The Conjecture of André-Oort and Diophantine Approximations

G. Wüstholz 24.04..2012

Contents

1 Introduction and Motivation

In this series of lecture we shall give the necessary background for studying and understanding the André-Oort conjecture. The conjecture can be stated for arbitrary Shimura varieties. We restrict ourselves however to simple cases which need only some classical mathematical background. We begin with studying the situation when the underlying Shimura variety is of the simplest possible form, namely a product $\mathbb{P}^1 \times \mathbb{P}^1$ of two projective lines. However here we meet already the prototype of the problem. The space $\mathbb{P}^1 \times \mathbb{P}^1$ can be seen as the space classifying those abelian surfaces which are products of two elliptic curves. To understand this moduly space, as it is called, we shall briefly introduce the concept of elliptic curves together with the concept of complex multiplication.

The next step in the complexity of the problem will be to replace the product of two elliptic curves by arbitrary abelian surfaces and study their moduli space $\mathcal{S}_2$ which is the Siegel upper half plane $\mathbb{H}_2$ consisting of complex 2×2-matrices subject to some extra condition and taken modulo the symplectic group $\mathrm{Sp}(4, \mathbb{Z})$. The Siegel upper half plane has dimension $\frac{n^2+n}{2}$ for general n which becomes 3 in the case of $\mathcal{S}_2$ and the real dimension of $\mathrm{Sp}(2n, \mathbb{R})$ is $n(2n+1)$ which is 10 when n=2. Again we shall briefly introduce this space and this gives our second example. Its points classify isomorphism classes of abelian varieties of dimension 2, so-called abelian surfaces which we shall also introduce in an elementary way.

The space $\mathbb{P}^1 \times \mathbb{P}^1$ mentioned above is a very particular case for such a moduli space and sits as an algebraic surface in $\mathcal{S}_2$. Another example to which will shall pay some attention are the famous Hilbert modular surfaces which were introduced and first studied by Hilbert. They classify abelian surfaces with a special type of endomorphism algebra which appears as a particular case in the classification theory of the endomorphism algebra of an abelian variety. There are four possible types which were found by Albert when establishing the classification. Going through the classification one sees that each class Φ of endomorphism algebras gives rise to a subvariety $\mathcal{S}_\Phi$ of $\mathcal{S}_2$. There are infinitely many such subspaces which are called Shimura (sub-)varieties. We shall carefully and in an elementary way introduce these objects and this then lays the ground for looking into the original conjecture of André-Oort.

The conjecture gives some very interesting statement about the geometric nature of the Zariski closure of a set, finite or infinite, of Shimura subvarieties of $\mathcal{S}_2$. When the Shimura subvarieties are all of dimension zero and then are just points in $\mathcal{S}_2$ we are in the situation of the original conjecture. It will turn out that the addressed closure will be again a finite coillection of Shimura subvarieties. This is in our situation the upshot of the conjecture of André-Oort.

In these lectures we shall explain the conjecture but not go into any detailed proof of it. There are several reasons. The conjecture is only proved in the case of the Shimura variety $\mathbb{P}^1 \times \mathbb{P}^1$ and there is so far no proof in the general situation. In the $\mathbb{P}^1 \times \mathbb{P}^1$-case there are three very different approaches which are all too involved as on can go into them in short time. One is by André, one by Pila and one by Kühne. The first two proofs are not effective whereas Kühne's proof relies on the Baker Theory and is fully effective. We leave it then to Kühne to give in a later lecture some account of his proof. In the case of arbitrary dimension one only knows that the Generalized Riemann Hypothesis implies the André-Oort conjecture. This has been shown in a paper by Yafaev and Klingler which however is since years in the refereeing process. But it is unknown whether the hypothesis is true or not.

2 Elliptic Curves

Elliptic curves belong to the simplest on the one side and on the other side richest geometric structures in mathematics. They come up in almost every mathematical subjects.

To define them we take the complex plane $\mathbb{C}$ and in it a lattice. This is a free and abelian subgroup of the form $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ of $\mathbb{C}$ which generates $\mathbb{C}$ over the reals. To give a lattice is the same as to give a group homomorphism $\omega : \mathbb{Z}^2 \longrightarrow \mathbb{C}$ such that if e_1, e_2 denotes the standard basis for $\mathbb{Z}^2$ then the imaginary part of ω_1/ω_2 is different from 0 for $\omega_1 = \omega(e_1)$ and $\omega_2 = \omega(e_2)$. The famous Weierstrass $\wp$-function

$$\wp(z) = \wp(z;\Lambda) = \frac{1}{z^2} + \sum_{0\neq\omega\in\Lambda}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

is a meromorphic function on the complex plane with double poles on Λ and periodic with period lattice Λ. The periodicity implies that the function descends to the quotient $\mathbb{C}/\Lambda$ which is a compact complex manifold. This means that it induces on the quotient a rational function with one pole of order two at the image of 0. Together with its derivative $\wp'(z;\Lambda)$ it defines a holomorphic map, called the exponential map,

$$\begin{aligned} \exp_\Lambda : \mathbb{C} &\longrightarrow \mathbb{P}^2 \\ z &\mapsto [\wp(z) : \wp'(z) : 1] \end{aligned} \tag{1}$$

from $\mathbb{C}$ into the complex plane with image a smooth projective curve given in affine coordinates (x, y) with $\exp_\Lambda^* x = \wp(z)$ and $\exp_\Lambda^* y = \wp'(z)$ by a cubic equation, called Weierstrass normal form or Weierstrass equation,

$$y^2 = 4x^3 - g_2 x - g_3. \tag{2}$$

The exponential map is a homomorphism and has as kernel the lattice Λ. The coefficients g_2 and g_3 are functions in Λ given by the Eisenstein series

$$g_i(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \frac{1}{\omega^{2i}}. \tag{3}$$

The discriminant $\Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2$ of the cubic on the right side of (2) is different from zero and again a function of the lattice. The same is true for the very important function

$$j(\lambda) = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)}, \tag{4}$$

Klein's j-invariant, and all the four functions are functions on the space of lattices. They are homogeneous of weight 4, 6, 12 and 0 with respect to the action $(t, \Lambda) \mapsto t\Lambda$ of $\mathbb{C}^\times$ on the space of lattices $\mathcal{L}$. This means that

$$f(t\Lambda) = t^{-w(f)} f(\Lambda)$$

for any of the four functions above with $w(f)$ the weight of f. This carries over to the elliptic functions $\wp$ and $\wp'$ if the action is extended to the variable z and we get

$$\begin{aligned} \wp(tz; t\lambda) &= t^{-2} \wp(z; \Lambda) \\ \wp'(tz; t\Lambda) &= t^{-3} \wp'(z; \Lambda). \end{aligned}$$

Any two lattices Λ and Λ' are said to be isomorphic if and only if $\Lambda' = t\Lambda$ for some $t \in \mathbb{C}^\times$. This shows that we may normalize the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ such that a basis is given by $\omega_1 = \tau$ and $\omega_2 = 1$ and with imaginary part $\Im(\tau) \neq 0$. In other words τ is taken from the disjoint union $\mathfrak{H}^+ \sqcup \mathfrak{H}^-$ where $\mathfrak{H}^+$ and $\mathfrak{H}^-$ denote the upper and the lower half plane respectively. We write Λ_τ for the normalized lattice. This amounts to the same as taking the quotient $\mathcal{L}/\mathbb{C}^\times$ which then consists of isomorphism classes of lattices. The group $\mathrm{GL}(2, \mathbb{R})$ acts on $\mathcal{L}$ by mapping the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ to the lattice $\gamma\Lambda$ with basis

$$\gamma\omega_1 = a\omega_1 + b\omega_2 \tag{5}$$

$$\gamma\omega_2 = c\omega_1 + d\omega_2 \tag{6}$$

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{R})$ and the action commutes with the $\mathbb{C}^\times$-action. On the normalized lattices Λ_τ it acts through fractional linear transformations

$$\tau \mapsto \gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

so that $\gamma\Lambda_\tau = (c\tau + d)\Lambda_{\gamma(\tau)} = (\gamma\omega_2)\Lambda_{\gamma(\tau)}$. The space of lattices $\mathcal{L}$ becomes a homogeneous space under this action and can be expressed as $\mathcal{L} = \mathrm{GL}(2, \mathbb{R}) \cdot \Lambda_{\sqrt{-1}}$.

We donote by $\mathbb{R}^\times_{>0}$ the multiplicative group of positive real numbers. The isomorphism

$$\iota : \mathbb{C}^\times \to \mathbb{R}^\times_{>0} \cdot \mathrm{SO}(2, \mathbb{R})$$

which maps $z = re^{i\phi}, 0 < r, \phi \in [0, 1)$, to

$$\iota(z) = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$$

gives a representation of $\mathbb{C}^\times$ in $\mathrm{GL}(2,\mathbb{R})$ and induces by right multiplication $(z,\gamma) \mapsto \gamma \cdot \iota(z)^T$ of matrices an action of $\mathbb{C}^\times$ on $\mathrm{GL}(2,\mathbb{R})$ for which we have

$$\iota(z)\Lambda_{\sqrt{-1}} = r(\cos\phi + i\sin\phi)\Lambda_{\iota(z)(\sqrt{-1})} = z\Lambda_{\sqrt{-1}}.$$

Since $\mathrm{GL}(2,\mathbb{R})$ acts on the union of the upper and lower half-plane $\mathfrak{H}^+ \sqcup \mathfrak{H}^-$ via fractional linear transformation and since i is fixed under this action of $\mathbb{R}^\times_{>0} \cdot \mathrm{SO}(2,\mathbb{R})$ one deduces that the map $\gamma \mapsto \Lambda_{\gamma(\sqrt{-1})}$ induces an isomorphism

$$\mathrm{GL}(2,\mathbb{R})/\mathbb{R}^\times_{>0} \cdot \mathrm{SO}(2,\mathbb{R}) \longrightarrow \mathcal{L}/\mathbb{C}^\times.$$

Any lattice is fixed under the group $\mathrm{SL}(2,\mathbb{Z})$ and therefor we may further divide out the stabilizer $\mathrm{SL}(2,\mathbb{Z})$of a lattice. This leads finally to an isomorphism

$$\mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{GL}(2,\mathbb{R})/\mathbb{R}^\times_{>0} \cdot \mathrm{SO}(2,\mathbb{R}) \simeq \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{L}/\mathbb{C}^\times \tag{7}$$

and one obtains the first and very elementary example of a Shimura variety which we denote by $\mathcal{S}_1$. The result of our construction is a complex manifold.

Remark: We write $\mathrm{GL}(2,\mathbb{R})$ as

$$\mathrm{GL}(2,\mathbb{R})^+ \sqcup \left[\mathrm{GL}(2,\mathbb{R})^+\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)\right]$$

with $\mathrm{GL}(2,\mathbb{R})^+$ the subgroup of element with positive determinant which can be written as $R^\times_{>0} \cdot \mathrm{SL}(2,\mathbb{R})$ by expressing γ as $\sqrt{\det(\gamma)}\,\delta$ with $\delta = \sqrt{\det(\gamma)^{-1}}\gamma \in \mathrm{SL}(2,R)$. Then the left side of (7) becomes

$$\mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{SL}(2,R)/\mathrm{SO}(2,R) \;\sqcup\; \mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{SL}(2,R)\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)/\mathrm{SO}(2,R) \tag{8}$$

and is isomorphic to

$$\mathrm{SL}(2,\mathbb{Z})\backslash\mathfrak{H}^+ \;\sqcup\; \mathrm{SL}(2,\mathbb{Z})\backslash\mathfrak{H}^-$$

with $\mathfrak{H}^\pm$ the upper respectively the lower half-plane. The isomorphism is induced by the map which sends γ to $\gamma(i)$. $\Box$

For an arithmetic analysis we need an algebraic manifold however and it should be defined over a number field. This means that we have to find an isomorphism of the Shimura variety, which so far is only a complex manifold, with an algebraic variety. All tools which are needed for establishing such an isomorphism are already to our disposal.

3 Elliptic Moduli Space and Complex Multiplication

In this second lecture we shall enrich the purely analytic theory which has been exposed in the previous lecture by its algebraic and number theoretical aspects. The first step is to make out of the Shimura variety an algebraic variety and the second step is to define the so-called CM-points which will become crucial for stating the André-Oort conjecture. For this we need to introduce complex multiplication on elliptic curves.

In the last lecture we have already made out of an complex torus $\mathbb{C}/\Lambda$ an elliptic curve E which is a plane algebraic curve and the exponential map furnishes such an isomorphism. The curve E is defined over the field $k(E) = \mathbb{Q}(g_2, g_3)$ with g_2 and g_3 the coefficients in the equation (2).

If $k(E)$ is an algebraic number field then we say that E is defined over an algebraic number field. More generally we say that an elliptic curve E^* is defined over an algebraic number field if it is isomorphic to an elliptic curve E with $k(E) \subset \overline{\mathbb{Q}}$.

Remark : From our description we see that the Zariski open set $\mathcal{U}$ in the affine plane $\mathbb{A}^2$ with coordinates g_2 and g_3 defined by $\Delta \neq 0$ is a parameter space for elliptic curves. If we divide out the action of $\mathbb{C}^\times$ given by

$$g_i \mapsto t^{-2i} g_i$$

for $i = 2, 3$ we get basically the algebraic variety $\mathbb{P}^1 \backslash \{\infty\}$ with the Klein j-function as isomorphism from $\mathbb{C}^\times \backslash \mathcal{U}$ to $\mathbb{P}^1 \backslash \{\infty\}$. This we carry out now on the level of lattices, respectively the upper half plane.
□

As we have seen, the function $j(\Lambda)$ is a function on $\mathcal{L}$ which is invariant under the action of the subgroup $\mathbb{C}^\times \cdot \mathrm{SL}(2,\mathbb{Z})$ and induces therefor a holomorphic map

$$j : \mathcal{S}_1 = \mathbb{C}^\times \backslash \mathcal{L} / \mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathbb{P}^1. \tag{9}$$

which maps the class of Λ to $j(\Lambda)$ for any Λ in the class. It is a 2-fold covering which has two connected components. They correspond to the two half planes $\mathfrak{H}^\pm$ as mentioned earlier. Instead of $\mathcal{S}_1$ we use now the upper half plane $\mathfrak{H} = \mathfrak{H}^+$ which is the more classical notion. Then the j-function gives a holomorphic map

$$\begin{array}{rcl} j : \mathfrak{H} & \longrightarrow & \mathbb{P}^1 \\ \tau & \mapsto & j(\tau) = 1728 \, \dfrac{g_2(\tau)^3}{\Delta(\tau)} \end{array}$$

where we write $g_2(\tau)$ for $g_2(\Lambda_\tau)$ and $\Delta(\tau)$ for $\Delta(\Lambda_\tau)$. Since the function $j(\tau)$ is invariant under the action of $\mathrm{SL}(2,\mathbb{Z})$ it factors through the quotient $X_0(1) = \mathrm{SL}(2,\mathbb{Z}) \backslash \mathfrak{H}$. Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is a matrix in $\mathrm{SL}(2,\mathbb{Z})$ which acts on $\mathfrak{H}$ by $\tau \mapsto \tau + 1$ we see that $j(\tau)$ is periodic with period 1 and therefor has a Fourier expansion

$$j(q) = \frac{1}{q} + 744 + 196884q + 21499760q^2 + 864299970q^3 + \cdots = \sum_{-1}^{\infty} c(n) q^n \tag{10}$$

in $q = e^{2\pi i \tau}$ with a pole of order 1 at the "cusp" ∞ [1].

[1]It is an interesting problem to see whether the coefficients $c(n)$ can be explained conceptually. One of the surprises in mathematics was that they are indeed related to a uniquely determined sporadic simple group, called the monster group $\mathbb{M}$. Its order is

$$2^{46} 3^{20} 5^9 7^6 11^2 13^3 171923293141475971 \equiv 8 \cdot 10^{53}$$

It was observed by Conway and Norton that the integers $c(n)$ are closely related to the degrees of the finitely many irreducible representations of the monster group $\mathbb{M}$. In fact they are linear combinations with non-negative coefficients in the degrees. This observation has been verified by Borcherds. He constructed an infinite dimensional graded module

$$V_\sharp = \sum_{-1}^{\infty} V_n$$

where each V_n is a finite dimensional representation of $\mathbb{M}$ (whence a direct sum of irreducible representations

The j-function induces an isomorphism

$$J : \mathcal{S}_1 \longrightarrow \mathbb{P}^1 \backslash \{\infty\} \tag{11}$$

with $\mathbb{P}^1$ as compactification. This shows that $\mathbb{P}^1$ can be regarded as a (smooth compactification of a) Shimura variety.

We have already indicated in the Remark above thatthe algebraic way to do this construction is to start with the open set

$$\mathcal{U} : \Delta \neq 0$$

and to take the ring $\mathcal{R}$ of regular functions on $\mathcal{U}$. It can be written as the localization $\mathcal{R}$ of the polynomial ring $\mathbb{Q}[g_2, g_3]$ at the multiplicative monoid generated by $\Delta = g_2^3 - 27g_3^2$ which can be expressed as $\mathbb{Q}[g_2, g_3, \Delta^{-1}]$. We let the group $G = \mathbb{Q}^\times$ act on $\mathcal{R}$ by $g_i \mapsto t^{2i} g_i$ and $\Delta \mapsto t^{12}\Delta$ and then take the ring of invariant polynomials $\mathcal{R}^G$, this means that those polynomials $F(g_2, g_3, \Delta^{-1})$ are selected for which

$$F(t^4 g_2, t^6 g_3, t^{-12}\Delta^{-1}) = F(g_2, g_4, \Delta^{-1}).$$

Using the defining equation for Δ we see that $\mathcal{R}$ may be written as $\mathbb{Q}[g_2, g_3, \Delta^{\pm}]$ and all powers of g_3 can be reduced modulo Δ to g_3^i with $i = 0, 1$. The invariant polynomials are now those which are homogeneous with respect to the weights $4, 6$ and 12 and this means that these are the polynomials in g_2 and Δ^{-1} which are composed of monomials $g_2^i \Delta^j$ for which $4i = -12j$ and these are the polynomials in g_2^3/Δ. They can be expressed in terms of j and this shows that the ring $\mathcal{R}^G$ is $\mathbb{Q}[j]$ where $j = 1728 \cdot g_2^3/\Delta$ and gives the ring of regular functions on $\mathbb{P}^1 \backslash \{\infty\}$. The inclusion $\mathbb{Q}[g_2, g_3] \subseteq \mathcal{R}^G$ defines a morphism

$$\mathbb{Q}^\times \backslash \mathcal{U} \longrightarrow \mathbb{P}^1 \backslash \{\infty\}$$

which is again (11).

Our next goal is to determine the endomorphism algebra of an elliptic curve E. Such an endomorphism is an endomorphism of $\mathbb{C}/\Lambda$ and so can be seen as an endomorphism $\varphi : \mathbb{C} \to \mathbb{C}$ with the property that $\varphi(\Lambda) \subseteq \Lambda$. An endomorphism φ of $\mathbb{C}$ is either zero or in $\mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^\times$ and then multiplication by some non-zero complex number ξ This means that $\varphi(\lambda) = \xi \cdot \lambda$ for any $\lambda \in \Lambda$. Since it is at the same time in $\mathrm{End}(\Lambda)$ we can represent φ, if not zero, by a matrix $\rho(\varphi) \in \mathrm{GL}(2, \mathbb{Z})$. From (5) we deduce after division by ω_2 that

$$\begin{aligned} \xi\tau &= a\tau + b \\ \xi &= c\tau + d \end{aligned}$$

and then that

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

---

with multiplicities) such that

$$j(q) = \sum_{-1}^{\infty} tr(1|V_n) q^n.$$

for 1 the neutral element of $\mathbb{M}$. The construction extends to any any element g of $\mathbb{M}$ and one obtains in general the so-called Thompson series

$$T_g(q) = \sum_{-1}^{\infty} \xi_n(g) q^n.$$

which leads to a quadratic equation

$$c\tau^2 + (d-a)\tau - b = 0 \tag{12}$$

for $\tau = \omega_2/\omega_1$. Clarly $c \neq 0$ if and only if this equation has two imaginary quadratic roots τ, $\bar{\tau}$ with exactly one lying in the half-plane $\mathfrak{H}^+$ and then the lattice takes up to isomorphism the shape $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Furthermore the endomorphism ξ is in $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. In this case we say that E has complex multiplication. Then ξ can be determined by the characteristic polynomial of $\rho(\xi)$ which is

$$T^2 - (a+d)T + ad - bc$$

and one sees that $\xi = c\tau + d$ is an algebraic integer. This shows that $\mathrm{End}(E) = \mathrm{End}(\Lambda_\tau)$ is an order, that is a subring of finite index in the ring of integers in $\mathbb{Q}[\tau]$. In general it differs from the ring of integers and the reason is that the lattice Λ_τ is only a module over $\mathbb{Z}$ and not necessarily an ideal. There is a small difference.
The ring can be determined in the following way. We consider the discriminant Δ of the equation (12). It is given by

$$(d-a)^2 - 4cb = (d+a)^2 - 4(ac - bd) = \mathrm{tr}\rho(\varphi)^2 - 4\det\rho(\varphi).$$

It depends on ξ and the chosen basis $1, \tau$ of the lattice. Since both, the trace and the determinant, are invariant under $\mathrm{SL}(2,\mathbb{Z})$ we find that Δ depends only on the lattice, not on the basis. If ψ is another endomorphism we get a second equation

$$c'\tau^2 + (d' - a')\tau - b' = 0 \tag{13}$$

for τ of the same form. Since both quadratic equations have the same roots τ and $\overline{\tau}$ we see that they must be proportional (since the minimal polynomial for τ is uniquely determined) and therefor both are multiples of the minimal polynomial. It follows that the discriminants differ only by a square.. This means that $\Delta = e^2\, D$ with D squarefree and independent of ξ, the discriminant $D(\tau)$ of $\mathbb{Q}(\tau)$. Then the ring of integers is

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\frac{D(\tau) - \sqrt{D(\tau)}}{2}$$

and the ring of endomorphisms is

$$\mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\frac{D(\tau) - \sqrt{D(\tau)}}{2}$$

with f the smallest among the numbers e introduced above.
If however $c = 0$ then we deduce that $\Im(d-a)\tau = 0$ which implies that $d = a$ and further that $b = 0$ whence $\rho(\xi) = a\,\mathrm{id}$. It follows that in this case the endomorphism algebra is $\mathbb{Z}$.

We now assume for the rest of this lecture that the curve E has complex multiplication by the ring of integers $\mathcal{O}$ in $\mathbb{Q}(\tau)$. We consider the class group of $\mathbb{Q}(\tau)$ which is by definition the group of fractional ideals modulo the subgroup of principal fractional ideals. [2] The order of the class group is the class number h_τ which is finite. It has been shown by Weber that the polynomial

$$\Phi(\tau) = \prod (T - j([\mathfrak{a}]))$$

[2] The set of ideals in $\mathcal{O}$ is a multiplicative monoid on which one introduces an equivalence relation. We say that $\mathfrak{a} \sim \mathfrak{b}$ if and only if there exist non-zero integers r and s in $\mathcal{O}$ such that $(r)\mathfrak{a} = (s)\mathfrak{b}$. The set of equivalence classes is the class group. The group structure comes from the relation $\mathfrak{a} \cdot \overline{\mathfrak{a}} = (N(\mathfrak{a}))$ which implies that $\mathfrak{a} \cdot \overline{\mathfrak{a}} \sim \mathcal{O}$.

with the product taken over all ideal classes of $\mathbb{Q}(\tau)$ is a polynomial of degree h_τ with coefficients in $\mathcal{O}$. It is monic and irreducible over $\mathbb{Q}(\tau)$ and this implies in particular that for imaginary quadratic τ the j-function takes values in the ring of integers of the field $\mathbb{Q}(\tau, j(\tau))$ which is a Galois extension of $\mathbb{Q}(\tau)$ with $[\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}(\tau)] = h_\tau$. A very deep theorem of Th. Schneider implies that τ and $\jmath(\tau)$ are both algebraic if and only if τ is imaginary quadratic. If this is the case then we call $j(\tau)$ a special point on the Shimura variety $\mathcal{S}_1$.

4 The Case $\mathbb{P}^1 \times \mathbb{P}^1$

The aim of this section is to take the basic Shimura varieties which has been obtained form lattices in $\mathbb{C}$ and study the surface $\mathbb{P}^1 \times \mathbb{P}^1$ which corresponds to the product of two copies of $X_0(\mathrm{SL}(2\mathbb{Z})$, see (11) and in different notation (9). The surface $\mathfrak{X} = X_0(\mathrm{SL}(2\mathbb{Z})) \times X_0(\mathrm{SL}(2\mathbb{Z}))$ can be written as the complement

$$\mathfrak{X} = \mathbb{P}^1 \times \mathbb{P}^1 - \{\infty\} \times \mathbb{P}^1 - \mathbb{P}^1 \times \{\infty\}$$

of a union of two projective lines and its special points are of the form $P = (J(\tau_1), J(\tau_2))$. A very interesting and conceptually new question is whether an algebraic curve $\mathcal{C}$ given by equations with coefficients in a number field k does contains infinitely many special points or not. Note that the special points on $\mathfrak{X}$ are dense even in the natural topology of $\mathfrak{X}$. The fields of definition of special points are $\mathbb{Q}(\tau_1, \tau_2)(J(\tau_1), J(\tau_2))$ and the degrees of these fields are unbounded. Our question asks for the existence of rational points on $\mathcal{C}$ in the compositum K of fields which has infinite degree over the rationals.
It turns out that the question can have totally different answers depending on the nature of the curve $\mathcal{C}$ and our first aim is to give an example of a curve in $\mathfrak{X}$ with infinitely many special points. This is done using the modular polynomial $\Phi_N(x, y)$ which has the property that it is irreducible and that $\Phi_N(j(\tau), j(N\tau)) = 0$. [3] Its degree is given by the Dedekind ψ-function and takes the value

$$\deg \Phi_N = \psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

and defines a curve $Y_0(N)$ in $\mathbb{A}^1 \times \mathbb{A}^1 \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1$. In the case $N = 1$ when $\Gamma_0(1) = \mathrm{SL}(2, \mathbb{Z})$ we simply have $Y_0(1) = \mathcal{S}_1$ with $\mathcal{S}_1$ defined in lecture 2 and then $Y_0(1) = \Gamma_0(1)\backslash\mathfrak{H}$. In the general case we get $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$ with

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}); c \equiv 0 \mod N \right\},$$

one of the famous congruence subgroups of $\mathrm{SL}(2, \mathbb{Z})$. From this description one sees that there is a holomorphic covering map $\pi_N : Y_0(N) \to Y_0(1)$ which explains in some sense the modular equation relating the points $j(\tau)$ and $j(N\tau)$. The curve $Y_0(N)$ is one of the famous modular curves and an algebraic model can be obtained by embedding the complex manifold $Y_0(N)$ using again modular forms. The curve is not compact but can be compactified and we then get an algebraic curve $X_0(N)$.

[3] The existence of a polynomial relation between $j(\tau)$ and $j(N\tau)$ is that the lattice $\Lambda_{N\tau}$ is a sublattice of the lattice Λ_τ with $\Lambda_\tau/\Lambda_{N\tau} \simeq \mathbb{Z}/N\mathbb{Z}$. The associated moduli space is then constructed from looking at pairs $(\Lambda_\tau, \Lambda_{N\tau})$ with $\Lambda_\tau/\Lambda_{N\tau} \simeq \mathbb{Z}/N\mathbb{Z}$. Going through the same procedure as we did with just lattices we get a new Shimura variety $\mathcal{S}_1(N)$. The functor which lets forget the sublattice $\Lambda_{N\tau}$ induces a covering $\mathcal{S}_1(N) \to \mathcal{S}_1$. This shows that the associated points $j(\tau)$ and $\jmath(N\tau)$ on the moduli spaces are related by an algebraic equation of degree the degree of the covering.

For each positive integer n we let $\mathrm{M}(N)$ be the set of all integer matrices $\delta = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right)$ matrices in $\mathrm{M}(2,\mathbb{Z})$ with $\det(\delta) = N$ and $M(N)^*$ the set of all primitive elements in $M(N)$, those with $(s,t,u,v) = 1$. Then writing Γ for $\mathrm{SL}(2,\mathbb{Z})$ we get

$$M^*(N) = \Gamma \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma \tag{14}$$

and a decomposition as a finite disjoint union

$$M^*(N) = \bigcup_{\alpha} \Gamma\,\alpha$$

into left cosets. As representatives we may take α of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad = N$ and $0 \leq b < d$. For short we write Γ for $SL(2\mathbb{Z})$ and define

$$\Gamma_\alpha = \Gamma \cap \left(\alpha \Gamma \alpha^{-1}\right)$$

and in the case of $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ one gets in particular $\Gamma_0(N)$. It is not so difficult to compute the index in Γ as $\psi(N) = [\Gamma : \Gamma_0(N)]$ (see [4], Prop. 9.3). Furthermore any two of the subgroups Γ_α are conjugate. This is because of the decomposition (14) of $M^*(N)$ as double coset which allows to wriite α as $\delta\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\epsilon$ with δ and ϵ in Γ and we deduce that $\alpha\Gamma\alpha^{-1}$ is conjugate to $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. Intersecting with Γ gives the claim.

For each representative α in the coset decomposition we define an embedding

$$\begin{array}{rcl} \Delta_\alpha : \mathfrak{H} & \longrightarrow & \mathfrak{H} \times \mathfrak{H} \\ \tau & \longmapsto & \Delta_\alpha(\tau) = (\tau, \alpha\tau) \end{array}$$

which is compatible with the action of Γ_α through the embedding

$$\begin{array}{rcl} \iota_\alpha : \Gamma_\alpha & \longrightarrow & \Gamma_\alpha \times \Gamma_\alpha \subseteq \Gamma \times \Gamma \\ \gamma & \longmapsto & (\gamma, \mathrm{ad}(\alpha)\gamma) \end{array}$$

which is a homomorphism as one can easily verify. To see the compatibility we calculate as follows: Let γ be in Γ_α. Then

$$\alpha(\gamma\tau) = (\alpha\gamma\alpha^{-1})\alpha\tau = (\mathrm{ad}(\alpha)\gamma)\alpha\tau$$

This implies that

$$\begin{array}{rcl} \Delta_\alpha(\gamma\tau) & = & (\gamma\tau, \alpha\gamma\tau) \\ & = & (\gamma\tau, (\mathrm{ad}(\alpha)\gamma)\alpha\tau) \\ & = & \iota_\alpha(\gamma)(\tau, \alpha\tau) \\ & = & \iota_\alpha(\gamma)\Delta_\alpha(\tau) \end{array}$$

and we deduce that Δ_α descends to a totally geodesic map

$$\iota_\alpha : \mathcal{S}_\alpha = \mathfrak{H}/\Gamma_\alpha \to \mathfrak{X} = \mathfrak{H} \times \mathfrak{H}/\Gamma \times \Gamma \tag{15}$$

from the Shimura curve $\mathcal{S}_\alpha$ to the Shimura variety $\mathfrak{X}$.

As before the Riemann surface $\mathcal{S}_\alpha$ has a algebraic model $Y(\Gamma_\alpha))$ and on it there are infinitely many special points. This shows that the question may have an unexpected answer. One would rather have expected that such a set of points should be finite. The construction shows that one has to avoid totally geodesic subvarieties. If one does then one gets the following theorem obtained by André which settles the Andé-Oort conjecture in the case of the Shimura variety $\mathfrak{X}$.

Theorem 4.1 (André). *Let $\iota : \mathcal{C} \to \mathfrak{X}$ be a curve defined over a number field and assume that the curve contains infinitely many special points. Then $\mathcal{C}$ is one of the totally geodesic subvarieties constructed above.*

As already mentioned the first proof was given by André in 1990 and we give now a short sketch of the proof by explaining the main ideas. If the curve is not already defined over $\mathbb{Q}$ we may replace it by the union of its conjugates and therefor may assume that it is defined over $\mathbb{Q}$. Under the obvious hypothesis that the curve is not contained in the boundary $\{\infty\} \times \mathbb{P}^1 - \mathbb{P}^1 \times \{\infty\}$ we considers the intersection of the curve with the boundary. If there are infinitely many special points on the curve they have a boundary point as a limit point. Since the curve and the boundary are defined over a number field the intersection points have coordinates in an algebraic number field. We call P_∞ a limit point and $P_n = (j(\tau_n), j(\tau_n'))$ a subsequence of the rational points on $\mathcal{C}$ converging to P_∞ and with τ_n, τ_n' both imaginary quadratic. Using class field theory and replacing the sequence possibly by a subsequence it is shown that the discriminants D_n, D_n' of the imaginary quadratic number fields associated with τ_n, τ_n' and with n large enough generate the same field and furthermore that he quotient D_n'/D_n takes a value which is independent of n for infinitely many n. At least one of the component of $P_\infty = (P_{\infty_1}, P_{\infty_2})$, say the first, has to be ∞. We put $\tau_n = s_n + it_n$ and deduce from the Fourier expansion (10) given in Lecture 3 that the numbers $j_n = j(\tau_n)$ satisfy

$$\log |j_n| \approx 2\pi t_n. \tag{16}$$

Furthermore we may assume that τ_n is in the fundamental domain and this implies that $t_n \geq \sqrt{2}/2$. On writing $\tau_n = \left(b_n + \sqrt{D_n}\right)/2a_n$ we find that $a_n \leq \sqrt{-D_n/2}$.
The next step in the proof is to show that $P_\infty = (\infty, \infty)$, the intersection of the two boundary divisors $\{\infty\} \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{\infty\}$. If not we could assume w.l.g. that $P_\infty = (\infty, j')$. Let

$$F(x, y) = 0 \tag{17}$$

be the equation for the curve $\mathcal{C}$. The rational transformation $(u, v) = (x^{-1}, y - j')$ gives an equation

$$G(u, v) = 0$$

for the curve such that $G(0, 0) = F(\infty, j') = 0$. In a neighborhood of $(0, 0)$ the curve decomposes into a finite number of connected analytic components which we can parametrize by Puisseux series, that is power series in X^ρ for rational $\rho \in (0, 1)$. We take the branch $v \approx u^\rho$ with $|j_n' - j'| \approx |j_n^{-\rho}|$ to deduce from (16) that

$$|j_n' - j'| \approx e^{-2\pi\rho\, t_n}.$$

Using again Fourier we get

$$|j_n' - j'| \approx |e^{2\pi i \tau_n} - e^{2\pi i \tau'}| \approx |\tau' - \tau_n'|$$

where τ' is choosen so to satisfy $j' = j(\tau')$. The last two approximations taken together lead to

$$|\tau' - \tau_n'| \approx e^{-2\pi\rho\, t_n}. \tag{18}$$

We may assume that $\tau' \neq \tau_n'$ for infinitely many n. Otherwise the curve has infinitely many points with second coordinate j' and this implies that the curve is $\mathbb{P}^1 \times \{j'\}$. By Schneider's theorem τ' must be transcendental since $j(\tau')$ is an intersection point of two curves defined over $\overline{\mathbb{Q}}$ and so is algebraic. In this case we write $\tau' = \omega_2'/\omega_1'$ and rewrite (18) as

$$|\omega_1' - \tau_n'\omega_2'| \approx |\omega_2'|\, e^{-2\pi\rho\, t_n}.$$

This is a linear form in two elliptic logarithms with algebraic coefficients and by a quantitative version of the Analytic Subgroup Theorem of Wüstholz [13] worked out by Hirata-Kohno [12] the logarithm of the absolute value of the linear form is $\gg -\sqrt{|D_n|}$, a contradiction. It follows that we made a wrong assumption and this means that $j' = \infty$ which proves our claim that $P_\infty = (\infty, \infty)$.

It remains to show that the points $P_n = (j(\tau_n), j(\tau_n'))$ are zeroes of some modular equation $\Phi_n(X,Y)$. To do so we consider a lattice of the form $\mathbb{Z} + \mathbb{Z}\tau$ with τ imaginary quadratic. The minimal polynomial $aT^2 + bT + c$ for τ can be normalized such that $|b| \leq a \leq c$. Then

$$\tau = \frac{b + \sqrt{D}}{2a}$$

with discriminant $D = b^2 - 4ac = f^2 d$ for square-free d. The order of the lattice becomes

$$\mathcal{O} = \mathbb{Z} + \frac{D + \sqrt{D}}{2}\mathbb{Z} = \mathbb{Z} + f\frac{d + \sqrt{d}}{2}\mathbb{Z}$$

and its index in $\mathcal{O} = \mathbb{Z} + \frac{d+\sqrt{d}}{2}\mathbb{Z}$ is f. Here we have used that $f^2 d \equiv fd \mod 2$.

We apply now the same type of asymptotics argument which were leading to (18). Since now also $j' = \infty$ we make the substitution $s = x^{-1}, t = y^{-1}$ which transforms (17) into an equation

$$H(s,t) = 0$$

around $(0,0)$ satisfied by infinitely many $P_N = (j(\tau_N)^{-1}, j(\tau_N')^{-1})$. As before we use Puiseux to see that

$$|j(\tau_N')^{-1} - j(\tau_N)^{-\rho}| \ll e^{-2\pi\rho\sqrt{D_N}}$$

which gives

$$|\tau_N' - \rho\,\tau_N| \ll e^{-2\pi\rho\sqrt{D_N}}.$$

This implies that $D_N \approx D_N'$ which we use to deduce by Liouville that if $\tau_N' \neq \rho\,\tau_N$ then

$$|\tau_N' - \rho\,\tau_N| \gg |D_N|^{-2},$$

a contradiction. This shows that with $0 \leq \rho = \frac{r}{s} \leq 1$ we get $\tau_N' = \rho\,\tau_N$ or, in other words, that

$$\tau_N' = \left(\begin{smallmatrix} r & 0 \\ 0 & s \end{smallmatrix}\right)\tau_N. \tag{19}$$

and we see that the curve is contained in the image of $\iota_{n,\delta}$ for $\delta = \left(\begin{smallmatrix} r & 0 \\ 0 & s \end{smallmatrix}\right)$ and $n = \det\delta$.

5 Abelian Surfaces and their Moduli Space

We turn now to the generalization of the elliptic theory to abelian surface. We already met the special case of a product of two elliptic curves which were classified by the product $\mathbb{P}^1 \times \mathbb{P}^1$. We repeat the construction briefly in the general case of an abelian surface and begin with lattices of rank 4 instead of rank two. The situation becomes slightly more complicated than in the elliptic set-up. We cannot just take a lattice because that would not lead to a nice space. Instead we have to consider triples $(\Lambda, J, E,)$ with Λ a lattice of rank 4, with $J \in \mathrm{End}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R})$ satisfying $J^2 = -\mathrm{id}$ and with $E : \Lambda \times \Lambda \to \mathbb{Z}$ a skew-symmetric form with $E = (J \times J)^* E$ such that if V denotes the space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ then the associated hermitian form

$$\begin{aligned} H : \mathrm{V} \times \mathrm{V} &\longrightarrow \mathbb{C} \\ H(v, w) &= E(Jv, w) + iE(v, w) \end{aligned}$$

is positive definite. We call such a triple a polarized lattice. It is called principally polarized if $\det(E) = 1$. In the case of lattices of rank 2 which we were studying in the first lectures the extra conditions are automatically satisfied and therefore did not become visible.

Remark : Polarized lattices arise naturally in geometry. If X is a smooth projective curve then the homology group $H_1(X, \mathbb{Z})$ is a polarized lattice. The skew-symmetric form E on $H_1(X, \mathbb{Z})$ is defined by taking the intersection of cycles and the elementary divisor theorem for skew-symmetric forms give a symplectic basis $e_1, \ldots, e_n, f_1, \ldots, f_n$. We then define $J \in GL_{2n}(\mathbb{Z})$ by $J(e_i) = f_i$ and $J(f_i) = -e_i$. It satisfies $J^2 = -1$ and $E(Ju, Jv) = E(u, v)$ and therefore $(H_1(X, \mathbb{Z}), J, E)$ is a principally polarized lattice. □

We can now proceed along the same lines as in the elliptic case and introduce the space $\mathcal{L}_2$ of polarized lattices of rank 4. The space $\mathcal{L}_1 \times \mathcal{L}_1$ injects into $\mathcal{L}_2$. In this case Igusa has introduced the analogues j_1, j_2, j_3 of the modular function j with the analogous properties with the difference that they have poles along $\mathcal{L}_1 \times \mathcal{L}_1$. Again they can be introduced via Eisenstein series (see [1]). Working out the symmetries on $\mathcal{L}_2$ one gets a representation of isomorphism classes of polarized lattices in terms of algebraic groups. The group $\mathrm{GL}(2, \mathbb{R})$ is replaced by the group of symplectic similitudes $\mathrm{GSp}(2, \mathbb{R})$ which have the property that if γ is one of its elements then

$$E(\gamma v, \gamma w) = m(\gamma) E(v, w)$$

for some multiplier $m(\gamma) \in \mathbb{Z}$ and $\mathrm{SL}(2, \mathbb{Z})$ becomes the symplectic group $\Gamma = \mathrm{Sp}(4, \mathbb{Z})$. The result is a Shimura variety $\mathcal{S}_2$.

Exercise. Fill in the deatails.

The analog of the upper half-plane becomes the Siegel upper half-plan[4] defined as

$$\mathfrak{H}_2 = \{\tau \in M_2(\mathbb{C}); \tau = {}^{\intercal}\tau, \Im(\tau) \text{ positive definite}\} \tag{20}$$

with an action of Γ given by

$$(\gamma, \tau) \in \Gamma \times \mathfrak{H}_2 \mapsto (a\tau + b)(c\tau + d)^{-1}.$$

for

$$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma, \quad a, b, c, d \in \mathrm{M}_2(\mathbb{R}).$$

[4]To give an explicit description for the space we write $\tau \in \mathfrak{H}_2$ as $\left(\begin{smallmatrix} u & w \\ w & u \end{smallmatrix}\right)$ and $\Im\tau$ as $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ and then the associated quadratic form is positive definite if and only if the discriminant $D(\tau) = \det(\Im\tau) = b^2 - 4ac$ is positive. As a consequence the Siegel upper halfplane becomes the affine 3-space with the real cone $D(\tau) \leq 0$ removed.

It is clear that the product $\mathfrak{H} \times \mathfrak{H}$ embeds into $\mathfrak{H}_2$. The embedding is again compatible with the action of the modular groups and gives an embedding

$$\iota : \mathrm{SL}(2,\mathbb{Z})\backslash\mathfrak{H} \times \mathrm{SL}(2,\mathbb{Z})\backslash\mathfrak{H} = \mathrm{SL}(2,\mathbb{Z}) \times \mathrm{SL}(2,\mathbb{Z})\backslash\mathfrak{H} \times \mathfrak{H} \longrightarrow \mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}.$$

Here we have obtained another example of a so-called modular embedding

$$\iota : \mathcal{S}_1 \times \mathcal{S}_1 \longrightarrow \mathcal{S}_2$$

of a Shimura variety of dimension 2 into a Shimura variety of dimension 3.

The definition of the functions j_1, j_2 and j_3 relies on Eisenstein series for the group $\mathrm{Sp}(4,\mathbb{Z})$. They are defined as

$$E_{2k}(\tau) = \sum_{c,d} \det(c\tau + d)^{-2k} \tag{21}$$

with the sum over all inequivalent bottom rows (c,d) with respect to left multiplication by $\mathrm{SL}(2,\mathbb{Z})$ taken from the set $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and with $\tau \in \mathfrak{H}_2$.
We define

$$\begin{aligned} \chi_{10} &= -43867 \cdot 2^{-12} \cdot 3^{-5} \cdot 5^{-2} \cdot 7^{-1} \cdot 53^{-1}(E_4E_6 - E_{10}) \\ \chi_{12} &= 131 \cdot 593 \cdot 2^{-13} \cdot 3^{-7} \cdot 5^{-2} \cdot 7^{-2} \cdot 337^{-1}\left(3^2 \cdot 7^2 E_4^3 + 2 \cdot 5^3 E_6^2 - 691 E_{12}\right) \end{aligned}$$

and then the Igusa modular functions become

$$j_1 = 2 \cdot 3^5 \frac{\chi_{12}^5}{\chi_{10}^6}, \quad j_2 = 2^{-3} \cdot 3^3 \frac{E_4\chi_{12}^3}{\chi_{10}^4} \quad j_3 = 2^{-5} \cdot 3 \frac{E_6\chi_{12}^2}{\chi_{10}^3} + 2^{-3} \cdot 3^2 \frac{E_4\chi_{12}^3}{\chi_{10}^4}.$$

The Igusa functions induce an rational map

$$\begin{aligned} j : \mathfrak{H}_2 &\longrightarrow \mathbb{P}^3 && (22) \\ \tau &\mapsto (j_1(\tau) : j_1(\tau) : j_1(\tau) : 1). && (23) \end{aligned}$$

which factors through the quotient

$$J : \mathcal{S}_2 \simeq \Gamma\backslash\mathfrak{H}_2 \longrightarrow \mathbb{P}^3.$$

and contracts the image of ι to a point.

The Igusa functions have a Fourier expansion which can be written as

$$\sum_T a(T) \exp\left(2\pi i \mathrm{tr}(T\tau)\right)$$

where the summation is over all symmetric and half-integer matrices $T = \left(\begin{smallmatrix} a & b/2 \\ b/2 & d \end{smallmatrix}\right)$ with integer coefficients a, b, c. The $a(T)$ are zero unless the quadratic form attached to T is positive semi-definite. This has been discovered by Köcher. It is very interesting for us to notice that the Fourier expansion of the modular form χ_{10} which defines the boundary of $\mathcal{S}_2$ takes the form

$$\chi_{10} \sim q_1q_2q_3\left(1 + \epsilon(q_1,q_2,q_3)\right)$$

with ϵ having only non-zero terms of degree at least 1.

With a principally polarized lattice Λ we can associate a complex torus $\mathbb{C}^2/\Lambda$ which is a compact complex manifold with the structure of a projective algebraic variety, the 2-dimensional analogue of an elliptic curve. The situation here is very similar to the elliptic case since there is a second interpretation of this moduli space as the moduli space of hyperelliptic curves of genus 2 given by an equation of the form

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)(x-\lambda_4) \tag{24}$$

with $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{A}^4$. The curve is non-singular provided that the discriminant Δ is non-zero. The zero locus $\Delta = 0$ of the discriminant is an arrangement of hyperplanes and we are in a similar situation as for elliptic curves. We do not follow further the point of view since one has to go into the theory of invariants of quintics and sextics. [5]
On the algebraic side there is the moduli space of principally polarized abelian surfaces $\mathcal{M}_2$. By a certain "blow-upo" construction [2] and [3] the moduli variety $\mathcal{A}_2$ and an embedding

$$J : \Gamma\backslash\mathfrak{H}_2 \hookrightarrow \mathcal{A}_2$$

are obtained. It has the property that it contains $\mathbb{P}^1 \times \mathbb{P}^1$ as a Shimura subvariety.

6 Albert's Classification and the Zoo of Shimura Varieties of low Dimension

In our last section we shall make an excursion into the Zoo of Shimura subvarieties of the Siegel space $\gamma\backslash\mathfrak{H}_2$. We shall construct in a very elementary way an infinite collection of species of

[5][**not yet complete**] Igusa considers the generic sextic

$$Y^2 = u_0x^6 + u_1x^5 + \cdots + u_5x + u_6 \tag{25}$$

with u_0, u_1,..., u_1 independent variables. which can be written in the form

$$Y^2 = u_0 \cdot \prod_1^6 (x - x_i).$$

There are four homogeneous polynomials $A(u)$, $B(u)$, $C(u)$ and $D(u)$ in the coefficients of the equation ([**?**]) with $D(u)$ the discriminant of the equation in u which are used to introduce

$$J_2 = 2^{-3}A, \quad , J_4 = 2^{-5}3^{-1}(4J^2 - D), \quad J_6 = 2^{-6}3^{-2}(8J_2^3 - 160J_2J_4 - C), \quad J_{10} = 2^{-12}D.$$

and it can be seen that

$$\mathbb{Z}[J] = \mathbb{Z}[J_2, J_4, J_6, J_{10}^{\pm}] = K[x_1, x_2, x_3, x_5^{\pm}]/(x_1x_3 - x_2^2 - 4x_4).$$

We put the weight i on the J_i for $1 \leq i \leq 4$, on J_{10} the weight 5 and denote by $\mathcal{R}$ the subring consisting of the elements of degree 0. Then

$$Proj\,\mathcal{R}$$

contains as an open subset $\mathcal{U}$ which is birationally equivalent to the moduli space $\mathcal{M}_2$ for hyperelliptic curves of genus 2 which coincides with the moduli space of abelian surfaces.

The elements

$$J_2^5 J_{10}^{-1}, \quad J_4^3 J_{10}^{-2}, \quad J_6^5 J_{10}^{-3}$$

in $\mathcal{R}$ are algebraically independent and invariant under the action of the group μ_5 of 5th roots of unity given by $J_i \mapsto \zeta^i J_i$ for some primitive 5th root of unity ζ and therefor isomorphic to the invariants $\mathbb{Q}[y_1, y_2, y_3]^{\mu_5}$ in $\mathbb{Q}[y_1, y_2, y_3]$ under the action $y_i \mapsto \zeta^i y_i$.

Shimura subvarieties. This can be done just by some linear algebra starting from polarized lattices as defined in lecture 5. The central point in the construction is the endomorphism algebra of a polarized lattice which we shall now going to introduce.
We say that a homomorphism $\varphi : \Lambda \to \Lambda'$ of lattices is a homomorphism between polarized lattices (λ, J, E) and (λ', J', E') if and only if $\varphi \circ J = J' \circ \varphi$ and if $E'(\varphi(u)\varphi(v)) = \lambda(\varphi)E(u,v)$ fur all $u, v \in \Lambda$ and some $\lambda(\varphi) \in \mathbb{Z}$ for some $\lambda : Hom(\Lambda \otimes_{\mathbb{Z}} \Lambda', \mathbb{Z}$ with the property that if $\Lambda = \Lambda'$ then χ is induced from a character of $\mathrm{End}(\Lambda)^t imes$. A homomorphism $\varphi : \Lambda \to \Lambda'$ is called an isogeny if it is surjective and has finite kernel. It is easy to see that the category of polarized lattices is semi-simple up to isogeny. This means that up to isogeny every projector $\pi : \Lambda \to \Lambda'$ has an orthogonal complement. Therefor any polarized lattice is isogenous to a finite product of polarized lattices which are simple. We now restrict ourselves to the simple case. In this case as one may again easily verify that the endomorphism algebra $\mathrm{End}^0((\lambda, J, E)) := \mathrm{End}((\lambda, J, E)) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra or in other terms a skew field.
An example for a division algebra are the Hamiltonian quaternions. This is a vector space $\mathbb{H}$ of dimension 4 and generated by elements 1, i, j and k and with algebra structure defined by

$$i^2 = -1 = j^2, \;\; ij = k = -ji.$$

This example has been generalized to get quaternion algebras. This is a vector space $\mathcal{Q}$ over a field K which we assume to have characteristic zero and which is generated by elements 1, i, j and k and with algebra structure given by

$$i^2 = a, j^2 = b, \;\; ij = k = -ji.$$

for a b in K. Depending on the field K and on a, b the algebra obtained is either a division algebra or the matrix algebra $M_2(k)$. Over the reals according to Frobenius the only possibilities are $\mathbb{H}$ or $M_2(\mathbb{R})$. If the field k can be injected into the reals then $\mathcal{Q} \otimes_k \mathbb{R}$ is a quaternion algebra over the reals and the alternatives from above apply. In the first case we say that $\mathcal{Q}$ is definite and in the second case that it is indefinite. Quaternion algebras turn up in the classification we are going to give.
Coming back to the polarized lattice we introduce $V = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ and canonically identify $\mathrm{End}_{\mathbb{Q}}(V)$ with $V^\vee \otimes_{\mathbb{Q}} V$ via $v^\vee \otimes v \mapsto t : v \mapsto v^\vee(v)$ for $v \in V, v^\vee \in V^\vee$. Then we define a trace map

$$\begin{aligned} \mathrm{tr} : \mathrm{End}^0((\lambda, J, E)) &\longrightarrow \mathbb{Q} \\ v^\vee \otimes v &\mapsto v^\vee(v) \end{aligned}$$

We assume that the lattice has a principal polarization and use this to obtain an isomorphism $\iota : V \tilde{\longrightarrow} V^\vee$ which maps v to $\iota(v) : w \mapsto E(v, w)$. Then the map $f \mapsto \iota^\vee \circ f^\vee \circ \iota$ with $f^\vee, \iota^\vee$ dual to f, ι gives an involution $f \mapsto f^\dagger$ on $\mathrm{End}^0((\lambda, J, E))$ called *Rosati involution.* It satisfies $(fg)^\dagger = f^\dagger g^\dagger$ and $\left(f^\dagger\right)^\dagger = f$ and is, as can be shown, a positive involution in the sense that the symmetric bilinear form $(f, g) \mapsto \mathrm{tr}(fg^\dagger)$ is positiv definite. Let K be the center of $\mathrm{End}^0((\Lambda, J, E))$ and K_0 be the subfield $\{k \in K; k^\dagger = k\}$. Then K_0 is totally real and either $K = K_0$ or an imaginary quadratic extension of K_0.

For the rest of the section we specialize to the case of a lattice of rank 4 which corresponds via the Riemann Existence theorem to abelian surfaces. We are going now to give the classification of the possible endomorphism algebras $\mathrm{End}^0((\Lambda, J, E))$ which appear in this situation:

Type I: $\mathbb{Z}$,

Type II: $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot f(D + \sqrt{D})/2$ with $0 \neq f \in \mathbb{Z}$, $K = \mathbb{Q}(\sqrt{D})$, $D > 0$ squarefree,

Type III: an order in an indefinite quaternion algebra over $\mathbb{Q}$,

Type IV: an order in a quartic CM-field $K \supset K_0 \supset \mathbb{Q}$.

Each of the types II, III, IV contains infinitely many algebras and for each type and each Φ in one of these families in the type there is is a moduli space $\mathcal{M}_\Phi$ of abelian surfaces $A_\Lambda = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}/\Lambda$ with $\mathrm{End}\left((\Lambda, J, E)\right) \supseteq \Phi$. The dimensions are 3 for Type I, 2 for Type II, 1 for Type III and 0 for IV. There is a natural ordering on the set of types with $I \leq II \leq III$ and $I \leq II \leq IV$ which carries over naturally to the $\mathcal{M}_\Phi$ with reversed ordering. The $\mathcal{M}_\Phi$ represent the Φ-species. The latter we call Φ-special. In the case of Type IV are the CM-points. This leads us to state the general conjecture of the type André-Oort:

Conjecture 6.1. *The Zariski closure of any set Σ of special subvarieties of $\mathcal{M}_2$ is a finite union of special subvarieties.*

This conjecture seems to be open even in the case when the set Σ consists of special points. It also covers the case of so-called Hilbert modular surfaces which were very intensively studied in the 80ies by Hirzebruch and Zagier. Hilbert modular surfaces are Shimura subvarieties of the moduli space of abelian surfaces which was discussed in lecture 5
To define Hilbert modular surfaces we fix a real quadratic number field $K = \mathbb{Q}(\sqrt{d})$ with d square-free. The discriminant D of K is

$$d = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4, \\ 4d, & \text{if } d \equiv 2, 3 \pmod 4. \end{cases} \tag{26}$$

We write $\omega = (D + \sqrt{D})/2$ and then the ring of integers of K is

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega.$$

There are two real embeddings σ_1 and σ_2 of F into $\mathbb{R}$. We define the Hilbert Modular group as

$$\Gamma_K = \mathrm{SL}_2(\mathcal{O}).$$

for which we have an embedding

$$\Gamma \hookrightarrow \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R}) \tag{27}$$

$$\gamma \mapsto (\gamma^{\sigma_1}, \gamma^{\sigma_2}) \tag{28}$$

and which acts on $\mathfrak{H} \times \mathfrak{H}$ as

$$\gamma(z, w) = (\gamma^{\sigma_1} z, \gamma^{\sigma_2} w)$$

The quotient $\mathcal{H} = \Gamma \backslash \mathfrak{H} \times \mathfrak{H}$ is called Hilbert Modular surface. It is a Shimura variety of dimension 2 and a subvariety of $\mathcal{S}_2$ and the moduli space of abelian surfaces with endomorphism algebra $\mathcal{O}$.
In [10] Mok studied totally geodesic subvarieties of Ball quotients and he proves the conjecture in this case. It would be very interesting to see whether the arithmetic part can also be proved. As a special case we have the Picard modular surfaces studied very carefully by Holzapfel in the 80ies.
Another question is whether one can prove à la Mok the geometric part when all $\sigma \in \Sigma$ have dimension at least 1. For the arithmetic case there is some hope since we consider it as not impossible to deal with it along the lines given by Kühne in his work on $\mathbb{P}^1 \times \mathbb{P}^1$ by looking very carefully at the Igusa moduli space.

References

[1] Reinier Bröker, Kristin Lauter, Modular Polynomials of Genus 2, LMS J. Comput. Math. **12** (2009), 326-339.

[2] J.-I. Igusa, Arithmetic Variety of Moduli for Genus Two, Ann. of Math. **72** (1960), 612-649).

[3] J.-I. Igusa, On Siegel Modular Forms of Genus Two, Am. J. Math, **84** (1962), 175-200.

[4] A. Knapp, Elliptic curves, Mathematical Notes, Princeton Univ. Press (1992).

[5] L. Kühne, The André-Oort Conjecture in $\mathbb{C}^2$, Master Thesis ETHZ (2009).

[6] L. Kühne, An effective result of André-Oort type I, to appear in Ann. Math. (2)

[7] L. Kühne, An effective result of André-Oort type II, submitted.

[8] J. S. Milne, Introduction to Shimura Varieties (2004).

[9] J. S. Milne, Modular Functions and Modular Forms (2009).

[10] N. Mok, On the Zariski Closure of a Germ of Totally Geodesic Complex Submanifold on a Subvariety of a Complex Hyperbolic Space Form of Finite Volume., Complex Analysis - Trends in Mathematics, 279-300, (2010).

[11] J. Silverman, Elliptic curves, Springer Graduate Texts.

[12] D. Sinnou, N. Hirata-Kohno, Linear forms in elliptic logarithms, J. Reine Angew. Math. **628** (2009), 37-89.

[13] G. Wuštholz, Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen, Ann. Math. **129** (1989), 501-517.