to the Skolem–Noether Theorem, an automorphism of a central simple algebra is an interior automorphism, i.e., $x \mapsto s^{-1}xs$ for some $s \in H^*$. This proves the second assertion.

Let us consider the quaternion algebra $H_{\mathbb{R}}$ over $\mathbb{R}$. As for the last assertion, let us prove that if $c := \rho^2 < 0$ then the anti-involution $x \to x^*$ is positive. Choosing a suitable isomorphism between $H_{\mathbb{R}}$ and $\mathrm{Mat}_2(\mathbb{R})$, we may assume that

$$H_{\mathbb{R}} = \mathrm{Mat}_2(\mathbb{R}), \quad \rho = \begin{pmatrix} c_2 & 0 \\ 0 & c_2 \end{pmatrix} \quad \text{where } 0 \neq c_2 = \sqrt{c} \in \mathbb{R}.$$

Then we get for each $x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R})$,

$$\mathrm{tr}(x) = \alpha + \gamma, \quad \bar{x} = \mathrm{tr}(x) - x = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix},$$

$$x^* = \begin{pmatrix} 0 & c_1 \\ -c_1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} 0 & c_1 \\ -c_1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix},$$

which is the transpose x^t of the matrix x. In other words, $x^* = x^t$. Since $\mathrm{tr}(xx^t)$ is positive for any non-zero real matrix x, we get the positiveness of the involution if $\rho^2 = c < 0$ on $H_{\mathbb{R}}$. In light of Remark 2.27, this implies the positiveness of the involution on H.

Now assume that $\rho^2 = c > 0$. In light of Remark 2.27, replacing F by $\mathbb{R}$ and H by $H_{\mathbb{R}}$, we may assume that $F = \mathbb{R}$. Choosing a suitable isomorphism between $H_{\mathbb{R}}$ and $\mathrm{Mat}_2(\mathbb{R})$, we may assume that

$$H = \mathrm{Mat}_2(\mathbb{R}), \quad \rho = \begin{pmatrix} c_2 & 0 \\ 0 & -c_2 \end{pmatrix} \quad \text{where } 0 \neq c_2 = \sqrt{c} \in \mathbb{R}.$$

If we put

$$x_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

then $\mathrm{tr}(x_0) = 0$, $\overline{x_0} = -x_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and

$$x_0^* = \begin{pmatrix} c_2 & 0 \\ 0 & -c_2 \end{pmatrix}^{-1} (-x_0) \begin{pmatrix} c_2 & 0 \\ 0 & -c_2 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = x_0.$$

This implies that

$$x_0 x_0^* = x_0^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

and therefore

$$\mathrm{tr}(x_0 x_0^*) = -2 < 0.$$

It follows that the obviously open (in the real topology) subset

$$X_- = \{x \in H_{\mathbb{R}} \mid \mathrm{tr}(xx^*) < 0\} \subset H_{\mathbb{R}}$$

is non-empty. On the other hand, we have

$$\mathbb{Q} \subset F \subset \mathbb{R}.$$

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, the (sub)field F is also dense in $\mathbb{R}$. It follows that H is everywhere dense in $H_{\mathbb{R}}$. This implies that the intersection of H and X_- is non-empty. Hence, our anti-involution on H is *not positive*. This ends the proof.

□

We will also need the following assertion that will be used in order to describe the Rosati involution on fake elliptic curves.

Proposition 5.2. *Let $\rho \in H^* \setminus F$ be an element of H with $\rho^2 \in F \setminus \{0\}$, and $x \mapsto u^* := \rho^{-1}\bar{u}\rho$ be the corresponding anti-involution of H. Then*

$$\mathrm{B}_{\mathrm{tr}}((\rho(ux), y) = \mathrm{B}_{\mathrm{tr}}(\rho x, u^* y) \quad \forall u, x, y \in H. \tag{5.2}$$

Proof. We have

$$\mathrm{B}_{\mathrm{tr}}((\rho(ux), y) = \mathrm{tr}(\rho u x \bar{y}) = \mathrm{tr}((\rho u)(x\bar{y})) = \mathrm{tr}((x\bar{y})(\rho u));$$

hence,

$$\mathrm{B}_{\mathrm{tr}}((\rho(ux), y) = \mathrm{tr}((x\bar{y})(\rho u)). \tag{5.3}$$

On the other hand, since $\bar{\rho} = -\rho$, we have

$$\mathrm{B}_{\mathrm{tr}}(\rho x, u^* y) = \mathrm{tr}\left(\rho x \overline{\rho^{-1}\bar{u}\rho y}\right) =$$

$$\mathrm{tr}\left(\rho x \bar{y}(-\rho) u(-\rho^{-1})\right) = \mathrm{tr}\left(\rho x \bar{y} \rho u \rho^{-1}\right) = \mathrm{tr}\left(x\bar{y}\rho u\right) = \mathrm{tr}\left((x\bar{y})(\rho u)\right).$$

Now (5.3) implies the desired equality. □

In what follows (unless otherwise stated) $F = \mathbb{Q}$ and $H = \left(\frac{a,b}{F}\right)$ is a quaternion $\mathbb{Q}$-algebra.

Following Proposition 2.26(v), let us consider

$$\mathcal{X}(H_{\mathbb{R}}) = \{\eta \in H_{\mathbb{R}} \mid \eta^2 = -1\}.$$

Then, the map

$$\mathcal{X}(H_{\mathbb{R}}) \ni \eta \mapsto J = \Phi_{\mathbb{R}}(\eta)\ \forall \eta \in \mathcal{X}(H_{\mathbb{R}})$$

is a bijection between $\mathcal{X}(H_{\mathbb{R}})$ and

$$\Phi_{\mathbb{R}}(\mathcal{X}(H_{\mathbb{R}})) = \{J \in \mathrm{Mat}_2(\mathbb{R}) \mid J^2 = -1\} = \mathcal{X}(\mathrm{Mat}_2(\mathbb{R})\} = \{J \in \mathrm{GL}(2,\mathbb{R}) \mid J^2 = -1\}.$$

(Later, we explain how to identify $\mathcal{X}(H_{\mathbb{R}})$ with $\mathbb{C} \setminus \mathbb{R}$.)

Definition 5.1. A *lattice* in H is an additive subgroup Λ of H that is a free $\mathbb{Z}$-module of rank $4 = \dim_{\mathbb{Q}} H$. Equivalently, an additive subgroup Λ of H is a lattice if and only if there is a basis $\{e_1, e_2, e_3, e_4\}$ of the $\mathbb{Q}$-vector space H such that

$$\Lambda = \mathbb{Z} \cdot e_1 + \mathbb{Z} \cdot e_2 + \mathbb{Z} \cdot e_3 + \mathbb{Z} \cdot e_4.$$

The determinant $\tilde{D}$ of the matrix $(\mathrm{B}_{\mathrm{tr}}(e_i, e_j))$ of the form B_{tr} with respect to $\{e_1, e_2, e_3, e_4\}$ is a nonzero rational number that does *not* depend on a choice of a basis of the $\mathbb{Z}$-module Λ. By Remark 2.43, $\tilde{D}$ is a square in $\mathbb{Q}$. Let us put $D\Lambda := \sqrt{\tilde{D}}$, which is a positive rational number that we call the discriminant of Λ.

Remark 5.3. Let Λ be a lattice in H. Then $\forall x \in H$ there exists a positive integer N such that $Nx \in \Lambda$. In addition, the natural homomorphisms of $\mathbb{Q}$-vector spaces

$$\Psi_{\Lambda,\mathbb{Q}} : \Lambda \otimes \mathbb{Q} \to H,\ \lambda \otimes r \mapsto r\lambda\ \forall \lambda \in \Lambda, r \in \mathbb{Q}$$

and of $\mathbb{R}$-vector spaces

$$\Psi_{\Lambda,\mathbb{Q}} : \Lambda \otimes \mathbb{R} \to H_{\mathbb{R}},\ \lambda \otimes r \mapsto r\lambda\ \forall \lambda \in \Lambda, r \in \mathbb{Q}$$

are isomorphisms. In other words, every basis of the $\mathbb{Z}$-module Λ is also a basis of the $\mathbb{Q}$-vector space H and a basis of the $\mathbb{R}$-vector space $H_{\mathbb{R}}$. Notice also that every subgroup of finite index in Λ is also a lattice in H. Moreover, an intersection of two (and even finitely many lattices in H is also a lattice in H.

Remark 5.4. Let Λ' be a subgroup of finite index, say, n in a lattice Λ in H. Then there are a basis $\{e_1, e_2, e_3, e_4\}$ of the $\mathbb{Z}$-module Λ and positive integers n_1, n_2, n_3, n_4 such that

$$\Lambda' = \oplus_{i=1}^{4} \mathbb{Z} \cdot (n_i e_i).$$

In particular, $\{n_1 e_1, n_2 e_2, n_3 e_3, n_4 e_4\}$ of the $\mathbb{Z}$-module Λ' and

$$n = \prod_{i=1}^{4} n_i.$$

This implies that the determinant $\tilde{D}'$ of the matrix $(\mathrm{B}_{\mathrm{tr}}(n_i e_i, n_j e_j))$ of the form B_{tr} with respect to $\{n_1 e_1, n_2 e_2, n_3 e_3, n_4 e_4\}$ is (in the notation of Definition 5.1) coincides with

$$\left(\prod_{1 \le i,j \le 4} n_i n_j \right) \cdot D = n^2 D = n^2 \left(\mathrm{discr}\Lambda\right)^2.$$

Hence

$$D(\Lambda') = n \cdot D(\Lambda).$$

A lattice $\mathfrak{o}$ in H is an *order* in H if it is a subring of H containing 1. Clearly, $\mathbb{Z} = \mathbb{Z} \cdot 1$ lies in $\mathfrak{o}$. The corresponding homomorphisms $\Psi_{\mathfrak{o},\mathbb{Q}}$ and $\Psi_{\mathfrak{o},\mathbb{R}}$ are actually isomorphisms of $\mathbb{Q}$-algebras and of $\mathbb{R}$-algebras respectively.

On the other hand,

$$\mathrm{tr}(x), \mathrm{Nm}(x) \in \mathbb{Z} \quad \forall x \in \mathfrak{o}. \tag{5.4}$$

Indeed,

$$\mathrm{tr}(x), \mathrm{Nm}(x) \in \mathbb{Q}.$$

Let $\{e_1, e_2, e_3, e_4\}$ be a basis of the free $\mathbb{Z}$-module $\mathfrak{o}$, and let $M(x) \in \mathrm{Mat}_4(\mathbb{Z})$ be the matrix of

$$\mathrm{mult}(x) : \Lambda \to \Lambda, \ y \mapsto xy$$

with respect to $\{e_1, e_2, e_3, e_4\}$. Let

$$\mathcal{P}_x(t) = \det(t \cdot 1 - M(x)) \in \mathbb{Z}[t]$$

be the characteristic polynomial of $M(x)$, which is a monic quartic polynomial with integer coefficients. It follows from Remark 2.28 that

$$\mathcal{P}_x(t) = \left(t^2 - \mathrm{tr}(x)t + \mathrm{Nm}(x)\right)^2.$$

Since $\mathcal{P}_x(t)$ is a monic polynomial with integer coefficients, it follows from Gauss' Lemma that the monic polynomial $t^2 - \mathrm{tr}(x)t + \mathrm{Nm}(x)$ also has integer coefficients, i.e.,

$$\mathrm{tr}(x), \mathrm{Nm}(x) \in \mathbb{Z}.$$

It follows that

$$\bar{x} = \mathrm{tr}(x) - x \in \mathbb{Z} \cdot 1 - x \subset \mathfrak{o} \quad \forall x \in \mathfrak{o}. \tag{5.5}$$

Hence, if $x, y \in \mathfrak{o}$ then $x\bar{y} \in \mathfrak{o}$ and therefore

$$\mathrm{B}_{\mathrm{tr}}(x, y) = \mathrm{tr}(x\bar{y}) \in \mathbb{Z}.$$

It follows from the definition of the discriminant of a lattice that $\mathrm{discr}(\mathfrak{o})$ is a *positive integer*.

Remark 5.5. Let $\mathfrak{o}_1$ and $\mathfrak{o}_2$ be orders in H. If $\mathfrak{o}_1 \subset \mathfrak{o}_2$ then $\mathfrak{o}_1$ is an additive group of finite index $[\mathfrak{o}_2 : \mathfrak{o}_1]$ in $\mathfrak{o}_2$ and

$$D(\mathfrak{o}_1) = [\mathfrak{o}_2 : \mathfrak{o}_1] \cdot D(\mathfrak{o}_2).$$

In particular, $D(\mathfrak{o}_2) \leq D(\mathfrak{o}_1)$; the equality holds if and only if $[\mathfrak{o}_2 : \mathfrak{o}_1] = 1$, i.e., $\mathfrak{o}_2 = \mathfrak{o}_1$.

We will need the following characterization of the multiplicative group $\mathfrak{o}^*$ of invertible elements in an order $\mathfrak{o}$.

Lemma 5.6. *Let $\mathfrak{o}$ be an order in H. Then it enjoys the following properties.*

(i)

$$\mathfrak{o}^* = \{x \in \mathfrak{o} \mid \mathrm{Nm}(x) = 1 \text{ or } -1\} = \{x \in \mathfrak{o} \mid \det(\Phi_{\mathbb{R}}(x)) = 1 \text{ or } -1\}.$$

In addition,

$$x^{-1} = \mathrm{Nm}(x) \cdot \bar{x} = \pm\bar{x} \quad \forall x \in \mathfrak{o}^*.$$

(ii) Let us consider

$$\mathfrak{o}^1 = \{x \in \mathfrak{o} \mid \mathrm{Nm}(x) = 1\}.$$

Then $\mathfrak{o}^1$ is a normal subgroup of $\mathfrak{o}^*$, whose index is either 1 or 2. In addition,

$$\mathfrak{o}^1 = \{x \in \mathfrak{o} \mid \Phi_{\mathbb{R}}(x) \in \mathrm{SL}(2, \mathbb{R})\}.$$

Proof. First, recall (5.1) that

$$\mathrm{Nm}(x) = \det(\Phi_{\mathbb{R}}(x)) \; \forall x \in \mathfrak{o}.$$

Second, suppose that $x \in \mathfrak{o}^*$. Then $x^{-1} \in \mathfrak{o}^*$. It follows that

$$\mathrm{Nm}(x), \mathrm{Nm}(x^{-1}) \in \mathbb{Z}, \quad 1 = \mathrm{Nm}(x) \cdot \mathrm{Nm}(x^{-1}),$$

which implies that both

$$\mathrm{Nm}(x), \mathrm{Nm}(x^{-1}) \in \{1, -1\}.$$

Conversely, if $x \in \mathfrak{o}$ then $\mathrm{Nm}(x) \in \{1, -1\}$ then

$$x\bar{x} = \mathrm{Nm}(x) \in \{1, -1\}, \quad \mathrm{Nm}(x)^{-1} = \mathrm{Nm}(x).$$

It follows that $\mathrm{Nm}(x)x^{-1} = \bar{x}$ and therefore

$$x^{-1} = \mathrm{Nm}(x)^{-1}\bar{x} = \mathrm{Nm}(x)\bar{x} = \pm\bar{x} \in \mathfrak{o}.$$

Hence, $x \in \mathfrak{o}^*$. This ends the proof of (i), which, in turn, implies readily (ii). □

Definition 5.2. An order $\mathfrak{o}$ in H is called *maximal* if it is not contained in a strictly larger order.

Remark 5.7. (i) Let $\mathfrak{o}$ be an order in H. Let us consider the set of all orders $\mathfrak{o}'$ containing $\mathfrak{o}$. It follows from Remark 5.5 that all the discriminants $D(\mathfrak{o}')$ do not exceed $D(\mathfrak{o})$; if we choose (among them) an order $\mathfrak{o}'$ with the smallest possible discriminant then $\mathfrak{o}'$ is a maximal order.

(ii) Let $\mathfrak{o}_1$ and $\mathfrak{o}_2$ be two maximal orders in H. Then $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are conjugate [170], i.e., there is $u \in H^*$ such that

$$\mathfrak{o}_2 = u\mathfrak{o}_1 u^{-1}, \ \ \mathfrak{o}_1 = u^{-1}\mathfrak{o}_2 u.$$

In particular, $D(\mathfrak{o}_2) = D(\mathfrak{o}_1)$, i.e., the discriminants of all maximal orders of H coincide.

(iii) Let $\mathfrak{o}$ be a *maximal* order in H. Then $\mathfrak{o}$ contains elements u, μ such that

$$\mathrm{Nm}(u) = -1, \quad \mu^2 = -D(\mathfrak{o}).$$

In addition,

$$\mathrm{tr}(\mu\mathfrak{o}) \subset -D(\mathfrak{o}) \cdot \mathbb{Z}$$

for every $\mu \in \mathfrak{o}$ with $\mu^2 = -D(\mathfrak{o})$. (see [170, Example 28.6.5, Sect. 43.6.6, and Lemma 43.6.7]). In particular,

$$u \in \mathfrak{o}^*, \quad \bar{\rho} = -\rho.$$

Remark 5.8. Let $\mathfrak{o}$ be a maximal order in H. Its discriminant $D(\mathfrak{o})$ admits the following description [170]. Let p be a prime, $\mathbb{Z}_p$ the ring of p-adic numbers, and $\mathbb{Q}_p$ the field of p-adic numbers. Then the quaternion $\mathbb{Q}_p$-algebra $H_{\mathbb{Q}_p} = H \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is isomorphic either to the matrix algebra $\mathrm{Mat}_2(\mathbb{Q}_p)$, or to a unique (up to isomorphism) central division algebra over $\mathbb{Q}_p$ of dimension 4. We say that p *ramifies* at H if $H_{\mathbb{Q}_p}$ is a division algebra. Otherwise, we say that the quaternion algebra H is unramified or *splits* over p . If $p \neq 2$, the quaternion division algebra over $\mathbb{Q}_p$ is isomorphic to $\left(\frac{e,p}{\mathbb{Q}_p}\right)$, where e is any element in $\mathbb{Z}_p$ that does not reduce to a square modulo p. If $p = 2$, the quaternion division algebra over $\mathbb{Q}_2$ is isomorphic to $\left(\frac{-1,-1}{\mathbb{Q}_2}\right)$. It is known that any field extension $L/\mathbb{Q}$ that splits H ramifies at every prime over which H ramifies. The set $\mathrm{Ram}(H)$ of ramified primes in H is non-empty, finite, and consists of an even number of elements. (It follows from the classical Brauer-Hasse-Noether Theorem.) In adddition,

$$D(\mathfrak{o}) = \prod_{p \in \mathrm{Ram}(H)} p, \tag{5.6}$$

i.e., the discriminant of $\mathfrak{o}$ coincides with the product of all ramified primes.

The following assertion may be viewed as a special case of [66, Lemma 2.4]

Lemma 5.9. *Let $\mathfrak{o}$ be a maximal order in H. Let μ be an element of $\mathfrak{o}$ such that*

$$\mu^2 = -D(\mathfrak{o}).$$

Let us put

$$\rho := \frac{\mu}{D(\mathfrak{o})} \in H.$$

Then

$$\mathbb{Q} \ni = \rho^2 = \frac{-D(\mathfrak{o})}{D(\mathfrak{o})^2} = \frac{-1}{D(\mathfrak{o})} < 0,$$

and the pairing

$$E_\rho = \frac{1}{D(\mathfrak{o})} E_\mu : \mathfrak{o}\times\mathfrak{o} \to \mathbb{Z}, \quad x, y \mapsto E_\rho(x,y) = \frac{1}{D(\mathfrak{o})} E_\mu(x,y) = \frac{1}{D(\mathfrak{o})} \mathrm{B}_{\mathrm{tr}}(\mu x, y) = \frac{1}{D(\mathfrak{o})} \mathrm{tr}(\mu x \bar{y}) = \mathrm{tr}(\rho x \bar{y})$$

is alternating and unimodular; the latter means that the determinant of the matrix of E_ρ with respect to a basis of $\mathfrak{o}$ is 1.

Proof. Let us put $D := D(\mathfrak{o})$. In light of Remark 5.7(iii),

$$\frac{1}{D(\mathfrak{o})} E_\rho(x,y) \in \mathbb{Z} \quad \forall x, y \in \mathfrak{o}.$$

It follows from Proposition 2.26 that E_ρ is an alternating pairing. This implies that $\frac{1}{D(\mathfrak{o})} E_\rho$ is also alternating. The index $[\mathfrak{o} : \rho\mathfrak{o}]$ is $D(\mathfrak{o})^2$. Indeed, we have the equality of indices

$$[\mathfrak{o} : \rho\mathfrak{o}] = [\rho\mathfrak{o} : \rho^2\mathfrak{o}] = [\rho\mathfrak{o} : D\mathfrak{o}].$$

It follows (recall that $\mathfrak{o}$ is a free $\mathbb{Z}$-module of rank 4) that

$$D^4 = [\mathfrak{o} : D\mathfrak{o}] = [\mathfrak{o} : \rho\mathfrak{o}] \cdot [\rho\mathfrak{o} : D\mathfrak{o}] = [\mathfrak{o} : \rho\mathfrak{o}]^2,$$

which implies that

$$[\mathfrak{o} : \rho\mathfrak{o}] = \sqrt{D^4} = D^2.$$

On the other hand, D^2 coincides (up to the sign) with the determinant of the matrix $(\mathrm{B}_{\mathrm{tr}}(e_i, f_j))$ where $\{e_1, e_2, e_3, e_4\}$ and $\{f_1, f_2, f_3, f_4\}$ are any bases of $\mathfrak{o}$. Clearly, $\{\rho e_1, \rho e_2, \rho e_3, \rho e_4\}$ is a basis of the free $\mathbb{Z}$-module $\rho\mathfrak{o}$. The formula for the index implies that the determinant of the matrix

$$(E_\rho(e_i, f_j)) = (\mathrm{B}_{\mathrm{tr}}(\rho e_i, f_j))$$

coincides (up to the sign) with the product $D^2 \cdot D^2 = D^4$. It follows that the determinant $(E_\rho(e_i, e_j))$ coincides (ip to the sign) with D^4. Since E_ρ is alternating, this determinant is a square in $\mathbb{Q}$ (the square of the pfaffian of E_ρ) and therefore equals D^4. It follows that the determinant of the matrix $\frac{1}{D}(E_\rho(e_i, e_j))$ is $D^4/D^4 = 1$, which ends the proof. □

5.2 PEL-Structures

Each lattice Λ gives rise to two orders in H– the *left order* $\mathrm{O}_{\mathbf{l}}(\Lambda)$ of Λ and the *right order* $\mathrm{O}_{\mathbf{r}}(\Lambda)$ of Λ defined by

$$\mathrm{O}_{\mathbf{l}}(\Lambda) = \{x \in H \mid x\Lambda \subset \Lambda\} \subset H, \quad \mathrm{O}_{\mathbf{r}}(\Lambda) = \{y \in H \mid \Lambda y \subset \Lambda\} \subset H. \tag{5.7}$$

Clearly,

$$\mathrm{O}_{\mathbf{l}}(\Lambda) = \{x \in H_{\mathbb{R}} \mid x\Lambda \subset \Lambda\} \subset H_{\mathbb{R}}, \quad \mathrm{O}_{\mathbf{r}}(\Lambda) = \{y \in H_{\mathbb{R}} \mid \Lambda y \subset \Lambda\} \subset H_{\mathbb{R}}. \tag{5.8}$$

If a lattice Λ is an order, then

$$\mathrm{O}_{\mathbf{l}}(\Lambda) = \mathrm{O}_{\mathbf{r}}(\Lambda) = \Lambda.$$

The lattice Λ carries the natural structure of a faithful left $\mathrm{O}_{\mathbf{l}}$-module, whose endomorphism ring coincides with $\mathrm{O}_{\mathbf{r}}(\Lambda)$. Identifying H with its image $H\otimes 1$ in $H_{\mathbb{R}}$, we may view Λ as a discrete lattice in $H_{\mathbb{R}}$. The corresponding quotient $H_{\mathbb{R}}/\Lambda$ can be provided with a family of natural structures of a polarized abelian surface A with $\mathrm{O}_{\mathbf{l}} \subset \mathrm{End}(A)$. Before defining the family (that requires choices of complex structures on $H_{\mathbb{R}}$), let us pick $\rho \in H$ with $\rho^2 < 0$. Since Λ is a free $\mathbb{Z}$-module, replacing ρ by $N\rho$ for sufficiently divisible positive integer N, we may and will assume that (in the notation of Proposition 2.26)

$$E_\rho(x,y) = E(x,y) = \mathrm{tr}(\rho x \bar{y}) \in \mathbb{Z}, \quad \forall x, y \in \Lambda. \tag{5.9}$$

Combining Proposition 2.26 and Lemma 5.1 applied to $H_{\mathbb{R}}$ over $\mathbb{R}$, we conclude that either, for all $\eta \in \mathcal{X}$,

$$E(x\eta, x) = \mathrm{tr}(\rho x \eta \bar{x}) > 0 \quad \forall x \in H_{\mathbb{R}} \setminus \{0\} \tag{5.10}$$

or or all $\eta \in \mathcal{X}$

$$E(x\eta, x) < 0 \quad \forall x \in H_{\mathbb{R}} \setminus \{0\}.$$

Replacing (if necessary) ρ by $-\rho$, we may and will assume that (5.10) holds.

Now, choose an element $\eta \in H_{\mathbb{R}}^*$ such that $\eta^2 = -1$ and define a *complex structure* (i.e., multiplication by $\mathbf{i} = \sqrt{-1}$) on the 4-dimensional real vector space $H_{\mathbb{R}}$ by

$$\mathbf{i} \cdot \mathbf{x} := \mathbf{x}\eta, \quad \forall \mathbf{x} \in \mathbf{H}_{\mathbb{R}}.$$

Then, $H_{\mathbb{R}}$ becomes the two-dimensional complex vector space, which we will denote by $H_{\mathbb{R}}(\eta)$. Let us consider the corresponding *complex torus*

$$A(\Lambda, \eta) := H_{\mathbb{R}}(\eta)/\Lambda. \tag{5.11}$$

and consider the $\mathbb{R}$-bilinear form

$$\mathcal{H} = \mathcal{H}_\rho : H_{\mathbb{R}}(\eta) \times H_{\mathbb{R}}(\eta) \to \mathbb{C}, \quad x, y \mapsto E_\rho(\mathbf{i}x, y) + \mathbf{i}E_\rho(x,y) = E_\rho(x\eta, y) + \mathbf{i}E_\rho(x,y). \tag{5.12}$$

In light of Proposition 2.26 and (5.9), $\mathcal{H}$ is a positive-definite Hermitian form on $H_{\mathbb{R}}(\eta)$, whose imaginary part E takes on integer values on $\Lambda \times \Lambda$. In other words, $\mathcal{H}$ is a polarization on the complex torus $A(\Lambda, \eta)$. In particular, $A(\Lambda, \eta)$ is a complex abelian surface.

Clearly, the polarization $\mathcal{H}_\rho$ is *principal* if and only if the alternating bilinear form

$$\mapsto E_\rho : \Lambda \times \Lambda \to \mathbb{Z}$$

is *unimodular*.

Since multiplications from the left commute with multiplications from the left on $H_{\mathbb{R}}$, we have the ring embedding

$$\mathrm{O}_{\mathbf{l}}(\Lambda) \hookrightarrow \mathrm{End}(A(\Lambda,\eta)), \quad u \mapsto \{x+\Lambda \mapsto ux+\Lambda\} \quad \forall u \in \mathrm{O}_{\mathbf{l}}(\Lambda), x \in H_{\mathbb{R}}. \tag{5.13}$$

On the other hand, let $A = V/\Pi$ be an abelian surface provided with a ring embedding $\mathrm{O}_{\mathbf{l}}(\Lambda) \hookrightarrow \mathrm{End}(A)$ such that the induced ring homomorphism $\mathrm{O}_{\mathbf{l}}(\Lambda) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Pi)$ provides Π with the structure of a left $\mathrm{O}_{\mathbf{l}}(\Lambda)$-module that is isomorphic to Λ. Let us fix an isomorphism $\psi : \Pi \cong \Lambda$ of $\mathrm{O}_{\mathbf{l}}(\Lambda)$-modules. Then, ψ extends by $\mathbb{R}$-linearity to the isomorphism of left $\mathrm{O}_{\mathbf{l}}(\Lambda) \otimes \mathbb{R} = H_{\mathbb{R}}$-modules

$$\psi_{\mathbb{R}} : V = \Pi \otimes \mathbb{R} \cong \Lambda \otimes \mathbb{R} = H_{\mathbb{R}}.$$

Since the endomorphism algebra of the left $H_{\mathbb{R}}$-module $H_{\mathbb{R}}$ consists of right multiplication by elements of $H_{\mathbb{R}}$, the multiplication by $\mathbf{i}$ in V corresponds (under $\psi_{\mathbb{R}}$) to right multiplication by some $\eta \in \mathcal{X} \subset H_{\mathbb{R}}$, i.e.,

$$\psi_{\mathbb{R}}(\mathbf{i}v) = \psi_{\mathbb{R}}(v)\eta \quad \forall v \in V.$$

It follows easily that the map

$$V/\Pi \to H_{\mathbb{R}}(\eta)/\Lambda,\ v+\Pi \mapsto \psi_{\mathbb{R}}(x)+\Lambda$$

is an isomorphism of abelian surfaces A and $A(\Lambda,\eta)$ that is compatible with the actions of $\mathrm{O}_{\mathbf{l}}(\Lambda)$.

Remark 5.10. Recall that the natural homomorphism of $\mathbb{Q}$-algebras

$$\mathrm{O}_{\mathbf{l}}(\Lambda) \otimes \mathbb{Q} \to H,\ u \otimes r \mapsto ru$$

is an isomorphism of $\mathbb{Q}$-algebras. Combining it with the embedding (5.13), we get the embedding of $\mathbb{Q}$-algebras

$$H \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta)).$$

Let us identify H with its image in $\mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta))$. Recall (Remark **??**) that there is the $\mathbb{Q}$-algebra embedding

$$\rho_r : \mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta)) \hookrightarrow \mathrm{End}(\Lambda_{\mathbb{Q}})$$

where $\Lambda_{\mathbb{Q}}$ obviously coincides with H. On the other hand, since

$$A(\Lambda,\eta) = H_{\mathbb{R}}(\eta)/\Lambda = H_{\mathbb{R}}/\Lambda,$$

it follows from the very definition of the embedding (5.13) that the composition

$$H \subset \mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta)) \stackrel{\rho_r}{\hookrightarrow} \mathrm{End}_{\mathbb{Q}}(H)$$

coincides with the map

$$x \mapsto \mathrm{mult}_H(x) : H \to H,\ y \mapsto xy.$$

It follows from the very definition of $\mathrm{O}_{\mathbf{l}}(\Lambda)$ that $\mathrm{O}_{\mathbf{l}}(\Lambda)$ coincides with the intersection of H and $\mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta))$ in $\mathrm{End}_{\mathbb{Q}}(A(\Lambda,\eta))$.

Remark 5.11. Recall that there is the anti-involution

$$x \mapsto x^* = \rho^{-1}\bar{x}\rho$$

on H. The non-degeneracy of the bilinear form E_ρ combined with Proposition 5.2 (applied to $F = \mathbb{Q}$) implies that x^* coincides with the image of x with respect to the Rosati involution attached to $\mathcal{H}_\rho$ for all $x \in H$. On the other hand, if H_ρ is *principal*, the image of any $u \in \mathrm{End}(A(\Lambda, \eta))$ under the corresponding Rosati involution lies in in $\mathrm{End}(A(\Lambda, \eta))$. In light of Remark 5.10, if

$$x \in \mathrm{O}_{\mathbf{l}}(\Lambda) \subset \mathrm{End}(A(\Lambda, \eta))$$

then

$$x^* \in \mathrm{End}(A(\Lambda, \eta)) \cap H = \mathrm{O}_{\mathbf{l}}(\Lambda).$$

In other words, $\mathrm{O}_{\mathbf{l}}(\Lambda)$ is stable under the anti-involution if H_ρ is principal. In light of (5.5),

$$\mathrm{O}_{\mathbf{l}}(\Lambda) = \rho \mathrm{O}_{\mathbf{l}}(\Lambda)\rho^{-1} \tag{5.14}$$

if H_ρ is a principal polarization.

Now, let $\eta_1, \eta_2 \in \mathcal{X}(H_{\mathbb{R}})$, and

$$f : A(\Lambda, \eta_1) \to A(\Lambda, \eta_2)$$

be a homomorphism of corresponding abelian surfaces that is compatible with the actions of $\mathrm{O}_{\mathbf{l}}(\Lambda)$. This means that the corresponding $\mathbb{R}$-linear homomorphism

$$f_a : H_{\mathbb{R}} \to H_{\mathbb{R}}$$

such that $f(x + \Lambda) = f(x) + \Lambda$ satisfies the following properties:

$$\begin{aligned} &f_a(\Lambda) \subset \Lambda, \quad f_a(x\eta_1) = f_a(x)\eta_2, \quad \forall x \in H_{\mathbb{R}}, \\ &f_a(ux) = u f_a(x), \ \forall \forall x \in H_{\mathbb{R}}, \ u \in \mathrm{O}_{\mathbf{l}}(\Lambda). \end{aligned} \tag{5.15}$$

The latter property actually means that

$$f_a(ux) = u f_a(x) \ \forall \forall x \in H_{\mathbb{R}}, \ u \in H_{\mathbb{R}}.$$

It follows that there is precisely one $w \in H_{\mathbb{R}}$ such that

$$f_a(x) = xw \ \forall lx \in H_{\mathbb{R}}.$$

By the first property of (5.15), we get $\Lambda \cdot w \subset \Lambda$. Since Λ generates H as the $\mathbb{Q}$-vector space, $w \in H$, and, therefore,

$$w \in \mathrm{O}_{\mathbf{r}}(\Lambda).$$

It follows from the second property of (5.15) that, for any $x \in H_{\mathbb{R}}$,

$$(x\eta_1)w = (xw)\eta_2.$$

This means that

$$\eta_1 w = w\eta_2.$$

It follows easily that if f is an isomorphism then $w \in \mathrm{O}_{\mathbf{r}}(\Lambda)^*$ and

$$\eta_1 = w\eta_2 w^{-1}.$$

Conversely, each $w \in \mathrm{O}_{\mathbf{r}}(\Lambda)$ defines (for all $\eta_2 \in \mathcal{X}$) the homomorphism of abelian surfaces

$$\mathrm{w}_{\mathbf{r}} : A(\Lambda, w\eta_1 w^{-1}) = H_{\mathbb{R}}(w\eta_1 w^{-1})/\Lambda \to A(\Lambda, \eta_2) := H_{\mathbb{R}}(\eta_2)/\Lambda,\ x + \Lambda \mapsto wx + \Lambda,$$

which is an isomorphism if and only if $w \in \mathrm{O}_{\mathbf{r}}(\Lambda)^*$.

Now, it is time to look closely at $\mathcal{X}(H_{\mathbb{R}})$, which may be identified (if we fix Φ) with

$$\mathcal{X}(\mathrm{Mat}_2(\mathbb{R})) = \{\mathcal{J} \in \mathrm{GL}(2, \mathbb{R}) = H_{\mathbb{R}}^*,\ \mathcal{J}^2 = -1\}.$$

Let us identify $\mathcal{X}(\mathrm{Mat}_2(\mathbb{R}))$ with $\mathbb{C} \setminus \mathbb{R}$ in the following way. Each $\mathcal{J} \in \mathcal{X}(\mathrm{Mat}_2(\mathbb{R}))$ is a linear operator in $\mathbb{R}^2$, whose eigenvalues are $\pm\mathbf{i}$, both of multiplicity 1. Let $v = (z_1, z_2) \in \mathbb{C}^2$ be an eigenvector of $\mathcal{J}$ with eigenvalue $\mathbf{i}$. Clearly, none of coordinates z_1, z_2 vanishes. Rescaling v by $\frac{1}{z_2} \cdot v$, we may assume that $z_2 = 1$, i.e., $v = (\tau, 1)$. Such a v is defined uniquely and

$$\tau := \tau(\mathcal{J}) \in \mathbb{C} \setminus \mathbb{R}.$$

On the other hand, such τ determines $\mathcal{J}$ uniquely, because the complex-conjugate vector $(1, \bar{\tau})$ is an eigenvector of $\mathcal{J}$ with eigenvalue $-\mathbf{i}$.

Conversely, if $\tau \in \mathbb{C}\setminus\mathbb{R}$, then let us define the $\mathbb{C}$-linear operator $\mathcal{J}(\tau)_{\mathbb{C}} : \mathbb{C}^2 \to \mathbb{C}^2$ by the property that $(\tau, 1) \in \mathbb{C}^2$ is an eigenvector of $\mathcal{J}(\tau)_{\mathbb{C}}$ with eigenvalue $\mathbf{i}$ and $(\bar{\tau}, 1) \in \mathbb{C}^2$ is an eigenvector of $\mathcal{J}(\tau)_{\mathbb{C}}$ with eigenvalue $-\mathbf{i}$. Since $\tau \notin \mathbb{R}$, vectors $(\tau, 1)$ and $(\bar{\tau}, 1)$ constitute a basis of $\mathbb{C}^2$, that implies that such a $\mathcal{J}(\tau)_{\mathbb{C}}$ exists and unique; in addition $\mathcal{J}(\tau)_{\mathbb{C}}^2 = -1$. It is also clear that $\mathcal{J}(\tau)_{\mathbb{C}}$ is defined over $\mathbb{R}$, i.e., there is a linear operator $\mathcal{J}(\tau)$ such that $\mathcal{J}(\tau)_{\mathbb{C}}$ is obtained from $\mathcal{J}(\tau)$ by extensions of scalars from $\mathbb{R}$ to $\mathbb{C}$. This implies that the maps

$$\mathfrak{A} : \mathcal{X}(\mathrm{Mat}_2(\mathbb{R})) \to \mathbb{C} \setminus \mathbb{R},\ \mathcal{J} \mapsto \tau(\mathcal{J}) \ \text{ and } \mathfrak{B} : \mathbb{C} \setminus \mathbb{R} \to \mathcal{X},\ \tau \mapsto \mathcal{J}(\tau) \tag{5.16}$$

are mutually inverse.

The group $\mathrm{GL}(2, \mathbb{R})$ acts on $\mathcal{X}(\mathrm{Mat}_2(\mathbb{R}))$ by conjugation:

$$\mathcal{J} \mapsto \mathcal{M}\mathcal{J}\mathcal{M}^{-1} \quad \forall \mathcal{M} \in \mathrm{GL}(2, \mathbb{R}).$$

The corresponding induced action of $\mathrm{GL}(2, \mathbb{R})$ on $\mathbb{C} \setminus \mathbb{R}$ is the standard action by fractional-linear transformations. Indeed, let

$$\mathcal{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R}).$$

If $\tau = \tau(\mathcal{J})$ for $\mathcal{J} \in \mathcal{X}$, then

$$\mathcal{M}(\tau, 1) = (\alpha\tau + \beta, \gamma\tau + \delta) \in \mathbb{C}^2$$

is an eigenvector of $\mathcal{M}\mathcal{J}\mathcal{M}^{-1}$ with eigenvalue $\mathbf{i}$. It follows that $(\frac{\alpha\tau+\beta}{\gamma\tau+\delta)}, 1)$ is the eigenvector of $\mathcal{M}\mathcal{J}\mathcal{M}^{-1}$ with second coordinate 1 (and eigenvalue $\mathbf{i}$). Hence,

$$\tau(\mathcal{M}\mathcal{J}\mathcal{M}^{-1}) = \frac{\alpha\tau+\beta}{\gamma\tau+\delta},$$

which ends the proof.

It follows that the set of $\mathcal{M}(\Lambda)$ of isomorphism classes of abelian surfaces $A = V/\Pi$ endowed with a ring embedding $\mathrm{O}_{\mathbf{l}}(\Lambda) \hookrightarrow \mathrm{End}(A)$ (that sends 1 to 1) and such that the corresponding $\mathrm{O}_{\mathbf{l}}(\Lambda)$-module Π is isomorphic to Λ are in one-to-one correspondence with points of the quotient $\mathrm{O}_{\mathbf{r}}(\Lambda)^* \backslash (\mathbb{C} \setminus \mathbb{R})$ (here we identify $\mathrm{O}_{\mathbf{r}}(\Lambda)^*$ with its image $\Phi(\mathrm{O}_{\mathbf{r}}(\Lambda)^*)$ in $\mathrm{GL}(2,\mathbb{R})$). This quotient is a compact Riemann surface (the *Shimura curve*, see below), whose compactness follows from the compactness of $\mathrm{O}_{\mathbf{r}}(\Lambda)^* \backslash \mathrm{GL}(2,\mathbb{R})/\mathbb{R}^*$. This gives us the bijection

$$\mathcal{M}(\Lambda) \to \mathrm{O}_{\mathbf{r}}(\Lambda)^* \backslash (\mathbb{C} \setminus \mathbb{R}) \tag{5.17}$$

induced by

$$\mathcal{X}(H_{\mathbb{R}}) \stackrel{\Phi_{\mathbb{R}}}{\to} \mathcal{X}(\mathrm{Mat}_2(\mathbb{R})) \to \mathbb{C} \setminus \mathbb{R}, \quad \eta \mapsto \Phi_{\mathbb{R}}(\eta) =: \mathcal{J} \mapsto \tau(\mathcal{J}).$$

In our description of $\mathcal{M}(\Lambda)$ we fixed the lattice and varied the complex structure in $\Lambda_{\mathbb{R}} = \Lambda \otimes \mathbb{R}$ that gives rise to the complex torus (actually, the abelian surface) $\Lambda_{\mathbb{R}}/\Lambda$ (fake elliptic curve). There is an alternative description of $\mathcal{M}(\Lambda)$ where we vary lattices in $\mathbb{C}^2$ (with fixed complex structure) that we are going to discuss right now. First, we have the inclusions

$$\Lambda \subset H \subset H_{\mathbb{R}} \stackrel{\Phi_{\mathbb{R}}}{\cong} \mathrm{Mat}_2(\mathbb{R}) \subset \mathrm{Mat}_2(\mathbb{C}).$$

Second, each $\tau \in \mathbb{C} \setminus \mathbb{R}$ gives rise to the isomorphism of 4-dimensional real vector spaces

$$\phi_\tau : H_{\mathbb{R}} \to \mathbb{C}^2, \quad x \mapsto \Phi_{\mathbb{R}}(x) \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Indeed, the dimension arguments imply that it suffices to check the injectiveness of the $\mathbb{R}$-linear map

$$\mathrm{Mat}_2(\mathbb{R}) \to \mathbb{C}^2,\ M \mapsto M \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

In order to check it, let

$$y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R}).$$

Then the vector

$$M \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} = (\alpha\tau+\beta, \gamma\tau+\delta)$$

equals $(0,0)$ if and only if $\alpha = \beta = 0 = \gamma = \delta$, because $\tau \notin \mathbb{R}$. This proves the desired injectiveness. Since $\phi_\tau : H_{\mathbb{R}} \to \mathbb{C}^2$ is an isomorphism of real vector spaces and Λ is a discrete lattice of rank 4 in $H_{\mathbb{R}}$, its image

$$\Lambda_\tau := \phi_\tau(\Lambda)$$

is a discrete lattice of rank 4 in $\mathbb{C}^2$. Third, if $J(\tau) = \Phi_{\mathbb{R}}(\eta)$ with $\eta \in \mathcal{X}(H_{\mathbb{R}})$ then

$$\phi_\tau : H_{\mathbb{R}}(\eta) = H_{\mathbb{R}} \to \mathbb{C}^2$$

is a $\mathbb{C}$-linear map and, therefore, is an isomorphism of two-dimensional complex vector spaces. Indeed, multiplication by $\mathbf{i}$ in $H_{\mathbb{R}}(\eta) = H_{\mathbb{R}}$ is multiplication by η from the right:

$$\mathrm{mult}_r(\eta) : H_{\mathbb{R}} \to H_{\mathbb{R}},\ x \mapsto x\eta.$$

Hence

$$\Phi_{\mathbb{R}}(\mathrm{mult}_r(\eta)(x)) = \Phi_{\mathbb{R}}(x\eta) = \Phi_{\mathbb{R}}(x)\Phi_{\mathbb{R}}(\eta) = \Phi_{\mathbb{R}}(x)J(\tau).$$

This implies that

$$\phi_\tau(x\eta) = (\Phi_{\mathbb{R}}(x)J(\tau)) \cdot \begin{pmatrix}\tau\\1\end{pmatrix} = \Phi_{\mathbb{R}}(x)\left(J(\tau)\cdot\begin{pmatrix}\tau\\1\end{pmatrix}\right).$$

Recall that

$$J(\tau)\cdot\begin{pmatrix}\tau\\1\end{pmatrix} = \mathbf{i}\begin{pmatrix}\tau\\1\end{pmatrix}.$$

It follows that

$$\phi_\tau(x\eta) = \Phi_{\mathbb{R}}(x)\cdot\left(\mathbf{i}\begin{pmatrix}\tau\\1\end{pmatrix}\right) = \mathbf{i}\left(\Phi_{\mathbb{R}}(x)\cdot\begin{pmatrix}\tau\\1\end{pmatrix}\right) = \mathbf{i}\phi_\tau(x).$$

This proves that the map ϕ_τ is $\mathbb{C}$-linear and (as we have already observed) is a $\mathbb{C}$-linear isomorphism. It follows that ϕ_τ induces an isomorphism of complex tori

$$\phi_{\eta,\tau} : A(\Lambda,\eta) = H_{\mathbb{R}}/\Lambda \to \mathbb{C}^2/\Lambda_\tau =: A_\tau.$$

Since $A(\Lambda,\eta)$ is an abelian surface, A_τ is also an abelian surface, and $\phi_{\eta,\tau}$ is an isomorphism of abelian surfaces. The induced action of $O_l(\Lambda)$ on A_τ is defined by the formula

$$O_l(\Lambda) \to \mathrm{End}(A_\tau),\ x \mapsto \{w+\Lambda_\tau \mapsto \Phi_{\mathbb{R}}(x)\cdot w + \Lambda_\tau\ \forall x \in O_l(\Lambda),\ w \in \mathbb{C}^2\}.$$

Remark 5.12. The polarization $\mathcal{H}_\rho$ (5.12) on $A(\Lambda,\eta)$ gives rise (via ϕ_τ) to the polarization $\mathcal{H}_{\rho,\tau}$ on $A_\tau = \mathbb{C}^2/\Lambda_\tau$ defined by the formula

$$\mathcal{H}_{\rho,\tau} : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}, \quad \phi_\tau(x), \phi_\tau(y)y \mapsto \mathcal{H}_\rho(x,y) \quad \forall x,y \in H_{\mathbb{R}}. \tag{5.18}$$

In particular, $\mathcal{H}_{\rho,\tau}$ is *principal* if and only if $\mathcal{H}_\rho$ is *principal*, i.e., the alternating form

$$E_\rho : \Lambda \times \Lambda \to \mathbb{Z}$$

is *unimodular*.

Now let us fix a maximal order $\mathfrak{o}$ in H and concentrate on the case when $\Lambda = \mathfrak{o}$. Then (as we have already seen)

$$O_l(\Lambda) = \mathfrak{o} = O_r(\Lambda) = \Lambda.$$

Then the "moduli space" is $\mathfrak{o}^* \backslash (\mathbb{C} \setminus \mathbb{R})$. We are going to endow abelian surfaces A_τ ($\tau \in \mathbb{C} \setminus \mathbb{R}$) with a principal polarization. First, notice that (thanks to Lemma 5.6) we may replace the "moduli space" $\mathfrak{o}^* \backslash (\mathbb{C} \setminus \mathbb{R})$ by the quotient $\mathfrak{o}^1 \backslash \mathfrak{H}$ of the upper half-plane $\mathfrak{H}$. Indeed, the inclusions

$$\mathfrak{H} \subset \mathbb{C} \setminus \mathbb{R}, \quad \mathfrak{o}^1 \subset \mathfrak{o}^*$$

give rise to the map

$$\mathfrak{o}^1 \backslash \mathfrak{H} \to \mathfrak{o}^* \backslash (\mathbb{C} \setminus \mathbb{R}) \cong \mathcal{M}(\mathfrak{o}), \quad \mathfrak{o}^1 \tau \mapsto \mathfrak{o}^* \tau \ \forall \tau \in \mathfrak{H}. \tag{5.19}$$

where the bijection $\mathfrak{o}^* \backslash (\mathbb{C} \setminus \mathbb{R}) \cong \mathcal{M}(\mathfrak{o})$ is defined in (5.17). We claim that this is a bijection. In order to check the surjectiveness, recall that since $\mathfrak{o}$ is maximal, it follows from Remark 5.7(iii) that there is $u \in \mathfrak{o}^*$ with $\mathrm{Nm}(u) = -1$. It follows that the the matrix $\Phi_{\mathbb{R}}(u) \in \mathrm{GL}(2, \mathbb{R})$ has determinant -1. This implies that if τ' is a complex number with negative real part then there is $\tau \in \mathfrak{H}$ such that $\Phi_{\mathbb{R}}(u)(\tau) = \tau'$. This implies that $\mathfrak{o}^* \tau'$ is the image of $\mathfrak{o}^1 \tau$, which proves the surjectiveness of the map (5.19). On the other hand, the injectiveness of (5.19) is equivalent to the following assertion.

If $\tau_1, \tau_2 \in \mathfrak{H}$ lie in the same $\mathfrak{o}^*$-orbit then they belong to the same $\mathfrak{o}^1$-orbit. Let us check it. Indeed, suppose that there is $w \in \mathfrak{o}^*$ such that the matrix $M = \Phi_{\mathbb{R}}(w) \in \mathrm{GL}(2, \mathbb{R})$ satisfies $M(\tau_1) = \tau_2$. Since both τ_1 and τ_2 lie in the upper half-plane, $\det(M) > 0$. Since

$$\det(M) = \mathrm{Nm}(w) \in \{1, -1\},$$

we get $\mathrm{Nm}(w) = 1$, i.e., $w \in \mathfrak{o}^1$. This implies that τ_1 and τ_2 lie the same $\mathfrak{o}^1$-orbit, which implies the injectiveness. This ends the proof of the bijectiveness of (5.19).

Our next step is to construct principal polarizations on all abelian surfaces A_τ ($\tau \in \mathfrak{H}$) that correspond to $\Lambda = \mathfrak{o}$. Recall (Remark 5.7(iii)) that there is $\mu \in H$ such that

$$\mu \in \mathfrak{o}, \quad \mu^2 = -D(\mathfrak{o}) \tag{5.20}$$

is a *negative integer*. In light of Proposition 2.26, replacing if necessary ρ by $-\rho$, we may and will assume that

$$E(x\eta, , x) = E_\mu(x\eta x, x) = \mathrm{B}_{\mathrm{tr}}(\mu x \eta, x) = \mathrm{tr}(\mu x \eta x) > 0 \quad \forall \eta \in \mathcal{X}(H_{\mathbb{R}}),\ x \in H_{\mathbb{R}} \setminus \{0\}. \tag{5.21}$$

Recall (Lemma 5.9) that if we put

$$\rho := \frac{\mu}{D(\mathfrak{o})} \in H$$

then

$$\mathbb{Q}\rho^2 = \frac{-1}{D(\mathfrak{o})} < 0,$$

and the alternating pairing $\frac{1}{D(\mathfrak{o})} E_\rho : \mathfrak{o} \times \mathfrak{o} \to \mathbb{Z}$ is unimodular. Clearly, the Hermitian form .

$$H_{\rho,\tau} = \frac{1}{D(\mathfrak{o})} H_{\rho,\tau}$$

defined in (5.18)is positive. In light of Remark 5.12, it is a *principal polarization* on $A(\tau)$. It follows from the definition of ρ (in terms of μ) that

$$\rho^{-1} \bar{x} \rho = \mu^{-1} \bar{x} \mu \quad \forall x \in H.$$

Now Remark 5.11 implies that that the Rosati involution H attached to the polarization $H_{\rho,\tau}$ coincides with the map

$$x \mapsto x^* = \rho^{-1}\bar{x}\rho = \mu^{-1}\bar{x};$$

in addition, $\mathfrak{o}$ is stable under this anti-involution, in light of (5.14).

Definition 5.3. A *PEL-structure* consists of a data $\mathcal{S} = (H, \mathfrak{o}, \Phi, \rho)$, where

1. $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ is a totally indefinite quaternion algebra over $\mathbb{Q}$,
2. $\mathfrak{o}$ is a maximal order in H,
3. Φ is an injective $\mathbb{Q}$-algebra homomorphism $H \hookrightarrow \mathrm{Mat}_2(\mathbb{R})$,
4. $\mu \in \mathfrak{o}$ such that $\mu^2 = -D(\mathfrak{o})$ and (5.21) holds.

A choice of a PEL-structure and $\tau \in \mathfrak{H}$ defines a map

$$\phi_\tau : H_{\mathbb{R}} \to \mathbb{C}^2, \quad x \mapsto \Phi(x) \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix}. \tag{5.22}$$

and a complex torus (actually, an abelian surface)

$$A_\tau := \mathbb{C}^2/\Lambda_\tau.$$

If we put $\rho := \mu/D(\mathfrak{o})$, then the symplectic form $E_\rho(x, y)$ defines a principal polarization with the symplectic form

$$E_\rho(\phi_\tau(x), \phi_\tau(y)) = \mathrm{tr}(\rho x \bar{y}).$$

The left action of $\mathfrak{o}$ on $\mathfrak{o}$ defines an embedding of

$$\iota : \mathfrak{o} \hookrightarrow \mathrm{End}(A_\tau),$$

and the corresponding Rosati involution on $\mathrm{End}(A_\tau)$ leaves invariant (the image of) $\mathfrak{o}$ and its restriction to $\mathfrak{o}$ coincides with the map

$$u \mapsto u^* = \mu^{-1}\bar{u}\mu = \rho^{-1}\bar{u}\rho \quad \forall u \in \mathfrak{o}.$$

Recall that to each $\tau \in \mathfrak{H}$ corresponds the principally polarized abelian surface

$$A_\tau = \mathbb{C}^2/\Lambda_\tau \cong H_{\mathbb{R}}(\eta)/\Lambda.$$

One should expect that such a correspondence arises from a certain "equivariant" holomorphic map $\mathfrak{H} \to \mathfrak{H}_2$. We are going to construct such a map, following (up to some point) a construction of Hashimoto [67, Sect. 3, 4]. First, let us consider the symplectic group attached to E_ρ that is a subgroup of the group of automorphisms $\mathrm{Aut}_{\mathbb{R}}(H_{\mathbb{R}})$ of the $\mathbb{R}$-vector space $H_{\mathbb{R}}$. Namely,

$$\mathrm{Sp}(H_{\mathbb{R}}, E_\rho) := \{u \in \mathrm{Aut}_{\mathbb{R}}(H_{\mathbb{R}}) \mid E_\rho(ux, uy) = E_\rho(x, y) \quad \forall x, y \in H_{\mathbb{R}}\}.$$

Similarly, let us define its $\mathbb{Z}$-form. Let us put

$$\Lambda := \mathfrak{o}$$

and consider

$$\mathrm{Sp}(\Lambda, E_\rho) := \{u \in \mathrm{Aut}_{\mathbb{Z}}(\Lambda) \mid E_\rho(ux, uy) = E_\rho(x, y) \quad \forall x, y \in \Lambda\}.$$

Clearly, one may view $\mathrm{Aut}_{\mathbb{Z}}(\Lambda)$ as the certain subgroup of $\mathrm{Aut}_{\mathbb{R}}(H_{\mathbb{R}})$ and

$$\mathrm{Sp}(\Lambda, E_\rho) = \mathrm{Sp}(H_{\mathbb{R}}, E_\rho) \cap \mathrm{Aut}_{\mathbb{Z}}(\Lambda).$$

On the other hand, if we consider the subgroup

$$H^1_{\mathbb{R}} = \{u \in H_{\mathbb{R}} \mid \mathrm{Nm}(x) = 1\} \subset H^*_{\mathbb{R}}$$

then there is the natural group embedding

$$H^1_{\mathbb{R}} \hookrightarrow \mathrm{Aut}_{\mathbb{R}}(H_{\mathbb{R}}), \quad u \mapsto \{x \mapsto x\bar{u}\} \ \ \forall u \in H^1_{\mathbb{R}},\ x \in H_{\mathbb{R}},$$

whose image lies in $\mathrm{Sp}(H_{\mathbb{R}}, E_\rho)$. Indeed, we have

$$E_\rho(x\bar{u}, \overline{y\bar{u}}) = \mathrm{tr}(\rho(x\bar{u}\overline{y\bar{u}}) = \mathrm{tr}(\rho x\bar{u}u\bar{y}) = \mathrm{tr}(\rho x\mathrm{Nm}(u)\bar{y}) = \mathrm{tr}(\rho x\bar{y}) = E_\rho(x, y) \quad \forall x, y \in H_{\mathbb{R}}.$$

This gives us the injective group homomorphism

$$\Psi : H^1_{\mathbb{R}} \hookrightarrow \mathrm{Sp}(H_{\mathbb{R}}, \rho), \quad u \mapsto \{x \mapsto x\bar{u}\} \ \ \forall u \in H^1_{\mathbb{R}},\ x \in H_{\mathbb{R}}, \tag{5.23}$$

which is obviously a homomorphism of real Lie groups. Now, (5.8) implies that

$$\Psi\left(H^1_{\mathbb{R}}\right) \cap \mathrm{Sp}(\Lambda, E_\rho) = \Psi(\mathfrak{o}^1). \tag{5.24}$$

Now let us consider the set

$$\mathcal{Y}(H_{\mathbb{R}}, \rho) = \{w \in \mathrm{Sp}(H_{\mathbb{R}}, \rho) \mid w^2 = -1\} \subset \mathrm{Sp}(H_{\mathbb{R}}, \rho) \subset \mathrm{Aut}_{\mathbb{R}}(H_{\mathbb{R}}).$$

Then Ψ gives rise to the embedding

$$\mathcal{X}(H_{\mathbb{R}}) \to \mathcal{Y}(H_{\mathbb{R}}, \rho), \quad \eta \mapsto \Psi(\eta).$$

In addition, this embedding is $H^1_{\mathbb{R}}$-equivariant, namely,

$$\Psi(u\eta u^{-1}) = \Psi(u)\Psi(\eta)\Psi(u)^{-1} \quad \forall u \in H^1_{\mathbb{R}},\ \eta \in \mathcal{X}(H_{\mathbb{R}}).$$

Recall that the isomorphism $\Phi_{\mathbb{R}} : H_{\mathbb{R}} \cong \mathrm{Mat}_2(\mathbb{R})$ gives rise to the bijection

$$\mathcal{X}(H_{\mathbb{R}}) \to \mathcal{X}(\mathrm{Mat}_2(\mathbb{R})),\ \eta \mapsto \Phi_{\mathbb{R}}(\eta).$$

In light of (5.17), this gives us the $H^1_{\mathbb{R}}$-equivariant embedding

$$\mathfrak{o}^1\backslash\mathfrak{H} \cong \mathcal{M}(\mathfrak{o}) = \mathfrak{o}^1\backslash\mathcal{X}(H_{\mathbb{R}}) =$$

$$\mathfrak{o}^1\backslash\mathcal{X}(\mathrm{Mat}_2(\mathbb{R})) \to \mathrm{Sp}(\mathfrak{o}, E_\rho)\backslash\mathcal{Y}(H_{\mathbb{R}})$$

(here the injectiveness follows from (5.24)).

This construction was motivated by [67, Sect. 3, 4] where it was done in more explicit way as follows.

Proposition 5.13. *Let $\mathfrak{o}$ be a maximal order in H, and u_1, u_2, u_3, u_4 be a basis of $\mathfrak{o}$ such that the period matrix of A_τ with respect to $(\omega_1 = \phi_\tau(u_1), \ldots, \omega_4 = \phi_\tau(u_4))$ is equal to $(Z_\tau\ D)$, where $Z_\tau \in \mathfrak{H}_2$. Then, there exists a homomorphism of real Lie groups groups*

$$\Psi : \mathrm{SL}(2, \mathbb{R}) \to \mathrm{Sp}(4, \mathbb{R})$$

such that, for any $g \in \mathrm{SL}_2(\mathbb{R})$, the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{H} & \xrightarrow{\tau \mapsto Z_\tau} & \mathfrak{H}_2 \\ \Big\downarrow{\scriptstyle g} & & \Big\downarrow{\scriptstyle \Psi(g)} \\ \mathfrak{H} & \xrightarrow{\tau \mapsto Z_\tau} & \mathfrak{H}_2 \end{array}$$

We apply this by restricting the diagram to the subgroup $\Gamma = \Phi(\mathfrak{o}_1^*) \subset \mathrm{SL}(2, \mathbb{R})$, where

$$\mathfrak{o}_1^* = \{u \in \mathfrak{o} : \mathrm{Nm}(u) = 1\}.$$

We obtain a homomorphism $\Gamma \to \mathrm{Sp}(4, \mathbb{Z})$ which defines a holomorphic embedding

$$\mathcal{A}_S = \Gamma \backslash \mathfrak{H} \hookrightarrow \mathcal{A}_2 = \mathrm{Sp}(4, \mathbb{Z}) \backslash \mathfrak{H}_2. \tag{5.25}$$

The orbit space $\mathcal{A}_\mathcal{S}$ is the moduli space of fake elliptic curves defined by the PEL-data $\mathcal{S}$.

The group Γ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ that is *cocompact*, i.e. the quotient $\Gamma \backslash \mathfrak{H}$ is a compact Riemann surface. Such a quotient is called a *Shimura curve* [8, 175]. Conversely, any point on the curve $\Gamma \backslash \mathfrak{H}$ defines a polarized abelian surface with endomorphism algebra containing a subring isomorphic to $\mathfrak{o}$.

The curve $\Gamma \backslash \mathfrak{H}$ is the coarse moduli space of such abelian surfaces.

Remark 5.14. The moduli space of elliptic curves (with some level structure) is the orbit space $\Gamma \backslash \mathfrak{H}$ for a (non-compact) arithmetical discrete subgroup of $\mathrm{SL}(2, \mathbb{R})$, This gives a reason for naming abelian surfaces of QM-type fake elliptic curves.

Note that $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ contains totally real, and totally imaginary quadratic extensions K of $\mathbb{Q}$. By permuting $\mathbf{I}, \mathbf{J}, \mathbf{K}$, we may assume that $a > 0, b < 0$. Then, $K = \mathbb{Q}(\sqrt{a})$ is a totally real field, and $K = \mathbb{Q}(\sqrt{b})$ is a totally imaginary field.

Suppose that $\mathfrak{o}_\Delta$ is an order in the field $\mathbb{Q}(\sqrt{\Delta})$ with positive discriminant Δ, which is contained in H. Assume that $\mathfrak{o}_\Delta \subset \mathfrak{o}$, and the involution $*$ acts identically on $\mathfrak{o}_\Delta$. Then, a period Z_τ satisfies Humbert's singular relation with discriminant Δ, and the image of the isomorphism class of A_τ in $\mathcal{A}_2$ belongs to the Humber surface H_Δ. If there are different fields $K \subset H$ with this property, then the locus of the fake elliptic curves $\mathcal{A}_S$ is contained in the intersection of the corresponding Humbert surfaces.

Let $K \subset H$ be a totally imaginary quadratic field, and R be an order in K that embeds in the order $\mathfrak{o}$ of H. We assume that it is maximal with this property. There is a unique $\tau \in \mathfrak{H}$ which is fixed by K, the orbit of τ modulo $\mathrm{SL}(2, \mathbb{Z})$ represents an elliptic curve E with complex multiplication by $\mathfrak{o}$. The corresponding point in the Shimura curve $\Gamma \backslash \mathfrak{H}$ is called a *CM-point*. The image of R in $\mathrm{End}(A)$ preserves the principal polarization and the abelian variety A_τ becomes isomorphic to the self-product $E \times E$. Each Shimura curve has infinitely many CM-points corresponding to different embeddings of totally imaginary quadratic fields into H.

5.3 Examples of Fake Elliptic Curves

Let us give some examples of fake elliptic curves. We choose E in the PEL-data S to define a principal polarization, so that the abelian surface A_τ is isomorphic to the Jacobian variety of a curve of genus 2.

Example 5.15. (see [66]) Let $H = \left(\frac{-6,2}{\mathbb{Q}}\right)$. Let

$$u_1 = 1,\ u_2 = \tfrac{1}{2}(\mathbf{I}+\mathbf{J}),\ u_3 = \tfrac{1}{2}(\mathbf{I}-\mathbf{J}),\ u_4 = \tfrac{1}{2}(2+2\mathbf{J}+\mathbf{K}).$$

We check that $u_1, \dots, u_4$ generate an order in H. We compute

$$(\mathrm{tr}(u_i\bar{u}_j)) = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 4 & -1 \\ 0 & 4 & 2 & 1 \\ 1 & -1 & 1 & -2 \end{pmatrix}$$

The determinant of this matrix is equal to 6^2. This shows that the discriminant D is equal to 6, the product or prime numbers, hence $\mathfrak{o}$ spanned by $u_1, \dots, u_4$ is a maximal order. We take $\rho = \mathbf{I}$ and compute the matrix of $E(x,y) = \mathrm{tr}(\rho x\bar{y})$:

$$(\mathrm{tr}(\mathbf{I}u_i\bar{u}_j) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

In a new basis $u_1' = u_3,\ u_2' = -u_4,\ u_3' = -u_1,\ u_4' = u_3 - u_2$, the matrix of $R(x,y)$ is the standard symplectic matrix $J_4 = \left(\begin{smallmatrix} 0 & I_2 \\ -I_2 & 0 \end{smallmatrix}\right)$. We define $\Phi : H \to \mathrm{Mat}_2(\mathbb{R})$ by

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

The period matrix Π with columns $\phi_\tau(u_1'), \phi_\tau(u_2'), \phi_\tau(u_3'), \phi_\tau(u_4')$ is

$$\Pi = \begin{pmatrix} -\frac{\sqrt{2}\tau}{2} + \frac{1}{2} & (-\frac{1}{2} - \frac{\sqrt{2}}{2})\tau + \frac{\sqrt{2}}{4} & -\tau & -\sqrt{2}\tau \\ -3\tau + \frac{\sqrt{2}}{2} & \frac{3\sqrt{2}\tau}{2} - \frac{1}{2} + \frac{\sqrt{2}}{2} & -1 & \sqrt{2} \end{pmatrix}$$

Multiplying on the left by the inverse of the matrix with the last two columns, we get the period point of A_τ:

$$Z_\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} = \begin{pmatrix} \frac{6\tau^2-1}{4\tau} & \frac{-6\sqrt{2}\tau^2+4\tau-\sqrt{2}}{8\tau} \\ \frac{-6\sqrt{2}\tau^2+4\tau-\sqrt{2}}{8\tau} & \frac{6\tau^2+4\tau-1}{8\tau} \end{pmatrix} \in \mathfrak{H}_2$$

One checks that Z satisfies two singular equations[1]

$$\begin{aligned} -\tau_1 + 2\tau_3 - 1 = 0 \quad &\text{with } \Delta = 8, \\ \tau_2 - \tau_3 + (\tau_2^2 - 2t_2 - \tau_1\tau_3 + t_1 = 0 \quad &\text{with } \Delta = 5. \end{aligned} \tag{5.26}$$

[1] There is a small typo in [66]; one has to subtract 1 from the entries τ_2, τ_3 of their period matrix.

The following is the equation of a genus 2 curve X_{set} whose Jacobian variety is isomorphic, as a principally polarized abelian surface, to the surface $A_\tau = \mathbb{C}^2/Z_\tau\mathbb{Z}^4$ for a "general" τ (see [8]):

$$X_{s,t} : y^2 - x(x^4 - Px^3 + Qx^2 - Rx + 1) = 0, \tag{5.27}$$

where

$$P = -2(s+t),\ R = -2(s-1),\ Q = \frac{(1+2t^2)(11-28t^2+8t^4)}{3(1-t^2)(1-4t^2)},$$

and $F(s,t) = 4s^2t^2 - s^2 + t^2 + 2 = 0$. The curve $V(F(s,t))$ is the affine part of the quartic curve $B := V(4s^2t^2 - s^2u^2 + t^2u^2 + 2u^4)$ with two ordinary nodes $(0:1:0)$ and $(1:0:0)$. The involution $\sigma : (s,t) \mapsto (s,-t)$ does not change the isomorphism class of the curve $X_{s,t}$. One can show, using the invariant of binary forms of degree 6, that involution also interchanges the branches at singular points, so that the quotient of the curve B by the involution is isomorphic to $\mathbb{P}^1$. The Shimura curve $\mathcal{S}_6 := \Gamma\backslash\mathfrak{H}_2$ is isomorphic to $\mathbb{P}^1$. The map $B/(\sigma) \to \mathcal{A}_S$ is not defined at the point $(s,t) = (\frac{1}{2}\sqrt{-2}, \sqrt{2})$ since the curve $X_{s,t}$ is singular. However, it extends to an isomorphism $B/(\sigma) \to \mathcal{A}_S$.

Let $K = \mathbb{Q}(\sqrt{-6})$ with maximal order $R = \mathbb{Z}[\sqrt{-6}]$. It embeds in H, and $\Phi(\sqrt{-6}) = \Phi(\mathbf{I}) = \left(\begin{smallmatrix} 0 & 1 \\ -6 & 0 \end{smallmatrix}\right)$. Its fixed point in $\mathfrak{H}$ is $\tau_0 = \frac{\mathbf{i}}{\sqrt{6}}$. The period point Z_{τ_0} of the abelian surface A_{τ_0} is

$$\begin{pmatrix} \frac{\mathbf{i}}{\sqrt{6}} & -\frac{1}{2}\mathbf{i} + \frac{\sqrt{6}}{4} \\ -\frac{1}{2}\mathbf{i} + \frac{\sqrt{6}}{4} & \frac{1}{2} \end{pmatrix}.$$

The abelian variety is the Jacobian variety of a curve of genus 2 which is isomorphic to the self-product of the elliptic curve with complex multiplication by $\sqrt{-6}$.

Example 5.16. (see [8]) Let $H = \left(\frac{2,5}{\mathbb{Q}}\right)$. Let $\mathfrak{o}$ be an order in H generated by

$$u_1 = 1,\ u_2 = \mathbf{I},\ u_3 = \tfrac{1}{2}(\mathbf{I} + \mathbf{K}), u_4 = \tfrac{1}{2}(1 + \mathbf{J})$$

We take $\rho = \mathbf{K}$ with $\rho^2 = -10$, and compute

$$(\mathrm{tr}(u_i\bar{u}_j) = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & -4 & -2 & 0 \\ 0 & -2 & 4 & 0 \\ 1 & 0 & 0 & -2 \end{pmatrix}.$$

The determinant of the matrix is equal to 10^2; hence $\mathfrak{o}$ is a maximal order. We take $\rho = \mathbf{K}$, and compute

$$(E(u_i,u_j)) = \frac{1}{10}(\mathrm{tr}(\rho u_i\bar{u}_j)) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Let $\Phi : H \hookrightarrow \mathrm{Mat}_2(\mathbb{R})$ be the embedding defined by

$$\Phi(\mathbf{I}) = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}, \quad \Phi(\mathbf{J}) = \begin{pmatrix} 0 & 1 \\ 5 & 0 \end{pmatrix}.$$

The period matrix is:

$$\Pi_\tau = \begin{pmatrix} \tau & \sqrt{2}\tau & \frac{\sqrt{2}}{2}(\tau+1) & \frac{1}{2}(\tau+1) \\ 1 & -\sqrt{2} & -\frac{\sqrt{2}}{2}(5\tau+1) & \frac{1}{2}(5\tau+1) \end{pmatrix}.$$

Multiplying on the left by the inverse of the matrix with the last two columns, we get the period point

$$Z_\tau = \begin{pmatrix} \frac{1}{2}\frac{\sqrt{2}(5\tau^2-1)}{5\tau^2+6\tau+1} & \frac{\tau}{\tau+1}+\frac{1}{5\tau+1} \\ \frac{\tau}{\tau+1}+\frac{1}{5\tau+1} & \frac{\sqrt{2}(5\tau^2-1)}{5\tau^2+6\tau+1} \end{pmatrix} \in \mathfrak{H}_2.$$

Let $K = \mathbb{Q}(\sqrt{-10})$ with discriminant equal to -40 and maximal order $\mathbb{Z}[\sqrt{-10}]$. It embeds in $\mathfrak{o}$ and $\Phi(\sqrt{-10}) = \Phi(\mathbf{K}) = \begin{pmatrix} 0 & \sqrt{2} \\ -5\sqrt{2} & \end{pmatrix}$. It fixes $\tau = \frac{\mathbf{i}}{\sqrt{5}}$. There is another embedding of K in $\mathfrak{o}$ corresponding to the automorphism of H defined by $x \mapsto (3-2\mathbf{I})x$. It fixes $\tau_2 = (3-2\sqrt{2})\tau$. This gives two CM-points in the Shimura curve defined by the same period matrix[2]

$$Z_{\tau_1} = Z_{\tau_2} = \begin{pmatrix} \frac{\sqrt{10}}{6} & \frac{1}{3} \\ \frac{1}{3} & \frac{\sqrt{10}}{3} \end{pmatrix}.$$

The corresponding hyperelliptic curves are isomorphic to the curve with the equation:

$$y^2 = x^5 + 2\sqrt{5}x^4 + \frac{125}{18}x^3 + 2\sqrt{5}x^2 + x.$$

[2]There is a mistake in the computation of the period matrix in [8] that causes the conclusion that the periods are different.

Chapter 6

K3 Surfaces and Abelian Surfaces

In the case of abelian surfaces, the associated Kummer surface admits a resolution of singularities which is isomorphic to a *K3 surface*, a complex projective algebraic surface X with the canonical class $K_X \in H^2(X, \mathbb{Z})$ equal to zero and the first Betti number $b_1(X)$ also equal to zero. In this chapter we discuss some geometrical properties of K3 surfaces arising from abelian surfaces.

6.1 Generalities about K3 Surfaces

Let X be an algebraic K3 surface. By definition, this means that X is a smooth and projective surface with $K_X = -c_1(X) = 0$ and $h^1(\mathcal{O}_X) = 0$. Note that there exist compact complex, but not algebraic surfaces satisfying these conditions. They admit a structure of a Kähler manifold. However, we will be concerned only with algebraic K3 surfaces.

Let us give a brief information about some important algebraic and topological invariants of X (we refer to [7] or [32, §10, Chapter 0] for details).

Since $c_1(K) = -K_X = 0$, by Wu's formula, $H^2(X, \mathbb{Z})$ is an even lattice with respect to the cup-product, which is a symmetric bilinear form. By Poincaré duality, it is unimodular. Since $h^1(\mathcal{O}_X) = 0$, the Betti numbers b_1 and b_3 are equal to zero. By Noether's formula

$$12(1 - h^1(\mathcal{O}_X) + h^2(\mathcal{O}_X)) = K_X^2 + c_2,$$

where the second Chern class c_2 coincides with the topological Euler-Poincaré characteristic of X. This gives us that the second Betti number b_2 is equal to 22. By Hirzebruch's signature theorem, the signature of the cup-product on $H^2(X, \mathbb{R})$ is equal to $(3, 19)$. Thus, by Milnor's theorem on unimodular indefinite quadratic lattices, we get an isomorphism of quadratic lattices

$$H^2(X, \mathbb{Z}) \cong \mathbf{L} := \mathsf{U}^{\oplus 3} \oplus \mathsf{E}_8^{\oplus 2},$$

where U is the integral hyperbolic plane, and E_8 is the E_8-lattice defined by the Dynkin diagram (3.15) in Section 3.1. The quadratic lattice $\mathbf{L}$ in the right-hand side is often called the *K3 lattice*

Let

$$\mathrm{H}^2(X,\mathbb{C}) = H^{2,0} \oplus H^{1,1} \oplus H^{0,2} \cong \mathbb{C} \oplus \mathbb{C}^{20} \oplus \mathbb{C}, \tag{6.1}$$

be the Hodge decomposition of $H^*(X,\mathbb{C})$. Since $h^{2,0} = h^{0,2}h^1(\mathcal{O}_X) = 1$, it $h^{1,1}(X) = 20$.

The Picard group $\mathrm{Pic}(X)$ is isomorphic to the Néron-Severi group $\mathrm{NS}(X)$. The Chern class homomorphism

$$c_1 \,:\, \mathrm{Pic}(X) \,\to\, H^2(X,\mathbb{Z}) \tag{6.2}$$

is injective and its image lies in $H^2(X,\mathbb{Z}) \cap H^{1,1}(X)$. This implies that the Picard number $\rho(X)$ satisfies

$$1 \,\leq\, \rho(X) \,\leq\, 20.$$

The intersection form on $\mathrm{Pic}(X)$ defines a structure of a quadratic lattice on $\mathrm{Pic}(X)$. The Chern class homomorphism c_1 respects the intersection forms on both sides and thus, identifies $\mathrm{Pic}(X)$ with a sublattice of $H^2(X,\mathbb{Z})$. Also, via the Poincaré Duality, it can be identified with the sublattice of $H_2(X,\mathbb{Z}) \,\cong\, H^2(X,\mathbb{Z})^\vee$. It is generated by the fundamental classes of irreducible algebraic curves in X. We denote it by S_X and call it the *Picard lattice*.

It follows from Lefschetz's theorem on $(1,1)$-classes that the lattice embedding (6.2) is primitive (the latter means that the quotient group has no torsion). By the Hodge Index Theory, the signature of the quadratic space $(S_X)_\mathbb{R}$ is equal to $(1,\rho(X)-1)$, so S_X is a primitive sublattice of $H^2(X,\mathbb{Z})$ of signature $(1,\rho(X))$.

Let T_X denote the orthogonal complement of S_X in $H^2(X,\mathbb{Z})$. It is a primitive sublattice of $H^2(X,\mathbb{Z})$, called the *transcendental lattice* of X. We use the Hodge decomposition (6.1). Since the image of S_X under the homomorphism c_1 is contained in $H^2(X,\mathbb{Z}) \cap H^{1,1}$,

$$(T_X)_\mathbb{C} = H^{2,0} \oplus H^{1,1}_0 \oplus H^{0,2} \cong \mathbb{C}^{22-\rho},$$

where $H^{1,1}_0 = (T_X)_\mathbb{C} \cap H^{1,1}$. Since the signature of $H^2(X,\mathbb{R})$ is equal to $(3,19)$, T_X is a primitive sublattice of $H^2(X,\mathbb{Z})$ of signature $(2,20-\rho(X))$.

The inclusion of the one-dimensional linear space $H^{2,0} \,\subset\, (T_X)_\mathbb{C}$ defines a point $\mathfrak{p}(X)$ in the projective space $|(T_X)_\mathbb{C}|$ of lines in $((T_X)_\mathbb{C}$ (or the projective space $\mathbb{P}((T_X^\vee)_\mathbb{C})$). It is called the *period* of X.

If we choose a holomorphic 2-form ω generating $H^{2,0}(X)$, then, considered as a linear function on $H_2(X,\mathbb{C})$, its value on a 2-cycle γ is equal to the integral $\int_\gamma \omega$. If γ is equal to the fundamental class of an irreducible curve, then $\int_\gamma \omega = 0$ (because the restriction of ω to a curve is equal to zero). This explains why the linear function $\int_\gamma$ can be considered as a linear function on $H_2(X,\mathbb{Z})/S_X$, and hence belongs to $H^{2,0} \oplus H^{0,2}$. Since, ω is represented by a complex differential form of type $(2,0)$, it belongs to $H^{2,0}$.

The cup-product on $H^2(X,\mathbb{C})$ corresponds, via the de Rham Theorem, to the exterior product $\omega_1 \wedge \omega_2$ of 2-forms. Since $\omega \in H^{2,0}$, we get $w \wedge w = 0$. The cup-product is the complexification of the intersection form on $H^2(X,\mathbb{Z})$, hence $\mathfrak{p}(X)$ belongs to a quadric Q in $|(T_X)_\mathbb{C}$ defined by the quadratic form of the transcendental quadratic lattice T_X.

Also, $\omega \wedge \bar{\omega}$ is a real differential 4-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 complex scalar multiple of ω, we may

choose an orientation on the four-manifold X to assume that it is positive. Thus, we get a second condition $\omega \wedge \bar{\omega} > 0$. Thus, $\mathfrak{p}(X)$ belongs to an an open (in the usual topology) subset Q^0 of Q.

Since the signature of the quadratic space $(T_X)_{\mathbb{R}}$ is equal to $(2, 20 - \rho(X))$, the Q^0 is not connected, it consists of two connected components, each isomorphic to a Hermitian symmetric domain of orthogonal type (or Type IV in Cartan's classification). To see these two components, we choose a basis in $(T_X)_{\mathbb{C}}$ with coordinates $t_1, t_2, \ldots, t_k$, where $k := \text{rank}(T_X)$, such that $\mathcal{D}_T$ consists of points in $|(T_X)_{\mathbb{C}}|$ with projective coordinates $[z_1, \ldots, z_n]$ satisfying

$$z_1^2 + z_2^2 - z_3^2 - \cdots - z_k^2 = 0,$$
$$|z_1|^2 + |z_2|^2 - |z_3|^2 - \cdots - |z_k|^2 > 0,$$

This set consists of two connected components that are distinguished by the sign of $\text{Im}(t_1/t_2)$. Another way to see this is to consider a real plane $P(z) \subset (T_X)_{\mathbb{R}}$ spanned by the imaginary and real part of a vector $z = x + iy \in (T_X)_{\mathbb{C}}$ that represents a point $[z]$ in the quadric Q. Then, $0 = z^2 = (x + iy)^2$ implies $x^2 - y^2 = x \cdot y = 0$ and $z \cdot \bar{z} = (x + iy) \cdot (x - iy) > 0$ implies $x^2 + y^2 > 0$. Thus, $x^2 = y^2 > 0$ and $x \cdot y = 0$ implies that $P(z)$ is a positive definite plane in $T_{\mathbb{R}}$. This defines a map from $\mathcal{Q}_N$ to the Grassmannian $G(2, (T_X)_{\mathbb{R}})^+$ of positive definite planes in $T_{\mathbb{R}}$. It consists of two connected components defined by a choice of orientation of the plane.

We would like to define the *period map* that assigns to the isomorphism class of X its period point $\mathfrak{p}(X) \in Q$. However, there is a problem because there is no canonical identification of the linear spaces $H^(X, \mathbb{C})$ for different X, and, even more, the linear subspaces $(T_X)_{\mathbb{C}}$ can vary in a family of K3 surfaces.

To solve this problem, one introduces the notions of a *lattice polarization* and a *marking* of X. The former is a primitive embedding:

$$j : S \hookrightarrow S_X$$

of lattices, where S is a fixed even quadratic sublattice of the K3-lattice $\mathbf{L}$ with signature $(1, \rho)$. The latter is an isomorphism: of quadratic lattices

$$\phi : \mathbf{L} \to H^2(X, \mathbb{Z}).$$

We assume that the two homomorphisms are compatible in the sense that the restriction of ϕ to S coincides with j. Moreover, we assume that $j(S)$ contains an ample divisor class in S_X.

Now, we repeat everything from above, replacing S_X with S, and denoting by T its orthogonal complement in $\mathbf{L}$. The signature of T is equal to $(2, 20 - \rho)$.

Let Q_T be the quadric in $|T_{\mathbb{C}}|$ defined by the quadratic form of T, and let $\mathcal{D}_T = Q_T^0$ be its open subset defined by the condition $x \cdot \bar{x} > 0$. It is called the *period domain* associated to the lattice T. Of course, as a complex manifold, it depends only on its dimension $19 - r$. It consists of two connected components. Each connected component is a complex domain in $\mathbb{C}^{20-\rho}$ of vectors $z = x + \mathbf{i}y$ with $y \cdot y > 0$.

The orthogonal group of the real space $T_{\mathbb{R}}$ is isomorphic to the orthogonal group $\text{O}(2, 19 - \rho)$ of the standard inner product space $\mathbb{R}^{2,19-r}$ defined by the quadratic form $x_0^2 + x_1^2 - \sum_{i=3}^{19-\rho} x_i^2$. It acts on the quadric Q_T leaving the subset $\mathcal{D}_T$ invariant. The action is transitive, and the stabilizer

subgroup isomorphic to the subgroup $\mathrm{SO}(2) \times \mathrm{O}(19-r)$. This defines a structure of homogenous spaces on $\mathcal{D}_T$ and on its connected component $\mathcal{D}_T^0$:

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

Now, let (X, S, j, ϕ) be a marked lattice polarized K3 surface and $\mathfrak{p}(X)$ be its period. Then, we can assign to X a point $\phi^{-1}(\mathfrak{p}) \in \mathcal{D}_T$, called the *period point* (X, S, j, ϕ). A different choice of the markings which restrict to the same polarization map $j : M \to S_X$ does not change the orbit of $\mathfrak{p}$ with respect to the group

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

There is a natural injective homomorphism $\Gamma_S \to \mathrm{O}(T)$. To describe its image, one introduces the notion of the *discriminant group* A_M of an even lattice M, and its quadratic form q_{A_M}. We assume that M is non-degenerate in sense that the natural map $\iota : M \to M^\vee = \mathrm{Hom}(M, \mathbb{Z})$ defined by the symmetric bilinear form on M, is injective. We set

$$\begin{aligned} A_M : &= M/\iota(M), \\ q_{A_M} &: A_M \to \mathbb{Q}/2\mathbb{Z}, \quad \tilde{m} + M \mapsto \tilde{m}^2 \mod 2\mathbb{Z}. \end{aligned} \tag{6.3}$$

Here $\tilde{m} \in M^\vee$ is a representative of a coset in A_M, and we extend the quadratic form of M to $M^\vee \subset M_{\mathbb{Q}}$.

An orthogonal transformation g of M extends to an orthogonal transformation of $M^\vee \subset M_{\mathbb{Q}}$ that induces an automorphism of the finite group A_T that preserves the function q_{A_M}. We denote the group of such automorphisms of A_M by $\mathrm{O}(A_M, q_{A_M})$. One can show that

$$\Gamma_S = \mathrm{Ker}(\mathrm{O}(T) \to \mathrm{O}(A_T, q_{A_T})).$$

Assume $\rho > 1$, so that the lattice $\mathrm{Pic}(X)$ is hyperbolic. By adjunction formula, any divisor class D with negative self-intersection satisfies $D^2 = -2$. By Riemann-Roch Theorem, D, or $-D$ is effective. If D is a curve on X representing D, then one of its irreducible components R satisfies $R^2 = -2$, and hence its arithmetic genus $\frac{1}{2}(R^2 + R \cdot K_X) + 1$ is equal to zero. Thus, $R \cong \mathbb{P}^1$ is a smooth rational curve on X. Such a curve R is called a (-2)-curve. Its divisor class is unique, therefore we can identify it with a vector in the Picard lattice $\mathrm{Pic}(X)$.

Now, we can consider the orbit space

$$\mathcal{M}_{K3,S} := \Gamma_T \backslash \mathcal{D}_T.$$

Thus, taking the orbit of the period of a marked lattice polarized K3 surface (X, S, ϕ, j) defines a point (the *period point*) in $\mathcal{M}_{K3,S}$ that does not depend on the marking. The orbit space is a quasi-projective algebraic variety of dimension $20 - \rho$. Under some mild conditions on S, e.g. the lattice T contains the integral hyperbolic plane U as its orthogonal complement, the orbit space is irreducible.

We have the fundamental Global Torelli Theorem for K3 surfaces due to I. Pyatetsky-Shapiro and I. Shafarevich:

Theorem 6.1. *Suppose two lattice polarized K3 surfaces (X, S, j) and (X', S, j') define the same period point in $\Gamma_S\backslash\mathcal{D}_S$. Then, there exists an isomorphism $f : X' \to X$ such that $j' = f^* \circ j$.*

Note that the period points belong to an open Zariski subset $\mathcal{D}_S^\circ$ of $\mathcal{D}_S$. Let us explain this. For any $\delta \in T$ with $\delta^{-2} = -2$, the orthogonal complement $\delta^\perp$ contains S. If If the period of (X, S, ϕ, j) belongs to H_δ, then δ must be equal to an algebraic cycle γ in X with $\gamma^2 = -2$. By Riemann-Roch Theorem on X, γ or $-\gamma$ is the divisor class of an effective divisor on X. However, this contradicts the assumption that $j(S)$ contains an ample divisor.

Let

$$\Delta_S = \cup_{\delta\in T,\delta^2=-2} H_\delta,$$

where $H_\delta = |\delta^\perp| \cap \mathcal{D}_S$. It follows that the period points belong to the complement $\mathcal{D}_S^\circ = \mathcal{D}_S \setminus \Delta_S$. The group Γ_S acts naturally on the set of vectors δ, and hence acts on the set Δ_S. We set

$$\mathcal{M}^a_{K3,S} := \Gamma_S\backslash\mathcal{D}_S^\circ.$$

Note that the image $\Gamma_S\backslash\Delta_S$ is a divisor in $\mathcal{M}_{K3,S}$. The number of its irreducible components is equal to the number of orbits of Γ_S on the set of vectors δ. The situation is similar to what we had for the description of irreducible components of Humbert surfaces. One has to warn, that the notation $\mathcal{M}_{K3,S}$ is rather ambiguous since the variety $\mathcal{M}_{K3,S}$ depends on the embedding of S into $\mathbf{L}$. However, in many cases, one can show that the embedding is unique modulo the orthogonal group of $\mathbf{L}$, and hence the orbits spaces are isomorphic.

One can show that $\mathcal{M}^a_{K3,S}$ is isomorphic to the coarse moduli space of lattice S polarized K3 surfaces. To do this, one extends the notion of a lattice polarized marked K3 surface to a smooth family $\mathcal{X} \to B$ of K3 surfaces. We define a marking of the family to be an isomorphism of local coefficient systems extra bracket was deleted $\phi : (\mathbf{L})_B \to H^2(X_t, \mathbb{Z})_{t\in B}$, where $(\mathbf{L})_B$ is the trivial local coefficient system with fiber $\mathbf{L}$. It is required that, for all $t \in B$, the image of S under the isomorphism $\phi_t : \mathbf{L} \to H^2(X_t, \mathbb{Z})$ is contained in $\mathrm{Pic}(X_t)$, and also contains an ample divisor class of X_t.

A family $\mathcal{X} \to B$ of lattice S polarized marked K3 surface defines the period map

$$\mathfrak{p}_B : B \to \mathcal{M}^a_{K3,S},$$

and, using the Global Torelli Theorem, one proves that, in this way, the algebraic variety $\mathcal{M}^a_{K3,S}$ is isomorphic to the coarse moduli spaces of lattice S polarized K3 surfaces. We refer to the details to [42].

One can also interpret $\mathcal{M}_{K3,S}$ as the moduli space of lattice polarized K3 surfaces where we drop the assumption that $j(S)$ contains an ample divisor, but assume only that it is a pseudo-ample divisor. However, it is too technical to describe it here.

One can extend the notion of a hyperplane $H_\delta, \delta^2 = -2$, by assuming that $\delta^2 = -N$, where N is any even positive integer N. Then, $T' = \delta^\perp$ is a sublattice of T of signature $(2, 18 - \rho)$ and $\mathcal{D}^\circ_{T'}$ is a Hermitian symmetric domain of the same type, and $\mathcal{D}_{T'}$ is realized as a hypersurface in $\mathcal{D}_T$. For any positive integer N consider

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

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 $\mathrm{Heeg}(S;N)$ and is called the *Heegner divisor* in the moduli space of lattice S polarized K3 surfaces.

In Section 6.4, we will compare the Heegner divisors

$$\mathrm{Heeg}_n(N) := \mathrm{Heeg}(S;N), \tag{6.4}$$

where $S = \mathsf{E}_8 \oplus \mathsf{E}_8 \oplus \langle -2n \rangle$ with the Humbert surfaces $\mathrm{Hum}_n(\Delta)$, where $N = \Delta/2n$.

6.2 Nikulin K3 Surfaces

Let $\mathrm{Kum}(A)$ be the Kummer surface of an abelian surface A and X be its minimal resolution of singularities obtained as the quotient of the blow-up $\tilde{A}$ of A at its set of 2-torsion points by the lift $\tilde{\iota}$ of the involution $\iota = [-1]_A$ of A. The cover $\tilde{\phi} : \tilde{A} \to X$ is a degree two cover with the branch divisor equal to the sum $R = R_1 + \cdots + R_{16}$ of exceptional curves of the resolution $\sigma : X \to \mathrm{Kum}(A)$.

In general, let $S' \to S$ be a double cover of smooth surfaces branched over a curve (necessary smooth) B on S. Let $\psi_U = 0$ be a local equation of B in an affine open subset U, then the pre-image of U in S' is isomorphic to the hypersurface in $V = U \times \mathbb{C}$ given by the equation $z_U^2 - \psi_U = 0$. Thus, locally the ring $\mathcal{O}(V)$ of regular functions on V is a free module of rank 2 over the ring $\mathcal{O}(U)$ of functions on U generated by 1 and z_U. Let $\mathcal{O}(U)z_u$ be the submodule of rank 1. One checks that, taking an affine cover of S, the $\mathcal{O}(U)$-modules $\mathcal{O}(U)z_u$ are glued together to define a line bundle L such that $L^{\otimes -2}$ is isomorphic to the line bundle $L(B) = \mathcal{O}_S(B)$ associated to the curve B. It may not have sections but its tensor square has a section with the zero divisor equal to B. In particular, we see that the divisor class of B is divisible by 2 in the Picard group $\mathrm{Pic}(S)$. Conversely, if B is a smooth curve on S such that its divisor class $[B]$ is divisible by two in $\mathrm{Pic}(S)$, there exists a double cover of smooth surfaces $S' \to S$ with the branch divisor B. The set of isomorphism classes of such covers is bijective to the set of square roots of $[B]$ in $\mathrm{Pic}(S)$. It is a principal homogeneous space over the group $\mathrm{Pic}(S)[2]$ of 2-torsion points in $\mathrm{Pic}(S)$.

Let us return to our example. We see that the sum $R = R_1 + \cdots + R_{16}$ must be divisible by 2 in $\mathrm{Pic}(\tilde{X})$. Since $\tilde{X}$ is a K3 surface, we have $\mathrm{Tors}(\mathrm{Pic}(\tilde{X})) = 0$, hence $[R] = 2[R_0]$ for a unique divisor class R_0. Since $R^2 = 16(-2) = -32$, we obtain $R_0^2 = -8$. It is easy to see that the line bundle $\mathcal{O}_{\tilde{X}}(R_0)$ has no sections but its tensor square has a unique section (up to a constant multiple) vanishing on R.

Suppose we have a disjoint set of (-2)-curves $E_1, \ldots, E_k$ on a K3 surface Y, we ask whether there exists a double cover $Y' \to Y$ with branch divisor equal to $E = E_1 + \cdots + E_k$. Since $E^2 = -2k = 4D^2$ for some divisor D and D^2 is even, we obtain that $k \in \{4, 8, 12, 16\}$ (it cannot be larger since the classes $[E_i]$ are linearly independent in $\mathrm{H}^2(Y, \mathbb{Q}) = \mathbb{Q}^{22}$). Let $f : Y' \to Y$ be the double cover with the branch divisor E and let $R = R_1 + \cdots + R_k$ be the ramification divisor on Y'. Since $f^*(E_i) = 2R_i$, we have $R_i^2 = -1$. The standard Hurwitz type formula gives us that $K_{Y'} = f^*(K_Y) + R = R$. Since each R_i is an exceptional curve of the first kind, we can blow down R to obtain a surface Y with $K_Y = 0$. It is known that a surface with trivial canonical class is either an abelian surface or a K3 surface. Now the standard topological formula gives us that

$e(Y') = 2e(X) - e(R) = 48 - 2k = e(Y) + k$. This gives $e(Y) = 48 - 3k$. If Y is an abelian surface, we obtain $k = 16$. If Y is a K3 surface, we obtain $k = 8$.

Note that a theorem of V. Nikulin asserts that any disjoint sum of sixteen (-2)-curves on a K3 surface is divisible by 2 in the Picard group and hence defines a double cover birationally isomorphic to an abelian surface A [132]. It is easy to see that it implies that X is birationally isomorphic to $\mathrm{Kum}(A)$.

In the case $k = 8$, we have more possibilities. A set of eight disjoint (-2)-curves on a K3 surface Y is called an *even eight*, if the divisor class of the sum is divisible by 2 in $\mathrm{Pic}(Y)$.

Let $E_1, \dots, E_8$ be an even eight on a K3 surface Y and $\pi : \tilde{Y} \to Y$ be the corresponding double cover. Let $\bar{E}_1 + \cdots + \bar{E}_8$ be the ramification divisor on $\tilde{Y}$. We have $\pi^*(E_i) = 2\bar{E}_i$, hence $4\bar{E}_i^2 = 2E_i^2 = -4$, hence $\bar{E}_i^2 = -1$. Also $\bar{E}_i \cong E_i$, hence $\bar{E}_i \cong \mathbb{P}^1$. Thus, $\bar{E}_i$ is an exceptional curve of the first kind, and hence, can be blown down to a smooth point of a surface. Let $\sigma : \tilde{Y} \to Y'$ be the blow-down of the eight exceptional curves $\bar{E}_i$. As above, we obtain that $e(\tilde{Y}) = 2e(Y) - e(\bar{E}) = 48 - 16 = 32$. This shows that $e(Y') = 32 - 8 = 24$. Also, we have $K_{\tilde{Y}} = \sigma^*(K_Y) + \bar{E} = \bar{E}$, hence $K_{Y'} = 0$. Together with the Noether formula this implies that $b_1(Y') = 0$, hence Y' is a K3 surface. Let $\tilde{\tau}$ be the deck transformation of the cover σ, it descents to an involution (= an automorphism of order 2) τ of Y'. It has 8 fixed points, the images of the curves $\bar{E}_i$ on Y'. The quotient $Y'/(\tau)$ is a surface $\bar{Y}$ with 8 ordinary double points. The rational map $\pi \circ \tilde{\pi} \circ \tilde{\sigma}^{-1} : Y \to \bar{Y}$ is a minimal resolution of the surface $\bar{Y}$. We have the following commutative diagram of regular maps:

$$\begin{array}{ccc} \tilde{Y} & \xrightarrow{\tilde{\sigma}} & Y \\ \downarrow{\scriptstyle \tilde{\pi}} & & \downarrow{\scriptstyle \pi} \\ Y' & \xrightarrow{\sigma} & \bar{Y} \end{array} .$$

Thus, we obtain that each even eight on a K3 surface Y defines a K3 surface Y' and an involution τ on Y' such that Y is isomorphic to a minimal resolution of the singular surface $Y/(\tau)$. One can show that any involution on a K3 surface that acts identically on a holomorphic 2-form (a *symplectic involution*) has eight fixed points. The group quotient $Y'/(\tau)$ has a minimal resolution of singularities isomorphic to a K3 surface with exceptional curves forming an even eight. A K3 surface obtained in this way is called a *Nikulin K3 surface*. One expects that the Picard number of a general Nikulin surface is equal to nine, and the moduli spaces of polarized Nikulin surfaces have dimension equal to 11.

We will be interested in Nikulin surfaces isomorphic to a nonsingular minimal model X of the Kummer surface $\mathrm{Kum}(A)$.

Let $E = E_1 + \cdots + E_8$ be an even eight on X. We know that $E \sim 2E_0$, where $E_0^2 = -4$. Let N be the sublattice of $\mathrm{Pic}(X)$ generated by E_0 and $E_1, \dots, E_8$. It is a negative definite even lattice of rank 8, called the *Nikulin lattice*. It contains the sublattice spanned by $E_1, \dots, E_8$ isomorphic to $\langle -2 \rangle^{\oplus 8}$, where $\langle a \rangle$ denotes the lattice of spanned by a vector v with $v^2 = a$. This lattice is of index 2 in the lattice N, hence the elementary theory of finite abelian groups tells us that the discriminant group of N is equal $(\mathbb{Z}/2\mathbb{Z})^6$. The inclusion $N \hookrightarrow S_X$ is a primitive embedding. Thus, each Nikulin surface must contain a primitive sublattice isomorphic to the Nikulin lattice.

One can show that the Nikulin involution τ acts on $\mathrm{H}^2(Y', \mathbb{Z}) \cong L_{K3} = \mathsf{U}^{\oplus 3} \oplus \mathsf{E}_8^{\oplus 2}$ as the identity on $U^{\oplus 3}$ and by sending a vector in E_8 to the same vector in the other copy of E_8. Let $H^\tau \cong \mathsf{U}^{\oplus 3} \oplus \mathsf{E}_8(2)$ be the sublattice of invariant elements and $H_\tau \cong \mathsf{E}_8(2)$ be the sublattice of anti-invariant elements (i.e. $\tau^*(\gamma) = -\gamma$).[1] Note that τ acts identically on $\Omega^2(X') \cong \mathbb{C}$, since otherwise the quotient has no regular 2-forms, so it must be a symplectic involution. Thus, for any cycle $\gamma \in H_\tau$, we have

$$0 = \int_{\gamma+\tau^*(\gamma)} \omega = \int_\gamma \omega + \int_{\tau^*(\gamma)} \tau^*(\omega) = 2\int_\gamma \omega.$$

By Lefschetz Theorem, this implies that $\gamma \in S_X = \mathrm{H}^2(X, \mathbb{Z})_{\mathrm{alg}}$. Since H_τ and H^τ are obviously orthogonal to each other, we obtain

$$\mathsf{E}_8(2) \cong H_\tau \subset S_X, \quad T_X \subset H^\tau \cong \mathsf{U}^{\oplus 3} \oplus \mathsf{E}_8(2).$$

Nikulin shows that the converse is true: if S_Y contains a primitive sublattice S isomorphic to $E_8(2)$, then there exists a Nikulin involution τ on Y' such that $S \subset H_\tau$.

Note that under the rational cover $f : Y' \to Y'/(\tau) \overset{\pi^{-1}}{\dashrightarrow} Y$, we have

$$f^*(T_Y) \cong T_Y(2) \subset T_{Y'}.$$

Now suppose $Y = \widetilde{\mathrm{Kum}}(A)$. One can show that, under the pre-image map $A \dashrightarrow Y$, we have $T_Y \cong T_A(2)$.

6.3 Shioda-Inose Structure

Suppose $\mathrm{Kum}(A)$ is a quotient of a K3 surface Y by a Nikulin involution. Then, by above, $T_Y(2) = T_A(4) \subset T_Y$. One can show that this inclusion comes from an inclusion $T_Y \subset T_A$ with quotient $(\mathbb{Z}/2\mathbb{Z})^\alpha$, where $0 \le \alpha \le 4$ (for any $x \in T_A$ we have $2x \in 2T_A \subset T_X$). Conversely, if there exists a primitive embedding $T_Y \hookrightarrow T_A$ with such a quotient, then Y admits a Nikulin involution with quotient isomorphic to $\mathrm{Kum}(A)$. If $\alpha = 0$, then we have $T_Y \cong T_A$, and, in this case we say that X admits a *Shioda-Inoue structure*. Even eights with $\alpha \neq 0$ were studied in [114].

Note that $T_A \subset \mathrm{H}^2(A, \mathbb{Z}) \cong U^{\oplus 3}$, hence,

$$T_Y \subset U^3 \subset L_{K3} = \mathsf{U}^3 \oplus \mathsf{E}_8 \oplus \mathsf{E}_8$$

and, we obtain that $\mathsf{E}_8 \oplus \mathsf{E}_8 \subset S_Y$. Here we have to use some lattice theory to check that all primitive embeddings of T_Y in L_{K3} are equivalent under orthogonal transformations of L_{K3}. Conversely, a theorem of D. Morrison [123] asserts that the condition that $\mathsf{E}_8 \oplus \mathsf{E}_8$ primitively embeds in S_X is necessary and sufficient in order X admits a Shioda-Inose structure. We express this structure by the triangle of rational maps

$$\begin{array}{ccc} X & & A\,. \\ & \searrow \quad \swarrow & \\ & \mathrm{Kum}(A) & \end{array} \tag{6.5}$$

[1] For any quadratic lattice M we denote by $M(k)$ the quadratic lattice obtained from M by multiplying its quadratic form by an integer k.

Example 6.2. Suppose A has a principal polarization L_0. We have $(L_0)^2 = 2$, hence

$$T_A \subset \langle L_0 \rangle^\perp = \mathsf{U} \oplus \mathsf{U} \oplus \langle -2 \rangle$$

(we embed $h = c_1(L_0)$ in one copy of $\mathsf{U} = \mathbb{Z}f + \mathbb{Z}g$ with the image of h equal to $f + g$, where f, g is a canonical basis of U). Let Y be a K3 surface with $T_Y \cong T_A$. Then, $T_Y \cong T_A \subset \mathsf{U} \oplus \mathsf{U} \oplus \langle -2 \rangle$ and $S_Y = (T_Y)^\perp$ contains $(\mathsf{U} \oplus \mathsf{U} \oplus \langle -2 \rangle)^\perp = \mathsf{E}_8 \oplus \mathsf{E}_8$. Hence Y is related to A by a Shioda-Inose structure. Let us construct such a surface Y.

Let B be a curve on $Q = \mathbb{P}^1 \times \mathbb{P}^1$ of bidegree $(4, 4)$ which is the union of a curve B_0 of bidegree $(3, 3)$ and some fibers F_1 and F_1' of the projections $Q \to \mathbb{P}^1$. We assume that B is invariant with respect to the involution $\alpha : (x, y) \mapsto (y, x)$ of Q, and B_0 has a cusp p at a point $q \in F_1$ with local equation $u^2 + v^3 = 0$, where $u = 0$ is a local equation of the fiber F_1 at q.

We assume that B_0 has no other singular points besides q and q'. Let $\pi : X' \to Q$ be the double cover of Q branched along B. It is a singular surface with singularities over q and $q' = \alpha(q)$ locally given by equations $z^2 = u(u^2 + v^3)$. This type of singularity is known as a *double rational point of type* E_7. Let X be a minimal resolution of X'. Its exceptional curve over q (resp. over q') is reducible and consists of 7 irreducible components which are (-2)-curves. Its intersection matrix is equal to the Coxeter matrix of type E_7 (multiplied by -1). The surface X is a K3 surface. Fix the first projection $Q \to \mathbb{P}^1$. The composition of the projections $X \to X' \to Q \to \mathbb{P}^1$ gives an elliptic fibration on X with two degenerate fibers of type II^* and III^* in Kodaira's notation. We also have 6 other irreducible singular fibers isomorphic to a nodal cubic curve. They correspond to 6 ordinary ramification points of the cover $\tilde{B}_0 \to B_0 \hookrightarrow Q \to \mathbb{P}^1$ of the normalization $\tilde{B}_0$ of B_0. The fiber of the first type lies over the fiber F_1 and the fiber of type III^* lies over the fiber F_2 of the same projection that passes through the point q'. The pre-image of F_1' on X defines a section S of the fibration. If we take the sublattice generated by one fiber f and the section s, we obtain a sublattice given by a matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)$. By changing a basis $f \to f + s, f \to f$, we reduce this matrix to the form $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Thus, this sublattice is isomorphic to U. The orthogonal complement to U in $\mathrm{Pic}(X)$ contains the classes of irreducible components of fibers that are disjoint from s. We easily find that this lattice is isomorphic to $\mathsf{E}_8 \oplus \mathsf{E}_7$. Thus, we obtain a lattice embedding (in fact, a primitive embedding)

$$\mathsf{U} \oplus \mathsf{E}_8 \oplus \mathsf{E}_7 \hookrightarrow \mathrm{Pic}(X).$$

It is easy to see that E_8 primitively embeds in $\mathsf{U} \oplus \mathsf{E}_7$, thus, $\mathsf{E}_8 \oplus \mathsf{E}_8$ embeds in $\mathrm{Pic}(X)$, and, by Morrison, X has a Shioda-Inose structure with

$$T_A \cong T_X \subset \mathsf{U} \oplus \mathsf{U} \oplus \langle -2 \rangle.$$

Since $(\mathsf{U} \oplus \mathsf{U} \oplus \langle -2 \rangle)^\perp_{\mathrm{H}^2(A,\mathbb{Z})} = \langle 2 \rangle \subset \mathrm{NS}(A)$, we obtain that A admits a principal polarization.

Let $Q \to \mathbb{P}^2$ be the quotient map of $Q \to Q/(s)$. The quadric Q is a cover of $\mathbb{P}^2$ branched along a conic K. Since B was invariant under the switch involution s, we see that it is equal to the pre-image of the plane curve under this cover. The plane curve is a cuspidal cubic C plus a line ℓ which is tangent to the conic K and intersects C at the cusp with multiplicity 3. Assume that C intersects K at 6 distinct points. One can show that the double cover of $\mathbb{P}^2$ branched along the union $K + C + \ell$ has a minimal resolution isomorphic to the Kummer surface $\mathrm{Kum}(A)$, where $A \cong \mathrm{J}(C)$

for some curve C of genus 2. We have the following diagram of rational maps

$$\begin{array}{ccc} X & \xrightarrow{\pi} & \mathbb{P}^1 \times \mathbb{P}^1 \\ \downarrow{\scriptstyle \phi} & & \downarrow \\ \widetilde{\mathrm{Kum}}(A) & \xrightarrow{\phi} & \mathbb{P}^2. \end{array}$$

One can see explicitly the even eight on $\mathrm{Kum}(A)$ defining the rational double cover $\phi : X \to \mathrm{Kum}(A)$ (see [114]).

Note that the six points $C \cap K$ define a curve C' of genus 2 which is in general not isomorphic to C. This curve is birationally isomorphic to the curve B_0. It comes with an additional structure. We have $3q \sim 2q' + a$ and $3q' \sim 2q + a'$, where $a + a' \sim K_{C'}$. This implies $3K_{C'} \sim 5q + a \sim 5q' + a'$. There are 16 pairs (q, q') with such property on a curve of genus 2. This implies that the Shioda-Inose construction gives a rational self-map from $\mathcal{M}_2$ to $\mathcal{M}_2$ of degree 16.

We see that X admits an elliptic fibration $|f|$ with two singular fibres

$$f_1 = 3R_0 + 2R_1 + 4R_2 + 6R_3 + 5R_4 + 4R_5 + 3R_6 + 2R_7 + R_8$$

and

$$f_2 = 2N_0 + N_1 + 2N_2 + 3N_3 + 4N_4 + 3N_5 + 2N_6 + N_7$$

of type $\tilde{E}_8$ and $\tilde{E}_7$. It is also has a section S. The fixed locus of τ consists of smooth rational curves $R_1, R_3, R_5, R_7, N_2, N_4, N_6, S$ and a genus 2 curve W which intersects R_0, N_0, N_7 with multiplicity 1. The switch involution lifts to an involution σ on X that transforms the elliptic fibration defined by the first projection $Q \to \mathbb{P}^1$ to the elliptic fibration $|f'|$ defined by the second projection. Its singular fibers are

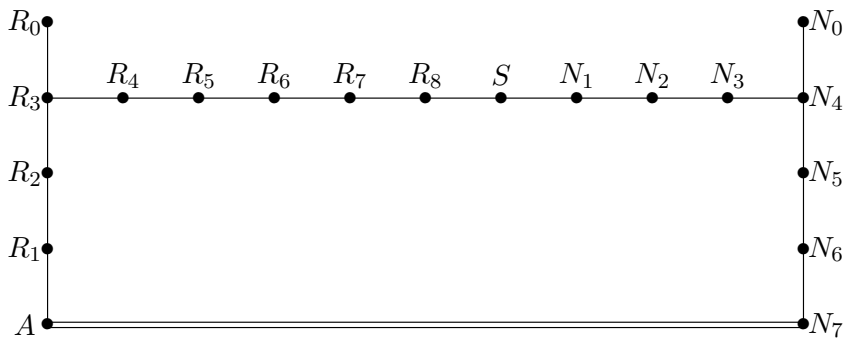
$$F_1' = 3N_0 + R_8 + 2S + 3N_1 + 4N_2 + 5N_3 + 6N_4 + 4N_5 + 2N_6$$

and

$$F_2' = 2R_0 + A + 2R_1 + 3R_2 + 4R_3 + 3R_4 + 2R_5 + R_6$$

of type $\tilde{E}_8$ and $\tilde{E}_7$. The curve R_7 is a section. The involution σ induces the hyperelliptic involution on W. Its set of fixed points are 2 points on the curve R_8 and 6 points on W. Also note that σ maps the fibration $|f|$ to the fibration $|f'|$.

We have altogether 19 (-2) curves whose incidence graph is the following



One can prove that these are all (-2)-curves on X.

Let $p = W \cap R_0, q = W \cap N_0, a = W \cap N_7, a' = W \cap A$. We have $3p \sim 2q + a$ and the fibration defines a g^1_3 on W spanned by the divisors $3p$ and $2q + a$.

It is easy to see that $q = \sigma(p), a' = \sigma(a)$. This gives $3p \sim 2K_W - 2p + a$, hence $5p \sim 2K_W + a$, or, equivalently, $3K_W \sim 5p + a'$.

Consider the divisor class $D = R_0 + R_1 + R_2 + R_3 + A + W$. We have $D^2 = 4$ and $D \cdot R_i = 0, i = 5, 6, 7, 8$ and $D \cdot N_i = 0, i = 1, \ldots, 6$. The linear system $|D|$ maps X to a quartic surface in $\mathbb{P}^3$ and blows down the four curves R_i (resp. 11 curves N_i) as above to double rational points of type A_5 (resp. A_{11}). [2] Its equation can be found in [23]

$$X(\alpha, \beta, \gamma, \delta) : y^2zw - 4x^3z + 3\alpha xzw^2 + \beta zw^3 + \beta zw^3 + \gamma xz^2w - \tfrac{1}{2}(\delta z^2w^2 + w^4) = 0. \quad (6.6)$$

Here $\alpha, \beta, \gamma, \delta$ are complex parameters with $\gamma, \delta \neq 0$. The surfaces $X(\alpha, \beta, \gamma, \delta)$ and $X(\alpha', \beta', \gamma', \delta')$ are birationally isomorphic if and only if there exists a nonzero number c such that $(\alpha', \beta', \gamma', \delta') = (c^2\alpha, c^3\beta, c^5\gamma, c^6\delta)$. It follows that $\mathcal{M}_{K3,U+E_8+E_7}$ is isomorphic to an open subset of the weighted projective space $\mathbb{P}(2, 3, 5, 6)$ known to be isomorphic to a compactification of $\mathcal{A}_2$.

An explicit correspondence between Kummer surfaces associated to curves of genus 2 and the Shioda-Inose K3 surfaces was given in [99], Theorem 11. Recall from Lecture 5 that a genus 2 curve $y^2 = f(x)$ is determined by the Clebsch invariants I_2, I_4, I_6, I_{10} of the binary form $f(x, y)$. We also recall that a K3-surface admitting an elliptic fibration with a section is birationally isomorphic to its *Weierstrass model*, a surface of degree 12 in $\mathbb{P}(1, 1, 4, 6)$

$$w^2 = z^3 + a(x, y)z + b(x, y),$$

where $a(x, y)$ and $b(x, y)$ are binary forms of degrees 8 and 12.

We have the following result.

Theorem 6.3. *Let*

$$y^2 = f_6(x, y)$$

be a nonsingular genus 2 curve, and I_2, I_4, I_6, I_{10} be the Clebsch invariants of the binary form $f_6(x, y)$. Then, the Shioda-Inose surface associated to Kum$(J(C))$ *is an elliptic K3 surface with Weierstrass equation*

$$w^2 = z^3 - t_0^4t_1^3(t_0 + \frac{I_4}{12}t_1)z + t_0^5(\frac{I_2}{24}t_0^2 + \frac{I_2I_4 - 3I_6}{108}t_0t_1 + \frac{I_{10}}{4}t_1^2). \quad (6.7)$$

Let X be a K3 surface admitting a Shioda-Inose structure with the corresponding rational map of degree 2 $X \dashrightarrow$ Kum(A). A theorem of Shouhei Ma [109] asserts that a minimal resolution Y of Kum(X) admits a Nikulin involution τ such that a minimal resolution of $Y/(\tau)$ is isomorphic to X. We say that Kum(A) is *sandwiched* between X. A geometric realization of the sandwich structure can be often seen as follows. One finds an elliptic fibration $\pi : X \to \mathbb{P}^1$ on X such that the Mordell-Weil group of its sections contains a non-zero 2-torsion section S so that the translation

[2] A singular point of type A_k is a surface singularity locally isomorphic to the singularity $u^2 + u^{k+1} = 0$.

automorphism t_S defines a Nikulin involution with quotient birationally isomorphic to Kum(A). Let β be the involution of X that induces the involution $[-1]_E$ on each smooth fiber of the elliptic fibration. The fixed locus of β consists of some irreducible components of fibers and a horizontal divisor $S_0 + S + T$, where S_0 is the zero section and T is a 2-section. The intersection of $S + T$ with a smooth fiber coincides with the set of non-trivial 2-torsion points. The curve T is invariant with respect to β and its image on Kum(A) defines a 2-torsion section $\bar{T}$ on the image of the elliptic fibration on X to Kum(A). The Nikulin involution defined by the translation $t_{\bar{T}}$ has the quotient birationally isomorphic to X. To see this one should restrict the action of t_S on the generic fiber E_η of π and observe that the composition of $t_{\bar{T}} \circ t_S$ is the map $E_\eta \to E_\eta/E_\eta[2] \cong E_\eta$.

In the previous example, the Nikulin involution is defined by the translation t_S, where S is a 2-torsion section of the elliptic fibration with singular fiber F of type $\tilde{D}_{14}$ equal to

$$F = R_0 + R_2 + 2(R_3 + \cdots + R_8 + S + N_1 + N_2 + N_3 + N_4) + N_0 + N_5.$$

We may take S_0 to be equal to R_1 and S to be equal to N_6. The curve T coincides with W.

Remark 6.4. In this and the previous chapters, we compared properties of abelian surfaces with the properties of the associated Kummer or Shioda-Inose K3 surfaces. There is also a connection to cubic surfaces in $\mathbb{P}^3$. Recall that a nonsingular cubic surface in $\mathbb{P}^3$ is isomorphic to the blow-up of 6 points in the plane, no three of which are on a line, and not all of them are on a conic. The birational map is given by the linear system of plane cubics through the six points. When we allow the six points to lie on a conic, the cubic becomes singular, the image of the conic is its ordinary double point. A set of 6 distinct points on a conic defines a genus 2 curve C, and the Kummer surface Kum(J(C)) has a double plane model with the branch curve equal to the union of the tangents to the conic at the six points. It would be interesting to find an explicit realization of the Humbert surface Hum(Δ) inside of the moduli space $\mathcal{M}_{\text{cub}}$ of cubic surfaces. We have already remarked that Hum(4) is realized as the locus of cubic surfaces with an Eckardt point. There is also another way to relate jacobians of curves of genus 2 with cubic surfaces. The Hessian surface $H(F)$ of a general cubic surface F is a quartic surface with 10 nodes (see [41]). Its minimal resolution is a K3 surface. It is known that there is a divisor in $\mathcal{M}_{\text{cub}}$ such that the Hessian surface of a general surface from this divisor is birationally isomorphic to a Kummer surface of a curve of genus 2 [70]. It is defined by vanishing of the invariant $I_8 I_{24} + 8 I_{32}$ of degree 32 of cubic surfaces (see [33], 6.6). Which properties of Kummer surfaces are special properties of Hessians of cubic surfaces? One answer in this direction is given in [134] where it is proven that J$(C) \in$ Hum(5) implies that the Hessian quartic surface admits an additional ordinary double point.

It is known that every K3 surface X with $\rho(X) = 19$ admits a Shioda-Inose structure (see [123]). Let T_X be the transcendental lattice of X. Suppose T_X contains a direct summand isomorphic to the hyperbolic plane U. Then, $T_X \cong T_n := \mathsf{U} \oplus \langle -2n \rangle$, where $2n$ is the discriminant of T_X. Let $M_n = (T_n)^\perp_{L_{K3}} \cong \mathsf{U}^{\oplus 2} \oplus \mathsf{E}_8^{\oplus 2} \oplus \langle 2n \rangle$. The moduli space $\mathcal{M}_{K3,M_n}$ is isomorphic to a non-compact modular curve $\Gamma_0^+ \backslash \mathfrak{H}$ (see [42]). The loc.cit. paper contains a construction of K3 surfaces from this moduli space for some small n. The corresponding abelian surfaces are isogenous to the product of two isogenous elliptic curves.

Suppose $T_X \cong T$ does not contain an isotropic vector. Then, the moduli space $\mathcal{M}_{K3,T^\perp}$ is known to be a compact Shimura curve. The corresponding abelian surfaces are fake elliptic curves. In general, they are simple abelian surfaces. We refer to K. Hashimoto [68] and A. Sarti [145], [146]

for description of some of these transcendental lattices and the families of the corresponding K3 surfaces.

6.4 Humbert Surfaces and Heegner Divisors

Let is explain an exceptional isomorphism between two Hermitian spaces of dimension 3, the Siegel space $\mathfrak{H}_2$ and a type IV domain associated to a 3-dimensional quadric. Recall that $\mathfrak{H}_2$ is isomorphic to an open subset of the Grassmannian $\mathsf{G}(2,4) := \mathsf{G}(2,\mathbb{C}^4)$ represented by complex 2×4-matrices of the form $[\tau \mathsf{D}]$, where τ is symmetric and $\mathrm{Im}(\tau) > 0$. In the Plücker embedding $\mathsf{G}(2,4) \hookrightarrow \mathbb{P}^5$, the Grassmannian becomes isomorphic to a nonsingular quadric, the *Klein quadric* given by the *Plücker equation*

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{24} = 0. \tag{6.8}$$

We will see that the open subset $\mathfrak{H}_2$ coincides with a Hermitian symmetric space of orthogonal type, which we used to construct the coarse moduli space of lattice polarized K3 surfaces. We will also see that the modular group $\mathrm{Sp}(J_{\mathsf{D}},\mathbb{Z})$ is isomorphic to the group Γ_T acting on $\mathcal{D}_{T_n}$, where the lattice T_n is determined by $\mathsf{D} = \mathrm{diag}[1,n]$, namely

$$T_n \cong \mathsf{U}\oplus\mathsf{U}\oplus\langle -2n\rangle.$$

The cohomology group $\mathrm{H}^1(A,\mathbb{Z})$ is a free abelian group H of rank 4 and $\mathrm{H}^2(A,\mathbb{Z}) \cong \bigwedge^2 \mathsf{H}$. The group $\mathrm{H}^2(A,\mathbb{Z})$ is a quadratic lattice with respect to the natural pairing

$$\bigwedge^2 \mathrm{H}^1(A,\mathbb{Z}) \times \bigwedge^2 \mathrm{H}^1(A,\mathbb{Z}) \to \bigwedge^4 \mathrm{H}^1(A,\mathbb{Z}) \cong H^4(A,\mathbb{Z}) \cong \mathbb{Z},$$

where we fix an isomorphism $H^4(A,\mathbb{Z}) = \bigwedge^4 \mathbb{Z}^4 \to \mathbb{Z}$, called an *orientation* on H. The quadratic lattice $\mathrm{H}^2(A,\mathbb{Z})$ is a unimodular even lattice of signature $(3,3)$. It is isomorphic to the orthogonal sum $U^{\oplus 3}$ of three hyperbolic planes U.

A choice of a basis (e_1,e_2,e_3,e_4) in $\mathrm{H}^1(A,\mathbb{Z}) \cong \mathbb{Z}^4$ defines a basis $e_1\wedge\cdots\wedge e_4$ of $\bigwedge^4 \mathsf{H}$, hence an orientation on H. We fix this choice.

We can choose a basis $(\gamma_1,\dots,\gamma_4)$ of $\mathrm{H}_1(A,\mathbb{Z})$ and a basis (ω_1,ω_2) of $\Omega^1(A)$ such that

$$\omega_1 = (z_1,z_2,1,0), \quad \omega_2 = (z_2,z_3,0,n).$$

Here $\tau = \left(\begin{smallmatrix} z_1 & z_2 \\ z_2 & z_3 \end{smallmatrix}\right), \mathsf{D} = \mathrm{diag}[1,n]$. In the Plücker embedding the plane spanned by ω_1,ω_2 is the point

$$\mathfrak{p} = \omega_1\wedge\omega_2 = (z_1z_3 - z_2^2)w_1 - z_2(w_2 - nw_5) - nz_1w_3 - z_3w_4 + nw_6,$$

where

$$(w_1,\dots,w_6) = (e_1\wedge e_2, e_1\wedge e_3, e_1\wedge e_4, e_2\wedge e_3, e_2\wedge e_4, e_3\wedge e_4).$$

is the corresponding basis in $\bigwedge^2 \mathsf{H}$. Let

$$(f_1,g_1,f_2,g_2,k) := (-w_1,w_6,-w_3,w_4,nw_5+w_2).$$

We see that $f_i^2 = g_i^2 = 0, f_i \cdot g_i = 1$ and

$$h_0 = w_2 - nw_5, \quad h_0^2 = 2n.$$

We can rewrite

$$\mathfrak{p} = (z_2^2 - z_1 z_3) f_1 + n g_1 + n z_1 f_2 + z_3 g_2 + z_2 k,$$

and check that

$$\mathfrak{p} \in (\mathbb{Z} h_0)^\perp, \quad \mathfrak{p}^2 = 0.$$

Thus, $\mathfrak{p}$ defines a point $[\mathfrak{p}]$ in the quadric $Q_{T_n} = Q \cap \mathbb{P}((T_n)_{\mathbb{C}})$. One checks that the condition $\mathrm{Im}(\tau) > 0$ translates into the condition that $[\mathfrak{p}]$ belongs to one of the two connected components of $Q^0_{T_n}$, which we fix and denote it by $\mathcal{D}^0_{T_n}$.[3]

Note that the matrix of the quadratic form in the basis (f_1, g_1, f_2, g_2, e) is equal to

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2n \end{pmatrix}.$$

So, this confirms that the lattice $\langle 2n \rangle^\perp$ in $\mathrm{H}^2(A, \mathbb{Z}) \cong U \oplus U \oplus U$ is isomorphic to $U \oplus U \oplus \langle -2n \rangle$.

Let L_0 be a polarization on A of degree $2n$ with $h_0 = c_1(L) \in \mathrm{H}^2(A, \mathbb{Z})$. We have $h_0^2 = 2n$. Choose a basis $(e_1, \ldots, e_4)$ of H and let

$$(w_1, \ldots, w_6) = (e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4)$$

be the corresponding basis in $\bigwedge^2 \mathsf{H}$. The intersection form is defined by the exterior product and the choice of an orientation. The matrix in this basis is equal to

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

In the dual basis $(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34})$, the quadratic form is equal to

$$q = 2(p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{24}). \tag{6.9}$$

The equation $q = 0$ is the Plücker equation (6.8). It is known that the Grassmannian contains two families of planes corresponding to lines through a fixed point or lines in a fixed plane. Any automorphism of $G(2, 4)$ preserving each of the families, originates from a projective automorphism of $|\mathsf{H}_{\mathbb{C}}|$ by taking the wedge square of the corresponding linear map. There is also an integral version

[3] If we write $z_i = x_i + \sqrt{-1} y_i$, then the condition $\mathrm{Im}(z_1) > 0$ chooses a connected component and the condition $y_1 y_3 - y_2^2 > 0$ makes sure that the point lies on the open subset $Q^0_{T_n}$ of the quadric and hence defines the period point of a marked polarized K3 surface.

of this isomorphism. The integral analog of plane in $\mathsf{G}(2,\mathfrak{H}_{\mathbb{C}})$ is a maximal isotropic sublattice F of rank 3 in $\bigwedge^2 \mathsf{H}$.[4] The homomorphism

$$\sigma : \mathrm{GL}(\mathsf{H})_0 \to \mathrm{GL}(\bigwedge^2 \mathsf{H}), \quad \phi \mapsto \phi \wedge \phi,$$

has the image equal to the index 2 subgroup $\mathrm{O}_0(\bigwedge^2 \mathsf{H})$ of the orthogonal group $\mathrm{O}(\bigwedge^2 \mathsf{H})$ of the lattice $\bigwedge^2 \mathsf{H}$. It consists of isometries preserving a family of maximal isotropic sublattices (see [9], Lemma 4).

Let h_0' be a primitive vector with $h_0'^2 = 2n$. It follows from Lemma 6.7 below that there exists an isometry $\sigma : \bigwedge^2 \mathsf{H} \to \bigwedge^2 \mathsf{H}$ that sends h_0' to h_0. Replacing $(w_1, \dots, w_6)$ with $(\phi(w_1), \dots, \phi(w_6))$ we may assume that

$$h_0 = w_2 - nw_5.$$

Let $\mathrm{O}(T_n)$ denote the orthogonal group of the lattice T_n. Let $A_{T_n} = T_n^\vee/T_n$ be the discriminant group equipped with the quadratic map (6.3). Let $\mathrm{O}(T_n)^\sharp$ be the kernel of the natural homomorphism $r : \mathrm{O}(T_n) \to \mathrm{O}(A_{T_n}, q_{A_{T_n}})$. We know from Chapter 8 that the orbit space

$$\mathrm{O}(T_n)^\sharp \backslash \mathcal{D}_{T_n} \cong Or_0(T_n)^\sharp \backslash \mathcal{D}^0_{T_n}$$

is isomorphic to the coarse moduli space $\mathcal{M}_{K3,M_n}$ of pairs (X, j), where j is a fixed primitive embedding of the lattice $M_n = T_n^\perp$ into $\mathrm{Pic}(X)$ (or, equivalently, a primitive embedding $T_X \hookrightarrow T_n$) (with some additional technical conditions formulated in terms of the Picard lattice $\mathrm{Pic}(X)$ of X (see [42])).

In our case, $A_{T_n} = \mathbb{Z}/2n\mathbb{Z}$ and the value of the discriminant quadratic form at its generator is equal to $-\frac{1}{2n} \mod 2\mathbb{Z}$. The group $\mathrm{O}(G(T_n))$ is isomorphic to the group $(\mathbb{Z}/2\mathbb{Z})^{p(n)}$, where $p(n)$ is the number of distinct prime factors of n and the homomorphism $r : \mathrm{O}(T_n) \to \mathrm{O}(A_{T_n})$ is surjective (see [147], Lemma 3.6.1).

Recall that we have defined earlier a surjective homomorphism $\sigma : \mathrm{SL}(\mathsf{H}) \to \mathrm{O}_0(\bigwedge^2 \mathsf{H})$, where $\mathrm{O}_0(\bigwedge^2 \mathsf{H})$ is a subgroup of index 2 of $\mathrm{O}(\bigwedge^2 \mathsf{H})$. Consider h_0 as an element of $\bigwedge^2 \mathsf{H}^\vee = \bigwedge^2 \mathrm{H}_1(A,\mathbb{Z})^\vee$. Then, the stabilizer subgroup of h_0 in $\mathrm{O}(\bigwedge^2 \mathsf{H})_0$ is equal to the image under σ of the subgroup of $\mathrm{SL}(\mathsf{H})$ that preserves the symplectic form h_0. It is isomorphic to the group $\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$, where $\mathsf{D} = \mathrm{diag}[1, n]$. This gives an isomorphism

$$\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})/(\pm 1) \cong \mathrm{O}_0(\bigwedge^2 \mathsf{H})_{h_0} \cong \mathrm{O}_0(T_n)^\sharp. \tag{6.10}$$

The latter isomorphism comes from the interpretation of the group $\mathrm{O}(T_n)^\sharp$ as a subgroup of T_n of isometries that lift to an isometry of $\bigwedge^2 \mathsf{H}$ leaving h_0 invariant. Note that the subgroup $\mathrm{Sp}(J_{\mathsf{D}}, \mathbb{Z})$ is conjugate to a subgroup Γ_n of $\mathrm{Sp}(4,\mathbb{Q})$ by the conjugation map $g \mapsto R^{-1}gR$, where R is the diagonal matrix $\mathrm{diag}(1, 1, 1, n)$ ([76], p. 11).

Let us record the previous information in the following:

[4] A sublattice of a lattice is called isotropic if the restriction of the quadratic form to the sublattice is identically zero.

Theorem 6.5. *There is an isomorphism of coarse moduli spaces*

$$\mathcal{A}_{2,n} \cong \mathcal{M}_{K3,M_n}.$$

Example 6.6. Consider the abelian surface $A = E \times E$, where E is an elliptic curve with complex multiplication by $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega, \omega = \sqrt{-5}$ from Example 3.12. Let us compute its lattice T_A. We have $\mathrm{End}^s(A) = \{M \in \mathrm{Mat}_2(\mathfrak{o}) : {}^t\bar{M} = M\}$. As a $\mathbb{Z}$-module, it has a basis formed by matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \omega \\ \bar{\omega} & 0 \end{pmatrix}. \tag{6.11}$$

Under the isomorphism $\mathrm{NS}(A) \to \mathrm{End}(A)$ induced by the principal polarization on $A = E \times E$, the first three matrices correspond to the divisors $E_1 = E \times \{0\}, E_1 = \{0\} \times E$ and the class $\Delta - E_1 - E_2$. The last matrix corresponds to some divisor D. Consider the basis $(\gamma_1, \gamma_2, \gamma_3, \gamma_4) = (\omega e_1, e_1, \omega e_2, e_2)$ of the lattice Λ. The reducible principal polarization H_0 is given in the basis (e_1, e_2) by the matrix $y^{-1}I_2$, where $y = \mathrm{Im}(\omega) = \sqrt{5}$. The corresponding symplectic form is defined by $h_0 = \gamma_1^* \wedge \gamma_2^* + \gamma_3^* \wedge \gamma_4^*$. The Hermitian forms corresponding to the four endomorphisms (6.11) are obtained by multiplying these matrices by y^{-1}. We give the alternating forms defining the first Chern class in terms of the dual basis $(\gamma_1^*, \dots, \gamma_4^*)$.

$$\gamma_1^* \wedge \gamma_2^*,\ \gamma_3^* \wedge \gamma_4^*,\ \gamma_1^* \wedge \gamma_4^* - \gamma_2^* \wedge \gamma_3^*,\ 5\gamma_1^* \wedge \gamma_3^* + \gamma_2^* \wedge \gamma_4^*.$$

To find the intersection matrix, we choose the volume form

$$h_0 \wedge h_0 = \gamma_1^* \wedge \gamma_2^* \wedge \gamma_3^* \wedge \gamma_4^*$$

and compute the exterior products. The result is the intersection matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -10 \end{pmatrix}.$$

The transcendental lattice is a rank 2 positive lattice isomorphic to $\langle 2 \rangle \oplus \langle 10 \rangle$.

Let us see the meaning of the singular equation (4.1) in terms of the period $[\mathfrak{p}]$ of a K3-surface. Consider the vector

$$\delta = ef_1 + dg_1 + cf_2 + ag_2 + \frac{b}{2n}k \in T_n^* \subset T(d)_{\mathbb{Q}}, \tag{6.12}$$

Using the singular equation (4.1), we have

$$\mathfrak{p} \cdot \delta = naz_1 + bz_2 + cz_3 + d(z_2^2 - z_1 z_3) + nk = 0.$$

Finally, we get

$$\delta^2 = -\frac{b^2}{2n} + 2(ac + ed) = -\frac{\Delta}{2n}. \tag{6.13}$$

We obtain that $\mathrm{End}^s(A) \neq \mathbb{Z}$ if and only if the period of the corresponding K3 surface lies on a hyperplane $H_\delta := \delta^\perp = \mathbb{P}((\mathbb{C}\delta)^\perp) \cap \mathcal{D}_T$.

We use the following result from the theory of quadratic lattices (see [147], Propositiuon 3.7.3).

Lemma 6.7. *Let L be an even lattice such that it contains $U \oplus U$ as a primitive sublattice. Let $v, w \in L^\vee$ be two primitive vectors with $v^2 = w^2$. Then, there exists $\sigma \in \mathrm{O}(L)$ such that $\sigma(v) = w$ if and only if the images of v, w in $L^\vee/L$ coincide.*

We apply this to our case where $L = T_n = U \oplus U \oplus \langle -2n \rangle$, where $\langle -2n \rangle$ is generated by a vector e with $e^2 = -2n$. We have $L^\vee/L \cong \mathbb{Z}/2n\mathbb{Z}$ and the generator $e^* = \frac{1}{2n}e + L$. We have $e^{*2} = (2ne^*)^2/2n = -1/2n$. Let $x = re^*$, then $x^2 = -r^2/2n$. Thus, x^2 is determined by $r^2 \mod 4n$. Suppose we have a singular equation defined by the vector δ from (6.12). So we obtain that the number of orbits of hyperplanes H_δ with $-2n\delta^2 = \Delta$ with respect to the group $\mathrm{O}_0(T(d))^*$ is equal to

$$\mu(\Delta; n) := \#\{r \in \mathbb{Z}/2n\mathbb{Z} : \Delta \equiv r^2 \mod 4n\}. \tag{6.14}$$

This number [5] is equal to the number of irreducible components of the Humbert surface $\mathrm{Hum}(\Delta; D)$ in $\mathcal{A}_{2,n}$. In particular, the Humbert surface $\mathcal{A}_{2,n}(\Delta)$ is irreducible if $n = 1$. If $n = 2$, we get two components corresponding to $r = 1, r = 3 \mod 4$ and $\Delta \equiv 1 \mod 8$. For $n = 3$ we have four irreducible components corresponding to $r = 1, 2, 4, 5 \mod 6$ and $\Delta \equiv 1, 4 \mod 12$.

Applying Proposition 6.5, we obtain a proof of Humbert's Lemma 4.1. In fact, assume that $\Delta \equiv 0 \mod 4$. We write $\Delta = 4m$ and choose $\delta = mf_3 - f_4$ and obtain the singular equation $mz_1 - z_3 = 0$. If $\Delta = 4m+1$, we choose $\delta = f_2 - f_5 + 2(f_3 - mf_4)$ to obtain the singular equation $mz_1 - z_2' - z_3' = 0$.

The divisors in the moduli spaces of lattice polarized K3 surfaces defined by requiring that the periods belong to the orthogonal complement of some vector with negative norm are called the *Heegner divisors*. The following theorem follows from the previous discussion.

Theorem 6.8. *Under the isomorphism $\mathcal{A}_{2,n} \cong \mathcal{M}_{K3,T_n}$, the image of the Humbert surface $\mathrm{Hum}_n(\Delta)$ is equal to the Heegner divisor $\mathrm{Heeg}_n(\delta)$, where*

$$\delta = -\frac{\Delta}{2n}.$$

Let A belongs to $\mathrm{Hum}_n(\Delta)$. Let $\mathfrak{o}_\Delta$ be the ring of integers in the real quadratic field with a fixed basis such that it can be identified with the algebra (4.5), where $b = 0, 1$. Let $\mathfrak{o}_\Delta(n)$ be the corresponding quadratic lattice. We know that it is isomorphic to the sublattice $\langle L_0, L_\Delta$ of $\mathrm{NS}(A)$ from (4.8). Let T_A be the lattice of transcendental cycles of A. It is contained in the orthogonal complement of $\mathfrak{o}_\Delta(n)$ in $U \oplus U \oplus U$. It is a lattice of signature $(2, 1)$ with discriminant group (together with the discriminant quadratic form) isomorphic to the discriminant group of $\mathfrak{o}_\Delta(-n)$. Let X be an Inose-Shioda K3-surface with $T_A \cong T_X$. Then, its Néron-Severi lattice is isomorphic to the orthogonal complement of T_A in $E_8^{\oplus 2} \oplus U^{\oplus 3}$. Its discriminant lattice is isomorphic to the discriminant lattice of $\mathfrak{o}_\Delta(n)$. An example of such a lattice is the lattice $E_8^{\oplus 2} \oplus \mathfrak{o}_\Delta(n)$. It follows from [133], Corollary 1.13.3 that the isomorphism class of a quadratic lattice with such discriminant group consists of one element. Thus, we obtain

Theorem 6.9. *There is an isomorphism of coarse moduli spaces*

$$\mathrm{Hum}_n(\Delta) \cong \mathcal{M}_{K3,S_\Delta},$$

[5] If we write $\Delta = Df^2$, where D is square-free, then this number is equal to the number of $\mathrm{SL}(2, \mathbb{Z})$-nonequivalent primitive representations of n by all binary quadratic forms of discriminant D.

where

$$S_\Delta = \mathsf{E}_8 \oplus \mathsf{E}_8 \oplus \mathfrak{o}_\Delta(n).$$

Recall that $\mathrm{Hum}_n(\Delta)$ may consist of several irreducible components. They correspond to different embedding of the lattice S_Δ in $\mathrm{NS}(X)$.

Example 6.10. Let $n = 1$. We have

$$\mathrm{Hum}(1) \cong \mathrm{Heeg}(-1/2) \cong \mathcal{M}_{K3,\mathsf{E}_8\oplus\mathsf{E}_8\oplus\mathfrak{o}_1},$$

where $\mathfrak{o}_1$ is defined by the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Obviously, it is isomorphic to U. Thus

$$\mathrm{Hum}(1) \cong \mathcal{M}_{K3,\mathsf{E}_8\oplus\mathsf{E}_8\oplus\mathsf{U}}.$$

These lattice polarized K3 surfaces contain an elliptic pencil with a section and two reducible fibers of type $\tilde{E}_8$ (of type II^* in Kodaira's notation). These surfaces are studied in [22], [80], [161], [99]. The surface admits a birational model isomorphic to the quartic surface

$$y^2zw - 4x^3z + 3axzw^2 - 12(z^2w^2 + w^4) + bzw^3 = 0.$$

The equation is a special case of equation (6.6). It admits a birational model isomorphic to the double cover of $\mathbb{P}^2$ branched along the union of a cuspidal cubic C, the cuspidal line L and the union of two lines intersecting at a point on L. Note that the Heegner divisor $\mathrm{Heeg}(-1/2)$ is equal to an irreducible component of the *discriminant* in $\mathcal{M}_{K3,T_1^\perp}$ corresponding to non-ample lattice polarized K3 surfaces.

Example 6.11. Similarly, we get that $\mathfrak{o}_4 \cong \langle 2\rangle \oplus \langle -2\rangle$, hence

$$\mathrm{Hum}(4) \cong \mathcal{M}_{K3,\mathsf{E}_8\oplus\mathsf{E}_8\oplus\langle 2\rangle\oplus\langle -2\rangle}.$$

Note that,

$$\mathsf{E}_8 \oplus \mathsf{E}_8 \oplus \langle 2\rangle \oplus \langle -2\rangle \cong \mathsf{U} \oplus \mathsf{E}_8 \oplus \mathsf{E}_7 \oplus \langle -2\rangle.$$

A K3 surface polarized with this lattice admits an elliptic fibration with a section and four singular fibers of Kodaira's types I_2, III^*, II^*, I_1. These surfaces define the second irreducible component of the discriminant.

In our example, the Weierstrass equation of the genus 2 curve could be chosen to be in the form

$$y^2 = x^3 - t_0^4t_1^3(\frac{3f - e^2}{3}t_1 - t_0) + t_0^5t_1^5(fgt_1^2 - \frac{54g + 9ef - 2e^3}{27}t_0t_1 + \frac{3g + ef}{3f}t_0^2) = 0,$$

where e, f, g are some constants (see [99]). Two such collections of scalars (e, f, g) and (e', f', g') define isomorphic surfaces if and only if there exists $\lambda \neq 0$ such that $(e', f', g') = (\lambda^2 e\lambda^4 f, \lambda^6 g)$. This shows that the moduli space of such surfaces is isomorphic to the weighted projective plane $\mathbb{P}(1, 2, 3)$. Thus, $\mathrm{Hum}(4) \cong \mathbb{P}(1, 2, 3)$ that confirms Corollary 4.12.

Comparing with Kumar's Theorem 6.3, we obtain that this surface is the Shioda-Inose surface associated with the Kummer surface of the Jacobian of the curve $y^2 = f_6(x, y)$ with Clebsch invariants

$$(I_2, I_4, I_6, I_{10}) = (8(3s + r)/r, -4(3r - 1), -4(6rs - 8s + 5r^2 - 2r)/r, 4rs),$$

where $r = f/e^2, s = g/e^3$ (see [100], 3.2). One can plug in these values of the invariants in the formula (4.15) to obtain that $I_{15} = 0$ to agree with Example 4.3.

One can find in [100] a similar explicit description of the Humbert surfaces of discriminants k^2 for $k \leq 11$.

Example 6.12. Let us look at the Humbert surface $\mathrm{Hum}_2(1) \subset \mathcal{A}_{2,2}$. Then, $\delta^2 = -1/4$ and we have 2 components corresponding to $\delta^* = 1, 3 \mod 4$. In the former case, we may represent δ by a generator $\frac{1}{4}e$, where $e \in T_2$ generates $\langle -4 \rangle$. Then, $\delta^\perp \cong \mathsf{U}^2$, so $\mathrm{Heeg}_2(1) \cong \mathcal{M}_{K3,\mathsf{U}\oplus\mathsf{U}}$ as in the case of $n = 1$. In the latter case we may represent δ by $\frac{1}{4}(3e + 4f - 4g) \in T_2^*$. We have $\delta^\perp \cong \mathsf{U} \oplus \langle f + g, 2e + 3f + 3g \rangle \cong U \oplus \langle 2 \rangle \oplus \langle -2 \rangle$. So, we obtain that the second irreducible component of $\mathrm{Hum}_2(1)$ is isomorphic to $\mathcal{M}_{K3,M}$, where $M \cong U \oplus E_7 \oplus \langle -2 \rangle$. It is isomorphic to an irreducible component of the discriminant variety in $\mathcal{M}_{K3,T_1^\perp}$. Thus, we obtain that the Humbert surface $\mathrm{Hum}_2(1)$ is isomorphic to the discriminant of $\mathcal{M}_{K3,M_1}$.

Example 6.13. The lattice $\mathfrak{o}_5$ could be defined by the matrix $\left(\begin{smallmatrix} 2 & 1 \\ 1 & -2 \end{smallmatrix}\right)$. We have

$$\mathrm{Hum}(5) \cong \mathrm{Heeg}(-5/2) \cong \mathcal{M}_{K3,\mathsf{E}_8^{\oplus 2}\oplus\mathfrak{o}_5}.$$

The Humbert surface $\mathrm{Hum}(5)$ admits a compactification $\overline{\mathrm{Hum}}(5)$ isomorphic to the symmetric Hilbert surface for the field $\mathbb{Q}(\sqrt{5})$. It has been explicitly constructed by F. Hirzebruch [71] (see also [92]). The ring of Hilbert modular forms (whose projective spectrum is isomorphic to $\mathrm{Hum}(5)$) is generated by four forms A, B, C, D of weights $2, 6, 10, 15$ with a relation of degree 30

$$-144D^2 - 1728B^5 + 720AB^3C - 80A^2BC^2 + 64A^3(5B^2 - AC)^2 + C^3 = 0.$$

According to F. Klein [89], II, 4,§3, this ring is isomorphic to the ring of invariants of the icosahedron group $\mathfrak{A}_5$ acing in its irreducible 3-dimensional linear representation. The projective spectrum is isomorphic to the weighted projective plane $\mathbb{P}(1, 3, 5)$. The surface $\mathrm{Hum}(5)$ is isomorphic to the complement of one point $[1, 0, 0]$. The symmetric Hilbert modular surface corresponding to a principal congruence subgroup of the Hilbert modular group associated to the ring of integers $\mathfrak{o}$ in $\mathbb{Q}(\sqrt{5})$ and the principal ideal $\mathfrak{a}$ generated by $\sqrt{5}$ has a natural action by the group $\mathfrak{o}/\mathfrak{a} \cong \mathfrak{A}_5$. According to F. Hirzebruch [73], it is $\mathfrak{A}_5$-equivariantly isomorphic to $\mathbb{P}^2$. So this explains the isomorphism $\overline{\mathrm{Hum}}(5) \cong \mathbb{P}^2/\mathfrak{A}_5$.

The projective representation of $\mathfrak{A}_5$ in $\mathbb{P}^2$ has a minimal 0-dimensional orbit that consists of 6 points, called the *fundamental points*. The blow-up of the plane at these points is isomorphic to the *Clebsch diagonal surface* $\mathcal{C}$ with automorphism group isomorphic to $\mathfrak{S}_5$ (see [41], 9.5.4). The Hilbert modular surface corresponding to the pair $(\mathfrak{o}, \mathfrak{a})$ is isomorphic to the double cover of $\mathbb{P}^2$ branched along the curve of degree 10 defined by the invariant of degree 10. It has 6 singular points, the pre-images of the fundamental points under the cover. Its minimal resolution is isomorphic to the blow-up of $\mathcal{C}$ at its 10 Eckardt points.

Chapter 7

The Igusa quartic threefold

The moduli space of principally polarized abelian surfaces together with a 2-level structure admits a compactification isomorphic to a degree four hypersurface in $\mathbb{P}^4$. It coincides with the classically known Castelnuovo hypersurface, defined as being the dual hypersurface to the Segre cubic primal, a compactification of the moduli space of genus two curves with an ordered set of its Weierstrass points. The moduli space of bielliptic genus two curves has an explicit realization as a surface in the Igusa quartic. In this chapter, we will discuss this beautiful geometry.

7.1 Modular Forms

Let us recall some definitions and known facts about modular forms on the Siegel half-space $\mathfrak{H}_g$.

A holomorphic function $\Phi : \mathfrak{H}_g \to \mathbb{C}$ is called a *Siegel modular form of weight* w with respect to a discrete group $\Gamma \subset \mathrm{Sp}(2g, \mathbb{R})$ of automorphisms of $\mathfrak{H}_g$ if it satisfies the following functional equation

$$\Phi((A\tau + B)(C\tau + D)^{-1}) = \det(C\tau + D)^w \Phi(\tau), \quad \sigma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma.$$

Let $\mathsf{M}_k(g, \Gamma)$ denote the complex linear space of such forms. The multiplication of functions defines the graded algebra over $\mathbb{C}$

$$\mathsf{M}(g; \Gamma) = \bigoplus_{k=0}^{\infty} \mathsf{M}_k(g, \Gamma).$$

It is called the algebra of Siegel modular forms.zeros

For example, when $\Gamma = \mathrm{Sp}(4, \mathbb{Z})$, the even part $\mathsf{M}(g; \Gamma)^{(2)}$ of this algebra is freely generated by four forms $E_4, E_6, \chi_{10}, \chi_{12}$ of weights indicated by the subscripts. The whole algebra is generated by $\mathsf{M}(g; \Gamma)^{(2)}$ and a cuspidal form χ_{35} of weight 35 [78].

Here

$$E_w(\tau) = \sum_{(C,D)} \det(C\tau + D)^{-w}$$

is an *Eisenstein series*, where the summation is taken over all representatives of all inequivalent block-rows of elements of $\mathrm{Sp}(4,\mathbb{Z})$ with respect to left multiplication by matrices from $\mathrm{SL}(2,\mathbb{Z})$. The other forms are expressed in terms of the Eisenstein series

$$\chi_{10} = E_4E_6 - E_{10}, \quad \chi_{12} = 3^2 7^2 E_4^3 + 50E_6^2 - 691E_{12}$$

(see [77, p. 195]). Thus, we may also say that the graded ring $\mathsf{M}(g;\Gamma)^{(2)}$ is generated by the Eisenstein series of degrees $4, 6, 10$, and 12.

Another way to define modular forms is by using *theta constants*. A *theta function with characteristic* $(\mathbf{m},\mathbf{m}')$ is a holomorphic function on $\mathfrak{H}_g$ defined by the infinite series

$$\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\mathbf{z};\tau) = \sum_{\mathbf{r}\in\mathbb{Z}^g} e^{2\pi i(\frac{1}{n}\mathbf{m}+\mathbf{r})\cdot\tau\cdot{}^t(\frac{1}{n}\mathbf{m}+\mathbf{r})+2(\mathbf{z}+\frac{1}{2}\mathbf{m}')\cdot(\frac{1}{2}\mathbf{m}+\mathbf{r}))},$$

where $(\mathbf{m},\mathbf{m}') \in (\mathbb{Z}/n\mathbb{Z})^g \times (\mathbb{Z}/n\mathbb{Z})^g$, $\mathbf{z}\in\mathbb{C}^g$ (we identify in matrix multiplication a row vector with a column vector). The corresponding *theta constant* $\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\tau)$ is the value of this function at $(0;\tau)$. One assumes here that $\mathbf{m}\cdot\mathbf{m}' = 0$, otherwise the constant is equal to zero. The main property of theta constants is the following functional equation ([79, pages 176 and 182]):

$$\theta\left[\sigma\cdot\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right]\right](\sigma\cdot\tau) = \kappa(\sigma)e^{2\pi i\phi_{(\mathbf{m},\mathbf{m}')}(\sigma)}\det(C\tau+D)^{\frac{1}{2}}\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right], \tag{7.1}$$

where $\sigma = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) \in \mathrm{Sp}(2g,\mathbb{Z})$, and

$$\begin{aligned}
\sigma\cdot\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right] &= ((\mathbf{m},\mathbf{m}')\cdot\sigma^{-1} + \tfrac{1}{2}(C\cdot{}^tD)_0(A\cdot{}^tB)_0),\\
\phi_{(\mathbf{m},\mathbf{m}')}(\sigma) &= -\tfrac{1}{2}(\mathbf{m}\cdot{}^tD\cdot B\cdot{}^t\mathbf{m} - 2\mathbf{m}\cdot{}^tB\cdot C\cdot{}^t\mathbf{m}' + \mathbf{m}'\cdot{}^tC\cdot A\cdot\mathbf{m}')\\
&\quad +\tfrac{1}{2}(\mathbf{m}\cdot{}^tD - \mathbf{m}'\cdot{}^t(A\cdot{}^tB)_0,\\
\kappa(\sigma)^8 &= 1.
\end{aligned}$$

where $()_0$ denotes the vector of diagonal elements of a square matrix. Let

$$\Gamma = \Gamma_g(n) := \{\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) \in \mathrm{Sp}(2g,\mathbb{Z}) : B\equiv C\equiv 0 \mod n, A\equiv D\equiv I_g \mod n\}.$$

Then, $\sigma\cdot\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right] = \left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right], \phi_{(\mathbf{m},\mathbf{m}')} = 0$, and we obtain

$$\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\sigma\cdot\tau) = \kappa(\sigma)\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\tau),$$

and $\kappa(\sigma)^2 = e^{\frac{gn}{2}\pi i}$. If $gn\equiv 0 \mod 4$, we get $\kappa(\sigma) = 1$, hence, $\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\tau)^2$ is a modular form of weight 1.

A *level n-structure* on a polarized abelian variety A is a symplectic isomorphism

$$\phi : (\mathbb{Z}/n\mathbb{Z})^{2g}, J_{\mathsf{D}}) \to \mathrm{H}_1(A,\mathbb{Z}/n\mathbb{Z}),$$

where $\mathrm{H}_1(A,\mathbb{Z}/n\mathbb{Z})$ is equipped with the symplectic form $\mathrm{Im}(H)_{|\Lambda\times\Lambda}$ taken modulo n. Here, H is the positive definite hermitian form of type D that defines a polarization on A (see Section 1.2).

The moduli space of abelian varieties with level n and polarization of type D is denoted by $\mathcal{A}_{g,\mathsf{D}}(n)$. We have

$$\mathcal{A}_{g,\mathsf{D}}(n) \cong \mathrm{Sp}(J_{\mathsf{D}},\mathbb{Z})\cap\Gamma_g(n)\backslash\mathfrak{H}_g.$$

If $D = I_g$, we set $\mathcal{A}_{g,\mathsf{D}}(n) = \mathcal{A}_g(n)$.

Let $C : y^2 = f_{2g+2}(x_0, x_1)$ be an equation of a hyperelliptic curve of genus g. It is known that a choice of an order on the zeros of the binary form f_6 is equivalent to an isomorphism of symplectic spaces $\mathbb{F}_2^{2g} \to \mathrm{J}(C)[2]$. This defines a point in $\mathcal{A}_g(2)$. For $g = 2$, we have the following *Rosenhain formula* expressing the zeros of $f_6(x_0, x_1)$ in terms of theta constants. We order the zeros of f_6 to assume that they are $(0,1), (1,0), (1,1), (1,\lambda), (1,\mu), (1,\gamma)$. Then

$$\lambda = \frac{\theta\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right]^2}, \quad \mu = \frac{\theta\left[\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]^2}, \quad \gamma = \frac{\theta\left[\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]^2}{\theta\left[\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right]^2 \theta\left[\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right]^2}. \tag{7.2}$$

Let $V(2g+2)$ be the linear space of binary forms of degree $2g+2$, the group $\mathrm{SL}(2)$ acts naturally on the vector space $V(6)$ and we denote by $\mathrm{Inv}(2g+2)$ the ring of invariants $S^\bullet(V(2g+2)^*)^{\mathrm{SL}(2)}$. The relationship between the graded algebra of modular forms $\mathsf{M}(g; \mathrm{Sp}(2g, \mathbb{Z}))$ and the graded algebra of polynomial invariants $\mathrm{Inv}(2, 2g+2)$ is given by the following theorem of Igusa [78], Theorem 4:

Theorem 7.1. *Suppose $g = 2, 4$ or g is odd. There exists a ring homomorphism*

$$\rho : \mathsf{M}(g; \Gamma_2(1)) \to \mathrm{Inv}(2g+2)$$

such that $\rho(\mathsf{M}(g; \mathrm{Sp}(2g, \mathbb{Z})_w) \subset \mathrm{Inv}(2g+2)_{\frac{1}{2}wg}$. If $g = 2$, the homomorphism defines an isomorphism of the fields of fractions.

For example, assume $g = 1$. Then, it is known that $\mathsf{M}(1; \mathrm{Sp}(2, \mathbb{Z}))$ is generated by the Eisenstein series g_4, g_6 (the coefficients of the Weierstrass equation) and the ring of invariants is generated by the invariants of degree 2 and 3.

We have (again up to multiplicative constants):

$$\begin{aligned} \rho(E_4) &= I_4, \quad \rho(E_6) = I_2 I_4 - 3I_6, \quad \rho(\chi_{10}) = I_{10}, \\ \rho(\chi_{12}) &= I_2 I_{10}, \quad \rho(\chi_{35}) = I_{10}^2 I_{15}, \end{aligned}$$

where we use the notation for the Clebsch invariants of binary sextics from Chapter 5 (see [15], [78, p. 848]).

Note that I_{10} is equal to the discriminant of a binary sextic. Thus, χ_{10} does not vanish on the jacobian locus of $\mathcal{A}_2$. It vanishes on the locus $\mathcal{A}_2^{\mathrm{decom}}$ of decomposable abelian varieties $E \times E'$ with decomposable principal polarization. We see that the divisor of zeros of χ_{35} is equal to $2\mathcal{A}_2^{\mathrm{decom}} + \mathrm{Hum}(4)$.

Let P_1^{2g+2} be the GIT-quotient of $(\mathbb{P}^1)^{2g+2}$ by the group $\mathrm{PGL}(2)$ with respect to the linearization defined by the invertible sheaf $\mathbb{L} = \mathcal{O}_{\mathbb{P}^1}^{\boxtimes 6}$ (see [39]). Its points are minimal closed orbits of ordered sets of points $(p_1, \ldots, p_{2g=2}$ on $\mathbb{P}^1$ with no more than $g+1$ points coincide. We have

$$\mathsf{P}_1^{2g+2} = \mathrm{Proj}\, \mathsf{R}_1^{2g+2},$$

where

$$\mathsf{R}_1^{2g+2} = \bigoplus_{n=0}^{\infty} H^0((\mathbb{P}^1)^{2g+2}, \mathbb{L}^{\otimes n})^{\mathrm{SL}(2)}.$$

The permutation group $\mathfrak{S}_{2g+2}$ acts on $(\mathbb{P}^1)^{2g+2}$, and via this action, acts on the ring R_1^{2g+2}. The ring of invariants is isomorphic to the graded ring $\mathrm{Inv}(2, 2g+2)$. Thus, we obtain

$$\mathsf{S}_1^{2g+2} := \mathrm{Proj}\ \mathrm{Inv}(2, 2g+2) \cong \mathsf{P}_1^{2g+2}/\mathfrak{S}_{2g+2}.$$

By taking the double cover ramified along an unordered set of $2g+2$ points on $\mathbb{P}^1$, we can identify the hyperelliptic locus $\mathcal{H}_g$ in $\mathcal{M}_g$ with an open subset of S_1^{2g+2} of orbits of unordered sets of $2g+2$ distinct points. The pre-image of this open subset in P_1^{2g+2} can be identified with the moduli space $\mathcal{H}_g(2)$ of hyperelliptic curves together with a 2-level on its Jacobian variety. The group $\mathfrak{S}_{2g+2}$ is a subgroup of $\mathrm{Sp}(2g+2, \mathbb{F}_2)$ that acts on $\mathcal{H}_g^{2g+2}$ via changing the 2-level structure.

7.2 The Segre Cubic Primal and the Castelnuovo-Richmond quartic

From now on we assume that $g = 2$. By computing explicitly the algebra of invariants R_1^6 one finds that it is generated by the subspace $(\mathsf{R}_1^6)_1 = H^0((\mathbb{P}^1)^6, \mathbb{L})^{\mathrm{SL}(2)}$ of dimension 4 with a defining cubic relation that defines an $\mathfrak{S}_6$-equivariant isomorphism between P_1^6 and the *Segre cubic primal*, a cubic 3-fold in $\mathbb{P}^5$ given by equations

$$\sum_{i=0}^{5} t_i = \sum_{i=0}^{5} t_i^3 = 0$$

in $\mathbb{P}^5$. The group $\mathfrak{S}_6$ acts by permuting the variables. The Segre cubic is characterized among all cubic threefolds with at most ordinary nodes as singularities by the property that it has maximal number of nodes equal to 10. The singular points is the $\mathfrak{S}_6$-orbit of the point $[1, 1, 1, -1, -1, -1]$. It also has 15 planes forming the $\mathfrak{S}_6$-orbit of the plane $t_0 + t_1 = t_2 + t_3 = t_4 + t_5 = 0$. Each plane contains 4 singular points and each singular point is contained in 6 planes. The smooth part $\mathcal{S}_3'$ of $\mathcal{S}_3$ parameterizes orbits of ordered sets of points with no more than two points coincide. As is explained in [41, 9.4.4], the intersection of each plane with $\mathcal{S}_3'$ parameterizes the sets of points with two equal points. The singular points represent the minimal closed orbits of sets of points where three points coincide.

The discriminant invariant I_{10} of binary forms of degree 6 is a $\mathrm{SL}(2)$-invariant homogeneous polynomials in the coefficients of degree 10. If we write it in terms of roots as the product of bracket functions $(ij)^2, i < j$, we obtain a $\mathfrak{S}_6$-invariant section from $(\mathsf{R}_1^6)_{10}$. In the coordinates t_i in $\mathbb{P}^4$, it is defined by a hypersurface of degree 10. Its divisor of zeros on $\mathcal{S}_3$ is a surface of degree 30 equal to the union D of 15 planes of $\mathcal{S}_3$ taken with multiplicity 2.

It is a remarkable fact that the dual hypersurface of the Segre cubic primal $\mathcal{S}_3$ is isomorphic to $\mathrm{Proj}\ \mathsf{M}(g; \Gamma_2(2))$, a compactification $\overline{\mathcal{A}_2(2)}$ of the moduli space $\mathcal{A}_2(2)$ of abelian surfaces with a 2-level structure. In fact, according to J. Igusa [78], the ring of modular forms $\mathsf{M}(g; \Gamma_2(2))$ is generated by fourth powers of 10 theta constants $\theta\left[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}\right](\tau)$ generating the 5-dimensional space of modular forms of weight 2. The generators satisfy an $\mathfrak{S}_6$-invariant quartic relation such that, in appropriate choice of a basis, defines an isomorphism between $\overline{\mathcal{A}_2(2)}$ and the quartic 3-fold $\mathcal{I}_4$ defined by the following equations in $\mathbb{P}^5$:

$$\sigma_1 = \sigma_2^2 - 4\sigma_4 = 0,$$

where σ_k denote the k-th power-sums symmetric polynomials in variables x_i (see [78], [167]). The group $\mathrm{Sp}(4,\mathbb{Z})/\Gamma_2(2) \cong \mathfrak{S}_6$ acts on $\mathcal{I}_4$ by permuting the unknowns.

We have

$$H^0(\mathcal{I}_4, \mathcal{O}_{\mathcal{I}_4}(n)) \cong \mathsf{M}(2, \Gamma_2(2)_{2n}).$$

Considered as a hypersurface in $\mathbb{P}^4$, the quartic $\mathcal{I}_4$ of degree 4 in $\mathbb{P}^4$ was classically known as the dual hypersurface of the Segre cubic primal. It was called the *Castelnuovo quartic*, but nowadays, because of the moduli interpretation, it is called the *Igusa quartic* (in [41] it is called the *Castelnuovo-Richmond quartic*). The duality map

$$\Phi : \mathcal{S}_3 \dashrightarrow \mathcal{I}_4 \tag{7.3}$$

is given by the polar quadrics of $\mathcal{S}_3$ defined by linear combinations of partial derivatives of the equation of $\mathcal{S}_3$ in $\mathbb{P}^4$

$$F_3 = t_0^3 + t_1^3 + t_2^3 + t_3^3 - (t_0 + t_1 + t_2 + t_3 + t_4)^3 = 0.$$

Let $P_i = \frac{1}{3}\frac{\partial F_3}{\partial t_i} = 3t_i^2 - 3L^2$, where $L = t_0 + t_1 + t_2 + t_3 + t_4$. If we put

$$Q_i = P_i - \frac{1}{3}(P_0 + P_1 + P_2 + P_3), \quad i = 0, \ldots, 4, \tag{7.4}$$

$$Q_5 = -(t_1 + \cdots + t_4), \tag{7.5}$$

than we observe that the action of the group $\mathfrak{S}_6$ on the variables $t_0, \ldots, t_4$ defines the action on the polynomials $Q_0, \ldots, Q_5$ by permuting the set $\{0, \ldots, 5\}$. The usual Plücker formula implies that the dual of $\mathcal{S}_3$ is a quartic hypersurface (see [41], 1.2.3). Thus, the image of Φ is equal to a quartic 3-fold given by the equations $\sigma_1 = \sigma_2^2 + \lambda\sigma_4 = 0$ in variables $x_0, \ldots, x_5$. Observe that

$$x_i - x_j = Q_i - Q_j = t_i^2 - t_j^2, \quad 0 \le i, j \le 5. \tag{7.6}$$

This shows that the image of the plane $t_0 + t_1 = t_2 + t_3 = t_4 + t_5 = 0$ in $\mathcal{S}_3$ is equal to the line $x_0 - x_1 = x_2 - x_3 = x_4 - x_5 = x_0 + \cdots + x_5 = 0$. After plugging in these relations in the equation of the dual hypersurface, we find that $\lambda = -4$. This gives us an equation of the Igusa quartic.

We also check that the 15 lines on $\mathcal{I}_4$ equal to the images of the 15 planes under the map Φ are the double lines. Also each line contains 3 points, and each point lies on three lines.

Via the moduli interpretation, the restriction of the map Φ to the complement of the 15 planes should be viewed as the *Torelli map* that assigns to a hyperelliptic curve of genus two with an ordered set of Weierstrass points its Jacobian variety with a 2-level structure defined by the ordering of the Weierstrass points.

The map Φ extends to a resolution of singularities of $\mathcal{S}_3$ with exceptional divisors isomorphic to quadrics. They are mapped isomorphically to 10 quadrics contained in $\mathcal{I}_4$, taken with multiplicity 2 that are cut out by 10 hyperplanes. The intersection of the 10 quadrics with the open subset $\mathcal{A}_2(2)$ is the locus of abelian surfaces with a 2-level structure that are isomorphic to the product of two elliptic curves. To find the equations of the quadrics, we use the following fact about the duality map. Suppose X is a hypersurface of degree d with an isolated ordinary point x_0 of multiplicity

$d-1$. Choose coordinates such that $x_0 = [1, 0, \ldots, 0]$, so that the equation of X can be written in the form

$$F = x_0 F_d(x_1, \ldots, x_n) + F_d(x_1, \ldots, x_n) = 0.$$

Then, the dual map is not defined at x_0, but the image of the exceptional divisor under the lift of the duality map to the blow-up of x_0 is equal to the hyperplane in the dual projective space corresponding to the partial derivative $\frac{\partial F}{\partial x_0} = F_d(x_1, \ldots, x_n)$. Applying this to our case, by taking the singular point $[1, 1, 1, -1, -1, -1]$ of $\mathcal{S}_3$, we obtain that the image of the exceptional divisor is cut out by the hyperplane $x_0 + x_1 + x_2 = 0$. Plugging in this equation in the equation of $\mathcal{I}_4$, we easily obtain

$$(x_0x_1 + x_0x_2 + x_1x_2 + x_3x_4 + x_3x_5 + x_4x_5)^2 = 0. \tag{7.7}$$

This shows that the hyperplane cuts out $\mathcal{I}_4$ along a quadric surface taken with multiplicity 2.

7.3 The Humbert Surfaces in the Igusa Quartic

Now, we are ready to see an invariant-theoretical interpretation of Igusa modular forms $\chi_{10}, \chi_{12}, \chi_{35}$ when they are considered as modular forms with respect to the congruence subgroup $\Gamma_2(2)$.

Let $\mathrm{Hum}(\Delta; n)$ denote the set-theoretical pre-image of the Humbert surface $\mathrm{Hum}(\Delta)$ under the cover $\mathcal{A}_2(n) \to \mathcal{A}_2$.

Considered as $\mathrm{SL}(2)$-invariant sections of the line bundle $\mathbb{L}$ on $(\mathbb{P}^1)^6$, the functions $t_i - t_j$ are expressed in terms of the bracket functions (up to a constant multiple) by the formula

$$t_i - t_j = [ab, cd, ef], \tag{7.8}$$

where $[ab, cd, ef] = (ad)(cf)(be) - (bc)(df)(fa)$ vanish on the orbits of point sets in $\mathcal{H}_2(2) \subset P_1^6$ representing bielliptic curves ([41], Proposition 9.4.9 and (9.44)). The sums $t_i + t_j$ are expressed in terms of the bracket functions by the formula

$$t_i + t_j = (ab)(cd)(ef) \in (\mathsf{R}_1^6)_1. \tag{7.9}$$

They vanish only on the union D of the 15 planes. Formulas (7.6) show that the pre-image of the hyperplane sections $x_i - x_j = 0$ of $\mathcal{I}_4$ in $\mathcal{S}_3$ is equal to the union of a plane and an irreducible component of the locus representing bielliptic curves.

Let us consider the $\mathfrak{S}_6$-invariant polynomial

$$D = \prod_{0 \le i < j < k \le 5} (x_i + x_j + x_k). \tag{7.10}$$

Since $\sigma_1 = 0$ on $\mathcal{I}_4$, when restricted to $\mathcal{I}_4$, it becomes a square of a section s_D of $\mathcal{O}_{\mathcal{I}_4}(10)$. The divisor of zeros of s_D is equal to the union of 10 quadric surfaces representing $\mathrm{Hum}(1; 2)$ taken with multiplicity 2. The subgroup of $\mathfrak{S}_6$ stabilizing each irreducible component is isomorphic to $H = \mathfrak{S}_3 \times \mathfrak{S}_3$. It acts on the quadric Q defined by equation (7.7) via permuting $(0, 1, 2)$ and $(3, 4, 5)$. The ring of invariant polynomials for the action of $\mathfrak{S}_3 \times \mathfrak{S}_3$ on $\mathbb{C}[x_0, \ldots, x_5]$ is generated by $\sigma_1, \sigma_2, \sigma_3, \sigma_1, \sigma_2, \sigma_3$, where σ_i (σ_i') is an elementary symmetric polynomial in x_0, x_1, x_2

(x_3, x_4, x_5). This easily implies that the quotient Q/H is isomorphic to $\mathbb{P}(2,3,3)$. This is a compactification of $\mathrm{Hum}(1)$. The boundary is equal to the union of two lines $z_1 = 0$ and $z_2 = 0$ intersecting at the unique singular point of $\mathbb{P}(2,3,3)$.

The pre-image of the section s_D under the map Φ is a $\mathfrak{S}_6$-invariant section of $\mathbb{L}^{\otimes 20}$ that vanishes on the union of 15 planes with multiplicity 4 (since the pre-image of each $x_i + x_j + x_k$ is a polar quadric of a singular point that vanishes on 6 planes containing the point). As we remarked earlier, the discriminant invariant I_{10} vanishes on the same set with multiplicity 2. This shows that

$$\Phi^*(s_D) = I_{10}^2.$$

Recall that the divisor of zeros of s_D on $\mathcal{I}_4$ is the union of 10 quadric surfaces taken with multiplicity 2. Applying Theorem 7.1, we find that χ_{10}, considered as a modular form with respect to $\Gamma_2(2)$ vanishes on the union of the ten quadrics with multiplicity 1. If we consider χ_{10} as a section of $\mathcal{O}_{\mathcal{I}_4}(5)$, we get the equality (up to a scalar factor) of sections of $\mathcal{O}_{\mathcal{I}_4}^{10}$

$$\chi_{10}^2 = s_D.$$

It is known that

$$\chi_{10} = \Delta_5^2,$$

where

$$\Delta_5 := \prod_{[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}]} \theta[\begin{smallmatrix}\mathbf{m}\\ \mathbf{m}'\end{smallmatrix}](\tau)^2.$$

However, Δ_5 does not represent a modular form, it is a modular form up to a non-trivial character taking values ± 1.

Let

$$H = \prod_{0 \le i < j \le 5} (x_i - x_j). \tag{7.11}$$

The square H^2 is a $\mathfrak{S}_6$-invariant polynomial, the discriminant of a general equation of degree 6 with roots $x_0, \dots, x_5$. Let s_H be the corresponding section of $\mathcal{O}_{\mathcal{I}_4}(30)$. It follows from (7.8) and (7.9) that the divisor of zeros of s_H is equal to the closure $\overline{\mathrm{Hum}}(4;2)$ of the surface $\mathrm{Hum}(4;2)$ in $\overline{\mathcal{A}_2(2)}$. It consists of 15 irreducible components cut out by the hyperplanes $x_i - x_j = 0$. It is easy to see from the formulas that each such component is isomorphic to the *Steiner quartic surface* in $\mathbb{P}^3$ with three concurrent non-coplanar double lines (see [41], p. 70). The boundary $\overline{\mathrm{Hum}}(4;2) \setminus \mathrm{Hum}(4;2)$ consists of the union of the three lines. The group $\mathfrak{S}_6$ permutes the 15 components with stabilizer subgroup isomorphic to $\mathfrak{S}_4$. The normal subgroup of $\mathfrak{S}_4$ generated by the products of two commuting transpositions acts identically on the component. Thus, we obtain

$$\overline{\mathrm{Hum}}(4) \cong \overline{\mathrm{Hum}}(4;2)/\mathfrak{S}_3.$$

It is known that the equation of a Steiner quartic surface can be reduced to the form

$$t_0t_1t_2t_3 + t_1^2t_2^2 + t_1^2t_3^2 + t_2^2t_3^2 = t_0s_3 + (s_2^2 - 2s_3s_1),$$

where s_i are elementary symmetric functions in t_1, t_2, t_3. The group $\mathfrak{S}_3$ acts by permuting the variables t_1, t_2, t_3. This shows that $\overline{\mathrm{Hum}}(4)$ is isomorphic to a hypersurface of degree 4 in the

weighted projective space $\mathbb{P}(1,1,2,3)$ given by the equation $z_3(z_0-2z_1)+z_2^2=0$. The union of the three singular lines in $\overline{\mathrm{Hum}}(4;2)$ has the equation $t_1t_2t_3=0$. Its image in $\overline{\mathrm{Hum}}(4)$ is given by the equation $z_3=0$. The complement is isomorphic to the affine plane $\mathbb{C}^2$.

The pre-image of S_H under the map Φ is a $\mathrm{SL}(2)$-invariant section of $\mathbb{L}^{60}$ which is invariant with respect to $\mathfrak{S}_6$. It vanishes on the union of the locus of bielliptic curves with multiplicity 2 and on the union of 15 planes with multiplicity 6. We know that the invariant I_{15} vanishes on the locus of bielliptic curves and the discriminant invariant I_{10} vanishes on the union of planes with multiplicity 2. This implies that

$$\Phi^*(s_H)=I_{10}^3I_{15}^2.$$

Comparing with Theorem 7.1, we find that

$$\chi_{35}^2=\chi_{10}s_H.$$

Taking the square root we obtain

$$\chi_{35}=\Delta_5\cdot\prod_{0\le i<j\le 5}(x_i-x_j)$$

As we saw before, this gives the irreducible component of (see [167], (8.3)). Note that each factor is not a modular form, but the product is.

Let us now see the surface $\mathrm{Hum}(5;2)$. We refer for the proofs to [167], 8.4. The surface $\overline{\mathrm{Hum}}(5;2)$ consists of 6 irreducible components $H_i, i=0,\dots,5$. Each component H_i is given by an additional equation

$$2(\sum_{j\neq i}x_j)^2-\sum_{j\neq i}x_j^2=0.$$

It contains 5 of the 15 triple points of $\mathcal{I}_4$ no two of which are on a double line. For example, H_5 contains the points $[1,1,1,1,-2.-2],[1,1,1,-2,1,-2],\dots,[-2,1,1,1,1,-2]$. The complement to these five points is $\mathrm{Hum}(5;2)$. The plane Π_{ijk} spanned by three points is contained in one of the hyperplanes $x_i+x_j+x_k=0$. For example, the first three points in above are contained in $x_2+x_3+x_5=0$. Thus, the intersection of $\Pi_{ijk}\cap\overline{\mathrm{Hum}}(5;2)$ is a conic contained in one of the 10 quadric surfaces cut out by a hyperplane $x_i+x_j+x_k=0$.

Consider the following divisor in $\mathcal{A}_2(2)$

$$\mathsf{G}_\Delta=\sum_{d\ge 1,d^2|\Delta}v(\Delta/d^2)_2\mathrm{Hum}(\Delta/v^2;2),$$

where $v(k)_2=\frac{1}{2}$ if $k=1$ and 1 otherwise.

Theorem 7.2. *The divisor G_Δ is the divisor of zeros of a Siegel modular form g_Δ of weight $-60H(2,\Delta)$.*

Here the number $H(2,\Delta)$ is defined as the coefficient of the infinite series

$$\sum_{k=0}^{\infty}H(2,4k)e^{2\pi i4kz}+\sum_{k=0}^{\infty}H(2,4k+1)e^{2\pi i(4k+1)z}$$

equal to the Fourier expansion of a certain modular form in one variable of weight $5/2$ with respect to the group $\Gamma_0(4)$. Its first 8 nonzero coefficients $H(2,N)$ are given by $-120H(2,N) = 10, 70, 48, 120, 250, 240, 240$ for $N = 1, 4, 5, 8, 9, 12, 13$, respectively. For example, we have $\mathsf{G}_4 = \frac{1}{2}\mathrm{Hum}(1;2) + \mathrm{Hum}(4;2)$ is the divisor of the image of χ_{35} in $\mathsf{M}(2,\Gamma(2))$. The coefficient $1/2$ is explained by the fact that the map $\mathcal{A}_2(2) \to \mathcal{A}_2$ is ramified along H_1.

If $\Delta = 1$, the modular form g_1 with respect $\Gamma_2(2)$ is the discriminant Δ_5, a square root of χ_{10}. One can construct a modular form on $\mathfrak{H}_2$ that vanishes exactly on a Humber surface $\mathrm{Hum}(\Delta)$ for every Θ (see [166]).

Chapter 8

The Jacobian variety of curves of genus 3

A principally polarized abelian surface not isomorphic to the product of abelian varieties of smaller dimension is realized as the Jacobian variety of a nonsingular curve of genus 3. In this chapter, we will discuss endomorphisms of the Jacobian varieties of curves of genus 3.

8.1 Bielliptic Curves of Genus Three

Let A be an abelian surface with primitive polarization L_0 of degree 2. We have $(L_0^2) = 4$ and $h^0(L_0) = 2$. We assume that $|L_0|$ has no fixed components (this could happen only if $L_0 \cong \mathcal{O}_A(E+2F)$, where E, F are elliptic curves). Then, $|L_0|$ has four simple base points and its general member is a smooth curve C of genus 3. Translating C by some point in A, we may assume that C is symmetric in the sense that it is invariant with respect to the involution $\iota = [-1]_A$. This implies that all members of the pencil $|L_0|$ are invariant with respect to ι. The base points are among fixed points of $\iota : C \to C$. It follows from the Riemann–Hurwitz's formula that there are no more fixed points, and the quotient $C/(\iota)$ is an elliptic curve. A smooth projective curve is called *bielliptic* if it admits a degree 2 cover of an elliptic curve. Conversely, suppose $\pi : C \to E$ is a degree 2 cover of an elliptic curve by a smooth curve of genus 3. Then, $A = \mathrm{J}(C)/\pi^*E$ is an abelian surface. Choose a point $c_0 \in C$ and consider the composition $\tau : C \to A$ of the Abel-Jacobi embedding $i_{c_0} : C \hookrightarrow \mathrm{J}(C)$ and the projection $\mathrm{J}(C) \to A$. It follows from [6], Proposition (1.8) that this composition is a closed embedding. By the adjunction formula, $\tau(C)^2 = 4$ and $L_0 = \mathcal{O}_A(\tau(C))$ defines a primitive polarization of degree 2 on A.

Note that one can also consider the Prym variety $\mathrm{Prym}(C/E)$ defined to be the connected component of the kernel of the norm map $\mathrm{J}(C) \to E$. It is proven in loc. cit., Proposition (1.12) that it is the dual abelian surface $\hat{A}$.

Counting constants, we expect that bielliptic curves of genus 3 depend on 4 moduli, i.e. they form a subvariety of codimension 2 in $\mathcal{M}_3$. Since a general curve has at most one bielliptic involution,

we see that the locus of bielliptic curves is birationally isomorphic to a $\mathbb{P}^1$-bundle over $\mathcal{A}_{2,2}$. In particular, it is a rational variety (see for another proof of this fact in [5]).

Let C be a canonical curve of genus 3 over $\mathbb{C}$ with a bielliptic involution $\sigma : C \to C$. In its canonical plane model, σ is induced by a projective involution $\tilde{\sigma}$ whose set of fixed points consists of a point x_0 and a line ℓ_0. The intersection $\ell_0 \cap C$ are the fixed points of σ on C.

Theorem 8.1 (S. Kowalevskaya [98])**.** *The point x_0 is the intersection point of four distinct bitangents of C. Conversely, if a plane quartic has four bitangents intersecting at a point x_0, then there exists a bielliptic involution σ of C such that the projective involution $\tilde{\sigma}$ has x_0 as its isolated fixed point.*

Proof. Choose the projective coordinates such that $\tilde{\sigma}$ is defined by the formula $(x, y, z) \mapsto (x, y, -z)$. The isolated fixed point is $x_0 = (0, 0, 1)$ and the line of fixed points is $z = 0$. Since C is invariant with respect to $\tilde{\sigma}$, the equation of C can be written in the form

$$f(x, y, z) = z^4 - 2a_2(x, y)z^2 + a_4(x, y) = (z^2 - a_2(x, y))^2 + (a_4(x, y) - a_2(x, y)^2) = 0. \quad (8.1)$$

Here, $V(a_4(x, y) - a_2(x, y)^2)$ is the union of four lines $\ell_1, \dots, \ell_4$ passing through the point $x_0 = (0, 0, 1)$. Each line $\alpha_i x - \beta_i y_i = 0$ is tangent to C at two points $p_i^{\pm} = (\beta_i, \alpha_i, \pm\sqrt{a_2(\beta_i, \alpha_i)})$. Note that the four lines are distinct; otherwise the curve has a singular point at some point $((\beta_i, \alpha_i, \pm\sqrt{a_2(\beta_i, \alpha_i)})$. Also note that, if $a_2(\beta_i, \alpha_i) = 0$, then the point $p_i^+ = p_i^-$ is the *undulation point*, i.e. a point of tangency contact of order 4. The locus of quartic curves with an undulation point is hypersurface in the projective space of plane quartic curves. It is contained in the locus of zeros of the *undulation invariant* I_{60} of degree 60 (see [27] and [139]).

Conversely, suppose that four bitangents $\ell_1, \dots, \ell_4$ intersect at a point x_0. By Proposition 6.1.4 from [41], any three of the lines form a syzygetic triad of bitangents, i.e., the corresponding six tangency points lie on a conic. This implies that all eight tangency points lie on a conic. Choose coordinates so that $x_0 = (0, 0, 1)$. Let $\ell_i : l_i = 0$ and $B_2(x, y, z) = 0$ be the equation of the conic K passing through the eight tangency points. Then, the curves $V(B_2^2)$ and $V(l_1 \cdots l_4)$ cut out the same divisor on C, hence the equation of C can be written in the form $F = B_2^2 + l_1 l_2 l_3 l_4 = 0$, where $\ell_i = V(l_i)$ and $B_2 = a_0 z^2 + 2a_1(x, y)z + a_2(x, y)$. If $a_1 \neq 0$, we replace z with $a_0 z + a_1(x, y)$ to assume that $a_1(x, y) = 0$. Now the equation of C is reduced to the form (8.1). The involution $(x, y, z) \mapsto (x, y, -z)$ is the bielliptic involution of C. □

Here is another characterization of bielliptic quartic curves.

Theorem 8.2. *A genius three curve C is bielliptic if and only if the following conditions are satisfied:*

(i) There exists a line ℓ intersecting C at four distinct points $p_1, \dots, p_4$ such that the tangent lines ℓ_i at the points p_i intersect at one point p_0.

(ii) Let $P_{p_0}(C)$ be the cubic polar of C with respect to the point p_0 and let Q be the conic component of $P_{p_0}(C)$ (note that the line ℓ from above is a line component of $P_{p_0}(C)$). Then, ℓ is the polar line of Q with respect to p_0.

Proof. Suppose C is bielliptic. Applying the previous theorem, we may assume that it is given by equation (8.1). The polar cubic $P_{x_0}(C)$ has the equation $q = z(z^2 - a_2(x,y)) = 0$. It is the union of the line $\ell_0 = V(z)$ and the conic $Q = V(z^2 - a_2(x,y))$. The line ℓ_0 intersects C at the points $(\beta_i, \alpha_i, 0)$, where $a_4(\beta_i, \alpha_i) = 0$. By the main property of polars, $P_{x_0}(C)$ intersects C at the points p such that the tangent line of C at p contains the point x_0. Thus, the tangent lines of C at the intersection points of ℓ_0 with C pass through the point x_0. This verifies the first property.

Let us check the second one. Using the equation, we compute the line polar $P_{x_0^3}(C) = V(\frac{\partial^3}{\partial z^3}(F))$ of C. It coincides with the line ℓ_0. On other hand.

$$P_{x_0^3}(C) = P_{x_0^2}(P_{x_0}(C)) = P_{x_0^2}(qz) = P_{x_0}(q + P_{x_0}(q)z) = 2P_{x_0}(q) + P_{x_0^2}(q)z = z$$

(where we identify the polar curves with the corresponding partial derivatives). This implies that $V(P_{x_0}(q)) = V(z) = \ell_0$. This checks property (ii).

Let us prove the converse. Choose projective coordinates to assume that $\ell = V(z)$ and the intersection point of the four tangent lines is $x_0 = (0,0,1)$. The cubic polar $P_{x_0}(C)$ must contain the line component equal to ℓ. Write the equation of C in the form

$$a_0 z^4 + a_1(x,y)z^3 + a_2(x,y)z^2 + a_3(x,y)z + a_4(x,y) = 0.$$

We get

$$P_{x_0}(C) = V(4a_0 z^3 + 3a_1(x,y)z^2 + a_2(x,y)z + a_3(x,y)),$$
$$P_{x_0^2}(C) = V(12a_0 z^2 + 6a_1(x,y)z + a_2(x,y)),\ P_{x_0^3}(C) = 24a_0 z + 6a_1(x,y)$$

Since z divides the equation of the cubic polar, we obtain that $a_3(x,y) = 0$. If $a_0 = 0$, then $x_0 \in C$ and the line polar $P_{x_0^3}(C)$ vanishes at x_0. However, this polar line coincides with the tangent line of C at x_0. This implies that C is singular at x_0. So, we may assume that $a_0 \neq 0$. Thus, the first condition implies that C can be written in the form

$$z^4 + a_1(x,y)z^3 + a_2(x,y)z^2 + a_4(x,y) = 0.$$

Now, as in the first part of the proof, we obtain that $a_1(x,y) = 0$ if and only if condition (ii) is satisfied. Thus, C can be written in the form (8.1), and hence it is a bielliptic curve. □

For any general line ℓ, let $\ell_1, \dots, \ell_4$ be the tangents of C at the points $C \cap \ell$. Let $\ell_i \cap C = 2a_i + c_i + d_i$. adding up, we see that $\sum(c_i + d_i) \sim 4K_C - 2\sum a_i \sim 4K_C - 2K_C = 2K_C$. This shows that there exists a conic $S(\ell)$ that cuts out on C the divisor $\sum(c_i + d_i)$ of degree 8. This conic is called the *satellite conic* of ℓ (see [26]). The map $S : \mathbb{P}^2 \dashrightarrow \mathbb{P}^5, \ell \mapsto S(\ell)$ is given by polynomials of degree 10 whose coefficients are polynomials in coefficients of C of degree 7. Since $2\ell + S(\ell)$ and $T = \ell_1 + \cdots + \ell_4$ cut out on C the same divisor, we obtain that the equation of C can be written in the form

$$F = l_1 \cdots l_4 + l^2 q = 0,$$

where $\ell_i = V(l_i), \ell = V(l)$, and $S(\ell) = V(q)$.

Assume that ℓ has the property

(*) the four tangents ℓ_i intersect at a common point x_ℓ.

Choose the coordinates such that $x_0 = (0, 0, 1)$ and $l = z$. Then, the equation of C is of the form

$$F = z^2(a_0z^2 + a_1(x, y)z + a_2(x, y)) + a_4(x, y) = 0.$$

It is a bielliptic curve if and only if $a_1(x, y) = 0$. This is equivalent to that $P_{x_0}(S(\ell)) = \ell$. Thus, we obtain

Theorem 8.3. *Suppose a line ℓ satisfies the property (*) from above. Then, C is a bielliptic curve if and only if the polar line of the satellite conic $S(\ell)$ with respect to the point x_ℓ coincides with ℓ.*

Let ℓ be a line satisfying (*). The polar cubic of $P_{x_\ell}(C)$ passes through $C \cap \ell$, hence it contains ℓ as an irreducible component. In particular, $P_{x_\ell}(C)$ is singular. Recall that the locus of points $x \in \mathbb{P}^2$ such that $P_x(C)$ is a singular cubic is the Steinerian curve $\mathrm{St}(C)$ [41], 1.1.6. If C is a general enough, the degree of $\mathrm{St}(C)$ is equal to 12 and it has 24 cusps and 21 nodes. The cusps correspond to points such that the polar cubic is cuspidal, the nodes correspond to points such that the polar cubic is reducible. The line components define the set of 21 lines satisfying property (*). In [26], the 21 lines are described as singular points of multiplicity 4 of the curve of degree 24 in the dual plane parameterizing lines ℓ such that the tangents to C at three intersection points of C and ℓ are concurrent.

According to [27], the equation of the satellite conic $S(\ell)$ is equal to

$$SC_{7,2,10} + lC_{7,1,9} + l^2C_{7,0,8} = 0,$$

where $C_{a,b,c} \in S^a(S^4(V^\vee)^\vee) \otimes S^b(V) \otimes S^c(V^\vee)$ is a commitant of degree a in coefficients of C, of degree b in coordinates in the plane and the degree c in the dual coordinates. Thus, the vanishing of $a_1(x, y)$ from above is equivalent to the vanishing of the commitant $C_{7,1,9}$. The loc. cit. paper of Cohen gives an explicit equation of $C_{7,1,9}$.

Theorem 8.4. *C is bielliptic if and only if $C_{7,1,9}$, considered as a map $\mathbb{P}(V) \dashrightarrow \mathbb{P}(V^\vee)$ has one of the 21 lines corresponding to the nodes of $\mathrm{St}(C)$ as its indeterminacy point. The rational map is given by polynomials of degree 9 with polynomial coefficients in coefficients of C of degree 7.*

Next we assume that C is a hyperelliptic curve of genus 3. It is given by an equation in $\mathbb{P}(1, 1, 4)$

$$z^2 - f_8(x, y) = 0,$$

where f_8 is a binary form of degree 8 without multiple zeros. Any involution of C different from the hyperelliptic involution $\iota_h : (x, y, z) \mapsto (x, y, -z)$ defines an involution of $\mathbb{P}^1$. After choosing an appropriate coordinates (x, y), it can be written in the form $(x, y) \mapsto (x, -y)$. In these coordinates, the binary octic, being invariant, must be of the form $f_8 = g_4(x^2, y^2)$, where $g_4(u, v)$ is a binary quartic. Since f_8 has no multiple roots, the fixed point $0, \infty$ are not among its zeros (otherwise f_8 is divisible by x or y and cannot be written in the form $g_4(x^2, y^2)$).

The involution $\iota_b : (x, y, z) \mapsto (x, -y, z)$ has four fixed points $(0, 1, \pm 1$ and $(1, 0, \pm 1)$. The quotient is an elliptic curve with equation $w^2 = g_4(u, v)$. The involution $\iota_h \circ \iota_e : (x, y, z) \mapsto (x, -y, -z)$ has no fixed points. The quotient is a curve D of genus 2. I believe that $\mathrm{Prym}(C/D) \cong E$.

We have already explained in Section 7.1 that an order on the set of zeros of f_8 is equivalent to a 2-level structure on $\mathrm{J}(C)$. Let $\mathcal{A}_3(2)$ be the moduli space of principally polarized abelian 3-folds with level 2-structure and let $\mathcal{H}yp_3$ in be the hypersurface in $\mathcal{A}_3$ of Jacobians of hyperelliptic curves of genus 3. Its pre-image in $\mathcal{A}_3(2)$ splits in $36 = [\mathrm{Sp}(8,\mathbb{F}_2) : S_8]$ irreducible components permuted by $\mathrm{Sp}(8,\mathbb{F}_2)$. One of this components $\mathcal{H}_3(2)^0$ corresponds to a special symplectic basis in $\mathrm{H}_1(C,\mathbb{Z})$ defined by the Weierstrass points of C. It is isomorphic to the GIT-quotient P_1^8 of the variety of 8 distinct ordered 8 points in $\mathbb{P}^1$ modulo the group $\mathrm{SL}(2)$ (see Section 7.3). An involution $(x,y) \mapsto (x,-y)$ divides the set of zeros of f_8 into four orbits that belong to the same g_2^1 on $\mathbb{P}^1$. As we know from Example 4.3, the condition is that the four binary forms defining these orbits are linearly dependent. Let $\pi : \mathsf{P}_1^8 \to \mathsf{P}_1^6$ be the map of the GIT-quotients defined by the projection $(p_1,\dots,p_8) \mapsto (p_1,\dots,p_6)$. The pre-image of a set of points corresponding to 3 pairs of points defining a bielliptic curve of genus 2 is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$.

Let us identify the points $(p_1,\dots,p_8)$ with the images in $\mathbb{P}^2$ under the Veronese map $\mathbb{P}^1 \to \mathbb{P}^2$. The four pairs (p_i,p_{i+1}) define a bielliptic curve of genus 3 if and only the lines $\langle p_i,p_{i+1}\rangle$ intersect at one point. Thus, the locus $\mathcal{H}yp_3^{\mathrm{biel}}(2)^0$ of bielliptic curves in $\mathcal{H}yp_3(2)^0$ is projected to the variety $\mathcal{M}_2^{\mathrm{biel}}$ of bielliptic curves of genus two with a 2-level structure in its Jacobian. The fibers are isomorphic to the pre-image of a line under the map $\mathbb{P}^1 \times \mathbb{P}^1 \to (\mathbb{P}^1)^{(2)} \cong \mathbb{P}^2$. They are conic in $\mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$. We know from the previous chapter that the GIT-compactification P_1^6 of Y_6 is isomorphic to the Segre cubic primal S_3. We also know from Section 7.3 that the condition that six points define a bielliptic curve is that the product of the differences $x_i - x_j$ is equal to zero. It consists of 15 irreducible components transitively permuted under $\mathfrak{S}_6$. Each irreducible component is isomorphic to a hyperplane section of S_3. It is isomorphic to a cubic surface. This shows that $\mathcal{H}yp_3^{\mathrm{biel}}(2)^0$ consists of 15 irreducible components each isomorphic to a conic fibration over a rational surface. It implies that $\mathcal{H}yp_3^{\mathrm{biel}}$ is birationally isomorphic to each such component and hence is a rational variety. An algebraic proof of this fact can be found in [110].

Remark 8.5. Let $tf_4(x,y,z) + g_2(x,y,z)^2 = 0$ be a pencil of plane quartics, where $V(f_4)$ is a nonsingular quartic curve and $V(g_2)$ is a nonsingular conic. For each t corresponding to a smooth quartic, we have 28 bitangents. When t goes to zero, these bitangents go to 28 chords connecting 8 intersection points $V(f_4) \cap V(g_2)$ (see [21], 5.3). This relates the Kowalevskaya's Theorem with the previous characterization of hyperelliptic bielliptic curves of genus 3.

8.2 Plane Quartic Curves and the Heegner Divisors

Let $C = V(f_4(x,y,z))$ be a nonsingular plane quartic. The quartic surface X given by the equation

$$w^4 + f_4(x,y,z) = 0$$

is a nonsingular K3 surface. It admits an automorphism σ of order 4, a generator of the group of deck transformations of the cover. The surface X can be also viewed as the double cover of the del Pezzo surface S of degree 2 given by the equation

$$u^2 + f_4(x,y,z) = 0.$$

Since S is isomorphic to the blow-up of 7 points in the plane, $\mathrm{Pic}(S) \cong I^{1,7}$, the standard odd unimodular hyperbolic lattice. This easily implies that $\mathrm{Pic}(X) \cong S := \langle 2\rangle \oplus \langle -2\rangle^{\oplus 7}$. Using

Nikulin's results [133], one can show that

$$T_X \cong T := \langle 2 \rangle^{\oplus 2} \oplus D_4^{\oplus 3}.$$

The automorphism σ acts on T_X and equips it with a structure of a quadratic lattice L of rank 7 over the ring of Gaussian integers $\mathbb{Z}[\mathbf{i}]$. It is isomorphic to the lattice T where $i = \sqrt{-1}$ acts preserving each direct summand and equal to the direct sum of the operators given by the following matrices

$$J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ -1 & 1 & 2 & 1 \end{pmatrix}.$$

Using this action, one equips the 14-dimensional linear space $L_{\mathbb{R}}$ with a structure of a complex linear space V of dimension 7. Let

$$\mathbb{B}_6 := \{[z] = [z_0, \dots, z_6] \in |V| : z_1^2 + \cdots + z_7 < z_0^2, z_0 \neq 0\} \cong \{(z_1, \dots, z_6) \in \mathbb{C}^6 : z_1^2 + \cdots + z_6 < 1\}.$$

It is a complex ball of dimension 6. The moduli space $\mathcal{M}_{K3,S,\phi}$ of lattice S polarized K3 surfaces together with an isomorphism $\phi : T \to L$ of $\mathbb{Z}[i]$-lattices is isomorphic to the orbit space

$$\Gamma \backslash \mathbb{B}_6,$$

where Γ is a certain *arithmetic group* acting discretely on the ball (see [95]). For any primitive vector $\delta \in L^\vee \subset V^\vee$ one defines a hyperplane

$$H_\delta = \{z \in |V| : \delta(z) = 0\} \cap \mathbb{B}_6.$$

The image of the union of H_δ with fixed $r = \delta^2 = -2n$ in $\mathcal{M}_{K3,S,\phi}$ is denoted by $\mathrm{Heeg}(n)$ and is called the *Heegner divisor*.

Let $\Lambda(\delta) = \langle \delta, \sigma^*(\delta) \rangle$. One checks that $\Lambda(\delta) \cong \langle -2n \rangle^{\oplus 2}$. It is clear that $H_\delta = H_{\sigma^*(\delta)}$, os that H_δ is described by a primitive embedding of Λ_δ in L. Suppose that the period point of X belongs to H_δ. Then, $S \oplus \Lambda_\delta$ primitively embeds in $\mathrm{Pic}(X)$, so that means that X acquires two additional linearly independent cycles. All vectors δ with fixed $\delta^2 = -2n$ are divided into two types according to whether $\frac{1}{2}\delta$ belongs to $L^\vee$ or not (types 1 and 2, respectively). They exists for any n and any type ([3], Proposition 3.4). We denote by $\mathrm{Heeg}(n)_i$ the image of the union of hyperplanes $H(\delta)$ with $\delta^2 = -2n$ and δ is of type $i = 1, 2$.

For example, $\mathrm{Heeg}(1)$ consists of two irreducible components $\mathrm{Heeg}(1)_1$ and $\mathrm{Heeg}(1)_2$. They parameterize, accordingly, the nodal quartic curves and the locus of hyperelliptic curves.

An irreducible plane curve D is called a *splitting curve* (cf. [3], Definition 4.4) if under the cover $X \to \mathbb{P}^2$ its pre-image splits in the union of four irreducible components. For example, a line intersecting $W = V(f_4)$ at one point is a splitting line. The main result of Artebani's paper is the following.

Theorem 8.6 (M. Artebani [3])**.** *If X belongs to $\mathrm{Heeg}(n)_i, n > 1$, then the quartic $C = V(f_4)$ admits a rational splitting curve of minimal degree $2(n-1)$ if $i = 1$ and degree $n - 2$ if $i = 2$. Moreover, C admits a splitting curve of odd degree if and only if X belongs to some $\mathrm{Heeg}(n)_2$.*

Here are examples:

- $\mathrm{Heeg}(3)_2$ is the locus of quartics admitting a hyperflex (i.e. a line intersecting the quartic at one point).
- $\mathrm{Heeg}(2)_1$ is the locus of quartics admitting a splitting conic.

Note that $\mathrm{Heeg}(3)_2$ is given by vanishing of an invariant of degree 60 on the projective space of quartics (see [27], [139]). We do not know whether it corresponds to the zero divisor of some automorphic form on the ball E_6. However, S. Kondō [97] constructs such automorphic forms for the Heegner divisors $\mathrm{Heeg}(1)_1$ and $\mathrm{Heeg}(1)_2$.

Remark 8.7. Every C admits a splitting curve of degree 4. To see this, take D to be defined by the equation $l^4 + f_4(x, y, z) = 0$, where l is a linear form. Then, D intersects C at four points $V(l) \cap C$. The pre-image of D on X splits in four plane sections $w^4 + l^4 = 0$. However, this obviously does not give rise to a Heegner divisor, see [3], Remark 4.11.

Suppose $A = \mathrm{J}(C)$ for some curve C of genus 3. It is easy to see from the description of moduli spaces of abelian varieties with the given type of endomorphisms that the condition that $\mathrm{End}(A) \neq \mathbb{Z}$ is not divisorial. However, it is interesting to investigate whether one can express this condition as the intersection of Heegner divisors.

8.3 Del Pezzo Surfaces and Plane Quartic Curves

In this section, following [184], we describe how to use Del Pezzo surfaces of degree 2, in order to construct plane quartics C such that the endomorphism ring of $\mathrm{End}(C)$ of their jacobian $J(C)$ is isomorphic to $\mathbb{Z}$.

Let us remind some basic facts about del Pezzo surfaces, referring for the proofs to [41, Chapter 8]. Recall that a del Pezzo surface X of degree d is a smooth projective surface with ample anti-canonical divisor $-K_X$. The number $d = K_X^2$ takes possible values in $\{1, \ldots, 9\}$. A del Pezzo surface of degree $d \geq 3$ is isomorphic to a surface of degree d in $\mathbb{P}^d$, embedded by the linear system $|-K_X|$.

If $d = 2$, the linear system $|-K_X|$ maps a del Pezzo surface of degree 2 to the projective plane $\mathbb{P}^2$. The map

$$\phi_{|-K_X|} : X \to \mathbb{P}^2$$

is a finite map of degree 2 ramified along a smooth plane quartic curve C. The linear system $|-K_X|$ on a del Pezzo surface of degree 1 is a pencil with one base point. However, the linear system $|-2K_X|$ defines a finite map of degree 2 onto a quadratic cone $Q \subset \mathbb{P}^3$. It is ramified along a smooth intersection of Q with a cubic surface in $\mathbb{P}^3$.

Any del Pezzo surface is a rational surface. Except the case when $d = 8$ and X is isomorphic to a smooth quadric in $\mathbb{P}^3$, there is a birational morphism

$$\pi : X \to \mathbb{P}^2 \tag{8.2}$$

that defines an isomorphism $X \cong \mathrm{Bl}_{\mathcal{P}}(\mathbb{P}^2)$ from X to the blow-up of the point set $\mathcal{P}$ of $9-d$ points $p_1, \dots, p_{9-d}$ in $\mathbb{P}^2$. The points must be in a *general position* in the following precise sense: no three points are collinear, no six points lie on a conic, and no cubic curves pass through the set $\mathcal{P}$ and is singular at one of the points. The last condition is void if $d \neq 1$.

Assume that X is not isomorphic to a smooth quadric. Let $\mathrm{Pic}(X)$ be the Picard group of X. Since X is a rational surface, it is a free abelian group isomorphic to the Néron-Severi group $\mathrm{NS}(X)$. The blowing-up structure (8.2) defines a basis $(e_0, e_1, \dots, e_{9-d})$, where e_0 is the divisor class of the pre-image $\pi^*(\ell)$ of a line in $\mathbb{P}^2$, and e_i is the divisor class of the exceptional curve E_i over $p_i \in \mathcal{P}$. It is a (-1)-*curve* on X, i.e. a smooth rational curve E with $E^2 = E \cdot K_X = -1$. Since the linear system $|E|$ consists only of E, we will identify E with its divisor class. We have $e_0^2 = 1, e_i^2 = -1, e_i \cdot e_j = 0$, if $i \neq j$. In particular, $(e_0, e_1, \dots, e_{9-d})$ is an orthonormal basis of the hyperbolic quadratic lattice $\mathrm{NS}(X)$. It defines an isomorphism of lattices $\mathrm{NS}(X) \to \mathsf{I}^{1,9-d}$, where $\mathsf{I}^{1,9-d}$ is the standard odd unimodular quadratic lattice of signature $(1, 9-d)$.

The known behavior of the canonical class under the blow-up a point on a smooth surface gives

$$K_X = -3e_0 + e_1 + \cdots + e_{9-d}.$$

Let $\mathbf{e}_0, \mathbf{e}_1, \dots, \mathbf{e}_{9-d}$ be the standard orthogonal basis in $\mathsf{I}^{1,9-d}$ satisfying $\mathbf{e}_0^2 = 1, \mathbf{e}_i^2 = -1$. A choice of an isomorphism of lattices

$$\phi : \mathsf{I}^{1,9-d} \to \mathrm{NS}(X) \tag{8.3}$$

satisfying

$$\phi(\mathbf{k}_{9-d}) = K_X,$$

is called a *geometric marking* of X. It is clear that a geometric basis of $\mathrm{NS}(X)$ defines a geometric marking of X.

The converse is also true. We use that $-K_X$ is ample, hence X has no (-2)-*curves* (i.e. smooth rational curves R with $R^2 = -1, R \cdot K_X = 0$). Then, the assertion follows from [41, Lemma 8.2.2].

Let $\mathrm{O}(\mathsf{I}^{1,9-d})_{\mathbf{k}_{9-d}}$ be the subgroup of the orthogonal group $\mathrm{O}(\mathsf{I}^{1,9-d})$ that fixes the vector $\mathbf{k}_{9-d}$. It is mapped to a subgroup $\mathrm{O}(\mathsf{E}_{9-d})'$ of the orthogonal group $\mathrm{O}(\mathsf{E}_{9-d})$, where $\mathsf{E}_{9-d} = \mathbf{k}_{9-d}^{\perp}$. The subgroup $\mathrm{O}(\mathsf{E}_{9-d})'$ contains the subgroup W_{9-d} generated by reflections

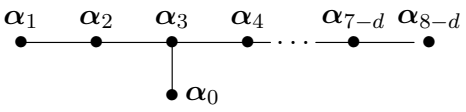
$$s_{\boldsymbol{\alpha}_i} : v \mapsto v + (v \cdot \boldsymbol{\alpha}_i)\boldsymbol{\alpha}_i.$$

It coincides with the whole group $\mathrm{O}(\mathsf{E}_{9-d})$ if $d = 1, 2$ and its index is equal 2 otherwise. For $d \leq 5$, the quadratic lattice E_{9-d} is isomorphic to the root lattice of a root system of type E_{9-d}, and the group W_{9-d} is isomorphic to the Weyl group of the root system.

In fact, we can fix a basis in E_{9-d} formed by the vectors

$$\boldsymbol{\alpha}_0 = \mathbf{e}_0 - \mathbf{e}_1 - \mathbf{e}_2 - \mathbf{e}_3, \quad \boldsymbol{\alpha}_1 = \mathbf{e}_1 - \mathbf{e}_2, \dots, \ \boldsymbol{\alpha}_6 = \mathbf{e}_{8-d} - \mathbf{e}_{9-d}.$$

If $d \leq 5$, the Gram matrix of this basis can be described by the diagram



(8.4)

in the same way, as it was explained earlier in the case $d = 1$ (see (3.15)). This diagram coincides with the *Dynkin diagram* of the root system of type E_{9-d}. The symmetry of the diagram is an involution in $\mathrm{O}(\mathsf{E}_{9-d})$ which does not belong to the image of $\mathrm{O}(\mathsf{I}^{1,9-d})_{\mathbf{k}_{9-d}}$ in $\mathrm{O}(\mathsf{E}_{9-d})$.

Fixing a geometric marking (8.3), we obtain a homomorphism

$$\rho : \mathrm{Aut}(X) \to W_{9-d} \subset \mathrm{O}(\mathsf{E}_{9-d}).$$

It is known to be injective for $d \leq 5$ [41, Corollary 8.2.40]. In particular, if $d = 2$ (resp. $d = 1$), the deck transformation γ (resp. β) of the double cover $\phi : X \to \mathbb{P}^2$, known as the *Geiser involution* (resp. the *Bertini involution*), defines an element in $W(E_7)$ (resp. $W(E_8)$). It is equal to the minus identity isometry w_0 in the Weil group.

It follows from above that any birational morphism $\pi : X \to \mathbb{P}^2$ is determined (up to a projective transformation of the plane) by a linear system $|\phi(\mathbf{e}_0)|$, where ϕ is a geometric marking of X. The vector $\mathbf{e}_0$, considered as a linear function on the sublattice $\mathsf{E}_{9-d} = \mathbf{k}_{9-d}$ coincides with the vector $\boldsymbol{\omega}_0$ from the dual basis basis $(\boldsymbol{\omega}_0, \dots, \boldsymbol{\omega}_{8-d})$ of the basis $(\boldsymbol{\alpha}_0, \dots, \boldsymbol{\alpha}_{8-d})$ of E_{9-d}. It is known that the Weyl group acts transitively on bases described by the Dynkin diagram (8.4). This shows that the number of non-projectively equivalent birational morphisms $\pi : X \to \mathbb{P}^2$ is equal to the cardinality of the orbit of $\mathbf{e}_0$. Its stabilizer is the subgroup of $W(E_{9-d})$ generated by reflections in vectors $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_{9-d}$. It is isomorphic to the symmetric group $\mathfrak{S}_{9-d}$ (the reflections s_{α_i} go to transpositions $(ii+1)$).

Known orders of the Weyl groups allow one to find the number of possible projective equivalence classes of birational morphisms $\pi : X \to \mathbb{P}^2$.

For example, in the case $d = 2$, the number is equal to 576. Thus, there are 576 non-projectively equivalent subsets $\mathcal{P}$ of seven points in general position which isomorphic to del Pezzo surfaces $\mathrm{Bl}_{\mathcal{P}}(\mathbb{P}^2)$.

Remark 8.8. The group W_{9-d} acts on geometric markings via its action on $\mathsf{I}^{1,9-d}$. This defines a homomorphism

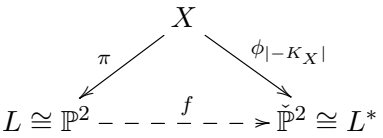
$$\mathrm{cr}_{2,9-d} : W_{9-d} \to \mathrm{Bir}(P_2^{9-d}),$$

where ${}^{\mathrm{gen}}P_2^{9-d} \subset (\mathbb{P}^2)^{9-d})//\mathrm{PGL}_3$ is the GIT-quotient of the of the open subset of $(\mathbb{P}^2)^{9-d}$ of ordered $9-d$ points in $\mathbb{P}^2$ in the general position. (see [41, Chapter VI]). In this action, the stabilizer subgroup of the orbit of a set $\mathcal{P}$ of $9-d$ points is isomorphic to the group of automorphisms of X. The Geiser and Bertini involutions generate the kernels of $\mathrm{cr}_{2,7}$ and $\mathrm{cr}_{2,8}$, respectively.

In this section, we will be interested only in the case $d = 2$. Denote by L the linear system of plane cubics with base locus equal to $\mathcal{P} = \{p_1, \dots, p_7\}$. Since $\mathcal{P}$ is in general position, all its members are irreducible curves. The proper transform of L in $X = \mathrm{Bl}_{\mathcal{P}}(\mathbb{P}^2)$ is equal to the anti-canonical linear system $|-K_X|$. The base locus of any pencil contained in L consists of two points p, q (maybe equal), the residual points of the intersection of two different members of the pencil. It defines a line $\langle p, q\rangle$ (if $p = q$, the line is the tangent line at p of all smooth cubics from the pencil). This allows us, via the projective duality, to identify L with the source plane of the anti-canonical map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$, and the dual plane L^* with its target plane.

Thus, the linear system L defines a rational map $f : L \dashrightarrow L^*$. The regular maps $\pi : X \to L$ and

$\phi_{|-K_X|} : X \to L^*$ make the following diagram commutative:



Recall that ϕ is a finite morphism of degree 2 with branch curve C of degree 4, and π is a birational morphism of the blowing up the closed subset $\mathcal{P}$ of $L = \mathbb{P}^2$.

Note that, via identification of the source $\mathbb{P}^2$ with L, each point $p_i \in \mathcal{P}$ can be identified with the cubic curve F_i in L with double point p_i. Its proper transform E_i' in X is a (-1)-curve, such that its image under the Geiser involution is the exceptional curve E_i of π. The intersection $E_i \cap E_i'$ consists of two points. The image $\phi(E_i + E_i')$ is a bitangent line ℓ_i of C with the tangency points $\phi(E_i \cap E_i')$.

The seven bitangents $\ell_1, \dots, \ell_7$ form an *Aronhold set* of bitangents [41, 6.3.3]. As is well known, there is a bijective correspondence between 28 bitangents and *odd theta characteristics* ϑ of C, the effective divisor classes with $2\vartheta = K_C$. An Aronhold set is defined by the property, that any three pairs of tangency points of bitangents from the set are not contained in a conic.

The proof of the fact that the images of $E_1, \dots, E_7$ under the map ϕ form an Aronhold set given in [41, 6.3.3] contains a mistake. So, we reprove it in the following:

Lemma 8.9. *The seven bitangents $\ell_1, \dots, \ell_7$ form an Aronhold set of bitangents.*

Proof. Let $E_i \cap E_i' = \{a_i, b_i\}$and $a_i', b_i' \in \mathbb{P}^2$ be their images under the map ϕ. Since $\pi^{-1}(\ell_i) = E_i + E_i'$, the ramification curve R of π passes through a_i, b_i. Suppose the tangency points $a_i'b_i'$ lie on a conic K. Let a, b be the residual pair of points in the intersection $K \cap B$. Then, $a + b \in |2K_C - \sum_{i=1}^3 (a_i' + b_i')|$ Since $2(a_i' + b_i') \in |K_C|$, we obtain that $a + b \in |K_C|$, hence a, b are the tangency points of some bitangent ℓ of C. The pre-image of ℓ in X splits into two (-1)-curves $E + \gamma(E)$. We have

$$2 = 2\ell \cdot \ell_i = (E + E') \cdot (E_i + E_i') = E + \gamma(E)) \cdot (E_i + \gamma(E_i)) = 2(E \cdot E_i) + 2(E' \cdot E_i).$$

Replacing E with $\gamma(E)$, and reordering the set $\{E_1, \dots, E_7\}$, if needed, we may assume that $E \cdot E_i = 1, i = 1, \dots, k$, and $E \cdot E_i = 0, i > k$, where $k \leq 3$. But then, $E = ae_0 - e_1 - \cdots - e_k$, and $E^2 = -1 = a^2 - k$. Since $0 < k \leq 3$, a^2 cannot be a square, this contradiction proves the lemma. □

It is known that there is a bijective correspondence between ordered Aronhold sets of bitangents and standard symplectic bases in $\mathrm{J}(C)[2]$. Both sets consist of 288 elements. Let is explain this correspondence. We identify a bitangent with an odd theta characteristic. An ordered Aronhold set $\vartheta_1, \dots, \vartheta_7$ of odd theta characteristics can be extended by adding one even theta characteristics θ_{ev} such that the ordered set of 8 theta characteristics $(\vartheta_1, \dots, \vartheta_7, \vartheta_{\text{ev}})$ becomes a *fundamental set* of theta characteristics (see [41, 5.4.3]). The set $\epsilon_i = \vartheta_i + \vartheta_{\text{ev}}$ is a normal set of 2-torsion points in

$\mathrm{J}(C)$, i.e. it satisfies $\omega(\epsilon_i, \epsilon_j) = 1, i \neq j$, where ω is the Weil pairing. The symplectic basis is $(u_1, u_2, u_3, \dots, u_6)$, where

$$u_i = \epsilon_1 + \cdots + \epsilon_{2i+2} + \epsilon_{2i+1}, \quad u_{i+3} = \epsilon_1 + \cdots + \epsilon_{2i+2} + \epsilon_{2i+2}, \quad i = 1, 2, 3.$$

The Weil group $W(E_7)$ acts transitively on geometric markings, and via this action, it acts transitively on the set of symplectic bases of $\mathrm{J}(C)[2]$. Fixing one geometric marking, we obtain a homomorphism

$$\alpha_{\mathcal{P}} : W(E_7) \to \mathrm{O}(\mathrm{J}(C)[2], \omega) \cong \mathrm{Sp}(6, \mathbb{F}_2).$$

Its kernel is equal to the subgroup (w_0) corresponding to the Geiser involutions γ. Comparing the orders of the groups, we find that α defines an isomorphism $W(E_7)/(w_0) \cong \mathrm{Sp}(6, \mathbb{F}_2)$.

Remark 8.10. The even theta characteristic ϑ_{ev} appears naturally in the geometry of del Pezzo surfaces of degree 2. For any even theta characteristic ϑ, the linear system $|K_C + \vartheta|$ consists of divisors $\mathfrak{d}$ of degree 6 on C such that $2\mathfrak{d}$ is cut out by a plane cubic. This defines an algebraic (non-linear) 3-dimensional system of contact cubics of C [41, 6.3.1]. Our theta characteristic ϑ_{ev} defines an algebraic system of cubics that contains the images of lines in $\mathbb{P}^2$ under the anti-canonical map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$. The pre-image of $f(\ell)$ is equal to $\ell + \ell'$, where ℓ' is a curve of degree 8 with triple points at the points p_i. The linear system of such curves defines a Cremona transformation of the plane, also called the *Geiser involution*. The sextic $\pi(R)$ is a projection to the plane of a curve of degree 6 in $\mathbb{P}^3$ equal to the image of C under the map given by the linear system $|K_C + \theta_{\mathrm{ev}}|$.

We already observed that, a choice of a geometric marking on X defines a surjective homomorphism from the Weil group W_7 to the group $\mathrm{Sp}(6, \mathbb{F}_2) \cong \mathrm{Aut}(\mathrm{J}(C([2], \omega)$. We can do better, and find a natural (i.e. independent of a choice of a geometric marking) surjective homomorphism

$$\Phi : \mathrm{NS}(X)_0/2\mathrm{NS}(X)_0 \to \mathrm{J}(C)[2]$$

whose kernel is equal to the radical of the quadratic form of $\mathrm{NS}(X)_0/2\mathrm{NS}(X)_0$ induced by the intersection form on $\mathrm{NS}(X)$.

We identify the branch quartic curve $C \subset \mathbb{P}^2$ of the anti-canonical map $\phi_{|-K_X|} : X \to \mathbb{P}^2$ with its ramification curve $R \subset X$. For any $D \in \mathrm{NS}(X)_0 = K_X^{\perp}$, the divisor class $\bar{D} := D \cap R$ belongs to $\mathrm{J}(C)$. Here we identify $D \cap R$ with the divisor class $c_1(\mathcal{O}_X(D) \otimes \mathcal{O}_R)$.

Lemma 8.11. *For any* $D \in 2\mathrm{NS}(X)_0$,

$$\bar{D} = 0.$$

Proof. Let γ be the Geiser involution of X. We know that, for any $D \in \mathrm{NS}(X)$, we have $D \cap R = \gamma(D) \cap R$. Since γ acts as $-\mathrm{id}_{\mathrm{NS}(X)_0}$, we get, for $D \in \mathrm{NS}(X)_0$,

$$D \cap R = \gamma(D) \cap R.$$

This implies the assertion of the lemma. □

It follows from the lemma that the homomorphism $\mathrm{NS}(X)_0 \to \mathrm{J}(C), D \mapsto D \cap R$. factors through a homomorphism

$$\Phi : \mathrm{NS}(X)_0/2\mathrm{NS}(X)_0 \to \mathrm{J}(C)[2].$$

Let M be the Gram matrix of the basis $(\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_7)$ of the quadratic lattice E_7. It is well known, and can be easily confirmed by explicit computation, that the reduction of M modulo 2 defines a symmetric bilinear form on $\mathsf{E}_7/2\mathsf{E}_7 \cong \mathbb{F}_2^7$ with radical generated by the vector $\mathbf{r} = \boldsymbol{\alpha}_0 + \boldsymbol{\alpha}_4 + \boldsymbol{\alpha}_6$ modulo $2\mathsf{E}_7$. The reduced matrix is the matrix of the symmetric form associated with a quadratic form on $\mathsf{E}_7/2\mathsf{E}_7$. We skip the verification that the homomorphism Φ is compatible with the Weil pairing on $\mathrm{J}(C)[2]$ (see [44, Chapter IX,§1, Lemma 2]).

Let $\mathrm{NS}(X)_{00} \cong \mathbb{Z}^6$ be the sublattice of $\mathrm{NS}(X)_0$ spanned by $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_6$. Its pre-image under the homomorphism $\mathsf{I}^{1,7} \to \mathrm{NS}(X)$ is equal to $\{\sum_{i=1}^7 a_i \mathbf{e}_i \in \mathsf{I}^{1,7} : a_1 + \dots + a_7 = 0\}$. It follows that the image $\overline{\mathrm{NS}}(X)_{00}$ of $\mathrm{NS}(X)_{00}$ in $\mathrm{NS}(X)_0/2\mathrm{NS}(X)_0$ does not contain the radical $\mathbb{F}_2\mathbf{r}$, hence it is mapped isomorphically onto $\mathrm{J}(C)[2]$.

Note that the stabilizer of $W(E_7)$ of the sublattice $\mathrm{NS}(X)_{00}$ of $\mathrm{NS}(X)$ is equal to the subgroup of $W(E_7)$ generated by reflections $s_{\boldsymbol{\alpha}_1}, \dots, s_{\boldsymbol{\alpha}_6}$. It is isomorphic to the permutation group $\mathfrak{S}_7$. It acts on $\overline{\mathrm{NS}}(X)_{00} \cong \mathbb{F}_2^6$ as the direct summand of the permutation representation of $\mathfrak{S}_7$ on $\mathbb{F}_2^7$. By definition of $\mathrm{NS}(X)_{00}$, there is an isomorphism of $\mathfrak{S}_7$-modules

$$\overline{\mathrm{NS}}(X)_{00} \cong (\mathbb{F}_2^{\mathcal{P}})^0,$$

where $(\mathbb{F}_2^{\mathcal{P}})^0 = \{\sum_{i=1}^7 a_i p_i, a_1 + \dots + a_7 = 0\}$.

This gives the following:

Proposition 8.12. *There is a natural isomorphism of $\mathfrak{S}_7$ modules*

$$\Phi : (\mathbb{F}_2^{\mathcal{P}})^0 \cong \mathrm{J}(C)[2]$$

that is compatible with the symplectic structure on the source and the target,

Remark 8.13. It follows from the previous discussion that there is a natural isomorphism between the orbit space U_2^7 of PGL_3 acting on the open subset ${}^{\mathrm{gen}}(\mathbb{P}^2)^7 \subset (\mathbb{P}^2)^7$ of ordered 7-tuples of points in the general position and the moduli space $\mathcal{M}_{3,\mathrm{can}}(2)$ of canonical curves of genus 3 with a 2-level structure on its jacobian. This beautiful fact was proven by Bert van Geemen in an unpublished manuscript.

Now, after we recalled some basic known facts about del Pezzo surfaces, let us return to our task: to construct smooth quartic curves C with $\mathrm{End}(\mathrm{J}(C)) \cong \mathbb{Z}$.

Let $f(t) = \sum_{i=0}^7 c_i t^i \in K[t]$ be an irreducible polynomial of degree 7 over K and $\alpha_1, \dots, \alpha_7$ be its roots in $\bar{K}$. We write $\mathcal{P}_f$ for the set of seven points $(1 : \alpha_i : \alpha_i^3)$ in $\mathbb{P}^2$.

Using the standard linear change of the variable $t' = t + \frac{c_6}{7c_7}$, we may assume that $c_6 = 0$ (without changing the Galois group of the polynomial $f(t)$). This is equivalent to the assumption $\alpha_1 + \ldots + \alpha_7 = 0$.

Lemma 8.14. *Assume $\alpha_i + \alpha_j + \alpha_k \neq 0$, for any three $\alpha_i, \alpha_j, \alpha_k$. Then, the points $p_i := (1 : \alpha_i : \alpha_i^3) \in \mathbb{P}^2$ are in a general position.*

Proof. We have to show that no three of the points from $\mathcal{P}_f$ are collinear, and no six points lie on a conic. Let $v_i = (1, \alpha_i, \alpha_i^3) \in \mathbb{C}^3$ represent $p_i \in \mathbb{P}^2$. Three points p_i, p_j, p_k lie on a line if and

and only if the determinant (ijk), where we assume that $i < j < k$, of the matrix with columns v_i, v_j, v_k is equal to zero. Computing this determinant, we find that it is equal to $-(\alpha_i - \alpha_j)(\alpha_j - \alpha_k)(\alpha_2 - \alpha_3)(\alpha_i + \alpha_j + \alpha_k)$. Our assumption implies that no three points are on a line.

Assume that six points are on a conic. Without loss of generality, we may assume that these points are $p_1, \dots, p_6$. It is classically known (see, for example, [24, p. 136, (9)]) that six points lie on a conic if and only if

$$(123)(145)(246)(356) - (124)(135)(236)(456) = 0$$

To prove this, one replaces v_6 with the vector of coordinates $v = (x, y, z)$ so that the left-hand side becomes a quadratic form in x, y, z. Then, replacing v with $v_i, i = 1, \dots, v_6$, we check that the quadratic form vanishes on $v_1, \dots, v_6$. Evaluating this expression, we find that it is equal to

$$\prod_{1 \le i < j \le 6} (\alpha_i - \alpha_j) \sum_{i=1}^{6} \alpha_i.$$

Since we assumed that $\alpha_1 + \dots + \alpha_7 = 0$, we see that the expression is not equal to zero.

□

Corollary 8.15. *Assume that the Galois group* $\mathrm{Gal}(f(t))$ *of* $f(t)$ *over* K *is a* 3*-transitive subgroup. Then, the points* $p_i = (1 : \alpha_i : \alpha_i^3)$ *are in a general position.*

Proof. By assumption, $\mathrm{Gal}(f(t))$ acts transitively on the sums of three roots. Thus, if the assumption of Lemma 8.14 is not satisfied, then all sums of three roots are equal to zero. Thus, we find that the sum of seven roots is equal to zero, in contradiction to our earlier assumption on the polynomial $f(t)$. □

Remark 8.16. Following [184, Proof of Lemma 1.3], let us give another proof of Corollary 8.15 that is based on elementary properties of polynomials in one variable. We will use a notation $(x : y : z)$ for homogeneous coordinates on $\mathbb{P}^2$. Suppose that here are three distinct points in $\mathcal{P}_f$ that lie on a line, say, $ax + by + cz = 0$ where a, b, c are three complex numbers and at least one of them is not zero. This means that there are three distinct roots $\alpha_1, \alpha_2, \alpha_3 \in \bar{K}$ of f such that all $a\alpha_i^3 + b\alpha_i + c = 0$ for all $i = 1, 2, 3$. It follows that the polynomial $ct^3 + bt + a \in \mathbb{C}[t]$ is not identically zero and has three distinct roots $\alpha_1, \alpha_2, \alpha_3$. This implies that $c \neq 0$ and

$$ct^3 + bt + a = c(t - \alpha_1)(t - \alpha_2)(t - \alpha_3).$$

It follows that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0.$$

Let us denote the remaining roots of f by $\alpha_4, \alpha_5, \alpha_6, \alpha_7$. Since $\mathrm{Gal}(K)$ acts 3-transitively on the roots of f, there exists $\sigma \in \mathrm{Gal}(K)$ such that

$$\sigma(\alpha_1) = \alpha_4, \sigma(\alpha_2) = \alpha_2, \sigma(\alpha_3) = \alpha_3$$

and therefore

$$\alpha_2 + \alpha_3 + \alpha_4 = \sigma(\alpha_2 + \alpha_3 + \alpha_1) = \sigma(0) = 0.$$

This implies that $\alpha_1 = \alpha_4$, which is not the case. The obtained contradiction proves that no three points of $\mathcal{P}_f$ lie on one line. Suppose that six points of $\mathcal{P}_f$ lie on one conic. Let

$$a_6z^2 + a_4yz + a_3xz + a_2y^2 + a_1xy + a_0x^2 = 0$$

be an equation of the conic. Then not all the coefficients a_i do vanish and there are six distinct roots of f, say, $\alpha_1, \cdots, \alpha_6$, such that

$$a_0\alpha_k^6 + \sum_{i=0}^{4} a_i\alpha_k^i = 0 \quad \forall i = 1, \ldots, 6.$$

This implies that the polynomial $a_6t^6 + \sum_{i=0}^{4} a_it^i$ is not identically zero and has 6 distinct roots $\alpha_1, \cdots \alpha_6$. It follows that $a_6 \neq 0$ and

$$a_6t^6 + \sum_{i=0}^{4} a_it^i = a_6 \prod_{i=1}^{6}(t - \alpha_i).$$

This implies that $\sum_{i=1}^{6} \alpha_i = 0$. Since the sum of all roots of f lies in K, the remaining seventh root of f lies in K. This contradicts to the irreducibility of f. The obtained contradiction proves that no six points of $\mathcal{P}_f$ lie on one conic. (Notice that we did not assume that $c_6 = 0$.)

Let the blowup $X(f) = \mathrm{Bl}_{\mathcal{P}}(\mathbb{P}^2)$ be the corresponding del Pezzo surface of degree 2. Since $\mathcal{P}_f$, considered as closed subscheme of $\mathbb{P}^2$, is defined over K, the surface is defined over K. Also, since the map $\phi : X(f) \to \mathbb{P}^2$ is given by the anti-canonical linear system, it is defined over K.

Let $L = |-K_X|$, considered as the linear system of plane cubic curves with base locus $\mathcal{P}_f$. It is equal to the projective space H_f, where is the $\bar{K}$-vector space of cubic ternary forms in $K[x, y, z]$ vanishing at seven points $(1, \alpha_i, \alpha_i^3)$.

The following lemma (see [184, Sect. 3]) gives an explicit map $\phi : X \to \mathbb{P}^2$ that confirms that it can be defined over K:

Lemma 8.17. *The following cubic forms form a basis of H_f:*

$$\begin{aligned} U &= xz^2 - y^3, \\ V &= c_7x^2y + c_6x^2z + c_5xy^2 + c_4xyz + c_3xz^2 + c_2y^2z + c_1yz^2 + c_0z^3, \\ U &= x^3 - (d_6x^2z + d_5xy^2 + d_4xyz + d_3xz^2 + d_2y^2z + d_1yz^2 + d_0z^3), \end{aligned}$$

where $r(t) = \sum_{i=0}^{7} d_it^i$ is the remainder of the division of t^9 by $f(t)$.

Proof. The cubic form U obviously vanishes on $\mathcal{P}_f$. The x-degree of u is 1. Taking into account that the degree 7 polynomial $f(t) = \sum_{i=0}^{7} c_it^i \in K[t]$ coincides with

$$c_7(t^3)^2 + c_5t^3t^2 + c_4t^3t + c_3t^3 + c_2t^2 + c_1t + c_0,$$

we conclude that the cubic form

$$V := c_7x^2y + c_5xy^2 + c_4xyz + c_3xz^2 + c_2y^2z + c_1yz^2 + c_0z^3$$

vanishes on $\mathcal{P}_f$. Since $\deg(f) = 7$, the coefficient $c_7 \neq 0$. Hence, the x-degree of v is 2. In order to find a third vanishing form (and get the basis), let us define a polynomial $r(t) \in K[t]$ as the (non-zero) remainder with respect to division by $f(t)$:

$$t^9 - r(t) \in f(t)K[t],\ \deg(r) < \deg(f) = 7.$$

We have

$$r(t) = \sum_{i=0}^{6} d_i t^i \in K[t].$$

Hence, if α is a root of $f(x)$ then

$$0 = \alpha^9 - h(\alpha) = \alpha^9 - \sum_{i=0}^{6} d_i \alpha^i = (\alpha^3)^3 - \left(d_6(\alpha^3)^2 + d_5(\alpha^3)\alpha^2 + d_4(\alpha^3)\alpha + d_3(\alpha^3) + d_2\alpha^2 + d_1\alpha + d_0\right).$$

This implies that the cubic form

$$W := x^3 - \left(d_6x^2z + d_5xy^2 + d_4xyz + d_3xz^2 + d_2y^2z + d_1yz^2 + d_0z^3\right)$$

vanishes on $\mathcal{P}_f$. The x-degree of w is 3. Since the forms U, V, W have x-degree 1,2,3 respectively, they are linearly independent over $\bar{K}$ and therefore constitute a basis of 3-dimensional $H_{\mathcal{P}_f}$. □

Remark 8.18. The anti-canonical map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ arises from the polynomial map of affine spaces $\mathbb{A}^3 \to \mathbb{A}^3$ defined by the polynomials U, V, W. It follows that the image $\pi(R)$ of the ramification curve of $\phi : X \to \mathbb{P}^2$ is a plane sextic given by the determinantal equation:

$$\begin{vmatrix} U_x & U_y & U_z \\ V_x & V_y & V_z \\ W_x & W_y & W_z \end{vmatrix} = 0.$$

Remark 8.19. Recall that our quartic curve lies in the dual plane $|-K_X|^*$ of $|-K_X|$ and seven points lie in $|-K_X|$. We considered seven points $(1 : \alpha_i : \alpha_i^2)$ lying on a cuspidal cubic $K = V(xz - y^2)$. That are nonsingular points on K. After we identify the set of nonsingular points on K with $\mathbb{C}$, we may identify the set of ordered seven nonsingular points on K with the vector space $\mathbb{C}^7$. Furthermore, one can identify this vector space with the Cartan algebra $\mathfrak{h}$ of the exceptional Lie algebra of type E_7 in such a way that the action of the Weyl group $W(E_7)$ on $\mathfrak{h}$ corresponds to the action of this group on the set of geometric markings of del Pezzo surfaces. In this way, one proves that the moduli space of geometrically marked del Pezzo surfaces of degree two together with a choice of a cuspidal anti-canonical divisor is isomorphic to the open subset $\mathbb{P}(\mathfrak{h})^\circ = \mathfrak{h}^\circ/\mathbb{C}^*$ of $\mathbb{P}(\mathfrak{h})$, where $\mathfrak{h}^\circ$ is the open Zariski subset of regular elements in the Cartan algebra [28]. It is known that a general set of seven points in the plane is contained in precisely 24 cuspidal cubic curves. Thus, the forgetting map of the moduli space of geometrically marked del Pezzo surfaces of degree 2 together with a choice of a cuspidal anti-canonical divisor is a degree 24 finite cover of the moduli space of geometrically marked del Pezzo surfaces of degree 2, and a finite cover of degree $24\#W(E_7)$ of the moduli space of del Pezzo surfaces of degree 2, or the moduli space of non-hyperelliptic curves of genus 3.

The absolute Galois group $\mathrm{Gal}(K) = \mathrm{Gal}(\bar{K}/K)$ acts naturally on $\mathbb{P}^2(\bar{K})$. Let $f(x) \in K[x]$ be with roots $\alpha_1, \dots, \alpha_7$ that add to zero, and $\mathcal{P}_f \subset \mathbb{P}^2(\bar{K})$ be as above.

By construction of $\mathcal{P}_f$, $\mathrm{Gal}(K)$ permutes elements of $\mathcal{P}_f$, i.e., one may view $\mathcal{P}_f$ as an effective 0-cycle in $\mathbb{P}^2$ that is defined over K.

The following assertion was proven in [184].

Theorem 8.20. *Let $C(f)$ be the branch curve of the anti-canonical map $X(f) \to \mathbb{P}^2$. Assume that the Galois group $\mathrm{Gal}(f)$ of the polynomial $f(t)$ contains $\mathfrak{A}_7$. Then,*

$$\mathrm{End}(\mathrm{J}(C(f))) \cong \mathbb{Z}.$$

Proof. By Corollary 8.15, the seven points $p_i = (1 : \alpha_i : \alpha_i^3)$ are in the general position, so that the del Pezzo surface $X(f)$ and the quartic curve $C(f))$ are defined.

The Galois action on the set $\mathfrak{R}_f$ of roots of $f(t)$ gives rise to the $\mathrm{Gal}(K)$-module $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ (see Section 2.3.)

It follows from Theorem 2.21 that the $\mathrm{Gal}(f)$-module $\left(\mathbb{F}_2^{\mathcal{P}_f}\right)^0$ is very simple. Since $\mathrm{Gal}(K)$ acts on $\left(\mathbb{F}_2^{\mathcal{P}_f}\right)^0$ through its quotient $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathcal{P}_f)$, the $\mathrm{Gal}(K)$-module $\left(\mathbb{F}_2^{\mathcal{P}_f}\right)^0$ is also very simple. Now, it follows from Proposition 8.12 that the $\mathrm{Gal}(K)$-module $\mathrm{J}(C(f))[2]$ is very simple as well. Applying Theorem 2.15 to $X = \mathrm{J}(C(f))$ and $\ell = 2$, we conclude that $\mathrm{End}(\mathrm{J}(C(f))) = \mathbb{Z}$. □

Remark 8.21. *Mutatis mutandis*, we can repeat most (but not all) of the arguments, by considering the del Pezzo surface $X(f)$ of degree 1 isomorphic to the blowup of the set $\mathcal{P}_f$ of 8 points $(1 : \alpha_i : \alpha_i^3)$, where $\alpha_1, \dots, \alpha_8$ are roots of an irreducible degree 8 polynomial $f(t)$ with the Galois group containing $\mathfrak{A}_8$. The branch curve of the bi-anticanonical map $\phi_{|-K_X|}$ is a canonical curve $C(f)$ lying on a singular quadric Q in $\mathbb{P}^3$. It differs from a general canonical curve of genus 4 (lying on a smooth quadric) by the condition that $\mathrm{J}(C(f))$ has a vanishing even theta characteristic. However, the corresponding Galois module $\mathrm{J}(C(f))[2]$ is isomorphic not to $\left(\mathbb{F}_2^{\mathcal{P}_f}\right)^0$ but to $\mathbb{F}_2^{\mathcal{P}_f}$ [185, Lemma 4.6]. In particular, it is *not* very simple and even not simple). Still, it is possible to prove that $\mathrm{End}(\mathrm{J}(C(f)))$ is either $\mathbb{Z}$ or an order in a quadratic field [185, Th. 4.7]. (In particular, $\mathrm{J}(C(f))$ is a simple abelian fourfold.)

Chapter 9

Hodge Structures and Shimura Varieties

In this chapter, we will discuss the moduli spaces of abelian varieties with the same type of the endomorphism algebra. The most convenient tool for the description of these moduli space used the theory of Hodge structure which we remind here.

9.1 Real forms of complex semi-simple algebraic groups

In the following, we will be using the theory of *real forms* of complex algebraic groups. Let us remind some basic construction of this theory. First, we start with real forms of complex finite-dimensional Lie algebras $\mathfrak{g}$. We denote by $\mathfrak{g}^{\mathbb{R}}$ the real Lie algebra obtained from $\mathfrak{g}$ by restriction of scalars. By definition, a real form of $\mathfrak{g}$ is a real Lie subalgebra $\mathfrak{b}$ of $\mathfrak{g}^{\mathbb{R}}$ such that there exists an isomorphism $\alpha : \mathfrak{b}_{\mathbb{C}} \cong \mathfrak{g}$ of complex Lie algebras. The conjugation automorphism $x + \mathbf{i}y \mapsto x - \mathbf{i}y$ of $\mathfrak{b}_{\mathbb{C}}$ defines, via α, an anti-involution θ of $\mathfrak{g}$, i.e. θ is an involution of $\mathfrak{g}^{\mathbb{R}}$ that satisfies $\theta(\lambda z) = \bar{\lambda}\theta(z)$, for any $z \in \mathfrak{g}$ and any $\lambda \in \mathbb{C}$. Conversely, any such involution θ defines a real form $\mathfrak{b}$ of $\mathfrak{g}$ by setting $\mathfrak{b} = \mathfrak{g}^{\theta} := \{z \in \mathfrak{g} : \theta(z) = z\}$. It is easy to check that this construction defines a bijection between the set of isomorphism classes of real forms of $\mathfrak{g}$ and the set of conjugacy classes of anti-involutions of $\mathfrak{g}$.

A real Lie algebra $\mathfrak{b}$ is called *compact* if it admits a positive definite bilinear B form that is invariant with respect to the adjoint representation (i.e., $B([x, y], z) = B(x, [y, z])$ for any $x, y, z \in \mathfrak{b}$).

An example of an invariant bilinear form on $\mathfrak{b}$ is provided by the *Killing form* defined by $B(x, y) = \mathrm{Tr}(\mathrm{ad}(x) \circ \mathrm{ad}(y))$, where

$$\mathrm{ad}(x) : \mathfrak{b} \to \mathfrak{b},\ y \mapsto [x, y]$$

is the adjoint representation of $\mathfrak{b}$. This form is non-degenerate if and only if $\mathfrak{b}$ is semi-simple. Since any invariant bilinear form on a semi-simple Lie algebra is a scalar multiple of the (non-degenerate) Killing form, we see that the Killing form on a simple compact Lie algebra is definite (in fact, negative definite). This implies that a real Lie algebra is compact if and only if its Killing form is negative definite. Every semi-simple complex Lie algebra admits a unique, up to isomorphism,

compact real form. The corresponding involution is called a *Cartan involution*.

Example 9.1. Let $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{C})$ generated over $\mathbb{C}$ by the matrices

$$h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \quad e = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \quad f = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right).$$

It admits a non-compact real from $\mathfrak{sl}_2(\mathbb{R})$ generated by the same matrices over $\mathbb{R}$ and a compact real form $\mathfrak{su}_2$ generated by the matrices

$$\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \quad e = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \quad f = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right).$$

The corresponding anti-involutions $\mathfrak{sl}_2(\mathbb{C})$ are defined by $A \mapsto \bar{A}$ and $A \mapsto -{}^t\bar{A}$, respectively.

The similar formulae define the anti-involutions on $\mathfrak{sl}_n(\mathbb{C})$ with a non-compact real form $\mathfrak{sl}_n(\mathbb{R})$ and a compact real form $\mathfrak{su}_n$. Note that any commutative Lie algebra is obviously compact. The Lie algebra $\mathfrak{gl}_n(\mathbb{C})$ has a compact form $\mathfrak{u}_n$.

The notions of a real form and a Cartan involution extends to algebraic groups. An algebraic group defined over $\mathbb{R}$ is a real form of a complex algebraic group G if $H_{\mathbb{C}} \cong G$. According to the general nonsense about Galois cohomology, the group H is determined uniquely by an element of $\mathrm{H}^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathrm{Aut}(G(\mathbb{C}))$ defined by an automorphism α of $G(\mathbb{C})$ such that $\alpha^{-1} = \bar{\alpha}$. The group H is reconstructed from this automorphism as an algebraic group with the group $H(K)$ of K-points equal to $G^{\alpha}(K) := \{g \in G^{\mathbb{R}}(K) : \alpha(g) = \bar{g}\}$, where $G^{\mathbb{R}} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}G$ is the Weil restriction of scalars functor on the category of complex algebraic groups which admits a natural action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ via the conjugation isomorphism $K \otimes_{\mathbb{R}} \mathbb{C} \to K \otimes_{\mathbb{R}} \mathbb{C}$. The involution α as above is called the *Cartan involution* of G. There is a natural bijection between the set of real forms of G and the conjugacy classes of Cartan involutions. The Lie algebra of the real Lie group $H(\mathbb{R})$ is a real form of the complex Lie algebra of the complex Lie group $G(\mathbb{C})$ and the converse is true if one additionally assumes that $G^{\mathbb{R}}$ is generated by H and its connected component of the identity.

A real algebraic group H is called *compact* if the real Lie group $H(\mathbb{R})$ is compact. The Lie algebra $\mathrm{Lie}(H(\mathbb{R}))$ of $H(\mathbb{R})$ is compact, a positive definite invariant symmetric form can be obtained by integral average over $H(\mathbb{R})$ of any positive symmetric bilinear form on $\mathrm{Lie}(H(\mathbb{R}))$. Every semi-simple complex algebraic group admits a unique, up to isomorphism, compact real form. The involutive automorphism α of G that defines a compact real form is called a *Cartan involution*.

Example 9.2. The complex multiplicative group $G = \mathbb{G}_{m,\mathbb{C}}$ has two non-isomorphic real forms: a non-compact form $\mathbb{G}_{m,\mathbb{R}}$ and a compact form $\mathbb{U}(1)$ which we introduced earlier. The first one corresponds to the involution $z \mapsto \bar{z}$, the second one corresponds to the involution $z \mapsto z^{-1}$.

The group SU_n is a compact form of $\mathrm{SL}_{n,\mathbb{C}}$ defined by the Cartan involution $A \mapsto {}^tA^{-1}$. A non-compact form is isomorphic to either $\mathrm{SL}_{n,\mathbb{R}}$, or $\mathrm{SU}_{p,n-p}$, or, if $n = 2m$, to the group $\mathrm{SL}_m(\mathfrak{H})$ defined by the involutions $A \mapsto A$, or $A \mapsto I_{p,n-p}{}^tAI_{p,n-p}^{-1}$, or $A \mapsto J_n{}^tAJ_n^{-1}$, where $I_{p,n-p} = \left(\begin{smallmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{smallmatrix}\right)$ and J_n is the matrix of the standard symplectic form on $\mathbb{R}^{2m}$. The group $\mathrm{SU}_{p,n-p}$ consists of complex matrices with determinant 1 preserving the Hermitian form $|z_1|^2 + \cdots + |z_p|^2 - |z_{p+1}|^2 - \cdots - |z_n|^2$. The group $\mathrm{SL}_m(\mathbb{H})$ consists of matrices of determinant 1 preserving a structure on $\mathbb{C}^{2m}$ of a module of rank m over the algebra of quaternions $\mathbb{H}$ (by viewing $(z_1, \ldots, z_{2m}) \in \mathbb{C}^{2m}$ as a vector $(z_1 + z_{m+1}\mathbf{j}, \ldots, z_m + z_{2m}\mathbf{j}) \in \mathbb{H}^m$).

9.2 Polarized Hodge Structures

Let V be a finite-dimensional vector space over $\mathbb{R}$. A *Hodge structure* on V is a direct sum decomposition

$$V_{\mathbb{C}} = \bigoplus_{p,q\in\mathbb{Z}} V^{p,q} \tag{9.1}$$

such that $\overline{V^{p,q}} = V^{q,p}$. We say that the Hodge structure is of *weight* n if $V^{p,q} = 0$ for $p + q \neq n$. .

A Hodeg structure of weight n defines a decreasing filtration

$$V_{\mathbb{C}} = F^0 \supset F^1 \supset \cdots \supset F^p \supset \{0\}$$

where $F^p = \oplus_{p'\geq p} V^{p',q}, \quad p = 0, \ldots, n$. It is called the *Hodge filtration*. It satisfies

$$V_{\mathbb{C}} = F^p \oplus \overline{F^{n-p+1}}$$

and recovers the Hodge structure since

$$V^{p,q} = F^p \cap \overline{F^q}.$$

A *polarized Hodge structure* consists of a Hodge structure on V and a non-degenerate bilinear form $Q : V \times V \to \mathbb{R}$ satisfying the following properties

(i) the conjugation map $V_{\mathbb{C}} \to V_{\mathbb{C}}$ maps induces an isomorphism $\bar{V}^{p,n-p} \cong V^{n-p,p}$;

(ii) $Q(a, b) = (-1)^n Q(b, a)$;

(iii $Q_{\mathbb{C}}(V^{p,q}, V^{p',q'}) = 0, \quad p' \neq n - p$;

(iv) $i^{p-q} Q_{\mathbb{C}}(x, \bar{x}) > 0$ if $x \in V^{p,n-p}, x \neq 0$.

A *rational (integral) polarized Hodge structure* of weight n is defined by an additional choice of a $\mathbb{Q}$-vector space $L_{\mathbb{Q}}$ (a lattice L of rank equal to $\dim V$) such that $V = L_{\mathbb{R}} = L_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$ ($V = L_{\mathbb{R}} = L \otimes \mathbb{R}$) and Q is obtained from a $\mathbb{Q}$-bilinear form ($\mathbb{Z}$-bilinear form)

$$Q_{\mathbb{Q}} : L_{\mathbb{Q}} \times L_{\mathbb{Q}} \to \mathbb{Q} \qquad (Q_{\mathbb{Z}} : L \times L \to \mathbb{Z}) \tag{9.2}$$

after tensoring with $\mathbb{R}$.

One can define the *category of rational polarized Hodge structures* by taking for morphisms linear maps defined over $\mathbb{Q}$ that preserve the Hodge filtrations and are compatible with the bilinear forms. One also put Hodge structure on the tensor product $V \otimes W$ by setting

$$(V \otimes W)^{p,q} = \bigoplus_{r+r'=p, s+s'=q} V^{r,s} \otimes W^{r',s'}.$$

and on the dual space by setting $F^p(V^\vee) = (V/F^{-p})^\vee = (F^{-p})^\perp$. In this way, the standard pairing $V \otimes V^\vee \to \mathbb{R}$, where $\mathbb{R} = \mathbb{R}^{0,0}$ becomes a morphism of Hodge structures. In particular, $(V^\vee)^{p,q} = V^{-p,-q}$.

Example 9.3. Define the Hodge structure $\mathbb{Z}(m)$ of weight $-2m$ on $V = \mathbb{R}$ by setting $V_{\mathbb{C}} = V^{-m,-m}$ with the polarization form $Q(x,y) = xy$. It has an integral structure with respect to the lattice $\mathbb{Z}$ in $\mathbb{R}$. Let $(V^{p,q})$ be a Hodge structure of weight n on a vector space V. Then, $V(m) := (V^{p,q}) \otimes \mathbb{Z}(m)$ is isomorphic to the Hodge structure $('V^{p,q})$ of weight $n-2m$ on V with $V(m)^{p,q} = V^{p-m,q-m}$. If $(V^{p,q})$ admits an integral structure defined by a lattice L in V, then $(V^{p,q}(m))$ admits an integral structure with $L(m) = L \otimes_Z \mathbb{Z} \cong L$ and $Q' = Q$. Note that, in particular,

$$V(m)^{0,0} = V^{m,m}.$$

The bilinear form Q defines an isomorphism $V^{p,q} \to (V^{n-p,p})^\vee = (V^\vee)^{p-n,-p} = V^\vee(n)^{p,q}$. Thus, we may view the polarization Q as a non-degenerate bilinear form of Hodge structures of weights n

$$V \times V \to \mathbb{R}(-n),$$

or as a tensor $q \in (V^\vee \otimes V^\vee)(-n)$ of type $(0,0)$.

Example 9.4. Let (V, J) be a complex structure on a real vector space V and $V_{\mathbb{C}} = V_{\mathbf{i}} \oplus V_{-\mathbf{i}}$ be the eigensubspace decomposition with respect to J. Putting $V^{-1,0} = V_i, V^{0,-1}$ defines a Hodge structure on W of weight -1. If Q is a symplectic form on V such that the complex structure is polarizable with respect to E, then the Hodge structure becomes Q-polarizable. The converse is also true, a Q-polarizable Hodge structure of weight -1 defines a Q-polarizable Hodge structure on V. Thus, the first homology space $\mathrm{H}_1(A, \mathbb{R})$ of an abelian variety acquires a polarizable Hodge structure of weight -1. The dual space $\mathrm{H}^1(A, \mathbb{R})$ acquires the dual Hodge structure of weight 1.

Example 9.5. Let X be any nonsingular complex algebraic variety of dimension n and $h_0 \in \mathrm{H}^2(X, \mathbb{Z})$ be the cohomology class of an ample divisor on X. The cup product $c \mapsto c \cup h_0$ defines a $\mathbb{Q}$-linear map $L : H^k(X, \mathbb{Q}) \to H^{k+2}(X, \mathbb{Q})$ and, by the Hard Lefschetz Theorem, for every positive $k \leq n$,

$$L^{n-k} : H^k(X, \mathbb{Q}) \to H^{2n-k}(X, \mathbb{Q})$$

is an isomorphism. One defines the *primitive cohomology* by setting

$$H^k(X, \mathbb{Q})_{\text{prim}} = \mathrm{Ker}(L^{n-k+1} : H^k(X, \mathbb{Q}) \to H^{2n+2-k}).$$

The primitive cohomology $H^k(X, \mathbb{Q})_{\text{prim}}$ admit a Hodge decomposition of weight k

$$H^k(X, \mathbb{C})_{\text{prim}} = \bigoplus_{p+q=k, p,q \geq 0} H^{p,q}(X),$$

which is polarizable with respect to the bilinear form

$$Q(\psi, \eta) = (-1)^{k(k-1)/2} \int_X h_0^{n-k} \wedge \psi \wedge \eta.$$

Note that in the case when X is a polarized abelian variety this agrees with the definition on the Hodge structure on $\mathrm{H}^1(A, \mathbb{Q}) = \mathrm{H}^1(A, \mathbb{Q})_{\text{prim}}$. We have

$$h_0^{n-1} \in H^{2n-2}(A, \mathbb{Q}) \cong H_2(A, \mathbb{Q}) = \bigwedge^2 \mathrm{H}_1(A, \mathbb{Q})^*$$

and we can consider the integral in the above as the value of the corresponding symplectic form on $\psi, \eta \in \mathrm{H}^1(A, \mathbb{Q})$.

Let $f : X \to S$ be a smooth projective morphism of complex manifolds. Then, it defines a variation of rational Hodge structures $(H^n(X_s, \mathbb{Q})_{\text{prim}}, H^{p,q}(X_s))$. We refer for the details to any exposition of the Hodge Theory on algebraic varieties (e.g. [171]).

Let M be a connected smooth complex manifold and $\mathcal{V}$ be a *complex local coefficient system* on M, i.e. locally constant sheaf sheaf (in the usual topology) of finite-dimensional real vector spaces on M. Suppose it is equipped with a decreasing filtration $(\mathcal{F}^p)$ such that it defines a Hodge filtration on each fiber $\mathcal{V}_t$ of $\mathcal{V}$.

Let $\underline{\mathcal{V}} := \mathcal{V} \otimes \mathcal{O}_M$ be the associated locally free sheaf of $\mathcal{O}_M$-modules, where $\mathcal{O}_M$ is the sheaf of holomorphic functions on M. We require that the sheaves $\mathcal{F}^p$ generate locally free submodules $\underline{\mathcal{F}^p}$ of $\underline{\mathcal{V}}$ (or, in terms of vector bundles, holomorphic subbundles of the holomorphic vector bundle $\underline{\mathcal{V}}$). Let

$$\Delta : \underline{\mathcal{V}} \to \underline{\mathcal{V}} \otimes \Omega^1_M$$

be the flat connection defined by differentiation of local trivializations of $\underline{\mathcal{V}}$ (it globalizes because the transition matrices have constant entries). We require that the following *transversality condition* is satisfied

$$\Delta(\underline{\mathcal{F}^p}) \subset \underline{\mathcal{F}^{p-1}} \otimes \Omega^1_M.$$

In the case when M is simply connected, $\mathcal{V}$ can be globally trivialized, and we can restate this condition in a simpler way. We consider the map

$$\phi : M \to G(f_p, V), \quad x \mapsto \mathcal{F}^p_x$$

to the Grassmannian of subspaces of V of dimension equal to $\dim \mathcal{F}^p_s$ (which does not depend on $s \in M$). The map is holomorphic and the image of the differential map of the tangent spaces of complex manifolds

$$d\phi_x : T^{\text{hol}}_{M,x} \to T^{\text{hol}}_{G(f_p,V),\mathcal{F}^p_x} = \mathrm{Hom}(\mathcal{F}^p_x, V/\mathcal{F}^p_x),$$

Following P. Deligne [37], one can reformulate the definition of a Hodge structure in the following way. Let

$$\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_{m,\mathbb{C}})$$

be the algebraic group over $\mathbb{R}$ obtained by Weil's restriction of scalars. It represents the functor $K \to (\mathbb{C} \otimes_{\mathbb{R}} K)^*$. It is easy to see that

$$\mathbb{S} = \mathrm{Spec}\ \mathbb{R}[X, Y, T]/((X^2 + Y^2)T - 1).$$

For any algebra K over $\mathbb{R}$, we have a natural bijection

$$\mathbb{S}(K) = \{\left(\begin{smallmatrix} a & b \\ -b & 0 \end{smallmatrix}\right) : a^2 + b^2 \neq 0\} \subset \mathrm{GL}_2(K).$$

In particular, we have a natural isomorphisms of groups

$$\mathbb{S}(\mathbb{R}) \to \mathbb{C}^*, \quad \left(\begin{smallmatrix} a & b \\ -b & 0 \end{smallmatrix}\right) \to a + b\mathbf{i}$$

and

$$\mathbb{S}(\mathbb{C}) \to (\mathbb{C}^*)^2, \quad \left(\begin{smallmatrix} a & b \\ -b & 0 \end{smallmatrix}\right) \to (a+b\mathbf{i}, a-b\mathbf{i}).$$

Under these isomorphism $\mathbb{S}(\mathbb{R})$ embeds in $\mathbb{S}(\mathbb{C})$ via $z \mapsto (z, \bar{z})$. Also there is an isomorphism of complex algebraic groups

$$\mathbb{S}_{\mathbb{C}} \to \mathbb{S} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{G}^2_{m,\mathbb{C}} \cong \text{Spec}(\mathbb{C}[Z, \bar{Z}, T/(Z\bar{Z}T - 1)).$$

The last isomorphism is of course defined by $Z = X + \mathbf{i}Y, \bar{Z} = X - \mathbf{i}Y$. The group $\mathbb{G}_{m,\mathbb{R}}(\mathbb{C})$ embeds in $\mathbb{S}(\mathbb{C})$ diagonally $z \mapsto (z, z)$. Let

$$\mathbb{U}(1) = \text{Spec } \mathbb{R}[U, V]/(U^2 + V^2 - 1)$$

be the real algebraic group with $\mathbb{U}(1)(\mathbb{R}) \cong \mathbb{U}(1) = \{z \in \mathbb{C} : |z| = 1\}$ and $\mathbb{U}(\mathbb{C}) \cong \mathbb{C}^*$. It is obviously a subgroup of $\mathbb{S}$ isomorphic to the kernel of the *norm homomorphism*

$$\text{Nm} : \mathbb{S} \to \mathbb{G}_{m,\mathbb{R}}, \quad \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mapsto a^2 + b^2.$$

Also it is isomorphic to the quotient $\mathbb{S}/\mathbb{G}_{m,\mathbb{R}}$ via the homomorphism $(z_1, z_2) \mapsto z_1/\bar{z}_2$.

Let $\rho : \mathbb{S} \to \text{GL}(V)$ be a homomorphism of real algebraic groups (a faithful real linear representation). It defines a complex linear representation $\rho_{\mathbb{C}} : \mathbb{S}(\mathbb{C}) \to \text{GL}(V_{\mathbb{C}})$. Restricting it to the subgroup $\mathbb{S}(\mathbb{R})$, we obtain an eigensubspace decomposition

$$V_{\mathbb{C}} = \oplus V^{p,q}, \quad V^{p,q} = \{v \in V_{\mathbb{C}} : \rho_{\mathbb{C}}(z_1, z_2) \cdot v = z_1^{-p}\bar{z}_2^{-q}v\}. \tag{9.3}$$

Obviously, $\overline{V^{p,q}} = V^{q,p}$, so $V^n := \oplus_{p+q=n} V^{p,q}$ is a Hodge structure on V^n of weight n. Any $z \in \mathbb{S}(\mathbb{R})$ acts on $V^{p,q}$ by multiplication $v \mapsto z^{-p}\bar{z}^{-q}$. In particular, any element in $\mathbb{G}_{m,\mathbb{R}}(\mathbb{R}) \subset \mathbb{S}(\mathbb{R})$ acts by scalar multiplication $v \mapsto \lambda^{-(p+q)}v$, and hence belongs to the center of $\text{GL}(V)$. So, the action of $\mathbb{G}_{m,\mathbb{R}}$ decomposes V into the direct sum of eigensubspaces V^n with eigencharacter $\lambda \mapsto \lambda^{-n}$ each of which is equipped with a Hodge structure of weight n.

Let $\mathbf{i} = \sqrt{-1}$ be considered as an element of $\mathbb{S}(\mathbb{R})$ and let $C = \rho(\mathbf{i})$. It is clear that C acts as $\mathbf{i}^{q-p}$ on $H^{p,q}$ and C^2 acts on V^n as the multiplication by $(-1)^n$. To get a polarized Hodge structure on V^n we require that the exists a bilinear form $Q : V \times V \to \mathbb{R}$ such that

$$Q(C(x), C(y)) = Q(x, y); \tag{9.4}$$

this implies that

$$Q(x, y) = (-1)^n Q(y, x) \text{ if } x, y \in V^n, \text{ and } Q(C(x), x) > 0 \text{ if } x \neq 0. \tag{9.5}$$

It is immediately checked that all properties of a polarized Hodge structure are satisfied. Conversely, a polarized Hodge structure on V defines a representation $\rho : \mathbb{S} \to \text{GL}(V)$ as above.

Definition 9.1. Let $(V, \rho : \mathbb{S} \to \text{GL}_{\mathbb{R}}(V), L_{\mathbb{Q}})$ be a rational Hodge structure (of weight n). Let $M_{\mathbb{Q}}$ be a $\mathbb{Q}$-vector subspace of $L_{\mathbb{Q}}$ and $W = M_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$ the corresponding real vector subspace of V. Let $\rho' : \mathbb{S} \to \text{GL}_{\mathbb{R}}(W)$ be the homomorphism of real algebraic groups that corresponds to the restriction of ρ to W. We say that $(W, \rho' : \mathbb{S} \to \text{GL}_{\mathbb{R}}(W), M_{\mathbb{Q}})$ is a rational Hodge substructure of $(V, L_{\mathbb{Q}})$ (of weight n) if W is $\mathbb{S}$-invariant. If this is the case, then $(W, \rho' : \mathbb{S} \to \text{GL}_{\mathbb{R}}(W), M_{\mathbb{Q}})$ becomes a rational Hodge structure of $(V, L_{\mathbb{Q}})$ (of weight n) with

$$W^{p,q} = V^{p,q} \cap W_{\mathbb{C}}.$$

Remark 9.6. Let $(V, \rho, L_{\mathbb{Q}})$ be a rational Hodge structure of weight n with a polarization Q. Let $(W, \rho', M_{\mathbb{Q}})$ be its rational Hodge substructure. Then, the restriction of Q

$$Q' = Q_{|W\times W} : W \times W \to \mathbb{R},\ x, y \mapsto Q(x, y)$$

is a polarization on $(W, M_{\mathbb{Q}})$. Indeed, all the properties of polarizations are obviously hold for $Q\prime$ except the non-degeneracy. In order to check the non-degeneracy of Q', notice that W is $C = \rho(i)$-invariant and if we put $C' = \rho'(i) \in \mathrm{Aut}_{\mathbb{R}}(W)$, then

$$C'(x) = C(x)\ \forall x \in W$$

and therefore

$$Q'(C'x), x) = Q(C(x), x) > 0\ \forall x \in W.$$

This implies that Q' is nondegenerate and therefore is a polarization on $(W, M_{\mathbb{Q}})$. Clearly, the restriction of Q' to $L_{\mathbb{Q}} \times L_{\mathbb{Q}})$ is a nondegenerare $\mathbb{Q}$-bilinear form with values in $\mathbb{Q}$.

Let $W^{\perp}$ be the orthogonal complement of W in V with respect to Q. The $\mathbb{S}$-semi-invariance of Q implies that $W^{\perp}$ is $\mathbb{S}$-invariant. We write $\rho'^{\perp} : \mathbb{S} \to \mathrm{GL}_{\mathbb{R}}(W^{\perp})$ for the corresponding homomorphism of real algebraic groups. The nondegeneracy of Q and its restriction Q' to W imply that $V = W \oplus W^{\perp}$; in addition, the restriction $Q'^{\perp}$ of Q to $M_{\mathbb{Q}}^{\perp}$ is nondegenerate. Similarly, if we write $M_{\mathbb{Q}}^{\perp}$ for the orthogonal complement of $M_{\mathbb{Q}}$ in $L_{\mathbb{Q}}$ then $L_{\mathbb{Q}} = M_{\mathbb{Q}} \oplus M_{\mathbb{Q}}^{\perp}$; in addition, $W^{\perp} = M_{\mathbb{Q}}^{\perp} \otimes_{\mathbb{Q}} \mathbb{R}$. Thus, $(W^{\perp}, \rho'^{\perp}, M_{\mathbb{Q}}^{\perp})$ becomes a rational Hodge structure of weight n with polarization $Q'^{\perp}$.

In other words, the polarized rational Hodge structure $(V, \rho, L_{\mathbb{Q}}, Q)$ is a direct sum of polarized rational Hodge structures $(W, \rho', M_{\mathbb{Q}}, Q')$ and $(W^{\perp}, \rho'^{\perp}, M_{\mathbb{Q}}^{\perp}, Q'^{\perp})$.

9.3 The Mumford-Tate Group

Let $(V, \rho : \mathbb{S} \to \mathrm{GL}_{\mathbb{R}}(V), L_{\mathbb{Q}})$ be a rational Hodge structure. Its *Mumford-Tate group* $\mathrm{MT}(L_{\mathbb{Q}}, \rho)$ is defined to be the smallest algebraic subgroup G of $\mathrm{GL}(L_{\mathbb{Q}})$ defined over $\mathbb{Q}$ such that $G(\mathbb{R})$ contains $\rho(\mathbb{S}(\mathbb{R}))$. Similarly, the special Mumford-Tate group (also called the *Hodge group*) $\mathrm{Hdg}(L_{\mathbb{Q}}, \rho)$ is defined to be the smallest algebraic subgroup H of $\mathrm{GL}(L_{\mathbb{Q}})$ defined over $\mathbb{Q}$ such that $H(U(1))$ contains $\rho(\mathbb{S}(\mathbb{R}))$.

Remark 9.7. Clearly, both $\mathrm{MT}(L_{\mathbb{Q}}, \rho)$ and $\mathrm{Hdg}(L_{\mathbb{Q}}, \rho)$ are connected linear algebraic groups over $\mathbb{Q}$. A $\mathbb{Q}$-vector subspace $M_{\mathbb{Q}}$ of $L_{\mathbb{Q}}$ is $\mathrm{MT}(L_{\mathbb{Q}}, \rho)$-invariant if and only if it is $\mathrm{Hdg}(L_{\mathbb{Q}}, \rho)$ -invariant, which means that $W = M_{\mathbb{Q}} \otimes \mathbb{R}$ gives rise to a rational Hodge substructure of V as in Definition 9.1. Both groups are reductive if the Hodge structure is polarizable. Indeed, the reductiveness means that each invariant subspace admits an invariant complement, whose existence is guaranteed, in light of Remark 9.6.

Let G be a reductive algebraic group over $\mathbb{Q}$ and (ID: Change the letter?)

$$\mathsf{h} : \mathbb{S} \to G_{\mathbb{R}}$$

be an injective homomorphism. For any faithful linear representation $\sigma : G \to \mathrm{GL}(V)$ of G in a $\mathbb{Q}$-vector space V, the composition $\rho = \sigma \circ h : \mathbb{S} \to \mathrm{GL}(V_{\mathbb{R}})$ defines a Hodge structure on V. Suppose V admits a polarization Q which is invariant with respect to the representation σ. Let $\theta = \mathsf{h}(\mathbf{i}) \in \mathsf{G}$ so that Q satisfies the symmetry and positivity conditions with respect to $C = \sigma(\theta)$. Suppose G acts on V via σ leaving Q invariant. Then, $\mathsf{h}(\mathbf{i}) \in G(\mathbb{R})$ is an element, whose square is mapped via σ to $-\mathrm{id}_V$. It follows that $\mathsf{h}(\mathbf{i})^2$ belongs to the center of $G(\mathbb{R})$ and even to the center of $G(\mathbb{C})$. It is known that the conjugation automorphism $\mathrm{Ad}(\mathsf{h}(\mathbf{i}))$ of $G_{\mathbb{C}}$ is a Cartan involution if and only if there exists a (equivalently, any) faithful linear representation $\sigma : G(\mathbb{R}) \to \mathrm{GL}(V)$ that preserves a bilinear form Q which is symmetric and positive with respect to $C = \sigma(\mathsf{h}(\mathbf{i}))$. Also the condition that G leaves the polarization on V invariant implies that G is a reductive group (see [37], Proposition 1.1.14).

Let D be a connected component of the conjugacy class of a homomorphism $h_0 : \mathbb{S} \to G_{\mathbb{R}}$ of algebraic groups over $\mathbb{R}$. We say that the pair (G, D) is a *Shimura data* if the following properties hold:

(S1) For any $\mathsf{h} \in \mathsf{D}$, $\mathsf{h}(\mathbb{G}_{m,\mathbb{R}})$ belongs to the center Z of $G_{\mathbb{C}}$ and the induced action of $U(1)$ on $\mathrm{Lie}(G^{\mathrm{ad}})_{\mathbb{C}}$ is via the characters $z, 1, \bar{z}$;

(S2) $\mathrm{Ad}(\mathsf{h}(\mathbf{i}))$ is a Cartan involution θ on $G^{\mathrm{ad}}_{\mathbb{C}} := G_{\mathbb{C}}/Z$;

(S3) G^{ad} has no $\mathbb{Q}$-factors on which the projection of h is trivial.

Let $\sigma : G_{\mathbb{R}} \to \mathrm{GL}(V)$ be a faithful linear representation of G as above. For any $\mathsf{h} \in X$, consider the composition $\rho_{\mathsf{h}} = \sigma \circ \mathsf{h} : \mathbb{S} \to \mathrm{GL}(V)$. It follows from the condition (S1) that the grading $V = \oplus_{n \in \mathbb{Z}} V^n$ defined by the action of $\mathbb{G}_{m,\mathbb{R}}$ on V does not depend on h. The condition $(S2)$ implies that G is a reductive algebraic group and that the stabilizer subgroup K_0 of h_0 is a maximal compact subgroup K of $G(R)$. The image $\mathsf{h}(U(1))$ of $(\mathbb{S}/\mathbb{G}_{m,\mathbb{R}}(\mathbb{R})$ is a subgroup of K_0. Let D be a connected component of $X = G(\mathbb{R})/K_0$. For any point $x \in \mathsf{D}$, the group $U(1)$ acts on the tangent space TD_x and defines a complex structure. In this way, D becomes equipped with a structure of a hermitian symmetric space. Condition (S3) implies that D is of non-compact type.

Fix a representation $\rho : G_{\mathbb{R}} \to \mathrm{GL}(V)$ and assume that it is defined over $\mathbb{Q}$ and preserves a bilinear for Q on V. So we obtain a *variation of Hodge structures* on V parameterized by $X = G(\mathbb{R})/K_0$.

Example 9.8. Let (V, J) be a complex structure on a real vector space V and $V_{\mathbb{C}} = V_{\mathbf{i}} \oplus V_{-\mathbf{i}}$ be the eigensubspace decomposition with respect to J. Putting $V^{-1,0} = V_i, V^{0,-1}$ defines a Hodge structure on W of weight -1. If Q is a symplectic form on V such that the complex structure is polarizable with respect to Q, then the Hodge structure becomes Q-polarizable. The converse is also true, a Q-polarizable Hodge structure of weight -1 defines a Q-polarizable Hodge structure on V. Thus, the homology space $\mathrm{H}_1(A, \mathbb{R})$ of an abelian variety acquires a polarizable Hodge structure of weight -1.

Let $G = \mathrm{CSp}(V; Q) \cong \mathrm{CSp}(2n)$ be the reductive group over $\mathbb{Q}$ whose set of K-points is equal to the set of linear maps $f : V \to V$ such that $Q(f(x), f(y)) = \lambda Q(x, y)$ for some $\lambda \in K^*$. Its center is isomorphic to $\mathbb{G}_m$ and the quotient G^{ad} is a simple algebraic group $\mathrm{Sp}(V; Q)$ of Q-isometries of V. Let $h : \mathbb{S} \to G$ be defined by sending $a + b\mathbf{i} \in \mathbb{S}(\mathbb{R})$ to $aI_{2n} + bJ$. Then, the

stabilizer of $h(\mathbb{S})$ in $G^{\mathrm{ad}}(\mathbb{R})$ consists of matrices $X = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(2n, \mathbb{R})$ such that $X^{-1}JX = J$. The fact that $X \in \mathrm{Sp}(2n, \mathbb{R})$ means that $A = D$ and $B = -C$. The second condition means that ${}^tBA - {}^tAB = 0$ and ${}^tAA + {}^tBB = I_n$. The map $X \mapsto \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \to A + \mathbf{i}B$ defines an isomorphism from the stabilizer subgroup to the unitary group $U(n)$ of complex matrices Z such that ${}^t\bar{Z}Z = I_n$. Thus

$$\mathsf{D} \cong \mathfrak{H}_n \cong \mathrm{U}(n)\backslash \mathrm{Sp}(2n, \mathbb{R}).$$

The Q-polarized Hodge structures on V of weight -1 correspond to the natural representation of G in V. This means that $z \in \mathbb{S}(\mathbb{R})$ acts on $V^{-1,0}$ by $x \mapsto zx$ and on $V^{0,-1}$ by $x \mapsto \bar{z}x$. This implies that it acts on the real vector space$V$ by $v \mapsto zv$.

We may also consider other linear representations of G, for example $\bigwedge^k V$ preserving the bilinear form $\bigwedge^k Q$. They define polarized Hodge structures on $\bigwedge^k V$ of weight $-k$. We could also consider the dual representation $V^\vee$ and the dual symplectic form Q^{-1} (where Q is considered as an invertible linear map $V \to V^\vee$). The Hodge structure on $V^\vee$ is of weight 1. We can view it as a Hodge structure on cohomology $\mathrm{H}^1(A, \mathbb{R})$ of an abelian variety $\mathbb{C}^g/\Lambda$, where $Q(\Lambda \times \Lambda) \subset \mathbb{Z}$. The Hodge structure on the exterior product $\bigwedge^k V^\vee$ is the Hodge structure on the cohomology $H^k(A, \mathbb{R})$. Its Hodge decomposition is $\oplus_{i=0}^k H^{k-i,i}$, where

$$h^{k-i,i} = \dim H^{k-i,i} = \binom{g}{i}^2.$$

One can also introduce other objects of the category of Hodge structures. For example, suppose $g = 2k + 1 > 1$ is odd. The polarization class $h \in \mathrm{H}^2(A, \mathbb{R})$ defined by Q belongs to the piece $H^{1,1}(A)$ of the Hodge structure. Consider the linear map

$$\Phi : H^1(A, \mathbb{R}) \to H^{2k+1}(A, \mathbb{R}),\ x \mapsto x \wedge h^{\wedge k}.$$

The quotient Hodge structure $H^{2k+1}(A, \mathbb{R})/\mathrm{Im}(\Phi)$ is of weight g and has the Hodge decomposition as in (9.3) with

$$h^{g-i,i} = \begin{cases} \binom{g}{i}^2 & \text{if } i \neq 1, g-1, \\ g^2 - g & \text{otherwise.} \end{cases}$$

We do not know whether there exists an algebraic variety whose Hodge structure on cohomology is naturally isomorphic to this Hodge structure.

Let D be a connected component of $X = G(\mathbb{R})/K$ regarded as a symmetric domain. The connected component of the group of holomorphic automorphisms of D is isomorphic to a connected component $G(\mathbb{R})^+$ of the identity of $G(\mathbb{R})$. A subgroup Γ of $G(\mathbb{Q})$ (a reductive algebraic group over $\mathbb{Q}$) is called a *congruence subgroup* if there exists a linear faithful representation $G \hookrightarrow \mathrm{GL}_n$ over $\mathbb{Q}$ such that the image of Γ contains a subgroup of finite index

$$\Gamma(N) = G(\mathbb{Q}) \cap \{g \in \mathbf{GL}_n(\mathbb{Z}) : g \equiv I_n \mod N\}.$$

A subgroup of $G(\mathbb{Q})$ is called *arithmetic* if it is commensurable with $\Gamma(1)$ (i.e. contains a subgroup of finite index in both of them). It is known that any arithmetic subgroup Γ acts discretely on D and the quotient $\Gamma\backslash\mathsf{D}$ has a structure of a quasi-projective algebraic variety. A *connected Shimura*

variety $\mathrm{Sh}^o(G,\mathsf{D})$ is the inverse system of locally symmetric spaces $\Gamma\backslash\mathsf{D}$ where Γ runs the set of torsion-free arithmetic subgroups of $G^{\mathrm{ad}}(\mathbb{Q})$ whose pre-image in $G(\mathbb{Q})$ is a congruence subgroup.

Let $\mathbb{A}_f$ be the ring of *finite adèles* of $\mathbb{Q}$, i.e. the subring of the product of the fields of p-adic numbers $\mathbb{Q}_p$ where all components except finitely many belong to the ring of integer p-adic numbers $\mathbb{Z}_p$. We use the p-adic topology on $\mathbb{Q}_p$ in which a base of open subsets of 0 is formed by the fractional ideals $p^\nu\mathbb{Z}_p$, where $\nu\in\mathbb{Z}$. For example, any element $x\in\mathbb{Q}_p$ contains an open compact neighborhood of the form $\{y\in\mathbb{Q}_p : y-x\in p^n\mathbb{Z}_p\}$. This topology make $\mathbb{Q}_p$ a locally compact field. One equips $\mathbb{A}_f$ with a topology whose base of open sets consist of subsets of the form $\prod_{p\in S}U_p\times\prod_{p\notin S}\mathbb{Z}_p$, where S is a finite set of prime numbers and U_p is an open subset of $\mathbb{Q}_p$. This topology, called the *adéle topology*. It is stronger than the product topology on $\mathbb{A}_f$. For an algebraic group G over $\mathbb{Q}$ one defines $G(\mathbb{A}_f)$ to be the subgroup of the product of groups $G(\mathbb{Q}_p)$ where all components except finitely many belong to $G(\mathbb{Z}_p)$. For example, when $G=\mathbb{G}_{m,\mathbb{Q}}$, we obtain the group of *idèles* $\mathbb{A}_f^*$. There is a canonical injection $G(\mathbb{Q})\to G(\mathbb{A}_f)$ defined by the homomorphisms $\mathbb{Q}\to\mathbb{Q}_p$. One can show that, for any compact subgroup K of $G(\mathbb{A}_f)$ the intersection $G(\mathbb{Q})\cap K$ is a congruence subgroup of $G(\mathbb{Q})$ ([117], Proposition 4.1). It follows that the induced topology on $G(\mathbb{Q})$ is a topology defined by a basis of open subsets equal to congruence subgroups. The *Strong Approximation Theorem* asserts that $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_f)$ if G is a semi-simple simply-connected with $G(\mathbb{R})$ of non-compact type.

The adèlic definition of the Shimura variety is based on an isomorphism

$$\Gamma\backslash\mathsf{D}\cong G(\mathbb{Q})\backslash\mathsf{D}\times G(\mathbb{A}_f)/K,$$

where K is a compact open subgroup of $G(\mathbb{A}_f)$ such that $K\cap G(\mathbb{Q})=\Gamma$, acting on $G(\mathbb{A}_f)$ on the right and $G(\mathbb{Q})$ acts on the product $\mathsf{D}\times G(\mathbb{A}_f)$ diagonally on the left so that

$$q\cdot(x,a)\cdot k=(qx,qak),\quad q\in G(\mathbb{Q}),x\in\mathsf{D},a\in G(\mathbb{A}_f),k\in K.$$

In this way $\mathrm{Sh}^o(G,\mathsf{D})$ becomes the inductive limit of $G(\mathbb{Q})\backslash\mathsf{D}\times G(\mathbb{A}_f)/K$, where K runs the set of open compact subgroups of $G(\mathbb{Q})$.

Let B be a semi-simple $\mathbb{Q}$-algebra with positive anti-involution $b\mapsto b'$ and let (V,Q) be a symplectic space that is a faithful $(B,')$-module. This means that the B-module V is faithful and

$$Q(bx,y)=Q(x,b'y)\ \forall b\in B;x,y\in V.$$

Then, one considers a reductive $\mathbb{Q}$-subgroup G of $\mathrm{CSp}(V,Q)$ that acts on V preserving the structure of a $(B,;)$-module. Then, there exists a homomorphism $\mathsf{h}:\mathbb{S}\to G(\mathbb{R})$ such that $\mathsf{h}(\bar z)=\mathsf{h}(z)'$ and $Q(\mathsf{h}(\mathbf{i})x,y)$ is a positive symmetric bilinear form. The conjugacy class of such h defines a Shimura data (G,X) that is mapped to the modular Shimura data $(\mathrm{CSp}(V,Q),\mathfrak{H}_g)$. When the algebra B is simple and the involution is the identity on the center, one says tha Shimura variety is of *PLE-type*.

Let (G,D) be a Shimura data and $h\in X$ and (V,h) be a Hodge structure defined by h. The *Mumford-Tate group* $\mathrm{MT}(h)$ is defined to be the smallest algebraic subgroup H of G defined over $\mathbb{Q}$ such that $G_{\mathbb{R}}$ contains $h(\mathbb{S})$. Let $\sigma:G\to\mathrm{GL}(V)$ be a faithful linear representation defined over $\mathbb{Q}$. We denote the image of $\rho=\sigma\circ h$ of $\mathrm{MT}(\mathsf{h})$ in $\mathrm{GL}(V)$ by $\mathrm{MT}(\sigma,\mathsf{h})$ (or $\mathrm{MT}(V,\mathsf{h})$ if no confusion arises). It is called the *Mumford-Tate group of the Hodge structure* on V defined by ρ. It

follows from the definition that the group $\mathrm{MT}(\mathsf{D},\mathsf{h})$ is the connected reductive group over $\mathbb{Q}$ equal to the $\mathbb{Q}$-closure of $\mathsf{h}(\mathbb{S})$ in $\mathbb{G}_{\mathbb{C}}$.

One can also define the *Hodge group* or *special Mumford-Tate group* by considering the restriction map $h' : \mathbb{U}(1) \to G^{\mathrm{ad}}$ and setting $\mathrm{Hg}(h)$ to be the smallest algebraic subgroup H over $\mathbb{Q}$ of G such that $H_{\mathbb{R}}$ contains $h'(\mathbb{U}(1))$. The groups $\mathrm{MT}(\mathsf{D},h)$ and $\mathrm{Hg}(\mathsf{D},h)\times\mathbb{G}_{m,\mathbb{Q}}$ are isogenous algebraic groups over $\mathbb{Q}$. Similarly, one defines the subgroup $\mathrm{Hg}(V,\mathsf{h})$ of $\mathrm{GL}(V)$ which is contained in $\mathrm{SL}(V)$.

For any nonnegative integers a and b, let $T^{a,b} = V^{\otimes a_i}\otimes V^{*\otimes b_i}$ be the tensor product space equipped with the tensor product Hodge structure of weight $a-b$. A rational vector $t\in\oplus_i T^{a_i,b_i}$ is of type $(0,0)$ if and only if it is invariant with respect to $\mathrm{MT}(V,\mathsf{h})$. In fact, if t is of type $(0,0)$, then $\mathsf{h}(\mathbb{S})$ leaves it invariant, hence the smallest algebraic subgroup that leaves it invariant must contain $\mathrm{MT}(V,\mathsf{h})$. Conversely, if t is invariant with respect to the Mumford-Tate group, then it is in particular invariant with respect to $h(\mathbb{S})$, hence it is of type $(0,0)$.

Since morphisms $V\to V$ preserving the Hodge structure correspond to tensors in $V\otimes V^\vee$ of type $(0,0)$, we obtain another equivalent definition of the Mumford-Tate group $\mathrm{MT}(V,\mathsf{h})$, it is the smallest algebraic $\mathbb{Q}$-subgroup of $\mathrm{GL}(V)$ such that

$$\mathrm{End}(V,\mathsf{h}) = \mathrm{End}(V)^{\mathrm{MT}(V,\mathsf{h})}.$$

More generally, if T is a subspace of the tensor algebra $T(V)\otimes T(V^\vee)$ with the inherited Hodge structure, then $\mathrm{MT}(V)$ acts in T and any $\mathbb{Q}$-subspace W of T is a Hodge substructure if and only if it is invariant under $\mathrm{MT}(V)$. In particular, if (V',h') is a Hodge substructure of (V,h), then $\mathrm{MT}(V',\mathsf{h}')$ coincides with the image of $\mathrm{MT}(V,\mathsf{h})$ in $\mathrm{GL}(V')$. In particular, $\mathrm{MT}(V',\mathsf{h}')$ is isomorphic to a quotient of $\mathrm{MT}(V,\mathsf{h})$.

In the case of the Hodge structure on cohomology of an algebraic variety X, we may consider Cartesian product X^d so that, by Künneth formula, their cohomology are isomorphic to the direct sums of tensor products $H^{a_1}(X,\mathbb{Q})\otimes\cdots\otimes H^{a_d}(X,\mathbb{Q})$. The cocycles of type (p,p) can be viewed as vectors of type $(0,0)$ in the tensor product with $\mathbb{Q}[r]$ for some r, where $\mathbb{Q}[r]$ is the one-dimensional space equipped with a Hodge structure of type $(-r,-r)$. Such classes are called *Hodge classes* (by Hodge's Conjecture they must be algebraic classes). Thus, in this situation, the special Mumford-Tate group is the smallest algebraic subgroup of $\mathrm{GL}(H^*(X,\mathbb{Q})$ that leaves invariant Hodge classes.

Example 9.9. Let A be an abelian variety and $V=\mathrm{H}_1(A,\mathbb{Q})$ with the Hodge structure of weight -1. The set of Hodge classes in $\mathrm{End}(V)=V^\vee\otimes V$ is equal to the set $\mathrm{End}_{\mathbb{Q}}(A)$. Hence

$$\mathrm{End}_{\mathbb{Q}}(A) = \mathrm{End}(V)^{\mathrm{MT}(V)}.$$

Using the notion of the Mumford-Tate group one can characterize abelian varieties of CM-type by the property that its Mumford-Tate group is commutative of the Hodge structure on its cohomology $H^*(X,\mathbb{Q})$ is commutative. It is conjectured that any complex projective algebraic variety with commutative Mumford-Tate group can be defined over a field of algebraic numbers [152]. Besides abelian varieties (Shimura - Taniyama [155]), this conjecture is known to be true for K3 surfaces [152].

In the next section, we will characterize abelian varieties of CM-type by the property that its Mumford-Tate group of is commutative A smooth projective algebraic variety is called of CM-*type* if the Mumford-Tate group of the Hodge structure on its cohomology $H^*(X,\mathbb{Q})$ is commutative. It is conjectured that such a variety can be defined over a field of algebraic numbers [152].

Example 9.10. Let A be an abelian variety with polarization skew-symmetric form Q. Let $D = \mathrm{End}_{\mathbb{Q}}(A)$ and $\mathrm{CSp}_D(V,\mathbb{Q}) := \mathrm{CSp}(V,\mathbb{Q})^D$. Since this group is a $\mathbb{Q}$-group containing $\mathsf{h}(\mathbb{S})$, we have

$$\mathrm{MT}(A) \subset \mathrm{CSp}_D(V,\mathbb{Q}). \tag{9.6}$$

When A is an elliptic curve, we get $\mathrm{Sp}(2) \cong \mathrm{SL}(2)$ and $\mathrm{CSp}(V,\mathbb{Q}) \cong \mathrm{GL}_{2,\mathbb{Q}}$. If $D = \mathbb{Q}$, then $\mathrm{MT}(A) = \mathrm{GL}_{2,\mathbb{Q}}$. If $D = \mathbb{Q}(\sqrt{-d})$, then $\mathrm{MT}(A)$ is conjugate to a subgroup of $\mathrm{GL}_{2,\mathbb{Q}}$ with the group of K-points equal to a subgroup of $\mathrm{GL}_2(K)$ of matrices of the form $\left(\begin{smallmatrix} x & y \\ -dy & x \end{smallmatrix}\right), x, y \in K$. The Hodge group $\mathrm{Hdg}(A)$ is defined by an additional condition that $x^2 + dy^2 = 1$.

Suppose A is a simple abelian surface. Then, we have the equality in (9.6). If $D = \mathbb{Q}$, then $\mathrm{MT}(A) \cong \mathrm{CSp}_{4,\mathbb{Q}}$. If $D = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then $\mathrm{MT}(A)$ is a subgroup of $\mathrm{Res}_{D/\mathbb{Q}}\mathrm{GL}_{2,D}$ whose group of K-points is equal to $\{g \in \mathrm{GL}_2(D \otimes_{\mathbb{Q}} K) : \det(g) \in K^*\}$. If D is an indefinite quaternion algebra, then $\mathrm{MT}(A)$ is the group of unites of the opposite algebra D, i.e. $\mathrm{MT}(A)(K) = (D^{\mathrm{op}} \otimes_{\mathbb{Q}} K)^*$. Finally, if D is a CM-field, then $\mathrm{MT}(A)$ is a subgroup of $\mathrm{Res}_{D/\mathbb{Q}}\mathbb{G}_{m,D}$ with $\mathrm{MT}(A)(K) = \{x \in (D \otimes K)^* : x\bar{x} \in K^*\}$. Note that, when $\dim A \geq 4$, the group $\mathrm{MT}(A)$ could be a proper subgroup of $\mathrm{CSp}_D(V,Q)$. For example, this happens in Mumford's example 11.1 of an abelian variety of dimension 4.

Example 9.11. Let X be a K3-surface that admits a non-symplectic automorphism σ of order m that acts identically on $\mathrm{Pic}(X)$. All such K3 surfaces have been classified in [94] and [172]. It is known that $\phi(m)$ divides the rank of the transcendental lattice T_X. All possible values of m are known. Assume that $m = \phi(m)$. Then, $m \in \{12, 28, 36, 42, 44, 66\}$ if T_X is unimodular and $m \in \{3, 5, 7, 9, 11, 13, 17, 19, 25, 27\}$ otherwise. There is only one isomorphism class of such a surface. Their lattices T_X are computed in [107].

The cyclotomic field $\mathbb{Q}(\zeta_m)$ acts on $(T_X)_{\mathbb{Q}}$ and hence equips it with a structure of a one-dimensional vector space over $\mathbb{Q}(\zeta_m)$. The proof of the previous proposition extends to this case and shows that the Mumford-Tate group of the Hodge structure on $(T_X)_{\mathbb{Q}}$ induced by the Hodge structure on $H^*(X,\mathbb{Q})$ is of CM-type.

Example 9.12. Let

$$X_m^1 : x_0^m + x_1^m + x_2^m = 0$$

be the *Fermat curve* of degree $m > 2$. For any pair (r,s) with $1 \leq r, s, r+s \leq m-1$, let

$$n = m/g.c.d.(m,r,s).$$

Let $\langle a \rangle$ denote the unique representative of $a \mod m$ between 0 and $m-1$ and let $H_{r,s}$ be the subset of $(\mathbb{Z}/n\mathbb{Z})^*$ of elements h such that

$$\langle rs \rangle, \langle hr \rangle \leq m-1.$$

It is easy to see that $H_{r,s}$ coincides with the set of representatives of the subgroup $\{\pm 1\}$ of $(\mathbb{Z}/n\mathbb{Z})^*$. Let us fix the standard isomorphism

$$\phi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \quad h \to \sigma_h : \zeta_n \to \zeta_n^h.$$

Define a lattice $\Lambda_{r,s}$ in $\mathbb{C}^{\phi(n)/2}$ to be the span of the vectors

$$\sigma_h(\omega_1, \ldots, \omega_{\phi(n)}), h \in H_{r,s},$$

where $(\omega_1, \ldots, \omega_{\phi(n)})$ is a basis of the ring of integers $\mathbb{Z}[\zeta_n]$. Since $H_{r,s} = hH_{\langle hr\rangle,\langle hs\rangle}$ for any $h \in H_{r,s}$, we obtain $\Lambda_{r,s} = \Lambda_{\langle hr\rangle,\langle hs\rangle}$. We say that the two pairs (r, s) and (r', s') related in this way are equivalent. Let $A_{r,s} = \mathbb{C}^{\phi(n)/2}/\Lambda_{r,s}$. There is an isogeny

$$\prod_{\{r,s\}} A_{r,s} \to \mathrm{J}(X_m^1), \tag{9.7}$$

where the product is taken over equivalence classes of pairs (r, s) as above [93]. Note that each variety $A_{r,s}$ is of dimension $\phi(n)/2$ and has multiplication by $\mathbb{Q}(\zeta_n)$, hence it is of CM-type. This implies that $\mathrm{J}(C)$ is of CM-type.

For example, take $m = p$ to be prime. Then, $n = p$, we have $p - 2$ equivalence classes of pairs (r, s) and obtain that $\mathrm{J}(C)$ is isogenous to the product of $p - 2$ copies of an abelian variety of dimension $\frac{1}{2}(p - 1)$ with complex multiplication by ζ_p.

Note that not all factors $J_{r,s}$ are simple abelian varieties, also some of the factors could be isomorphic. This is investigated in [93].

Example 9.13 (T. Katsura, T. Shioda [87])**.** Let X_m^r denote the Fermat hypersurface of degree m and dimension r:

$$x_0^m + \cdots + x_{r+1}^m = 0.$$

We will show that it is of CM-type. The assertion is true for $r = 1$, since we already know that the Jacobian variety of the Fermat curve is of CM-type. Let us consider the following rational map

$$X_m^r \times X_m^s \dashrightarrow X_m^{r+s},$$

defined by

$$\big([x_0, \ldots, x_{r+1}], [y_0, \ldots, y_{s+1}]\big) \mapsto [z_0, \ldots, z_{r+s+1}],$$

where

$$z_i = x_i y_{s+1}, \quad i = 0, \ldots, r, \quad z_{r+1+j} = \epsilon_{2m} x_{r+1} y_j,\ j = 0, \ldots, s,$$

and $\epsilon_{2m} = e^{\pi i/m}$. It is clear that the map is dominant and its set $Z_m^{r,s}$ of indeterminacy points consists of the product $V(x_{r+1}) \times V(y_{s+1}) \cong X_m^{r-1} \times X_m^{s-1}$. After we blow up $Z_m^{r,s}$, we obtain a morphism $f : Y_m^{r,s} \to X_m^{r+s}$. Let Y_0 (resp. Y_∞) be the proper inverse transform of $X_m^r \times V(y_{s+1}) \cong X_m^r \times X_m^{s-1}$ (resp. $V(x_{r+1}) \times X_m^s \cong X_m^{r-1} \times X_m^s$). The restriction morphism

$$\tilde{f} : U_m^{r,s} := Y_m^{r,s} \setminus (Y_0 \cup Y_\infty) \to X_m^{r+s} \setminus X_m^{r-1} \cup X_m^{s-1}$$

is a finite morphism. It is an étale map outside of the pre-image of the divisor $B = V(z_0^m + \cdots + z_r^m)$.

The group μ_m of mth roots of unity acts on $X_m^r \times X_m^s$ by multiplying the last coordinate in each factor by a root from μ_m. The locus of fixed points is the subvariety $Z_m^{r,s}$. The extended action of μ_m to the blow-up $Y_m^{r,s}$ has the locus of fixed points equal to the smooth exceptional divisor of the blow-up. This implies that the quotient $\tilde{X}_m^{r+s} = Z_m^{r,s}/\mu_m$ is a nonsingular variety. The map

$\tilde{f} : Z_m^{r,s} \to X_m^{r+s}$ factors as the composition of the quotient morphism $p : Z_m^{r,s} \to \tilde{X}_m^{r+s}$ and the blow-up $\phi : \tilde{X}_m^{r+s} \to X_m^{r+s}$ of $f(Y_0 \cup Y_\infty) = X_m^{s-1} \cup X_m^{r-1}$ in X_m^{r+s}.

$$\begin{array}{ccccccc} & & Z_m^{r+s} & \xrightarrow{/\mu_m} & \tilde{X}_m^{r+s} & \hookleftarrow & \mathbb{P}^r \times X_m^{s-1} \cup X_m^{r-1} \times \mathbb{P}^{s-1} \\ & & \downarrow & \overset{\tilde{f}}{\searrow} & \downarrow & & \downarrow \\ X_m^{r-1} \times X_m^{s-1} & \hookrightarrow & X_m^r \times X_m^s & \overset{f}{\dashrightarrow} & X_m^{r+s} & \hookleftarrow & X_m^{s-1} \cup X_m^{r-1} \end{array}$$

For example, take $m = 3, r = s = 1$, so that we have a map $E \times E \dashrightarrow X$ of the self-product of the Fermat plane cubic onto the Fermat cubic surface X_3^2. The open subset $U_m^{r,s}$ is equal to the complement of three fibers E_1, E_2, E_3 and E_1', E_2', E_3' of each projection $E \times E \to E$. The set $Z_3^{1,1}$ is the union of 9 intersection points $p_{ij} = E_i \cap E_j$. The curves E_i, E_j' are blown down to 6 points q_i, q_i' on X_3^2 lying on two lines $\ell : z_0 = z_1 = 0$ and $\ell' : z_2 = z_3 = 0$. The images of the exceptional curves R_{ij} over p_{ij} are the 9 lines on the cubic surface that join a point on one line to a point on another one. The rational map $E \times E$ is given by the linear subsystem $|\sum E_i + \sum E_i' - \sum p_{ij}|$ of curves in the complete linear system $|\sum E_i + \sum E_i'|$ that pass through the points p_{ij}. The inverse transform of this linear system on the blow-up $Y_3^{1,1}$ is the complete linear 3-dimensional system $|\tilde{D}|$ with $\tilde{D}^2 = 9$. It defines a morphism of degree 3 onto the cubic surface X_3^2. The morphism $\tilde{f} : Y_3^{1,1} \to X_3^2$ factors through a finite Galois map $Y_3^{1,1} \to \tilde{X}_3^2$ of degree 3 and the blow-up $\tilde{X}_3^2 \to X_3^2$ of the six points q_i, q_i'. The branch divisor of the first map is the disjoint union of nine smooth rational curves R_{ij} with self-intersection equal to -3. They are the proper inverse transform of the 9 lines $\langle q_i, q_j' \rangle$ on the cubic surface X_3^2 to the blow-up $\tilde{X}_3^2$.

Note that one can show that the existence of 9 lines and 6 points on a cubic surface forming a configuration $(6_3, 9_2)$ characterizes the Fermat cubic surface.

Applying inductively the construction, we obtain a rational map

$$(X_m^1)^r \dashrightarrow X_m^r$$

of the self-product of the Fermat plane curve X_m^1 to the Fermat hypersurface X_m^r.

We have already observed that the Mumford-Tate group of a Hodge substructure is isomorphic to a quotient of the Mumford-Tate group of the Hodge structure. The following lemmas (see [140], Lemma 7.1.4, Lemma 7.1.5) allow us to conclude that the Fermat hypersurface X_m^r is of CM-type.

Lemma 9.14. *Let (V, h) and (V', h') be nonzero rational polarized Hodge structures. Then,* $\mathrm{MT}(V \otimes_{\mathbb{Q}} V', \mathsf{h} \otimes \mathsf{h}')$ *is commutative if and only* $\mathrm{MT}(V, \mathsf{h})$ *and* $\mathrm{MT}(V', \mathsf{h}')$ *are commutative.*

Lemma 9.15. *Let Y be the blow-up of a smooth variety X along a smooth subvariety Z of codimension 2. Then, the Mumford-Tate group of $H^k(Y, \mathbb{Q})$ is commutative if and only if the Mumford-Tate groups of $H^k(X, \mathbb{Q})$ and of $H^{k-2}(Z, \mathbb{Q})$ are commutative.*

From the previous example we know that all Fermat curves $\mathrm{J}(X_m^1)$ are of CM-type (see [93]). Applying this to Katsura-Shioda construction, we obtain that a Fermat hypersurface X_m^n has commutative Mumford-Tate group of $H^n(X_m^n, \mathbb{Q})$ (and hence for all other cohomology since it is a hypersurface).

Remark 9.16. A generalization of a Fermat hypersurface is a *Delsarte hypersurface* defined to be a hypersurface in $\mathbb{P}^{r+1}$ given by a homogeneous polynomial of degree m equal to the sum of $r+2$ monomials $x_0^{a_{j0}} \cdots x_{r+1}^{a_{jr+1}}, j = 0, \ldots, r+1$, such that the matrix $A = (a_{ij})$ is nondegenerate and all its rows add up to m. One also assumes that each columns contains at least one zero entry. An example of a Delsarte surface is a surface

$$x_0 x_1^{m-1} + x_1 x_2^{m-1} + x_2^{m-1} + x_3^m = 0.$$

Let A^* be the adjugate matrix of the matrix A, i.e. $AA^* = \det(A) I_{r+2}$. Let δ be the greatest common divisor of the entries a_{ij}^* of A^*, and $d = \det(A)/\delta$ so that $B = dA^{-1} = \delta^{-1} A^*$ is an integral matrix. One constructs a dominant rational map from the Fermat hypersurface X_d^r to a Delsarte hypersurface of degree d defined by the formulas

$$(x_0, \ldots, x_{r+1}) \to (\prod_{j=0}^{r+1} y_j^{b_{0j}}, \ldots, \prod_{j=0}^{r+1} y_j^{b_{r+1j}}),$$

where $B = (b_{ij})$.

One can use this to prove that Delsarte hypersurfaces are of CM-type. Finally note that one can also consider a weighted homogenous version of a Delsarte hypersurface by giving the weights to the unknowns x_i. They are finitely covered covered by Delsarte polynomials. One uses this method in [107] to prove that some K3 surfaces are of CM-type.

Remark 9.17. One can generalize the constriction from Example 9.13 as follows. Let $F(x_0, \ldots, x_r)$ be a weighted homogeneous polynomial of degree d with weights $q_0, \ldots, q_r$ and $G(y_0, \ldots, y_s)$ be a weighted homogeneous polynomial of degree m with weightes $q_0', \ldots, q_s'$. Consider the hypersurfaces $X = V(F + x_{r+1}^m), Y = V(G + y_{s+1}^m)$ and $Z = V(F(z_0, \ldots, z_r) + G(z_{r+1}, \ldots, z_{r+s}))$ in the weighted projective spaces $\mathbb{P}(q_0, \ldots, q_r, 1), \mathbb{P}(q_0', \ldots, q_s', 1)$ and $\mathbb{P}(q_0, \ldots, q_r, q_{r+1}', \ldots, q_{r+s+1}')$, respectively. Then, the rational map

$$X \times Y \dashrightarrow Z,$$

given by the same formula as in Example 9.13 is a dominant map of finite degree defined over the complement of $V(x_{r+1}) \times V(y_{s+1}$. In particular, any smooth surface of degree m in $\mathbb{P}^3$ defined by an equation $f(x, y) + g(z, w) = 0$ can be finitely rationally covered by the product of two smooth plane curves of degree m.

Example 9.18 ([176])**.** Let X be an algebraic K3 surface. Let $\mathrm{Hdg}(X)$ and $\mathrm{MT}(X)$ be the Hodge group and the Mumford-Tate group of the rational Hodge structure on $\mathrm{H}^2(X, \mathbb{Q})$. It fixes algebraic cycles and preserves the intersection form on the lattice of transcendental cycles T_X, hence

$$\mathrm{Hdg}(X) \subset \mathrm{SO}(T_{X,\mathbb{Q}}).$$

Let C be the *Weil operator* on $T_{X,\mathbb{R}}$, it acts as -1 on $\{(x, \bar{x}) \in H^{2,0}(X) \oplus H^{0,2}(X)\}$ and as 1 on $H^{1,1}(X) \cap T_{X,\mathbb{R}}$. Thus, the form $(x, y) \mapsto \langle x, Cy \rangle$ is a positive definite symmetric form on $T_{X,\mathbb{R}}$. This defines a polarized rational Hodge structure on $T_{X,\mathbb{Q}}$. This implies that $\mathrm{MT}(X)$ and $\mathrm{Hdg}(X)$ are reductive algebraic groups over $\mathbb{Q}$. Consider $V = T_{X,\mathbb{Q}}$ as a linear $\mathbb{Q}$-representation of $\mathrm{Hdg}(X)$. Then, it is an irreducible representation (it is true for any surface with $p_g = 1$) ([176], Theorem 1.4.1). Let

$$E_X = \mathrm{End}_{\mathrm{Hdg}(X)}(V).$$

Since V is a simple $\mathrm{Hdg}(X)$-module, E_X is a division algebra. In fact, it is a commutative field, a totally real field or an imaginary quadratic extension of a totally real field E_0. To show that it is commutative one considers a natural non-trivial homomorphism $E_X \to \mathrm{End}(H^{2,0}(X))$. Since it sends 1 to 1, it an injective homomorphism, hence E_X is commutative. The assertion about the structure of the field E_X follows from the existence of a positive anti-involution $x \mapsto x'$ on E_X defined by the taking the adjoint operator with respect to the bilinar form $\langle x, y\rangle = (x, Cy)_X$.

For any $x, y \in E_X$, consider the linear function $E_X \to \mathbb{Q}$ defined by $e \mapsto (ex, y)_X$. Since the bilinear form $(a, b) \mapsto \mathrm{tr}_{E_X/\mathbb{Q}}(ab)$ is non-degenerate, there exists $\alpha_{x,y} \in E_X$ such that $(ex, y) = \mathrm{tr}_{E_X/\mathbb{Q}}(e\alpha_{x,y})$. Define a bilinear form by setting

$$\Phi : V \times V \to E_X, \quad (x, y) \mapsto \alpha_{x,y}.$$

Since $(ex, y)_X = (x, e'y)_X = (e'y, x)_X$, we obtain that $\Phi(x, y) = \Phi(y, x)'$. Also, it is easy to see that $\Phi(ex, y) = e\Phi(x, y)$. In particular, if E_X is a totally real field (resp. a CM-field), then Φ is a symmetric (resp. Hermitian) bilinear form on the E_X-vector space V. Since Hdg_X commutes with E and preserves the intersection form on X, we see that Hdg_X preserves Φ.

The main result of [176] is the following.

$$\mathrm{Hdg}_X = \mathrm{SO}(T_{X,\mathbb{Q}}, \Phi),$$

if E_X is a totally real field, and

$$\mathrm{Hdg}_X = \mathrm{U}(T_{X,\mathbb{Q}}, \Phi),$$

otherwise. In the former (resp. the latter case) the dimension of the Hodge group is equal to $\frac{t_X^2 - t_X}{2}$ (resp. $\frac{t_X}{4}$, where $t_X = \mathrm{rank} T_X = 22 - \rho(X)$.

For example, when $E_X = \mathbb{Q}$, $\mathrm{Hdg}_X \cong \mathrm{SO}(T_{X,\mathbb{Q}})$.

9.4 Abelian Varieties of CM-Type

We have already discussed elliptic curves with complex multiplication. In this section, as promised, we extend it to higher dimension.

Let us start with an example. Suppose A admits an automorphism g of order m. Let $\Phi_m(x)$ be the cyclotomic polynomial, a minimal polynomial of the cyclotomic field $\mathbb{Q}(\zeta_m)$. Then,

$$\mathbb{Q}(\zeta_m) \cong \mathbb{Q}[x]/(\Phi_m(x)) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A), \quad x \mapsto g.$$

The Galois group of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is isomorphic to the group of invertible elements in the ring $\mathbb{Z}/m\mathbb{Z}$ and its order is equal to the value $\phi(m)$ of the Euler function. Let $m = p$ be an odd prime, the field $\mathbb{Q}(\zeta_{p^k})$ is a cyclic extension of $\mathbb{Q}$. It is a quadratic extension of a totally real subfield $\mathbb{Q}(\eta), \eta = \zeta_{p^k} + \zeta_{p^{-k}}$, by a complex number ζ_{p^k}. If $p = 2$ and $k > 2$, then $\mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}(\eta, \sqrt{-1})$ and the Galois group is the direct product of two cyclic groups of orders 2^{k-2} and 2.

A cyclotomic field is an example of a CM-*field*, an imaginary quadratic extension K of a totally real field K_0. This means that $K = K_0(\alpha)$, where $\rho(\alpha^2) < 0$ for all embeddings $\rho : K \hookrightarrow$

$\mathbb{C}$. Equivalently, a CM-field K can be characterized by the property that there exists a non-trivial automorphism ι of K (called the *conjugation*) that commutes with any embedding $\rho : K \hookrightarrow \mathbb{C}$. The Galois closure of a CM-field in any larger field is known to be a CM-field.

Recall that in Chapter 3 we have defined an abelian variety of CM-type by the property

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

Suppose A is a simple abelian variety of CM-type. Then, $R = \mathrm{End}_{\mathbb{Q}}(A)$ is a division algebra and its center is of degree e over $\mathbb{Q}$, hence $[R : \mathbb{Q}]_{\mathrm{red}} = en = 2 \dim A$ for some n. We use the classification of possible types of R from Section 2.5. If R is of type II or III, then $2e$ must divide $\dim A$, and this obviously impossible in our case. If R is of type I, then R is a totally real field with $e|g$. Since $n = 1$ in this is again impossible. This leaves us with type IV, and its definition shows that R is a CM-field with K_0 to be a totally real field of degree $e_0 = \dim A$ over $\mathbb{Q}$.

One defines a CM-*algebra* to be a finite product of CM-fields. A not necessary simple, abelian variety A is of CM-type if it is isogenous to a product of simple abelian varieties of CM-type, hence $\mathrm{End}_{\mathbb{Q}}(A)$ contains a CM-algebra of dimension $2 \dim A$, but necessary coincides with it.

We say that a simple abelian variety has a *complex multiplication* if its endomorphism ring $\mathrm{End}_{\mathbb{Q}}(A)$ is of the fourth type, i.e the Rosati involution acts non-trivially on the center of K. In this case $e = 2e_0$ and $e_0 d^2 | g$. If, additionally, $e_0 = g$, then A is of CM-type. Obviously, abelian varieties of CM-type admit real multiplication by a field of degree g. In particular, in the case $g = 2$, their isomorphism classes are points in the Humbert surface.

Example 9.19. Suppose a simple abelian variety A admits an automorphism of prime order $p > 2$. Then, $e_0 \leq g$, hence the degree $\frac{1}{2}(p-1)$ of the real subfield of $\mathbb{Q}(\zeta_p)$ is less than or equal to g, hence $p \leq 2g + 1$. For example, a simple abelian surface does not have automorphisms of prime order > 5. An example of an abelian variety of dimension g admitting an automorphism of order $p = 2g + 1$ is the Jacobian of the hyperelliptic curve

$$C_p : y^2 = x^p - 1. \tag{9.8}$$

The Jacobian of the curve C_5 defines one of the 19 isomorphism classes of principally polarized abelian surfaces of CM-type defined over $\mathbb{Q}$ (see [130], [173]). The corresponding CM-fields are

$$\mathbb{Q}(\sqrt{-(2+\sqrt{2})}),\ \mathbb{Q}(\sqrt{-(5+2\sqrt{5})}),\ \mathbb{Q}(\sqrt{-(13+2\sqrt{13})}),\ \mathbb{Q}(\sqrt{-(29+2\sqrt{29})}),$$
$$\mathbb{Q}(\sqrt{-(37+6\sqrt{37})}),\ \mathbb{Q}(\sqrt{-(53+2\sqrt{53})}),\ \mathbb{Q}(\sqrt{-(61+6\sqrt{61})}),\ \mathbb{Q}(\sqrt{-5(2+\sqrt{2})}),$$
$$\mathbb{Q}(\sqrt{-(5+\sqrt{5})}),\ \mathbb{Q}(\sqrt{-13(5+2\sqrt{5})}),\ \mathbb{Q}(\sqrt{-17(5+2\sqrt{5})}),\ \mathbb{Q}(\sqrt{-(13+3\sqrt{13})}),$$
$$\mathbb{Q}(\sqrt{-5(13+2\sqrt{13})}).$$

The field $\mathbb{Q}(\sqrt{-(5+2\sqrt{5})})$ is equal to $\mathbb{Q}(\zeta_5)$ and corresponds to the curve C_5. Note that the Shioda-Inose K3 surface associated to this curve admits a non-symplectic automorphism of order 5. The surface admits an elliptic fibration with two reducible fibers of types $\tilde{E}_8$ and $\tilde{E}_7$ with Weierstrass equation

$$y^2 = x^3 + t^3 x - t^7 = 0$$

[94]. Note that the rank of the Mordell-Weil group of this fibration is equal to 1 (and not 0 as was in the case of Example 6.2). The surface can be also given by the following equation in the weighted projective space $\mathbb{P}(5,7,8,20)$

$$x^8 + xy^5 + z^5 + w^2 = 0.$$

The group of order 5 acts by $(x,y,z,w) \mapsto (x,y,\zeta_5 z,w)$. The Picard lattice is isomorphic to $E_8^{\oplus 2} \oplus \left(\begin{smallmatrix} -2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$ (see [10], [107]). Finally, note that the isomorphism class of the associated abelian surface belongs to the Humbert surface $\mathrm{Hum}(5)$.

More generally, for any prime p and $0 < a < p$, the Jacobian of the normalization of the curve

$$y^p = x^a(x^{p^{e-1}} - 1), \tag{9.9}$$

is a simple abelian variety of dimension $p^{e-1}(p-1)/2$ with complex multiplication by $\mathbb{Q}(\zeta_{p^e})$ [2].

Another series of examples of simple abelian varieties with automorphisms of prime (odd) order p is provided by the following construction. Let K be a subfield of $\mathbb{C}$, let $n \geq 5$ an integer, and $f(x) \in K[x]$ a degree n irreducible polynomial over K, whose Galois group over K is either $\mathfrak{S}_n$ or $\mathfrak{A}_n$. Let $J_{f,p}$ be the jacobian of the normalization of the curve

$$y^p = f(x).$$

Then, $J_{f,p}$ is a simple abelian variety, whose endomorphism ring is the pth cyclotomic ring $\mathbb{Z}[\zeta_p]$ [179, 182] and therefore its automorphism group is a cyclic group of order $2p$. (The proof is based on Theorem 2.21 applied to $\ell = p$ and $\mathfrak{R}$= the n-element set of roots of $f(x)$.) As for $\dim(J_{f,p})$, it equals $(n-1)(p-1)/2$ if p does *not* divide n and $(n-2)(p-1)/2$ if it does.

Let R be a CM-algebra and $\iota : R \to R$ be an automorphism that induces the conjugation on each CM-field component. The set of $\mathbb{Q}$-homomorphisms a CM-algebra R to $\mathbb{C}$ consists of pairs $(\rho, \iota \circ \rho)$. A choice of one element in each pair gives a set Φ of homomorphisms and the pair (R,Φ) is called a CM-*type* of R. One can construct an abelian variety of CM-type as follows. Let (R,Φ) be a CM-type. Choose a lattice L in R, i.e. a free $\mathbb{Z}$-submodule of R of rank equal to $[R:\mathbb{Q}]$. Let $\mathfrak{o} = \{x \in R : x \cdot L \subset L\}$. This is an order in R. We have a natural pairing

$$R \times \Phi \to \mathbb{C},\ (r,\rho) \mapsto \rho(r).$$

It defines an isomorphism

$$R_{\mathbb{R}} \to \mathbb{C}^{\Phi} \cong \mathbb{C}^{\frac{1}{2}[R:\mathbb{Q}]}.$$

The image of L is a lattice Λ in $\mathbb{C}^{\Phi}$, we set $A = \mathbb{C}^{\Phi}/\Lambda$. Let $\mathfrak{o} = \{x \in R : x \cdot L \subset LK\}$. This is an order in R, and $\mathfrak{o} \subset \mathrm{End}(A)$ so that $R \subset \mathrm{End}_{\mathbb{Q}}(A)$. To define a polarization we consider the following bilinear form on R

$$E : R \times R \to \mathbb{Q}, \quad (x,y) \mapsto \mathrm{Tr}_{R/\mathbb{Q}}(\alpha x \bar{y}),$$

where $\alpha \in R^*$ satisfies

(i) $\bar{\alpha} = -\alpha$,

(ii) $\mathrm{Im}(\rho(\alpha) > 0$ for all $\rho \in \Phi$.

One can always find such α. It follows from (i) that E is a skew-symmetric bilinear form. Also it implies

$$E(x,y) = \sum_{\rho\in\Phi} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\rho(\alpha x\bar{y})) = \rho(\alpha)(x\bar{y} - \bar{x}y),$$

hence,

$$E(\mathbf{i}x, \mathbf{i}y) = \sum_{\rho\in\Phi} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\rho(\alpha i x\bar{\mathbf{i}}\bar{y})) = E(x,y),$$

and, using (i) and (ii),

$$E(\mathbf{i}x, y) = \sum_{\rho\in\Phi} \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\rho(\alpha \mathbf{i} x\bar{y})) = \mathbf{i}\rho(\alpha)(x\bar{y} + \bar{x}y) > 0,$$

Thus, E defines a polarization on A. Its type is equal to the discriminant of the bilinear form E restricted to the lattice L.

Abelian varieties of CM-type do not vary in families. They are isolated points in $\mathcal{A}_{g,n}$. However, less restrictive condition that the endomorphism algebra is of type IV, allows one to construct the moduli space. We refer to [106], Chapter 9 for the general theory. Note that in this case the Hermitian symmetric spaces of unitary type appear.

Proposition 9.20. *An abelian variety A is of* CM*–type if and only if the Mumford-Tate group of the Hodge structure on $V = \mathrm{H}^1(A, \mathbb{Q})$ is commutative (hence isomorphic to $\mathbb{G}_m^r$ over $\mathbb{C}$).*

Proof. Suppose A is of CM-type. Let R be the CM-algebra acting on V. Its center is a $\mathbb{Q}$-subalgebra K of dimension $2\dim A = \dim V$, so that V is a vector space of dimension 1 over K. The action of $K \otimes_{\mathbb{Q}} \mathbb{R}$ on V commutes with the complex structure, hence $\mathbb{C}$ is contained in the centralizer of $K \otimes_{\mathbb{Q}} \mathbb{R}$ in $\mathrm{End}_{\mathbb{R}}(V)$ and hence coincides with it. This shows that the Mumford-Tate group is a subgroup of the torus $\mathbb{C}^*$ considered as an algebraic group $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_{m,K}$ over $\mathbb{Q}$.

Conversely, assume that $\mathrm{MT}(V) \subset \mathrm{GL}(V)$ is a torus T. Let R be the subalgebra of $\mathrm{End}_{\mathbb{Q}}(V)$ of endomorphisms that are endomorphisms of the $\mathrm{MT}(V)$-module V. Since $\mathrm{MT}(V)$ contains $\mathbb{C}^* = \mathbb{S}(\mathbb{R})$ that acts on V by $v \mapsto zv, z \in \mathbb{C}^*$, we see that R is isomorphic to a sublalgebra of $\mathrm{End}_{\mathbb{Q}}(A)$. Since $G = \mathrm{MT}(V)$ is a diagonalizable commutative algebraic group, we have $[R : \mathbb{Q}]_{\mathrm{red}} = \dim_{\mathbb{Q}} V$. In fact, we have decomposition of V into eigenspaces $V = \oplus_{\chi\in\mathcal{X}(G)} V_\chi$, hence $R = \prod_\chi \mathrm{End}_{\mathbb{Q}}(V_\chi)$. This implies that the reduced degree of R over $\mathbb{Q}$ is equal to $\sum_\chi \dim_{\mathbb{Q}} V_\chi = \dim_{\mathbb{Q}} V$. Thus, $\mathrm{End}_{\mathbb{Q}}(A)$ contains a central algebra of reduced degree equal to $\dim A$. This algebra is a CM-algebra, and hence A is of CM-type. □

Chapter 10

Endomorphisms of Jacobian Varieties

In this chapter, we will discuss the endomorphism algebra of the Jacobian variety of an algebraic curve C of genus $g > 1$. In particular, we introduce some tools that help to decide whether C is general in the sense that $\mathrm{End}(\mathrm{J}(C)) \cong \mathbb{Z}$.

10.1 Correspondences on a Smooth Projective Algebraic Curve

Let C be a nonsingular projective curve of genus $g > 1$. We are interested in a question when $\mathrm{End}(\mathrm{J}(C)) \neq \mathbb{Z}$. Of course, easy examples are curves admitting a non-trivial group of automorphisms or admitting a degree d cover to a curve of lower genus $g' > 0$. In the latter case, the Jacobia variety is not simple. We also saw in the previous chapters many examples of curves of genus 2 with real or complex multiplication with simple Jacobian.

Let L be a line bundle on the product $C \times C$. For any point $x \in C$, let $L(x) = i_x^*(L) \in \mathrm{Pic}(C)$, where $i_x : C \to C \times C$ be the closed embedding map $c \mapsto (x, c)$. We will prefer to switch from line bundles. Extending this map by linearity, we obtain a homomorphism

$$u_L : \mathrm{J}(C) \to \mathrm{J}(C),$$

where $\mathrm{J}(C)$ is identified, via the Abel-Jacobi map, with the group of divisor classes of degree 0 on C. Let T be the subgroup of $\mathrm{Pic}(C \times C)$ generated by line bundles of the form $p_1^*(M), p_2^*(M)$, where $p_i : C \times C \to C$ are the two projections. It is easy to see that $u_L = 0$ for any $L \in T$. Applying the Seesaw Theorem ([41], Appendix), one shows that any L with $u_L = 0$ belongs to T.

Thus, we obtain an injective homomorphism of abelian groups

$$\mathfrak{u} : \mathrm{Corr}(C) := \mathrm{NS}(C \times C)/T \to \mathrm{End}(\mathrm{J}(C)), \quad L \mapsto u_L.$$

An element of the group $\mathrm{Corr}(C)$ is called a *correspondence* on C.

Remark 10.1. One can interpret this homomorphism as follows. First, via the inclusion $C \hookrightarrow \mathrm{J}(C)$ we identify $\mathrm{H}^1(C, \mathbb{Z})$ with $\mathrm{H}^1(\mathrm{J}(C), \mathbb{Z})$. This is compatible with the Hodge structures on $\mathrm{H}^1(C, \mathbb{C})$

and $\mathrm{H}^1(\mathrm{J}(C),\mathbb{C})$. Using the principal polarization, we can identify $\mathrm{J}(C)$ with the dual abelian variety $H^{0,1}(C,\mathbb{C})/\mathrm{H}^1(C,\mathbb{Z})$. The Küneth Formula and the Poicaré Duality, give a homomorphism

$$\mathrm{H}^2(C\times C,\mathbb{Z})\cong \mathrm{H}^1(C,\mathbb{Z})\otimes H^1(C,\mathbb{Z})\cong \mathrm{End}(\mathrm{H}_1(C,\mathbb{Z}))$$

Using the Hodge decomposition, we obtain a map

$$\mathrm{NS}(C\times C)=H^{1,1}(C)\cap \mathrm{H}^2(C\times C,\mathbb{Z})\to H^{1,0}(C)\otimes H^{0,1}(C)\cong \mathrm{End}(H^{0,1}(C)).$$

This defines a rational and algebraic representation of the endomorphism ϕ_L, where $c_1(L)\in H^{1,1}(C\times C)\cap \mathrm{H}^2(C\times C,\mathbb{Z})$.

Let us use divisor classes on $C\times C$ instead of line bundles, so, for example, we write u_D instead of u_L. Since the sum F_1+F_2 of two fibers of the projections $C\times C\to C$ is an ample divisor on the surface $C\times C$, adding some multiple of it, we may assume that a correspondence is represented by an effective divisor. Also, replacing some positive multiple D by a linearly equivalent divisor, we may assume that a correspondence is represented by a divisor of the form $\frac{1}{r}Z$, where Z is an irreducible curve. One may consider Z as a map $C\to C^{(d_1)}, x\mapsto Z\cap\{x\}\times C$, where d_1 is the degree of the projection $p_1: Z\to C$. Similarly, Z defines a map $C\to C^{(d_2)}, x\mapsto Z\cap C\times\{x\}$, where d_2 is the degree of the projection $p_2: Z\to C$. The switch of the factors automorphism $C\times C\to C\times C$ is an involution $D\to D'$ on $\mathrm{Corr}(C)$. Note that the numbers (d_1,d_2) can be defined for any divisor class on $C\times C$, but are not well-defined for correspondences. However, the following number

$$t(D)=d_1+d_2-(D,\Delta), \tag{10.1}$$

where Δ is the diagonal, is a well-defined linear function on $\mathrm{Corr}(C)$. We have

$$t(D)=\mathrm{tr}((u_D)_r).$$

To prove this, we apply the Lefschetz fixed-point formula for correspondences (see [57], Example 16.1.15) that gives

$$(D,\Delta)=\mathrm{tr}(u_D^*|H^0(C,\mathbb{Q}))+\mathrm{tr}(u_D^*|\mathrm{H}^2(C,\mathbb{Q}))-\mathrm{tr}(u_D^*|\mathrm{H}^1(C,\mathbb{Q})).$$

It is easy to see that $d_1=\mathrm{tr}(u_D^*|H^0(C,\mathbb{Q})), d_2=\mathrm{tr}(u_D^*|\mathrm{H}^2(C,\mathbb{Q}))$ and $\mathrm{tr}(u_D^*|\mathrm{H}^1(C,\mathbb{Q}))=\mathrm{tr}(u_D^*|\mathrm{H}^1(\mathrm{J}(C),\mathbb{Q}))=\mathrm{tr}((u_D))_r)$.

One defines the inverse of the map $\mathfrak{u}$ as follows. Recall that $\mathrm{J}(C)$ comes with a natural principal polarization defined by the class in $\mathrm{NS}(\mathrm{J}(C))$ of a *theta divisor* Θ, the image of the symmetric product $C^{(g-1)}$ in $\mathrm{J}(C)$ under the Abel-Jacobi map. As a divisor this image depends on a choice of points $(p_1,\dots,p_{g-1})$ on C. One can always choose a theta divisor Θ to be symmetric, i.e. satisfy $[-1]^*_{\mathrm{J}(C)}(\Theta)=\Theta$. It is still not defined uniquely. One can show that there exists a divisor class ϑ of degree $g-1$ satisfying $2\vartheta=K_C$ (a *theta characteristic*) such that

$$\Theta+\vartheta:=\{\vartheta+D, D\in \mathrm{J}(C)\}=\{\text{effective divisor classes on } C \text{ of degree } g-1\}.$$

Fix a symmetric theta divisor Θ and embedding $\iota_c: C\hookrightarrow \mathrm{J}(C)$ via the Abel-Jacobi map defined by a choice of a point $c\in C$. For any $u\in\mathrm{End}(\mathrm{J}(C))$, consider the map

$$d_u: C\times C\to \mathrm{J}(C),\quad (x,y)\mapsto u(\iota_c(x))-\iota_c(y),$$

and define

$$\beta(u) = d_u^*(\Theta) \mod T.$$

In other terms, let $\Theta_u = \{(a,b) \in \mathrm{J}(C) \times \mathrm{J}(C) : u(a) - b \in \Theta\}$, then $\beta(u) = (\iota_c \times \iota_c)^*(\Theta_u)$. It is clear that choosing different c, replaces the image of $C \times C$ in $\mathrm{J}(C) \times \mathrm{J}(C)$ by a translate by some point in the abelian variety $\mathrm{J}(C) \times \mathrm{J}(C)$, hence replaces $\beta(u)$ by an algebraically equivalent divisor on $C \times C$.

We refer to [106, Chapter 11, §5], for the proof of the fact that β is the inverse of $\mathfrak{u}$ making an isomorphism

$$\mathfrak{u} : \mathrm{Corr}(C) \cong \mathrm{End}(\mathrm{J}(C)). \tag{10.2}$$

Note that β gives a natural section of $\mathrm{NS}(C \times C) \to \mathrm{Corr}(C)$, we can call the corresponding divisor class $\beta(u) \in \mathrm{NS}(C \times C)$ a *canonical correspondence* associated to u. Fixing ϑ and a point $c \in C$, we can even choose a representative of $\beta(u)$ in $\mathrm{Div}(C \times C)$. Note that

$$d_1(\beta(u)) = (C, \Theta), \quad d_2(\beta(u)) = (u(C), \Theta).$$

It is known that $(C, \Theta) = g$ [106, 11.2.2].

In fact, the isomorphism (10.2) is an isomorphism of rings, where the ring structure is defined by the composition of correspondences

$$D \lozenge D' = (p_{13})_*(p_{12}^*(D) \cdot p_{23}^*),$$

where $p_{ij} : C \times C \times C \to C \times C$ are the natural projections. One easily checks that the multiplication law is well-defined on $\mathrm{Corr}(C)$. The homomorphism $\mathfrak{u}$ becomes an isomorphism of rings.

Next we define a symmetric bilinear form on $\mathrm{Corr}(C)$ by setting

$$\sigma(D, D') = d_1 d_2' + d_1' d_2 - (D, D').$$

Obviously, the radical of the form contains the subgroup of divisors algebraically equivalent to zero. It also contains the subgroup T. Thus, it defines a symmetric bilinear form on the group $\mathrm{Corr}(C)$. The *Castelnuovo inequality* asserts that the corresponding quadratic form

$$\sigma(D) := \sigma(D, D) = 2d_1 d_2 - (D, D) \tag{10.3}$$

is positive definite. An exercise in [65, p. 368] sketches a proof.

Note that our trace function (10.1) can be expressed in terms of the symmetric form σ

$$t(D) = \sigma(D, \Delta).$$

Let $D \to D'$ be the involution on $\mathrm{Corr}(C)$ defined by the switch of the factors of $C \times C$. Under the isomorphism (10.2), it corresponds to the Rosati involution $f \mapsto f'$ [106], 11.5.3. Considering effective correspondences D_1, D_2 as multi-valued maps $C \to C$, one checks that

$$d_1(D_1 \lozenge D_2') = n_1(D_1) n_2(D_2),\ n_2(D_1 \lozenge D_2') = n_2(D_1) n_1(D_2),\ (D_1, D_2) = (D_1 \lozenge D_2', \Delta).$$

(cf. [57], Chapter 16, Examples 16.3.3 and 16.3.4). This implies that

$$\sigma(D_1, D_2) = n_1(D_1 \lozenge D_2') + n_2(D_1 \lozenge D_2') - (D_1 \lozenge D_2', \Delta) = \mathrm{tr}(\alpha(D_1 \lozenge D_2')).$$

Thus, the symmetric bilinear form $\sigma(D_1, D_2)$ coincides, under the isomorphism α, with the symmetric form $\mathrm{tr}(f\phi')$ on $\mathrm{End}(\mathrm{J}(C))$.

It is known that, under the isomorphism $\mathfrak{u}$, the symmetric form becomes the symmetric form $\mathrm{Tr}(\phi\psi')$ defined by the Rosati involution. Note that, taking D to be the diagonal Δ in $C \times C$, we obtain that $\sigma(D) = 2 - (2 - 2g) = 2g$ and $\phi(\Delta) = \mathrm{id}_{\mathrm{J}(C)}$, so the formulas agree.

Note, that, applying the adjunction formula, we have $D^2 = 2p_a(D) - 2 - (2g - 2)(d_1 + d_2)$, so we may rewrite (10.3) in the form

$$\sigma(D) = 2d_1d_2 + (2g - 2)(d_1 + d_2) - 2p_a(D) + 2. \tag{10.4}$$

A correspondence $D \in \mathrm{Corr}(C)$ such that $u_D = [-\nu]_{\mathrm{J}(C)}$ is called a correspondence with *valence* ν. In this case, it can be represented by a curve Z in $C \times C$ with the class $[C]$ in $\mathrm{H}^2(C \times C, \mathbb{Z})$ equal to

$$(d_1 + \nu)[C \times \{x\}] + (d_2 + \nu)[\{x\} \times C] - \nu[\Delta]$$

So, $\mathrm{End}(\mathrm{J}(C)) \neq \mathbb{Z}$ if and only if C admits a correspondence without valence. Many classical enumerative problems are solved by constructing correspondence with valence and applying the *Brill-Noether formula* that expresses the valence in terms of the number (D, Δ) of *united points* of the correspondence.

$$(D, \Delta) = d_1d_2 - 2\nu g,$$

where g is the genus of C (see [41], Corollary 5.5.2).

A correspondence D is called *symmetric* if $D' = D$. It follows from above that the subgroup $\mathrm{Corr}(C)^s$ of symmetric correspondences is isomorphic to the group of symmetric endomorphisms of $\mathrm{J}(C)$, and hence to the Néron-Severi group $\mathrm{NS}(\mathrm{J}(C))$. Note that a canonical representative $D = \beta(u)$ of a symmetric endomorphism u must satisfy $d_1 = d_2 = g$, hence $(D, \Delta) = 2g - t(D) = 2g - \mathrm{tr}(u_r)$.

An example of a symmetric correspondence with valence -1 on a curve of genus g is the *Scorza correspondence* R_θ with $d_1 = d_2 = (g, g)$ defined by a choice of a non-effective theta characteristic ϑ (see [41], 5.5). It is equal

$$\beta_\theta(\mathrm{id}_{\mathrm{J}(C)}) = \{(x, y) \in C \times C : x - y \in \Theta_\theta\}.$$

Note that it does not depend on a choice of an embedding of C in $\mathrm{J}(C)$.

Example 10.2. Let $f : C \to C'$ be a finite map of curves. It defines a correspondence

$$\Gamma(f) = C \times_X C = \{(x, y) : f(x) = f(y)\}.$$

It follows from the definition that $\mathfrak{u}(\Gamma(f))$ maps a divisor class $d = \sum x_i \in \mathrm{Pic}(C)^0$ to the divisor class $\sum f^*(f(x_i)) \in \mathrm{Pic}^0(C)$. Obviously, it is equal to $f^*(\mathrm{Nm}(d))$, where $\mathrm{Nm} : \mathrm{J}(C) \to \mathrm{J}(C')$ is the norm map and $f^* : \mathrm{J}(C) \to \mathrm{J}(C')$ is the pull-back map. Since the norm map is surjective, we obtain that the image of the endomorphism $u = \phi(\Gamma(f))$ is equal to $f^*(\mathrm{J}(C'))$. Thus, if $g(C') > 0$, the endomorphism u coincides with the norm map of the abelian subvariety $f^*(\mathrm{J}(C'))$ of $\mathrm{J}(C)$.

Example 10.3. Let $f : C \to C$ be an automorphism of C and $D = \Gamma_f$ be its graph. Then, $d_1(D) = d_2(D) = 1$ and $p_a(D) = g$. Applying (10.4), we get $\sigma(\Gamma_f) = \sigma(\Delta) = 2-(2-2g) = 2g$. Let $\nu = (\Gamma_f, \Delta)$ be the number of fixed points of f. Thus, $\sigma(\Gamma_f, \Delta) = 2 - (\Gamma_f, \Delta) = 2 - \nu$. Since the quadratic form σ is positive definite, we have

$$\sigma(\Gamma_f)\sigma(\Delta) - \sigma(\Gamma_f, \Delta)^2 = 4g^2 - (2-\nu)^2 = (2g-2+\nu)(2g+2-\nu) > 0,$$

unless $\Gamma_f = m\Delta$ in $\mathrm{Corr}(C)$. If $g = 1$, the inequality holds only if $\nu = 0$ or $\nu = 4$, i.e. f is a translation by a point or the quotient by (f) is $\mathbb{P}^1$. If $g > 1$, the latter happens only if $\nu = 2g + 2$. Since the eigenvalues of $f^* : \mathrm{H}^1(C, \mathbb{C}) \to \mathrm{H}^1(C, \mathbb{C})$ are roots of unity, we have $|\mathrm{tr}(f^*)| \le 2g$. The Lefschetz fixed-point formula gives us that $\nu = 2 - \mathrm{tr}(f^*) \le 2 + 2g$ with the equality taking place if and only if $f^* = -\mathrm{id}$. This happens only if f is an involution with quotient isomorphic to $\mathbb{P}^1$, hence C is a hyperelliptic curve and f is its hyperelliptic involution.

Observe that the graph of an automorphism f is symmetric if and only if $f = f^{-1}$, i.e. f is an involution. Thus, if f is of order > 2, the corresponding automorphism of $\mathrm{J}(C)$ is not symmetric. For example, it can never define a real multiplication of $\mathrm{J}(C)$.

Example 10.4 (I. Shimada [160])**.** Let $f : C \to C'$ be a finite cover of curves and let G be its Galois group. The Galois theory of finite covers provides us with a finite map $\phi : X \to C$ such that the composition $f \circ \phi : X \to C'$ is a Galois cover with the Galois group G and $C \cong X/H$ for some subgroup H of C. We assume that H is not a normal subgroup, or, equivalently, the cover f is not a Galois cover. Let $g \in G$ be such that $H' = gHg^{-1} \ne H$. Then, the map $g : X \to X$ induces an isomorphism $\alpha_g : C = X/H \to X/H'$, hence defines a map $(\phi, \alpha_g) : X \to C \times C$. Let S be the correspondence defined by the image of this map. It consists of points $(\phi(x), \phi(g(x)), x \in X$. The curve S is birationally isomorphic to X, it is isomorphic to X if no element of the double coset HgH has a fixed point on X. We have $d_1(S) = d_2(S) = d = [H : H' \cap H]$ and S is symmetric if and only if g is an involution.

We have

$$(S, \Delta) = \sum_{h \in H} X^{hg},$$

where X^{hg} denotes the set of fixed points of hg. Thus

$$t(u_S) = 2d - (S, \Delta) = 2[H : H' \cap H] - \sum_{h \in H} X^{hg}. \tag{10.5}$$

suppose $u_S = [m]_{\mathrm{J}(C)}$ for some $m \in \mathbb{Z}$. Then, $t(u_S) = 2gm$, so we can construct a correspondence without valence if the right-hand side of (10.5) is not a multiple of $2g$. For example, suppose f is an unramified cover, so that its Galois closure is unramified too. Then, H acts without fixed points. Hence, if $\#H < 2g$, we obtain $0 < t(u_S) < 2g$, so we get a non-trivial endomorphism.

In the case $C' = \mathbb{P}^1$, Shimada gives another criterion when u_S has no valence:the Galois group acts 2-transitively on fibers of $C \to C'$.

10.2 Hyperelliptic Jacobians

The aim of this section is to construct explicitly a plenty of hyperelliptic curves C of genus $g > 1$, whose jacobian $\mathrm{J}(C)$ has endomorphism ring $\mathrm{End}(\mathrm{J}(C)) = \mathbb{Z}$. The idea is to look for curves defined over a field K such that the Galois module $\mathrm{J}(C)[2]$ is very simple and apply Theorem 2.15.

Let K be a finitely generated subfield of $\mathbb{C}$ and $f(x) \in K[x]$ be a degree $n = 2g + 1$ monic polynomial without repeated roots. We write $\mathfrak{R}_f$ for the n-element set of roots of $f(x)$ in $\bar{K}$. We have

$$f(x) = \prod_{\alpha \in \mathfrak{R}_f} (x - \alpha) \in \bar{K}[x] \subset \mathbb{C}[x].$$

We write $K(\mathfrak{R}_f)$ for the subfield of $\bar{K}$ obtained by adjoining to K all elements of $\mathfrak{R}_f$. By definition, $K(\mathfrak{R}_f)$ is the splitting field of $f(x)$, which is a finite Galois extension of K, and

$$\mathfrak{R}_f \subset K(\mathfrak{R}_f) \subset \bar{K} \subset \mathbb{C}.$$

The Galois group $\mathrm{Gal}(f/K)$ of $f(x)$ over K is the Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K)$ of the field extension $K(\mathfrak{R}_f)/K$. Since $f(x)$ has coefficients in K, the Galois group $\mathrm{Gal}(K(\mathfrak{R}_f)/K$ permutes elements of $\mathfrak{R}_f$, which gives rise to the group embedding

$$\mathrm{Gal}(f/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f) \cong \mathfrak{S}_n$$

where $\mathrm{Perm}(\mathfrak{R}_f)$ is the group of all permutations of the n-element set $\mathfrak{R}_f$ and $\mathfrak{S}_n$ is the group of permutations on n letters. We write $\mathrm{Alt}(\mathfrak{R}_f)$ for the only index 2 subgroup of $\mathrm{Perm}(\mathfrak{R}_f) \cong \mathfrak{S}_n$, which is isomorphic to the alternating group $\mathfrak{A}_n$. We will apply constructions of Section, 2.3 to

$$n = 2g + 1, R = \mathfrak{R}_f, G = \mathrm{Gal}(f/K)$$

and the faithful $G = \mathrm{Gal}(f/K)$-module $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ of $\mathbb{F}_2$-dimension $n - 1 = 2g$. Notice that the action of $\mathrm{Gal}(K)$ on $\mathfrak{R}_f$ factors through the natural *surjection*

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(f/K), \tag{10.6}$$

which allows us to consider $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ as the $\mathrm{Gal}(K)$-module.

Remark 10.5. In light of Remark 2.14(0), the surjectivity of (10.6) implies that $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ is very simple as the $\mathrm{Gal}(f/K)$-module if and only if it is very simple as the $\mathrm{Gal}(K)$-module. In light of Theorem 2.21(ii) to $R = \mathcal{R}_f$ and $G = \mathrm{Gal}(f/K)$, the $\mathrm{Gal}(K)$-module $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ is very simple if $\mathrm{Gal}(f/K) = {}_n$ or $\mathfrak{A}_n$. (Recall that $g \geq 2$ and therefore $n = 2g + 1 \geq 5$.)

Let C_f be the irreducible smooth projective curve, that is, the smooth projective model of the smooth plane affine curve

$$\tilde{C}_f : y^2 = f(x).$$

It is a genus g curve that is defined over K, whose field of rational functions is the field of fractions of the ring $K[x, y]/(y^2 - f(x))$. Its set of complex points $C_f(\mathbb{C})$ is the union of $\tilde{C}_f(\mathbb{C})$ and one

point, denoted by ∞. It is defined over K, and it is the only pole of rational functions x and y. More precisely, ∞ is a double pole of x and a pole of order $2g+1$ of y. The $(2g+1)$-element set of points

$$\mathfrak{W}_\alpha = (\alpha, 0) \in \tilde{C}_f(\bar{K}) \subset C_f(\bar{K}) \subset C_f(\mathbb{C}),\ (\alpha \in \mathfrak{R}_f)$$

is the set of zeros of y; all of them are simple. In addition, each $\mathfrak{W}_\alpha$ is the only zero of the rational function $x-\alpha$, and this zero is double. Hence, the divisor of each rational function $x-\alpha$ on C_f is equal to $2(\mathfrak{W}_\alpha) - 2(\infty)$, while the divisor of y is

$$\big(\sum_{\alpha\in\mathfrak{R}_f}(\mathfrak{W}_\alpha)\big) - (2g+1)(\infty) = \sum_{\alpha\in\mathfrak{R}_f}(\mathfrak{W}_\alpha) - (\infty).$$

This implies that the linear equivalence class of each divisor $(\mathfrak{W}_\alpha) - (\infty)$ has order 2 in the Picard group of C_f. In addition, the $(2g+2)$-element set of all Weierstrass points of C_f consists of ∞ and all $\mathfrak{W}_\alpha$.

There is a hyperelliptic biregular involution $\iota : C_f \to C_f$ such that

$$\iota^* x = x, \iota^* y = -y;$$

in particular, the subfield of ι-invariant rational functions on C_f coincides with $\mathbb{C}(x)$; the $\mathbb{C}$-subspace of ι-antiinvariant rational functions on C_f coincides with $y\cdot\mathbb{C}(x)$. On the other hand, the set of fixed points of ι consists of ∞, and all $\mathfrak{W}_\alpha$, i.e., coincides with the set of all Weierstrass points of C_f. (See [128] for details.)

Lemma 10.6. *Let D be a divisor on C with support in $\{\mathfrak{W}_\alpha \alpha \in \mathfrak{R}_f\}$, i.e.,*

$$D = \sum_{\alpha\in\mathfrak{R}_f} m_\alpha(\mathfrak{W}_\alpha),\ \ \textit{all } m_\alpha \in \mathbb{Z},\ \sum_{\alpha\in\mathfrak{R}_f} m_\alpha = 0.$$

Then, D is principal if and only if D is divisible by 2 in the group of divisors on C, i.e., all $m_\alpha \in 2\cdot\mathbb{Z}$.

This lemma gives us the following description of the Galois module $\mathrm{Pic}^0(C_f)[2]$ of points of order (dividing) 2 on the Picard group of C_f that is actually contained in [128], see also [189, p. 103].

Claim 10.7. The $\mathrm{Gal}(K)$-modules $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ and $\mathrm{J}(C_f)[2]$ are canonically isomorphic.

Proof of Claim 10.7 modulo Lemma 10.6. Let us consider the $\mathrm{Gal}(K)$-module $\mathbb{Z}^{\mathfrak{R}_f}$ of $\mathbb{Z}$-valued functions on $\mathfrak{R}_f$ and its submodule

$$\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 = \{\tilde{\phi} : \mathfrak{R}_f \to \mathbb{Z} \mid \sum_{\alpha\in\mathfrak{R}_f} \tilde{\phi}(\alpha) = 0\}.$$

Clearly, $\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0$ is a free $\mathbb{Z}$-module of rank $n-1 = (2g+1)-1 = 2g$ and its quotient $\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 / 2\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0$ is a vector space over $\mathbb{F}_2$ of dimension $2g$. Let us consider the homomorphism of $\mathrm{Gal}(K)$-modules

$$\tilde{\Psi} : \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 \to J(C_f)[2]$$

that assigns to a function $\tilde{\phi} : \mathfrak{R}_f \to \mathbb{Z}$ the linear equivalence class of the divisor

$$\sum_{\alpha \in \mathfrak{R}_f} \tilde{\phi}(\alpha)(\mathfrak{W}_\alpha) = \sum_{\alpha \in \mathfrak{R}_f} \tilde{\phi}(\alpha)\left((\mathfrak{W}_\alpha) - (\infty)\right).$$

By Lemma 10.6, the kernel of $\tilde{\Psi}$ coincides with $2 \cdot \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0$. Hence, $\tilde{\Psi}$ induces the injective homomorphisms if $\mathrm{Gal}(K)$-modules

$$\Psi : \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 / 2\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 \hookrightarrow J(C_f)[2].$$

Since the source and the target of Ψ have the same $\mathbb{F}_2$-dimension (namely, $2g$), Ψ is an isomorphism of $\mathrm{Gal}(K)$-modules. To finish the proof, we need to produce an isomorphism of $\mathrm{Gal}(K)$-modules $\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 / 2\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0$ and $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$, which is straightforward. Indeed, let us consider the homomorphism of $\mathrm{Gal}(K)$-modules

$$\tilde{\Phi} : \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 \to \left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0, \ \tilde{\phi} \mapsto \phi = \tilde{\phi} \bmod 2.$$

Clearly, the kernel of $\tilde{\Phi}$ coincides with $2 \cdot \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0$. Hence $\tilde{\Phi}$ induces an injective homomorphism of $\mathrm{Gal}(K)$-modules

$$\Phi : \left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 / 2\left(\mathbb{Z}^{\mathfrak{R}_f}\right)^0 \hookrightarrow \left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0.$$

Since the source and the target of Φ have the same $\mathbb{F}_2$-dimension (namely, $2g$), Φ is an isomorphism of $\mathrm{Gal}(K)$-modules. This ends the proof of the claim. □

Proof of Lemma 10.6. Let

$$D = \sum_{\alpha \in \mathfrak{R}_f} m_\alpha(\mathfrak{W}_\alpha) \tag{10.7}$$

be a degree 0 divisor on C. In particular,

$$0 = \deg(D) = \sum_{\alpha \in \mathfrak{R}_f} m_\alpha.$$

Suppose that all the integers m_α are *even*, i.e., $m_\alpha = 2d_\alpha$ for some integers d_α and

$$\sum_{\alpha \in \mathfrak{R}_f} 2d_\alpha = \sum_{\alpha \in \mathfrak{R}_f} m_\alpha = 0.$$

This implies that

$$D = \sum_{\alpha \in \mathfrak{R}_f} m_\alpha(\mathfrak{W}_\alpha) - 0(\infty) = \left(\sum_{\alpha \in \mathfrak{R}_f} 2d_\alpha(\mathfrak{W}_\alpha)\right) - \left(\sum_{\alpha \in \mathfrak{R}_f} 2d_\alpha\right)(\infty) =$$

$$\sum_{\alpha \in \mathfrak{R}_f} d_\alpha\left(2(\mathfrak{W}_\alpha) - 2(\infty)\right) = \sum_{\alpha \in \mathfrak{R}_f} d_\alpha \mathrm{div}(x - \alpha) = \mathrm{div}\left(\prod_{\alpha \in \mathfrak{R}_f} (x - \alpha)^{d_\alpha}\right)$$

is a *principal* divisor. Conversely, suppose that D is a principal divisor, i.e., there is a nonzero ration function $f \in \mathbb{C}(C)$ such that $D = \mathrm{div}(f)$. Since D is ι-invariant, $\iota^* f = c \cdot f$ for some nonzero $c \in \mathbb{C}$. Since ι is an involution,

$$f = (\iota^2)^* f = \iota^*(\iota^* f) = \iota^*(c \cdot f) = c \cdot \iota^*(f) = c \cdot (c \cdot f) = c^2 \cdot f,$$

and therefore, $c^2 = 1$, that is, either $c = 1$ or $c = -1$. Therefore, f is either ι-invariant (i.e., lies in $\mathbb{C}(x)$) or is ι-antiinvariant (i.e., lies in $y \cdot \mathbb{C}(x)$).

- Suppose that our nonzero $f \in \mathbb{C}(x)$. This means that

$$f = \mu \prod_{\beta \in \mathbb{C}} (x - \beta)^{e_\beta};\ \mu \in \mathbb{C}^*,\ e_\beta \in \mathbb{Z},$$

  where $e_\beta = 0$ for all but finitely many $\beta \in \mathbb{C}$. Since $\mathrm{div}(f) = D$, all the poles and zeros of f lie in $\{\mathfrak{W}_\alpha \mid \alpha \in \mathfrak{R}_f\}$. It follows that $e_\beta = 0$ for all $\beta \notin \mathfrak{R}_f$. This implies that

$$f = \mu \prod_{\alpha \in \mathfrak{R}_f} (x - \alpha)^{e_\alpha},$$

  and therefore,

$$D = \mathrm{div}(f) = \sum_{\alpha \in \mathfrak{R}_f} e_\alpha \mathrm{div}(x - \alpha) = \sum_{\alpha \in \mathfrak{R}_f} e_\alpha \left(2(\mathfrak{W}_\alpha) - 2(\infty)\right) =$$

$$2 \left(\sum_{\alpha \in \mathfrak{R}_f} e_\alpha (\mathfrak{W}_\alpha) \right) - 2 \left(\sum_{\alpha \in \mathfrak{R}_f} e_\alpha \right) (\infty).$$

  In light of (10.7),

$$\sum_{\alpha \in \mathfrak{R}_f} e_\alpha = 0,\ m_\alpha = 2e_\alpha \in 2\mathbb{Z}\ \forall \alpha \in \mathfrak{R}_f,$$

  and we are done.

- Now, suppose that our nonzero $f \in y \cdot \mathbb{C}(x)$, i.e,

$$f = y \cdot h(x) \ \text{ where } h(x) = \mu \prod_{\beta \in \mathbb{C}} (x - \beta)^{e_\beta};\ \mu \in \mathbb{C}^*,\ e_\beta \in \mathbb{Z},$$

  where $e_\beta = 0$ for all but finitely many $\beta \in \mathbb{C}$. Notice that y has a pole of *odd* order $n = 2g+1$ at ∞. On the other hand, each $x - \beta$ has a pole of order 2 at ∞. This implies that f has a zero of pole (of odd order) at ∞, which contradicts (10.7). This ends the proof.

□

Corollary 10.8. *If the* $\mathrm{Gal}(f/K)$*-module* $\left(\mathbb{F}_2^{\mathfrak{R}_f}\right)^0$ *is very simple, then* $\mathrm{End}(\mathrm{J}(C_f)) = \mathbb{Z}$*. In particular,* $J(C_f)$ *is a simple abelian variety.*

Proof. It follows from Claim 10.7 combined with Remark 10.5 that the $\mathrm{Gal}(K)$-module $\mathrm{J}(C_f)[2]$ is very simple. Now the desired result follows from Theorem 2.15 applied to $X = \mathrm{J}(C_f)$ and $\ell = 2$. □

Combining Corollary 10.8 with Remark 10.5, we obtain the following assertion:

Theorem 10.9. *Suppose that $g \geq 2$ is an integer, K is a finitely generated subfield of $\mathbb{C}$, and $f(x) \in K[x]$ a monic polynomial of degree $n = 2g + 1$ without repeated roots. Suppose that $\mathrm{Gal}(f/K) = \mathbb{S}_n$ or $\mathbb{A}_n$. Then, $\mathrm{End}(\mathrm{J}(C_f)) = \mathbb{Z}$. In particular, $\mathrm{J}(C_f)$ is a simple abelian variety.*

Remark 10.10. Theorem 10.9 remains valid even if we do not assume that K is finitely generated and $f(x)$ is monic.

10.3 Abelian Varieties with Non-trivial Automorphism Group

Let G be a finite group acting faithfully on an abelian variety $A = V/\Lambda$ of dimension g. Then, G acts linearly on the complex linear space V leaving the lattice Λ invariant. Let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$. The action of G on A defines a structure of $\mathbb{Z}[G]$-module on Λ and on its dual lattice $\Lambda^\vee$. After tensoring with $\mathbb{C}$, the linear representation $(\Lambda^\vee)_{\mathbb{C}}$ decomposes into the direct sum of complex linear g-dimensional representations $H^{1,0}(A, \mathbb{C}) \oplus H^{0,1}(A, \mathbb{C})$ with characters χ and $\bar{\chi}$ such that $\chi + \bar{\chi}$ is defined over $\mathbb{Q}$. IDIs χ real?

Let $\mathbb{Q}[G]$ be the group algebra of G over $\mathbb{Q}$. By Theorem of Maschke, $\mathbb{Q}[G]$ is a semi-simple algebra. It contains a finite number of idempotents $e_1, \ldots, e_r$ from the center $Z(G)$ of G such that $e_i^2 = e_i, 1 = e_1 + \cdots + e_r$, and $\mathbb{Q}[G] \cong \oplus_{i=1}^r \mathbb{Q}[G]_i$, where $\mathbb{Q}[G]_i = e_i\mathbb{Q}[G]$ is a simple $\mathbb{Q}$-lagebra. Any direct factor $\mathbb{Q}[G]_i$ is isomorphic to a matrix algebra $M_{n_i}(D)$ over some division algebra D_i. Every finite-dimensional $\mathbb{Q}$-linear representation of G splits into a direct sum of irreducible representations, each defining an irreducible module over $\mathbb{Q}[G]_i$.

In particular, $\Lambda_{\mathbb{Q}}$ splits into the direct sum of irreducible representations of G. Let e_W be the central idempotent corresponding to an irreducible rational representation W contained in $\Lambda_{\mathbb{Q}}$. Let n be the smallest integer such that $\rho(ne_W) \in \mathrm{End}(A)$. Then, the image of ne_W is an abelian subvariety A_W of $\mathrm{J}(C)$. We have

$$A_W \cong V_W/\Lambda_W,$$

where $V_W = \rho_a(e_W)$ and $\Lambda_W = \mathrm{Im}(\rho_r(e_W)) \cap \Lambda$. Here, the intersection is taken in $\Lambda_{\mathbb{Q}}$. If the inclusion $\Lambda_W \to \Lambda$ is given by a matrix P, then the type of the polarization of J_W is equal to the type of the symplectic form defined by the matrix ${}^tPJP$, where J_{D} is the symplectic matrix defining a polarization on A.

An abelian variety A with a faithful G-action is called *G-simple* if it does not contain proper G-invariant abelian subvarieties. Similar to the case when $G = \{1\}$, one constructs an isogeny

$$A_1 \times \cdots \times A_k \to A,$$

where A_i are G-simple abelian varieties (see [106], 13.6). The varieties A_i are called *isotypical components* of A. Each isotypical component is G-isomorphic to a subvariety of A_W for some W.

For example, if $G = \{1, g\}$ is of order 2, then A decomposes into a g-invariant and g-anti-invariant parts corresponding to the idempotents $\frac{1}{2}(1+g)$ and $\frac{1}{2}(1-g)$.

Let L_0 be an ample line bundle on A that defines a polarization $\phi_{L_0} : A \to \hat{A}$. The action of G on $V^\vee$ and $\Lambda^\vee$ defines a faithful action on $\hat{A}$. Viewing $\hat{A}$ as the Picard variety of A, the action is the natural action $L \mapsto g^*(L)$. The homomorphism ϕ_{L_0} is a G-equivariant homomorphism if and only if L_0 admits a *G-linearization*, i.e. the Hermitian form $H : V \times V \to \mathbb{C}$ defining L is G-invariant with respect to the diagonal action of G on $V \times V$.

The action of G on A defines a homomorphism

$$\rho : \mathbb{Q}[G] \to \mathrm{End}_{\mathbb{Q}}(A).$$

It is injective on any simple direct summand $\mathbb{Q}[G]_i$. In particular, $\mathrm{End}(A) \neq \mathbb{Z}$ if $G \neq \{1\}$.

Example 10.11. Suppose C is a nonsingular projective curve of genus $g > 1$ and let G be a subgroup of its group of automorphisms. Then, G acts faithfully on the Jacobian variety $\mathrm{J}(C)$ preserving its principal polarization. Conversely, by the Torelli Theorem, if C is hyperelliptic, G acts faithfully on $\mathrm{J}(C)$ and preserves the natural principal polarization on the Jacobian variety, then the action of G on $\mathrm{J}(C)$ arises from the action on C. This follows from a variant of *Torelli's Theorem* [118, §12, Th. 12.1], which was proven by A. Weil [174]. If C is not hyperelliptic then it is not necessarily true, because multiplication by -1 on $\mathrm{J}(C)$ respects the polarization but is not induced by any automorphism of C.

Example 10.12. Assume G is a finite abelian group. First, we decompose G into the direct sum of cyclic groups G_i of orders m_i. Then, $\mathbb{Q}[G] \cong \prod_i \mathbb{Q}[G_i]$. Assume $G = (g)$ is cyclic of order m generated by g. Then,

$$\mathbb{Q}[G] \cong \prod_{d|m} \mathbb{Q}[t]/(\Phi_d(t)),$$

where $\Phi_d(t)$ is an irreducible cyclotomic polynomial of degree $\phi(d)$. Each direct factor is a cyclotomic field of degree $\phi(m)$ over $\mathbb{Q}$. It is generated by the central idempotent $f_d = \phi_d(g)$, where $\phi_d(t) \in (\Phi_d(t))$ and $1 = \sum_{d|m} \phi_i(t)$. For example, if $m = 3$, we may take $f_1 = \frac{1}{3}(1-g)(2+g)$ and $f_3 = \frac{1}{3}(1+g+g^2)$.

The group G acts on each summand $Q_i \cong \mathbb{Q}(\zeta_d)$ considered as a linear space over $\mathbb{Q}$ of dimension $\phi(d)$. This is an irreducible rational representation of G. Of course, considered as a complex representation it splits into the direct sum of one-dimensional representations.

Let G be a finite irreducible subgroup of a finite-dimensional complex linear space V. This means that the induced complex linear representation of G in V is irreducible, which may be restated as follows.

Let $\mathbb{C}G$ (respectively $\mathbb{Q}G$) be the $\mathbb{C}$-vector subspace (respectively the $\mathbb{Q}$-vector subspace) of $\mathrm{End}_{\mathbb{C}}(V)$ generated by

$$G \subset \mathrm{Aut}_{\mathbb{C}}(V) \subset \mathrm{End}_{\mathbb{C}}(V).$$

Since G is a multiplicative subgroup of $\mathrm{End}_{\mathbb{C}}(V)$, $\mathbb{C}G$ is a $\mathbb{C}$-subalgebra (respectfully $\mathbb{Q}G$ is a $\mathbb{Q}$-algebra) of the $\mathbb{C}$-algebra $\mathrm{End}_{\mathbb{C}}(V)$. By definition,

$$\mathbb{Q}G \subset \mathbb{C}G \subset \mathrm{End}_{\mathbb{C}}(V).$$

Now the irreducibility of G implies that

$$\mathbb{C}G = \mathrm{End}_{\mathbb{C}}(V)$$

(see, for instance, [149, Sect. 6.2]). On the other hand, the $\mathbb{Q}$-algebra $\mathbb{Q}G$ is obviously isomorphic to the quotient of the semi-simple group algebra $\mathbb{Q}[G]$ and therefore is also semi-simple.

Let us look at the *center* $\mathbf{Z}_G$ of $\mathbb{Q}G$. The semi-simplicity of the $\mathbb{Q}$-algebra $\mathbb{Q}G$ implies that $\mathbf{Z}_G$ is either a number field or is isomorphic to a direct sum of number fields. Since $\mathbb{C}G = \mathrm{End}_{\mathbb{C}}(V)$ consists of $\mathbb{C}$-linear combinations of $G \subset \mathbb{Q}G$, we have the inclusion $\mathbf{Z}_G \subset \mathbb{C} \cdot \mathrm{id}_V \cong \mathbb{C}$, because the latter is the center of $\mathrm{End}_{\mathbb{C}}(V)$. This implies that $\mathbf{Z}_G$ has *no* zero divisors and therefore is a (number) field. It follows that the semisimple $\mathbb{Q}$-algebra $\mathbb{Q}G$ is actually simple and therefore is isomorphic to $\cong M_r(D)$ for some division algebra D with center $\mathbf{Z}_G$.

Let $\chi_{G,V}$ be the character of the representation of G in V. Then, $\mathbf{Z}_G$ coincides with the subfield $\mathbb{Q}(\chi_{G,V}) \subset \mathbb{C}$ generated by the values of the character. Let $S_{G,V}$ be the *Schur index* of $\chi_{G,V}$ defined to be the minimum of degrees $[K : \mathbb{Q}]$ of extension $K/\mathbb{Q}(\chi_{G,V})$ over which the representation is defined. Equivalently, $S_{G,V}$ is the square root of the $\mathbf{Z}_G$-dimension of D. It is a classical result of R. Brauer and Speiser [54, Cor. 2.4 on p. 277] that $S_{G,V} = 1$ or 2 if $\chi_{V,G}$ is a *real character.*

The condition that irreducible G leaves a lattice $\Lambda \subset V$ invariant imposes some strict conditions on the Schur index.

Given an irreducible finite subgroup $G \subset \mathrm{GL}(V)$ one may ask whether V contains a G-invariant lattice Λ such that V/Λ is an abelian variety.

The following theorem is proven in [138, Theorem 2.6].

Theorem 10.13. *The following properties are equivalent:*

(i) There is a nonzero G-invariant lattice in V.

(ii) Either $S_{G,V} = 1$ and $\mathbb{Q}(\chi_{G,V}) = \mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$, or $S_{G,V} = 2$ and $\mathbb{Q}(\chi_{G,V}) = \mathbb{Q}$.

(iii)

Theorem 10.14. *Let Λ be a G-invariant lattice of rank $2g$ in V.*

(i) Suppose $S_{G,V} = 1$. Then, the complex torus V/Λ is an abelian variety V/Λ is isogenous to the self-product of an elliptic curve. In addition, if $\mathbf{Z}_G$ is an imaginary quadratic field, then V/Λ is isomorphic to a product of mutually isogenous elliptic curves with complex multiplication.

(ii) Suppose that $S_{G,V} = 2$ and $\chi_{G,V}$ is a rational character, i.e., $\mathbf{Z}_G = \mathbb{Q}$. Then, g is even and there exists a quaternion algebra H over $\mathbb{Q}$ such that $\mathbb{Q}[G] \cong M_{g/2}(H)$.

Example 10.15. (See also [138, Example 3.2]. [1])

[1] In loc. cit. one should read $\mathrm{PSL}_2(\mathbf{F}_q)$ instead of $\mathrm{SL}_2(\mathbf{F}_q)$ and add the assumption $q \geq 7$.

Suppose that p is a prime that is congruent to 3 modulo 4 and r is a positive integer such that

$$q = p^{2r-1} \geq 7.$$

Clearly, q is also congruent to 3 modulo 4. Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$, which is a finite simple non-abelian group. It is known that the Schur index of every irreducible character of G is equal to 1. ([82, Corollary on p. 4], see also [54, Theorem 6.2]).

It follows from the character table of G (which can be found in [45, Sect. 38]) that G admits two complex-conjugate irreducible faithful representations $G \hookrightarrow \mathrm{Aut}_{\mathbb{C}}(V)$ with characters η_1 and η_2 of dimension $\frac{1}{2}(q-1)$ defined over an imaginary quadratic field

$$\mathbb{Q}(\eta_k) = \mathbb{Q}(\sqrt{-q}) = \mathbb{Q}(\sqrt{-p}).$$

By Theorem 10.13, V admits a $\mathrm{PSL}_2(\mathbb{F}_q)$-invariant sublattice Λ of rank $q-1$ such that V/G is an abelian variety of dimension $(q-1)/2$, which is isomorphic to the product of mutually isogenous elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-p})$.

For example, take $q = 7$. Then, $G = \mathrm{PSL}_2(\mathbb{F}_7)$ is the Klein group of order 168 which can be realized as the group of automorphisms of the Klein curve X of genus 3 isomorphic to a plane curve given by equation

$$x^3y + y^3z + z^3x = 0.$$

The abelian variety V/Λ is realized as the Jacobian variety of X. It is known that the quotients of the Klein curve by subgroups of G of order $2, 3$ and 4 are elliptic curves and the quotients by other non-trivial subgroups are rational curves. The fact that the elliptic quotients of the Jacobian variety of X have complex multiplication by $\mathbb{Q}(\sqrt{-7})$ can be found in [48] and [85].

In another special case, where we take $q = 11$. The group $\mathrm{PSL}_2(11)$ acts faithfully on a *Klein cubic hypersurface* X in $\mathbb{P}^4$ given by equation

$$x^2y + y^2z + z^2w + w^2z = 0.$$

It also acts on its intermediate Jacobian variety $J(X)$ which is a principally polarized abelian variety of dimension 5. The period matrix of $J(X)$ was computed in [141]. It confirms that $J(X)$ is isogenous to the product of five copies of an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-11})$.

Example 10.16. Let $f : C \to \mathbb{P}^1$ be a cover of nonsingular curves with cyclic Galois group G of order m. Let $B = \{p_1, \ldots, p_{r+1}\}$ be the set of its branch points, and let e_i be the ramification index of a ramification point lying over p_i, so that we have m/e_i ramification points over p_i. We assume that the genus of C is larger than 0, this implies that $r \geq 3$. Let $U = \mathbb{P}^1 \setminus B$ and $\gamma_1, \ldots, \gamma_{r+1}$ be standard generators of the fundamental group $\pi_1(U)$ satisfying the relation $\gamma_1 \cdots \gamma_{r+1} = 1$. The cover defines a surjective homomorphism $\tau : \pi_1(U) \to \mathbb{Z}/m\mathbb{Z}$. Let $\chi(\gamma_i) = a_i \mod m$. Since $\tau(\gamma_i^{e_i}) = 1$, we must have $e_i a_i \equiv 0 \mod m$ and $\sum a_i \equiv 0 \mod m$. Since τ is surjective,

$$(a_1, \ldots, a_{r+1}) = 1 \mod m.$$

Let $\bar{\mathrm{e}}_i$ be the images of the unit vectors in $\mathbb{Z}^{r+1}$ in $(\mathbb{Z}/m\mathbb{Z})^{r+1}$ and $\bar{e} = \bar{e}_1 + \cdots + \bar{e}_{r+1}$. We can factor τ through a surjective homomorphisms

$$\sigma : \pi_1(U) \to A_{m,r} := (\mathbb{Z}/m\mathbb{Z})^{r+1}/(\bar{e}),$$

that sends γ_j to $\bar{\mathbf{e}}_j$. Let $X \to C$ be the Galois cover corresponding to the homomorphism σ. Its Galois group is equal to $H = \mathrm{Ker}(\sigma)$.

Let

$$\mathrm{H}^1(X, \mathbb{C}) = \oplus_\chi \mathrm{H}^1(X, \mathbb{C})_\chi$$

be the decomposition of $\mathrm{H}^1(C, \mathbb{C})$ into direct sum of eigensubspaces with characters $\chi \in \mathrm{Hom}(A_{d,r}, \mu_m)$. We have

$$\mathrm{H}^1(C, \mathbb{C}) \cong \mathrm{H}^1(X, \mathbb{C})^H = \oplus_{\chi, \chi|H=1} \mathrm{H}^1(X, \mathbb{C})_\chi. \tag{10.8}$$

The group $\mathcal{X}$ of characters whose restriction to H is the identity is a cyclic group generated by the character $\chi_{\boldsymbol{\mu}}$ that sends $\bar{\mathbf{e}}_j \in A_{m,r}$ to $e^{2\pi i a_j/m}$. Here we use $\boldsymbol{\mu}$ to denote the vector

$$\boldsymbol{\mu} = (\frac{a_1}{m}, \dots, \frac{a_{r+1}}{m}).$$

It satisfies the condition that $|\boldsymbol{\mu}| = \mu_1 + \cdots + \mu_{r+1} \in \mathbb{Z}$. Any other character in $\mathcal{X}$ is a power $\chi^n_{\boldsymbol{\mu}}, n = 0, \dots, m-1$. It corresponds to the vector

$$\boldsymbol{\mu}^n := (\frac{(na_1)}{m}, \dots, \frac{(na_{r+1})}{m}),$$

where the round brackets denote the remainder of the number for the division by m. We set

$$d_n = |\boldsymbol{\mu}^n| := \frac{1}{m} \sum_{i=1}^{r+1} (na_i).$$

The curve X is easy to describe by equations. For convenience, let us choose projective coordinates on $\mathbb{P}^1$ such that

$$p_i = [1, x_i], \quad p_{r+1} = [0, 1]$$

and consider a linear embedding

$$\alpha : \mathbb{P}^1 \to \mathbb{P}^r, \quad [t_0, t_1] \mapsto [x_1 t_0 - t_1, \dots, x_r t_0 - t_1, t_0].$$

Let $r_m : \mathbb{P}^r \to \mathbb{P}^r$ be the cover given by raising the coordinates in mth power. Then, X is isomorphic to the pull-back of the cover s to C, i.e. we have a commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & \mathbb{P}^r \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle s} \\ C & \xrightarrow{\alpha} & \mathbb{P}^r \end{array}$$

It follows that X is isomorphic to the complete intersection of Fermat hypersurfaces

$$F_i = \sum_{i=0}^{r} \alpha_{ij} y_i^m = 0, \quad j = 1, \dots, r-1,$$

where $M = (\alpha_{ij})$ is a matrix of size $(r-1) \times 2$ and rank $r-1$ satisfying

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ x_1 & x_2 & \dots & x_r & 1 \end{pmatrix} \cdot M = 0.$$

The curve C is explicitly computed by using the action of $A_{m,r}$ on X. It is birationally isomorphic to the curve

$$y^m = (x - x_1)^{a_1} \cdots (x - x_r)^{a_r}, \tag{10.9}$$

where $e_i = m/(m, a_i)$ with $a_{r+1} \equiv -(a_1 + \cdots + a_r) \mod m$.[2] Note that, for any k prime to m, the curve (10.9) is isomorphic to the curve with the same branch points but with $(a_1, \ldots, a_r)$ replaced by $(ka_1, \ldots, ka_r) \mod m$.

Applying the Riemann–Hurwitz formula, we obtain that the genus of C is equal to

$$g = 1 + \frac{m(r-1) - \sum_{i=1}^{r+1}(m, a_i)}{2}. \tag{10.10}$$

We have

$$\mathrm{H}^1(C, \mathbb{C})_{\chi_{\boldsymbol{\mu}}^n} = H^{1,0}(C)_{\chi_{\boldsymbol{\mu}}^n} \oplus H^{0,1}(C)_{\chi_{\boldsymbol{\mu}}^n},$$

and the well known formula due to Hurwitz and Chevalley-Weil gives:

$$\dim H^{1,0}(C)_{\chi_{\boldsymbol{\mu}}^n} = d_n, \quad \dim H^{1,0}(C)_{\chi_{\boldsymbol{\mu}}^n} = d_{m-n}, \quad n = 1, \ldots, m-1, \tag{10.11}$$

and $\mathrm{H}^1(C, \mathbb{C})_1 = \{0\}$. There are many proofs of this formula. For example, one computes the cohomology $\mathrm{H}^1(X, \mathbb{C})$ as a representation of $A_{N,r}$ (see [165]):

$$\mathrm{H}^1(X, \mathbb{C}) \cong \mathbb{C}[T_0, \ldots, T_r, \lambda_1, \ldots, \lambda_{r-1}]/J,$$

where J is the ideal generated by partial derivatives in y_j and λ_k of the equation $F(y, \lambda) = \sum_{i=1}^{r-1} \lambda_i F_i$. Here each coset of a monomial $y_0^{s_0} \cdots y_r^{s_r}$ is an eigenvector of $A_{N,r}$ with eigenvalue $-r + \sum_{j=0}^{r} s_j/N$.[3]

The case $|\boldsymbol{\mu}| = 2$ is special since it gives a one-dimensional part $H^{1,0}(C)_{\chi_{\boldsymbol{\mu}}}$ of $H^{1,0}(C)$ that allows one to construct an *eigenperiod map* for curves C with varying $(x_1, \ldots, x_r)$ with values in a complex ball. For some spacial $\boldsymbol{\mu}$ one relates this period map with the period map of certain families of K3 surfaces (see [40]).

The cyclic group G acts on C and hence acts on its Jacobian variety $\mathrm{J}(C)$. For example, if $m = p$ is prime, we get

$$g = \tfrac{1}{2}(r-1)(p-1),$$

and taking $r = 2$, i.e. a cover with 3 branch points, we obtain that $g = \frac{1}{2}(p-1)$ and $\mathrm{J}(C)$ has multiplication by the CM-field $\mathbb{Q}(\zeta_p)$. This agrees with *Belyi's Theorem* that any cover of $\mathbb{P}^1$ ramified over 3 points is defined over $\bar{\mathbb{Q}}$ [11].

Suppose $m'|m$, then the surjective homomorphism of cyclic group $G_m = (\mathbb{Z}/m\mathbb{Z}) \to G_{m'} = (\mathbb{Z}/m'\mathbb{Z})$ defines a Galois cover $C \to C'$ with the cyclic Galois group of order m/m'. It is easy to see that

$$C' : y^{m'} = (x - x_1)^{\bar{a_1}} \cdots (x - x_r)^{\bar{a_r}}, \tag{10.12}$$

where $0 \le \bar{a}_i < m', a_i \equiv \bar{a}_i \mod m'$.

[2] One can also view C as the normalization of the cover defined by a line bundle $L = \mathcal{O}_{\mathbb{P}^1}(\frac{1}{m}\sum_{i=1}^{r+1} a_i x_i)$ on $\mathbb{P}^1$ and a section of $L^{\otimes m}$ with the divisor of zeros equal to $\sum_{i=1}^{r+1} a_i x_i$.

[3] This method extends to a similar computation for cyclic covers of projective spaces branched over an arrangement of hyperplanes, see [40].

Chapter 11

Special Families of Abelian Varieties

In this chapter, we will study families of abelian varieties that contain a dense Zariski subset of abelian varieties with complex multiplication.

11.1 Families of Abelian Varieties with a Fixed Hodge Group

Let $f : \mathcal{A} \to T$ be a smooth family of polarized abelian varieties over a smooth manifold T. This means that there exists a relatively line bundle $\mathcal{L}$ on $\mathcal{A}$ such that its restriction to each fiber defines a polarization of type D that does not depend on $t \in T$. The family is called *special* if it contains a dense set of points $t \in T$ such that the fiber $\mathcal{A}_t$ is of CM type. For example, a constant family $\mathcal{A} = A \times T \to T$ is special if A is of CM-type.

Similarly, using the variation of polarized rational Hodge structures one can define a special family of families of polarized algebraic varieties.

Passing to the universal cover of S we obtain a family $\tilde{\mathcal{X}} \to \tilde{T}$ such that we can identify the lattice $\Lambda_{\tilde{t}} = \mathrm{H}_1(\mathcal{A}_{\tilde{t}}, \mathbb{Z}))$ with a fixed lattice $\Lambda = \mathbb{Z}^{2g}$ so that the cohomology $\mathrm{H}_1(\mathcal{A}_{\tilde{t}}, \mathbb{R})$ can be identified with $W = \Lambda_{\mathbb{R}}$. We can also fix the symplectic form E on Λ. The E-polarized complex structure on $\Lambda_{\mathbb{R}}$ defined by the complex structure on $\mathcal{A}_{\tilde{t}}$ defines a point in the Grassmannian $\mathsf{G}(g, \Lambda_{\mathbb{C}})_E$, and gives rise to the (marked) period map

$$\tilde{p} : \tilde{T} \to \mathsf{G}(g, \Lambda_{\mathbb{C}})_E \cong \mathfrak{H}_g.$$

Its composition with the projection to $\mathcal{A}_g$ defines the period map

$$p : T \to \mathcal{A}_g.$$

Fix a connected algebraic group $G_{\mathbb{Q}}$ defined over $\mathbb{Q}$ and a faithful homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{Sp}(W, E)_{\mathbb{Q}},$$

where $\mathrm{Sp}(W,E)_{\mathbb{Q}}$ is the algebraic group over $\mathbb{Q}$ whose points in a $\mathbb{Q}$-algebra K is the group of linear transformations of the symplectic form (W_K, E_K). In particular, ρ defines a homomorphism

$$\rho_{\mathbb{R}} : G_{\mathbb{Q}}(\mathbb{R}) \to \mathrm{Sp}(W,E)_{\mathbb{Q}}(\mathbb{R}) = \mathrm{Sp}(W,E) \cong \mathrm{Sp}(2g, J_{\mathsf{D}}).$$

We also fix an arithmetic subgroup Γ of $G_{\mathbb{Q}}$ such that $\rho(\Gamma)$ leaves $\Lambda \subset W$ invariant. A E-polarized complex structure on W is determined by a homomorphism

$$\phi : \mathbb{U}(1) \to \mathrm{Sp}(W,E)$$

that sends $e^{i\theta}$ to the multiplication by $e^{i\theta}$ in W. It can be viewed as the restriction of the unique $\mathsf{h}_\phi : \mathbb{S} \to \mathrm{Sp}(W,E)_{\mathbb{Q}}$ by passing to real points and restricting h to the subgroup of $\mathbb{S}^1$ of $\mathbb{S}$ such that $\mathbb{S}^1(\mathbb{R}) = \mathbb{U}(1) \subset \mathbb{C}^*$. We fix one complex structure ϕ_0 and consider the orbit of ϕ_0 under the action of $\rho(G), g \mapsto \rho(g)\phi_0\rho(g)^{-1}$. The orbit is a homogeneous space $G_{\mathbb{R}}/K^0_{\mathbb{R}}$, where $K_{\mathbb{R}}$ is the connected component of the stabilizer of ϕ_0. It can be shown that the orbit defines a family of polarized abelian varieties

$$\mathcal{X}(G,\Gamma,\rho,\phi_0) \to T = \Gamma\backslash G_{\mathbb{R}}/K^0_{\mathbb{R}}. \tag{11.1}$$

The base of the family is a Hermitian symmetric domain if the following condition is satisfies:

$$\rho(G(\mathbb{R})) \text{ is normalized by } \phi_0(\mathbb{U}(1)). \tag{11.2}$$

Let $\mathrm{MT}(h_\phi) \subset \mathrm{CSp}(W,E)_{\mathbb{Q}}$ be the Mumford-Tate group and $\mathrm{Hg}(\phi) \subset \mathrm{Sp}(W,E)$ be the Hodge group. In above take $G = \mathrm{Hg}(\phi_0)$ to obtain a family $\mathcal{X}(\mathrm{Hg}(\phi_0),\Gamma,\rho,\phi_0)$ of fixed Hodge type. For example, if ϕ_0 defines an abelian variety of CM type, then $\mathrm{Hg}(\phi_0)$ is commutative, hence it must coincide with the centralizer subgroup of ϕ_0, hence $G = K$, and the orbit consists of one point. Now, one shows that any family of Hodge type contains an abelian variety of CM-type (a CM-point in the base of the family). The idea is simple (see [126]): any G as above contains a maximal torus defined over $\mathbb{Q}$. One takes a maximal torus T of the stabilizer subgroup K of ϕ_0, then for some $g \in G$, its conjugate gTg^{-1} must be contained in a maximal torus T' of G defined over $\mathbb{Q}$, then $\mathrm{Hg}(g\phi_0 g^{-1})$ must be contained in T', hence must be commutative. Thus, the point $g\phi_0 g^{-1}$ defines a CM-point. In fact, we have a dense set of CM-points since $G_{\mathbb{Q}}(\mathbb{Q})$ is a dense subset of $G_{\mathbb{Q}}(\mathbb{R})$, so we take the $G_{\mathbb{Q}}(\mathbb{Q})$-orbit of a CM-point to a get a dense subset of CM-points.

Thus, we see that families of Hodge type are examples of special families. Note that the converse is true, namely a family (11.1) with a CM-point is isomorphic to a family of Hodge type.

Example 11.1. In dimension ≤ 3 all Hodge families are determined by Hodge classes that define special endomorphisms of the abelian variety. The following is an example of Mumford [126] of a Hodge family not determined by a special property of endomorphism algebra of its members.

Let K/K^0 be a finite extension of fields of characteristic 0 of degree n and D be a central simple algebra over K. Recall that isomorphism classes of central simple algebras over a field F form a group, the *Brauer group* of this field. It is isomorphic to $\mathrm{H}^2(\mathrm{Gal}(\bar{F}/F), \bar{F}^*)$. The extension L/K gives rise to the natural homomorphism of group cohomology $\mathrm{Cor} : \mathrm{Br}(K) \to \mathrm{Br}(K_0)$ that assigns to D the isomorphism class of the algebra $\mathrm{Cor}_{K/K_0}(D)$ constructed as follows. Let $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$ be the set of distinct K_0-embeddings of K into its algebraic closure, then the Galois group of K acts naturally on the tensor product $E = \otimes(D \otimes_{\sigma_i} \bar{K})$ and $\mathrm{Cor}_{K/K_0}(D)$ is the

subalgebra of invariants for this action. An element d of the tensor product can be written in the form

$$d = \sum a_{i_1 \dots i_n} \sigma_1(e_{i_1}) \otimes \cdots \sigma_n(e_{i_n}),$$

where $e_1, \dots, e_{r^2}$ is a basis of D over K and $a_{i_1 \dots i_n} \in K$. An element τ of the Galois group acts by sending d to

$$\tau(d) = \sum \tau(a_{i_1 \dots i_n}) \sigma_{\tau(1)}(e_{i_1}) \otimes \cdots \sigma_{\tau(n)}(e_{i_n}),$$

where $\sigma_{\tau(i)} := \tau \circ \sigma_i$. By choosing a normal basis of L over K, one sees that Cor_{K/K_0} is a central simple algebra of degree r^{2n} over K and $\mathrm{Cor}_{K/K_0} \otimes_K \bar{K} \cong E$. It comes equipped with the norm homomorphism

$$\mathrm{Nm} : D^* \to \mathrm{Cor}_{K/K_0}(D)^* \tag{11.3}$$

that sends an invertible element $d \in D^*$ to the tensor product $(d \otimes 1) \otimes \cdots (d \otimes 1) \in E$ which is obviously invariant with respect to the action of the Galois group.

For example, if $D = K$, we obtain $\mathrm{Cor}_{K/K_0}(K) = K_0$ and the norm homomorphism is the usual norm map for field extensions.

In Mumford's example, one takes K to be a totally real cubic extension of $K_0 = \mathbb{Q}$ and D be a quaternion division algebra over K. One chooses the extension and D in such a way that

$$\mathrm{Cor}_{K/K_0}(D) \cong \mathrm{Mat}_8(\mathbb{Q}), \quad D \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{K} \oplus \mathbb{K} \oplus \mathrm{Mat}_2(\mathbb{R}),$$

where $\mathbb{K} = H((\frac{-1,-1}{\mathbb{Q}}))$ is the standard quaternion algebra over $\mathbb{Q}$. The norm map becomes a natural homomorphism $D^* \to \mathrm{GL}(8, \mathbb{Q})$.

Let $G_{\mathbb{Q}}$ be an algebraic group over $\mathbb{Q}$ such that its set of F-points is equal to $\{x \in D \otimes_{\mathbb{Q}} F)^* : xx' = 1\}$, where $x \mapsto x'$ is the standard involution of D. For example, $G_{\mathbb{Q}}(\mathbb{Q}) = D_1^* = \{x \in D^* : xx' = 1\}$. and

$$G_{\mathbb{Q}}(\mathbb{R}) = \mathbb{K}_1^* \times \mathbb{K}_1^* \times \mathrm{SL}(2, \mathbb{R}) \cong \mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SL}(2, \mathbb{R}).$$

The group $\mathrm{SU}(2) \times \mathrm{SU}(2)$ embeds naturally in $\mathrm{SU}(4)$ and hence acts on $\mathbb{C}^4$ preserving the standard Hermitian form on $\mathbb{C}^4$. Thus, it preserves its real part that gives an embedding $\mathrm{SU}(2) \times \mathrm{SU}(2) \hookrightarrow \mathrm{SO}(4)$. The group $\mathrm{SO}(4) \times \mathrm{SL}(2, \mathbb{R})$ acts naturally on the tensor product $W = \mathbb{R}^4 \otimes \mathbb{R}^2 \cong \mathbb{R}^8$ preserving the skew-symmetric form A, the tensor product of the standard symmetric bilinear form on $\mathbb{R}^4$ and the standard symplectic form on $\mathbb{R}^2$. This gives rise to a real linear representation $\rho : G_{\mathbb{Q}}(\mathbb{R}) \to \mathrm{Sp}(W, A) \cong \mathrm{Sp}(8, \mathbb{R})$ that can be shown to correspond to the norm homomorphism (11.3).

Let Λ be a lattice in $\mathbb{R}^8$ and Γ be an arithmetic subgroup of $G_{\mathbb{Q}}$ that preserves this lattice. Also, let

$$\phi_0 : \mathbb{U}(1) \to \mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SL}(2, \mathbb{R}) \subset \mathrm{Sp}(W, A), \quad e^{i\theta} \mapsto (I_2, I_2, \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right)).$$

It is clear that $\rho(G(\mathbb{R}))$ is normalized by $\phi_0(\mathbb{U}(1))$ and hence we obtain the data $(G_{\mathbb{Q}}, \Gamma, \rho, \phi_0)$ from (11.1) satisfying (11.2). This allows us to construct a Kuga family

$$\mathcal{X}(G_{\mathbb{Q}}, \Gamma, \rho, \phi_0) \to \Gamma \backslash G_{\mathbb{R}} / K_{\mathbb{R}}^0$$

of abelian 4-folds, where the base is a compact Shimura curve. The abelian varieties in the family correspond to $\rho(g)\phi_0\rho(g)^{-1} : \mathbb{U}(1) \to \mathrm{Sp}(V, A)$. Obviously, the Hodge group H containing the image of $\rho(g)\phi_0\rho(g)^{-1}$ cannot be a proper subgroup of G for all g. Hence, the Hodge group of a general member coincides with $G_{\mathbb{Q}}$. On the other hand, since the representation ρ is irreducible over $\mathbb{C}$, we obtain, for any point where the Hodge group coincides with $G_{\mathbb{Q}}$, the corresponding abelian variety does not have non-trivial endomorphisms.

11.2 The André-Oort Conjecture

The *André-Oort Conjecture* asserts that any special family is a pull-back of some family of Hodge type. We refer to [122] for a more precise and a general definition of this conjecture.

Note that a marked family $\tilde{\mathcal{X}} \to \tilde{T}$ as above defines a family of the Mumford-Tate groups $\mathrm{MT}_{\tilde{t}}$ of the Mumford-Tate groups of fibers. This gives a stratification of T by the type of the Mumford-Tate group of fibers. Since the Mumford-Tate group is determined by the set of Hodge tensors that it fixes, the loci of points with fixed Mumford-Tate group are called the *Hodge loci*. Among them are, of course, the loci of abelian varieties with some special algebra of endomorphisms (since any endomorphism give rise to a Hodge class on the self-product of the variety).

Let $f : \mathcal{C} \to T$ be a smooth family of projective curves of genus $g \geq 2$. It defines a smooth family of Jacobian varieties $\mathcal{J} \to T$ of fibers of f. One asks whether such a family can be a special family of principally polarized abelian varieties. The current conjecture is that it is possible only if $g \leq 7$ (the modified *Oort Conjecture*). In fact, a modified *Coleman Conjecture* asserts that, for $g > 7$, the locus of Jacobians in $\mathcal{A}_\}$ contains only a finitely many CM-points.

We refer for the discussion of these conjectures to excellent surveys [121] and [122]. We only discuss one example.

Example 11.2. Fix a finite group G and consider families $f : \mathcal{C} \to T$ of curves together with a faithful homomorphism $\rho : G \to \mathrm{Aut}(\mathcal{C}/T)$. We call such a G-family of curves. For example a family of curves (10.9) can be considered as such a family where the base T is the open subset of $(\mathbb{P}^1 \setminus \{\infty\}^r$ that consists of distinct points. Under the map $T \to \mathcal{M}_g$, the image is a subvariety of $\mathcal{M}_g$ of dimension $r - 2$. Similarly, one defines a G-family of polarized abelian varieties.

In general, the local deformation theory of the pair (C, G) tells us that the local dimension of the moduli space of pairs (C, G) is a smooth variety of dimension $\dim \mathrm{H}^1(C, T_C)^G = H^0(C, K_C^{\otimes 2})^G$. Note that the linear space $\mathrm{H}^1(C, T_C)$ can be naturally identified with the tangent space of the local deformation space of C. The tangent space of the local deformation space for a polarized abelian variety $A = V/\Lambda$ is naturally isomorphic to the tangent space of the corresponding point $V \in \mathsf{G}(g, \Lambda_{\mathbb{C}})_E$. The tangent space of the Grassmannian $\mathsf{G}(g, \Lambda_{\mathbb{C}})$ at the point V is naturally isomorphic to $\mathrm{Hom}(V, \Lambda_{\mathbb{C}}/V)$. If V happens to be a Lagrangian subspace with respect to a symplectic form E, then we can identify $\Lambda_{\mathbb{C}}/V$ with $V^\vee$ and one can show that the tangent space of $\mathsf{G}(g, \Lambda_{\mathbb{C}})_E$ at V is isomorphic to the symmetric square of $S^2(V^\vee) \subset \mathrm{Hom}(V, V^\vee) = V^\vee \otimes V^\vee$. In our case, $V = H^{-1,0}(A) \cong \Omega^1(A)^*$, and the tangent space becomes naturally isomorphic to the linear space of quadratic forms on $\Omega^1)(A)$. In this way, one proves that the moduli space of abelian varieties with a fixed action of a finite group G has local dimension equal to $\dim(S^2(\Omega^1(A))^*)^G$.

A G-family of principally polarized varieties is a special case of a family of Hodge type. So, it is a special family of principally polarized varieties. Thus, a G-family of Jacobian varieties is special if its dimension is equal to $\dim(S^2(\Omega^1(A))^*)^G$, where $A = \mathrm{J}(C)$ is a general member of the family. These dimensions can be computed by using a formula of Hurwitz and Chevalley-Weil (10.11). We have

$$\dim S^2(\Omega^1(\mathrm{J}(C))^*)^G = \dim S^2(\Omega^1(C)^*)^G = \dim S^2(H^{0,1}(C))^G$$

Since we know the characters of G in its representation on $H^{0,1}(C)$, we easily find

$$\dim S^2(\Omega^1(\mathrm{J}(C))^*)^G = \sum_{n=1}^{m_1} d_n d_{m-n} + \begin{cases} d_k(d_k+1)/2 & \text{if }, m = 2k \text{ is even} \\ 0 & \text{otherwise.} \end{cases}$$

The following is the Table from [121] that gives a list of 20 triples $(m, r, (a_1, \ldots, a_r)$ defining families of cyclic covers such that its image S in $\mathcal{A}_g$ under the Torelli map coincides with the locus of abelian varieties with a cyclic group action that contains S. It is proven by J. Rohde in [140] that the list is complete.

	g	m	$(a_1, \ldots, a_{r+1})$			g	m	$(a_1, \ldots, a_{r+1})$
(1)	1	2	$(1,1,1,1)$		(11)	4	5	$(1,3,3,3)$
(2)	2	2	$(1,1,1,1,1,1)$		(12)	4	6	$(1,1,1,3)$
(3)	2	3	$(1,1,2,2)$		(13)	4	6	$(1,1,2,2)$
(4)	2	4	$(1,2,2,3)$		(14)	4	6	$(2,2,2,3,3)$
(5)	2	6	$(2,3,3,4)$		(15)	5	8	$(2,4,5,5)$
(6)	3	3	$(1,1,1,1,2)$		(16)	6	5	$(2,2,2,2,2)$
(7)	3	4	$(1,1,1,1)$		(17)	6	7	$(2,4,4,4)$
(8)	3	4	$(1,1,2,2,2)$		(18)	6	10	$(3,5,6,6)$
(9)	3	6	$(1,3,4,4)$		(19)	7	9	$(3,5,5,5)$
(10)	4	3	$(1,1,1,1,1,1)$		(20)	7	12	$(4,6,7,7)$

Remark 11.3. The case (16) is especially nice. Consider a general curve C from the family as a plane quintic

$$t_2^5 = (t_1 - x_1 t_0)(t_1 - x_2 t_0)(t_1 - x_3 t_0)(t_1 - x_4 t_0)(t_1 - x_5 t_0).$$

Let L be the line $t_2 = 0$ that intersects it at 5 distinct points. Now let X' be the double cover of $\mathbb{P}^2$ branched along the union $C \cup L$:

$$X : t_3^2 + t_2^5 + f_5(t_0, t_1) = 0.$$

After we blow-up its 5 singular points from $L \cap C$, we obtain a K3 surface X whose group of automorphisms contains a non-symplectic automorphism g of order 5. The moduli space of such K3 surfaces was studied in [97]. It is isomorphic to the moduli space of cyclic covers of type (16). Both spaces are naturally isomorphic to the quotient of an open subset of a 2-dimensional ball by an arithmetic hypergeometric reflection group of type $(\frac{2}{5}, \frac{2}{5}, \frac{2}{5}, \frac{2}{5}, \frac{2}{5})$. Kondo shows that a surface X as above is a quotient of the product $D \times C$ by a cyclic group of automorphisms of order 5. The curve D is isomorphic to the genus 2 curve with an automorphism of order 5. Under the

rational projection $D \times C \dashrightarrow X$, the transcendental lattice $T_X \otimes \mathbb{Q}$, considered as a 3-dimensional vector space over $\mathbb{Q}(\zeta_5)$ becomes isomorphic to a direct summand of the rational Hodge structure on $\mathrm{H}^1(D, \mathbb{Q}) \otimes \mathrm{H}^1(C, \mathbb{Q}) \cong \mathbb{Q}(\zeta_5)^{12}$. So, our family of K3 surfaces is a special family.

Another example of the appearance of an isomorphic moduli space of K3 surfaces is the case (6) from the list. Here we consider a family of K3 surfaces birationally isomorphic to the double cover of $\mathbb{P}^2$ branched along the union of a nonsingular plane quartic curve C with equation

$$z^3 x + f_4(x, y) = 0$$

and the lines $L : z = 0$ and $M : x = 0$. The double cover has five ordinary singular points over the points in $L \cap C$ and $L \cap M$, and one singular point of type E_6 over the point $[0, 0, 1]$. The pencil of lines through the point $[0, 0, 1]$ lifted to the cover defines a pencil of elliptic curves with four reducible fibers of type IV and one reducible fiber of type $\tilde{E}_6 = IV^*$. There are no more singular fibers. After the base change to the degree 3 cover $C \to \mathbb{P}^1$, as in the case (6), ramified over the five points corresponding to the singular fibers, the elliptic fibration becomes isomorphic to the trivial fibration $E \times C \to C$. Here, E is an elliptic curve with complex multiplication by $\mathbb{Q}(\zeta_3)$. The transcendental lattice is isomorphic to $\mathsf{U}(3) \oplus \mathsf{U}(3) \oplus \mathrm{Inv}_2$. It is a free module over $\mathbb{Z}[\zeta_3]$. The surface is birationally isomorphic to the quotient $C \times E/(\sigma)$, where σ is an automorphism of order 3. It has 15 fixed points over the points $x_1, \ldots, x_4, \infty \in C$. The action at a point over x_i is locally given by $(z_1, z_2) \mapsto (\zeta_3 z_1, \zeta_3 z_2)$ that gives rise a quotient singularity of type $\frac{1}{3}(1, 1)$. The action at a point over ∞ is locally given by $(z_1, z_2) \mapsto (\zeta_3 z_1, \zeta_3^2 z_2)$ that gives rise a singular point of type A_2.

Note that, under transcendental lattice of $C \times E \to X$ is isomorphic as a $\mathbb{Z}[\zeta_3]$-module to the tensor product $\mathrm{H}^1(C, \mathbb{Z}) \otimes \mathrm{H}^1(E, \mathbb{Z}) \cong \mathbb{Z}[\zeta_3]^6$. Under the cover $C \times E \to X$, the transcendental lattice of X become a direct summand of $\mathbb{Z}[\zeta_3]^6$. This implies that the family of K3's is special, since for all CM-point in the family of curves C, the Hodge structure on the transcendental part of the corresponding K3 is also of CM-type. An example of a CM-point in the family is the curve $C : z^3 x = x^4 + y^4$ which is isomorphic to the curve

$$z^4 + x^4 - 2\sqrt{-3} x^2 y^2 + y^4 = 0$$

with automorphism group of order 48 isomorphic to $4.\mathfrak{A}_4$ (type III from Table 6.1. in [41]). The corresponding K3 surface is isomorphic to the surface

$$w^2 = (x^2 - (i+1)x^2 y^2 - i y^2)(z^4 + x^4 - 2\sqrt{-3} x^2 y^2 + y^4).$$

Note that the moduli space of K3 surfaces birationally isomorphic to the double plane

$$w^2 + xz(z^3 x + f_4(x, y)) = 0$$

is a closed subvariety of one of the three irreducible components of the moduli space of K3 surfaces with a non-symplectic automorphism of order 3. Our component is of dimension 9 and its general member has the lattice of invariant algebraic cycles isomorphic to U. It is a quotient of a 9-dimensional ball and our family is the quotient of a 2-dimensional subball.

Also we may consider the case (17). The curve is isomorphic to the plane curve of degree 7

$$z^7 = x^4 y(x - y)(x - ay).$$

Applying the Cremona transformation $[x, y, z] \mapsto [z^2, xy, xz]$ we transform this curve to a curve of degree 6

$$x^6 = yz(z^2 - xy)(z^2 - axy).$$

The curve has one triple point $[0, 1, 0]$ and one double point infinitely near to the triple point. So, its genus is equal to 6, as it should be. Now we can consider the double cover of the plane branched along this sextic curve

$$w^2 + x^6 + yz(z^2 - xy)(z^2 - axy) = 0.$$

The cyclic group (ζ_7) acts by $[x, y, z, w] \mapsto [\zeta_7^2 x, y, \zeta_7 z, \zeta_7^6 w]$. Its minimal resolution is a K3 surface with a non-symplectic automorphism of order 7. The pencil of lines in the plane through the point $[0, 1, 0]$ defines an elliptic pencil on X with two reducible fibers of type $I_0^* = \tilde{D}_4$ and IV, and 12 singular fibers of type I_1. The transcendental lattice is of rank 14, so that the Hodge structure $(T_X)_{\mathbb{Q}}$ is a 2-dimensional linear space over the field $\mathbb{Q}(\zeta_7)$. This shows that the moduli space of such surfaces is a modular curve $\Gamma\backslash\mathfrak{H}$ embedded in the moduli space of lattice polarized K3 surfaces.

Finally, we refer to [108] for some recent advance on the existence of special families of Jacobian varieties. This is based on the characterizations of families $f : X \to T$ of abelian varieties achieving the *Arakelov's bound* for the slope of the sheaf $f_*\Omega^1_{X/T}$. In particular, the authors prove the non-existence of special families of hyperelliptic Jacobians of genus $g \geq 8$. Special families of hyperelliptic curves of genus 3 and curves of genus 4 were constructed in [62], [63] and in [108].

Special family of abelian varieties must define a geodesic subvariety in $\mathcal{A}_g$. A recent paper [29] studies totally geodesic submanifolds of $\mathcal{A}_g$ that are contained in the Jacobian locus.

Bibliography

[1] M. Alsina, P. Bayer, Quaternion Orders, Quadratic Forms, and Shimura Curves. CRM Monograph Series **22**, American Mathematical Society, Providence, RI, 2004

[2] N. Aoki, *Hodge cycles on CM abelian varieties of Fermat type*. Comment. Math. Univ. St. Paul. **51** (2002), 99–130.

[3] M. Artebani, *Heegner divisors in the moduli space of genus three curves*, Trans. Amer. Math. Soc. **360** (2008), 1581–1599.

[4] R. Auffarth, *Elliptic curves on abelian varieties*, Ph. D. Thesis, Pontifica Universidad Católica de Chile, 2014.

[5] F. Bardelli, A. Del Centina, *Bielliptic curves of genus three: canonical models and moduli space*. Indag. Math. (N.S.) **10** (1999), 183–190.

[6] W. Barth, *Abelian surfaces with (1,2)-polarization*. Algebraic geometry, Sendai, 1985, 41–84, Adv. Stud. Pure Math., 10, North-Holland, Amsterdam, 1987.

[7] Barth, W., Hulek, K., Peters, C., Van de Ven: A.: Compact complex surfaces. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer–Verlag, Berlin (2004)

[8] P. Bayer, J. Guàrdia, *On equations defining fake elliptic curves*. J. Théor. Nombres Bordeaux **17** (2005), 57–67.

[9] A. Beauville, *Le théorème de Torelli pour les surfaces de Kummer*. Geometry of K3 surfaces: moduli and periods (Palaiseau, 1981/1982). Astérisque No. 126 (1985), 99–110.

[10] S.-M. Belcastro, *Picard lattices of families of K3 surfaces*. Comm. Algebra **30** (2002), no. 1, 61–82.

[11] G. V. Belyi, *Another proof of the three points theorem*. Sbornik: Mathematics **193:3** (2002), 329–332.

[12] A. Besser, *Elliptic fibrations of K3 surfaces and QM Kummer surfaces*. Math. Z. **228** (1998), 283–308.

[13] C. Birkenhake, H. Wilhelm, *Humbert surfaces and the Kummer plane*. Trans. Amer. Math. Soc. **355** (2003), 1819–1841.

[14] F.A. Bogomolov, *Points of finite order on an Abelian variety*. Math. USSR-Izv. **17:1** (1981), 55–72.

[15] O. Bolza, *Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen θ-Functionen*, Math. Ann., **30** (1887), 478–495.

[16] Z. Borevich, I. Shafarevich, *Number theory*. Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London, 1966.

[17] M. Borovoi, *The Hodge group and the algebra of endomorphisms of an abelian variety*. (Russian) Problems in group theory and homological algebra, 124–126, Yaroslavl. Gos. Univ., Yaroslavl, 1981; English translation arXiv:1310.5236 [math.AG].

[18] N. Bourbaki, *Éléments de mathématique. Algébre. Chapitre 8. Modules et anneaux semi-simples*. Second revised edition of the 1958 edition. Springer, Berlin, 2012.

[19] C. Bramble, *A collineation group isomorphic to the group of double tangents to the plane quartic*, Amer. J. Math. **40** (1918), 351–365.

[20] H. Burhardt, *Untersuchen aus dem Gebiete der hyperelliptischen Modulfunctionen Erste Theil*, Math. Ann. **36** (1869), 371–434.

[21] C. H. Clemens, *A scrapbook of complex curve theory*. Second edition. Graduate Studies in Mathematics, 55. American Mathematical Society, Providence, RI, 2003.

[22] A. Clingher, Ch. Doran, *Modular invariants for lattice polarized K3 surfaces*. Michigan Math. J. **55** (2007), 355–393.

[23] A. Clingher, Ch. Doran, *Lattice polarized K3 surfaces and Siegel modular forms*. Adv. Math. **231** (2012), 172–212.

[24] Coble, A.: *Algebraic geometry and theta functions*. Amer. Math. Soc. Coll. Publ. vol. 10, Providence, R.I. (1929; 4d ed., 1982).

[25] T. Cohen, *A Comitant Curve of the Plane Quartic*. Amer. J. Math. 39 (1917), no. 3, 221–232.

[26] T. Cohen, *The Asymptotic Equation and Satellite Conic of the Plane Quartic*. Amer. J. Math. 38 (1916), no. 3, 325–336.

[27] T. Cohen, *Investigations on the Plane Quartic*. Amer. J. Math. 41 (1919), no. 3, 191–211.

[28] E. Colombo, B. van Geemen, E. Looijenga, *Del Pezzo moduli via root systems*. Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, 291-–337. Progr. Math., **269**. Birkhäuser Boston, Ltd., Boston, MA, 2009

[29] E. Colombo, P. Frediani, A. Ghigi, *On totally geodesic submanifolds in the Jacobian locus*, Internat. J. Math. **26** (2015), no. 1, 1550005, 21 pp.

[30] A. Comessatti, *Sulle superficie di Jacobi simplicimente singolari.* Mem. Ital. delle Scienze (dei XL) (3), **21** (1919), 45–71.

[31] G. Cornell and J. H. Silverman (editors), Arithmetic geometry (Conf., Storrs, Conn., 1984), Springer-Verlag, 1986.

[32] F. Cossec, I. Dolgachev, C. Liedtke, *Enriques surfaces I*, Springer, 2024 (to appear).

[33] E. Dardanelli, B. van Geemen, *Hessians and the moduli space of cubic surfaces*. Algebraic geometry, 17–36, Contemp. Math., 422, Amer. Math. Soc., Providence, RI, 2007.

[34] O. Debarre, *Annulation de theta constantes sur les variétés abéliennes de dimension quatre*. C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), no. 20, 885–888.

[35] O. Debarre, *Complex tori and abelian varieties*. Translated from the 1999 French edition by Philippe Mazaud. SMF/AMS Texts and Monographs, 11. American Mathematical Society, Providence, RI; Société Mathématique de France, Paris, 2005

[36] P. Deligne, *Théorie de Hodge II*. Publ. Math. IHES **40** (1971), 5–57.

[37] P. Deligne, *Travaux de Shimura*. Séminaire Bourbaki, 23éme année (1970/71), Exp. No. 389, pp. 123–165. Lecture Notes in Math., Vol. 244, Springer, Berlin, 1971.

[38] M. Demazure, *Surfaces de Del Pezzo* II,III,IV,V. Lecture Notes in Math. **777** (1980), 23–69.

[39] I. Dolgachev, *Lectures on invariant theory*. London Mathematical Society Lecture Note Series, 296. Cambridge University Press, Cambridge, 2003.

[40] I. Dolgachev, S. Kondō, *Moduli of K3 surfaces and complex ball quotients*. Arithmetic and geometry around hypergeometric functions, 43–100, Progr. Math., 260, Birkhäuser, Basel, 2007.

[41] I. Dolgachev, *Classical algebraic geometry. A modern view*. Cambridge University Press, Cambridge, 2012

[42] I. Dolgachev, *Mirror symmetry of lattice polarized K3 surfaces*, Journal of Math. Sciences, **81** (1996), 259–2630

[43] I. Dolgachev, *O*n certain families of elliptic curves in projective space, Ann. Mat. Pura Appl. (4), 1983 (2004), 317-313

[44] I. Dolgachev, D. Ortland, *Point sets in projective spaces and theta functions*. Astérisque **165** (1986).

[45] L. Dornhoff, *Group Representation Theory*, Part A. Marcel Dekker, Inc. New York, 1971.

[46] T. Ekedahl, J.-P. Serre, *Exemples de courbes algébriques à jacobienne complètement décomposable*. C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 5, 509–513.

[47] F. Galluzzi, G. Lombardo, *Correspondences between K3 surfaces. With an appendix by Igor Dolgachev*. Michigan Math. J. **52** (2004), 267–277.

[48] N. Elkies, *The Klein quartic in number theory*. The eightfold way, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[49] G. Faltings, *Arakelov's theorem for abelian varieties*. Invent. Math.**73** (1983), 337–347.

[50] G. Faltings, *Endlihkeitssätze für abelshe Varietäten über Zählkorpern*. Invent. Math. **73** (1983), 349–366; Erratum **75** (1984), 381. English translation in [31].

[51] G. Faltings, *Complements to Mordell*. In: G. Faltings and G. W'ustholz (editors), Rational points Vieweg & Sohn, Braunshweig, 1984; 2nd ed., 1986.

[52] G. Faltings and G. Wüstholz (editors), Rational points Vieweg & Sohn, Braunshweig, 1984; 2nd ed., 1986.

[53] G. Faltings, *Arithmetische Kompaktifizierung des Modulraums der abelschen Varietäten*. Lecture Notes in Math. **1111** Springer-Verlag, Berlin, 1985.

[54] W. Feit, *The computations of some Schur indices*. Israel J. Math. 46 (1983), no. 4, 274-–300.

[55] R. Fricke, *Die Elliptischen Funktionen und ihre Anwendungen*, Teubner (1922).

[56] R. Fricke, Lehrbuch der Algebra, B. 3. Braunschweig. 1926.

[57] W. Fulton, *Intersection theory*. Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 2. Springer-Verlag, Berlin, 1998.

[58] Pj. Gille, T. Szamuelly, *Central Simple Algebras and Galois Gohomology*, 2nd edition. Cambridge studies in Advanced Mathematics **165**, Cambridge University Press, 2017.

[59] E. Goursat, *Sur la réduction des integrales hyperelliptiques*, Bull. Soc. Math. France, **13** (1885), 143–162.

[60] V. Gritsenko, V. Nikulin, *Igusa modular forms and "the simplest" Lorentzian Kac-Moody algebras*. Mat. Sb. 187 (1996), no. 11, 27–66; translation in Sb. Math.**187** (1996), 1601–1641.

[61] V. Gritsenko, K. Hulek, *Minimal Siegel modular threefolds*. Math. Proc. Cambridge Philos. Soc. **123** (1998), 461–485.

[62] S. Grushevsky, M. Möller. *Shimura curves within the locus of hyperelliptic Jacobians in genus three*, Int. Math. Res. Not. IMRN 2016, no. 6, 1603-–1639

[63] S. Grushevsky, M. Möller, *Explicit formulas for infinitely many Shimura curves in genus 4*. Asian J. Math. 22 (2018), no. 2, 3810–390.

[64] J. Gutierrez, T. Shaska, *Hyperelliptic curves with extra involutions*. LMS J. Comput. Math. **8** (2005), 102–115.

[65] R. Hartshorne, Algebraic Geometry, GTM **52**, Springer-Verlag, 1977.

[66] K. Hashimoto, N. Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*. Tohoku Math. J. (2) **47** (1995), 271–296.

[67] K. Hashimoto, *Explicit form of quaternion modular embeddings.* Osaka J. Math. **32** (1995), no. 3, 533-–546.

[68] K. Hashimoto, *Period map of a certain K3 family with an S_5-action. With an appendix by Tomohide Terasoma*. J. Reine Angew. Math. **652** (2011), 1–65.

[69] T. Hayashida, M. Nishi, *Existence of curves of genus two on a product of two elliptic curves*. J. Math. Soc. Japan **17** (1965), 1–16.

[70] J. Hutchinson, *The Hessian of the cubic surface. II*. Bull. Amer. Math. Soc. **6** (1900), 328–337.

[71] F. Hirzenbuch, *The ring of Hilbert modular forms for real quadratic fields in small discriminant. Modular functions of one variable*, VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 287–323. Lecture Notes in Math., Vol. 627, Springer, Berlin, 1977.

[72] F. Hirzebruch, A. Van de Ven, *Hilbert modular surfaces and the classification of algebraic surfaces*. Invent. Math. **23** (1974),1–29.

[73] F. Hirzebruch, *The Hilbert modular group for the field Q(Ã5), and the cubic diagonal surface of Clebsch and Klein*. (Russian) Translated from the German by Ju. I. Manin. Uspehi Mat. Nauk **31** (1976), no. 5(191), 153–166.

[74] S. Hosono, B.-H. Lian, K. Oguiso, S.-T. Yau, *Kummer structures on K3 surface: an old question of T. Shioda*. Duke Math. J. **120** (2003), 635–647.

[75] K. Hulek, H. Lange, *The Hilbert modular surface for the ideal $(\sqrt{5})$ and the Horrocks-Mumford bundle*. Math. Z. **198** (1988), 95–116.

[76] K. Hulek, C. Kahn, S. Weintraub, *Moduli spaces of abelian surfaces: compactification, degenerations, and theta functions*. de Gruyter Expositions in Mathematics, 12. Walter de Gruyter and Co., Berlin, 1993.

[77] J.-I. Igusa, *On Siegel modular forms of genus two*. Amer. J. Math. **84** (1962), 175–200.

[78] J.-I. Igusa, *Modular forms and projective invariants*. Amer. J. Math. **89** (1967), 817–855.

[79] J.-I. Igusa, *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. Springer-Verlag, New York-Heidelberg, 1972.

[80] H. Inose, *Defining equations of singular K3 surfaces and a notion of isogeny*. Proc. International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977), pp. 495–502, Kinokuniya Book Store, Tokyo, 1978.

[81] N. Jacobson, *Lie Algebras*. Dover Publications, Inc., New York, 1979.

[82] G. Janusz, *Simple components of $\mathbb{Q}[\mathrm{SL}(2,q)]$*, Comm. Algebra **1** (1974), 1–22.

[83] E. Kani, W. Schanz, *Modular diagonal quotient surfaces*. Math. Z. **227** (1998), 337–366.

[84] E. Kani, *Hurwitz spaces of genus 2 covers of an elliptic curve*. Collectanea Math. **54** (2003), 1–51.

[85] H. Karcher, M. Weber, *The geometry of Klein's Riemann surface*. The eightfold way, 9–49, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge, 1999.

[86] T. Katsura, *On the structure of singular abelian varieties*, Proc. Japan Acad. **51** (4) (1975), 224–228.

[87] T. Katsura, T. Katsura, *On Fermat varieties*. Tohoku Math. J. (2) **31** (1979), 97–115.

[88] G. Kempf, *Complex abelian varieties and theta functions*. Universitext. Springer-Verlag, Berlin, 1991.

[89] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*, Leipzig, Teubner, 1884 [English translation by G. Morrice, Diover Publ. 1956; German reprint edited by P. Slodowy, Basel, Birkhüser, 1993].

[90] F. Klein, *Über die Transformationen elder Ordnung der elliptischen Funktionen*, Math. Ann. **15** (1879).

[91] M. Kneser, *Klassenzahlen definiter quadratischer Formen*. Arch. der Math. **8** (1957), 241–250.

[92] R. Kobayashi, K. Kushibiki, I. Naruki, *Polygons and Hilbert modular groups*. Tohoku Math. J. (2) **41** (1989), 633–646.

[93] N. Koblitz, D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*. Canad. J. Math. **30** (1978), 1183–1205.

[94] S. Kondō, *Automorphisms of algebraic K3 surfaces which act trivially on Picard groups*. J. Math. Soc. Japan 44 (1992), no. 1, 75–98.

[95] S. Kondō, *A complex hyperbolic structure for the moduli space of curves of genus three*. J. Reine Angew. Math. **525** (2000), 219–232.

[96] S. Kondō, *The moduli space of 5 points on $\mathbb{P}^1$ and K3 surfaces*. Arithmetic and geometry around hypergeometric functions, 189–206, Progr. Math., 260, Birkhäuser, Basel, 2007.

[97] S. Kondō, *Moduli of plane quartics, Göpel invariants and Borcherds products*. Int. Math. Res. Not. IMRN **2011** (2011), 2825–2860.

[98] S. Kowalevski, *Über Reduction einer bestimmten Klasse Abelscher Integrale 3ten Ranges auf elliptische Integrale*, Acta Mathematica **4**, (1884), 393-416.

[99] A. Kumar, *K3 surfaces associated with curves of genus two*. Int. Math. Res. Not. IMRN 2008, no. 6, Art. ID rnm165, 26 pp.

[100] A. Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, arXiv:1412.2849.

[101] T. Y. Lam, *A first course in noncommutative rings* Grad. Texts in Math., 131 Springer-Verlag, New York, 2001.

[102] S. Lang, *Abelian varieties*. Reprint of the 1959 original. Springer-Verlag, New York-Berlin, 1983.

[103] S. Lang, *Introduction to Algebraic and Abelian Functions*, 2nd edition. Springer-Verlag New York Inc., 1982.

[104] S. Lang, *Fundamentals of Diophantine Geometry*. Springer-Verlag, New York-Berlin, 1983.

[105] H. Lange, *Jacobian surfaces in P^4*. J. Reine Angew. Math. **372** (1986), 71–86.

[106] H. Lange, C. Birkenhake, *Complex abelian varieties*. Second edition. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 302. Springer-Verlag, Berlin, 2004

[107] R. Livné, M. Schütt, N. Yui, *The modularity of K3 surfaces with non-symplectic group actions*. Math. Ann. **348** (2010), 333–355.

[108] X. Lu, K. Zuo, *The Oort conjecture on Shimura curves in the Torelli locus of curves*. J. Math. Pures Appl. (9) 123 (2019), 41-–77.

[109] S. Ma, *On K3 surfaces which dominate Kummer surfaces*. Proc. Amer. Math. Soc. **141** (2013), 131–137.

[110] K. Magaard, T. Shaska, H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*. Forum Math. **21** (2009), 547–566.

[111] Yu. I. Manin, *The Mordell-Weil Theorem*. Appendix to [127].

[112] Yu.I. Manin, *Cubic forms*, 2nd edition. North Holland, Amsterdam, 1986.

[113] C. McMullen, *Dynamics of $SL_2(R)$ over moduli space in genus two*. Ann. of Math. (2) **165** (2007), 397–456

[114] A. Mehran, *Double covers of Kummer surfaces*. Manuscripta Math. **123** (2007), 205–235.

[115] A. Mehran, *Kummer surfaces associated to (1,2)-polarized abelian surfaces*. Nagoya Math. J. **202** (2011), 127–143.

[116] J. Milne, *Complex multiplication*, http://www.jmilne.org/math/CourseNotes/cm.html.

[117] J. Milne, *Notes on Shimura varieties*, http://www.jmilne.org/math/xnotes/svh.pdf

[118] J. Milne, *Jacobian varieties*, Arithmetic geometry. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. Edited by Gary Cornell and Joseph H. Silverman. Springer-Verlag, New York, 1986

[119] J. Milne, *Elliptic curves*. Second edition. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, [2021], ©2021

[120] J. Milnor, D. Husemoller, *Symmetric bilinear forms*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. Springer-Verlag, New York-Heidelberg, 1973

[121] B. Moonen, *Special subvarieties arising from families of cyclic covers of the projective line*. Doc. Math. **15** (2010), 793–819.

[122] B. Moonen, F. Oort, *The Torelli locus and special subvarieties*, Handbook of moduli. Vol. II, 549–594, Adv. Lect. Math. (ALM), 25, Int. Press, Somerville, MA, 2013.

[123] D. Morrison, *On K3 surfaces with large Picard number*. Invent. Math. **75** (1984), 105–121.

[124] B. Mortimer, *The modular permutation representations of of the known doubly transitive oermutation groups*. Proc. London Math. Soc. (3) **41** (1980), 1–20.

[125] S. Mukai, *On the moduli space of bundles on K3 surfaces. I*. Vector bundles on algebraic varieties (Bombay, 1984), 341–413, Tata Inst. Fund. Res. Stud. Math., 11, Tata Inst. Fund. Res., Bombay, 1987.

[126] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*. Math. Ann. **181** (1969), 345–351.

[127] D. Mumford, *Abelian varieties*, 2nd edition. Oxford University Press, 1974.

[128] D. Mumford, *Tata Lectures on Theta II*. Progress in Math. vol. **43** Birkhäuser, Boston, 1984.

[129] N. Murabayashi, *The moduli space of curves of genus two covering elliptic curves*. Manuscripta Math. **84** (1994), 125–133.

[130] N. Murabayashi, A. Umegaki, *Determination of all Q-rational CM-points in the moduli space of principally polarized abelian surfaces*. J. Algebra **235** (2001), 267–274.

[131] N. Murabayashi, *Determination of simple CM abelian surfaces defined over Q*. Math. Ann. **342** (2008), 657–671.

[132] V. Nikulin, *Kummer surfaces*. Izv. Akad. Nauk SSSR Ser. Mat. **39**, 278–293 (1975).

[133] V. Nikulin, *Integral quadratic forms and some of its geometric applications*, Izv. Akad. nauk SSSR, Ser. Math. **43** (1979), 103–167.

[134] H. Ohashi, *Hutchinson-Weber involutions degenerate exactly when the Jacobian is Comessatti*. Publ. Res. Inst. Math. Sci. **48** (2012), 107–127.

[135] A. L.Onischik, E.B. Vinberg, *Lie groups and algebraic groups*. Translated from the Russian and with a preface by D. A. Leites. Springer Series in Soviet Mathematics. Springer-Verlag, Berlin, 1990

[136] R. Pierce, Associative Algebras. GTM **88**, Springer-Verlag, New York Heidelberg Berlin, 1982.

[137] H. Pinkham, *Résolution simultanée de points double rationells*. Singularités de surfaces. Lect. Notes in Math. **777**, pp. 179–203, Springer–Verlag (1979)

[138] V. Popov, Yu. Zarhin, *Finite linear groups, lattices, and products of elliptic curves*. J. Algebra **305** (2006), 562–576.

[139] A. Popolitov, S. Shakirov, *On Undulation Invariants of Plane Curves*, arXiv:1208.5775.

[140] J. Rohde, *Cyclic coverings, Calabi-Yau manifolds and complex multiplication*. Lecture Notes in Mathematics, 1975. Springer-Verlag, Berlin, 2009.

[141] X. Roulleau, *The Fano surface of the Klein cubic threefold*. J. Math. Kyoto Univ. 49 (2009), no. 1, 113-–129.

[142] W. Ruppert, *Two-dimensional complex tori with multiplication by* $\sqrt{d}$. Arch. Math. (Basel) **72** (1999), 278–281.

[143] W. Ruppert, *When is an abelian surface isomorphic or isogenous to a product of elliptic curves?* Math. Z. **203** (1990), 293–299.

[144] G. Salmon, *Lessons introductory to the modern higher algebra*, Hodges, Foster and Co. Dublin. 1876 (5th edition), reprinted by Nabu Press, 2010.

[145] A. Sarti, *Group actions, cyclic coverings and families of K3-surfaces*. Canad. Math. Bull. **49** (2006), 592–608.

[146] A. Sarti, *Transcendental lattices of some K3-surfaces*. Math. Nachr. **281** (2008), 1031–1046.

[147] F. Scattone, *On the compactification of moduli spaces for algebraic K3 surfaces*. Mem. Amer. Math. Soc. 70 (1987), no. 374.

[148] J.-P. Serre, *Cours de Arithmétique*, Pres. Univ. de France, Paris, 1970.

[149] J.-P. Serre, *Linear representations of finite groups*. GTM **42**, Springer-Verlag, New York, Inc. 1977.

[150] J.-P. Serre, *Bounds for the orders of the finite subgroups of G(k)*. EPFL Press, Lausanne; distributed by , 2007, 405—450.

[151] J.-P. Serre, *Finite Groups: An Introduction*, second revised edition. International Press, 2022.

[152] I. Pyatetskij-Shapiro, I. Shafarevich, *Arithmetic of K3 surfaces*, Proceedings of the International Conference on Number Theory (Moscow, 1971). Trudy. Mat. Inst. Steklova, **132** (1973), 44–54.

[153] C. Schoen, *Produkte Abelscher Varietäten und Moduln über Ordnungen*, J. Reine Angew. Math. **429** (1992) 115–123.

[154] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*. Forum Math. **16** (2004), 263–280.

[155] G. Shimura, *Abelian varieties with complex multiplication and modular functions*. Princeton University Press, 1998.

[156] T. Shioda, N. Mitani, *Singular abelian surfaces and binary quadratic forms*. In: Classification of Algebraic and Compact Complex Manifolds, Lecture Notes in Math., vol. **412**, Springer-Verlag, 1974, pp. 259–287.

[157] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*. J. Pure Applied Algebra **77** (1992), 253–262.

[158] J. Silverman, *The arithmetic of elliptic curves*. Second edition. Graduate Texts in

[159] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Graduate Texts in Mathematics **151**. Springer-Verlag, New York, 1994.

[160] I. Shimada, *A construction of algebraic curves whose Jacobians have non-trivial endomorphisms*. Comment. Math. Univ. St. Paul. **43** (1994), 25–34.

[161] T. Shioda, *Kummer sandwich theorem of certain elliptic K3 surfaces*. Proc. Japan Acad. Ser. A Math. Sci. **82** (2006), 137–140.

[162] M. Suzuki, *Group Theory I*. Springer-Verlag, 1982.

[163] L. Szpiro (editor), Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell. Astérisque **127**. Soc. Math. France, Paris, 1985.

[164] T. Terasoma, *A Hecke correspondence on the moduli of genus 2 curves*. Comment. Math. Univ. St. Paul. **36** (1987), 87–115.

[165] T. Terasoma, *Infinitesimal variation of Hodge structures and the weak global Torelli theorem for complete intersections*. Ann. of Math. (2) **132** (1990), 213–235.

[166] G. van der Geer, *On the geometry of a Siegel modular threefold*. Math. Ann. **260** (1982), 317–350.

[167] G. van der Geer, *Hilbert modular surfaces*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 16. Springer-Verlag, Berlin, 1988

[168] R. Varley, *Weddle's surfaces, Humbert's curves, and a certain 4-dimensional abelian variety*. Amer. J. Math. **108** (1986), 931–952.

[169] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, 800. Springer, Berlin, 1980.

[170] J. Voight, *Quaternion algebras*. GTM **288**, Springer Cham, 2021.

[171] C. Voisin, *Hodge theory and complex algebraic geometry. I-II*. Translated from the French by Leila Schneps. Reprint of the 2002 English edition. Cambridge Studies in Advanced Mathematics, 76. Cambridge University Press, Cambridge, 2007.

[172] S. Vorontsov, *Automorphisms of even lattices arising in connection with automorphisms of algebraic K3-surfaces*. Vestnik Moskov. Univ. Ser. I Mat. Mekh. (1983), no. 2, 19–21.

[173] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*. Math. Comp. **68** (1999), 307–320

[174] A. Weil, Zum Beweis des Torellischen Satzes. Nachr. Akad. Wiss. Göttingen **2** (1957), 33–53; reprinted in ÖEvres **II** [1957a], Springer-Verlag, New York Heidelberg Berlin, 1980.

[175] What is a good roadmap for learning Shimura curves? https://mathoverflow.net/questions/11219/what-is-a-good-roadmap-for-learning-shimura-curves .

[176] Yu. G. Zarhin, *Hodge groups of K3 surfaces*. J. Reine Angew. Math. **341** (1983), 193–220.

[177] Yu. G. Zarhin, A.N. Parshin, *Finiteness problems in Diophantine Geometry*. In: "Eight papers translated from the Russian", AMS Translations, Series 2, Vol. **143**; arXiv:0912.4325 [math.NT].

[178] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Research Letters **7** (2000), 123–132.

[179] Yu. G. Zarhin, *Cyclic covers, their jacobians and endomorphisms*. J. reine angew. Math. **544** (2002), 91–110.

[180] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (C. Faber, G. van der Geer, R Oort, eds.), pp. 473–490, Progress in Math., Vol. **195**, Birkhauser, Basel-Boston-Berlin, 2001.

[181] Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. Proceedings of the Steklov Institute of Mathematics **241** (2003), 90–104.

[182] Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.

[183] Yu. G. Zarhin, *Very simple representations: Variations on a theme of Clifford*. In: Progress in Galois Theory, Springer Science, 2005.

[184] Yu. G. Zarhin, *Del Pezzo surfaces of Degree 2 and jacobians without Complex multiplication*. Amer. Math. Soc. Transl. (2) **218** (2006), 67–75; arXiv:math/0405156 [math.AG].

[185] Yu. G. Zarhin, *Del Pezzo surfaces of Degree 1 and Jacobians*. Math. Annalen **340** (2008), 407–435; arXiv:math/0605592 [math.AG].

[186] Yu. G. Zarhin, *Isogeny classes of abelian varieties over function fields*. Proc. Lond. Math. Soc. (3) **96** (2008), 312–334.

[187] Yu. G. Zarhin, *Endomorphisms of abelian varieties, cyclotomic extensions, and Lie algebras*. Sb. Math. **201** (2010), 1801–1810.

[188] Yu. G. Zarhin, *Complex tori, theta groups and their Jordan properties*. Proceedings of the Steklov Institute of Mathematics **307** (2019), 22–50.

[189] Yu. G. Zarhin, *Halves of points of an odd degree hyperelliptic curve in its jacobian*. In: Integrable Systems and Algebraic Geometry (R. Donagi, T. Shaska, eds.). Cambridge University Press: LMS Lecture Notes Series, Volume 2: Algebraic Geometry, 2020, pp. 102–118.

[190] Yu. G. Zarhin, *On matrices of endomorphisms of abelian varieties*. Math. Research Reports **1** (2020), 55–68.

[191] Yu. G. Zarhin, *Non-isogenous elliptic curves and hyperelliptic jacobians*. Math. Research Letters **30** (2023), no. 1, 267–294.

[192] Yuri Zarhin, Answer to "A possible gap in Faltings note to prove the Tate conjecture for finitely generated field over $\mathbb{Q}$". URL (version: 2022-09-06): https://mathoverflow.net/q/429849

[193] Yu. G. Zarhin, *Superelliptic jacobians and central simple representations*. arXiv:2305.12022 [math.NT].

Index